Appendix three – Essential 8 maturity model

Maturity level zero	Maturity level one	Maturity level two	Maturity level three
Application control (whitelisting)			
Application control is not fully implemented on workstations, or running in audit mode. Application control is not occurring on servers.	Application control is implemented on all workstations to restrict the execution of executables to an approved set. Application control is implemented on all servers to restrict the execution of executables to an approved set.	Application control is implemented on all workstations to restrict the execution of executables and software libraries scripts and installers to an approved set. Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.	Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set. Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set. Microsoft's latest recommended block rules are implemented to prevent application control bypasses.
Patch applications			
Patches to security vulnerabilities in applications and drivers assessed as extreme risk are not applied consistently or applied on a greater than monthly basis. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are still being used.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. An automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.

Maturity level zero	Maturity level one	Maturity level two	Maturity level three
Configure Microsoft Office macro settings			
Microsoft Office macros can execute without prompting users for approval. Microsoft Office macro settings can be configured by users.	Microsoft Office macros are allowed to execute, but only after prompting users for approval. Microsoft Office macro security settings cannot be changed by users.	Only signed Microsoft Office macros are allowed to execute. Microsoft Office macros in documents originating from the internet are blocked. Microsoft Office macro security settings cannot be changed by users.	Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros. Microsoft Office macros in documents originating from the internet are blocked. Microsoft Office macro security settings cannot be changed by users.
User application hardening			
Web browsers allow Adobe Flash, web advertisements and Java from the Internet. Unneeded features in Microsoft Office, web browsers and PDF viewers aren't disabled.	Web browsers are configured to block or disable support for Flash content.	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements. Web browsers are configured to block Java from the internet.	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements. Web browsers are configured to block Java from the internet. Microsoft Office is configured to disable support for Flash content. Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.
Restricting administrative privileges			
Requirements for privileged accounts are not consistently validated. No duties-based restrictions on privileged accounts are applied. Privileged accounts are capable of reading emails and web browsing.	Privileged access to systems, applications and information is validated when first requested. Policy security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.	Privileged access to systems, applications and information is validated when first requested and revalidated on an annual or more frequent basis. Policy security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.	Privileged access to systems, applications and information is validated when first requested and revalidated on an annual or more frequent basis. Privileged access to systems, applications and information is limited to that required for personnel to undertake their duties. Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.

Maturity level zero	Maturity level one	Maturity level two	Maturity level three
Patching operating systems			
Patching for extreme risk security vulnerabilities in operating systems are not consistently applied or applied on a greater than monthly basis. A non-vendor supported operating system is used.	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. An automated mechanism is used to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place. Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor supported versions.
Multi-factor authentication			
Multi-factor authentication is not implemented for remote access or when accessing sensitive data repositories or when performing privileged actions.	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication uses at least two of the following authentication factors: passwords with six or more characters, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smartcards, mobile app one-time password tokens, SMS messages, emails, voice calls or software certificates.	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Multi-factor authentication uses at least two of the following authentication factors: passwords with six or more characters, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smartcards or mobile app one-time password tokens.	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Multi-factor authentication is used to authenticate all users when accessing important data repositories. Multi-factor authentication uses at least two of the following authentication factors: passwords with six or more characters, Universal 2nd Factor security keys, physical one-time password tokens, biometrics or smartcards.

Maturity level zero	Maturity level one	Maturity level two	Maturity level three
Daily backups			
Backups of important new/changed data, software and configuration settings are not performed consistently or are performed less often than monthly, or Full recovery has not been tested for backups of important information, software and configuration settings.	Backups of important information, software and configuration settings are performed monthly. Backups are stored for between one to three months. Partial restoration of backups is tested on an annual or more frequent basis.	Backups of important information, software and configuration settings are performed weekly. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for between one to three months. Full restoration of backups is tested at least once. Partial restoration of backups is tested on a bi-annual or more frequent basis.	Backups of important information, software and configuration settings are performed at least daily. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for three months or greater. Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur. Partial restoration of backups is tested on a quarterly or more frequent basis.

Source: CSP Reporting Template (May 2020).