

NIS Report Requirements

Task

In the aforementioned context, your task in this individual assignment task is to analyse the related security issues and design the network by considering the questions or tasks below. You should structure your report using the IMRD (a.k.a. IMRaD) model and pay careful attention to effective key messaging to deliver a clear and concise report (please revisit the Guest Lecture by The ANU Academic Skills for further information). The maximum word length for the report is 3000 words plus the list of references. The cover page must include your name, email address, and uniID. Please name your document as Firstname.Lastname.uniID.pdf where the Firstname, Lastname, and uniID refer to your personal identifiers.

1. Outline the major security threats in this context. Be sure to identify those that you think are major threats and those that are minor threats. (0-2 marks)

Draft: "In general, security threats can be classified into two broad categories: ensuring business continuity and preventing unauthorized access."

Elaborate more in the report.

Ensuring business continuity

- a) Disruptions, the loss or reduction in the network service. (minor)
- b) Destruction of data. (minor)
- c) Natural (or human-made) disasters. (minor)

Preventing unauthorized access

- a) Intrusion from outside networks. External attackers gaining access to organizational data files and resources from across the Internet. (major)
- b) Intrusions from within the organizations. Half of the incidents involve employees within the organizations.

1. Prepare a risk assessment that includes the major assets, threats, and controls.

You need to make some reasonable assumptions and document them. (0-3 marks)

Impact Area	Priority	Low Impact	Medium Impact	High Impact	
Productivity					
Reputation					
Legal					
Safety					

Refer to Figure 11-5 and 11-6

1. Propose a set of security controls in the context of disruption, destruction, disaster, unauthorised access, managing threats of intrusion, network controls, preventive controls, detective controls, and corrective controls. (0-5 marks)

Refer to 11.3 Business Continuity and 11.4 Intrusion Prevention

Network controls

Preventive controls

Detective controls

Corrective controls

1. How do you ensure business continuity by mitigating or preventing various levels of threats and intruders? What are the differences between threats and intruders? (0-4 marks)

A. Ensuring business controls

B. Differences between threats and intruders

1. Identify, describe, and justify five context-relevant Apps, web pages, or other networked information systems. Remember to add a URL and possible a reference for further information about your chosen technologies. For maximal points, the technologies should be layperson friendly (i.e., remember Ellen and Karen's experiences from weekly assignment tips) and timely (e.g., released in 2018–2020). The justifications should consider laypersons' perspective. (0-5 marks)

- a) Apple watch integrated with iOS app: Apple Health
- b) Wearable sensors including novel devices such as paper on chip
- c) Sports equipments for athletes to monitor the performance
- d) HomeCourt using AR and ML to analyze the exercise
- e) Intelligent medical system

1. Only for COMP6340 students: Design your network by addressing the location of the security threats in the communication process (as an example, see the textbook cases on how email/ webmail/ messenger work) of Figure 1 by developing a necessary diagram and describing your design (e.g., how email/ webmail/ messenger work?). (0-5 marks)

Refer to Figure 2-13 How Email Works

1. Include a reflection section or paragraph in your Discussion section. (0-1 marks)