Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Essential Eight Assessment Process Guide

First published: November 2022
Last updated: August 2023

Introduction

The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies, in the form of the *Strategies to Mitigate Cyber Security Incidents*, to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight.

This publication details a process for undertaking assessments of the Essential Eight. In doing so, it includes guidance on assessment methods that can be used for assessing both the implementation and effectiveness of controls that underpin the Essential Eight – as articulated within the *Essential Eight Maturity Model* (November 2022 release).

This publication should be read and used in conjunction with other ASD guidance and tools. This includes the:

- *Essential Eight Maturity Model*
- *Essential Eight Maturity Model FAQ*
- *Essential Eight Assessment Report Template*
- Essential Eight assessment toolkit.

Note, all vendor products mentioned within this publication are for illustrative purposes only and should not be interpreted as an explicit endorsement by ASD.

Overview

Assessments against the Essential Eight are conducted using the *Essential Eight Maturity Model*. This maturity model describes three target maturity levels (Maturity Level One through to Maturity Level Three) which are based on mitigating increasing levels of targeting and tradecraft. The maturity model also includes Maturity Level Zero which exists for capturing instances in which the requirements of Maturity Level One are not met.

Although the approach to conducting an assessment depends on the size and complexity of a system, there are foundational principles that are common to each assessment. As such, the guidance in this publication should be incorporated by assessors, noting that assessors should still use their own judgement and expertise.

While the Essential Eight may be applied to a non-Microsoft Windows system, specific mitigation strategies, or parts thereof, may not be applicable or even the most effective mitigation strategies available. In these instances, such as for Linux workstations and servers, cloud computing or enterprise mobility, organisations should consider alternative guidance provided by ASD.

Finally, in determining compensating control effectiveness, assessors should ensure that any compensating controls that have been implemented provide an equivalent level of protection to those recommended under the Essential

Eight. This will assist in ensuring that an equivalent level of overall protection against a specific level of targeting and tradecraft can be achieved and maintained.

Evidence quality

In conducting an assessment, assessors need to gather and review credible evidence to support conclusions they draw on the effectiveness of controls. In general terms, the evidence used to determine the effectiveness of controls will vary in quality depending on the approach taken. As such, when conducting an assessment, assessors should seek to gather and use the highest quality evidence where reasonably practicable. This guide defines four levels of evidence quality:

- **Excellent evidence:** Testing a control with a simulated activity designed to confirm it is in place and effective (e.g. attempting to run an application to check application control rulesets).
- **Good evidence:** Reviewing the configuration of a system through the system's interface to determine whether it should enforce an expected policy.
- **Fair evidence:** Reviewing a copy of a system's configuration (e.g. using reports or screenshots) to determine whether it should enforce an expected policy.
- **Poor evidence:** A policy or verbal statement of intent (e.g. sighting mention of controls within documentation).

Determining effective implementation of mitigation strategies

Upon concluding assessment activities, assessors will need to determine whether mitigation strategies were implemented effectively or not. This determination requires a combination of judgement and consideration of the following factors:

- adoption of a risk-based approach to the implementation of mitigation strategies
- ability to test the mitigation strategies across an accurate representative sample of workstations (including laptops), servers and network devices
- level of assurance gained from assessment activities and any evidence provided (noting the quality of evidence)
- any exceptions, including associated compensating controls, and whether they have been accepted by an appropriate authority as part of a formal exception process.

Assessors should use ASD's standardised assessment outcomes which are:

- **Effective:** The organisation is effectively meeting the control's objective.
- **Ineffective:** The organisation is not adequately meeting the control's objective.
- **Alternate control:** The organisation is effectively meeting the control's objective through an alternate control.
- **Not assessed:** The control has not yet been assessed.
- **Not applicable:** The control does not apply to the system or environment.
- **No visibility:** The assessor was unable to obtain adequate visibility of a control's implementation.

It is important that assessors do not allow organisational risk acceptance without sufficient compensating controls as a justification for not implementing a mitigation strategy (e.g. a system owner has risk accepted not implementing application control or multi-factor authentication). In these scenarios, without adequate compensating controls, the mitigation strategy is considered to be not implemented.

For a system owner to claim they have implemented a mitigation strategy, all controls specified within the mitigation strategy must be assessed as 'effective' or 'alternate control'. If one of the controls specified for a mitigation strategy is assessed as 'ineffective', the system owner cannot claim to have met the requirements for that maturity level. In turn, this applies to the determination of whether a system owner has met the target maturity level for their system (i.e. if one or more mitigation strategies are deemed to be not implemented then the target maturity level for the system cannot be claimed to have been met).

Where exceptions to a mitigation strategy's controls have been identified, the assessor should review and evaluate any compensating controls that are in place to determine whether they address the intent of the original controls and are implemented effectively. Two examples have been provided below.

Example: During an internal review, an organisation identified a low-risk Windows server that could not be patched. As a result, the organisation implemented a plan to decommission the server within two months.

In this situation, it was still important for the organisation to apply compensating controls that reduced the risk to an acceptable level, and to align with the requirements of the Essential Eight's exception process. As a result, a risk owner was assigned, and strong compensating controls were put in place.

In this instance, as the exception was being effectively managed and strong compensating controls were in place, an assessor determined that the exception should not preclude the organisation from reaching their target maturity level. Conversely, if the organisation had not applied strong compensating controls, it would not have aligned with the requirements of the Essential Eight's exception process and should have precluded the organisation from reaching their target maturity level.

Example: During an internal review, an organisation identified cloud services that did not have available multi-factor authentication functionality enabled. In assessing the situation, the organisation decided it was not worth the time and effort to enable such functionality, not to mention the complaints they expected they would receive from users.

In this situation, the organisation had chosen to simply accept the risk of not implementing a control rather than implementing strong compensating controls.

In this instance, as the exception was not being effectively managed nor were strong compensating controls in place, an assessor determined that the organisation should be precluded from reaching their target maturity level.

It is important that the use of exceptions for a system are documented and approved by an appropriate authority through a formal process. Documentation for exceptions should include the following:

- detail, scope and justification for exceptions
- detail of compensating controls associated with exceptions, including:
  - detail, scope and justification for compensating controls
  - expected implementation lifetime of compensating controls
  - when compensating controls will next be reviewed
- system risk rating before and after the implementation of compensating controls
- any caveats placed on the use of the system as a result of exceptions
- acceptance by an appropriate authority of the residual risk for the system
- when the necessity of exceptions will next be considered by an appropriate authority (noting exceptions should not be approved beyond one year).

The appropriate use of a formal exception process, along with compensating controls, should not preclude an organisation from being assessed as meeting the requirements for their target maturity level.

Stages of an assessment

At a high-level, assessments are comprised of four stages:

- **Stage 1:** The assessor plans and prepares for the assessment.
- **Stage 2:** The assessor determines the scope and approach for the assessment.
- **Stage 3:** The assessor assesses the controls associated with each of the mitigation strategies.
- **Stage 4:** The assessor develops the security assessment report.

The activities and considerations for each stage of an assessment are discussed in further detail below.

Stage 1: Assessment planning and preparation

Assessment planning

Prior to commencing an assessment, the assessor should conduct assessment planning activities. These activities require the assessor to discuss with the system owner:

- system classification and assessment scope (see further detail below)
- access to low and high-privileged user accounts, devices, documentation, personnel, and facilities
- intended assessment approach and any approvals required to run scripts and tools (see further detail below)
- evidence collection and protection, including any requirements following the conclusion of the assessment
- where the security assessment report will be developed (e.g. on an assessor's device or on an alternative device)
- approach to stakeholder engagement and consultation (including key points of contact)
- whether any managed service providers or other outsourced providers manage any aspects of the system (including appropriate points of contact)
- access to any relevant prior security assessment reports for the system
- appropriate use, retention and marketing of the security assessment report by both parties.

Assessors may also develop an assessment test plan and share it with the system owner. Example assessment test plans are included as Annex A through Annex C.

Note, test cases listed within the example assessment test plans included as Annex A through Annex C should not be treated as mandatory assessment requirements. Rather, assessors should apply their own judgement and experience in the development of their own assessment test plans.

Stage 2: Determination of assessment scope and approach

Determine assessment scope

In determining the assessment scope, assessors should first clarify the target maturity level with the system owner, noting that the Essential Eight is required to be implemented and assessed as a package. For example, if a system owner has not previously had an assessment demonstrating that they have implemented Maturity Level One, they should not begin an assessment against Maturity Level Two until they have done so, and likewise for Maturity Level Two before being assessed against Maturity Level Three.

Having identified a suitable target maturity level, the assessor should familiarise themselves with the requirements for that maturity level as it will impact the components or aspects of the system within scope of the assessment. At this time it may also be useful to request an approximate percentage breakdown of the operating systems used on workstations and servers for the system.

Once the scope of the assessment has been identified, and agreed upon with the system owner, a more accurate determination of the assessment's duration and any milestones will likely be possible.

The scope of the assessment should be documented within the security assessment report. Any components or aspects of a system deemed out-of-scope should also be documented and accompanied by a justification for their exclusion.

Determine assessment approach

In determining a suitable assessment approach, both qualitative and quantitative testing techniques should be considered. For example, qualitative testing techniques include documentation reviews and interviews with personnel administering or managing system security, while quantitative testing techniques include system configuration reviews and the use of scripts and tools. Sample sizes for testing should also be determined in consultation with the system owner, with the aim to assess an accurate representative sample population of workstations (including laptops), servers and network devices.

Conducting assessments using interviews, reports and screenshots will always be inferior to conducting assessments using scripts and tools. Particularly as scripts and tools often assess many workstations and servers on a network, rather than a single sample workstation or server, and often identify issues that may be missed in interviews or overlooked by human analysis of reports and configuration settings. If adequate assessment scripts and tools are not already present on a system, assessors may wish to use their own scripts and tools following approval by the system owner.

Any assessment limitations including sample sizes and constraints on technical testing should be documented within the security assessment report.

Stage 3: Assessment of controls

The assessment of each mitigation strategy is performed by reviewing and testing the effectiveness of controls. This section provides guidance on the approach to assessing each mitigation strategy at a given target maturity level, along with relevant assessment considerations. Guidance on determining the effectiveness of the controls within each mitigation strategy is also provided within this section.

Assessment guidance for maturity levels in this section is cumulative. For example, the guidance provided in the Maturity Level Two section is focused on unique requirements above those of Maturity Level One. Likewise, the

guidance provided in the Maturity Level Three section is focused on unique requirements above those of Maturity Level Two. This aligns with the manner in which assessments should be conducted against target maturity levels.

Maturity Level One

The focus of this maturity level is malicious actors who are content to simply leverage commodity tradecraft that is widely available to gain access to, and control of, a system. For example, malicious actors opportunistically using a publicly-available exploit for a vulnerability in an unpatched internet-facing service, or authenticating to an internet-facing service using credentials that were stolen, reused, brute forced or guessed.

Generally, malicious actors are looking for any victim rather than a specific victim and will opportunistically seek common weaknesses in many targets rather than investing heavily in gaining access to a specific target. Malicious actors will employ common social engineering techniques to trick users into weakening the security of a system and executing malicious code, for example, via a Microsoft Office macro.

Malicious actors will also often seek to compromise user accounts. If successful, they may seek to exploit privileges associated with these accounts or escalate privileges to higher levels. Depending on their intent, malicious actors may also seek to steal or destroy data (including backups) or make data otherwise unavailable through various denial-of-service techniques.

Application control

Context

Application control assessments can be done without tools but efforts will be severely limited in their effectiveness and are likely to miss edge cases that malicious actors would look to exploit. For example, malicious actors may use custom tools to scan for weak or vulnerable paths on a system. This could be achieved with a Microsoft Office macro.

It is important to note that the last major update to the maturity model introduced compiled Hypertext Markup Language (HTML) (.chm files), HTML applications (.hta files) and control panel applets (.cpl files) to the list of file types that need to be controlled. Depending on the application control solution selected, it may not support these file types.

When conducting assessments, paths for standard user profiles and temporary folders used by operating systems, web browsers, and email clients can include those from the list below. Note, depending on the system configuration, there may be overlap (e.g. %temp% and %tmp% generally reside within %userprofile%*).

- %userprofile%*
- %temp%*
- %tmp%*
- %windir%\Temp*.

To check if application control is implemented within the user profile directory, attempt to run a benign executable file inside the directory. The executables tested should cover .exe, .com, .dll, .ocx, .ps1, .bat, .vbs, .js, .msi, .mst, .msp, .chm, .hta, and .cpl. If any of the executables run within the user profile directory or operating system temporary folders, application control is ineffective.

Note, while a dedicated application control solution is not required at Maturity Level One (i.e. file system permissions can be used instead), organisations may still choose to implement a dedicated application control solution if they intend to eventually implement requirements for Maturity Level Two.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
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.	Due to the complexity of advanced file system permissions, and various user groups that a user account may belong to, the only truly effective way to check application control implementations is to attempt to write to and execute from all locations accessible to a user on the file system. There are several free tools available to support the assessment of this control, including ASD's Essential Eight Maturity Verification Tool (E8MVT) and Application Control Verification Tool (ACVT), AirLock Digital's Application Whitelist Auditor, and CyberArk's Evasor. There are also several paid tools available. In choosing a tool to use, make sure that it has been thoroughly tested beforehand to ensure it is fit-for-purpose. If the system owner is willing to allow the use of trusted Microsoft tools, but not other third-party tools, the SysInternals AccessChk application can be used to generate the output of folder permissions, noting this is only relevant to a path-based approach. For example, by running 'accesschk -dsuvw [path] > report.txt', it is possible to generate a list of all writable paths and their access permissions for all users. Note, the 'whoami /groups' command would also need to be run to determine which user groups a typical standard user belonged to in order to determine the effective permissions for each path. Alternatively, PowerShell cmdlets can be used to test and review AppLocker policy where applicable. For a system on which tools cannot be run, assuming a path-based approach is used, screenshots of the 'effective access' permissions for specified folders can be requested. This, however, has limitations, because unless screenshots of access permissions are requested for every folder and sub-folder (for which there may be many), it will not be possible to comprehensively assess whether read, write and execute permissions exist for a given user. At a minimum, screenshots for key paths (such as temporary folders used by the operating system, web browsers and email clients) should be requested and examined to determine whether inheritance is set, noting that at any point in a path, application control inheritance previously set by an operating system may be disabled by an application installer.

Patch applications

Context

Most vendors of internet-facing services regularly release updated versions of their applications to fix vulnerabilities. Applications that exist on a system can be compared to the latest versions available from the vendor to determine whether existing versions are the latest, and if not, how long-ago updates were made available by the vendor, based on release dates and patch notes. Services such as the SANS Internet Storm Centre, Microsoft Security Response Centre or the Cybersecurity and Infrastructure Security Agency's *Known Exploited Vulnerabilities Catalog* can be used to determine whether public exploits exist for a given internet-facing service.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	Ask for a demonstration of a method of asset discovery being used in an automated manner to identify assets associated with the system, such as workstations, servers and network devices. This may be a dedicated asset discovery tool or it may be equivalent functionality built into a vulnerability scanner. In addition, request evidence of previous automated asset discovery scans and pay attention to the date/time stamp and their scope. Note, while an automated method of asset discovery should be used at least fortnightly, system owners may elect to align the frequency of asset discovery scans to more frequent timeframes used for vulnerability scans (such as daily or weekly) in order to perform both activities at the same time for optimal effect. Finally, in addition to identifying assets for follow-on vulnerability scanning activities, automated asset discovery can also be used to identify any unauthorised assets that may have been connected to a system between scheduled scans. If unknown assets are identified as part of asset discovery scans, they should be immediately investigated and treated as suspicious until confirmed otherwise.
A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	Ask for a demonstration of a vulnerability scan. In addition, request evidence of the date/time stamp of when the vulnerability database used for the scan was last updated. Ideally, this should be within 24 hours of the vulnerability scan taking place.
A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in internet-facing services.	Ask for a demonstration of a vulnerability scan. In addition, request evidence of previous vulnerability scans and pay attention to the date/time stamp and scope of event logs. Check whether the list of scanned internet-facing services matches the internet-facing services. Request evidence of previous vulnerability scans and pay attention to the date/time stamp and scope of event logs.
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	Ask for a demonstration of a vulnerability scan. In addition, request evidence of previous vulnerability scans and pay attention to the date/time stamp and scope of event logs. Request evidence of previous vulnerability scans and pay attention to the date/time stamp and scope of event logs.

Patches, updates or other vendor mitigations for vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.	A network-based vulnerability scanner can be used to identify internet-facing services, their versions and install dates. This can then be reviewed alongside the date of release for each to determine whether patch timeframes have been met. The use of these tools can quickly determine service versions and whether they are the latest versions available from vendors. There are several free tools available to support the assessment of this control, including ASD's E8MVT, Nessus Essentials, Nexpose Community Edition, OpenVAS and Qualys Community Edition. There are also several paid tools available. In choosing a tool to use, make sure that it has been thoroughly tested beforehand to ensure it is fit-for-purpose. Note, a scanner may not identify missing vendor mitigations such as specific configuration changes. If a network-based vulnerability scanner cannot be used, screenshots of versions of internet-facing services can be requested. This allows for manual checking against the latest versions available from vendors. Alternatively, a list of services may be requested (noting that malicious actors often exploit vulnerabilities in internet-facing services that the system owner may have forgotten about or that have been installed by users without the system owner's knowledge).
Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.	A vulnerability scanner can be used to assess applications, their versions and install dates. The above output must be reviewed alongside the date of release for each application to determine whether the timeframe has been met.

Alternatively, PowerShell can be used to identify applications with registered uninstall functionality. However, this method alone will not always cover all applications that are installed on a system. As a result, it should be combined with the list of installed applications within 'Programs and Features'.

While this approach can be used for assessments, the limitations in coverage should be noted. For key applications though, it will likely be sufficient. If any key applications appear to be missing in reports provided, this should be raised for clarification.

Below is a PowerShell script to output a list of installed applications with registered uninstall functionality. This list should be reviewed in conjunction with the list of installed applications within 'Control Panel – Programs – Programs and Features' to ensure no applications are missed.

```
function Analyze( $p, $f) {
   Get-ItemProperty $p |foreach {
      if (($_.DisplayName) -or ($_.version)) {
         [PSCustomObject]@{
            From = $f;
            Name = $_.DisplayName;
            Version = $_.DisplayVersion;
            Install = $_.InstallDate
         }
      }
   }
}
$s = @()
$s += Analyze 'HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\*' 64
$s += Analyze 'HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\*' 32
$s | Sort-Object -Property Name
```

The combined list of installed applications must be reviewed alongside the date of release for each application patch to determine whether the timeframe has been met.

