UNIVERSITY
OF
JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE	**IT00302/IT08X32** Critical Information Infrastructure Protection
CAMPUS	**APK**
EXAM SSA	**NOVEMBER 2020**

ASSESSORS:	MR SP SITHUNGU MR K LEBEA
MODERATOR:	PROF BL TAIT
DURATION: 120 MINUTES	**MARKS:** 100

PLEASE TAKE CAREFUL NOTE OF THE FOLLOWING:

1. Write clearly and legibly.
2. Answer all the questions.
3. When done, save your work as a PDF and upload to https://eve.uj.ac.za/ → Practicals → Exam SSA.
4. Remember to download, complete and upload your Honesty Declaration to https://eve.uj.ac.za/ → Practicals → Honesty Declaration SSA.
5. Download time: 15 minutes.
6. Upload time: 15 minutes.

QUESTION 1

1.1 As one of the country's Critical Information Infrastructure Protection practitioners, you have been approached to assist in implementing a CIIP strategy for Utopia. In order to lay a solid foundation, your first task is to write a report that describes and discusses CIIP as a means to help non-experts understand the need for CIIP. In your discussion you have been asked to ensure that the following aspects are included: **(25)**

- A definition of the term "Critical Infrastructure"
- Two examples of Critical Infrastructure (explain why each of your listed examples can be classified as Critical Information Infrastructure)
- Critical Infrastructure interdependencies
- A discussion of Critical Information Infrastructure and where it fits within the context of Critical Infrastructure
- Two examples of Critical Information Infrastructure Systems
- Types of attacks on Critical Information Infrastructure and possible consequences

[25]

QUESTION 2

2.1 In the context of South Africa, choose one type of information infrastructure which you deem critical and answer the following questions:

2.1.1 Name the chosen Critical Information Infrastructure (CII) **(1)**

2.1.2 Evaluate the criticality of the chosen CII in terms of: **(6)**
- What the **degree of disruption** to essential services would be if the CII was compromised
- The **extent of the disruption** in terms of **population** and **geographical** spread
- The **length of time** that the disruption would persist

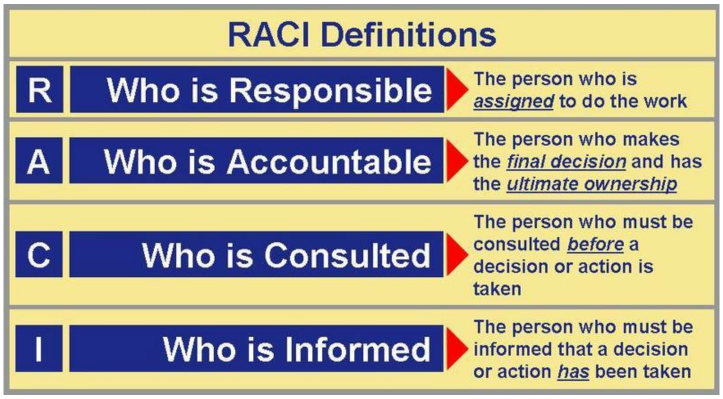
2.1.3 Describe the challenges you believe to be currently faced by the CII in terms of **Assets**, **Vulnerabilities** and **Countermeasures**. **(10)**

[17]

QUESTION 3

3.1 Describe the public-private partnership (PPP) and explain why it would be beneficial in protecting your chosen CII in Question 2. **(4)**

3.2 Governance structures are crucial in the implementation and maintenance of CIIP in a country. Based on the RACI definitions shown in the figure below, explain how the government – along with the private sector – can realise efficient protection for your chosen CII in Question 2. Be sure to include all the aspects (i.e. R, A,C and I) in your discussion. **(10)**



RACI Definitions

R	Who is Responsible	The person who is *assigned* to do the work
A	Who is Accountable	The person who makes the *final decision* and has the *ultimate ownership*
C	Who is Consulted	The person who must be consulted *before* a decision or action is taken
I	Who is Informed	The person who must be informed that a decision or action *has* been taken

[14]

QUESTION 4

4.1 The Utopian Department of Cybersecurity has decided that the next phase of Utopia's CIIP strategy development is to establish a Computer Security Incident Response Team (CSIRT). You have been tasked with writing a concise report that explains the importance of a CSIRT to be distributed to all relevant stakeholders. The brief must include the following aspects: **(14)**

- A description of the term "Security Incident"
- The purpose of a CSIRT
- How incident management is more than just reacting (hint: refer to the relevant diagram)
- The principles of Incident Response.

[14]

QUESTION 5

5.1 Name and compare the two main Network Protection Strategies discussed in class. In your comparison, be sure to identify **at least one** strength and weakness of each strategy. **(8)**

5.2 In your opinion, how important is staff training as a Network Protection Strategy (refer to the class discussion on how humans can be the weakest link in an information security chain)? **(2)**

[10]

QUESTION 6

6.1 In your own words, briefly describe the idea behind cyberwarfare. **(4)**

6.2 When countries engage in cyberwarfare, what is the main commodity that they are likely aiming to be superior in? **(1)**

6.3 Cyberwarfare is made possible through three key areas **preparation**, **offensive strategies** and **defensive strategies**. Discuss how each of these areas make cyberwarfare possible. **(9)**

6.4 Briefly describe the three remedies available under International Law in the case of cyberwarfare. **(6)**

TOTAL: 100 MARKS