Learning Outcome number and Time	Expanded Outcomes	Method	Assessment Type
	implementation and enforcement of a security plan • Discuss legal, regulations, and compliance • IT control frameworks	tools and case studies)	
3. (2 weeks)	Analyse and distinguish between strategic level planning through to operational implementation of security technologies • Discuss elements of IT strategic plans • Information security strategic and operational plans • Implementing information strategic and operational plans • Information security program	Lecture Discussion, collaborative work, student presentations. Critical reflection of on-line research, databases and industry inquiry.	Test: to review self-efficacy
4. (2 weeks)	Critically analyse past and current activities that threaten organisational processes • Evolving technologies and their impact on cyber security (web and mobile application, virtualisation and cloud computing) • Standards and regulatory requirements • Business dynamics	Lecture Discussion, collaborative work. Critical reflection of on- line research, databases and industry inquiry.	Test: to review self-efficacy
5. (2 weeks)	Develop an understanding for creating an organisational cyber security policy • Identify business and regulatory requirements • Develop security policy – case study • Security awareness programs • Ensuring adherence to organisation's security policy • IS auditing, process, general and	Lecture Discussion, collaborative work. Critical reflection of on-line research, databases	Test: to review self-efficacy