FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE:	IT08X32
	CRITICAL INFORMATION INFRASTRUCTURE PROTECTION
CAMPUS:	APK
ASSESSMENT:	EXAM

MEMORANDUM

DATE: 27/10/2021	**TIME:** 08:30
ASSESSOR:	MR SP SITHUNGU
MODERATOR:	PROF BL TAIT
DURATION:	120 MINUTES
MARKS:	100
NUMBER OF PAGES:	4

PLEASE READ THE FOLLOWING INTRUCTIONS CAREFULLY:

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.
4. Remember to download, complete and upload your **Honesty Declaration** to https://eve.uj.ac.za/ → Practicals → Honesty Declaration Exam.
5. Download time: 15 minutes.
6. Upload time: 15 minutes.

QUESTION 1

1.

1.1 **Discuss** Critical Information Infrastructure (CII). Include in the following in your discussion:

- A definition of the term "Critical Infrastructure"
- A definition of the term "Critical Information Infrastructure"
- Two examples of CII (6)

- **According to the United States' Department of Homeland Security:**
  - *"**Critical infrastructure** is the **backbone** of our **nation's economy**, **security** and **health**. We know it as the power we use in our homes, the water we drink, the transportation that moves us, and the communication systems we rely on to stay in touch with friends and family."*
  - *"**Critical infrastructure** are the **assets**, **systems**, and **networks**, whether **physical or virtual**, **so vital** to the United States **that their incapacitation** or **destruction** would have a **debilitating effect** on **security**, **national economic security**, **national public health** or **safety**, or **any combination thereof**."*
- As with most other modern day systems, **technology has been a major driver** in the efficient provisioning of crucial services in Critical Infrastructure.
- Information systems used to manage Critical Infrastructures are known as **"Critical Information Infrastructure Systems"**.
- **Critical Information Infrastructures (CII)** are the **systems** used to **run** and **manage** the **infrastructures** that contribute to the social well-being and economic stability of a country.

- The student may produce any two examples of critical information infrastructure

1.2 **Briefly discuss** Critical Information Infrastructure Protection. (4)

- **Operating failure in critical information infrastructure can create serious disruptions to critical services** provided to a country's society (Ten, Manimaran and Liu, 2010).
- **The protection of such highly networked systems is therefore seen as being of the utmost importance for a country**

1.3 Critical Information Infrastructure (CII) is said to be highly distributed and interconnected. **Explain** how CII exhibits these characteristics. (2)

- The use of **real time information is key in the provision of services** in Critical Infrastructure.

- **Critical Information Infrastructures** provide the layer which allows the **effective and efficient** control of Critical Infrastructure.

- These computer aided systems collect information using a wide array of sensors from all spectrums involved in the provision of an infrastructure's services.

1.4 Provide a **comprehensive discussion** of public-private partnerships. In your discussion be sure to **address the following**:

- In your own words, describe public-private partnerships.

- The cooperation between the public and private sectors is mainly driven by the need for assets that can only be found in the private sector (Eckert, 2005).
- It is therefore seen as a much more cost-effective option to create partnerships with the private sector to get access to these assets in order to provide services.
- **Public-Private Partnership:**
  - "A contractual arrangement between a public sector institution and a private party in which the private party performs an institutional function or uses state assets and assumes substantial financial, technical and operational risks in the design, financing, building and/or operation of the project, in return for a benefit" (Eichler, Auxila and Pollock, 2001).

- In your own words, describe the objectives of public-private partnerships

- Shuping and Kabane (2008) listed the following as some of the **objectives public-private partnerships attempt to achieve:**
  - The public sector is able to leverage private finance to strengthen the public sector;
  - The sharing of scarce resources between the sectors maximises benefits for the broader population;
  - There is an improvement in the quality of services rendered;
  - This partnership promotes an equitable allocation of resources.

- Briefly discuss one advantage of public-private partnerships. (8)
- The student may any advantage of public-private partnerships. Merely stating an advantage will only result in 1 mark as the question asked the student to briefly discuss.

