UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

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

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 INSTRUCTIONS CAREFULLY:

1. Write clearly and legibly.
2. Answer all the questions.
3. When done, save your work as a PDF and upload it 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 the following in your discussion:

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

1.2 **Briefly discuss** Critical Information 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 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.
- In your own words, describe the objectives of public-private partnerships
- Briefly discuss one advantage of public-private partnerships. (8)

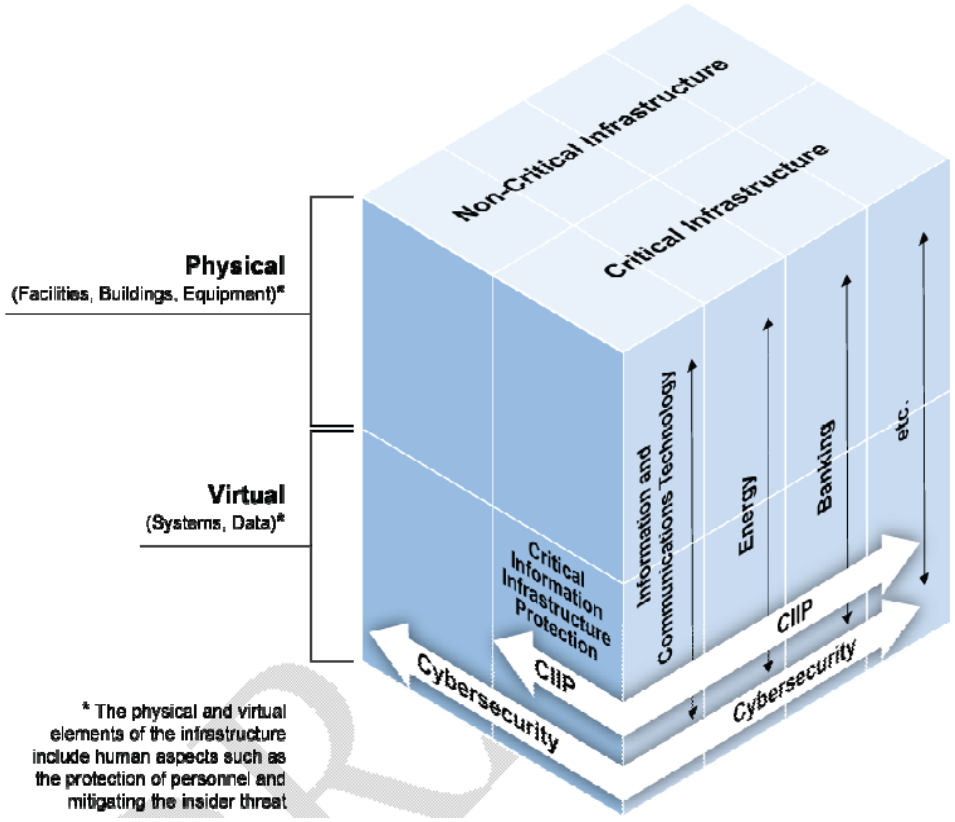
[20]

QUESTION 2

2.

2.1 In order to identify CII at any scale (whether organisational or national), it is important to have an approach for **CII Designation and Risk Management**. 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 lose marks without one). (20)

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



[25]

QUESTION 3

3. The ITU National Cybersecurity Strategy Guide has a National Cybersecurity Strategy Process that outlines key tasks various stakeholders must perform throughout the process. **Discuss** this process and the steps associated with it. **[20]**

QUESTION 4

4.

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

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

4.3 Does Information Security Governance (ISG) fall entirely within the scope of corporate governance? If not, what other type of governance is necessary to complete ISG? (1)

[17]

QUESTION 5

5. Unity for Justice (UJ) is one of the governmental structures created after establishing NationOfTheFuture's Cybersecurity Framework. One of UJ's core responsibilities is to evaluate companies' Information Assurance (IA) maturity levels. Automation First (AF) is one of the many companies that UJ assesses. UJ realised that AF's board of directors is aware of the criticality of IA to the business and its legal requirements. Moreover, UJ realised that the board had initiated a few activities and 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)

5.2 **Discuss** the **next logical** maturity level that AF needs to aim for and what AF needs to accomplish to reach that level. (4)

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. (10)

[18]

TOTAL: [100]