UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE	**IT00302/IT08X32** Critical Information Infrastructure Protection
CAMPUS	**APK**
EXAM SSA	**JANUARY 2017**

ASSESSORS:	MR SMA MAVEE MR JL DU TOIT
MODERATOR:	PROF KRITZINGER
DURATION: 120 MINUTES	**MARKS:** 100

PLEASE TAKE CAREFUL NOTE OF THE FOLLOWING:

1. Answer **ALL** questions **ONLY** in the supplied **ANSWER SHEET**.

2. **Do NOT write in pencil**. **Anything in pencil WILL NOT BE MARKED**.

3. Write neatly and legibly.

4. Answers must pertain to the material covered during the course of the module.

5. **NO** calculators may be used.

6. This question paper consists of 4 (including this cover page) pages.

7. This question paper consists of 7 question sections.

QUESTION 1

1.1 Briefly discuss Critical Infrastructure. Include in the following in your discussion: **(8)**

- A definition of the term "Critical Infrastructure",
- Three examples of Critical Infrastructure sectors, and
- An explanation of how each of your listed examples can be classified as Critical Infrastructure.

1.2 List four potential consequences that can come from successful Critical Infrastructure attacks. **(4)**

1.3 List four goals of Critical Information Infrastructure Protection (CIIP) programmes. **(4)**

[16]

QUESTION 2

2.1 Name and briefly discuss four characteristics exhibited by Critical Information Infrastructure. **(8)**

2.2 Challenges in the CIIP field generally come from the assets used, vulnerabilities they face and countermeasures used. List six challenges generally faced in the Critical Information Infrastructure Protection field. **(6)**

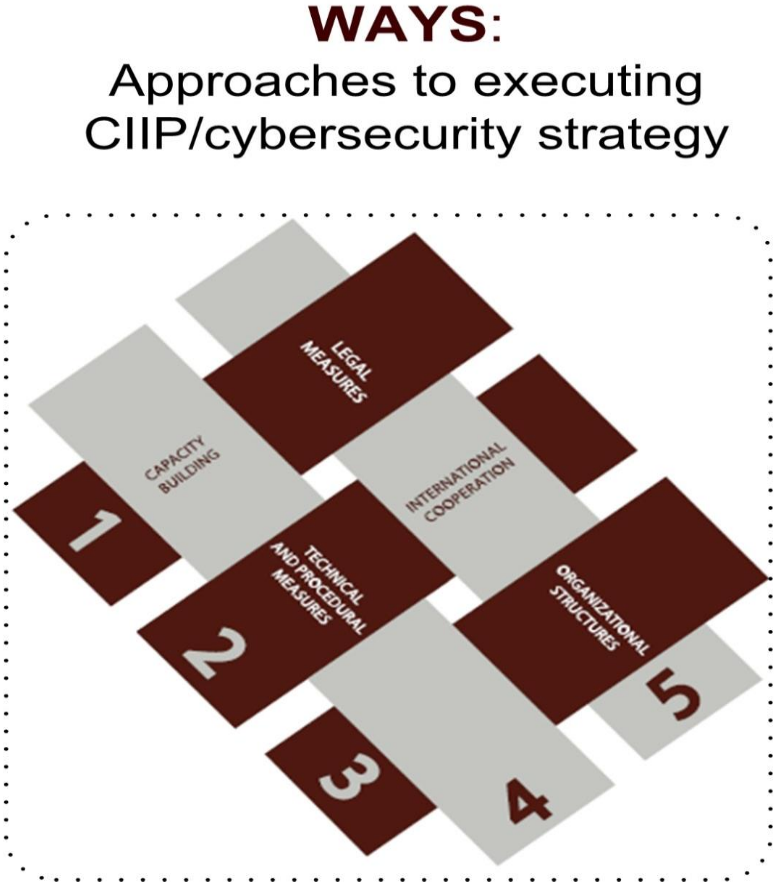
[14]

QUESTION 3

The International Telecommunication Union (ITU) agency, prescribed a holistic CIIP and Cybersecurity Strategy Model that can be used when defining policies for countries. The diagram below shows five of the approaches that can be followed to execute a successful CIIP or Cybersecurity strategy in a country.

In your own words, briefly discuss how the following three approaches can be used by a nation's government to create enable an appropriate CIIP/Cybersecurity strategy:

- Capacity Building,
- Organisational Structures, and
- Technical and Procedural Measures.


WAYS:
Approaches to executing CIIP/cybersecurity strategy
LEGAL MEASURES
CAPACITY BUILDING
INTERNATIONAL COOPERATION
TECHNICAL AND PROCEDURAL MEASURES
ORGANIZATIONAL STRUCTURES
1
2
3
4
5

[6]

QUESTION 4

As an aspect of good governance, it is often advisable that public-private partnerships be establish to run critical infrastructure. Briefly discuss private-private partnerships in critical infrastructure. Include in your discussion:

- A definition of public-private partnerships as explained in South African law,
- The value that such partnerships add to critical infrastructure,
- Factors that contribute to a Public-Private Partnerships' success,
- Challenges that Public Private Partnerships in South Africa face, and
- Cybersecurity points of concern that Public Private organizations need to address.

[14]

QUESTION 5

5.1 Name and describe the four high-level design principles software developers are encouraged to consider, when designing more secure software. **(8)**

5.2 Briefly describe the principle of variable depth security **(2)**

5.3 Briefly describe why "Foreign Influence" is a concern in supply chain risk management **(3)**

5.4 Describe the role of the Cyber Command, as defined by the Cybercrimes and Cyber Security Bill **(2)**

5.5 Describe why Information Assurance is an important aspect of a country's critical information infrastructure **(2)**

[17]

QUESTION 6

Supervisory Control and Data Acquisition (SCADA) is a control system that interact with various components on an industrial network. A SCADA industrial network can easily contain at least eight (8) different components.

List and describe the various components that can be found in a SCADA industrial network.

[13]

QUESTION 7

Utopia Government has been experiencing an unprecedented increase in cyber-attacks on their critical information infrastructure. The President of Utopia, Ronald Drum, has contracted your company to write and present a report on the different offensive aspects of cyber warfare.

Prepare and write a report that covers **offensive** aspects of cyberwarfare. DO NOT include preparation or defensive aspects, keep the focus on offensive aspects. Make sure to cover all aspects under offensive strategies, not just the tools that is available in a cyberwarfare attack.

Structure your report logically to ensure easy readability using good report writing techniques.

Marks are awarded as follows:

Neatness and readability	**(4)**
Content	**(16)**

[20]

TOTAL: 100 MARKS