Comparison of maturity levels

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Patch applications	**An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.**	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	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.	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.	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.
	–	**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.**	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.
	Patches, updates or other vendor mitigations for vulnerabilities in	Patches, updates or other vendor mitigations for vulnerabilities in	Patches, updates or other vendor mitigations for vulnerabilities in online

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
	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.	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.	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.
	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.	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.	**–**
	–	**–**	**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 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.**
	–	**–**	**Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security**

Mitigation Strategy	**Maturity Level One**	**Maturity Level Two**	**Maturity Level Three**
			products are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	–	**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.**	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.
	Online services that are no longer supported by vendors are removed.	Online services that are no longer supported by vendors are removed.	Online services that are no longer supported by vendors are removed.
	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.	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.	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.
	–	**–**	**Applications other than 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.**
Patch operating systems	**An automated method of asset discovery is used at least fortnightly to support the detection**	An automated method of asset discovery is used at least fortnightly to support the detection of assets for	An automated method of asset discovery is used at least fortnightly to support the detection of assets for

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	of assets for subsequent vulnerability scanning activities.	subsequent vulnerability scanning activities.	subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	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.	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.	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.
	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.	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.	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.
	–	**–**	**A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers.**
	–	**–**	**A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware.**
	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	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	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

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	vulnerabilities are assessed as critical by vendors or when working exploits exist.	assessed as critical by vendors or when working exploits exist.	assessed as critical by vendors or when working exploits exist.
	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.	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.	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.
	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.	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.	**–**
	–	**–**	**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 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.**
	–	**–**	**Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are**

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
			applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	–	–	Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
	–	–	Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	–	–	Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
	–	–	Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	–	–	The latest release, or the previous release, of operating systems are used.

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	Operating systems that are no longer supported by vendors are replaced.	Operating systems that are no longer supported by vendors are replaced.	Operating systems that are no longer supported by vendors are replaced.
Multi-factor authentication	**Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.**	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.
	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.
	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.	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.	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.
	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.	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.	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.
	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.	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.	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.
	Multi-factor authentication is used to authenticate customers to online	Multi-factor authentication is used to authenticate customers to online	Multi-factor authentication is used to authenticate customers to online

Mitigation Strategy	**Maturity Level One**	**Maturity Level Two**	**Maturity Level Three**
	customer services that process, store or communicate sensitive customer data.	customer services that process, store or communicate sensitive customer data.	customer services that process, store or communicate sensitive customer data.
	–	**Multi-factor authentication is used to authenticate privileged users of systems.**	Multi-factor authentication is used to authenticate privileged users of systems.
	–	**Multi-factor authentication is used to authenticate unprivileged users of systems.**	Multi-factor authentication is used to authenticate unprivileged users of systems.
	–	**–**	**Multi-factor authentication is used to authenticate users of data repositories.**
	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.	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.	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.
	–	**Multi-factor authentication used for authenticating users of online services is phishing-resistant.**	Multi-factor authentication used for authenticating users of online services is phishing-resistant.
	–	**Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.**	**–**
	–	**–**	**Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.**
	–	**Multi-factor authentication used for authenticating users of systems is phishing-resistant.**	Multi-factor authentication used for authenticating users of systems is phishing-resistant.

