Victorian Government Cyber Maturity Benchmark

In partnership with the Department of Government Services, Victoria

Benchmark Frameworks (Updated 2024)

Contents

VMIA is the Victorian Government's insurer and risk adviser

Level 10 South
161 Collins Street
Melbourne VIC 3000

P (03) 9270 6900
contact@vmia.vic.gov.au
ABN 39 682 497 841

vmia.vic.gov.au

Victorian Managed Insurance Authority (VMIA) acknowledges the Traditional Custodians of the land on which we do business, and we pay our respects to Elders past, present, and emerging. We acknowledge the important contribution that Aboriginal and Torres Strait Islander peoples make in creating a thriving Victoria.

ACSC Essential Eight Mitigation Strategies

The Victorian Government Cyber Maturity Benchmark uses the current Australian Cyber Security Centre's (ACSC) Essential Eight Maturity Model. ACSC recommends organisations implement the Essential Eight mitigation strategies as a baseline.

Mitigation Strategy	Description
Application control	Application control is a security approach designed to protect against malicious code (also known as malware) executing on systems. When implemented robustly, it ensures only approved applications (e.g. executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers) can be executed. While application control is primarily designed to prevent the execution and spread of malicious code, it can also prevent the installation or use of unapproved applications.
Patch applications	Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patching applications is the systematic implementation of software updates to ensure functionality and security updates/fixes are applied to applications within your ICT environment. Patching applications prevents attackers from using known security vulnerabilities to breach your network and achieve their objectives.
Configure Microsoft Office macro settings	Microsoft Office applications commonly used across the Victorian public sector can execute macros to automate routine tasks. A macro is an embedded code containing a series of commands which can enable highly efficient repetitive processes. However, macros can contain malicious code resulting in unauthorised access to sensitive information as part of a targeted cyber intrusion, including being used to download other malicious software. Microsoft Office environments can be configured to prevent macros which have come from the internet or have not been identified as trusted or verified.
User application hardening	User application hardening reduces the 'attack surface' malicious cyber actors can utilise to deploy malicious software onto user systems (e.g. workstations). Blocking or removing common software used to download or run malicious software prevents malicious software from running on organisation networks and disrupting ICT services.
Restrict administrative privileges	User accounts with administrative privileges for operations systems and applications are able to make significant changes to workstations and network configurations, bypass security settings and access, modify or delete sensitive information. Higher level administrators, such as Domain Administrators, have similar ability on entire networks. Attackers when they have access to accounts with administrator access, can access more computer and system resources than regular users. This can occur when an administrators account is breached or a regular user account's privileges are escalated to those of an

Mitigation Strategy	Description
	administrator. Restricting administers privileges does not seek to prevent legitimate administrator activity but introduce safeguards from preventing account misuse. Restricting administers privileges can also prevent unintentional changes to network environments. To be effective, all administrators accounts must have restrictions placed on their use.
Patch operating systems	Patching operating systems is the process of keeping our workstations and servers up to date with the latest stable software released by the vendor to mitigate any identified vulnerabilities that may be present. Patching improves security, functionality, reliability and user experience. Updating operating systems, like patching applications, is the systematic implementation of software updates to ensure functionality and security updates/fixes are applied to your ICT environment. Patching operating systems prevents attackers from using known security vulnerabilities to attack your network devices and achieve their objectives.
Multi-factor authentication	Multi-factor authentication is one of the most effective security measures organisations can implement to prevent attackers from gaining access to networks and devices. Multi-factor authentication makes it significantly more difficult for an adversary to get a complete set of credentials even if they get to know the username and password. Multi-factor authentication should be implemented for remote access solutions, users performing privileged actions and users accessing important (sensitive or high availability) data. The most common form of multi-factor authentication is using two-factor authentication, where a one-time code is required in addition to a username and password to access a system. More secure forms of multi-factor build on this by requiring a physical token in addition to the username, password and one-time code. It is important to consider the risks associated with your system to determine whether higher levels of multi-factor are necessary.
Regular backups	Backups of important/new information and software are a means to restore system operating systems quickly following a service disruption. Critically, backups must be tested to ensure they are functioning correctly, and organisations have sufficient processes to effectively recover the data they need. Storing backup data 'offline', where backups cannot be accessed or written over from the network, is an increasingly important security control as attackers commonly target backups. Regular backups of important system data is increasingly important as more government services move online, and critical data must be retained in the case of a cyber incident to minimise disruptions to service operations.

