

Essential Eight Assessment

Prepared by Ridgeline IT

0

Below Level 1

Overall maturity: Below Level 1

Below the Level 2 target

Maturity levels are cumulative, and an organisation's overall rating is set by its weakest strategy rather than an average. 105 of 304 requirements were assessed as implemented.

Summary by strategy

Mitigation Strategy	Achieved	Target	Result
Patch applications	Level 1	Level 2	Gap
Patch operating systems	Level 1	Level 2	Gap
Multi-factor authentication	Level 2	Level 2	Met
Restrict administrative privileges	Level 1	Level 2	Gap
Application control	Below Level 1	Level 2	Gap
Restrict Microsoft Office macros	Below Level 1	Level 2	Gap
User application hardening	Level 1	Level 2	Gap
Regular backups	Level 2	Level 2	Met

Where the gaps are

These strategies sit below the Level 2 target. They are listed worst first, which is the order they are usually worth addressing.

Application control — currently Below Level 1

ML1 Application control is implemented on workstations.	Not implemented
ML1 Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	Not implemented

ML1 Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	Not implemented
ML2 Application control is implemented on workstations.	Partly implemented
ML2 Application control is implemented on internet-facing servers.	Not implemented
ML2 Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	Not implemented
ML2 Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.	Partly implemented
ML2 Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	Not implemented
ML2 Microsoft's recommended application blocklist is implemented.	Not implemented
ML2 Application control rulesets are validated on an annual or more frequent basis.	Partly implemented
ML2 Allowed and blocked application control events are centrally logged.	Not implemented
ML2 Event logs are protected from unauthorised modification and deletion.	Not implemented
ML2 Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Partly implemented
ML2 Cyber security events are analysed in a timely manner to identify cyber security incidents.	Not implemented
ML2 Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.	Not implemented
ML2 Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Partly implemented
ML2 Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Not implemented

Restrict Microsoft Office macros — currently Below Level 1

ML1 Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	Partly implemented
--	--------------------

ML1 Microsoft Office macros in files originating from the internet are blocked.	Not implemented
ML1 Microsoft Office macro antivirus scanning is enabled.	Not implemented
ML1 Microsoft Office macro security settings cannot be changed by users.	Partly implemented
ML2 Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	Not implemented
ML2 Microsoft Office macros in files originating from the internet are blocked.	Not implemented
ML2 Microsoft Office macro antivirus scanning is enabled.	Partly implemented
ML2 Microsoft Office macros are blocked from making Win32 API calls.	Not implemented
ML2 Microsoft Office macro security settings cannot be changed by users.	Not implemented

Patch applications — currently Level 1

ML2 An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	Partly implemented
ML2 A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	Not implemented
ML2 A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	Not implemented
ML2 Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.	Partly implemented
ML2 Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.	Not implemented

Patch operating systems — currently Level 1

ML2 An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	Not implemented
--	-----------------

ML2 Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

Partly implemented

ML2 Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.

Not implemented

Restrict administrative privileges — currently Level 1

ML2 Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.

Partly implemented

ML2 Privileged access to systems and applications is disabled after 45 days of inactivity.

Not implemented

ML2 Privileged operating environments are not virtualised within unprivileged operating environments.

Partly implemented

ML2 Unprivileged user accounts cannot logon to privileged operating environments.

Not implemented

ML2 Privileged access events are centrally logged.

Partly implemented

ML2 Privileged user account and security group management events are centrally logged.

Not implemented

ML2 Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.

Partly implemented

ML2 Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.

Not implemented

User application hardening — currently Level 1

ML2 Web browsers do not process Java from the internet.

Partly implemented

ML2 Web browsers do not process web advertisements from the internet.

Not implemented

ML2 Microsoft Office is blocked from injecting code into other processes.

Partly implemented

ML2 Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.

Not implemented

ML2 PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.

Partly implemented

ML2 PDF software security settings cannot be changed by users.

Not implemented

ML2 Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.

Partly implemented

ML2 Cyber security events are analysed in a timely manner to identify cyber security incidents.

Not implemented

Recommended plan

Ordered by priority, then by how much work each item is — so the quick wins that lift the rating come first.