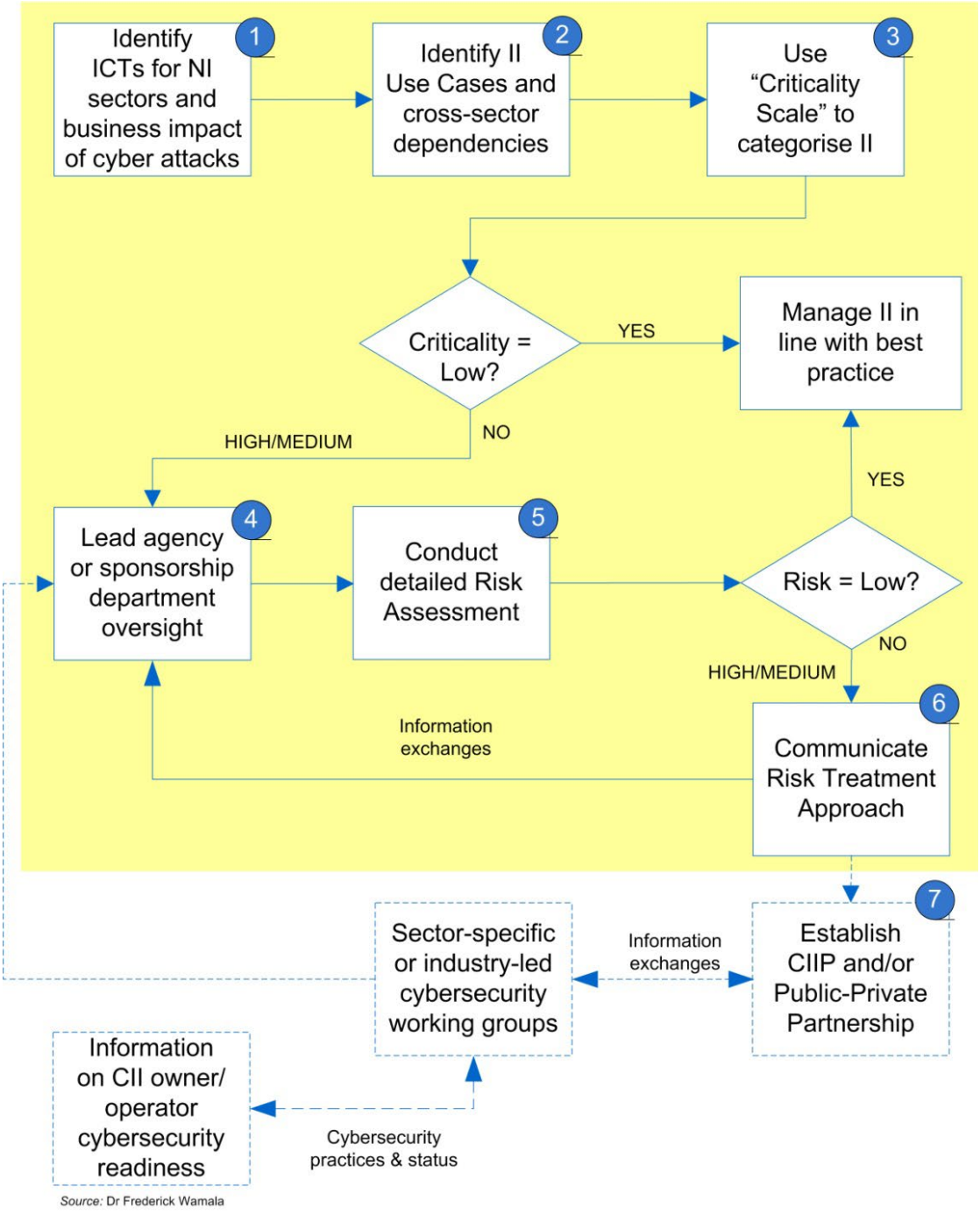
[20]

QUESTION 2

2.