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	–	**Multi-factor authentication used for authenticating users of data repositories is phishing-resistant.**
	–	**Successful and unsuccessful multi-factor authentication events are centrally logged.**	Successful and unsuccessful multi-factor authentication events are centrally logged.
	–	**Event logs are protected from unauthorised modification and deletion.**	Event logs are protected from unauthorised modification and deletion.
	–	**Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.**	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	–	–	**Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.**
	–	–	**Event logs from workstations are analysed in a timely manner to detect cyber security events.**
	–	**Cyber security events are analysed in a timely manner to identify cyber security incidents.**	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	–	**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.**	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.
	–	**Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.**	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	**Following the identification of a cyber security incident, the cyber security incident response plan is enacted.**	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict administrative privileges	**Requests for privileged access to systems, applications and data repositories are validated when first requested.**	Requests for privileged access to systems, applications and data repositories are validated when first requested.	Requests for privileged access to systems, applications and data repositories are validated when first requested.
	–	**Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.**	Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.
	–	**Privileged access to systems and applications is disabled after 45 days of inactivity.**	Privileged access to systems and applications is disabled after 45 days of inactivity.
	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.
	–	–	**Privileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties.**
	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.
	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	required for users and services to undertake their duties.	required for users and services to undertake their duties.	for users and services to undertake their duties.
	–	–	**Secure Admin Workstations are used in the performance of administrative activities.**
	Privileged users use separate privileged and unprivileged operating environments.	Privileged users use separate privileged and unprivileged operating environments.	Privileged users use separate privileged and unprivileged operating environments.
	–	**Privileged operating environments are not virtualised within unprivileged operating environments.**	Privileged operating environments are not virtualised within unprivileged operating environments.
	Unprivileged user accounts cannot logon to privileged operating environments.	Unprivileged user accounts cannot logon to privileged operating environments.	Unprivileged user accounts cannot logon to privileged operating environments.
	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.
	–	–	**Just-in-time administration is used for administering systems and applications.**
	–	**Administrative activities are conducted through jump servers.**	Administrative activities are conducted through jump servers.
	–	**Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.**	Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.
	–	–	**Memory integrity functionality is enabled.**

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	–	**Local Security Authority protection functionality is enabled.**
	–	–	**Credential Guard functionality is enabled.**
	–	–	**Remote Credential Guard functionality is enabled.**
	–	**Privileged access events are centrally logged.**	Privileged access events are centrally logged.
	–	**Privileged user account and security group management events are centrally logged.**	Privileged user account and security group management events are centrally logged.
	–	**Event logs are protected from unauthorised modification and deletion.**	Event logs are protected from unauthorised modification and deletion.
	–	**Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.**	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	–	–	**Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.**
	–	–	**Event logs from workstations are analysed in a timely manner to detect cyber security events.**
	–	**Cyber security events are analysed in a timely manner to identify cyber security incidents.**	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	–	**Cyber security incidents are reported to the Chief Information Security Officer, or one of their**	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
		delegates, as soon as possible after they occur or are discovered.	possible after they occur or are discovered.
	–	**Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.**	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	–	**Following the identification of a cyber security incident, the cyber security incident response plan is enacted.**	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Application control	**Application control is implemented on workstations.**	Application control is implemented on workstations.	Application control is implemented on workstations.
	–	**Application control is implemented on internet-facing servers.**	Application control is implemented on internet-facing servers.
	–	–	**Application control is implemented on non-internet-facing servers.**
	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.
	–	**Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.**	Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.
	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	–	**Application control restricts the execution of drivers to an organisation-approved set.**
	–	**Microsoft’s recommended application blocklist is implemented.**	Microsoft’s recommended application blocklist is implemented.
	–	–	**Microsoft’s vulnerable driver blocklist is implemented.**
	–	**Application control rulesets are validated on an annual or more frequent basis.**	Application control rulesets are validated on an annual or more frequent basis.
	–	**Allowed and blocked application control events are centrally logged.**	Allowed and blocked application control events are centrally logged.
	–	**Event logs are protected from unauthorised modification and deletion.**	Event logs are protected from unauthorised modification and deletion.
	–	**Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.**	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	–	–	**Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.**
	–	–	**Event logs from workstations are analysed in a timely manner to detect cyber security events.**
	–	**Cyber security events are analysed in a timely manner to identify cyber security incidents.**	Cyber security events are analysed in a timely manner to identify cyber security incidents.

