**Discussion 2**

List 5 information security standards frameworks. Briefly describe about those framework.

**International Standards Organisation (ISO) 27K**

One of the most widely known security standards, this is a mature framework focused on information security. It’s very comprehensive and broad, and can be used across a wide range of types and sizes of businesses. Developed by the International Standards Organisation (ISO), it is the security equivalent of the ISO 9000 quality standards for manufacturers and operational excellence.

Because it’s tried and tested, countries often use it as a basis on which to create a manual about security and what to do; an example being the New Zealand Information Security Manual (NZISM). However, like many of the ISO standards, it can be a bit daunting, and many smaller organisations are put off by the effort required to gain accreditation and the perception that it can be difficult to implement.

**NZISM Protective Security Requirements (PSR) Framework**

This is New Zealand’s national technical security policy, and it describes baseline and minimum mandatory security standards for government departments and agencies. It forms an important part of the New Zealand Security Intelligence Service’s Protective Security Requirements (PSR) framework, which sets out the Government's expectations for managing personnel, information and physical security.

As it’s a New Zealand document, it’s a popular starting point for Kiwi companies, and it has been made publicly available to allow greater access, increase awareness, improve transparency, and to share good practice.

**Australian Signals Directorate (ASD) Essential 8**

Not a standard as such, the Australian Signals Directorate (ASD) Essential 8 is a set of controls or strategies that, if implemented correctly, could mitigate up to 85% of the most common information security attack techniques.

The Essential 8 are part of a larger set of strategies that make up the ASD Strategies to Mitigate Cyber Security Incidents. These are based on the ASD’s experience in responding to real-world attacks and in performing vulnerability assessments and penetration testing of Australian Government agencies. The ASD state that the Essential 8 are so effective, they consider them to be the cyber-security baseline for all organisations.

**Control Objectives for Information and Related Technology (COBIT)**

COBIT is a high level framework focussed on identifying and mitigating risk. It was developed for IT governance professionals to reduce technical risk, but it’s evolved into a standard to align IT with business goals. What it lacks is informative practical advice. While it’s not as widely followed as others, COBIT is mostly used within the finance industry to comply with standards such as Sarbanes-Oxley, but if your business wants to adopt a formal risk management framework, it’s also worth considering.

**US National Institute of Standards and Technology (NIST)**

The NIST framework has evolved over 20 years and could be seen as the father figure for others. It contains a wide ranging collection of information security standards and best practices. It is mature and very comprehensive and is very good for large enterprises, as well as those with a US connection. It can be aligned to the ISO standards, such as ISO 9000 quality management. Because NIST contains a lot of practical guidance, it can also be adapted relatively easily to smaller and non-US organisations.

**Industry-Specific Standards**

In addition to the common frameworks above, there are also a number of industry-specific standards such as PCI DSS (for credit card handling), HIPAA (US legislation to safeguard health/medical information) and HISO (the NZ health information security framework) as well as any number of local regulations such as the European GDPR and the NZ Privacy Act. Adopting one of the more general security frameworks above may not make you fully compliant with these specific standards or regulations, but they will go a long way to helping you achieve compliance.