D. Glossary

Term	Definition
Application whitelisting	A security approach to prevent the running and installation of malicious code and unauthorised applications. It only allows programs that have been explicitly approved to be run and installed.
Cyber security	A process for protecting an entity's information by preventing, detecting and responding to cyber attacks. Such attacks could be through breaches of physical and network security, and through using information obtained through social networks.
Database administrative privileges	Administrative access to database systems that enables a user to create user accounts, set passwords, and manage and maintain databases that can contain sensitive data.
Encryption	A process for encoding a message or file so that it can only be read by authorised people. It makes sensitive data more secure and reduces the likelihood that an unauthorised person could intercept it to view it.
Endpoint security	Involves making sure there is security on the endpoints (potential entry points) of a network, like laptops and wireless and mobile devices.
Essential Eight	The Australian Cyber Security Centre (ACSC) has compiled a list of mitigating strategies entities can use to improve their ability to protect against cyber security risks. It has developed eight mitigation strategies that it says should be implemented as a baseline where practicable. They are known as the 'Essential Eight.'
Entities	We use the term 'entities' in this report to refer broadly to all Queensland public sector entities (including departments and statutory bodies) and local governments.
Execute	The process of running a computer software or command.
Information asset	A collection of data that is recognised as having business value and enables an entity to perform its business functions.
Jump server	A jump box (or jump server) ensures that access to a secure server cannot be obtained from a less secure zone on the corporate network.
Malicious or threat actor	An individual, group of individuals, or entity that attempts to conduct malicious activities against an entity by taking advantage of vulnerabilities to gain unauthorised access to systems and data.
Network segmentation	Involves segregating part of a computer network. This helps to reduce what is available to an attacker if they successfully compromise part of the network.
Open source threat intelligence assessment	An assessment that involves investigating publicly available information from the internet and the hidden web to determine whether any sensitive information about an entity can be obtained from public (or 'open') sources. The hidden web includes the 'deep web', which is the part of the world wide web where content is not discoverable using standard search engines, and the 'dark web', which is the part of the world wide web only accessible using special software.
Patches	Released by software and hardware vendors to mitigate known vulnerabilities that attackers could exploit (as well as to address a software flaw or to improve the stability of an application/program).

Term	Definition
Phishing	A fraudulent scamming attempt to obtain sensitive information from an end user (for example, username, passwords, and credit card information). For example, asking a user to click on a link that results in malicious software being installed.
Privileged user access	Administrative access to systems. For example, a user with privileged user access can create user accounts and set passwords, configure systems, have access to sensitive data, and execute other software and scripts.
Red team assessment	A red team engagement tries to find the quickest method to access an entity's security mechanisms and compromise its sensitive applications and data. In doing so, it considers the target and resources available, and may attempt social engineering, physical entry, and data exploitation.
Security posture	The security status of an entity's networks, information, and systems based on its resources (for example, people, processes, and technology) and ability to defend the entity from cyber attacks and to react as the situation changes.
Server	A computer program or a device that is dedicated to managing network resources to provide services to computer programs on end-user devices (for example, desktops, laptops, phones, and tablets).
Subdomains	A subdomain is an internet domain that is part of a primary domain. For example, a primary domain may be xxx.qld.gov.au and a subdomain of this could be yyy.xxx.qld.gov.au.
Two-factor authentication (or multi-factor authentication)	Requires more than one authentication method to gain access to a system, for example, a username and password, plus a code sent to a mobile phone.
Virtual private network (VPN)	Provides additional security to protect sensitive data on a corporate network. It provides an encrypted connection from a device to the network over the internet. It allows the user to work remotely and prevents unauthorised users from eavesdropping on the network traffic.