Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Essential Eight Assessment Process Guide

First published: November 2022
Last updated: August 2024

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 2023 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 tradecraft (i.e. tools, tactics, techniques and procedures) and targeting. 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.

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 tradecraft and targeting 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 a test 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 or controls being discussing during interviews with personnel administering or managing system security).

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:

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

It is important that assessors do not allow risk acceptance as a justification for not implementing an entire mitigation strategy (e.g. a system owner has risk accepted not implementing application control or multi-factor authentication). In these cases, 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 have not been 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 Microsoft 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 to reduce the identified 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 had been put 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 been precluded from reaching their target maturity level.

Example: During an internal review, an organisation identified a cloud service that did not have 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. As such, the organisation chose 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 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 (i.e. assessment boundary) 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:

- assessment scope (i.e. assessment boundary) and assessment approach (see further detail below)
- access to unprivileged and privileged user accounts, devices, documentation, personnel, and facilities
- any approvals required to run scripts and tools on the system (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 service providers manage 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.

Stage 2: Determination of assessment scope and approach

Determine assessment scope

In determining the assessment scope (i.e. assessment boundary), 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.

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 of assessing a reasonable representative sample 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 seek 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 maturity level, along with relevant assessment considerations. Guidance on determining the effectiveness of 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 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 accounts that malicious actors compromise have special privileges they will exploit it. Depending on their intent, malicious actors may also destroy data (including backups).

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.
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 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. *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.
	A vulnerability scanner can be used to assess online services and whether they are end of life.
Online services that are no longer supported by vendors are removed.	Request a demonstration that shows the versions of online service being used. This allows for manual checking against a list of supported versions.
	A vulnerability scanner can be used to assess applications and whether they are end of life.

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.	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. 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 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-internet-facing servers and non-internet-facing network devices are applied within one month of release.	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.
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 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 account creation or whether customers need to set it up themselves after initial account creation.

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 accounts are often targeted by malicious actors for their greater control over, and access to, organisational resources. For this reason, privileged 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 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 account to be used solely for duties requiring privileged access.	Discuss whether privileged users are assigned separate unprivileged and privileged accounts or whether they use a single privileged 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 accounts with privileged access to determine if there are any discrepancies.
Privileged 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 accounts. In addition, 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 accounts that may be missed when utilising PowerShell alone. Note, some privileged accounts, such as those used to manage cloud services, may have access to the internet. In such cases, determine whether the accounts have been explicitly authorised to do so via a formal process.
Privileged 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 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 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 operating environment using a standard user account. BloodHound can be used to assess whether any unprivileged accounts have connected to privileged operating 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 an unprivileged operating environment. Note, 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 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 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, 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.
	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 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 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 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 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.
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 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 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 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 in order 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 launch malicious applications. If accounts that malicious actors compromise have special privileges they will exploit it, otherwise they will seek accounts with special privileges. Depending on their intent, malicious actors may also destroy all data (including backups) accessible to an account with special privileges.

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.

Patch applications

Context

At this maturity level, vulnerability scanning and patching requirements for additional applications is introduced.

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 fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	Use the guidance provided in Maturity Level One of this guide but apply it to applications other than office productivity suites, web browsers and their extensions, email clients, Portable Document Format (PDF) software, and security products using the identified timeframe.
Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.	Use the guidance provided in Maturity Level One of this guide but apply it to applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products using the identified timeframe.

Patch operating systems

Context

At this maturity level, no assessment is required as the controls are the same as those for Maturity Level One.

Multi-factor authentication

Context

At this maturity level, a requirement for users logging onto systems (e.g. their workstations) to use multi-factor authentication is introduced. Furthermore, all multi-factor authentication, with the exception of customers authenticating to online customer services, should be phishing-resistant.

At this maturity level, event logs for multi-factor authentication events should be centrally collected and analysed as often the lack of sufficient logging can impact the ability of an organisation to identify or determine the extent of a cyber security 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)
Multi-factor authentication is used to authenticate privileged users of systems.	Observe a privileged user authenticating to a workstation. Check whether they are required to use multi-factor authentication. Alternatively, request evidence of the logon screen for a privileged user. The logon screen should show multiple authentication methods being requested.
Multi-factor authentication is used to authenticate unprivileged users of systems.	Observe an unprivileged user authenticating to a workstation. Check whether they are required to use multi-factor authentication. Alternatively, request evidence of the logon screen for an unprivileged user. The logon screen should show multiple authentication methods being requested.
Multi-factor authentication used for authenticating users of online services is phishing-resistant.	Observe both unprivileged and privileged users authenticating to their organisation's online services that process, store or communicate their organisation's sensitive data, as well as third-party online services that process, store or communicate their organisation's sensitive or non-sensitive data. Check whether they are required to use a phishing-resistant form of multi-factor authentication, such as a security key, smart card or passkey.
Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.	Observe security settings for a customer's account relating to any of the organisation's online customer services that process, store or communicate sensitive customer data, as well as any third-party online customer services that process, store or communicate sensitive customer data. Check whether there is the ability to configure authentication settings to use a phishing-resistant form of multi-factor authentication, such as a security key, smart card or passkey.
Multi-factor authentication used for authenticating users of systems is phishing-resistant.	Observe an unprivileged and privileged user authenticating to a workstation. Check whether they are required to use a phishing-resistant form of multi-factor authentication, such as a security key, smart card or passkey. Observe a privileged user authenticating to a server. Check whether they are required to use a phishing-resistant form of multi-factor authentication, such as a security key, smart card, or passkey.
Successful and unsuccessful multi-factor authentication events are centrally 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'. In addition, determine if these event logs are being centrally stored.
	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.

