Maturity Level One

The focus of this maturity level is malicious actors who are content to simply leverage commodity tradecraft that is widely available in order to gain access to, and likely control of, a system. For example, malicious actors opportunistically using a publicly-available exploit for a vulnerability in an online service which has not been patched, or authenticating to an online 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 launch malicious applications. If user accounts that malicious actors compromise have special privileges they will exploit it. Depending on their intent, malicious actors may also destroy data (including backups).

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.
	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.
	Online services that are no longer supported by vendors are removed.
	Office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.
Patch operating systems	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.

Mitigation Strategy	Description
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.
	Operating systems that are no longer supported by vendors are replaced.
Multi-factor authentication	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.
	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.
	Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation's non-sensitive data.
	Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.
	Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.
	Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.
	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.
Restrict administrative privileges	Requests for privileged access to systems, applications and data repositories are validated when first requested.
	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.
	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.

Mitigation Strategy	Description
	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.
	Privileged users use separate privileged and unprivileged operating environments.
	Unprivileged user accounts cannot logon to privileged operating environments.
	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.
Application control	Application control is implemented on workstations.
	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.
	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.
Restrict Microsoft Office macros	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.
	Microsoft Office macros in files originating from the internet are blocked.
	Microsoft Office macro antivirus scanning is enabled.
	Microsoft Office macro security settings cannot be changed by users.
User application hardening	Internet Explorer 11 is disabled or removed.
	Web browsers do not process Java from the internet.
	Web browsers do not process web advertisements from the internet.
	Web browser security settings cannot be changed by users.
Regular backups	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.
	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.
	Backups of data, applications and settings are retained in a secure and resilient manner.
	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.
	Unprivileged user accounts cannot access backups belonging to other user accounts.
	Unprivileged user accounts are prevented from modifying and deleting backups.

MATURITY LEVEL ONE – DEEP DIVE

Patch applications

Context

Most vendors of online services and applications regularly release updated versions to fix vulnerabilities. As such, online services and applications can be compared to the latest versions available from vendors to determine whether existing versions are the latest, and if not, how long ago updates were made available 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 the criticality of vulnerabilities and whether working exploits exist or not.

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 the automated method of asset discovery being used 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 the 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.

Control	Assessment Guidance (ordered by effectiveness)
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 online 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 online services matches the list of online services that are known to be used.
	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 online services matches the list of online services that are known to be used.
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.	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 applications includes the list of applications that should have been scanned.
	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 applications includes the list of applications that should have been scanned.
Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	A network-based vulnerability scanner can be used to identify online services, their versions and install dates. This can then be reviewed alongside the release date of patches to determine whether patching timeframes have been met. There are several free tools available to support the assessment of this control, including ASD's Essential Eight Maturity Verification Tool (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 configuration changes.
	If a network-based vulnerability scanner cannot be used, screenshots of versions for online services can be requested. This allows for manual checking against the latest versions available from vendors. Alternatively, a list of online services may be requested (noting that malicious actors often exploit

Control	Assessment Guidance (ordered by effectiveness)
	vulnerabilities in online services that the system owner may have forgotten about or have been installed without the system owner's knowledge).
Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	A network-based vulnerability scanner can be used to identify online services, their versions and install dates. This can then be reviewed alongside the release date of patches to determine whether patching timeframes have been met. 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 configuration changes.
	If a network-based vulnerability scanner cannot be used, screenshots of versions for online services can be requested. This allows for manual checking against the latest versions available from vendors. Alternatively, a list of online services may be requested (noting that malicious actors often exploit vulnerabilities in online services that the system owner may have forgotten about or that were installed without their 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 two weeks of release.	A vulnerability scanner can be used to assess applications, their versions and install dates. The above output should be reviewed alongside the release date for each application to determine whether patching timeframes have 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, 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 'Programs and Features' to ensure no applications are missed.

Control	Assessment Guidance (ordered by effectiveness)
	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 should be reviewed alongside the release date for each application to determine whether patching timeframe have 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.
Online services that are no longer supported by vendors are removed.	A vulnerability scanner can be used to assess online services and whether they are end of life.
	Request a demonstration that shows the versions of online service being used. This allows for manual checking against a list of supported versions.
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 applications being used. This allows for manual checking against a 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 Microsoft Windows. If Adobe Flash Player was installed manually from another source, it will not be removed by this hotfix.

Patch operating systems

Context

Operating system vendors regularly publish updates to mitigate vulnerabilities. In addition, unsupported operating systems of internet-facing servers and internet-facing network devices are often common targets for malicious actors.

While operating systems of workstations, non-internet-facing servers and non-internet-facing network devices 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 tradecraft and targeting 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 the criticality of vulnerabilities and whether working exploits exist or not.

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 the automated method of asset discovery being used 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.