2.1 In order to identify CII at any scale (whether organizational or national), it is important

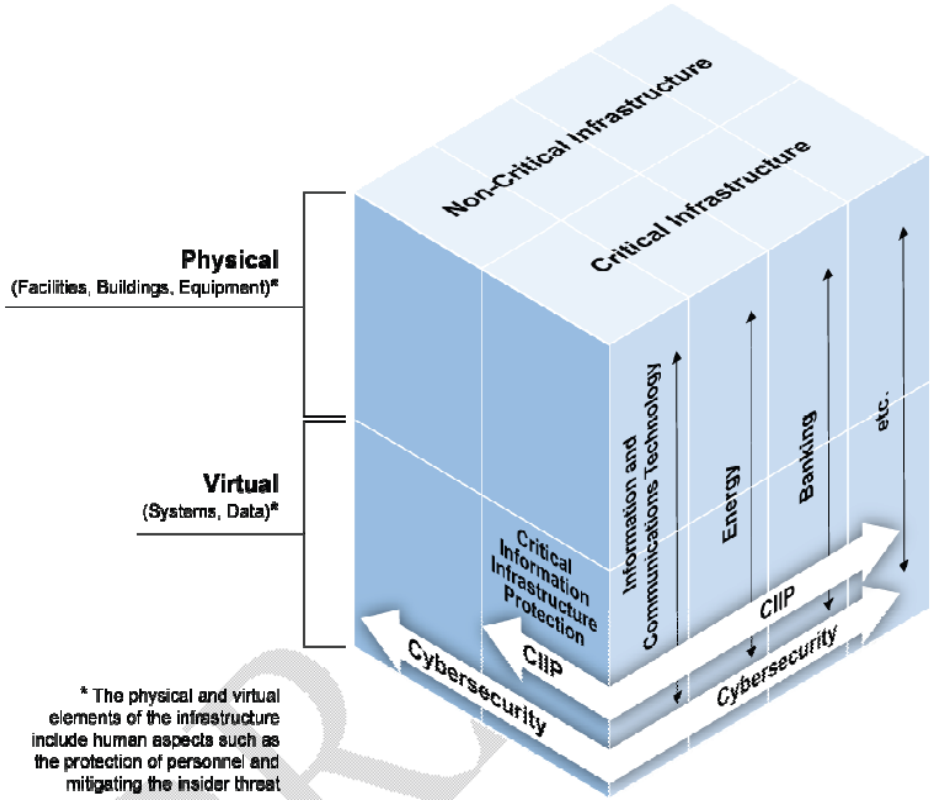
to have an approach for **CII Designation and Risk Managemement**. Discuss the steps you would follow to designate an infrastructure as critical while also conducting a detailed risk assessment (you may provide a diagram to aid your discussion but you will not loose marks without one). (20)



Source: Dr Frederick Wamala

2.2 **Discuss** legislation specificity with regards to Critical Inrastructure. **Refer** to the diagram below to aid your discussion. (5)

- Any valid discussion highlighting the fact that cybersecurity legislation spans both critical and non-critical infrastructure and that CIIP falls within the scope of cybersecurity. The student can also make the distinction between CIP and CIIP by highlighting that CIIP only applies to CII.



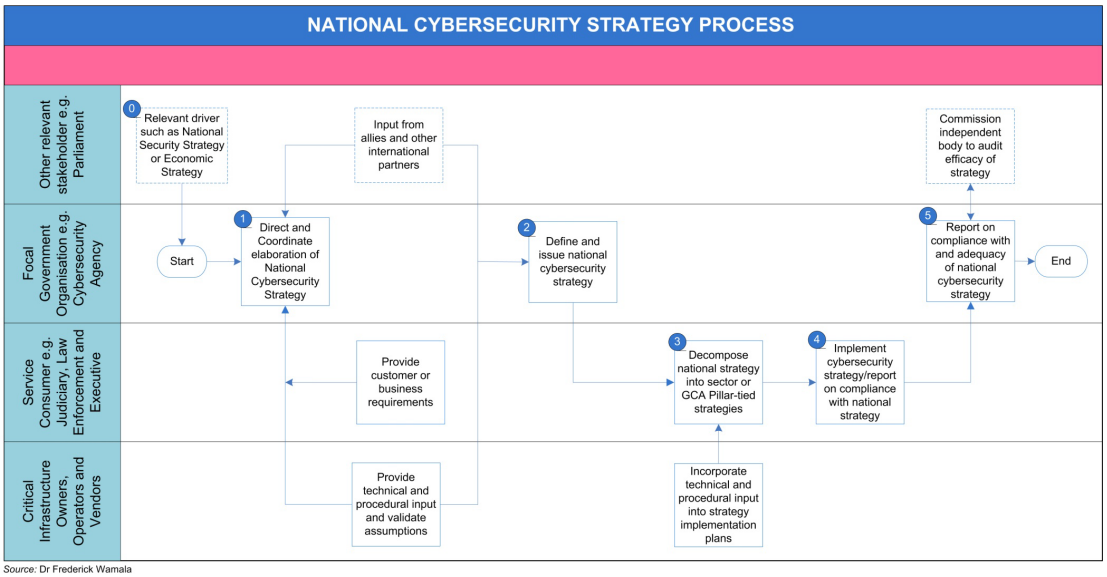
[25]

QUESTION 3

3.

3.1 The ITU National Cybersecurity Strategy Guide" has a National Cybersecurity Strategy Process that outlines key tasks that must be performed by each stakeholder within the process. **Discuss** this process. **[20]**

- Please zoom in the diagram.

