



Essential Eight Report – ISM Compliance

For
"White Rook Cyber"

Prepared by
Emerson Pyrke

Your nominated Maturity Level is:
Maturity Level 2 (ML2)

Report Period

This Essential Eight Report covers the period of 8th Nov 2024 - 8th Nov 2024.

Purpose of this report

This report measures your organisation's alignment with the ISM controls required to meet ACSC's Essential Eight mitigations. (Please see Attachment A for more information on the Essential Eight).

Interpreting the report

This report contains an evaluation of the organisation's adherence to the Information Security Manual (ISM) controls that make up the Essential Eight Strategies throughout the reporting period, reporting the last recorded result for each device in the reporting period.

What is the Maturity Model?

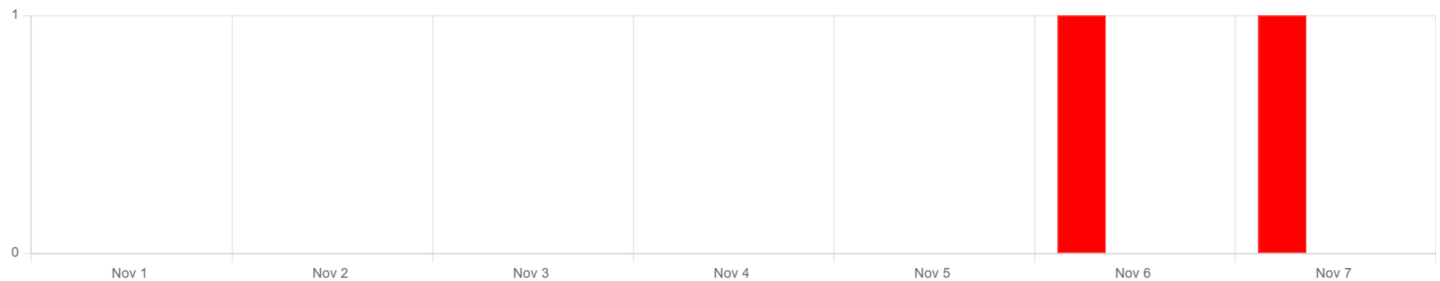
To assist organisations with their implementation of the Essential Eight, four maturity levels have been defined (Maturity Level Zero through to Maturity Level Three). With the exception of Maturity Level Zero, the maturity levels are based on mitigating increasing levels of adversary tradecraft (i.e. tools, tactics, techniques and procedures). Your organisation has elected to report its compliance against Maturity Level 2.

Maturity Level	Description
0	Not aligned with mitigation strategy objectives.
1	Partly aligned with mitigation strategy objectives.
2 – Recommended Minimum Level	Mostly aligned with mitigation strategy objectives.
3	Fully aligned with mitigation strategy objectives.

Compliance Summary

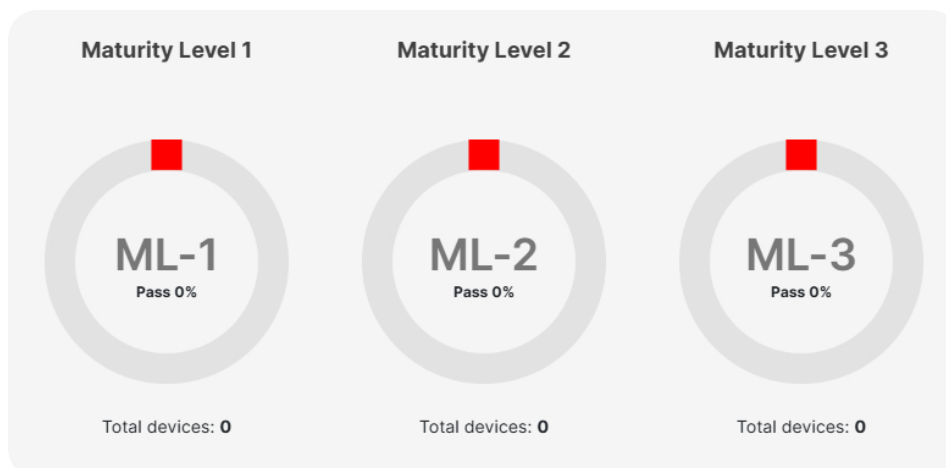
Maturity Level 2	Number of Controls	Number of Devices	ML2 Pass Rate	ML2 Fail
Patch Applications	11	0	0%	100.00%
Patch Operating Systems	8	0	0%	100.00%
Multi-factor Authentication	19	0	0%	100.00%
Restricting Administrative Privileges	20	0	0%	100.00%
Application Control	14	0	0%	100.00%
Restrict Microsoft Office Macro	5	0	0%	100.00%
User Application Hardening	22	0	0%	100.00%
Regular Backups	8	0	0%	100.00%
Total Controls	107			
Pass rate %	0%			