Control	Assessment Guidance (ordered by effectiveness)
	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 the 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 servers and internet-facing 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.
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.	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 servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	A network-based vulnerability scanner 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 patching timeframes have been met. 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

Control	Assessment Guidance (ordered by effectiveness)
	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, are stuck or 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 for vulnerabilities that have been identified as critical by the vendor, or are currently being exploited, to determine whether all applicable hotfixes have been applied or not.
Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	A network-based vulnerability scanner 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 patching timeframes have been met. 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, are stuck or 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 for vulnerabilities to determine whether all applicable hotfixes have been applied or not.
Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-	A network-based vulnerability scanner can be used to identify operating systems, their versions and install dates. This can

Control	Assessment Guidance (ordered by effectiveness)
internet-facing servers and non-internet-facing network devices are applied within one month of release.	then be reviewed alongside the release date of patches to determine whether patching timeframes have been met. 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, are stuck or 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 for vulnerabilities to determine whether all applicable hotfixes have been applied or not.
Operating systems that are no longer supported by vendors are replaced.	A vulnerability scanner can be used to identify 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 an operating system. Request a screenshot of the output of running this command for workstations and servers (assuming a Standard Operating Environment [SOE] is used for workstations). The versions output can then be checked against Microsoft release information to determine whether the operating systems are still supported or not. For Linux workstations and servers, the 'cat /etc/os-release' command can be run to determine the version of an operating system. Request a screenshot of the output of running this

Control	Assessment Guidance (ordered by effectiveness)
	command for workstations and servers (assuming a SOE is used for workstations). The versions output can then be checked against release information for Linux distributions being used to determine whether they are still supported 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, online service or application. When implemented correctly, multi-factor authentication can make it significantly more difficult for malicious actors to steal and abuse legitimate credentials as it is not as susceptible to brute force attacks that target traditional single-factor authentication methods based on memorised secrets (e.g. personal identification numbers [PINs], passwords and passphrases).

At this maturity level, the implementation of multi-factor authentication should focus on online services. In addition, the authentication factors that can be used, and in what combination, are restricted to avoid weaker multi-factor authentication 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 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.

Finally, at this maturity level, organisations may choose to implement multi-factor authentication solutions that are phishing-resistant, such as security keys, smart cards or passkeys, if they intend to eventually implement requirements for 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)**
Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.	Attempt to logon to an organisation's own online services that users access. Typically, the logon screen will show a request for two or more authentication factors, such as a password and an OTP. Note, in some cases an online 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. As such, assessors should determine if any additional authentication portals are exposed to the internet.
Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.	Attempt to logon to third-party online services that users 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 to authenticate users to third-party online services that process, store or communicate their organisation's non-sensitive data.	Attempt to logon to third-party online services that users 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 used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.	Attempt to logon to an organisation's own online customer services that users access. In cases where multi-factor authentication is not used, confirm that such functionality is not offered.
Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.	Attempt to logon to third-party online customer services that users 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 used to authenticate customers to online customer services that process, store or communicate sensitive customer data.	Attempt to logon to online customer services that customers (e.g. citizens) access. Discuss whether multi-factor authentication is setup as part of user account creation or whether customers need to set it up themselves after initial user account creation.

Control	Assessment Guidance (ordered by effectiveness)
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 and customers. Note, multiple different forms of multi-factor authentication may exist depending on the number of different systems and online services that are being authenticated 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 online 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, smart card or passkey 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.

Restrict administrative privileges

Context

Policies, processes and procedures for managing privileged access to systems, applications and data repositories should be documented and enforced within organisational workflows. In doing so, privileged access to systems, applications and data repositories should be requested via a form, service desk ticket or email from users, and require approval from a supervisor or either an application owner or data repository owner, to maintain a record of all such requests. System owners should also maintain a list of all applications and data repositories on their system that require privileged access.

Privileged user accounts are often targeted by malicious actors for their greater control over, and access to, organisational resources. For this reason, privileged user accounts should not have access to the internet, email and web services except in specific circumstances in which such access is explicitly authorised and strictly limited to only what is required for such user accounts to undertake their duties.

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 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)**
Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.	Discuss whether privileged users are assigned separate unprivileged and privileged user accounts or whether they use a single privileged user account for all their duties.
Requests for privileged access to systems, applications and data repositories are validated when first requested.	Request copies of forms, support tickets or emails provided by users requesting privileged access to systems, applications or data repositories along with the support of their supervisor or either an application owner or data repository owner. This can then be compared to screenshots of user accounts with privileged access to determine if there are any discrepancies.
Privileged user accounts (excluding those explicitly authorised to access online services) 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 user accounts. In addition, run the below PowerShell command to check if privileged user 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 user accounts that may be missed when utilising PowerShell alone. Note, some privileged user accounts, such as those used to manage cloud services, may have access to the internet. In such cases, determine whether the user accounts have been explicitly authorised to do so via a formal process.
Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.	In cases where privileged user accounts have been explicitly authorised to access online services, such as for the management of cloud services, determine to what extent they are limited from accessing all other online services over the internet.
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

Control	Assessment Guidance (ordered by effectiveness)
	this can be implemented beyond that separate privileged and unprivileged operating environments have been implemented.
Unprivileged user accounts cannot logon to privileged operating environments.	Attempt to logon to a privileged operating environment using a standard user account. BloodHound can be used to assess whether any unprivileged user accounts have connected to privileged operating environments by looking for cached credentials.
Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Request a demonstration of a privileged user account attempting to logon to an unprivileged operating environment. Note, this test should be done using a privileged user account set up specifically for this purpose. The privileged user account should then be removed immediately after testing is complete. BloodHound can be used to assess whether any privileged user accounts have connected to unprivileged operating environments by looking for cached credentials.