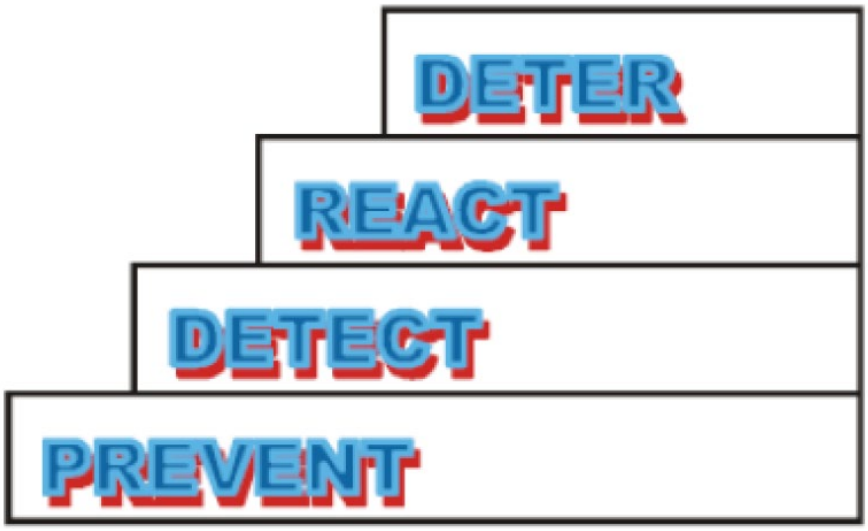


Source: Dr Frederick Wamala

QUESTION 4

4.

4.1 **Briefly discuss** the **four** principles of Incident Response (you may provide a diagram to aid your discussion). (8)



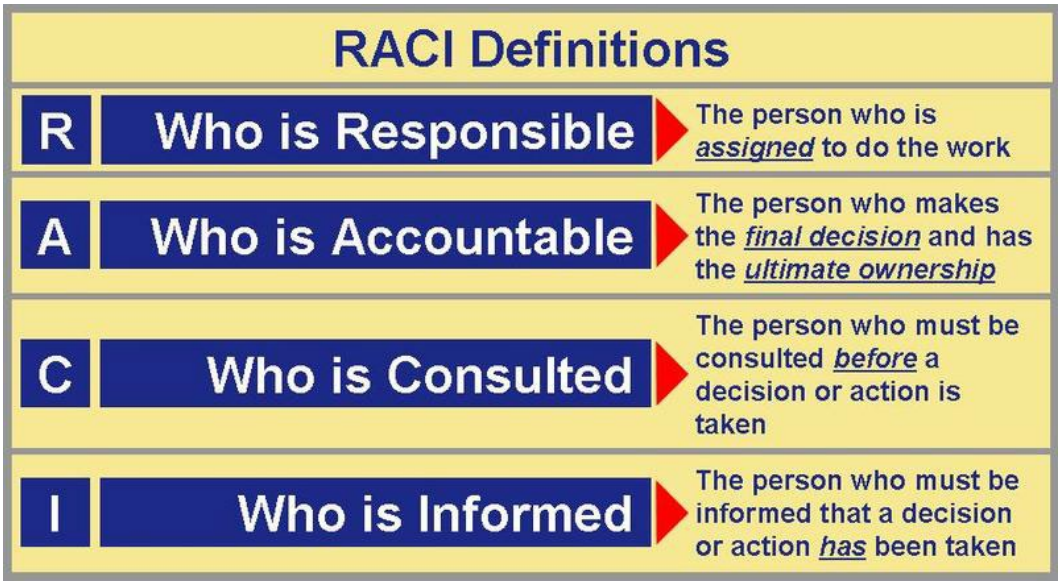
- **Prevent**
  - Pillar/Logical or physical

- **Detect**
  - Detective measures e.g. checking of log files, logical or physical alarms build on preventative measures such as intrusion detection

- **React (to most people this is CIRT)!**
  - Actions taken once an incident is detected