If tools cannot be used, request a demonstration that shows the versions of installed applications and their install date. This allows for manual checking against the latest versions available from vendors.

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.	A vulnerability scanner can be used to assess applications and whether they are end of life. Request a demonstration that shows the versions of the referenced applications and services. This allows for manual checking against the list of supported versions. In addition, check if hotfix KB4577586 has been applied to demonstrate that Adobe Flash Player is no longer supported. Note, this hotfix will only remove Adobe Flash Player if it was installed by Windows. If Adobe Flash Player was installed manually from another source, it will not be removed by this hotfix.

Configure Microsoft Office macro settings

Context

All users should be denied the ability to execute Microsoft Office macros by default unless they have a specific business requirement. If certain users are required to run Microsoft Office macros, they should be restricted to only the specific applications required (rather than all Microsoft Office applications). In addition, a record of their business requirement and associated approvals should be kept. This record should align with the list of users within the Active Directory group that have permission to run Microsoft Office macros. Note, once a business requirement can no longer be demonstrated by a user, permission to run Microsoft Office macros should be revoked.

Microsoft Defender is commonly used to perform Microsoft Office macro antivirus scanning. This product uses the Antimalware Scan Interface to integrate applications and services with any antimalware installed on a machine. Other antivirus solutions may use this interface or other processes to scan Microsoft Office macros.

Microsoft Office applications that can execute Microsoft Office macros include Microsoft Access, Microsoft Excel, Microsoft Outlook, Microsoft PowerPoint, Microsoft Project, Microsoft Publisher, Microsoft Visio and Microsoft Word.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	ASD's E8MVT can be used to assist with assessing this control. Refer to supporting E8MVT documentation.
	The 'gpresult' command can be run on workstations to generate an RSoP report to identify Microsoft Office macro settings applied via group policy settings. Within the report, look for the 'VBA Macro Notification Settings' setting at 'User Configuration\Policies\Administration Templates\<Microsoft Office Application>\Application Settings\Security\Trust Center\'. The 'VBA Macro Notification Settings' setting should be enabled and configured to 'Disable all macros without notification' for most users. If this setting is not configured, all Microsoft Office macros will be disabled but users will receive a prompt via the Trust Bar asking whether they would like to enable them. For users with a demonstrated business requirement for Microsoft Office macro use, this group policy setting may either not be configured, disabled or enabled and set to any other setting – as long as antivirus scanning is enabled and Microsoft Office macros in files originating from the internet are being blocked.

	Within each Microsoft Office application, check or request demonstration showing Trust Center macro settings (File – Options – Trust Center – Trust Center Settings – Macro Settings) for users that are not allowed to run Microsoft Office macros and for users with a business requirement to do so. For users that are allowed to run Microsoft Office macros, request documentation that outlines the business need. Consider requesting the percentage of the organisation's userbase that have been granted approval to run Microsoft Office macros. For the assessment of Microsoft Office macro security, identify what setting is selected for 'macro settings'. For most users, the desired setting should be 'Disable all macros without notification'. However, for users with a demonstrated business requirement for Microsoft Office macro use, any other setting is acceptable at this maturity level. In these instances, identify any compensating controls such as antivirus scanning and if Microsoft Office macros in files originating from the internet are being blocked.
Microsoft Office macros in files originating from the internet are blocked.	ASD's E8MVT can be used to assist with assessing this control. Refer to supporting E8MVT documentation. Within the RSoP report, look for the 'Block macros from running in Office files from the Internet' setting at 'User Configuration\Policies\Administration Templates\<Microsoft Office Application>\Application Settings\Security\Trust Center\'. It should be enabled. If this setting is not configured, all Microsoft Office macros from the internet will be able to run. In addition, if users have the ability to access a file's properties, they can remove the Mark of the Web. To prevent this, the 'Hide mechanisms to remove zone information' setting at 'User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager\' should also be enabled. Users can also remove the Mark of the Web by copying files from NTFS formatted storage media to external FAT/FAT32/exFAT formatted storage media and back. Unless external storage media (which is typically FAT32/exFAT formatted) is disabled for a system, it will be difficult to prevent users bypassing this control if they know how to – or malicious actors tell them how to (which is more likely at higher maturity levels).
Microsoft Office macro antivirus scanning is enabled.	ASD's E8MVT can be used to assist with assessing this control. Refer to supporting E8MVT documentation. Check if the following group policy setting is enabled for each Microsoft Office application. Within the RSoP report, look for the 'Macro Runtime Scan Scope' setting at 'User Configuration/Policies/Administrative Templates/Microsoft Office <Version>/ Security Settings/Macro Runtime Scan Scope'. It should be enabled with a value of either: 0 - No macro scanning 1 - Macros in files with the MoTW (Default) 2 - Macros in all files (Ideal). Alternatively, a pseudo-malicious Microsoft Office macro that contains an EICAR antivirus test string can be used for testing purposes. ASD's E8MVT has a benign sample file that can be used for testing without running the tool.

	If an Antimalware Scan Interface compatible antivirus product is not being used, ask for a screenshot of any Microsoft Office macro scanning configuration settings that might be present.
Microsoft Office macro security settings cannot be changed by users.	ASD's E8MVT can be used to assist with assessing this control. Refer to supporting E8MVT documentation.
	Within the RSoP report, look for the 'VBA Macro Notification Settings' setting at 'User Configuration\Policies\Administration Templates\<Microsoft Office Application>\ Application Settings\Security\Trust Center\'. If it is either enabled or disabled, then users will not be able to change their Microsoft Office macro security settings.
	Using a user account, open each Microsoft Office application and attempt to change Microsoft Office macro security settings in the Trust Centre. If Microsoft Office macro security settings have been configured via group policy settings, they should appear greyed out.

User application hardening

Context

Malicious actors are known to indiscriminately use 'malvertising' in their attempts to compromise systems. Blocking web advertisements using web browser add-ins or extensions, or via web content filtering, can prevent the compromise of a system.

Internet Explorer 11 lacks many of the security features of modern web browsers and ceased to be supported by Microsoft on 15 June 2022. As such, it is more regularly targeted by malicious actors. Ideally, Internet Explorer 11 should be removed from systems and Microsoft Edge (running in 'IE mode' for legacy sites), or other modern web browsers, should be used instead.

Web browser security settings should be configured via group policy settings. In addition, default web browser security settings should not be relied upon as users may tinker with these settings to enable content or change settings when guided to do so by malicious actors. Web browser security settings that are configured via group policy settings typically appear greyed out to users, have a hover over message explaining the setting is configured by their organisation or have an icon such as a padlock.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Web browsers do not process Java from the internet.	A list of the web browsers installed on a system can be derived from the list of all installed applications. For each web browser installed on the system, visit a specific web page that contains Java, such as the Is Java installed? website. Additionally, review any plug-ins or extensions that are installed for each web browser present on the system. This can be used to check whether any web browsers have Java plug-ins or extensions installed, and if so, whether they are disabled. If the system owner requires Java content to be accessed on their intranet, other controls should be assessed to determine whether internet-based Java content is blocked via a web content filter.
Web browsers do not process web advertisements from the internet.	Check whether web browsers have either an ad blocker add-in or extension installed. Alternatively, check whether a web content filter or proxy is blocking web advertisements. A simple check is to request a user to browse to a website that is known to display ads (to observe if any ads are displayed) or to browse to AdBlock Tester website (for comprehensive testing) and provide a screenshot of the results. Note, built-in settings within web browsers to block pop-ups do not meet the intent of this control.
Internet Explorer 11 does not process content from the internet.	Determine whether Internet Explorer 11 is installed on the system. If it is, attempt to access any website on the internet, such as https://www.google.com.au. Check that Internet Explorer 11 is not the default web browser (Settings – Apps – Default apps – Web browser) and check for any file associations (Settings – Apps – Default apps – Choose default applications by file type) tied to Internet Explorer 11.
Web browser security settings cannot be changed by users.	Check the security settings of each web browser present on the system. Identify if settings are greyed out (Internet Explorer 11 and Mozilla Firefox), have an icon with a hover over message that says 'This setting is managed by your organisation' (Microsoft Edge) or 'This setting is managed by your administrator' (Google Chrome). This indicates that settings have been configured via group policy settings and cannot be changed by users. In addition, identify whether Java Control Panel settings can be changed by the user.

Restrict administrative privileges

Context

Policies, processes and procedures for managing privileged access to systems should be documented and enforced within organisational workflows. In doing so, privileged access to systems and applications should be requested via a form, service desk ticket or email from users, and require approval from a supervisor or application owner, to maintain

a record of all such requests. System owners should also maintain a list of all applications on their system that require privileged access.

Privileged accounts are often targeted by malicious actors for their greater control and access to organisational resources. For this reason, privileged accounts should not have access to the internet, email and web services.

Note, while no constraints are placed on how privileged and unprivileged operating environments are separated for privileged users at Maturity Level One, organisations may choose to implement an approach that avoids virtualising a privileged operating environment within an unprivileged operating environment if they intend to eventually implement requirements for Maturity Level Two.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Requests for privileged access to systems and applications are validated when first requested.	Request copies of forms, support tickets or emails provided by users requesting access – along with the support of their supervisor or applicable application owner. This can then be compared to screenshots of accounts with privileged access to determine if there are any discrepancies.
Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services.	Attempt to browse the internet as a privileged user, review the internet proxy on the network to determine whether it is configured to block traffic from privileged accounts and run the below PowerShell command to check if privileged accounts have access to mailboxes and email addresses: *Get-ADUser -Filter {(admincount -eq 1) -and (emailaddress -like "*") -and (enabled -eq $true)} -Properties EmailAddress | Select samaccountname, emailaddress* Tools such as BloodHound can assist in identifying privileged users that may be missed when utilising PowerShell alone.
Privileged users use separate privileged and unprivileged operating environments.	Discuss how privileged operating environments have been implemented for the management of the system. Note, at this maturity level there are no constraints on how this can be implemented beyond that separate privileged and unprivileged operating environments have been implemented.
Unprivileged accounts cannot logon to privileged operating environments.	Attempt to logon to a privileged workstation using a standard user account. Bloodhound can be used to assess whether any unprivileged accounts have connected to privileged environments by looking for cached credentials.

Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Request a demonstration of a privileged account attempting to logon to a standard user workstation. Note, the moment a privileged account's username and password are entered into a standard user workstation, the account should be considered compromised (noting this is the reason behind having separate operating environments). This test should be done using a privileged account set up specifically for this purpose. The privileged account should then be removed immediately after testing is complete. Bloodhound can be used to assess whether any privileged accounts have connected to unprivileged environments by looking for cached credentials.

Patch operating systems

Context

Operating system vendors regularly publish updates to address vulnerabilities. In addition, unsupported and out-of-date operating systems of internet-facing workstations and servers are a common target for malicious actors.

While operating systems of workstations, servers and network devices that are not internet-facing are at a lower risk of exploitation, as malicious actors need to compromise another system to then obtain network-based access to the unpatched operating system, it is still important that such operating systems are patched in a reasonable timeframe given the level of targeting and tradecraft the system owner is attempting to protect their system against.

Services such as the SANS Internet Storm Centre, Microsoft Security Response Centre or the Cybersecurity and Infrastructure Security Agency's *Known Exploited Vulnerabilities Catalog* can be used to determine whether public exploits exist for operating systems of workstations, servers and network devices.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	Ask for a demonstration of a method of asset discovery being used in an automated manner to identify assets associated with the system, such as workstations, servers and network devices. This may be a dedicated asset discovery tool or it may be equivalent functionality built into a vulnerability scanner. In addition, request evidence of previous automated asset discovery scans and pay attention to the date/time stamp and their scope. Note, while an automated method of asset discovery should be used at least fortnightly, system owners may elect to align the frequency of asset discovery scans to more frequent timeframes used for vulnerability scans (such as daily or weekly) in order to perform both activities at the same time for optimal effect. Finally, in addition to identifying assets for follow-on vulnerability scanning activities, automated asset discovery can also be used to identify any unauthorised assets that may have been connected to a system between scheduled scans. If unknown assets are identified as part of asset discovery scans, they should be immediately investigated and treated as suspicious until confirmed otherwise.

A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	Ask for a demonstration of a vulnerability scan. In addition, request evidence of the date/time stamp of when the vulnerability database used for the scan was last updated. Ideally, this should be within 24 hours of the vulnerability scan taking place.
A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing services.	Ask for a demonstration of a vulnerability scan. In addition, request evidence of previous vulnerability scans and pay attention to the date/time stamp and scope of event logs. Request evidence of previous vulnerability scans and pay attention to the date/time stamp and scope of event logs.
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, servers and network devices.	Ask for a demonstration of a vulnerability scan. In addition, request evidence of previous vulnerability scans and pay attention to the date/time stamp and scope of event logs. Request evidence of previous vulnerability scans and pay attention to the date/time stamp and scope of event logs.
Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.	Network-based vulnerability scanners can be used to identify operating systems, their versions and install dates. This can then be reviewed alongside the release date of patches to determine whether the timeframe has been met. The use of these tools can quickly determine patches that have been applied, which can then be compared to patch release dates. There are several free tools available to support the assessment of this control, including ASD's E8MVT, Nessus Essentials, Nexpose Community Edition, OpenVAS and Qualys Community Edition. There are also several paid tools available. In choosing a tool to use, make sure that it has been thoroughly tested beforehand to ensure it is fit-for-purpose. If using Windows Server Update Services (WSUS) for the assessment of this control, it is important to consider that WSUS does not necessarily report accurate patch levels. Specifically, WSUS has been known to report patches or updates that have been deployed but not whether they were successfully applied, stuck and if the machine was rebooted (if required). Request WMIC or PowerShell be used to generate a list of hotfixes and the date that they were applied to an operating system. This can then be compared to available patches, especially those that are currently being exploited, to determine whether they have been applied or not.

Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release.	Network-based vulnerability scanners can be used to identify operating systems, their versions and install date. This can then be reviewed alongside the release date of the patches to determine whether the timeframe has been met. The use of these tools can quickly determine patches that have been applied, which can then be compared to the patch release date. There are several free tools available to support the assessment of this control, including ASD's E8MVT, Nessus Essentials, Nexpose Community Edition, OpenVAS and Qualys Community Edition. There are also several paid tools available. In choosing a tool to use, make sure that it has been thoroughly tested beforehand to ensure it is fit-for-purpose. If using WSUS for the assessment of this control, it is important to consider that WSUS does not necessarily report accurate patch levels. Specifically, WSUS has been known to report patches or updates that have been deployed but not whether they were successfully applied, stuck and if the machine was rebooted (if required). Request WMIC or PowerShell be used to generate a list of hotfixes and the date that they were applied to an operating system. This can then be compared to available patches, especially those that are currently being exploited, to determine whether they have been applied or not.
Operating systems that are no longer supported by vendors are replaced.	Network-based vulnerability scanners can be used to identify operating systems and their versions. The use of these tools can quickly determine operating system versions which can then be checked against the list of supported operating systems from vendors. For Microsoft Windows workstations and servers, the 'winver' command can be run to determine the version of the operating system. Request a screenshot of the output of running the 'winver' command for servers and workstations (assuming a Standard Operating Environment is used for workstations). This version can then be checked against Microsoft release information to determine whether it is a supported version or not.

Multi-factor authentication

Context

Multi-factor authentication is one of the most effective controls an organisation can implement to prevent malicious actors from gaining access to a system, service or application. When implemented correctly, multi-factor authentication can also make it significantly more difficult for malicious actors to steal legitimate credentials to facilitate further malicious activities.

Multi-factor authentication should be implemented for remote access solutions, users performing privileged actions and users of important data repositories. Using multi-factor authentication provides a secure authentication mechanism that is not as susceptible to brute force attacks, such as traditional single-factor authentication methods based on memorised secrets (e.g. personal identification numbers (PINs), passwords and passphrases).

At this maturity level, any two or more authentication methods can be used as long as they are not of the same class (e.g. something users know, something users have or something users are). There is no requirement that one factor must be a memorised secret. Biometrics and Trusted Signals are also acceptable as an authentication method at this maturity level.

Note, while any two or more authentication methods can be used at Maturity Level One, organisations may still choose to implement multi-factor authentication solutions, such as those that include something the user has or are phishing-resistant, if they intend to eventually implement requirements for Maturity Level Two or Maturity Level Three.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Multi-factor authentication is used by an organisation's users when they authenticate to their organisation's internet-facing services.	Attempt to logon to internet-facing services that staff access. Typically, the logon screen will show a request for two or more authentication factors, such as a password and a one-time PIN. Note, in some cases a service may request the second authentication factor after the first authentication factor has been validated. Organisations might only share their primary login portal and may not disclose any other portals that may not have MFA in place. Assessors should undertake activities to determine if any additional authentication portals are exposed to the internet.
Multi-factor authentication is used by an organisation's users when they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.	Attempt to logon to third-party internet-facing services that staff access. In cases where multi-factor authentication is not used, confirm that the vendor or service provider does not offer that functionality.
Multi-factor authentication (where available) is used by an organisation's users when they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.	Attempt to logon to third-party internet-facing services that staff access. In cases where multi-factor authentication is not used, confirm that the vendor or service provider does not offer that functionality.
Multi-factor authentication is enabled by default for an organisation's non-organisational users (but they can choose to opt out) when they authenticate to the organisation's internet-facing services.	Attempt to logon to internet-facing services that customers/citizens access. Discuss whether multi-factor authentication is setup as part of account creation (opt-out) or whether customers/citizens need to set it up themselves after initial account creation (opt-in).

Regular backups

Context

Backup and retention frequencies should be defined by the system owner in accordance with their organisation's business continuity and disaster recovery requirements. In doing so, it is important that restoration of systems and data from backups be tested as part of regular (at least annual) disaster recovery exercises and not left to after the first major security incident is experienced.

At this maturity level, it is important that unprivileged users cannot access the backups of any other users – although it is not necessarily a problem if they are able to access their own backups. It is worth noting, at this maturity level, that privileged accounts may still be able to access the backups of any user.

