Unit 1 Reflection

This unit introduced students to information security management (ISM) which encompasses both people, processes, information, and information technology. I consider these four parts a single whole because no information system exists in isolation but consists of actors that act upon it and upon which it works. I learned that the triad of information security management (Confidentiality, Integrity and Availability) serves as the foundation of ISM. GDPR policies address confidentiality, integrity is only as good as the data sources or inputs, and availability can be resolved using cloud providers. The concept of Non-Repudiation as part of the triad was interesting because it concerns a system's ability to prove who/what performed actions within the system. A practical application of non-repudiation is monitoring application log files frequently.

The collaborative discussion, initiated in this unit, helped me understand how threat prevention takes multiple forms and must involve infrastructure managed by organisations or cloud providers. For example, firewalls, two-factor authentication, intrusion detection systems, password policies, and data encryption. For me, assigning the least privilege to user accounts is the quickest and simplest means to reducing potential threats. Important too is *enabling* customers to easily report new threats and to consider not just software aspects of information systems, but also mundane items such as the buildings, a business's processes and the people that interact.

References