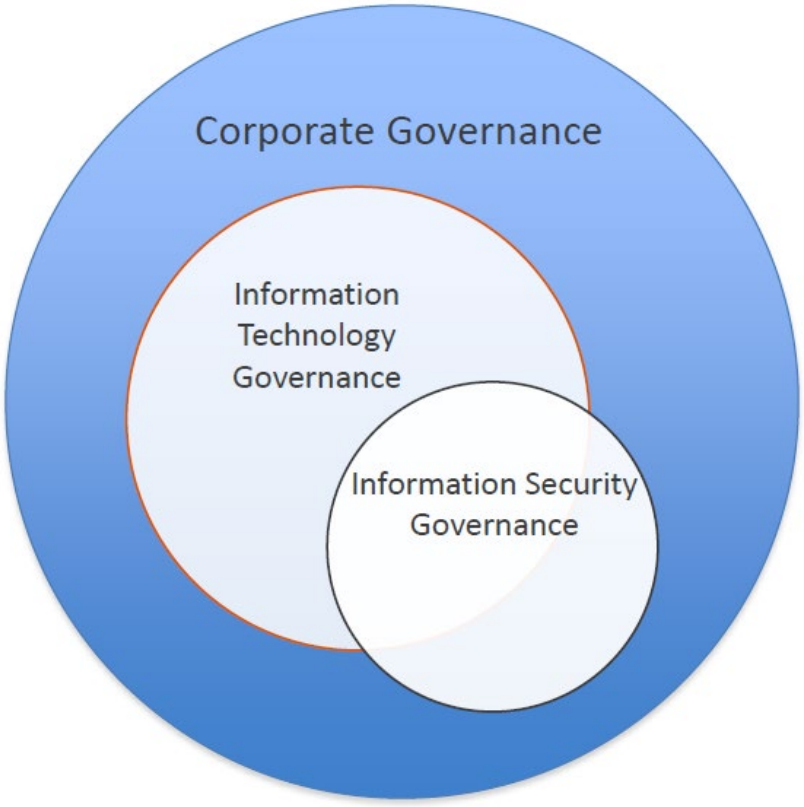
- **Deter**
  - Active steps to beat off intrusion
  - Intrusion Prevention Systems react in real-time

4.2 Governance structures are crucial when it comes to building effective cybersecurity structures within a country. **Use** the RACI matrix and your discretion to **decide** who is **responsible**, **accountable**, **consulted** and **informed** in terms of ensuring cybersecurity for a country's critical infrastructures. You may include public-private partnerships in your discussion. (8)



- The student may use their discretion to specify the parties that are **responsible**, **accountable**, **consulted** and **informed.** The only requirement is that they provide a sensible discussion.

4.3 Does Information Security Governance (ISG) fall entirely within the scope of corporate governance? If no, what other type of governance is necessary to complete ISG? (1)



[17]

QUESTION 5

5. The Unity for Justice (UJ) is one of the governmental structures that were created after the establishment of Automation First's (AF) Cybersecurity Framework for their Critical Infrastructure. One of UJ's core responsibilities is to evaluate companies' Information Assurance (IA) maturity levels. Upon inspection, UJ realised that the AF's main board is aware of the criticality of IA to the business and of its legal requirements. Moreover, UJ realised that the board has initiated a few activities and there is a policy to guide the improvement process.

5.1 Based on the above assessment: as the director of UJ, which maturity level would you assign to AF's IA processes? Justify your choice. (4)

- Correct answer: Level 1

IA Maturity Model Levels

- **Level 1 – Initial**
  - Main Board is aware of the criticality of IA to the business and of its legal requirements.
  - Board has initiated activity to address areas of immediate weakness and has policy in place to guide the improvement process.
- **Level 2 – Established**
  - IA processes are institutionalised within the organisation, its delivery partners/suppliers
  - Board has endorsed strategic approach to IA
  - Targeted IA awareness has been initiated
- **Level 3 – Business Enabling**
  - Awareness across the organisation has increased leading to a measured improvement in IRM behaviours within the organisation/suppliers
  - Building on Level 2, Level 3 will be achieved when all critical areas of the business are subject to a robust IA regime
- **Level 4 – Quantitatively Managed**
  - Evidence to show that staff attitudes and behaviours towards assuring information are aligned to the needs of the business.
  - The regime established at level 3 for critical areas of the business is extended to all areas
  - IA metrics available to take an informed approach to managing the risk to the information used by the business.
- **Level 5 – Optimised**
  - IA is fully integrated as an aspect of normal business and the culture of the business is such that at all levels of management.
  - IA is judged to be a **business enabler**.

5.2 Discuss what is the next logical maturity level that AF needs to aim for and what needs to be accomplished for AF to be assigned that level. (4)

• Level 2	
5.3 Cybersecurity is concerned with several different stakeholders. Name the stakeholders and **briefly** explain what role each stakeholder plays regarding a nation's cybersecurity strategy. • **Cyber security is concerned with a number of different stakeholders:** • Government • associated governmental entities • Governmental service providers • Industry • Academia • Individuals • Civil Society	(10)
	[18]

TOTAL: [100]