While unprivileged accounts can access (i.e. read) their own backups, it is important that they do not have the ability to modify or delete those backups. This requirement exists as any ransomware running with the privileges of an unprivileged user should be blocked from overwriting or deleting backups. Note, malicious actors escalating privileges to privileged accounts, or backup administrator accounts, to overwrite backups are addressed at higher maturity levels.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements.	Discuss backup and retention frequencies specified for the system. Request a copy of the business continuity plan and disaster recovery plan to check that the frequency and retention periods have been documented.
Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time.	It is important that any backup activities are synchronised to enable restoration to a common point in time. For example, if important data stores are being backed up out of sync to software and configuration settings then it will hamper restoration efforts and data will be lost.
Backups of important data, software and configuration settings are retained in a secure and resilient manner.	Check what efforts have been made to ensure that backup processes and procedures are secure and resilient. For example, are backups encrypted and how quickly can they be used to recover from ICT equipment failure?

Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises.	Discuss if any disaster recovery exercises have been conducted for the system, how often these are conducted, when the last exercise was conducted and if partial or full restoration of the system (including important data, software and configuration settings) was exercised. Ideally, some form of after-action review or post-exercise report should be available to demonstrate what disaster recovery processes and procedures where exercised and any lessons that were learnt, such as the coordination of restoration activities across different business areas (if applicable). Note that business-as-usual recovery of user files is not sufficient. The intent of this control is the restoration of a significant component of a system as part of a scheduled exercise.
Unprivileged accounts cannot access backups belonging to other accounts.	Review the backup solution and Active Directory security groups to determine who has access to backups. Check whether unprivileged accounts have the ability to access all backups or just their own backups. If backups are stored on network shares, request a demonstration of effective access permissions to show that an unprivileged user account is incapable of accessing backups beyond their own.
Unprivileged accounts are prevented from modifying and deleting backups.	Check whether unprivileged accounts have the ability to modify or delete their own backups. If backups are stored on network shares, request a demonstration of effective access permissions to show that an unprivileged user account is incapable of modifying or deleting their backups – or taking ownership of content to change permissions.

Maturity Level Two

The focus of this maturity level is malicious actors operating with a modest step-up in capability from the previous maturity level. These malicious actors are willing to invest more time in a target and, perhaps more importantly, in the effectiveness of their tools. For example, these malicious actors will likely employ well-known tradecraft to better attempt to bypass controls implemented by a target and evade detection. This includes actively targeting credentials using phishing and employing technical and social engineering techniques to circumvent weaker methods of multi-factor authentication.

Generally, malicious actors are likely to be more selective in their targeting but still somewhat conservative in the time, money and effort they may invest in a target. Malicious actors will likely invest time to ensure their phishing is effective and employ common social engineering techniques to trick users into weakening the security of a system and executing malicious code, for example, via a Microsoft Office macro.

Malicious actors will also often seek to compromise user accounts. If successful, they may seek to exploit privileges associated with these accounts or escalate privileges to higher levels. Depending on their intent, malicious actors may also seek to steal or destroy data (including backups) or make data otherwise unavailable through various denial-of-service techniques.

The guidance below outlines the requirements to be assessed in addition to the requirements of the previous maturity level. In doing so, assessments against Maturity Level Two should focus on the delta between Maturity Level One and Maturity Level Two.

Application control

Context

For Maturity Level Two, application control requires the use of a dedicated application control solution. This may be one of the in-built solutions from Microsoft (e.g. AppLocker or Windows Defender Application Control) or it may be a third-party solution (e.g. AirLock Digital's AirLock, Ivanti's Device and Application Control, Trend Micro Endpoint Application Control or VMWare Carbon Black App Control).

The majority of application control solutions will have a form of logging or auditing mode. As such, event logs for application control solutions should be collected and stored in case there is a cyber incident and they are required for forensic analysis or cyber incident response activities. Often, the lack of sufficient logging can impact the ability to determine the extent of a cyber incident, how it occurred and what vulnerabilities need to be mitigated.

Assessment Guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Application control is implemented on workstations and internet-facing servers.	Check whether a dedicated application control solution has been implemented on all 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 organisation-approved set**.	Due to the complexity of application control rulesets, the best way to assess application control implementations is to attempt to write to and execute from all locations accessible to a user on the file system. There are several free tools available to support the assessment of this control, including ASD's ACVT, AirLock Digital's Application Whitelist Auditor and CyberArk's Evasor. There are also several paid tools available. In choosing a tool to use, make sure that it has been thoroughly tested beforehand to ensure it is fit-for-purpose. If publisher-based rules are used for the system, check that wildcards are not used for publisher or product names. In addition, if path-based rules are used for the system, check that users don't have write access to any paths specified in application control rulesets. Finally, if a version of an application has been trojanised, and would otherwise be allowed to execute due to an existing publisher or hash rule, a hash-based deny rule should be implemented for that version. Tools used for assessments are unlikely to detect this scenario, therefore, it will need to be identified on a case-by-case basis.
Allowed and blocked execution events on workstations and internet-facing servers are logged.	Ask whether logging is available for the application control solution used and request screenshots of any logging output that shows records of executable content that was allowed to execute as well as executable content that was blocked from executing.

Patch applications

Context

At this maturity level, the timeframe for patching vulnerabilities in internet-facing systems is decreased from one month to two weeks. In addition, this maturity level introduces patching timeframes for additional applications, and an increase in associated vulnerability scanning frequencies and scope.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
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.	Use the guidance provided in Maturity Level One of this guide and apply the Maturity Level Two timeframes.
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in other applications.	Use the guidance provided in Maturity Level One of this guide but apply it to other applications using the identified timeframes.
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.	Use the guidance provided in Maturity Level One of this guide and apply the Maturity Level Two timeframes.
Patches, updates or other vendor mitigations for vulnerabilities in other applications are applied within one month of release.	Use the guidance provided in Maturity Level One of this guide but apply it to other applications using the identified timeframes.

Configure Microsoft Office macro settings

Context

At this maturity level, an additional requirement is introduced relating to the use of the attack surface reduction (ASR) rule 'Block Win32 API calls from Office macros'. This ASR rule prevents Microsoft Office macros from calling Win32 APIs, which malicious actors can exploit to run malicious code that is more powerful than the actions they can perform using the Microsoft Office VBA macro language itself.

Event logs for Microsoft Office macro execution events should be collected and stored in case there is a cyber incident and they are required for forensic analysis or cyber incident response activities. Often, the lack of sufficient logging can impact the ability to determine the extent of a cyber incident, how it occurred and what vulnerabilities need to be mitigated.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Microsoft Office macros are blocked from making Win32 API calls.	ASD's E8MVT can assist in determining the implementation of this control as it includes a test file that contains a Microsoft Office macro designed to test this ASR rule. Note, this test will need to be conducted with an account that is allowed to execute Microsoft Office macros.
	Within the RSoP report, look for the 'Configure Attack Surface Reduction rules' setting at 'Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\'. It should be enabled and include an entry of '92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B' with a value of 1 (i.e. enabled).
	If a third-party solution is being used, discuss if the third-party solution has similar functionality to the ASR rule. If so, request evidence as required.
Allowed and blocked Microsoft Office macro execution events are logged.	Within Trust Center, check whether 'Enable Trust Center Logging' has been enabled within the 'Message Bar' section. Request screenshots of any logging output that shows records of Microsoft Office macros that were allowed to execute and Microsoft Office macros that were blocked from executing.

User application hardening

Context

This maturity level requires the implementation of several ASR rules to prevent malicious actors from using Microsoft Office applications to create child processes that can be used to download and run malicious code, write malicious code to disk or inject malicious code into other processes. In addition, the ASR rule 'Block Adobe Reader from creating child

processes' should be implemented to prevent malicious actors from using Adobe Reader to create child processes which can be used to download and run malicious code.

Malicious actors often attempt to exploit vulnerabilities in Microsoft Office through its support for Object Linking and Embedding (OLE) packages. This maturity level requires Microsoft Office to be configured to prevent activation of these OLE packages.

The implementation of ACSC or vendor hardening guidance can assist in reducing the attack surface of applications. This is particularly important for key applications that are commonly targeted by malicious actors such as web browsers, Microsoft Office and Portable Document Format (PDF) software (e.g. Adobe Reader). In cases where ACSC hardening guidance conflicts with vendor hardening guidance, consideration should be given to what the hardening guidance is attempting to achieve.

Event logs for blocked attempts to execute PowerShell scripts should be collected and stored in case there is a cyber incident and they are required for forensic analysis or cyber incident response activities. This should not be confused with 'module logging', 'script block logging' and 'transcription' functionality of PowerShell, which while recommended for good cyber hygiene, are not within scope of Essential Eight assessments. Often, the lack of sufficient logging can impact the ability to determine the extent of a cyber incident, how it occurred and what vulnerabilities need to be mitigated.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
ACSC or vendor hardening guidance for web browsers is implemented.	Generally, hardening guidance can be configured via group policy setting templates that are made available by vendors. This will be included as part of any RSoP reports that are provided. ACSC hardening guidance for Microsoft Edge is available within the *Hardening Microsoft Windows 10 version 21H1 Workstations* publication. Microsoft hardening guidance for Microsoft Edge is available from their Microsoft Security Baselines Blog. Google hardening guidance for Google Chrome is available within their *Chrome Browser Enterprise Security Configuration Guide*.
Microsoft Office is blocked from creating child processes.	ASD's E8MVT can assist in determining the implementation of this control as it includes test files that contain Microsoft Office macros designed to test each ASR rule. Note, this test will need to be conducted with an account that is allowed to execute Microsoft Office macros. Within the RSoP report, look for the 'Configure Attack Surface Reduction rules' setting at 'Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\'. It should be enabled and include the entries of 'D4F940AB-401B-4EFC-AADC-AD5F3C50688A' and '26190899-1602-49E8-8B27-EB1D0A1CE869' with a value of 1 (i.e. enabled).

Microsoft Office is blocked from creating executable content.	ASD's E8MVT can assist in determining the implementation of this control as it includes test files that contain Microsoft Office macros designed to test each ASR rule. Note, this test will need to be conducted with an account that is allowed to execute Microsoft Office macros. Within the RSoP report, look for the 'Configure Attack Surface Reduction rules' setting at 'Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\'. It should be enabled and include the entries of '3B576869-A4EC-4529-8536-B80A7769E899' and 'BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550' with a value of 1 (i.e. enabled).
Microsoft Office is blocked from injecting code into other processes.	ASD's E8MVT can assist in determining the implementation of this control as it includes a test file that contains a Microsoft Office macro designed to test this ASR rule. Note, this test will need to be conducted with an account that is allowed to execute Microsoft Office macros. Within the RSoP report, look for the 'Configure Attack Surface Reduction rules' setting at 'Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\'. It should be enabled and include the entry of '75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84' with a value of 1 (i.e. enabled).
Microsoft Office is configured to prevent activation of OLE packages.	ASD's E8MVT can assist in determining the implementation of this control. Within the RSoP report, look for the 'PackagerPrompt' registry setting at 'HKEY_CURRENT_USER\Software\Microsoft\Office\<version>\<Microsoft Office Application>\Security\'. It should exist and be set to 'REG_DWORD 0x00000002 (2)'.
ACSC or vendor hardening guidance for Microsoft Office is implemented.	Generally, hardening guidance can be configured via group policy setting templates that are made available by vendors. This will be included as part of any RSoP reports that are provided. ACSC hardening guidance for Microsoft Office is available within the *Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016* publication. Microsoft hardening guidance for Microsoft Office is available from their Microsoft Security Baselines Blog.
Microsoft Office security settings cannot be changed by users.	ASD's E8MVT can assist in determining the implementation of this control. Within the RSoP report, look for security-related group policy settings that have been defined for Microsoft Office. Alternatively, request a screenshot of the security settings of each Microsoft Office application present on the system. Identify if settings are greyed out, thereby indicating they cannot be changed by users.

PDF software is blocked from creating child processes.	ASD's E8MVT can assist in determining the implementation of this control. This attack surface reduction rule applies only to Adobe PDF software. As such, open any Adobe PDF software that exists on the system, such as Adobe Acrobat, and use File-Open to browse to a location with an exe, such as the Windows directory, change the view to show all files, right click on an executable such as calc.exe and select Open. The ASR rule if implemented will block this action. Within the RSoP report, look for the 'Configure Attack Surface Reduction rules' setting at 'Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\'. It should be enabled and include the entry of '7674BA52-37EB-4A4F-A9A1-F0F9A1619A2C' with a value of 1 (i.e. enabled).
ACSC or vendor hardening guidance for PDF software is implemented.	Generally, hardening guidance for PDF software can be configured via registry settings. This will be included as part of any RSoP reports that are provided. Adobe hardening guidance for Adobe Acrobat and Adobe Reader is available within their *Security Configuration Guide for Acrobat* publication.
PDF software security settings cannot be changed by users.	Within the RSoP report, look for security-related group policy settings that have been defined for PDF software. Alternatively, request a screenshot of the security settings of any PDF software present on the system. Identify if settings are greyed out, thereby indicating they cannot be changed by users.
Blocked PowerShell script execution events are logged.	ASD's E8MVT can assist in determining the implementation of this control. If an application control solution has been suitably configured, it should already capture any blocked attempts to execute PowerShell scripts. If not, discuss what other logging mechanisms are in place to capture any blocked attempts to execute PowerShell scripts on the system and seek supporting evidence.

Restrict administrative privileges

Context

To avoid users collecting privileges and access as they change roles throughout an organisation, and to enforce the principle of least-privileged role-based access control, privileged users should be required to regularly revalidate their requirement for privileged access. As such, privileged accounts that have not been used within 45 days strongly indicate that they are no longer required. Rather than accounts remaining active, and a possible target for malicious actors to exploit, inactive accounts should be disabled on a regular basis.

For Maturity Level Two, privileged operating environments must not be virtualised within unprivileged operating environments. This constraint allows for three implementation scenarios:

- physically separate operating environments
- an unprivileged operating environment virtualised within a privileged operating environment

- both a privileged and unprivileged operating environment virtualised within a physical host's hardened operating environment.

Jump servers play an important role as a centralised logging and tool enforcement point for administrative activities, even when privileged operating environments are used.

The use of a common local administrator password for every workstation and server is a common approach in poorly-secured networks due to its ease of use. A marginally more secure approach is using passwords that are a combination of a fixed component and a dynamic component (e.g. including a unique asset identifier). While the latter may appear to be secure, if malicious actors are able to compromise one or more local administrator passwords they may be able to discern a pattern. Ideally, an approach that ensures local administrator and service accounts are unique, unpredictable and managed should be used. For example, Microsoft's Local Administrator Password Solution.

Event logs relating to the use of, and changes to, privileged accounts should be collected and stored in case there is a cyber incident and they are required for forensic analysis or cyber incident response activities. Often, the lack of sufficient logging can impact the ability to determine the extent of a cyber incident, how it occurred and what vulnerabilities need to be mitigated.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.	Check whether an account expiry date is set in Active Directory under account profiles and whether a mechanism exists to automatically disable accounts after 12 months unless revalidated beforehand. Ask for a screenshot of the output of the following PowerShell commands that check for accounts with either no expiration date or have an expiration date that exceeds 12 months: *Get-ADUser -Filter {(admincount -eq 1) -and (enabled -eq $true)} -Properties AccountExpirationDate \| Where-Object {$_.AccountExpirationDate -like "" | Select @{n='Username'; e={$_.SamAccountName}}, @{n='Account Expiration Date'; e={$_.AccountExpirationDate}}, @{n='Enabled'; e={$_.Enabled}}* *Get-ADUser -Filter {(admincount -eq 1) -and (enabled -eq $true)} -Properties AccountExpirationDate \| Where-Object {$_.AccountExpirationDate -gt (Get-Date).AddMonths(12)} | Select @{n='Username'; e={$_.SamAccountName}}, @{n='Account Expiration Date'; e={$_.AccountExpirationDate}}, @{n='Enabled'; e={$_.Enabled}}*
Privileged access to systems and applications is automatically disabled after 45 days of inactivity.	Microsoft provides guidance on the use of PowerShell to identify inactive accounts based on when they were last used to logon to a system. Ask for a screenshot of the output of the following PowerShell command that checks for inactive accounts to demonstrate that this activity takes place on a daily basis: *Get-ADUser -Filter {(admincount -eq 1) -and (enabled -eq $true)} -Properties LastLogonDate \| Where-Object {$_.LastLogonDate -lt (Get-Date).AddDays(-45) -and$_.LastLogonDate -ne $null} \| Select @{n='Username'; e={$_.samaccountname}}, @{n='Last Logon Date'; e={$_.LastLogonDate}}, @{n='Enabled'; e={$_.enabled}}*

Privileged operating environments are not virtualised within unprivileged operating environments.	Discuss how privileged operating environments have been implemented for the management of the system. It should align to one of the implementation scenarios within the context section of this mitigation strategy and be covered within the security documentation for the system.
Administrative activities are conducted through jump servers.	Tools such as BloodHound can be used to determine the path administrators are using to log in and which servers are jump servers. Request a system administrator demonstrate creating and removing a test user account to confirm the use of jump servers. Discuss the network structure for the system to determine if jump servers have been implemented for administrative activities. This should be visible in network diagrams for the system.
Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed.	Discuss how local administrator and service accounts are managed. Confirm if Microsoft's Local Administrator Password Solution, or another suitable approach that results in long, unique and unpredictable passwords for each workstation and server, is used. To check if all computers have LAPS configured, run the following PowerShell commands and compare the output: *Get-ADComputer -Filter {ms-Mcs-AdmPwdExpirationTime -like "*"} -Properties ms-Mcs-AdmPwdExpirationTime | measure* *Get-ADComputer -Filter {Enabled -eq $true} | measure* Discuss how group Managed Service Accounts (gMSAs) are managed. gMSAs are domain accounts that use 240-byte randomly generated complex passwords. gMSAs shift password management to the Windows operating system, which changes the password every 30 days.
Privileged access events are logged.	Within the RSoP report, look for the 'Audit Sensitive Privilege Use' setting at 'Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\'. It should be enabled with a value of 'Success and Failure'. In addition, look for the 'Audit Logon', 'Audit Other Logon/Logoff Events' and 'Audit Special Logon' settings at 'Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff'. They should be enabled with a value of 'Success and Failure'. Finally, look for the 'Audit Logoff' setting at 'Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff'. It should be enabled with a value of 'Success'.

Privileged account and group management events are logged.	Using the specific event IDs (available from Microsoft Docs), check whether changes to privileged accounts and groups are logged in event viewer or a SIEM tool. More information on security operations for privileged accounts in Active Directory, including specific event IDs for this control, can be found at Microsoft Docs.
	Within the RSoP report, look for the 'Audit Computer Account Management' and 'Audit User Account Management' settings at 'Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\'. They should be enabled with a value of 'Success and Failure'. In addition, look for the 'Audit Security Group Management' setting at 'Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\'. It should be enabled with a value of 'Success and Failure'.

