Appendix B: Abbreviations, acronyms and glossary

Abbreviations

We use the following abbreviations in this report:

Abbreviation	
secure score	Microsoft Secure Score

Acronyms

We use the following acronyms in this report:

Acronym	
BYOD	bring your own device
CIEM	cloud infrastructure entitlement management
CIS	Center for Internet Security
DISA	Defence Information Systems Agency
EDR	endpoint detection and response
EMM	enterprise mobility management
EPP	Endpoint Protection Platform
IAM	identity and access management
IT	information technology
MAM	mobile application management
MCSB	Microsoft cloud security benchmark
MDM	Mobile Device Management
MFA	multi-factor authentication
MTD	Mobile Threat Defence
NGAV	Next Generation Anti-virus
SIEM	security information and event management
SOAR	Security Orchestration, Automation, and Response
SOC	security operation centre
UEM	unified endpoint management
UES	unified endpoint security
VAGO	Victorian Auditor-General's Office
XDR	extended detection and response

Glossary

This glossary includes an explanation of the types of engagements we perform:

Term	
Reasonable assurance	We achieve reasonable assurance by obtaining and verifying direct evidence from a variety of internal and external sources about an agency's performance. This enables us to express an opinion or draw a conclusion against an audit objective with a high level of assurance. We call these audit engagements. See our assurance services fact sheet for more information.
Limited assurance	We obtain less assurance when we rely primarily on an agency's representations and other evidence generated by that agency. However, we aim to have enough confidence in our conclusion for it to be meaningful. We call these types of engagements assurance reviews and typically express our opinions in negative terms. For example, that nothing has come to our attention to indicate there is a problem. See our assurance services fact sheet for more information.
The cloud	The cloud is when a service provider supplies software, data storage and other services over the internet. The cloud is more economical, effective and efficient compared to traditional computing, which relies on in house servers and databases.
Compliance policy	A compliance policy is a set of rules that a device must comply with. For example, an agency may require devices to have antivirus software.
Conditional access policies	Agencies can implement conditional access policies to require a user to complete an action if they want to access their networks.
Cybersecurity solution	Modern cybersecurity solutions use technology such as threat and artificial intelligence to analyse user behaviours and other signals. These solutions can be used to detect and respond to threats. A native cybersecurity solution is one from the cybersecurity platform provider, such as Microsoft.
Managed service arrangement	Under a managed service arrangement, the agency determines and oversees the controls. The service provider is responsible for implementing them.
MFA	MFA is a control that requires users to verify their identity using at least 2 methods before they can access an agency's systems or documents.
Microsoft 365 tenancy	A Microsoft 365 tenancy is a dedicated environment within the Microsoft 365 cloud. It provides a range of services from Microsoft. When an agency buys a Microsoft 365 subscription, it is allocated to a tenancy. Agencies can share a tenancy.
Passwordless authentication	Passwordless authentication lets a user access an application or IT system without entering a password. Instead, the user may log in with passwordless technology, such as biometrics. This reduces the risk of people relying on remembering passwords to access systems.
Privileged access management	Agencies can give some users access to more functions than standard users, such as accessing, modifying or deleting sensitive information as well as making changes to servers, devices and user accounts.
Security configuration baseline	A security configuration baseline is the recommended settings that an agency can use to set up its devices.
Shared service arrangement	Under a shared service arrangement, the service provider determines and implements controls. An agency needs to assess if the controls meet its requirements before entering the engagement.

Term	
The zero trust model's 6 pillars	Identities, devices, applications, data, infrastructure and networks are 6 foundational elements, or pillars, that make up modern IT operations. The zero trust model is a high-level strategy. It assumes that users, devices and services attempting to access resources, even from inside the network, cannot automatically be trusted.