ASD Essential Eight: November 2023 Changes

The table below shows the November 2023 changes to the ASD Essential Eight Standards. The markup indicates where the previous wording has been amended and where new mitigations have been added or removed.

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 ~~internet-facing~~online services.	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in ~~internet-facing~~online services.	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in ~~internet-facing~~online services.
	A vulnerability scanner is used at least ~~fortnightly~~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 ~~other applications.~~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 ~~other applications.~~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 ~~internet-facing~~online services are applied within ~~two weeks~~48 hours of release~~,~~ when vulnerabilities are assessed as critical by vendors or ~~within 48 hours if an exploit exists~~when working exploits exist.	Patches, updates or other vendor mitigations for vulnerabilities in ~~internet-facing~~online services are applied within ~~two weeks~~48 hours of release~~,~~ when vulnerabilities are assessed as critical by vendors or ~~within 48 hours if an exploit exists~~when working exploits exist.	Patches, updates or other vendor mitigations for vulnerabilities in ~~internet-facing~~online services are applied within ~~two weeks~~48 hours of release~~,~~ when vulnerabilities are assessed as critical by vendors or ~~within 48 hours if an exploit exists~~when working exploits exist.

ASD Essential Eight: November 2023 Changes

IIS Partners

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	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 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 products are applied within ~~one month~~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 two weeks of release~~, or within 48 hours if an exploit exists~~. when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.**
	–	**Patches, updates or other vendor mitigations for vulnerabilities in ~~other~~ 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 ~~other~~ 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.
	~~Internet facing services, office~~**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.**	~~Internet facing services, office~~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~~** 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.

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	–	**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 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 operating systems of internet-facing ~~services.~~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 ~~services.~~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 ~~services.~~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 ~~**weekly**~~ 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 ~~weekly~~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.**

ASD Essential Eight: November 2023 Changes

IIS Partners

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing ~~services~~servers and internet-facing network devices are applied within ~~two weeks~~48 hours of release~~,~~ when vulnerabilities are assessed as critical by vendors or ~~within 48 hours if an exploit exists~~when working exploits exist.	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing ~~services~~servers and internet-facing network devices are applied within ~~two weeks~~48 hours of release~~,~~ when vulnerabilities are assessed as critical by vendors or ~~within 48 hours if an exploit exists~~when working exploits exist.	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing ~~services~~servers and internet-facing network devices are applied within ~~two weeks~~48 hours of release~~,~~ when vulnerabilities are assessed as critical by vendors or ~~within 48 hours if an exploit exists~~when working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of ~~workstations,~~internet-facing servers and internet-facing network devices are applied within ~~one month~~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,~~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,~~internet-facing servers and internet-facing network devices are applied within two weeks of release~~, or within 48 hours if an exploit exists~~ 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 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 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 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.**

ASD Essential Eight: November 2023 Changes

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	=	=	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.**
	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** ~~by an organisation's users when they~~ **to authenticate users to their organisation's** ~~internet facing~~**online services that process, store or communicate their organisation's sensitive data.**	Multi-factor authentication is used ~~by an organisation's users when they~~ to authenticate users to their organisation's ~~internet facing~~online services that process, store or communicate their organisation's sensitive data.	Multi-factor authentication is used ~~by an organisation's users when they~~ to authenticate users to their organisation's ~~internet facing~~online services that process, store or communicate their organisation's sensitive data.
	Multi-factor authentication is used ~~by an organisation's users when they~~ **to authenticate users to third-party** ~~internet facing~~**online services that process, store or communicate their organisation's sensitive data.**	Multi-factor authentication is used ~~by an organisation's users when they~~ to authenticate users to third-party ~~internet facing~~online services that process, store or communicate their organisation's sensitive data.	Multi-factor authentication is used ~~by an organisation's users when they~~ to authenticate users to third-party ~~internet facing~~online services that process, store or communicate their organisation's sensitive data.
	Multi-factor authentication (where available) is used ~~by an organisation's users when they~~**to authenticate users to third-party** ~~internet facing~~**online services that process, store or communicate their organisation's non-sensitive data.**	Multi-factor authentication (where available) is used ~~by an organisation's users when they~~to authenticate users to third-party ~~internet facing~~online services that process, store or communicate their organisation's non-sensitive data.	Multi-factor authentication (where available) is used ~~by an organisation's users when they~~to authenticate users to third-party ~~internet facing~~online services that process, store or communicate their organisation's non-sensitive data.