Patch operating systems

Context

At this maturity level, the timeframe for patching vulnerabilities in operating systems is decreased from one month to two weeks. In addition, this maturity level requires weekly vulnerability scanning.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
A vulnerability scanner is used at least **weekly** to identify missing patches or updates for vulnerabilities in operating systems of workstations, servers and network devices.	Use the guidance provided in Maturity Level One of this guide and apply the Maturity Level Two timeframes.
Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, servers and network devices are applied within **two weeks** of release.	Use the guidance provided in Maturity Level One of this guide and apply the Maturity Level Two timeframes.

Multi-factor authentication

Context

At this maturity level, an additional requirement for all privileged users logging onto systems, both locally and remotely, to use multi-factor authentication is introduced. In addition, the authentication methods that can be used, and in what combination, are restricted to avoid weaker implementations. Specifically, acceptable multi-factor authentication implementations include:

- something users have (i.e. look-up secret, out-of-band device, single-factor one-time PIN (OTP) devices, single-factor cryptographic software or single factor cryptographic device) in addition to something users know (i.e. a memorised secret)
- something users have that is unlocked by something users know or are (i.e. multi-factor OTP device, multi-factor cryptographic software or multi-factor cryptographic device).

Biometrics are not acceptable at this maturity level. This is due to biometric characteristics not being secrets, biometric matching being probabilistic rather than deterministic and there being a reliance on the security of biometric capture software installed on devices. However, biometrics can be used to unlock another authentication factor (e.g. a certificate stored in a Trusted Platform Module or an OTP generator app on a smartphone). Trusted Signals are also not acceptable at this maturity level. This is due to issues associated with placing trust in the signal itself, which can be targeted and spoofed by malicious actors.

While not yet excluded at this maturity level, organisations may want to avoiding authentication methods increasingly being subject to MFA fatigue or social engineering attempts by malicious actors, such as push notifications and SMS codes.

Event logs for multi-factor authentication events should be collected and stored in case there is a cyber incident and they are required for forensic analysis or cyber incident response activities. The lack of sufficient logging can impact the ability to determine the extent of a cyber incident, how it occurred and what vulnerabilities need to be mitigated.

Note, at this maturity level organisations may choose to implement multi-factor authentication solutions that are phishing-resistant, such as security keys or smartcards, if they intend to eventually implement requirements for Maturity Level Three.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Multi-factor authentication is used to authenticate privileged users of systems.	Observe an administrator authenticate to a system to check whether they are required to use MFA. Alternatively, request evidence of the logon screen for a privileged user. The logon screen should show multiple authentication methods being requested.

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.	Discuss the implementation of multi-factor authentication for users. Note, multiple different forms of multi-factor authentication may exist depending on the number of different systems and internet-facing services that users authenticate to. For example, multi-factor authentication for administration of cloud services might involve a different implementation to multi-factor authentication for administration of on-premises services. Furthermore, not all third-party internet-facing services may offer the same multi-factor authentication implementation. Discussions should also include distinguishing between multi-step authentication and multi-factor authentication, as well as different levels of security provided by different multi-factor authentication implementations. For example, a security key or smartcard is more secure than a hardware OTP device which is more secure than an OTP mobile app which is more secure than a push notification or SMS code sent to a smartphone.
Successful and unsuccessful multi-factor authentication events are logged.	Within the RSoP report, look for the 'Audit Logon' and 'Audit Special Logon' settings at 'Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\'. They should be enabled with a value of 'Success and Failure'. For certain MFA implementations the above guidance may not be applicable. In these instances discuss whether logging is available for all systems that users authenticate to and seek evidence that such logging is in place. If an administrator logon was observed (per the first control in this table), request recent event logs to check that there is a corresponding event log entry.

Regular backups

Context

At this maturity level, privileged accounts (with the exception of backup administrator accounts) are limited to only accessing their own backups, and should not be able to modify and delete backups.

It is important that backup administrator accounts (as well as user accounts in general) are provisioned following the principles of least privilege and separation of duties. As such, backup administrator accounts should only be given to a small group of trusted administrators and a separate group should be setup for the purpose of restoring backups. Excessive permissions for accounts increases the chance that they will be compromised. Should this occur for these accounts, malicious actors performing ransomware attacks can easily encrypt or delete all backups.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.	Use the guidance provided in Maturity Level One of this guide and apply the Maturity Level Two access control requirements. Specifically, privileged accounts should only be able to access their own backups (except for backup administrator accounts). Active Directory queries and tools such as BloodHound can help to identify privileged accounts including backup administrator accounts.
Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.	Use the guidance provided in Maturity Level One of this guide and apply the Maturity Level Two access control requirements. Specifically, privileged accounts should no longer be able to modify and delete backups. Such activities should be restricted to backup administrator accounts. Active Directory queries and tools such as BloodHound can help to identify privileged accounts including backup administrator accounts.

Maturity Level Three

The focus of this maturity level is malicious actors who are more adaptive and much less reliant on public tools and techniques. These malicious actors are able to exploit the opportunities provided by weaknesses in their target's cyber security posture, such as the existence of older operating systems or inadequate logging and monitoring. Malicious actors do this to not only extend their access once initial access has been gained to a target, but to evade detection and solidify their presence. Malicious actors make swift use of exploits when they become publicly available as well as other tradecraft that can improve their chance of success.

Generally, at this level, malicious actors are more focused on particular targets and, more importantly, are willing and able to invest effort into circumventing particular policy and technical controls implemented by their targets. For example, this includes socially engineering a user to execute a malicious Microsoft Office macro or circumventing multi-factor authentication implementations by stealing authentication token values to impersonate a user. Once a foothold is gained on a system, malicious actors seek to gain privileged credentials or password hashes, pivot to other parts of a network, and cover their tracks. Depending on their intent, malicious actors may also destroy all data (including backups).

The guidance below outlines the requirements to be assessed in addition to the requirements of the previous maturity level. In doing so, assessments against Maturity Level Three should focus on the delta between Maturity Level Two and Maturity Level Three.

Application control

Context

At this maturity level, the scope of application control is expanded to include drivers and all servers (not just internet-facing servers). Note, while Microsoft AppLocker does not currently support the control of drivers, Windows Defender Application Control (WDAC) does. This maturity level also includes the requirement for centralised logging of allowed and blocked execution events on workstations and servers.

Microsoft maintains a list of application control bypasses and malicious drivers that have been discovered by security researchers and malicious actors. Implementing Microsoft's recommended block rules and recommended driver block

rules can help to provide protection from malicious actors that would have looked at using these against an otherwise robust application control implementation to gain access to a system.

When implementing an application control solution, an organisation may develop application control rulesets but fail to ensure they remains fit-for-purpose by reviewing them on a regular basis. This can lead to the potential failure to identify several scenarios, such as operating system vendors changing permissions on paths as part of updates or upgrades, exploitable applications or drivers remaining approved for a system, vendor code-signing certificates being compromised, or system administrators introducing exceptions to 'get things working' or troubleshoot but failing to remove the workarounds afterwards. Each of these scenarios are real, having been observed during assessments, and introduce additional vulnerabilities into a system that may be exploited by malicious actors.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Application control is implemented on workstations and **servers**.	It is important to note that at this maturity level the scope has been expanded to include all servers. As such, use the guidance provided in Maturity Level Two of this guide and apply it to all servers rather than just internet-facing servers.
Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets **and drivers** to an organisation-approved set.	Depending on the application control solution, controlling the execution of drivers may or may not be supported. Request a copy of application control rulesets to check for the inclusion of drivers.
Microsoft's 'recommended block rules' are implemented.	Request a copy of application control rulesets. Check whether Microsoft's recommended block rules have been specified.
Microsoft's 'recommended driver block rules' are implemented.	Depending on the application control solution, controlling the execution of drivers may or may not be supported. Request a copy of application control rulesets to check for the inclusion of drivers. If drivers are included, check whether Microsoft's recommended driver block rules have been specified.
Application control rulesets are validated on an annual or more frequent basis.	Discuss how application control rulesets are validated and with what frequency. In addition, discuss the governance processes and procedures around making changings to application control rulesets and any testing or reviews that are conducted following operating system upgrades and the addition or removal of applications.

Allowed and blocked execution events on workstations and **servers** are **centrally** logged.	Request the event logs associated with the testing performed using application control testing tools. Discuss whether event logs are stored locally or centrally. Note, organisations that are comfortable that certain events have a high probability of being legitimate may choose to filter them out as part of their centralised collection in order to simplify event log analysis and reduce storage requirements.
Event logs are protected from unauthorised modification and deletion.	Discuss whether a security information and event management (SIEM) solution is appropriately configured for the protection of event logs.
Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	Discuss whether a SIEM solution supported by security operations centre (SOC) analysts is used to monitor event logs for signs of compromise and respond when any signs of compromise are detected.

Patch applications

Context

At this maturity level, patches, updates or other vendor mitigations must be applied within 48 hours rather than two weeks if an exploit exists. In addition, all applications that are no longer supported by vendors should be removed.

This requirement can be assessed in a similar way to Maturity Level Two, except that if an exploit exists, patches, updates or other vendor mitigations must be applied within 48 hours rather than two weeks.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting an assessment method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release**, or within 48 hours if an exploit exists**.	Use the relevant guidance provided in Maturity Level One of this guide and apply the Maturity Level Three timeframes when exploits exist for vulnerabilities.

Applications that are no longer supported by vendors are removed.	Use the relevant guidance provided in Maturity Level One of this guide and extend it to all applications.

Configure Microsoft Office macro settings

Context

Disabling the use of Microsoft Office macros represents an optimal security outcome, however, some users will have a business requirement for their use. In such situations, additional controls should be implemented to make the use of Microsoft Office macros as secure as possible. This may include either running Microsoft Office macros from within a sandboxed environment, from an appropriately controlled Trusted Location or ensuring they are digitally signed by a trusted publisher.

As Microsoft Office allows any files that are opened from a Trusted Location to bypass security checks, it is critical that only trusted users can write to or modify content in these locations. Under no circumstances should Trusted Locations be specified within a user's profile, such as their desktop or documents folders.

If the 'Disable all macros except digitally signed macros' setting is used, this will allow any Microsoft Office macro signed by a trusted publisher to execute without prompting the user for permission. However, any Microsoft Office macro that is digitally signed by an untrusted publisher will ask users to decide as to whether they would like to allow the Microsoft Office macro to execute via the Message Bar or Backstage View. While this prompt can be disabled using a group policy setting, the removal of the option to enable Microsoft Office macros via the Backstage View requires the implementation of an undocumented graphical user interface setting.

When implementing a digitally signed Microsoft Office macro approach, an organisation may identify a list of trusted publishers but fail to review them on a regular basis for their ongoing suitability. This can create issues when a vendor's code-signing certificate is compromised. Ideally, an organisation should acquire their own code-signing certificate and re-sign any Microsoft Office macros they trust, even if already signed by a third party. While introducing additional overhead, this mitigates the risk of trusting compromised third-party code-signing certificates.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
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.	Within the RSoP report, look for the 'VBA Macro Notification Settings' setting at 'User Configuration\Policies\Administration Templates\<Microsoft Office Application>\Application Settings\Security\Trust Center\'. It should be enabled and configured to 'Disable all macros without notification' (if Trusted Locations are used) or 'Disable all macros except digitally signed macros' (if digitally signed Microsoft Office macros are used). Note, an organisation may choose to use a combination of Trusted Locations and digitally signed Microsoft Office macros. However, if only digitally signed Microsoft Office macros are used then Trusted Locations should be disabled.

	Within each Microsoft Office application, request a screenshot showing Trust Center macro settings (File – Options – Trust Center – Trust Center Settings – Macro Settings). In addition, request a screenshot showing Trust Center trusted publisher settings (File – Options – Trust Center – Trust Center Settings – Trusted Publishers). For the assessment of Microsoft Office macro security, identify what setting is selected for 'macro settings'. The setting should either be set to 'Disable all macros without notification' (if Trusted Locations are used) or 'Disable all macros except digitally signed macros' (if digitally signed Microsoft Office macros are used). For the assessment of Trusted Locations, check whether the 'Disable all trusted locations' option has been checked or not. If it has not, then Trusted Locations are enabled and should be individually assessed for their suitability.
Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.	For each Trusted Location that is specified, review the effective file system permissions for that location (i.e. similar to the assessment for application control at Maturity Level One). If able to, the assessor should seek to review file system permissions themselves rather than requesting a screenshot. Check the total number of users who are in the groups that have the relevant file system permissions.
Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.	Within the RSoP report, look for the 'Disable all Trust Bar notifications for security issues' setting at 'User Configuration\Policies\Administration Templates\Microsoft Office <version>\Security Settings\'. It should be enabled. In addition, look for the 'Disable commands' setting at 'User Configuration\Policies\Administration Templates\<Microsoft Office Application>\Disable Items in User Interface\Custom\'. It should be enabled with a value of 'Enter a command bar ID to disable: 19092'.
Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.	For the assessment of trusted publishers, check which publishers are listed. Ideally, this should only be a code-signing certificate belonging to the organisation. Alternatively, if external vendors' code-signing certificates are listed, discuss how often these are reviewed and what mechanisms are used to identify when/if these need to be removed due to compromise by malicious actors as part of supply chain attacks.
Allowed and blocked Microsoft Office macro execution events are **centrally** logged.	Request the event logs associated with the testing performed using tools that attempt to run Microsoft Office macros. Discuss whether event logs are stored locally or centrally. Note, organisations that are comfortable that certain events have a high probability of being legitimate may choose to filter them out as part of their centralised collection in order to simplify event log analysis and reduce storage requirements.
Event logs are protected from unauthorised modification and deletion.	Discuss whether a SIEM solution is appropriately configured for the protection of event logs.

Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	Discuss whether a SIEM solution supported by SOC analysts is used to monitor event logs for signs of compromise and respond when any signs of compromise are detected.

User application hardening

Context

At this maturity level, Internet Explorer 11 must be disabled or removed from operating systems rather than just blocked from accessing the internet or opening files from the internet.

.NET Framework 3.5 (including .NET 2.0 and 3.0) is often targeted by malicious actors due to its lack of security functionality when compared to newer versions of the .NET Framework, as well as due to its linkages to PowerShell 2.0. Within Microsoft Windows there are two separate features relating to the .NET Framework, '.NET Framework 3.5 (includes .NET 2.0 and .NET 3.0)' and '.NET Framework 4.8 Advanced Services'.

Microsoft ended support for Windows PowerShell 2.0 in late 2017. At that time, Microsoft noted that Windows PowerShell 2.0 lacked the security functionality of Windows PowerShell 5.0 and higher.

Constrained Language Mode for PowerShell is designed to prevent PowerShell users (which may include malicious actors) from running tools that exploit PowerShell or load Component Object Model objects, libraries and classes into a PowerShell session.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Internet Explorer 11 **is disabled or removed**.	Within the RSoP report, look for the 'Computer Configuration/Administrative Templates/Windows Components/Internet Explorer/Disable Internet Explorer 11 as a standalone browser' setting. It should be enabled. Alternatively, request a screenshot of the 'Windows Features' that are installed. This can be accessed via (Settings – Apps & features – Programs and Features – Turn Windows features on or off). Check whether Internet Explorer 11 is installed by checking for a tick or black square. Note, if Internet Explorer 11 has already been removed it may not appear in the list of Windows Features. Note, as standard users will still be able to launch Internet Explorer 11, even in Microsoft Windows 11, an application control block rule should be set for iexplore.exe.

.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.	Request a screenshot of the 'Windows Features' that are installed. For Microsoft Windows 11, this can be accessed via (Settings – Apps – Optional features – More Windows features). For Microsoft Windows 10, this can be accessed via (Settings – Apps & features – Programs and Features – Turn Windows features on or off). Check which of the .NET Frameworks are installed by checking for a tick or black square. Note, enabling .NET Framework 3.5 will automatically enable PowerShell 2.0.
Windows PowerShell 2.0 is disabled or removed.	Request a screenshot of the 'Windows Features' that are installed. For Microsoft Windows 11, this can be accessed via (Settings – Apps – Optional features – More Windows features). For Microsoft Windows 10, this can be accessed via (Settings – Apps & features – Programs and Features – Turn Windows features on or off). Check if legacy versions of PowerShell are installed by checking for a tick or black square against 'Windows PowerShell 2.0'. To check if a downgrade to PowerShell 2.0 is available, run the following PowerShell command: *Get-WindowsOptionalFeature -online | Where-Object {$_.FeatureName -match "PowerShellv2"}*
PowerShell is configured to use Constrained Language Mode.	Request a screenshot of the output of running the following PowerShell command: *$ExecutionContext.SessionState.LanguageMode*. If Constrained Language Mode is enabled, the output will be 'ConstrainedLanguage'. Otherwise, the output will be 'FullLanguage'.
Blocked PowerShell script execution events are **centrally** logged.	Run a PowerShell script that should be blocked and request evidence of the associated event log entry. Discuss whether event logs are stored locally or centrally. Note, organisations that are comfortable that certain events have a high probability of being legitimate may choose to filter them out as part of their centralised collection in order to simplify event log analysis and reduce storage requirements.
Event logs are protected from unauthorised modification and deletion.	Discuss whether a SIEM solution is appropriately configured for the protection of event logs.
Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	Discuss whether a SIEM solution supported by SOC analysts is used to monitor event logs for signs of compromise and respond when any signs of compromise are detected.

Restrict administrative privileges

Context

Staff seeking access to systems and applications, especially with privileged access, should have a genuine business requirement to do so. Once a requirement to access a system or application is established, staff should be provided with only the privileges they require to undertake their duties. This can be achieved using role-based access controls.

Just-in-time (JIT) privileged access management (PAM) is an extension of role-based access control in which privileged users are only granted the access required to perform their duties immediately before that access is required and for only as long as it is required.