Application control

Context

At this maturity level, the use of an application control solution is required. 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).

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 depending on the application control solution implemented, it may not support compiled Hypertext Markup Language (HTML) (.chm files), HTML applications (.hta files) and control panel applets (.cpl files).

When conducting application control assessments, paths for standard user profiles and temporary folders used by operating systems, web browsers and email clients can include those listed 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 benign executable files 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.

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.	Check whether an application control solution has been implemented on workstations.
Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	Check whether the application control solution implementation covers, at a minimum, user profiles and temporary folders used by the operating system, web browsers and email clients. Note, this is only applicable to implementations reliant on path-based rules as the use of publisher-based rules and hash-based rules automatically apply across the entire system.
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 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 E8MVT and Application Control Verification Tool, 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 only willing to allow the use of trusted Microsoft tools, the SysInternals AccessChk application can be used to generate the output of

Control	Assessment Guidance (ordered by effectiveness)
	folder permissions, noting this is only relevant to path-based implementations. 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 implementation is used, screenshots of the 'effective access' permissions for specified folders can be requested. This, however, has limitations as 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.

Restrict Microsoft Office macros

Context

All users should be denied the ability to execute Microsoft Office macros by default unless they have a demonstrated business requirement for their use. In such cases, users should still be restricted to using macros in only the specific applications required for their duties. 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 software 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 in order to identify Microsoft Office macro settings applied via group policy settings. 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. Furthermore, the 'VBA Macro Notification Settings' setting should be 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 Message 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 a demonstration showing Trust Center macro settings (File – Options – Trust Center – Trust Center Settings – Macro Settings) for both users that are not allowed to run Microsoft Office macros and for users with a demonstrated business requirement to do so. For users that are allowed to run Microsoft Office macros, request documentation that outlines their business requirement. Consider determining the percentage of the organisation's user base that have been granted approval to run Microsoft Office macros (to ensure approval for Microsoft Office macro use is not overly permissive). For the assessment of Microsoft Office macro security, identify what setting is selected for 'macro settings'. For most users, the 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,

Control	Assessment Guidance (ordered by effectiveness)
	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 again. 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 2016\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.

Control	Assessment Guidance (ordered by effectiveness)
	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

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. Therefore, Internet Explorer 11 should be disabled or removed from systems and Microsoft Edge, or another modern web browser, should be used instead.

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.

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)
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 looking 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'.
Web browsers do not process Java from the internet.	A list of web browsers installed on the 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, compensating controls should be assessed to determine whether, for example, 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 the Can You Block It? website 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.
Web browser security settings cannot be changed by users.	Check the security settings for each web browser installed on the system. Identify if settings are greyed out (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

Control	Assessment Guidance (ordered by effectiveness)
	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.

Regular backups

Context

Backups of data, applications and settings should be performed and retained in accordance with business criticality and business continuity requirements for an organisation. In doing so, it is important that restoration of data, applications and settings from backups be tested as part of regular (at least annually) disaster recovery exercises and not left until 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 also worth noting, at this maturity level, that privileged user accounts may still be able to access the backups of any user.

While unprivileged user 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 ransomware running with the privileges of an unprivileged user should be blocked from overwriting or deleting backups. Note, malicious actors escalating privileges to privileged user accounts, or backup administrator accounts, to overwrite backups is 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 data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.	Discuss backup and retention frequencies specified for the system, including the business criticality of different data sets and applications. Request a copy of the business continuity plan to check that the frequency and retention periods for backups have been documented.
Backups of data, applications and 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 data is being backed up out of sync to associated applications and settings then it will hamper restoration efforts and data may be lost.

Control	Assessment Guidance (ordered by effectiveness)
Backups of data, applications and 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 IT equipment failures?
Restoration of data, applications and 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 data, applications and 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, for this control, business-as-usual recovery of user files is not sufficient. Rather, the intent of this control is the restoration of a significant component of a system as part of a scheduled exercise.
Unprivileged user accounts cannot access backups belonging to other user accounts.	Review the backup solution and Active Directory security groups to determine who has access to backups.
	Check whether unprivileged user 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 user accounts are prevented from modifying and deleting backups.	Check whether unprivileged user 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.