Week 4: Regulations and Standards

Welcome to our second lecture this week; a presentation (with voiceover), on regulations and standards.

We have seen in the first lecture that a number of policies and procedures are needed in order for an organisation to be compliant with information and data protection, and the importance of transparency and accountability. It is essential that organisations implement the necessary security precautions to ensure that security breaches are prevented. We have also seen in a previous lecture the importance of policies and procedures and the need for professional ethics in planning and ensuring security and risk management. We will now look at some of the regulations and standards that can be adopted by organisations to improve security standards and management practices.

One of an organisation's greatest challenges is to develop an adequate, robust security policy.

The first and most important step in security planning is the actual plan itself, its design and development, and deciding on an overall control framework or structure to be used and implemented. Planning for standards and compliance are essential factors, and security policies require placement of controls in processes specific to systems.

We have already been introduced to Control Objectives for Information and Related Technology (COBIT), a framework for ensuring quality, reliability, and control of information and related technology. There is also another approach; The Open Source

Security Testing Methodology Manual (OSSTMM), that is a methodology for security testing. This manual is updated every six months to remain up to date with the current state of security testing, and is maintained by the Institute for Security and Open Methodologies (ISECOM). Another framework that we have also already been introduced to, is the Information Technology Infrastructure Library (ITIL); this model aligns to the business strategy and customer needs, and provides the best practice framework for both a common language and tools, to enable collaboration within IT teams to deliver value for the organisation.

These are all frameworks that might be employed by organisations in the quest of developing a robust security plan. The difference between ITIL and COBIT is that ITIL is a framework that enables IT services to be managed across their lifecycle, and COBIT helps IT governance to generate added value to the organisation by way of investments by mitigating risks and optimising resources.

The next slide will look at ISO standards.

ISO standards have been developed by an independent, nongovernmental international organisation to ensure quality, safety, and efficiency of products, services and systems. They demonstrate that the said organisation meets the requirements of international legislation and regulation. Obtaining ISO certification ensures a reduced risk of liability within an organisation.

Amongst the ISO standards, is the ISO/IEC 27002: 2013 that is a set of guidelines for information security standards and management practices within an organisation. These include the selection, implementation and management controls taking into consideration the organisation's information security risk environment. It is designed for organisations who intend to select elements of controls for implementing an Information Security Management System (ISMS) that is based on the ISO/IEC 27001. This ISO standard 27001 is discussed in the next slide.

The ISO 27001, provides an international methodology specifically for information security and if an organisation holds this certification, it demonstrates conformity of the ISMS requirements with documented standards and consequently provides assurance for system security and aids the security and risk management process. It is relevant to understanding the needs and expectations of 'interested parties' and defining

the scope of the ISMS. Top management should demonstrate leadership and commitment to the ISMS, mandate policy, and assign information security roles, responsibilities and authorities. It is used for planning, as it outlines the process to identify, analyse and plan in order to treat information risks, and clarify the objectives of information security. It provides support in that adequate, competent resources must be assigned, awareness raised, and that relevant documentation is prepared and controlled. This standard also provides more detail with the operation of assessing and treating information risks, managing changes, and documenting them in order that they might be audited by the certification auditors. It provides performance evaluation by monitoring, measuring, analysing, evaluating and auditing for reviewing the information security controls, processes and management system. It also provides improvements and refinements systematically where needed.

In summary, this lecture has given us an overview of some frameworks and standards to help with the challenges facing security and risk management. Now take a break and reflect on what we have learned so far before moving on to the next task where you will read a paper on to consolidate what we have covered in the lecture.