Within an active user session, credentials are cached within the Local Security Authority System Service process to allow for access to network resources without users having to repeatedly enter their credentials. Windows Defender Credential Guard is designed to assist in protecting this process. Windows Defender Remote Credential Guard provides a similar functionality for remote access.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.	Discuss the approach that the organisation has taken to restrict privileged users to only what is required for them to undertake their duties. Often this will involve identifying several different roles, developing policies for those roles and assigning privileged users to one or more of those roles depending on their duties. A system administrator should be able to demonstrate the different user groups and policies or access controls that apply to each. This can confirmed via an RSoP report.
Privileged accounts are prevented from accessing the internet, email and web services.	Use the relevant guidance provided in Maturity Level One of this guide and extend to include privileged service accounts.
Just-in-time administration is used for administering systems and applications.	The implementation of JIT PAM is a complex activity that forms the basis for restricting administrative privileges at Maturity Level Three. Given the complex nature of JIT PAM, it will become apparent from discussions as to whether a JIT PAM approach has been adopted or not. In doing so, it may be worthwhile observing the process of a system administrator requesting and being granted JIT access.

Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.	Within the RSoP report, look for the 'Turn On Virtualization Based Security' setting at 'Computer Configuration\Policies\Administrative Templates\System\Device Guard\'. It should be enabled with a value of 'Credential Guard Configuration: Enabled with UEFI lock'. In addition, look for the 'Restrict delegation of credentials to remote servers' setting at 'Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation\'. It should be enabled with a value of 'Use the following restricted mode: Require Remote Credential Guard'. Note, the use of Windows Defender Credential Guard and Windows Defender Remote Credential Guard has several hardware and software requirements. More information on Windows Defender Credential Guard can be found at Microsoft Docs.
Privileged access events are **centrally** logged.	Request event logs that should have been generated for typical activities associated with the use of a privileged account, such as logging onto a system. Discuss whether event logs are stored locally or centrally. Note, organisations that are comfortable that certain events have a high probability of being legitimate may choose to filter them out as part of their centralised collection in order to simplify event log analysis and reduce storage requirements.
Privileged account and group management events are **centrally** logged.	If an administrator account was created for testing purposes, request the associated event logs that should have been generated when the account was created and added to a privileged group. Discuss whether event logs are stored locally or centrally. Note, organisations that are comfortable that certain events have a high probability of being legitimate may choose to filter them out as part of their centralised collection in order to simplify event log analysis and reduce storage requirements.
Event logs are protected from unauthorised modification and deletion.	Discuss whether a SIEM solution is appropriately configured for the protection of event logs.
Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	Discuss whether a SIEM solution supported by SOC analysts is used to monitor event logs for signs of compromise and respond when any signs of compromise are detected.

Patch operating systems

Context

At this maturity level, patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, servers and network devices are required to be applied within two weeks of release, or within 48 hours if an exploit exists.

Modern operating systems for workstations, servers and network devices often contain security functionality that is not available in earlier releases, even if those earlier releases remain supported by vendors. It is important that an

organisation takes advantage of new security functionality in later releases to further mitigate malicious actors' activities.

The latest release of Microsoft Windows and Microsoft Server will depend on the servicing branch being used. Further release information is available from Microsoft. Similar information is often available from vendors of network devices.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Patches, updates or other vendor mitigations for 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**.	Use the relevant guidance provided in Maturity Level One of this guide and apply the Maturity Level Three timeframes when exploits exist for vulnerabilities.
The latest release, or the previous release, of operating systems are used.	Network-based vulnerability scanners can be used to identify operating systems and their versions. The output of these tools can then be used to check against the latest operating system versions available from vendors.
	For Microsoft Windows workstations and servers, the 'winver' command can be run to determine the version of the operating system. Request a screenshot of the output of running the 'winver' command for servers and workstations (assuming a Standard Operating Environment is used for workstations).

Multi-factor authentication

Context

At this maturity level, all users of important data repositories should be using multi-factor authentication. Furthermore, the types and combinations of multi-factor authentication are further restricted to avoid weaker forms of multi-factor authentication, especially those susceptible to phishing attacks. This can be achieved by ensuring that clients cryptographically verify the authenticity of the server that they are authenticating to. For example, using phishing-resistant multi-factor authentication would result in fake Microsoft 365 login pages being identified as such, rather than fooling users and capturing their credentials (including additional authentication factors).

The acceptable forms of multi-factor authentication at this maturity level are generally limited to including either a security key, smartcard or Trusted Platform Module.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Multi-factor authentication is used to authenticate users of important data repositories.	Request a list of important data repositories for the system and associated screenshots of users attempting to access each of these data repositories. The screenshots should show multiple forms of authentication being requested.
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.	Discuss the form of multi-factor authentication that has been implemented. Note, different forms of multi-factor authentication may exist depending on the range of systems, services and data repositories that users authenticate to.
Successful and unsuccessful multi-factor authentication events are **centrally** logged.	Use the guidance provided in Maturity Level Two of this guide and extend it to include event logs for multi-factor authentication performed when accessing important data repositories. Discuss whether event logs are stored locally or centrally. Note, organisations that are comfortable that certain events have a high probability of being legitimate may choose to filter them out as part of their centralised collection in order to simplify event log analysis and reduce storage requirements.
Event logs are protected from unauthorised modification and deletion.	Discuss whether a SIEM solution is appropriately configured for the protection of event logs.
Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	Discuss whether a SIEM solution supported by SOC analysts is used to monitor event logs for signs of compromise and respond when any signs of compromise are detected.

Regular backups

Context

At this maturity level, only a subset of privileged accounts (i.e. backup administrator accounts) should be able to access backups. The increasing level of controls around which accounts can access backups, and to what extent, progressively limits the damage that may be caused by a ransomware incident.

In addition, at this maturity level, all accounts (except for break glass accounts) should not be able to modify and delete backups.

Assessment guidance

The section below provides guidance tailored to the assessment method. When selecting a method, the quality of the evidence provided by each method should be strongly considered.

Control	Assessment Guidance (ordered by effectiveness)
Unprivileged accounts cannot access backups belonging to other accounts**, nor their own accounts**.	Use the guidance provided in Maturity Level One of this guide and apply the Maturity Level Three access control requirements. Specifically, unprivileged accounts should no longer be able to access their own backups.
Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts**, nor their own accounts**.	Use the guidance provided in Maturity Level One of this guide and apply the Maturity Level Three access control requirements. Specifically, privileged accounts (excluding backup administrator accounts) should no longer be able to access their own backups. Active Directory queries and tools such as BloodHound can help to identify privileged accounts including backup administrator accounts.
Privileged accounts (**including** backup administrator accounts) are prevented from modifying and deleting backups **during their retention period**.	Use the guidance provided in Maturity Level One of this guide and apply the Maturity Level Three access control requirements. Specifically, backup administrator accounts should no longer be able to modify and delete backups during their retention period, but may do so after the retention period has been exceeded. The modification and deletion of backups during their retention period, should such activities be required, need to be restricted to break glass accounts. Active Directory queries and tools such as BloodHound can help to identify privileged accounts (including backup administrator accounts) and break glass accounts.

Stage 4: Development of the security assessment report

In developing the security assessment report, assessors should use the *Essential Eight Assessment Report Template*. However, assessors can use their own report templates for branding purposes if all sections from the template are included.

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

A mapping between the requirements of the *Essential Eight Maturity Model* and the *Information Security Manual* can be found in the *Essential Eight Maturity Model to ISM Mapping* publication.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Annex A: Example Assessment Test Plan – Maturity Level One

Mitigation Strategy	Control Description	Test ID	Test Description	Test Methodology
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.	ML1-AC-01	(Workstations) Executable files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	The tester should attempt to execute a benign executable (EXE or COM) file inside of the user profile directory. The tester should be aware that subfolders within the user profile may have different behaviour depending on the configuration. ACVT can perform path enumeration tests to assist in identifying locations within the user directories that can execute executable files. E8MVT will perform limited testing for file execution in user profiles and temporary directories.
		ML1-AC-02	(Workstations) Software library files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	The tester should attempt to execute a benign software library (DLL or OCX) file inside of the user profile directory. The tester should be aware that subfolders within the user profile may have different behaviour depending on the configuration. E8MVT will perform limited (single folder) testing for file execution in user profiles and temporary directories.
		ML1-AC-03	(Workstations) Script files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	The tester should attempt to execute multiple benign script (PS, VBS, BAT or JS) files inside of the user profile directory. The tester should be aware that subfolders within the user profile may have different behaviour depending on the configuration. E8MVT will perform limited (single folder) testing for file execution in user profiles and temporary directories.
		ML1-AC-04	(Workstations) Installer files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	The tester should attempt to execute a benign installer (MSI, MST or MSP) file inside of the user profile directory. The tester should be aware that subfolders within the user profile may have different behaviour depending on the configuration. E8MVT will perform limited (single folder) testing for file execution in user profiles and temporary directories.
		ML1-AC-05	(Workstations) Compiled HTML files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	The tester should attempt to execute a benign compiled HTML (CHM) file inside of the user profile directory. The tester should be aware that subfolders within the user profile may have different behaviour depending on the configuration. E8MVT will perform limited (single folder) testing for file execution in user profiles and temporary directories.
		ML1-AC-06	(Workstations) HTML applications files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	The tester should attempt to execute a benign HTML application (HTA) file inside of the user profile directory. The tester should be aware that subfolders within the user profile may have different behaviour depending on the configuration. E8MVT will perform limited (single folder) testing for file execution in user profiles and temporary directories.
		ML1-AC-07	(Workstations) Control panel applet files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	The tester should attempt to execute a benign control panel applet (CPL) file inside of the user profile directory. The tester should be aware that subfolders within the user profile may have different behaviour depending on the configuration. E8MVT will perform limited (single folder) testing for file execution in user profiles and temporary directories.
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	ML1-PA-01	An automated method of asset discovery is run and reviewed at least fortnightly.	Confirm that a method of asset discovery is in place (such as an asset discovery tool or a vulnerability scanner with equivalent functionality) and that it is configured to be run in an automated manner at least every fortnight. Confirm that any anomalies that are identified are reviewed and actioned.
	A vulnerability scanner with an up-to-date vulnerability database	ML1-PA-02	A vulnerability scanner with an up-to-date vulnerability database is being used for vulnerability scanning activities.	Confirm that a vulnerability scanner is in place and that the vulnerability database it uses is being updated within 24 hours prior to its use.

	is used for vulnerability scanning activities.			
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in internet-facing services.	ML1-PA-03	(Internet-Facing Services) A vulnerability scanner for internet-facing services is run and reviewed daily.	Confirm that a vulnerability scanner is in place, and it is configured to scan the organisation's internet-facing services. Confirm that reports from the vulnerability scanner are reviewed by the responsible staff daily, and that identified issues have been observed and actioned.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	ML1-PA-04	A vulnerability scanner is run and reviewed at least fortnightly to scan the organisation's office productivity suites, web browsers, email clients, PDF software and security products.	Confirm that a vulnerability scanner is in place, and it is configured to scan the organisation's applications listed, typically requiring a credentialed scan. Confirm that reports from the vulnerability scanner are reviewed by the responsible staff fortnightly, and that identified issues have been observed and actioned.
	Patches, updates or other vendor mitigations for vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.	ML1-PA-05	(Internet-Facing Services) The organisation has a process for identifying vulnerabilities in internet-facing services within 48 hours and has an example of where an available exploit has been identified and patched within 48 hours.	Review the process in place for identifying vulnerabilities in internet-facing systems. Request evidence of the identification and patching of a system that contained an exploitable vulnerability within the environment.
		ML1-PA-06	(Internet-Facing Services) Applications with an exploit that has been available for greater than 48 hours are patched or mitigated.	Use a vulnerability scanner to identify applications within the environment and check that they have been patched against a known exploit. Determine the date the patch was installed and compare to when the patch was made available.
		ML1-PA-07	(Internet-Facing Services) Applications are patched or mitigated within two weeks.	Use a vulnerability scanner to identify applications within the environment and check that they have been patched against a known exploit. Determine the date the patch was installed and compare to when the patch was made available.
	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.	ML1-PA-08	The organisation has an effective process for patching office productivity suites, web browsers, email clients, PDF software and security products within one month.	Confirm the existence of a list of applications, and where the applications are installed. Ensure a process for identifying vulnerabilities for software in the list is consistently followed. Request evidence of the patching of these applications within one month.
		ML1-PA-09	Office productivity suites, web browsers, email clients, PDF software and security products do not have vulnerabilities older than one month.	Use a vulnerability scanner to identify the listed applications within the organisation's environment, and check that they have been patched against a known exploit. Check the date the application was updated and compare to the date the patch was released. Ensure that the gap between is not greater than one month. E8MVT will perform basic checks of some Microsoft Office applications based on version numbers and file modification dates to determine if the software has been updated recently.
	Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player,	ML1-PA-10	The organisation has removed unsupported internet-facing services from the environment.	Confirm that the environment does not contain software on internet-facing systems that is no longer supported by the vendor. Use a vulnerability scanner to identify applications within the environment and check they are supported.
		ML1-PA-11	The organisation has removed unsupported office productivity suites, web browsers, email clients, PDF software and security products from the environment.	Confirm that the environment does not contain any of the listed software that is no longer supported by the vendor. Use a vulnerability scanner to identify applications within the environment and check they are supported.

	and security products 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.	ML1-OM-01	A technical solution exists that blocks Microsoft Office macros for users who are not approved under the Microsoft Office macro policy.	Run RSOP on workstations to identify the Microsoft Office macro security settings applied by group policy settings. This should typically be set to 'Disable without notification'. Note 'Disable with notification' allows users to bypass this control and does not meet the intent. Check for Active Directory security groups that enforce Microsoft Office macro blocking. Test running Microsoft Office macros on a user in the disallowed group. E8MVT will attempt to execute a Microsoft Office macro within a document.
		ML1-OM-02	A record is kept of users that have been approved to allow Microsoft Office macro execution, and this list matches the list of users within the technical solution.	Confirm a repository of approved requests for users to execute Microsoft Office macros is maintained and up to date and matches the technical implementation. Typically, this means the Active Directory Security Group that permits Microsoft Office macro use should match the list of users who have been approved to run Microsoft Office macros.
	Microsoft Office macros in files originating from the internet are blocked.	ML1-OM-03	Microsoft Office files from the internet are unable to execute Microsoft Office macros.	Attempt to run Microsoft Office macros in Microsoft Office files from the internet. Confirm these files are blocked when received by download and email. Do this for all installed Microsoft Office applications. E8MVT will open a test file that contains a zone identifier to indicate it is from the internet.
		ML1-OM-04	Microsoft Office has been configured to block Microsoft Office macros from running in Microsoft Office files from the internet.	Check if the following group policy setting is enabled. Do this for all installed Microsoft Office applications *User Configuration/Policies/Administrative Templates/Microsoft <Application><Version>/Application Settings/Security/Trust Center/Block macros from running in Office files from the internet*. Check if the following registry value exists and is set to 1. Do this for all installed Microsoft Office applications *Computer\HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\office\<version>\<Application>\security\blockcontentexecutionfromInternet*. E8MVT will check that these registry settings are configured to the correct setting. *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\<version>\<application>\security\" | Select-Object -Property blockcontentexecutionfromInternet* Example: *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\" | Select-Object -Property blockcontentexecutionfromInternet*
	Microsoft Office macro antivirus scanning is enabled.	ML1-OM-05	The system has macroruntimescope enabled for Microsoft Office applications in registry settings or has an alternative Microsoft Office macro scanning ability in place.	Check if the following group policy setting is enabled for all Microsoft Office applications *User Configuration/Policies/Administrative Templates/Microsoft Office <Version>/Security Settings/Macro Runtime Scan Scope*. E8MVT will check the registry to confirm that the policy setting is configured.
		ML1-OM-06	System anti-virus successfully detects a virus test signature inside of a Microsoft Office macro in a Microsoft Office file.	Attempt to run a pseudo malicious Microsoft Office macro that contains an EICAR test string. E8MVT will open a test file containing a Microsoft Office macro that will write the EICAR test string to a file.
	Microsoft Office macro security settings cannot be changed by users.	ML1-OM-07	A standard user is unable to modify the security settings for Microsoft Office macros in all Microsoft Office applications.	Open the application and attempt to change the Microsoft Office macro security settings in the Trust Center. Do this for all installed Microsoft Office applications.
User application hardening	Web browsers do not process Java from the internet.	ML1-AH-01	Java content does not execute in Microsoft Edge.	Load a website with known Java content and check if it renders in the web browser. Check the registry keys at *HKLM:\SOFTWARE\Oracle\JavaDeploy\WebDeployJava* and *HKLM:\SOFTWARE\JavaSoft\Java Plug-in*\. *Get-ItemProperty -Path "HKLM:\SOFTWARE\Oracle\JavaDeploy\WebDeployJava"* *Get-ItemProperty -Path "HKLM:\SOFTWARE\JavaSoft\Java Plug-in"*

