	Learning outcomes.
1.	Evaluate the significance of having an organisational cyber security policy
2.	Investigate the roles and responsibilities of the cyber security function in governance, responsibility and policy
3.	Analyse and distinguish between strategic level planning through to operational implementation of security technologies
4.	Critically analyse past and current activities that threaten organisational processes
5.	Develop adequate understanding for the creation of an organisational cyber security policy in a given case study setting
6.	Develop an understanding of cyber security monitoring in a given situation

Topics/Content outline:

Learning Outcome number and Time	Expanded Outcomes	Method	Assessment Type
1. (2 weeks)	Evaluate the significance of having an organisational cyber security policy • Understand an organisation's mission, objectives and goals and how these relate to security • Explain the importance of managing risk • Describe the CIA Triad • Distinguish between policy, guidelines, standards and procedures • Be able to apply security classifications to information and infrastructure	Lecture Discussion, collaborative work, student presentations. Critical reflection of on-line research, databases and industry inquiry.	Individual assignment
2. (3 weeks)	Investigate the roles and responsibilities of the cyber security function in governance, responsibility and policy • Discuss computer related crime, the law, and investigations • Discuss the security roles and responsibilities within organisations • Discuss the many different plans and their procedures that compose a comprehensive security plan • Discuss the system certification and accreditation process for ensuring the	Lecture Discussion, collaborative work, student presentations, (individual and collaborative exercises in the use of commercial	Individual assignment