Benchmark Framework - Essential Eight (November 2023)

Common across all controls

Current maturity level (0-3)	Desired maturity level (0-3)

Control effective: Coverage	
Amount of compliant systems (Systems in scope which have implemented the mitigation strategy)	Less than half (<50%), Approx half (51-70%), Most (71-99%), All (100%)
Risk impact of non-compliant systems (VPDSF BIL)	Insignificant, Minor, Moderate, Major, Severe

Control effective: Assurance	
Assurance over the controls	Self-assessed, SME assessed, Internal audit, External audit
How old is that assurance?	<1 year, 1-2 years, 2-3 years, >3 years

Maturity level zero

The maturity level zero was introduced from 2021 update onwards. This maturity level signifies that there are weaknesses in an organisation's overall cyber security posture. When exploited, these weaknesses could facilitate the compromise of the confidentiality of their data, or the integrity or availability of their systems and data, as described by the tradecraft and targeting in Maturity Level One below.

- Not yet Maturity Level One, or not yet aligned to the intent of the mitigation strategy.

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.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	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 online 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 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 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-	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.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	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 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 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,	Office productivity suites, web browsers and their extensions, email	Office productivity suites, web browsers and their extensions, email

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	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 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 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-	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations,	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations,

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	facing servers and non-internet-facing network devices.	non-internet- facing servers and non-internet-facing network devices.	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 vulnerabilities are 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 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 internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
	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,

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
			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.
	–	–	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

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
			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 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	Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate	Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	their organisation's non-sensitive data.	their organisation's non-sensitive data.	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 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 systems.
	–	–	Multi-factor authentication is used to authenticate users of data repositories.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	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.
	–	–	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	Event logs from internet-facing servers are analysed in a timely

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
		manner to detect cyber security events.	manner to detect cyber security events.
	–	–	Event logs from non-internet-facing servers 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.
	–	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.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	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 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, applications and data repositories is limited to only what is required for users and services to undertake their duties.
	Privileged accounts (excluding 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 (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.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	Privileged operating environments are not virtualised within unprivileged operating environments.	Privileged operating environments are not virtualised within unprivileged operating environments.
	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.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	–	Remote Credential Guard 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.
	–	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	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
		soon as possible after they occur or are discovered.	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.	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	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	control panel applets to an organisation-approved set.	control panel applets to an organisation-approved set.	control panel applets 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 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.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	–	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.
	–	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

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
			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 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.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	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.
	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.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	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.
	–	–	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.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	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.
	–	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.

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.
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 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.
	–	–	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.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	–	–	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 (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.

Benchmark Framework - Essential Eight (November 2022)

Common across all controls

Current maturity level (0-3)
Desired maturity level (0-3)

Control effective: Coverage	
Amount of compliant systems	Less than half, Approx half, Most, All
Risk impact of non-compliant systems	Insignificant, Minor, Moderate, Major, Severe

Control effective: Assurance	
Assurance over the controls	Self-assessed, SME assessed, Internal audit, External audit
How old is that assurance?	<1 year, 1-2 years, 2-3 years, >3 years

Maturity level zero

The maturity level zero was introduced from 2021 update onwards. This maturity level signifies that there are weaknesses in an organisation's overall cyber security posture. When exploited, these weaknesses could facilitate the compromise of the confidentiality of their data, or the integrity or availability of their systems and data, as described by the tradecraft and targeting in Maturity Level One below.

- Not yet Maturity Level One, or not yet aligned to the intent of the mitigation strategy.