Rolling 28-day Trend for ML2



Overall Average Score

This is a single score that represents the maturity of the organisation by Maturity Level.



Patch Applications

Maturity Level



Total devices: 0

Pass (0 devices)

Override Pass (0 devices)

Fail (0 devices)

Failed ISM's 11

Why should Patch Applications be implemented?

Patching applications is one of the most effective controls an organisation can implement to prevent cyber criminals from gaining access to their devices and sensitive information. Patches improve the security of applications by fixing known vulnerabilities. Cyber criminals exploit vulnerabilities as soon as they are publicly disclosed so organisations should patch their applications as a priority.

Cyber criminals scan internet-facing services with automated tools that gather information about potentially vulnerable systems. This information can be used by cyber criminals to target at-risk businesses. Regular vulnerability scanning can identify gaps in an organisation's attack surface that require patching.

ISM	Type	Pass	Fail	Description
ISM 1690	T	0	0	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.
ISM 1691	T	0	0	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.
ISM 1693	T	0	0	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.
ISM 1698	T	0	0	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
ISM 1699	P	0	0	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.
ISM 1700	P	0	0	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.
ISM 1704	T	0	0	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.

Essential Eight Report – ISM Compliance

ISM	Type	Pass	Fail	Description
ISM 1807	P	0	0	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
ISM 1808	P	0	0	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
ISM 1876	P	0	0	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.
ISM 1905	P	0	0	Online services that are no longer supported by vendors are removed.

 Pass  Fail  Override Pass  Partial Pass  Not Applicable

Patch Operating Systems

Maturity Level



Total devices: 0

Pass (0 devices)

Override pass (0 devices)

Fail (0 devices)

Failed ISM's 8

Why should Patch Operating Systems be implemented?

Patch Operating Systems is one of the most effective controls an organisation can implement to prevent an adversary from gaining access to their devices and sensitive information. Patches improve the security of Operating Systems by fixing known vulnerabilities.

ISM	Type	Pass	Fail	Description
ISM 1501	T	0	0	Operating systems that are no longer supported by vendors are replaced.
ISM 1694	T	0	0	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.
ISM 1695	T	0	0	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.
ISM 1701	T	0	0	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.
ISM 1702	P	0	0	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.
ISM 1807	P	0	0	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
ISM 1808	P	0	0	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
ISM 1877	T	0	0	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of

Essential Eight Report – ISM Compliance

ISM	Type	Pass	Fail	Description
-----	------	------	------	-------------

ISM 1877

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.

 Pass  Fail  Override Pass  Partial Pass  Not Applicable

Multi-factor Authentication

Maturity Level



Total devices: 0

Pass (0 devices)

Override Pass (0 devices)

Fail (0 devices)

Failed ISM's 19




Why should Multi-factor Authentication be implemented?

Multi-factor authentication (MFA) is in place when an organisation uses two or more different types of actions to verify its identity. Example include receipt of an authentication code by SMS text message after entering a password to log into an online account. MFA is one of the best ways to protect against someone breaking into an account. It makes it harder for cyber criminals to take over accounts, by adding extra layers of protection.

