Principle	Objectives	
Management of Information Security Risks & Threats	• The Organisation provides commitment and support to information security • A Governance structure exists to manage risk • The Organisation has a risk strategy and tolerance levels defined • Risks are being identified, and assessed against potential impacts and the likelihood of occurrence • Risks are being treated • Effectiveness of risk treatments are monitored • Staff are aware of the risks and actions to treat them • Legal and Regulatory requirements are known and addressed	
Prevention against Cyber Attacks	Access Control	• Access control is defined and managed • Access to systems is controlled • Accounts are managed • Permissions and privileges are managed
	Communications Security	• Network controls exist to protect systems and applications • Network traffic is restricted and monitored • Networks are segregated
	Data Security	• Data is protected from unauthorised access • Data is protected at rest • Data is protected during processing • Data is protected in motion • Data controls meet any legal or regulatory requirements
	Malicious Software	• Controls exist to prevent malicious software • Controls exist to restrict unauthorised software • Staff are aware of malicious software
	Operational Security	• Systems are configured to a defined standard • Operational procedures are documented • Audits and Checks are performed against systems
	Software Development & Acquisition Security	• Security is part of the software development lifecycle • Developers are aware of common exploitable attacks • Penetration Testing is performed • Security Diligence is performed on Software purchased from Vendors
	Vulnerability Management	• Systems and applications are patched regularly • Security notifications are reviewed as part of a defined process • Systems are periodically assessed to ensure they are not susceptible to vulnerabilities

Principle	Objectives
System Resilience to Service Outages	• A strategy exists for System Resilience • Change Control Processes and Procedures are used • Redundancy and Capacity Planning is performed • Risks to system availability have been reviewed • Systems have a defined Recovery Point Objective • Systems have a defined Recovery Time Objective • The Organisation is prepared for business interruptions and disasters • Third Party Supplier Resilience is considered
Incident Management	• The organisation is prepared to detect, prevent, contain and recover from incidents • Systems are monitored and events which could be precursors to incidents analysed • In the event of an incident, accurate evidence can be examined • Conduct regular incident simulations and assess effectiveness of incident management • Can request assistance where necessary to manage incidents
Restoration of Services	• Has alternate plans in the event of total system loss • The ability to fully restore services within three working days • Perform testing of recovery plans • Can recover data in the event of any primary data storage loss