Maturity level descriptors

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Application control	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.	Application control is implemented on workstations and internet-facing servers. Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an	Application control is implemented on workstations and servers. Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
		organisation-approved set. Allowed and blocked execution events on workstations and internet-facing servers are logged.	**drivers** to an organisation-approved set. Microsoft's 'recommended block rules' are implemented. Microsoft's 'recommended driver block rules' are implemented. Application control rulesets are validated on an annual or more frequent basis. Allowed and blocked execution events on workstations and **servers** 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.
Patch applications	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 is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software,	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 is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. A vulnerability scanner is used at least **weekly** to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software,	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 is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software,

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	and security products. Patches, updates or vendor mitigations for security vulnerabilities in internet- facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release. Internet-facing services, 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.	and security products. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications. Patches, updates or vendor mitigations for security vulnerabilities in internet- facing services are applied within **two weeks** of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security 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 vendor mitigations for security vulnerabilities in other applications are applied within one month of release. Internet-facing services, 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.	and security products. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications. Patches, updates or vendor mitigations for security vulnerabilities in internet- facing services are applied within two weeks of release, **or within 48 hours if an exploit exists.** Patches, updates or vendor mitigations for security 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. Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month of release. **Applications** that are no longer supported by vendors are removed.
Configure Microsoft Office macro settings	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. Microsoft Office macros in files originating from the internet are blocked. Microsoft Office macro antivirus scanning is enabled.	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. Microsoft Office macros in files originating from the internet are blocked. Microsoft Office macro antivirus scanning is enabled.	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.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	Microsoft Office macro security settings cannot be changed by users.	Microsoft Office macros are blocked from making Win32 API calls. Microsoft Office macro security settings cannot be changed by users. Allowed and blocked Microsoft Office macro execution events are logged.	Only privileged users responsible for validating 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'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 macro antivirus scanning is enabled. Microsoft Office macros are blocked from making Win32 API calls. Microsoft Office macro security settings cannot be changed by users. 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	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 does not process	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 does not process	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 is disabled or

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	content from the internet.	content from the internet.	removed.
	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 OLE packages.	Microsoft Office is configured to prevent activation of OLE packages.
		Microsoft Office security settings cannot be changed by users.	Microsoft Office 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 security settings cannot be changed by users.	PDF software security settings cannot be changed by users.
		ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.	ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.
		Blocked PowerShell script execution events are logged.	.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.
			Blocked PowerShell script execution events are centrally logged.
			Event logs are protected from unauthorised modification and deletion.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
			Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.
Restrict administrative privileges	Requests for privileged access to systems and applications are validated when first requested. Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Requests for privileged access to systems and applications are validated when first requested. Privileged access to systems and applications is automatically disabled after 12 months unless revalidated. Privileged access to systems and applications is automatically disabled after 45 days of inactivity. Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Privileged operating environments are not virtualised within unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. Administrative activities are conducted through jump servers. Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed.	Requests for privileged access to systems and applications are validated when first requested. Privileged access to systems and applications is automatically 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 limited to only what is required for users and services to undertake their duties. Privileged accounts are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Privileged operating environments are not virtualised within unprivileged operating environments. Unprivileged accounts cannot logon to privileged 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.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
		Privileged access events are logged. Privileged account and group management events are logged.	Administrative activities are conducted through jump servers. Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed. Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled. Privileged access events are centrally logged. Privileged account and group management 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.
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. 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 security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in	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 is used at least daily to identify missing patches or updates for security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in	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 is used at least daily to identify missing patches or updates for security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	operating systems of workstations, servers and network devices. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release. Operating systems that are no longer supported by vendors are replaced.	operating systems of workstations, servers and network devices. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within **two weeks** of release. Operating systems that are no longer supported by vendors are replaced.	operating systems of workstations, servers and network devices. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release, **or within 48 hours if an exploit exists.** The latest release, or the previous release, of operating systems are used. Operating systems that are no longer supported by vendors are replaced.
Multi-factor authentication	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services. Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services. Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services. Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services.	default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services. Multi-factor authentication is used to authenticate privileged users of systems. 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. Successful and unsuccessful multi-factor authentication events are logged.	default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services. Multi-factor authentication is used to authenticate privileged users of systems. Multi-factor authentication is used to authenticate users accessing important data repositories. Multi-factor authentication is phishing-resistant and uses either: something users have and something users know, or something users have that is unlocked by something users know or are. Successful and unsuccessful multi-factor authentication 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.
Regular Backups	Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements. Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time. Backups of important data, software and	Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements. Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time. Backups of important data, software and	Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements. Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time. Backups of important data, software and

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	configuration settings are retained in a secure and resilient manner. Restoration of important data, software 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 are prevented from modifying and deleting backups.	configuration settings are retained in a secure and resilient manner. Restoration of important data, software 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. Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts. Unprivileged accounts are prevented from modifying and deleting backups. Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.	configuration settings are retained in a secure and resilient manner. Restoration of important data, software 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, nor their own accounts. Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts, nor their own accounts. Unprivileged accounts are prevented from modifying and deleting backups. Privileged accounts (including backup administrator accounts) are prevented from modifying and deleting backups during their retention period.