ISM	Type	Pass	Fail	Description
ISM 0123	P	0	0	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.
ISM 0140	P	0	0	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
ISM 0974	P	0	0	Multi-factor authentication is used to authenticate unprivileged users of systems.
ISM 1173	P	0	0	Multi-factor authentication is used to authenticate privileged users of systems.
ISM 1228	P	0	0	Cyber security events are analysed in a timely manner to identify cyber security incidents.
ISM 1401	P	0	0	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.
ISM 1504	P	0	0	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.
ISM 1679	P	0	0	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.
ISM 1680	P	0	0	Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation's non-sensitive data.
ISM 1681	P	0	0	Multi-factor authentication is used to authenticate customers to online customer services that

Essential Eight Report – ISM Compliance

ISM	Type	Pass	Fail	Description
ISM 1681				process, store or communicate sensitive customer data.
ISM 1682	P	0	0	Multi-factor authentication used for authenticating users of systems is phishing-resistant.
ISM 1683	P	0	0	Successful and unsuccessful multi-factor authentication events are centrally logged.
ISM 1815	P	0	0	Event logs are protected from unauthorised modification and deletion.
ISM 1819	P	0	0	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
ISM 1872	P	0	0	Multi-factor authentication used for authenticating users of online services is phishing-resistant.
ISM 1873	P	0	0	Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.
ISM 1892	P	0	0	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.
ISM 1893	P	0	0	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.
ISM 1906	P	0	0	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.

 Pass  Fail  Override Pass  Partial Pass  Not Applicable

Restrict Administrative Privileges

Maturity Level



Total devices: 0

Pass (0 devices)

Override Pass (0 devices)

Fail (0 devices)

Failed ISM's 20

Why should Restrict Administrative Privileges be implemented?

Restricting administrative privileges is one of the most effective mitigation strategies to ensure the security of systems.

Users with administrative privileges for Operating Systems and applications are able to make significant changes to their configuration and operation, bypass critical security settings and access sensitive data. Domain administrators have similar abilities for an entire network domain, which usually includes all of the workstations and servers on the network.

Malicious actors often use malicious code (also known as malware) to exploit vulnerabilities in workstations and servers. Restricting administrative privileges makes it more difficult for malicious actors to elevate privileges, spread to other hosts, hide their existence, persist after reboot, obtain sensitive data or resist removal efforts.

An environment where administrative privileges are restricted is more stable, predictable, and easier to administer and support, as fewer users can make significant changes to their operating environment, either intentionally or unintentionally.

ISM	Type	Pass	Fail	Description
ISM 0123	P	0	0	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.
ISM 0140	P	0	0	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
ISM 0445	P	0	0	Privileged users are assigned a dedicated privileged account to be used solely for duties requiring privileged access.
ISM 1175	P	0	0	Privileged accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.
ISM 1228	P	0	0	Cyber security events are analysed in a timely manner to identify cyber security incidents.
ISM 1380	P	0	0	Privileged users use separate privileged and unprivileged operating environments.
ISM 1387	P	0	0	Administrative activities are conducted through jump servers.
ISM 1507	P	0	0	Requests for privileged access to systems, applications and data repositories are validated when first requested.
ISM 1509	P	0	0	Privileged access events are centrally logged.

Essential Eight Report – ISM Compliance

ISM	Type	Pass	Fail	Description
ISM 1647	P	0	0	Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.
ISM 1648	P	0	0	Privileged access to systems and applications is disabled after 45 days of inactivity.
ISM 1650	P	0	0	Privileged account and group management events are centrally logged.
ISM 1685	P	0	0	Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.
ISM 1687	P	0	0	Privileged operating environments are not virtualised within unprivileged operating environments.
ISM 1688	P	0	0	Privileged operating environments are not virtualised within unprivileged operating environments.
ISM 1689	P	0	0	Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.
ISM 1815	P	0	0	Event logs are protected from unauthorised modification and deletion.
ISM 1819	P	0	0	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
ISM 1883	P	0	0	Privileged accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.
ISM 1906	P	0	0	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.

 Pass  Fail  Override Pass  Partial Pass  Not Applicable

Application Control

Maturity Level



Total devices: 0

Pass (0 devices)

Override pass (0 devices)

Fail (0 devices)

Failed ISM's 14

Why should Application Control be implemented?

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.

In addition to preventing the execution of unapproved applications, Application Control can contribute to the identification of attempts by malicious actors to execute malicious code. This can be achieved by configuring Application Control to generate event logs for allowed and blocked executions. Such event logs should ideally include information such as the name of the file, the date/time stamp and the username of the user attempting to execute the file.