ACTION	STRATEGY	PRIORITY	EFFORT	OWNER / DUE
Block macros in Office files originating from the internet A Group Policy change. Roughly an hour of work for a full maturity level on this strategy.	Restrict Microsoft Office macros	High	Small	—
Move the two remaining Windows 10 machines to a supported build Both are out of vendor support and cannot receive patches.	Patch operating systems	High	Medium	—
Deploy application control to the four reception workstations No application control is in place. This is the single control holding the overall rating below Level 1.	Application control	High	Large	—
Turn on multi-factor authentication for the two remaining shared logins Front desk and the imaging PC still sign in with a shared password.	Multi-factor authentication	Medium	Small	—
Document and test the restore process Backups are running and monitored, but a restore has never been attempted.	Regular backups	Medium	Medium	—
Review privileged accounts quarterly rather than annually Three accounts hold local administrator rights that are no longer needed.	Restrict administrative privileges	Low	Small	—

Full results

Patch applications — Level 1

ML1	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Online services that are no longer supported by vendors are removed.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	Implemented Verified in Intune configuration profile, 8 Sep

ML2	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	Partly implemented
ML2	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	Not implemented
ML2	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	Not implemented
ML2	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.	Partly implemented
ML2	Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.	Not implemented
ML2	Online services that are no longer supported by vendors are removed.	Implemented Verified in Intune configuration profile, 8 Sep

ML2	Office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	Implemented Verified in Intune configuration profile, 8 Sep
ML3	<i>13 requirements above the Level 2 target, not assessed.</i>	

Patch operating systems — Level 1

ML1	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Operating systems that are no longer supported by vendors are replaced.	Implemented Verified in Intune configuration profile, 8 Sep

ML2	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	Not implemented
ML2	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Partly implemented
ML2	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.	Not implemented
ML2	Operating systems that are no longer supported by vendors are replaced.	Implemented Verified in Intune configuration profile, 8 Sep
ML3	<i>16 requirements above the Level 2 target, not assessed.</i>	

Multi-factor authentication — Level 2

ML1	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.	Implemented Verified in Intune configuration profile, 8 Sep
-----	---	---

ML1	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation's non-sensitive data.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation's non-sensitive data.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.	Implemented Verified in Intune configuration profile, 8 Sep

ML2	Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Multi-factor authentication is used to authenticate privileged users of systems.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Multi-factor authentication is used to authenticate unprivileged users of systems.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Multi-factor authentication used for authenticating users of online services is phishing-resistant.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Multi-factor authentication used for authenticating users of systems is phishing-resistant.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Successful and unsuccessful multi-factor authentication events are centrally logged.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Event logs are protected from unauthorised modification and deletion.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Cyber security events are analysed in a timely manner to identify cyber security incidents.	Implemented Verified in Intune configuration profile, 8 Sep

ML2	Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Implemented Verified in Intune configuration profile, 8 Sep
ML3	<i>23 requirements above the Level 2 target, not assessed.</i>	

Restrict administrative privileges — Level 1

ML1	Requests for privileged access to systems, applications and data repositories are validated when first requested.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Privileged users use separate privileged and unprivileged operating environments.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Unprivileged user accounts cannot logon to privileged operating environments.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Implemented Verified in Intune configuration profile, 8 Sep

ML2	Requests for privileged access to systems, applications and data repositories are validated when first requested.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.	Partly implemented
ML2	Privileged access to systems and applications is disabled after 45 days of inactivity.	Not implemented
ML2	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Privileged users use separate privileged and unprivileged operating environments.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Privileged operating environments are not virtualised within unprivileged operating environments.	Partly implemented
ML2	Unprivileged user accounts cannot logon to privileged operating environments.	Not implemented
ML2	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Administrative activities are conducted through jump servers.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Privileged access events are centrally logged.	Partly implemented
ML2	Privileged user account and security group management events are centrally logged.	Not implemented

ML2	Event logs are protected from unauthorised modification and deletion.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Cyber security events are analysed in a timely manner to identify cyber security incidents.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.	Partly implemented
ML2	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Not implemented
ML2	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Implemented Verified in Intune configuration profile, 8 Sep
ML3	<i>29 requirements above the Level 2 target, not assessed.</i>	