		ML1-AH-02	Java content does not execute in Google Chrome.	Load a website with known Java content and check if it renders in the web browser.
		ML1-AH-03	Java content does not execute in Mozilla Firefox.	Load a website with known Java content and check if it renders in the web browser.
	Web browsers do not process web advertisements from the internet.	ML1-AH-04	Web ads do not display in Microsoft Edge.	Load a website in Microsoft Edge with known ads and check if it renders in the web browser. Check the 'Block ads on sites that show intrusive or misleading ads' setting is configured. Check if any ad blocking plugins are configured in the web browser.
		ML1-AH-05	Web ads do not display in Google Chrome.	Load a website in Google Chrome with known ads and check if it renders in the web browser. Check the 'Block ads on sites that show intrusive or misleading ads' setting is configured. Check if any ad blocking plugins are configured in the web browser.
		ML1-AH-06	Web ads do not display in Mozilla Firefox.	Load a website in Mozilla Firefox with known ads and check if it renders in the web browser. Check if any ad blocking plugins are configured in the web browser.
	Internet Explorer 11 does not process content from the internet.	ML1-AH-07	Internet Explorer 11 is unable to connect to internet sites. Internet Explorer 11 may be allowed to access internal web applications only.	If Internet Explorer 11 is installed, access an external website using the web browser and ensure it is blocked. If it is not installed, use a manual request method (script, curl, proxy) with modified request headers to imitate IE (e.g. User-Agent) and check if the request is blocked. Review proxy or firewall configuration for the existence of rules to prevent IE specific browsing from reaching the internet.
	Web browser security settings cannot be changed by users.	ML1-AH-08	Microsoft Edge settings cannot be changed by a standard user.	Check that group policy settings are configured for Microsoft Edge. Open the web browser configuration panel and look for existence of a 'Managed by organisation' message or similar. Attempt to change a setting related to networking or security, such as blocking of ads, proxy settings or security level.
		ML1-AH-09	Google Chrome settings cannot be changed by a standard user.	Check that group policy settings are configured for Google Chrome. Open the web browser configuration panel and look for existence of a 'Managed by organisation' message or similar. Attempt to change a setting related to networking or security, such as blocking of ads, proxy settings or security level.
		ML1-AH-10	Mozilla Firefox settings cannot be changed by a standard user.	Check that group policy settings are configured for Mozilla Firefox. Open the web browser configuration panel and look for existence of a 'Managed by organisation' message or similar. Attempt to change a setting related to networking or security, such as blocking of ads, proxy settings or security level.
		ML1-AH-11	Internet Explorer 11 settings cannot be changed by a standard user.	Check that group policy settings are configured for Internet Explorer 11. Open the web browser configuration panel and look for existence of a 'Managed by organisation' message or similar. Attempt to change a setting related to networking or security, such as blocking of ads, proxy settings or security level.
Restrict administrative privileges	Requests for privileged access to systems and applications are validated when first requested.	ML1-RA-01	A process exists and is enforced for granting privileged access to systems.	Confirm the organisation has a documented, approved and enforced privileged access process that outlines the requirements for provisioning a privileged account to a system or application. Confirm the organisation has a list of systems and applications that require privileged access. Review documented privileged access process and systems. Request evidence of process being followed (e.g. support tickets).
	Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services.	ML1-RA-02	Privileged accounts (excluding privileged service accounts) cannot access the internet or web services via a web browser or other mechanism.	While logged in as a privileged user, attempt to browse to an internet website. Review the configuration preventing internet access and attempt to change this as a privileged user not responsible for administering that system. Privileged accounts not responsible for administering these systems should not be able to change settings to access the internet. While privileged account policies should be reviewed, they do not satisfy this control without additional technical mechanisms.
		ML1-RA-03	Privileged accounts are not configured with mailboxes and email addresses.	Attempt to open Microsoft Outlook on a system using the privileged account. Run the following PowerShell command *Get-ADUser -Filter {(admincount -eq 1) -and (emailaddress -like "*") -and (enabled -eq $true)} -Properties EmailAddress | Select samaccountname, emailaddress*

	Privileged users use separate privileged and unprivileged operating environments.	ML1-RA-04	All administrative activities are performed in an administrative environment that is segmented from the standard user network environment. A separate environment is provisioned for the use of privileged access and is not used for any other purpose.	Attempt to access the administrative network environment using a standard account. Attempt to access the standard environment using a privileged account. Look for evidence of administrative access to unprivileged environments, using tools such as Bloodhound. Check for the existence of workstations that exist solely for privileged access purposes. The privileged operating environment must not be virtualised within the unprivileged operating environment for Maturity Level Two or Maturity Level Three. However, it can be for Maturity Level One.
	Unprivileged accounts cannot logon to privileged operating environments.	ML1-RA-05	Unprivileged accounts are not able to logon to systems in the privileged environment.	Use Bloodhound to analyse Active Directory data and look for which users and groups have RDP access to servers. Review group policy settings for RDP permissions.
		ML1-RA-06	Unprivileged user prevented from using the PowerShell remote PSRemote windows feature.	Run the following PowerShell command *(Get-PSSessionConfiguration -Name Microsoft.PowerShell).Permission* Check the members of the built-in Active Directory Security Group Remote Management Users.
	Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	ML1-RA-07	A privileged account cannot be used to authenticate and interactively login to standard user workstations, or other unprivileged environments. Limited-permission administrative accounts can be used to meet business requirements in unprivileged environments, such as for help desk personnel.	Attempt to login with a privileged account to a standard user workstation. Check group policy settings for 'Deny logon locally' and 'Deny log on through Remote Desktop Services user rights' to workstations for privileged accounts. Limited-permission administrative accounts can be used to meet business requirements in unprivileged environments, such as for help desk personnel. These accounts should not be highly privileged. Review list of administrative users who can login to unprivileged environments. None of the users should be highly privileged, for example Domain Administrators. These users should not be able to access the privileged environment.
		ML1-RA-08	An unprivileged account logged into a standard user workstation cannot raise privileges to a privileged user.	While logged in as a standard user, attempt to use 'runas' to open an application as an administrator. Attempt other ways (e.g. WinRM, Computer Management or RDP) to escalate privileges to an administrator.
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.	ML1-PO-01	An automated method of asset discovery is run and reviewed at least fortnightly.	Confirm that a method of asset discovery is in place (such as an asset discovery tool or a vulnerability scanner with equivalent functionality) and that it is configured to be run in an automated manner at least every fortnight. Confirm that any anomalies that are identified are reviewed and actioned.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	ML1-PO-02	A vulnerability scanner with an up-to-date vulnerability database is being used for vulnerability scanning activities.	Confirm that a vulnerability scanner is in place and that the vulnerability database it uses is being updated within 24 hours prior to its use.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing services.	ML1-PO-03	A vulnerability scanner is run and reviewed daily to scan the organisation's internet-facing services.	Confirm that a vulnerability scanner is in place, and it is configured to scan the organisation's internet-facing services. Confirm that reports from the vulnerability scanner are reviewed by the responsible staff daily, and that identified issues have been observed and actioned.
	A vulnerability scanner is used at least fortnightly to identify missing patches or	ML1-PO-04	A vulnerability scanner is run and reviewed at least fortnightly to scan the organisation's operating systems.	Confirm that a vulnerability scanner is in place, and it is configured to scan the organisation's operating systems, typically requiring a credentialed scan. Confirm that reports from the vulnerability scanner are reviewed by the responsible staff fortnightly, and that identified issues have been observed and actioned.

	updates for vulnerabilities in operating systems of workstations, servers and network devices.			
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.	ML1-PO-05	The organisation has an example of where an available exploit has been identified and patched within 48 hours.	If available, request evidence of the identification and patching of a system that contained an exploitable vulnerability within the environment.
		ML1-PO-06	Internet-facing system that have a vulnerable operating system with an exploit that has been available for greater than 48 hours are patched or mitigated.	View vulnerability management solution, logon to server to verify patch applied successfully or review mitigation strategy. E8MVT will assesses based on most recently installed critical patch. Does not test for existing exploits or 48-hour timeframe requirements.
		ML1-PO-07	Internet-facing systems that have a vulnerable operating system are patched or mitigated within two weeks.	Use vulnerability management solution to perform a patch audit of servers. Retrieve the update history of the workstation, noting the release date of the patch and the date it was installed. Look for differences greater than two weeks.
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release.	ML1-PO-08	The organisation has an effective process for patching operating systems within one month.	Confirm the existence of a list of managed operating systems, and where they are located. Ensure a process for identifying vulnerabilities for operating systems in the list is consistently followed. Request evidence of the patching of these systems within one month.
		ML1-PO-09	Operating systems that have a vulnerability are patched or mitigated within one month.	Use a vulnerability management solution to perform a patch audit of all systems. Retrieve the update history of the systems in scope, noting the release date of the patch and the date it was installed. Look for differences greater than one month.
	Operating systems that are no longer supported by vendors are replaced.	ML1-PO-10	The organisation has removed unsupported operating systems from the environment.	Confirm that the environment does not contain any operating systems no longer supported by the vendor. Use a vulnerability scanner to identify operating systems within the environment and check they are supported.
Multi-factor authentication	Multi-factor authentication is used by an organisation's users when they authenticate to their organisation's internet-facing services.	ML1-MF-01	The organisation has a verified and approved list of internet-facing services operating within the organisation.	Confirm an approved list of internet-facing services exists and this list is regularly checked.
		ML1-MF-02	The organisational remote access desktop solution presents a MFA challenge when attempting to authenticate.	Verify the user is presented with a MFA challenge when authenticating to the organisation's remote solution.
		ML1-MF-03	Organisational internet-facing systems present a MFA challenge when attempting to authenticate.	Verify the user is presented with a MFA challenge when authenticating to the organisation's internet-facing systems.
	Multi-factor authentication is used by an organisation's users when they authenticate to third-party internet-facing services that process, store or communicate	ML1-MF-04	Third-party internet-facing services that hold sensitive data are configured to require users to use MFA.	Verify the organisation's sensitive third-party internet-facing services are configured with MFA. Confirm the organisation has a policy that MFA will be implemented on all third-party internet-facing services that hold sensitive data.

	their organisation's sensitive data.			
	Multi-factor authentication (where available) is used by an organisation's users when they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.	ML1-MF-05	Third-party internet-facing services that hold non-sensitive data are configured to require users to use MFA.	Verify the organisation's third-party internet-facing services are configured with MFA. Confirm the organisation has a policy that MFA will be implemented on all third-party internet-facing services that hold non-sensitive data.
	Multi-factor authentication is enabled by default for an organisation's non-organisational users (but they can choose to opt out) when they authenticate to the organisation's internet-facing services.	ML1-MF-06	The organisational internet-facing services with non-organisational user presents a multi-factor challenge when attempting to authenticate by default.	Verify non-organisational users are presented with a MFA challenge when accessing organisational systems by default. Users may elect to opt out of this feature.
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.	ML1-RB-01	The organisation has a business continuity plan (BCP) that outlines their important data, software and configuration settings that require backing up.	Request the current BCP. Note when the BCP was last modified as old BCPs often don't reference the current environment. Confirm the organisation has a defined list of important data, software and configuration settings.
		ML1-RB-02	Important data, software and configuration settings are backed up and retained as per the timeframes outlined within the BCP.	Verify important data, software and configuration settings are backed up and retained in accordance with the BCP.
	Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time.	ML1-RB-03	Important data, software and configuration settings are backed up in a synchronised manner using a common point in time.	Verify important data, software and configuration settings are backed up in a synchronised manner using a common point in time.
	Backups of important data, software and configuration settings are retained in a secure and resilient manner.	ML1-RB-04	Important data, software and configuration settings are backed up and retained in a secure and resilient manner.	Verify important data, software and configuration settings are backed up and 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.	ML1-RB-05	The organisation has documented evidence of a disaster recovery exercise being performed. This includes examples of where important data, software and configuration settings have been restored from backups.	Verify the organisation has conducted a disaster recovery exercise. Verify the organisation has successfully restored important data, software and configuration settings as part of this exercise. Confirm the existence of a disaster recovery plan (DRP), and ensure it is appropriate, relevant, and followed during incidents and exercises.
	Unprivileged accounts cannot access backups belonging to other accounts.	ML1-RB-06	Unprivileged users are unable to access backups that do not belong to them.	Verify access controls restrict access to only the owner of the information.
	Unprivileged accounts are prevented from modifying and deleting backups.	ML1-RB-07	Unprivileged users are unable to modify and delete backups.	Verify access controls restrict the modification and deletion of backups.

Annex B: Example Assessment Test Plan – Maturity Level Two

Mitigation Strategy	Control Description	Test ID	Test Description	Test Methodology
Application control	**Application control is implemented on workstations and internet-facing servers.**	ML2-AC-01	(Workstations & Internet-facing servers) A dedicated application control solution is implemented.	Check whether an in-built or third-party application control solution has been implemented.
	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets **to an organisation-approved set**.	ML2-AC-02	(Workstations & Internet-facing servers) The system is only able to execute approved executables.	Attempt to execute an unapproved, benign executable. Depending on the policy, there may be directories or specific versions of software that may be allowed to run, but might not be organisationally approved. The tester will have to consider possible policy bypass locations when performing this test. E8MVT will attempt to run an exe file within the local AppData temp directory. ACVT will recursively copy an exe file to the file system and attempt to execute it.
		ML2-AC-03	(Workstations & Internet-facing servers) The system is only able to execute approved software libraries.	Attempt to execute an unapproved, benign software library. Depending on the policy, there may be directories or specific versions of software that may be allowed to run, but might not be organisationally approved. The tester will have to consider possible policy bypass locations when performing this test. E8MVT will attempt to run a dll file within the local AppData temp directory. ACVT will recursively copy a dll file to the file system and attempt to execute it.
		ML2-AC-04	(Workstations & Internet-facing servers) The system is only able to execute approved scripts.	Attempt to execute an unapproved, benign scripts. Depending on the policy, there may be directories or specific versions of software that may be allowed to run, but might not be organisationally approved. The tester will have to consider possible policy bypass locations when performing this test. E8MVT will attempt to run multiple script files within the local AppData temp directory. ACVT will recursively copy multiple script files to the file system and attempt to execute them.
		ML2-AC-05	(Workstations & Internet-facing servers) The system is only able to execute approved installers.	Attempt to execute an unapproved, benign installers. Depending on the policy, there may be directories or specific versions of software that may be allowed to run, but might not be organisationally approved. The tester will have to consider possible bypass locations when performing this test. E8MVT will attempt to run a MSI file that will install a text file into the local AppData temp directory.
		ML2-AC-06	(Workstations & Internet-facing servers) The system is only able to execute approved compiled HTML files.	Attempt to execute an unapproved benign compiled HTML file. Depending on the policy, there may be directories or specific versions of software that may be allowed to run, but might not be organisationally approved. The tester will have to consider possible bypass locations when performing this test. The tester should first test that HH.exe is allowed to execute. If HH.exe is unable to execute than further testing may not be required. E8MVT will attempt to run a compiled HTML file within the local AppData temp directory.
		ML2-AC-07	(Workstations & Internet-facing servers) The system is only able to execute approved HTML applications.	Attempt to execute an unapproved, benign HTML applications. Depending on the policy, there may be directories or specific versions of software that may be allowed to run, but might not be organisationally approved. The tester will have to consider possible bypass locations when performing this test. The tester should first test that MSHTA.exe is allowed to execute. If MSHTA.exe is unable to execute than further testing may not be required. E8MVT will attempt to run an HTML Application file within the local AppData temp directory.

		ML2-AC-08	(Workstations & Internet-facing servers) The system is only able to execute an approved control panel applets.	Attempt to execute an unapproved benign control panel applet. Depending on the policy, there may be directories or specific versions of software that may be allowed to run, but might not be organisationally approved. The tester will have to consider possible bypass locations when performing this test. The tester should first test that CONTROL.exe is allowed to execute. If CONTROL.exe is unable to execute than further testing may not be required. E8MVT will attempt to run a Control Panel Applet file within the local AppData temp directory.
	Allowed and blocked execution events on workstations and internet-facing servers are logged.	ML2-AC-09	(Workstations & Internet-facing servers) The system is logging the application control product when it allows and blocks execution.	Verify event logs contain required data (does not require central storage). Ensure all systems are logging.
Patch applications	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.	ML2-PA-01	A vulnerability scanner is run and reviewed at least weekly to scan the organisation's office productivity suites, web browsers, email clients, PDF software and security products.	Confirm that a vulnerability scanner is in place, and it is configured to scan the organisation's applications listed, typically requiring a credentialed scan. Confirm that reports from the vulnerability scanner are reviewed by the responsible staff weekly, and that identified issues have been observed and actioned.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in other applications.	ML2-PA-02	A vulnerability scanner is run and reviewed at least fortnightly to scan the organisation's other applications.	Confirm that a vulnerability scanner is in place, and it is configured to scan the organisation's other applications, typically requiring a credentialed scan. Confirm that reports from the vulnerability scanner are reviewed by the responsible staff fortnightly, and that identified issues have been observed and actioned.
	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.	ML2-PA-03	The organisation has an effective process for patching office productivity suites, web browsers, email clients, PDF software and security products within two weeks.	Confirm the existence of a list of applications, and where the applications are installed. Ensure a process for identifying vulnerabilities for software in the list is consistently followed. Request evidence of the patching of these applications within two weeks.
		ML2-PA-04	Office productivity suites, web browsers, email clients, PDF software and security products do not have vulnerabilities older than two weeks.	Use a vulnerability scanner to identify the listed applications within the organisation's environment, and check that they have been patched against a known exploit. Check the date the application was updated and compare to the date the patch was released. Ensure that the gap between is not greater than two weeks. E8MVT will perform basic checks of some Microsoft Office applications based on version numbers and file modification dates to determine if the software has been updated recently.
	Patches, updates or other vendor mitigations for vulnerabilities in other applications are applied within one month of release.	ML2-PA-05	Other applications that have a vulnerability are patched or mitigated within one month.	Use a vulnerability scanner to identify vulnerable applications within the organisation's environment, and check that they have been patched against a known exploit. Check the date the application was updated and compare to the date the patch was released. Ensure that the gap between is not greater than one month.

Configure Microsoft Office macro settings	**Microsoft Office macros are blocked from making Win32 API calls.**	ML2-OM-01	Microsoft Office macros in Microsoft Office files are unable to make Win32 API calls.	Open a file that contains a Microsoft Office macro that makes a Win32 API call. Do this for all installed Microsoft Office applications. E8MVT can assist with this test.
	Allowed and blocked Microsoft Office macro execution events are logged.	ML2-OM-02	Allowed execution of a Microsoft Office macro within a Microsoft Office file is logged.	Check that TrustCenter logging is enabled by checking the Enable Logging registry key at *HKCU:\Software\Microsoft\Office\16.0\Common\TrustCenter*. *Get-ItemProperty -Path "HKCU:\Software\Microsoft\Office\<version>\Common\TrustCenter\" | Select-Object -Property EnableLogging* Example: *Get-ItemProperty -Path "HKCU:\Software\Microsoft\Office\16.0\Common\TrustCenter\" | Select-Object -Property EnableLogging* Request evidence of event logs for allowed Microsoft Office macro execution events.
		ML2-OM-03	Blocked execution of a Microsoft Office macro within a Microsoft Office file is logged.	Check that TrustCenter logging is enabled by checking the EnableLogging registry key at *HKCU:\Software\Microsoft\Office\16.0\Common\TrustCenter*. *Get-ItemProperty -Path "HKCU:\Software\Microsoft\Office\<version>\Common\TrustCenter\" | Select-Object -Property EnableLogging* Example: *Get-ItemProperty -Path "HKCU:\Software\Microsoft\Office\16.0\Common\TrustCenter\" | Select-Object -Property EnableLogging* Request evidence of event logs for blocked Microsoft Office macro execution events. Microsoft Office macros blocked due to AV can be found in the Event Viewer.
User application hardening	**ACSC or vendor hardening guidance for web browsers is implemented.**	ML2-AH-01	The ACSC guidance for hardening Microsoft Edge is implemented. OR The Microsoft guidance for hardening Microsoft Edge is implemented.	Use the Microsoft Policy Analyzer to validate the effective state of the system against the Microsoft Edge security baseline.
		ML2-AH-02	The Google guidance for hardening Google Chrome is implemented.	Determine if Google Chrome is configured via group policy settings and if the configured settings are in line with the *Chrome Browser Enterprise Security Configuration Guide* provided by Google at https://support.google.com/chrome/a/answer/9710898?hl=en.
	Microsoft Office is blocked from creating child processes.	ML2-AH-03	Microsoft Office files cannot create child processes.	Open a file that contains a Microsoft Office macro that will create a child process. Confirm it is unable to do this. Check the ASR rule 'd4f940ab-401b-4efc-aadc-ad5f3c50688a' is configured in block mode, or another solution is in place to prevent creation of child processes. Running E8MVT will confirm if the ASR rule to prevent creation of child processes is enabled, or if child process creation has been blocked through a PowerShell command. Running E8MVT will execute a test that opens a file containing a Microsoft Office macro that creates a child process. *$ASR_Rules = Get-MPPreference \| Select -ExpandProperty AttackSurfaceReductionRules_Ids* *$match = $false* *Foreach($rules in $ASR_Rules) {If ($rules -match "d4f940ab-401b-4efc-aadc-ad5f3c50688a") {$match = $true}}* *If($match -eq $true) {Write-Output("Block all Office applications from creating child processes (d4f940ab-401b-4efc-aadc-ad5f3c50688a) is enabled")} else {Write-Output("Block all Office applications from creating child processes (d4f940ab-401b-4efc-aadc-ad5f3c50688a) is not present or disabled")}*
	Microsoft Office is blocked from creating executable content.	ML2-AH-04	Microsoft Office files cannot create executable content.	Open a file that contains a Microsoft Office macro that will create executable content. Confirm it is unable to do this. Check the ASR rule '3b576869-a4ec-4529-8536-b80a7769e899' is configured in block mode, or another solution is in place to prevent creation of executable content.