ISM	Type	Pass	Fail	Description
ISM 0123	P	0	0	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.
ISM 0140	P	0	0	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
ISM 0843	T	0	0	Application control is implemented on workstations.
ISM 1228	P	0	0	Cyber security events are analysed in a timely manner to identify cyber security incidents.
ISM 1490	T	0	0	Application control is implemented on internet-facing servers.
ISM 1544	T	0	0	Microsoft's recommended application blocklist is implemented.
ISM 1582	P	0	0	Application control rulesets are validated on an annual or more frequent basis.
ISM 1657	T	0	0	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.
ISM 1660	T	0	0	Allowed and blocked application control events are centrally logged.
ISM 1815	P	0	0	Event logs are protected from unauthorised modification and deletion.

Essential Eight Report – ISM Compliance

ISM	Type	Pass	Fail	Description
ISM 1819	P	0	0	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
ISM 1870	T	0	0	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.
ISM 1871	T	0	0	Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.
ISM 1906	P	0	0	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.

 Pass  Fail  Override Pass  Partial Pass  Not Applicable

Restrict Microsoft Office Macros

Maturity Level



Total devices: 0

Pass (0 devices)

Override Pass (0 devices)

Fail (0 devices)

Failed ISM's 5

Why should Restrict Microsoft Office Macros be implemented?

Microsoft Office files can contain embedded code, known as a macro, that is written in the Visual Basic for Applications (VBA) programming language. These Macros may contain a series of commands that have been coded or recorded that can be replayed at a later time in order to automate repetitive tasks. Macros are powerful tools that can be easily created by users to greatly improve their productivity, however, malicious actors can also create macros to perform a variety of malicious activities, such as assisting in the compromise of systems in order to exfiltrate or deny access to sensitive data.

ISM	Type	Pass	Fail	Description
ISM 1488	T	0	0	Microsoft Office macros in files originating from the internet are blocked.
ISM 1489	T	0	0	Microsoft Office macro security settings cannot be changed by users.
ISM 1671	T	0	0	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.
ISM 1672	T	0	0	Microsoft Office macro antivirus scanning is enabled.
ISM 1673	T	0	0	Microsoft Office macros are blocked from making Win32 API calls.

● Pass
 ● Fail
 ● Override Pass
 ● Partial Pass
 ● Not Applicable

User Application Hardening

Maturity Level



Total devices: 0

Pass (0 devices)

Override pass (0 devices)

Fail (0 devices)

Failed ISM's 22





Why should User Application Hardening be implemented?

User application hardening protects an organisation from a range of threats including malicious websites, advertisements running malicious scripts and exploitation of vulnerabilities in unsupported software. These attacks often take legitimate application functionality and use it for malicious purposes. User application hardening makes it harder for cyber criminals to exploit vulnerabilities or at-risk functionality in an organisation's applications.

ISM	Type	Pass	Fail	Description
ISM 0123	P	0	0	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.
ISM 0140	P	0	0	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
ISM 1228	P	0	0	Cyber security events are analysed in a timely manner to identify cyber security incidents.
ISM 1412	T	0	0	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
ISM 1485	T	0	0	Web browsers do not process web advertisements from the internet.
ISM 1486	T	0	0	Web browsers do not process Java from the internet.
ISM 1542	T	0	0	Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.
ISM 1585	T	0	0	Web browser security settings cannot be changed by users.
ISM 1623	P	0	0	PowerShell module logging, script block logging and transcription events are centrally logged.
ISM 1654	T	0	0	Internet Explorer 11 is disabled or removed.

Essential Eight Report – ISM Compliance

ISM	Type	Pass	Fail	Description
ISM 1667	T	0	0	Microsoft Office is blocked from creating child processes.
ISM 1668	T	0	0	Microsoft Office is blocked from creating executable content.
ISM 1669	T	0	0	Microsoft Office is blocked from injecting code into other processes.
ISM 1670	T	0	0	PDF software is blocked from creating child processes.
ISM 1815	P	0	0	Event logs are protected from unauthorised modification and deletion.
ISM 1819	P	0	0	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
ISM 1823	T	0	0	Office productivity suite security settings cannot be changed by users.
ISM 1824	T	0	0	PDF software security settings cannot be changed by users.
ISM 1859	T	0	0	Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
ISM 1860	T	0	0	PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
ISM 1889	P	0	0	Command line process creation events are centrally logged.
ISM 1906	P	0	0	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.

