G. Glossary

Term	Definition
Business continuity plan	A plan which outlines how an organisation's critical business functions will either – continue to operate despite serious incidents or disasters that might otherwise have interrupted them; or will be recovered to an operational state within a reasonably short period.
Communities of practice – Cyber Security Unit	CSU's communities of practice aim to raise awareness of information security and develop and share information, methods, and tools to create a knowledge base for public sector entities, including local governments.
Cyber communication plan	A plan which outlines an entity's approach to communicating with internal and external stakeholders in the event of a cyber incident.
Cyber incident	An unwanted or unexpected cyber security event or series of such events that have a significant probability of compromising business operations.
Cyber resilience	The ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations. This includes the ability to detect, manage, and recover from cyber security incidents.
Cyber security	A process for protecting an entity's information by preventing, detecting, and responding to cyber incidents. Such attacks could be through breaches of physical and network security, or through using information obtained through social networks.
Cyber security simulations	Workshops to test how key incident response personnel (both technical and non-technical) respond to a cyber incident within their information systems or networks. Simulations can help identify vulnerabilities, assess risks, and improve security measures.
Cyber threat intelligence	Information that helps organisations better protect against cyber incidents by providing an understanding of current and emerging threats and vulnerabilities. It can incorporate recent threat actor behaviours, and successful remedial procedures, tools, and techniques.
Denial of service attacks	A malicious, targeted attack that floods a network with false requests to disrupt business operations.
Digital forensics	Capabilities that enable incident responders to investigate the source, entry point, and extent of a cyber incident or data breach.
Exploitation risk	The likelihood and the impact of a threat actor (refer to definition below) intentionally exploiting a weakness in a system, causing disruptions or losses.
Incident response plan	A plan which outlines the activities undertaken to support an effective response and prompt recovery in the event of a cyber security incident.
Information asset	A collection of data that is recognised as having business value and enables an entity to perform its business functions.
Information security management system (ISMS)	A system that preserves the confidentiality, integrity, and availability of information by applying a risk management process. It gives confidence to interested parties that risks are adequately managed.
Insider privilege abuse (insider threats)	Internal actors, such as current or former employees, who can pose a threat to an organisation because they have direct access to the company network, sensitive data, and intellectual property (IP), as well as knowledge of business processes, company policies, or other information that would help carry out such an attack.

Term	Definition
IS18:2018	The Queensland Government Information Security Policy (IS18:2018) aims to ensure all departments apply a consistent, risk-based approach to the implementation of information security to maintain confidentiality, integrity, and availability. While IS18:2018 only applies to departments defined under the *Public Sector Act 2022*, all statutory bodies should be aware of and consider implementing the policy. Local governments and government owned corporations can also consider it and whether it is suitable for their needs.
ISO 27000 series	A set of standards for establishing an information security management system (ISMS) and underlying controls. It not only includes a large library of technical controls but also requires entities to commit to maintaining a culture of cyber safety and resilience.
ISO 27001 certification	An international certification that demonstrates to stakeholders and customers that an entity is committed to and able to manage information securely and safely based on ISO 27001 *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.
Machine learning	A type of artificial intelligence which is focused on teaching computers to learn from data.
Malware	Malware is any software used to gain unauthorised access to IT systems to steal data, disrupt system services, or damage IT networks in any way.
National Institute of Standards and Technology (NIST) Cyber Security Framework	A risk-based approach to managing cyber security risk that reinforces the connection between business drivers and cyber security activities.
Phishing	Phishing refers to online scams enticing users to share private information using deceitful or misleading tactics.
Playbooks	Incident response procedures for a particular incident type. Examples could include ransomware, insider privilege abuse, social engineering, denial of service attacks, malware, and phishing.
Public sector entities	In this report, this refers broadly to all Queensland public sector entities (departments, statutory bodies, and government owned corporations) and local government entities.
Ransomware	Ransomware is a type of malware (refer to definition above) identified by specified data or systems being held captive by attackers until a form of payment or ransom is provided.
Social engineering	Social engineering is a term that describes cyber attacks that use psychological tactics to manipulate people into taking a desired action, like giving up confidential information. Social engineering attacks work because humans can be compelled to act by powerful motivations, such as money, love, and fear. Adversaries play on these characteristics by offering false opportunities to fulfill those desires.
Threat actor	Any person or organisation that intentionally exploits weaknesses in computers, networks, and systems to disrupt individuals or organisations.