ASD Essential Eight: November 2023 Changes

IIS Partners

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	Multi-factor authentication is ~~enabled by default for an organisation's non-organisational users (but they can choose~~**used to** ~~opt out) when they~~ **authenticate users to** ~~the~~**their organisation's online customer services that process, store or communicate their organisation's** ~~internet-facing services~~**sensitive customer data.**	Multi-factor authentication is ~~enabled by default for an organisation's non-organisational users (but they can choose~~used to ~~opt out) when they~~ authenticate users to ~~the~~their organisation's online customer services that process, store or communicate their organisation's ~~internet-facing services~~sensitive customer data.	Multi-factor authentication is ~~enabled by default for an organisation's non-organisational users (but they can choose~~used to ~~opt out) when they~~ authenticate users to ~~the~~their organisation's online customer services that process, store or communicate their organisation's ~~internet-facing services~~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 customer services that process, store or communicate sensitive customer data.	Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.	Multi-factor authentication is used to authenticate customers to online 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 ~~**important data repositories**~~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 ~~**is phishing-resistant and**~~~~uses~~ 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.**

ASD Essential Eight: November 2023 Changes

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	**Multi-factor authentication used for authenticating users of systems is phishing-resistant.**	Multi-factor authentication used for authenticating users of systems is phishing-resistant.
	–	–	**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.**	**~~Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.~~**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.

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

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	Unprivileged accounts cannot logon to privileged operating environments.	Unprivileged accounts cannot logon to privileged operating environments.	Unprivileged accounts cannot logon to privileged operating environments.
	Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Privileged 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.**
	–	–	**Local Security Authority protection functionality is enabled.**
	–	–	**Credential Guard functionality is enabled.**
	–	–	~~**Credential Guard and**~~ **Remote Credential Guard** ~~**are**~~**functionality is enabled.**
	–	**Privileged access events are centrally logged.**	Privileged access events are centrally logged.
	–	**Privileged account and group management events are centrally logged.**	Privileged account and group management events are ~~**centrally**~~~~**logged**~~ 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.

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	–	**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.**	**~~Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.~~**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.
Application control	**~~–~~Application control is implemented on workstations.**	Application control is implemented on workstations **~~and internet-facing servers~~**.	Application control is implemented on workstations **~~and servers~~**.
	–	**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.

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	~~The~~**Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets** ~~is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.~~**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 ~~and drivers~~ ~~to an organisation-approved set.
	–	–	**Application control restricts the execution of drivers to an organisation-approved set.**
	–	~~–~~**Microsoft's recommended application blocklist is implemented.**	Microsoft's ~~'~~recommended ~~block rules' are~~application blocklist is implemented.
	–	–	**Microsoft's ~~'recommended~~vulnerable driver ~~block rules' are~~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 ~~execution~~application control events ~~on workstations and internet-facing servers~~ are centrally logged.**	Allowed and blocked ~~execution~~application control events ~~on workstations and~~ ~~servers~~ are ~~centrally~~logged 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 ~~monitored for signs of compromise and actioned when any signs of compromise are detected~~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.**

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	**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.
	–	**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.
~~Configure~~Restrict **Microsoft Office ~~macro settings~~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 ~~validating~~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 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.**

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	–	**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.
	~~–~~	~~**Allowed and blocked Microsoft Office macro execution events are logged.**~~]	~~Allowed and blocked Microsoft Office macro execution events are **centrally** logged.~~
	~~–~~	~~–~~	~~**Event logs are protected from unauthorised modification and deletion.**~~
			~~**Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.**~~
User application hardening	**Internet Explorer 11** ~~does not process content from the internet~~ **is disabled or removed.**	Internet Explorer 11 ~~does not process content from the internet~~ **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 ~~or~~and vendor hardening guidance ~~for web browsers is implemented~~, with the most restrictive guidance taking precedence when conflicts occur.**	Web browsers are hardened using ASD ~~or~~and vendor hardening guidance ~~for web browsers is implemented~~, with the most restrictive guidance taking precedence when conflicts occur.
	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.