				Running E8MVT will confirm if the ASR rule to creation of executable content is enabled. Running E8MVT will execute a test that opens a file containing a Microsoft Office macro that creates executable content. *$ASR_Rules = Get-MPPreference \| Select -ExpandProperty AttackSurfaceReductionRules_Ids* *$match = $false* *Foreach($rules in $ASR_Rules) {If ($rules -match "3b576869-a4ec-4529-8536-b80a7769e899") {$match = $true}}* *If($match -eq $true) {Write-Output("Block Office applications from creating executable content (3b576869-a4ec-4529-8536-b80a7769e899) is enabled")} else {Write-Output("Block Office applications from creating executable content (3b576869-a4ec-4529-8536-b80a7769e899) is not present or disabled")}*
	Microsoft Office is blocked from injecting code into other processes.	ML2-AH-05	Microsoft Office files cannot inject code into other processes.	Open a file that contains a Microsoft Office macro that will inject code into another process. Confirm it is unable to do this. Check the ASR rule '75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84' is configured in block mode, or another solution is in place to prevent code injection. Running E8MVT will confirm if the ASR rule to prevent injection of code into other processes is enabled. Running E8MVT will execute a test that opens a file containing a Microsoft Office macro that will attempt to inject code into the explorer.exe process. *$ASR_Rules = Get-MPPreference \| Select -ExpandProperty AttackSurfaceReductionRules_Ids* *$match = $false* *Foreach($rules in $ASR_Rules) {If ($rules -match "75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84") {$match = $true}}* *If($match -eq $true) {Write-Output("Block Office applications from injecting code into other processes (75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84) is enabled")} else {Write-Output("Block Office applications from injecting code into other processes (75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84) is not present or disabled")}*
	Microsoft Office is configured to prevent activation of OLE packages.	ML2-AH-06	Microsoft Office files do not execute OLE packages.	Open a file that contains an OLE object. Check the PackagerPrompt registry key within the Trust Center settings is set to 2. E8MVT will check the required registry key. *Get-ItemProperty -Path "HKCU:\SOFTWARE\Microsoft\office\<version>\<application>\security\" | Select-Object -Property PackagerPrompt* Example: *Get-ItemProperty -Path "HKCU:\SOFTWARE\Microsoft\office\16.0\excel\security\" | Select-Object -Property PackagerPrompt*
	ACSC or vendor hardening guidance for Microsoft Office is implemented.	ML2-AH-07	The ACSC guidance for hardening Microsoft Office is implemented. OR The Microsoft guidance for hardening Microsoft Office is implemented.	Use the Microsoft Policy Analyzer to validate the effective state of the system against the Microsoft Office security baseline.
	Microsoft Office security settings cannot be changed by users.	ML2-AH-08	Microsoft Office security setting are unable to be modified by a standard user account.	Attempt to modify security settings in Microsoft Office. Check that the vbawarnings registry key is configured via policy and that a user is unable to change the Microsoft Office macro settings within the Trust Center options. E8MVT will check the required registry key. *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\<version>\<application>\security\" | Select-Object -Property vbawarnings* Example: *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\" | Select-Object -Property vbawarnings*
	PDF software is blocked from creating child processes.	ML2-AH-09	PDF software cannot create child processes.	Adobe Reader can be tested by opening the application, selecting Open from the File menu, selecting 'All Files (*.*)' from the dropdown menu in the corner, browsing to system32 folder, find calc.exe. Right click and select Open. Check ASR rule 7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c is enabled. Can also run *Get-ProcessMitigation -Name acrobat.exe).ChildProcess.DisallowChildProcessCreation* to check if it has been disabled this way. E8MVT will check that the Adobe child process creation ASR rule is enabled. *$ASR_Rules = Get-MPPreference \| Select -ExpandProperty AttackSurfaceReductionRules_Ids* *$match = $false*

				Foreach($rules in $ASR_Rules) {If ($rules -match "7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c") {$match = $true}} If($match = $true) {Write-Output("Block Adobe Reader from creating child processes (7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c) is enabled")} else {Write-Output("Block Adobe Reader from creating child processes (7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c) is not present or disabled")}
	ACSC or vendor hardening guidance for PDF software is implemented.	ML2-AH-10	Vendor guidance for hardening PDF software is implemented.	Determine the PDF software in use, and if the vendor provides hardening guidance for the product. Follow the guidance to determine if the product has been hardened. Adobe Acrobat and Adobe Reader hardening guidance can be found at https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/index.html.
	PDF software security settings cannot be changed by users.	ML2-AH-11	PDF software security settings are unable to be modified by a standard user account.	Attempt to modify security settings within all allowed PDF readers.
	Blocked PowerShell script execution events are logged.	ML2-AH-12	PowerShell scripts that have been blocked are logged.	Verify event logs contain required data (does not require central storage). Note, if application control is used to restrict the execution of scripts, PowerShell script execution events may already be captured. Ensure all systems are logging.
Restrict administrative privileges	**Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.**	ML2-RA-01	A process for disabling known privileged accounts exists and is enforced. Users are made aware of this requirement when being provisioned with a privileged account.	Review documented process to disable privileged access after 12 months. Review evidence, such as support tickets, emails, logs, or the automated disabling procedure, to confirm accounts are disabled after 12 months unless revalidated.
		ML2-RA-02	There are no privileged accounts that have an Active Directory expiry date that is greater than 12 months or do not have an expiry date.	Query Active Directory using PowerShell commands or tools such as ADRecon to identify accounts with distant or no expiry dates. The following PowerShell command returns privileged accounts with no account expiry set. *Get-ADUser -Filter {(admincount -eq 1) -and (enabled -eq $true)} -Properties AccountExpirationDate \| Where-Object {$_.AccountExpirationDate -like "" | Select @{n='Username'; e={$_.SamAccountName}}, @{n='Account Expiration Date'; e={$_.AccountExpirationDate}}, @{n='Enabled'; e={$_.Enabled}}* The following PowerShell command returns any privileged accounts that have an expiry date greater than 12 months. *Get-ADUser -Filter {(admincount -eq 1) -and (enabled -eq $true)} -Properties AccountExpirationDate \| Where-Object {$_.AccountExpirationDate -gt (Get-Date).AddMonths(12)} | Select @{n='Username'; e={$_.SamAccountName}}, @{n='Account Expiration Date'; e={$_.AccountExpirationDate}}, @{n='Enabled'; e={$_.Enabled}}*
	Privileged access to systems and applications is automatically disabled after 45 days of inactivity.	ML2-RA-03	A process for disabling privileged accounts that have not been used for 45 days exists and is enforced by the entity. Evidence exists for the usage of the 45 days inactive disabling process, including support tickets or administrative logs that show accounts were disabled.	Review documented process to disable privileged access after 45 days of inactivity. Review evidence, such as support tickets, automated disabling procedure to confirm accounts have been disabled.
		ML2-RA-04	There are no enabled privileged accounts that have a lastlogondate that is greater than 45 days.	Query Active Directory using PowerShell commands or tools such as ADRecon to identify enabled privileged accounts with a 'lastlogondate' greater than 45 days. *Get-ADUser -Filter {(admincount -eq 1) -and (enabled -eq $true)} -Properties LastLogonDate \| Where-Object {$_.LastLogonDate -lt (Get-Date).AddDays(-45) -and$_.LastLogonDate -ne $null} \| Select @{n='Username'; e={$_.samaccountname}}, @{n='Last Logon Date'; e={$_.LastLogonDate}}, @{n='Enabled'; e={$_.enabled}}*
	Privileged operating environments are not virtualised within unprivileged operating environments.	ML2-RA-05	Where a privileged environment is virtualised, the virtualised image is not located in an unprivileged environment. This includes virtual machines on a standard unprivileged SOE.	Confirm with the entity where the privileged environment infrastructure is hosted. Look for privileged environments on unprivileged virtual hosts and SOE workstations.

	Administrative activities are conducted through jump servers.	ML2-RA-06	Servers are configured to not allow remote access traffic or connections from systems that are not jump servers.	Attempt to connect to servers or administrator-only systems from an unprivileged environment. Verify Firewall configuration.
	Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed.	ML2-RA-07	The Microsoft Local Administrator Password Solution (LAPS) or a similar solution is implemented on Windows workstations and servers.	Run the following PowerShell commands to retrieve the number of computers with LAPS and compare with the number of computers in Active Directory. Run the following PowerShell command to get number of computers with LAPS. *Get-ADComputer -Filter {ms-Mcs-AdmPwdExpirationTime -like "*"} -Properties ms-Mcs-AdmPwdExpirationTime | measure* Run the following PowerShell command to get the number of enabled computers in Active Directory. *Get-ADComputer -Filter {Enabled -eq $true} | measure*
		ML2-RA-08	Services account passwords are generated to be long, unique and unpredictable. Service account passwords are stored in a secure location, such as a password manager or a Privileged Access Management solution.	Observe evidence of a password management or privileged access management solution in use for managing service account passwords. Ensure generated passwords are unique, unpredictable, and have a minimum length requirement. Look for accounts with identical passwords. Confirm how passwords are generated for local accounts, and that they are managed. If using LAPS for local accounts, check the following group policy setting *Computer Configuration/Administrative Templates/LAPS/Password Settings*.
		ML2-RA-09	Passwords should be changed at least once every 12 months.	Query Active Directory using PowerShell commands or tools such as ADRecon to identify service accounts with passwords last set more than 12 months ago. Run the following PowerShell command to get service accounts with passwords older than 12 months. Replace SVC_* with service account naming convention. *$PassLastSetTimeFrame = (Get-Date).AddMonths(-12)* *Get-ADUser -Filter "enabled -eq 'true' -and SamAccountName -like 'SVC_*'" -Properties pwdlastset \| Where-Object{$_.pwdlastset -like '0' -or ([datetime]::FromFileTime($_.pwdLastSet) -lt $PassLastSetTimeFrame)} \| Select-Object SAMAccountName, @{name ="pwdLastSet"; expression={([datetime]::FromFileTime($_.pwdLastSet))}}*
	Privileged access events are logged.	ML2-RA-10	Successful and failed logins of privileged accounts are logged.	Event logs need to be retained/backed up for a minimum period, so they are available if required. Verify the existence of the following event logs. Event ID 4672 is created when an account with special privileges successfully logs in. Event ID 4625 is created when a logon request fails.
	Privileged account and group management events are logged.	ML2-RA-11	Changes made to privileged accounts and groups within Active Directory are logged.	Event logs need to be retained/backed up for a minimum period, so they are available if required. Verify the existence of the following event logs. Event ID 4738 is created when a user account is modified in Active Directory. Event ID 4728 is created when a member is added to an Active Directory Security Group. Event ID 4729 is created when a member is removed from an Active Directory Security Group. Event ID 4737 is created when a change is made to an Active Directory Security Group.
Patch operating systems	A vulnerability scanner is used at least **weekly** to identify missing patches or updates for vulnerabilities in operating systems of	ML2-PO-01	A vulnerability scanner is run and reviewed at least weekly to scan the organisation's operating systems.	Confirm that a vulnerability scanner is in place, and it is configured to scan the organisation's operating systems, typically requiring a credentialed scan. Confirm that reports from the vulnerability scanner are reviewed by the responsible staff weekly, and that identified issues have been observed and actioned.

	workstations, servers and network devices.			
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, servers and network devices are applied within **two weeks** of release.	ML2-PO-02	The organisation has an effective process for patching operating systems within two weeks.	Confirm the existence of a list of managed operating systems, and where they are located. Ensure a process for identifying vulnerabilities for operating systems in the list is consistently followed. Request evidence of the patching of these systems within two weeks.
		ML2-PO-03	Operating systems that have a vulnerability are patched or mitigated within two weeks.	Use vulnerability management solution to perform a patch audit of all systems. Retrieve the update history of the system, noting the release date of the patch and the date it was installed. Look for differences greater than two weeks.
Multi-factor authentication	**Multi-factor authentication is used to authenticate privileged users of systems.**	ML2-MF-01	A privileged user who is performing administrative activities is required to respond to an MFA challenge at some point in the authentication lifecycle. This can be implemented when authenticating to a machine (such as a jump server) or when attempting to raise privileges. The organisation has a list of systems that have privileged users or support privileged functions.	Verify a privileged user is presented with a MFA challenge when authenticating to a machine or attempting to raise privileges. Confirm the organisation has a list of privileged systems and is regularly updated.
	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.	ML2-MF-02	The organisation requires that internet-facing services use multi-factor authentication that uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	Verify MFA for internet-facing services uses either: Something users have (e.g. look-up secrets, out-of-band devices, single-factor OTP devices, single-factor cryptographic software or single-factor cryptographic devices) AND something users know (e.g. memorised secrets) OR Something users have that is unlocked by something users know or are (e.g. multi-factor OTP devices, multi-factor cryptographic software and multi-factor cryptographic devices)
		ML2-MF-03	The organisation requires that privileged users utilise multi-factor authentication that uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	Verify MFA for internet-facing services uses either: Something users have (e.g. look-up secrets, out-of-band devices, single-factor OTP devices, single-factor cryptographic software or single-factor cryptographic devices) AND something users know (e.g. memorised secrets) OR Something users have that is unlocked by something users know or are (e.g. multi-factor OTP devices, multi-factor cryptographic software and multi-factor cryptographic devices)
	Successful and unsuccessful multi-factor authentication events are logged.	ML2-MF-04	The organisation's internet-facing systems log successful MFA attempts.	Verify successful MFA events are logged for organisations internet-facing systems.
		ML2-MF-05	Administrative access connections log successful MFA attempts.	Verify successful MFA events are logged for administrative access.
		ML2-MF-06	The organisation's internet-facing systems log unsuccessful MFA attempts.	Verify unsuccessful MFA events are logged for organisations internet-facing systems.
		ML2-MF-07	Administrative access connections log unsuccessful MFA attempts.	Verify unsuccessful MFA events are logged for administrative access.
Regular backups	**Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.**	ML2-RB-01	Privileged users (excluding backup administrator accounts) are unable to access backups that do not belong to them.	Verify access controls restrict the access of backups to the owner of the backup and backup administrator accounts.

	Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.	ML2-RB-02	Privileged users (excluding backup administrator accounts) are unable to modify and delete backups.	Verify access controls restrict the modification and deletion of backups to backup administrator accounts.