 Pass  Fail  Override Pass  Partial Pass  Not Applicable

Regular Backups

Maturity Level



Total devices: 0

Pass (0 devices)

Override Pass (0 devices)

Fail (0 devices)

Failed ISM's 8

Why should Regular Backups be implemented?

Implementing regular backups will assist an organisation to recover and maintain its operations in the event of a cyber incident, for example, a ransomware attack. If access to files is lost, restoring from secure backups will enable the organisation to recover and start operating again sooner. Backups must be carefully scoped to ensure that they include all information an organisation requires to recover from a cyber incident. This typically includes important data, software and configuration settings. Regularly testing that backups can restore systems, software and important data will give an organisation confidence that it can recover from a cyber incident. By ensuring that unprivileged accounts can only access their own backups, the risk that a malicious actor will be able to compromise backups is reduced.

ISM	Type	Pass	Fail	Description
ISM 1511	P	0	0	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.
ISM 1515	P	0	0	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.
ISM 1705	P	0	0	Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.
ISM 1707	P	0	0	Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.
ISM 1810	P	0	0	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.
ISM 1811	P	0	0	Backups of data, applications and settings are retained in a secure and resilient manner.
ISM 1812	P	0	0	Unprivileged accounts cannot access backups belonging to other accounts.
ISM 1814	P	0	0	Unprivileged accounts are prevented from modifying and deleting backups.

● Pass
 ● Fail
 ● Override Pass
 ● Partial Pass
 ● Not Applicable

Attachment A - What is the Essential Eight

The Australian Cyber Security Centre (ACSC) recommends eight essential strategies to prevent malware delivery, limit the impact of cybersecurity attacks and improve recovery.

These strategies are defined as follows:

Mitigation Strategy	Applicable Controls	Why the Control is important
Patch Applications	Apply security fixes/patches or mitigations (temporary workarounds) for programs within a timely manner (48 Hours for internet-reachable applications). Do not use applications which are out-of-support and do not receive security fixes.	Unpatched applications can be exploited by attackers; and in the worst case enable an attacker to completely take over an application, access all information contained within and use this access to access connected systems.
Patch Operating Systems	Apply security fixes/patches or temporary workarounds/mitigations for Operating Systems (e.g. Windows) within a timely manner (48 Hours for internet-reachable applications). Do not use versions of an Operating System which are old and/or not receiving security fixes	Unpatched Operating Systems can be exploited by attackers and in the worst case enable an attacker to completely takeover an application, access all information contained within, and use this access to access connected systems.
Multi-factor Authentication	A method of validating the user logging-in by using additional checks, separate to a password, such as a code from an SMS/Mobile application or fingerprint scan.	Makes it significantly more difficult for adversaries to use stolen user credentials to facilitate further malicious activities.
Restrict Administrative Privileges	Limit how accounts with the ability to administer and alter key system and security settings can be accessed and used.	Administrator accounts are 'the keys to the kingdom'. Controlling their use will make it more difficult for an attacker to identify and successfully gain access to one of these accounts, which would give them significant control over systems.
Application Control	Checking programs against a pre-defined approved list and blocking all programs not on this list.	Unapproved programs, including malware, are unable to start. This prevents attackers from running programs that enable them to gain access to your environment or steal an organisation's data.
Restrict MS Office Macro Settings	Only allow Microsoft Office macros (automated commands) where there is a business requirement and restrict the type of commands a macro can execute. Also monitor usage of Macros.	Macros can be used to run automated malicious commands that could let an attacker download and install malware.
User Application Hardening	Configure key programs (web browsers, Microsoft Office, PDF software, etc) to apply settings that will make it more difficult for an attacker to successfully run commands to install malware.	Default settings on key programs, like web browsers, may not be the most secure configuration. Making changes will help reduce the ability of a compromised/malicious website from successfully downloading and installing malware.
Regular Backups	Regular backups of important new or changed data, software and configuration settings, stored disconnected and retained for at least three months. Test the restoration process when the backup to ensure information can be accessed following a cyber-security incident e.g. a ransomware incident.	To ensure information can be accessed following a cyber-security incident e.g. a ransomware incident