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	**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.**	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.
	–	**Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.**	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	–	**Following the identification of a cyber security incident, the cyber security incident response plan is enacted.**	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict Microsoft Office macros	**Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.**	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.
	–	–	**Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute.**
	–	–	**Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations.**
	–	–	**Only privileged users responsible for checking that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.**
	–	–	**Microsoft Office macros digitally signed by an untrusted publisher**

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
			cannot be enabled via the Message Bar or Backstage View.
	–	–	**Microsoft Office macros digitally signed by signatures other than V3 signatures cannot be enabled via the Message Bar or Backstage View.**
	–	–	**Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.**
	Microsoft Office macros in files originating from the internet are blocked.	Microsoft Office macros in files originating from the internet are blocked.	Microsoft Office macros in files originating from the internet are blocked.
	Microsoft Office macro antivirus scanning is enabled.	Microsoft Office macro antivirus scanning is enabled.	Microsoft Office macro antivirus scanning is enabled.
	–	**Microsoft Office macros are blocked from making Win32 API calls.**	Microsoft Office macros are blocked from making Win32 API calls.
	Microsoft Office macro security settings cannot be changed by users.	Microsoft Office macro security settings cannot be changed by users.	Microsoft Office macro security settings cannot be changed by users.
User application hardening	**Internet Explorer 11 is disabled or removed.**	Internet Explorer 11 is disabled or removed.	Internet Explorer 11 is disabled or removed.
	Web browsers do not process Java from the internet.	Web browsers do not process Java from the internet.	Web browsers do not process Java from the internet.
	Web browsers do not process web advertisements from the internet.	Web browsers do not process web advertisements from the internet.	Web browsers do not process web advertisements from the internet.
	–	**Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.**	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	Web browser security settings cannot be changed by users.	Web browser security settings cannot be changed by users.	Web browser security settings cannot be changed by users.
	–	**Microsoft Office is blocked from creating child processes.**	Microsoft Office is blocked from creating child processes.
	–	**Microsoft Office is blocked from creating executable content.**	Microsoft Office is blocked from creating executable content.
	–	**Microsoft Office is blocked from injecting code into other processes.**	Microsoft Office is blocked from injecting code into other processes.
	–	**Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.**	Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.
	–	**Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.**	Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	–	**Office productivity suite security settings cannot be changed by users.**	Office productivity suite security settings cannot be changed by users.
	–	**PDF software is blocked from creating child processes.**	PDF software is blocked from creating child processes.
	–	**PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.**	PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	–	**PDF software security settings cannot be changed by users.**	PDF software security settings cannot be changed by users.
	–	–	**.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.**

Mitigation Strategy	**Maturity Level One**	**Maturity Level Two**	**Maturity Level Three**
	–	–	**Windows PowerShell 2.0 is disabled or removed.**
	–	–	**PowerShell is configured to use Constrained Language Mode.**
	–	**PowerShell module logging, script block logging and transcription events are centrally logged.**	PowerShell module logging, script block logging and transcription events are centrally logged.
	–	**Command line process creation events are centrally logged.**	Command line process creation events are centrally logged.
	–	**Event logs are protected from unauthorised modification and deletion.**	Event logs are protected from unauthorised modification and deletion.
	–	**Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.**	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	–	–	**Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.**
	–	–	**Event logs from workstations are analysed in a timely manner to detect cyber security events.**
	–	**Cyber security events are analysed in a timely manner to identify cyber security incidents.**	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	–	**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.**	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.

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	**Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.**	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	–	**Following the identification of a cyber security incident, the cyber security incident response plan is enacted.**	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Regular backups	**Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.**	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.
	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.
	Backups of data, applications and settings are retained in a secure and resilient manner.	Backups of data, applications and settings are retained in a secure and resilient manner.	Backups of data, applications and settings are retained in a secure and resilient manner.
	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.
	Unprivileged user accounts cannot access backups belonging to other user accounts.	Unprivileged user accounts cannot access backups belonging to other user accounts.	Unprivileged user accounts cannot access backups belonging to other user accounts.
	–	–	**Unprivileged user accounts cannot access their own backups.**
	–	**Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.**	Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	–	**Privileged user accounts (excluding backup administrator accounts) cannot access their own backups.**
	Unprivileged user accounts are prevented from modifying and deleting backups.	Unprivileged user accounts are prevented from modifying and deleting backups.	Unprivileged user accounts are prevented from modifying and deleting backups.
	–	**Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.**	Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.
	–	–	**Backup administrator accounts are prevented from modifying and deleting backups during their retention period.**