Benchmark Framework - Essential Eight (July 2021)

Common across all controls

Current maturity level (0-3)
Desired maturity level (0-3)

Control effective: Coverage	
Amount of compliant systems	Less than half, Approx half, Most, All
Risk impact of non-compliant systems	Insignificant, Minor, Moderate, Major, Severe

Control effective: Assurance	
Assurance over the controls	Self-assessed, SME assessed, Internal audit, External audit
How old is that assurance?	<1 year, 1-2 years, 2-3 years, >3 years

Maturity level zero

The maturity level zero was introduced from 2021 update onwards. This maturity level signifies that there are weaknesses in an organisation's overall cyber security posture. When exploited, these weaknesses could facilitate the compromise of the confidentiality of their data, or the integrity or availability of their systems and data, as described by the tradecraft and targeting in Maturity Level One below.

- Not yet Maturity Level One, or not yet aligned to the intent of the mitigation strategy.

Maturity level descriptors

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Application control	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.	**Application control is implemented on workstations and internet-facing servers to restrict** the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets **to an organisation-approved set.**	Application control is implemented on workstations and **servers** to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets **and drivers** to an organisation-approved set. Microsoft's 'recommended block rules' are

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
		Allowed and blocked executions on workstations and internet-facing servers are logged.	implemented. Microsoft's 'recommended driver block rules' are implemented. Application control rulesets are validated on an annual or more frequent basis. Allowed and blocked executions on workstations and servers are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.
Patch applications	Patches, updates or vendor mitigations for security vulnerabilities in internet- facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release. A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	Patches, updates or vendor mitigations for security vulnerabilities in internet- facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security 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 vendor mitigations for security vulnerabilities in other applications are applied within one month. A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. A vulnerability scanner is used at least **weekly** to identify missing patches or updates for security vulnerabilities in office	Patches, updates or vendor mitigations for security vulnerabilities in internet- facing services are applied within two weeks of release, or **within 48 hours if an exploit exists.** Patches, updates or vendor mitigations for security 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.** Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month. A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches or

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	Internet-facing services, 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.	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 security vulnerabilities in other applications. Internet-facing services, 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.	updates for security 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 security vulnerabilities in other applications. Applications that are no longer supported by vendors are removed.
Configure Microsoft Office macro settings	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. Microsoft Office macros in files originating from the internet are blocked. Microsoft Office macro antivirus scanning is enabled. Microsoft Office macro security settings cannot be changed by users.	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. Microsoft Office macros in files originating from the internet are blocked. Microsoft Office macro antivirus scanning is enabled. Microsoft Office macros are blocked from making Win32 API calls. Microsoft Office macro security settings cannot be changed by users. Allowed and blocked Microsoft Office macro executions are logged.	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. Only privileged users responsible for validating 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'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 macro antivirus scanning is

