



## FACULTY OF SCIENCE

### ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

<b>MODULE</b>	<b>IT00302/IT08X32</b> Critical Information Infrastructure Protection
<b>CAMPUS</b>	<b>APK</b>
<b>EXAM</b>	<b>NOVEMBER 2016</b>

**ASSESSORS:**

MR SMA MAVEE  
MR JL DU TOIT

**MODERATOR:**

PROF KRITZINGER

**DURATION:** 120 MINUTES

**MARKS:** 100

---

**PLEASE TAKE CAREFUL NOTE OF THE FOLLOWING:**

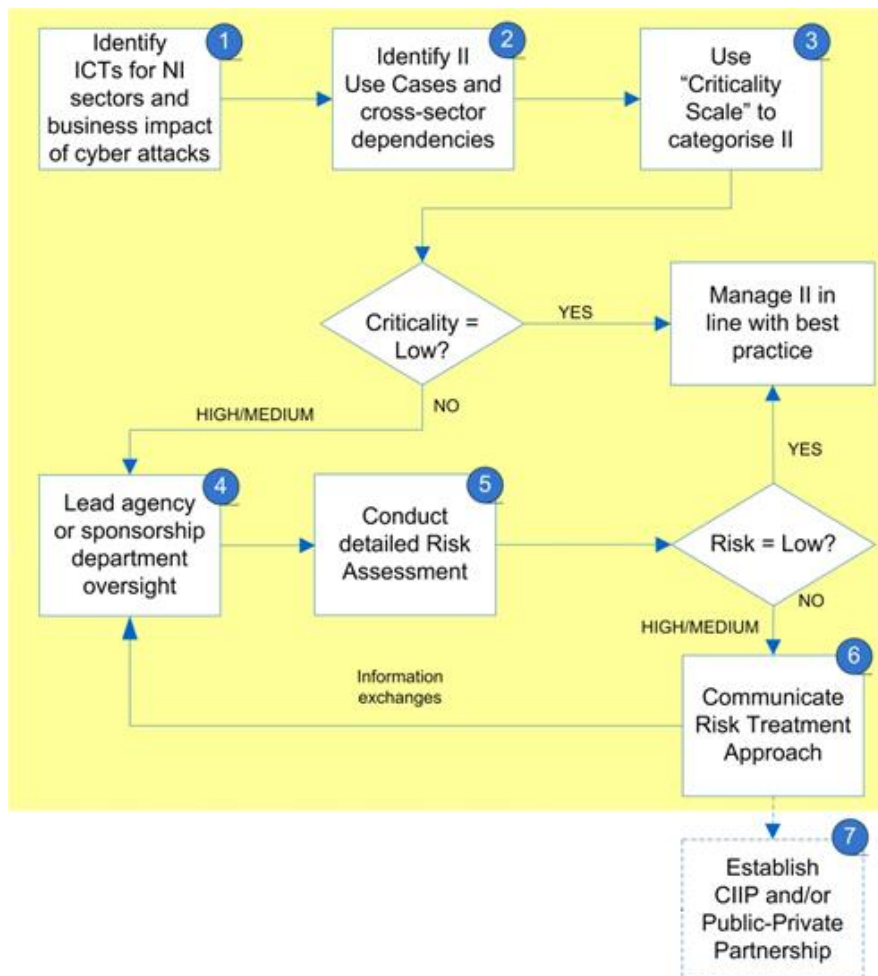
1. Answer **ALL** questions **ONLY** in the supplied **ANSWER SHEET**.
2. **Do NOT write in pencil. Anything in pencil WILL NOT BE MARKED.**
3. Write neatly and legibly.
4. Answers must pertain to the material covered during the course of the module.
5. **NO** calculators may be used.
6. **This question 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: (6)
- A definition of the term “Critical Infrastructure”,
  - Two examples of Critical Infrastructure, and
  - An explanation of how each of your listed examples can be classified as Critical Infrastructure.
- 1.2 Briefly discuss Critical Infrastructure Protection. (4)
- 1.3 Critical Information Infrastructure (CII) is said to be highly distributed and interconnected. Explain how CII exhibits these characteristics. (2)
- 1.4 List four potential consequences that can come from successful Critical Infrastructure attacks. (4)
- 1.5 List four goals of Critical Information Infrastructure Protection (CIIP) programmes. (4)

**QUESTION 2**

The diagram below represents the Critical Information Infrastructure Designation and Risk Management process.