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	**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 ~~OLE~~Object Linking and Embedding packages.**	Microsoft Office is configured to prevent activation of ~~OLE~~Object Linking and Embedding packages.
	–	**Office productivity suites are hardened using ASD ~~or~~and vendor hardening guidance ~~for Microsoft Office is implemented~~, with the most restrictive guidance taking precedence when conflicts occur.**	Office productivity suites are hardened using ASD ~~or~~and vendor hardening guidance ~~for Microsoft Office is implemented~~, with the most restrictive guidance taking precedence when conflicts occur.
	–	**~~Microsoft~~ Office productivity suite security settings cannot be changed by users.**	~~Microsoft~~ 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 ~~or~~and vendor hardening guidance ~~for PDF software is implemented~~, with the most restrictive guidance taking precedence when conflicts occur.**	PDF software is hardened using ASD ~~or~~and vendor hardening guidance ~~for PDF software is implemented~~, 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.**
	–	–	**Windows PowerShell 2.0 is disabled or removed.**
	–	–	**PowerShell is configured to use Constrained Language Mode.**

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	~~Blocked~~ **PowerShell module logging, script ~~execution~~block logging and transcription events are centrally logged.**	~~Blocked~~ PowerShell module logging, script ~~execution~~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.**	**~~Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.~~**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.
Regular backups	**Backups of ~~important~~ data, ~~software~~applications and ~~configuration~~ settings are performed and retained ~~with a frequency and retention timeframe~~ in accordance with business criticality and business continuity requirements.**	Backups of ~~important~~ data, ~~software~~applications and ~~configuration~~ settings are performed and retained ~~with a frequency and retention timeframe~~ in accordance with business criticality and business continuity requirements.	Backups of ~~important~~ data, ~~software~~applications and ~~configuration~~ settings are performed and retained ~~with a frequency and retention timeframe~~ in accordance with business criticality and business continuity requirements.

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	Backups of ~~important~~ data, ~~software~~applications and ~~configuration~~ settings are synchronised to enable restoration to a common point in time.	Backups of ~~important~~ data, ~~software~~applications and ~~configuration~~ settings are synchronised to enable restoration to a common point in time.	Backups of ~~important~~ data, ~~software~~applications and ~~configuration~~ settings are synchronised to enable restoration to a common point in time.
	Backups of ~~important~~ data, ~~software~~applications and ~~configuration~~ settings are retained in a secure and resilient manner.	Backups of ~~important~~ data, ~~software~~applications and ~~configuration~~ settings are retained in a secure and resilient manner.	Backups of ~~important~~ data, ~~software~~applications and ~~configuration~~ settings are retained in a secure and resilient manner.
	Restoration of ~~important~~ data, ~~software~~applications and ~~configuration~~ settings from backups to a common point in time is tested as part of disaster recovery exercises.	Restoration of ~~important~~ data, ~~software~~applications and ~~configuration~~ settings from backups to a common point in time is tested as part of disaster recovery exercises.	Restoration of ~~important~~ data, ~~software~~applications and ~~configuration~~ settings from backups to a common point in time is tested as part of disaster recovery exercises.
	Unprivileged accounts cannot access backups belonging to other accounts.	Unprivileged accounts cannot access backups belonging to other accounts.	Unprivileged accounts cannot access backups belonging to other accounts~~, nor their own accounts~~.
	–	–	**Unprivileged accounts cannot access their own backups.**
	–	**Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.**	Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts~~, nor their own accounts~~.
	–	–	**Privileged accounts (excluding backup administrator accounts) cannot access their own backups.**
	Unprivileged accounts are prevented from modifying and deleting backups.	Unprivileged accounts are prevented from modifying and deleting backups.	Unprivileged accounts are prevented from modifying and deleting backups.
	–	**Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.**	Privileged accounts (~~including~~ excluding backup administrator accounts) are prevented from modifying and deleting backups ~~during their retention period~~.
	–	–	**Backup administrator accounts are prevented from modifying and deleting backups during their retention period.**