Application control — Below Level 1

ML1	Application control is implemented on workstations.	Not implemented
ML1	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	Not implemented
ML1	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	Not implemented
ML2	Application control is implemented on workstations.	Partly implemented
ML2	Application control is implemented on internet-facing servers.	Not implemented
ML2	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	Not implemented
ML2	Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.	Partly implemented

ML2	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	Not implemented
ML2	Microsoft's recommended application blocklist is implemented.	Not implemented
ML2	Application control rulesets are validated on an annual or more frequent basis.	Partly implemented
ML2	Allowed and blocked application control events are centrally logged.	Not implemented
ML2	Event logs are protected from unauthorised modification and deletion.	Not implemented
ML2	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Partly implemented
ML2	Cyber security events are analysed in a timely manner to identify cyber security incidents.	Not implemented
ML2	Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.	Not implemented
ML2	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Partly implemented
ML2	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Not implemented
ML3	<i>19 requirements above the Level 2 target, not assessed.</i>	

Restrict Microsoft Office macros — Below Level 1

ML1	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	Partly implemented
ML1	Microsoft Office macros in files originating from the internet are blocked.	Not implemented
ML1	Microsoft Office macro antivirus scanning is enabled.	Not implemented
ML1	Microsoft Office macro security settings cannot be changed by users.	Partly implemented
ML2	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	Not implemented

ML2	Microsoft Office macros in files originating from the internet are blocked.	Not implemented
ML2	Microsoft Office macro antivirus scanning is enabled.	Partly implemented
ML2	Microsoft Office macros are blocked from making Win32 API calls.	Not implemented
ML2	Microsoft Office macro security settings cannot be changed by users.	Not implemented
ML3	<i>11 requirements above the Level 2 target, not assessed.</i>	

User application hardening — Level 1

ML1	Internet Explorer 11 is disabled or removed.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Web browsers do not process Java from the internet.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Web browsers do not process web advertisements from the internet.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Web browser security settings cannot be changed by users.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Internet Explorer 11 is disabled or removed.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Web browsers do not process Java from the internet.	Partly implemented
ML2	Web browsers do not process web advertisements from the internet.	Not implemented
ML2	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Web browser security settings cannot be changed by users.	Implemented Verified in Intune configuration profile, 8 Sep

ML2	Microsoft Office is blocked from creating child processes.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Microsoft Office is blocked from creating executable content.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Microsoft Office is blocked from injecting code into other processes.	Partly implemented
ML2	Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.	Not implemented
ML2	Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Office productivity suite security settings cannot be changed by users.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	PDF software is blocked from creating child processes.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Partly implemented
ML2	PDF software security settings cannot be changed by users.	Not implemented
ML2	PowerShell module logging, script block logging and transcription events are centrally logged.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Command line process creation events are centrally logged.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Event logs are protected from unauthorised modification and deletion.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Partly implemented

ML2	Cyber security events are analysed in a timely manner to identify cyber security incidents.	Not implemented
ML2	Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Implemented Verified in Intune configuration profile, 8 Sep
ML3	<i>27 requirements above the Level 2 target, not assessed.</i>	

Regular backups — Level 2

ML1	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Backups of data, applications and settings are retained in a secure and resilient manner.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Unprivileged user accounts cannot access backups belonging to other user accounts.	Implemented Verified in Intune configuration profile, 8 Sep
ML1	Unprivileged user accounts are prevented from modifying and deleting backups.	Implemented Verified in Intune configuration profile, 8 Sep

ML2	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Backups of data, applications and settings are retained in a secure and resilient manner.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Unprivileged user accounts cannot access backups belonging to other user accounts.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Unprivileged user accounts are prevented from modifying and deleting backups.	Implemented Verified in Intune configuration profile, 8 Sep
ML2	Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.	Implemented Verified in Intune configuration profile, 8 Sep
ML3	<i>11 requirements above the Level 2 target, not assessed.</i>	

Ridgeline IT · Example report · Not a real business

Assessed against the Essential Eight Maturity Model (November 2023), published by the Australian Signals Directorate. This report records the assessor's findings on the date shown and is not a certification.

Contains material from the Essential Eight Maturity Model (November 2023), © Commonwealth of Australia, Australian Signals Directorate, reproduced under a Creative Commons Attribution 4.0 International licence.