Appendix two – Glossary

Item	Definition
Business continuity plan	A plan that outlines how an organisation will respond effectively to disruptions and ensure continuity of service delivery, safety and availability of staff, availability of information technology and other systems, financial management and governance
Classification	The categorisation of systems and information according to the expected impact if it was to be compromised
Cyber attack	A deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity
Cyber incident	An unwanted or unexpected security event, or a series of such events, that have a significant probability of compromising business operations
Cyber incident response plan	A plan for responding to cyber security incidents
Cyber security	Measures used to protect the confidentiality, integrity and availability of systems, devices and the information residing on them
Cyber security maturity	An assessment of the organisation's preparedness to identify, respond and recover from cyber attacks. This may include consideration of cyber security models such as the ACSC Essential Eight, or policies and guidance such as the Cyber Security NSW Cyber Security Policy and Cyber Security Guidelines – Local Government
Cyber threat	Any circumstance or event with the potential to harm systems or information
Disaster recovery plan	A plan that outlines an organisation’s recovery strategy for how they are going to respond to a disaster
DMARC	Domain-based message authentication, reporting and conformance is an email authentication protocol to prevent hostile actors using ‘spoofed’ or forged email accounts
Essential Eight	The Essential Eight are eight essential mitigation strategies that the ACSC recommends organisations implement as a baseline to reduce the risk of adversaries compromising systems
ICT	Information and Communications Technology, also referred to as Information Technology (IT), includes software, hardware, network, infrastructure, devices and systems that enable the digital use and management of information and the interaction between people in a digital environment
Information security	The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability
Multi-factor authentication	A method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are)
Patching	The action of updating, fixing, or improving a computer program
Risk appetite	The amount and type of risk that an organisation is willing to accept

Source: Audit Office of New South Wales based on internal and publicly available information.