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
			enabled. Microsoft Office macros are blocked from making Win32 API calls. Microsoft Office macro security settings cannot be changed by users. Allowed and blocked Microsoft Office macro executions are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.
User application hardening	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 does not process content from the internet. Web browser security settings cannot be changed by users.	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 does not process content from the internet. Microsoft Office is blocked from creating child processes. Microsoft Office is blocked from creating executable content. Microsoft Office is blocked from injecting code into other processes. Microsoft Office is configured to prevent activation of OLE packages. PDF software is blocked from creating child processes. ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 is disabled or removed. Microsoft Office is blocked from creating child processes. Microsoft Office is blocked from creating executable content. Microsoft Office is blocked from injecting code into other processes. Microsoft Office is configured to prevent activation of OLE packages. PDF software is blocked from creating child processes. ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
		Web browser, Microsoft Office and PDF software security settings cannot be changed by users. Blocked PowerShell script executions are logged.	Web browser, Microsoft Office and PDF software security settings cannot be changed by users. .NET Framework 3.5 (including .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. Blocked PowerShell script executions are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.
Restrict administrative privileges	Requests for privileged access to systems and applications are validated when first requested. Privileged accounts are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Requests for privileged access to systems and applications are validated when first requested. Privileged access to systems and applications is automatically disabled after 12 months unless revalidated. Privileged access to systems and applications is automatically disabled after 45 days of inactivity. Privileged accounts are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Privileged operating environments are not virtualised within unprivileged operating	Requests for privileged access to systems and applications are validated when first requested. Privileged access to systems and applications is automatically 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 limited to only what is required for personnel and services to undertake their duties. Privileged accounts and service accounts are prevented from accessing the internet, email and web services.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
		environments. Unprivileged accounts cannot logon to privileged operating environments. Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. Administrative activities are conducted through jump servers. Credentials for local administrator and service accounts are unique, unpredictable and managed. Use of privileged access is logged. Changes to privileged accounts and groups are logged.	Privileged users use separate privileged and unprivileged operating environments. Privileged operating environments are not virtualised within unprivileged operating environments. Unprivileged accounts cannot logon to privileged 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. Credentials for local administrator and service accounts are unique, unpredictable and managed. Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled. Use of privileged access is centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected. Changes to privileged accounts and groups are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Patch operating systems	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release. A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least fortnightly to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices. Operating systems that are no longer supported by vendors are replaced.	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release. A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices. Operating systems that are no longer supported by vendors are replaced.	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release, or within 48 hours if an exploit exists. A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices. The latest release, or the previous release, of operating systems are used for workstations, servers and network devices. Operating systems that are no longer supported by vendors are replaced.
Multi-factor authentication	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation’s internet-facing services. Multi-factor authentication is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation’s internet-facing services. Multi-factor authentication is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation’s internet-facing services. Multi-factor authentication is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation’s internet-facing services.	organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation’s internet-facing services. Multi-factor authentication is used to authenticate privileged users of systems. 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. Successful and unsuccessful multi-factor authentications are logged.	organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation’s internet-facing services. Multi-factor authentication is used to authenticate privileged users of systems. Multi-factor authentication is used to authenticate users accessing important data repositories. Multi-factor authentication **is verifier impersonation resistant and** uses either: something users have and something users know, or something users have that is unlocked by something users know or are. Successful and unsuccessful multi-factor authentications are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.
Regular Backups	Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business	Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business	Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	continuity requirements.	continuity requirements.	continuity requirements.
	Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises.	Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises.	Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises.
	Unprivileged accounts can only access their own backups.	Unprivileged accounts, **and privileged accounts (excluding backup administrators)**, can only access their own backups.	Unprivileged accounts, and privileged accounts (excluding backup administrators), **can't access backups.**
	Unprivileged accounts are prevented from modifying or deleting backups.	Unprivileged accounts, **and privileged accounts (excluding backup administrators)**, are prevented from modifying or deleting backups.	Unprivileged accounts, and privileged accounts (excluding backup **break glass accounts**), are prevented from modifying or deleting backups.

Benchmark Framework - Essential Eight (June 2020)

Common across all controls

Current maturity level (1-3)
Desired maturity level (1-3)

Control effective: Coverage	
Amount of compliant systems	Less than half, Approx. half, Most, All
Risk impact of non-compliant systems	Insignificant, Minor, Moderate, Major, Severe

Control effective: Assurance	
Assurance over the controls	Self-assessed, SME assessed, Internal audit, External audit
How old is that assurance?	<1 year, 1-2 years, 2-3 years, >3 years

Maturity level descriptors

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Application control	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, 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	Security vulnerabilities in applications and drivers assessed as extreme risk are	Security vulnerabilities in applications and drivers assessed as extreme risk are	Security vulnerabilities in applications and drivers assessed as extreme risk are

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
	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.	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.	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.
Configure Microsoft Office macro settings	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 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

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
			activation of Object Linking and Embedding packages.
Restrict administrative privileges	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 data repositories 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 data repositories is validated when first requested and revalidated on an annual or more frequent basis. Privileged access to systems, applications and data repositories 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.
Patch operating systems	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.

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Multi-factor authentication	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, 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, 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, Universal 2nd Factor security keys, physical one-time password tokens, biometrics or smartcards.
Daily backups	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.

More information

For more information on the Essential Eight Maturity Model changes, please visit: Essential Eight Maturity Model FAQ | Cyber.gov.au