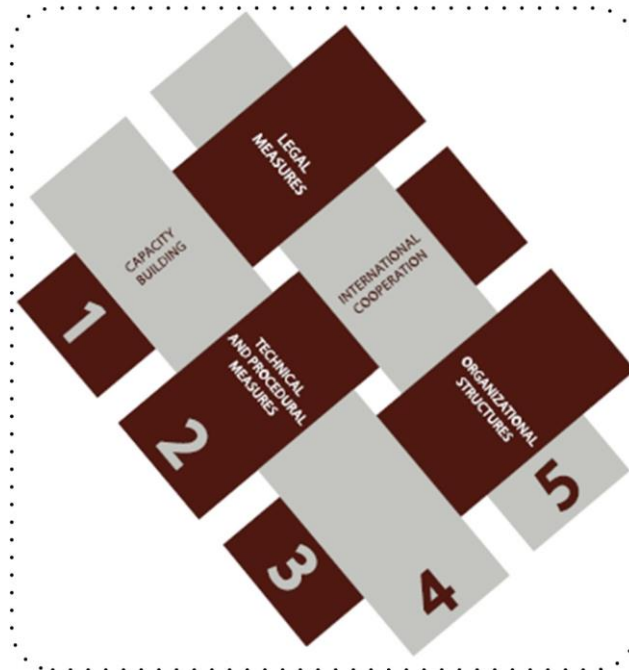
Briefly discuss the purpose of following the designation and risk management process. Additionally, briefly discuss the main steps of the process. (10)

[10]

**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.

**WAYS:**  
Approaches to executing  
CIIP/cybersecurity strategy



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: **(6)**

- Legal Measures,
- Capacity Building, and
- International Cooperation.

**[6]****QUESTION 4**

**4.1** Define the term "Security Incident", as used in the Information Security field. **(2)**

**4.2** Briefly discuss Computer (Security) Incident Response Teams (CSIRTs). Include the following in your discussion: **(12)**

- Their purpose,
- A list of their guiding principles, and
- A brief discussion of each of their guiding principles.

**[14]**

**QUESTION 5**

- 5.1 In ITU-T X.1205, one of the network protection strategies is Uniform Access Management. List and describe at least five aspects that Uniform Access Management should strive towards. (5)
- 5.2 Name and describe four of the components that comprise a SCADA system. (4)
- 5.3 In a supply chain environment, name four of risks associated with supply chains. (4)
- 5.4 What cyber security document was accepted by cabinet in 2015? (1)
- 5.5 According to the draft version of Cybercrimes and Cyber Security Bill released in October 2015, who is responsible for Identification and declaring National Critical Information Infrastructures in South Africa (1)
- 5.6 Name one of the Information Assurance Model goals. (1)
- 5.7 Name two items that governments are held accountable for when dealing with risk in the country's national supply chain. (1)

**[17]****QUESTION 6**

Cyber security awareness is one of the major aspects that can result in a very good return on investment for a country or company. With Cyber security awareness in mind answer the following questions.

- 6.1 The government of a country is accountable for national cyber security awareness. List five of the aspects that government is accountable for with regards to the national cyber security awareness programs. (5)
- 6.2 Name and describe three of the key issues that a national cyber security awareness program should take into account. (6)
- 6.3 List two of the techniques that can be used by the government to implement cyber security awareness. (2)

**[13]****QUESTION 7**

Given the course content on cyber warfare. Describe what is necessary for a nation to take part in cyber warfare. Ensure to cover the three aspects of cyber warfare such as:

**Preparation.** Discuss all the aspects of how a nation can prepare for cyber warfare.

**Offensive strategies.** Discuss the various aspects that a nation should take into account when they want to attack a target.

**Defensive strategies.** Discuss the aspects that must be taken into account when a nation needs to defend against cyber-attacks.

Structure your answer into three distinct sections with three different headings. Marks are awarded as follows:

- Presentation, (6)
- Offensive strategies, and (8)
- Defensive strategies. (6)

**[20]****TOTAL: 100 MARKS**