Annex C: Example Assessment Test Plan – Maturity Level Three

Mitigation Strategy	Control Description	Test ID	Test Description	Test Methodology
Application control	Application control is implemented on workstations and **servers**.	ML3-AC-01	(Servers) A dedicated application control solution is implemented.	Check whether an in-built or third-party application control solution has been implemented.
	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets **and drivers** to an organisation-approved set.	ML3-AC-02	(Servers) The system is only able to execute approved executables.	Attempt to run a non-approved executable in a directory that is not part of an application control path-based rule. E8MVT will attempt to run an exe file within the local AppData temp directory. ACVT will recursively copy an exe file to the file system and attempt to execute it.
		ML3-AC-03	(Servers) The system is only able to execute approved software libraries.	Attempt to run a non-approved software library (DLL) in a directory that is not part of an application control path-based rule. E8MVT will attempt to run a dll file within the local AppData temp directory. ACVT will recursively copy a dll file to the file system and attempt to execute it.
		ML3-AC-04	(Servers) The system is only able to execute approved scripts.	Attempt to run a non-approved software script (vbs, ps1, py) in a directory that is not part of an application control path-based rule. E8MVT will attempt to run multiple script files within the local AppData temp directory. ACVT will recursively copy multiple script files to the file system and attempt to execute them. If the environment includes Python, VBA, or other scripting languages, consider testing additional scripts for these languages.
		ML3-AC-05	(Servers) The system is only able to execute approved installers.	Attempt to run a non-approved installer (msi) in a directory that is not part of an application control path-based rule. E8MVT will attempt to run a MSI file that will install a text file into the local AppData temp directory.
		ML3-AC-06	(Servers) The system is only able to execute approved compiled HTML files.	Attempt to run a non-approved compiled HTML file (CHM) in a directory that is not part of an application control path-based rule. E8MVT will attempt to run a compiled HTML file within the local AppData temp directory.
		ML3-AC-07	(Servers) The system is only able to execute approved HTML applications.	Attempt to run a non-approved HTML application in a directory that is not part of an application control path-based rule. E8MVT will attempt to run a HTML Application file within the local AppData temp directory.
		ML3-AC-08	(Servers) The system is only able to execute approved control panel applets.	Attempt to run a non-approved Control Panel applet in a directory that is not part of an application control path-based rule. E8MVT will attempt to run a Control Panel Applet file within the local AppData temp directory.
		ML3-AC-09	(Workstations & Servers) The system is only able to execute approved drivers.	Attempt to run a non-approved driver in a directory that is not part of an application control path-based rule.
	Microsoft's 'recommended block rules' are implemented.	ML3-AC-10	(Workstations & Servers) The Microsoft recommended Block rules are configured on the system.	Attempt to run a binary that is on the recommended block list such as wmic, mshta or wscript. E8MVT will retrieve the latest version of the block list rules from Microsoft. It will compare each of these rules against those configured on the system and return a failed result if any do not match. This will not consider any rules that are determined to be necessary for business purposes and are risk managed.
	Microsoft's 'recommended driver	ML3-AC-11	(Workstations & Servers) The Microsoft recommended driver Block rules are configured on the system.	Attempt to install a driver that is on the recommended block list. Verify rules for the blocked drivers exist in an application control configuration, and that they are enforced.

	block rules' are implemented.			E8MVT will retrieve the latest version of the block list rules from Microsoft. It will compare each of these rules against those configured on the system and return a failed result if any do not match. This will not consider any rules that are determined to be necessary for business purposes and are risk managed.
	Application control rulesets are validated on an annual or more frequent basis.	ML3-AC-12	The organisational list of allowed applications rules are reviewed for accuracy with current business requirements and threat profiles.	Check that the Application Control owner has a process for reviewing the list of allowed applications on an annual or more frequent basis. Mature organisations will outline the process of assessing threats in applications and what supporting business case details are required from the requesting group. Check that there is evidence that the organisation has enacted the annual application list review within the last 12 months. This evidence will typically exist as support tickets, email correspondence, or threat and risk assessments.
	Allowed and blocked execution events on workstations and **servers** are **centrally** logged.	ML3-AC-13	(Workstations & Servers) Application control event logs are sent to a centralised location.	Verify event logs for each required event are collected at a centralised location. Verify the number of systems logging to this location align with total expected systems (i.e. all systems are logging here).
	Event logs are protected from unauthorised modification and deletion.	ML3-AC-14	Application control event logs are protected from unauthorised modification and deletion.	Verify standard and unauthorised users are unable to modify or delete event logs.
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	ML3-AC-15	Application control event logs are monitored for signs of compromise.	Verify a process is in place to monitor application control event logs for signs of compromise. Verify the information gathered is sufficient to effectively identify compromise. Look for evidence that this process is being followed. This evidence will typically exist as support tickets, email correspondence, or threat and risk assessments.
		ML3-AC-16	The organisation has an example where they investigated or responded to signs of compromise triggered by application control monitoring.	Verify the organisation has responded to a sign of compromise trigged by application control monitoring. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments.
Patch applications	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release**, or within 48 hours if an exploit exists**.	ML3-PA-01	The organisation has an effective process for patching office productivity suites, web browsers, email clients, PDF software and security products within 48 hours, and has an example of where an available exploit has been identified and patched within 48 hours.	Confirm the existence of a list of applications, and where the applications are installed. Ensure a process for identifying vulnerabilities for software in the list is consistently followed. Request evidence of the patching of these applications within 48 hours.
		ML3-PA-02	Office productivity suites, web browsers, email clients, PDF software and security products do not have vulnerabilities older than 48 hours.	Use a vulnerability scanner to identify the listed applications within the organisation's environment, and check that they have been patched against a known exploit. Check the date the application was updated and compare to the date the patch was released. Ensure that the gap between is not greater than 48 hours. E8MVT will perform basic checks of some Microsoft Office applications based on version numbers and file modification dates to determine if the software has been updated recently.
	Applications that are no longer supported by vendors are removed.	ML3-PA-03	The organisation has removed unsupported applications from the environment.	Confirm that the environment does not contain any software that is no longer supported by the vendor.

Configure Microsoft Office macro settings	**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.**	ML3-OM-01	Microsoft Office is configured to only allow Microsoft Office macros to execute from trusted locations. OR Microsoft Office is configured to only allow Microsoft Office macros digitally signed by a trusted publisher to execute. OR Microsoft Office macros are only executed from within a sandbox environment.	Attempt to execute Microsoft Office macros from untrusted locations, and trusted locations if configured. OR Attempt to execute signed and unsigned Microsoft Office macros from untrusted publishers, and trusted publishers if configured. OR Determine if a sandbox solution is in place and effective for Microsoft Office. An example of this would be Application Guard for Office 365.
	Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.	ML3-OM-02	The organisational has a defined standard for validating and accepting Microsoft Office macros in Microsoft Office files before adding them to the trusted location.	Confirm that trusted locations are used by the organisation. If so, check that a process exists for allowing write access to these locations and that users with this level of access are validating that Microsoft Office macros are free of malicious code.
		ML3-OM-03	A user is not able to write a file into locations contained within the trusted locations list.	Get trusted locations for each product from the registry at *HKCU:\software\microsoft\office\<version>\<product>\security\trusted locations* and attempt to write a file into each of these locations. E8MVT will find configured Trusted Locations and attempt to write a file to each location. *Get-ItemProperty -Path "HKCU:\SOFTWARE\policies\microsoft\office\<version>\<product>\security\trusted locations"*
	Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.	ML3-OM-04	Microsoft Office macros signed by an untrusted publisher are unable to execute, and users cannot change configuration or otherwise allow execution.	Attempt to execute Microsoft Office macros in a Microsoft Office file signed by an untrusted publisher. Check the value in the registry to confirm that TCID19092 exists for each product *HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\office\<version>\<product>\disabledcmdbaritemslist*. Check the value is set to 1 at *HKCU:\Software\Microsoft\Office\16.0\Common\TrustCenter\trustbar*. *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\<version>\<product>\" | Select-Object -Property disabledcmdbaritemslist* Example: *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\16.0\word\" | Select-Object -Property disabledcmdbaritemslist* *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\<version>\Common\TrustCenter\" | Select-Object -Property trustbar* Example: *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\16.0\Common\TrustCenter\" | Select-Object -Property trustbar*
	Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.	ML3-OM-05	The organisation has a process for validating the listed of trusted publishers on an annual or more frequent basis.	Confirm that a list of trusted publishers exists and that a process is in place to regularly review this list to allow/remove trusted publishers. Request evidence of an annual validation having taken place.
	Allowed and blocked Microsoft Office macro execution events are **centrally** logged.	ML3-OM-06	Microsoft Office macro execution event logs are sent to a centralised location.	Verify event logs for each required event are collected at a centralised location. Verify the number of systems logging to this location align with total expected systems (i.e. all systems are logging here).
	Event logs are protected from unauthorised	ML3-OM-07	Microsoft Office macro execution event logs are protected from unauthorised modification and deletion.	Verify standard and unauthorised users are unable to modify or delete Microsoft Office macro execution event logs.

	modification and deletion.			
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	ML3-OM-08	Microsoft Office macro execution event logs are monitored for signs of compromise.	Verify a solution or process is in place to monitor the Microsoft Office macro execution event logs for signs of compromise. Check that the environment owner has a process for detecting and handling any signs of compromise relating to Microsoft Office macro execution.
		ML3-OM-09	The organisation has an example where they investigated or responded to signs of compromise triggered by Microsoft Office macro execution monitoring.	Verify the organisation has responded to a sign of compromise trigged by Microsoft Office macro execution monitoring. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments.
User application hardening	Internet Explorer 11 **is disabled or removed**.	ML3-AH-01	The Internet Explorer 11 binary (iexplore.exe) does not exist on the system or is not able to be opened due to an application control policy.	E8MVT will perform a check of the group policy setting to disable Internet Explorer 11. In addition, check that the folder containing Internet Explorer 11 in Program Files (x86) has been removed and that the iexplore.exe binary does not exist on the system. E8MVT will check for the existence of the iexplore.exe binary in *Program Files.Get-ItemProperty -Path "(HCKU/HKLM):\Software\Policies\Microsoft\Internet Explorer\Main\" | Select-Object -Property NotifyDisableIEOptions*. Note, even in Microsoft Windows 11, the *C:\Program Files (x86)\Internet Explorer\iexplore.exe* binary still exists and various methods can be used to open Internet Explorer 11 as a standalone browser. To prevent this from occurring, either the iexplore.exe binary should be removed or an application control block rule is implemented to block its execution.
	.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.	ML3-AH-02	.NET Framework 3.5 has been removed from the system by unselecting it from the list of optional Windows Features.	Select the 'Turn Windows Features on or off' option from the Control Panel and confirm that .NET Framework (includes .NET 2.0 and 3.0) is not selected.
		ML3-AH-03	Older .NET Frameworks are unable to be found in the registry.	Check the registry keys below for the existence of older .NET Frameworks. E8MVT will check this location to determine if older .NET Framework versions exist on the system. *Get-ChildItem -Path "HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP"* *Get-ChildItem -Path "HKLM:\Software\Microsoft\.NETFramework\Policy\"*
	Windows PowerShell 2.0 is disabled or removed.	ML3-AH-04	PowerShell 2.0 and below has been removed from the system and traces of it cannot be found in the registry.	Run the following PowerShell command *Get-ChildItem "HKLM:\SOFTWARE\Microsoft" -Recurse -Include PowerShellEngine* and confirm that version 2.0 is not found in the results. The PowerShell command $PSVersionTable will display a list of supported PowerShell versions. Ensure that 2.0 and below is not part of this list. The command *$PSVersionTable.PSVersion.Major* can be used to confirm the running version. E8MVT will check the described registry key to locate old PowerShell versions. *Get-ChildItem "HKLM:\SOFTWARE\Microsoft\Powershell" -Recurse -Include PowerShellEngine*
		ML3-AH-05	PowerShell cannot be downgraded to version 2.0 or below.	Enter *powershell -Version 2* into a PowerShell prompt to check if the system can be downgraded. The command *$PSVersionTable.PSVersion.Major* can be used to confirm the running version.
	PowerShell is configured to use Constrained Language Mode.	ML3-AH-06	The default configuration for PowerShell on the system is to start in Constrained Language Mode.	Run *$ExecutionContext.SessionState.LanguageMode* in PowerShell to check if ConstrainedLanguage is configured. E8MVT will not run if the system is configured for Constrained Language Mode.
		ML3-AH-07	PowerShell will not allow a user to change to Full Language mode.	Confirm that PowerShell is running in CLM. *Run $ExecutionContext.SessionState.LanguageMode = 'FullLanguage'* in PowerShell. If the mode can change, the test has failed. E8MVT will not run if the system is configured for Constrained Language Mode.

	Blocked PowerShell script execution events are **centrally** logged.	ML3-AH-08	PowerShell script execution event logs are sent to a centralised location.	Verify event logs for each required event are collected at a centralised location. Verify the number of systems logging to this location align with total expected systems (i.e. all systems are logging here).
	Event logs are protected from unauthorised modification and deletion.	ML3-AH-09	PowerShell script execution event logs are protected from unauthorised modification and deletion.	Verify standard and unauthorised users are unable to modify or delete event logs.
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	ML3-AH-10	PowerShell script execution event logs are monitored for signs of compromise.	Verify a solution or process is in place to monitor the PowerShell script execution event logs for signs of compromise. Check that the environment owner has a process for detecting and handling any signs of compromise relating to PowerShell script execution.
		ML3-AH-11	The organisation has an example where they investigated or responded to signs of compromise triggered by PowerShell script execution monitoring.	Verify the organisation has responded to a sign of compromise trigged by PowerShell script execution monitoring. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments.
Restrict administrative privileges	**Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.**	ML3-RA-01	The existing users of systems and applications are provided with the correct level of privilege required to perform their duties.	Review the configured users of systems and applications. Ensure their assigned privileges match their expected duties and role. Query Active Directory using PowerShell commands or tools such as Bloodhound and ADRecon to identify users with more privileges than required in their role. Ensure privileged Active Directory groups such as Domain Administrators have limited members.
	Privileged accounts are prevented from accessing the internet, email and web services.	ML3-RA-02	Service accounts cannot access the internet or web services via a web browser or other mechanism. This might be due to a proxy configuration, system configuration, or another solution.	While logged in as a service account, attempt to browse to an internet website. Review the configuration preventing internet access and attempt to change this as a privileged user not responsible for administering that system.
		ML3-RA-03	Service accounts are not configured with mailboxes and email addresses. Note tests for Maturity Level One already cover internet restrictions for privileged accounts excluding service accounts.	Attempt to open Microsoft Outlook on a system using a service account. Run the following PowerShell command and identify any service accounts in the output. *Get-ADUser -Filter {(admincount -eq 1) -and (emailaddress -like "*") -and (enabled -eq $true)} -Properties EmailAddress | Select samaccountname, emailaddress*
	Just-in-time administration is used for administering systems and applications.	ML3-RA-04	Groups that are identified as having privileged access to systems and applications contain no active users.	Query Active Directory using PowerShell commands or tools such as ADRecon to identify privileged users and groups. Consider some users may currently have Just-in-time access, and ensure they are not permanently members of a privileged group.
		ML3-RA-05	Users that are approved access to privileged administration groups are provided with access for a limited time to fulfil their duties. A Just-in-time administration solution has been successfully deployed and configured.	Review evidence of valid use of this system, such as service requests or support tickets. Look for evidence of this solution being bypassed, such as users in privileged groups for extended periods of time. Ensure the system configuration meets the intent of this control, such as limiting who can receive privileged access.
	Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.	ML3-RA-06	Windows Defender Credential Guard is enabled on the system.	Check the registry setting at *HKLM:\System\CurrentControlSet\Control\LSA* and confirm that LsaCfgFlags is set to 1 or 2. Can also check using the PS command *(Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard).SecurityServicesRunning* and confirming that the result = 1. E8MVT is able to check the registry setting for this control. *Get-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\LSA\" | Select-Object -Property lsacfgflags**
		ML3-RA-07	Windows Defender Remote Credential Guard is enabled on the system.	Check the registry setting at *HKLM:\System\CurrentControlSet\Control\LSA* and confirm that DisableRestrictedAdmin is set to 0.

				E8MVT is able to check the registry setting for this control. *Get-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\LSA\" | Select-Object -Property DisabledRestrictedAdmin*
	Privileged access events are **centrally** logged.	ML3-RA-08	Privileged access event logs are sent to a centralised location.	Verify event logs for each required event are collected at a centralised location. Verify the number of systems logging to this location align with total expected systems (i.e. all systems are logging here).
	Privileged account and group management events are **centrally** logged.	ML3-RA-09	Privileged account and group management event logs are sent to a centralised location.	Verify event logs for each required event are collected at a centralised location. Verify the number of systems logging to this location align with total expected systems (i.e. all systems are logging here).
	Event logs are protected from unauthorised modification and deletion.	ML3-RA-10	Privileged access event logs are protected from unauthorised modification and deletion.	Verify standard and unauthorised users are unable to modify or delete event logs.
		ML3-RA-11	Privileged account and group management event logs are protected from unauthorised modification and deletion.	Verify standard and unauthorised users are unable to modify or delete event logs.
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	ML3-RA-12	Privileged access event logs are monitored for signs of compromise.	Verify a solution or process is in place to monitor the privileged access event logs for signs of compromise. Check that the environment owner has a process for detecting and handling any signs of compromise relating to privileged access.
		ML3-RA-13	The organisation has an example where they investigated or responded to signs of compromise triggered by privileged access monitoring.	Verify the organisation has responded to a sign of compromise trigged by privileged access monitoring. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments.
		ML3-RA-14	Privileged account and group management event logs are monitored for signs of compromise.	Verify a solution or process is in place to monitor the privileged account and group management event logs for signs of compromise. Check that the environment owner has a process for detecting and handling any signs of compromise relating to privileged account and group management.
		ML3-RA-15	The organisation has an example where they investigated or responded to signs of compromise event triggered by privileged account and group management monitoring.	Verify the organisation has responded to a sign of compromise trigged by privileged account and group management monitoring. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments.
Patch operating systems	Patches, updates or other vendor mitigations for 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**.	ML3-PO-01	Operating systems vulnerable to an exploit that has been available for greater than 48 hours are patched or mitigated.	View vulnerability management solution, logon to server to verify patch applied successfully or review mitigation strategy.
	The latest release, or the previous release, of operating systems are used for.	ML3-PO-02	The minimum version of the operating system is the current, or previous release (N-1 version).	Query Active Directory using PowerShell commands or tools such as ADRecon or Bloodhound to identify operating system versions within the environment. Use a vulnerability management solution to scan all systems to record their operating system version.

Multi-factor authentication	**Multi-factor authentication is used to authenticate users of important data repositories.**	ML3-MF-01	The organisation has a list of important data repositories.	Confirm the organisation has a list of important data repositories and this list is regularly checked.
		ML3-MF-02	Data repositories that have been listed as important require MFA to access.	Verify important data repositories are configured to present a MFA challenge. The organisation will determine important / sensitive 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.	ML3-MF-03	The MFA implementation requires the use of a phishing-resistant solution.	Verify that MFA requires a smart card, security key, Windows Hello for Business or any other solution this is resistant to phishing attacks.
	Successful and unsuccessful multi-factor authentication events are **centrally** logged.	ML3-MF-04	MFA event logs are sent to a centralised location.	Verify event logs for each required event are collected at a centralised location. Verify the number of systems logging to this location align with total expected systems (i.e. all systems are logging here).
	Event logs are protected from unauthorised modification and deletion.	ML3-MF-05	MFA event logs are protected from unauthorised modification and deletion.	Verify standard and unauthorised users are unable to modify or delete event logs.
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	ML3-MF-06	MFA event logs are monitored for signs of compromise.	Verify a solution or process is in place to monitor the integrity and validity of MFA event logs.
		ML3-MF-07	The organisation has an example where they investigated or responded to signs of compromise triggered by MFA monitoring.	Verify the organisation has responded to a sign of compromise trigged by MFA monitoring. This evidence will typically exist as support tickets, email correspondence or threat and risk assessments.
Regular backups	Unprivileged accounts cannot access backups belonging to other accounts**, nor their own accounts**.	ML3-RB-01	Unprivileged users are unable to access backups, including their own.	Verify access controls restrict unprivileged users from accessing backup repositories.
	Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts**, nor their own accounts**.	ML3-RB-02	Privileged users (excluding backup administrator accounts) are unable to access backups, including their own.	Verify access controls restrict privileged users (excluding backup administrator accounts) from accessing backup repositories.

	Privileged accounts (**including** backup administrator accounts) are prevented from modifying and deleting backups **during their retention period**.	ML3-RB-03	Privileged users (including backup administrator accounts) are unable to modify and delete backups during their retention period.	Verify access controls restrict the modification and deletion of backups during their retention period to break glass accounts.