Event logs are protected from unauthorised modification and deletion.	Discuss whether a SIEM, or equivalent solution, is used to protect event logs from unauthorised modification and deletion.
Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Discuss whether security operations centre (SOC) analysts monitor event logs for signs of compromise (i.e. security events).
Cyber security events are analysed in a timely manner to identify cyber security incidents.	Discuss how security events are analysed by SOC analysts to determine whether a cyber security incident has occurred. Reviewing an organisation's cyber security incident register may also provide evidence of the analysis of cyber security events in order to identify cyber security incidents.
Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.	Discuss to what extent cyber security incidents are reported to an organisation's Chief Information Security Officer, or one of their delegates, after they occur or are discovered. Determine whether typical reporting timeframes are reasonable (i.e. is reporting occurring as soon as possible).
Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Discuss to what extent cyber security incidents are reported to ASD after they occur or are discovered. Determine whether typical reporting timeframes are reasonable (i.e. is reporting occurring as soon as possible).
Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Request access to a copy of the cyber security incident response plan for the system. Discuss to what extent it is followed following a cyber security incident.

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 can 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.

For this maturity level, privileged operating environments should 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 static component and a dynamic component (e.g. incorporating 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 (e.g. if machine names are the same as their asset identifier). Ideally, an approach that ensures break glass accounts, local administrator accounts and service accounts are unique, unpredictable and managed should be used. For example, Microsoft's Local Administrator Password Solution.

At this maturity level, event logs relating to the use of, and changes to, privileged accounts should be centrally collected and analysed as often the lack of sufficient logging can impact the ability of an organisation to identify or determine the extent of a cyber security 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, applications and data repositories is disabled after 12 months unless revalidated.	Check whether an account expiry date is set for privileged accounts in Active Directory under account profiles and whether a mechanism exists to disable such 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 disabled after 45 days of inactivity.	Microsoft provides guidance on the use of PowerShell in order 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 logon 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 break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.	Discuss how break glass accounts, local administrator accounts and service accounts are managed. Confirm that 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 Microsoft Windows operating system, which changes the password every 30 days.
Privileged access events are centrally 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'. Furthermore, 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'. Finally, determine if these event logs are being centrally stored.
Privileged account and group management events are centrally logged.	Leveraging related Windows Event IDs, check whether changes to privileged accounts and groups are logged. In addition, determine if these event logs are being centrally stored. More information on security operations for privileged accounts in Active Directory, including related Windows Event IDs, is available from Microsoft.

	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'.
Event logs are protected from unauthorised modification and deletion.	Discuss whether a SIEM, or equivalent solution, is used to protect event logs from unauthorised modification and deletion.
Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).
Cyber security events are analysed in a timely manner to identify cyber security incidents.	Discuss how security events are analysed by SOC analysts to determine whether a cyber security incident has occurred. Reviewing an organisation's cyber security incident register may also provide evidence of the analysis of cyber security events in order to identify cyber security incidents.
Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.	Discuss to what extent cyber security incidents are reported to an organisation's Chief Information Security Officer, or one of their delegates, after they occur or are discovered. Determine whether typical reporting timeframes are reasonable (i.e. is reporting occurring as soon as possible).
Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Discuss to what extent cyber security incidents are reported to ASD after they occur or are discovered. Determine whether typical reporting timeframes are reasonable (i.e. is reporting occurring as soon as possible).
Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Request access to a copy of the cyber security incident response plan for the system. Discuss to what extent it is followed following a cyber security incident.

Application control

Context

At this maturity level, a requirement is introduced relating to the use of application control for internet-facing servers. In addition, any path-based implementations should provide coverage for all locations on disk and Microsoft's recommended application blocklist should be implemented to mitigate malicious actors using living off the land techniques.

Furthermore, when implementing an application control solution, the application control ruleset may, over time, become unfit for purpose if it is not regular reviewed and validated for its correctness and ongoing suitability. The failure to regularly review application control results can lead to several scenarios, such as exploitable applications or drivers remaining approved for a system, vendor code-signing certificates that have compromised remaining authorised, or system administrators introducing exceptions to 'get things working' or troubleshoot but failing to remove the workarounds afterwards. Each of these scenarios are real, have been observed during assessments and introduce additional vulnerabilities for a system that may be exploited by malicious actors.

The majority of application control solutions will have a form of logging. As such, event logs for application control solutions should be centrally collected and analysed as often the lack of sufficient logging can impact the ability of an organisation to identify or determine the extent of a cyber security 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 internet-facing servers.	Check whether an application control solution has been implemented on internet-facing servers.
Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.	Use the guidance provided in Maturity Level One of this guide but apply it to all other locations on disk.
Microsoft's recommended application blocklist is implemented.	Request a copy of application control rulesets. Check whether Microsoft's recommended application blocklist has 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 the addition or removal of applications.

Allowed and blocked application control events are centrally logged.	Ask whether logging is available for the application control solution 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. In addition, determine if these event logs are being centrally stored.
Event logs are protected from unauthorised modification and deletion.	Discuss whether a SIEM, or equivalent solution, is used to protect event logs from unauthorised modification and deletion.
Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).
Cyber security events are analysed in a timely manner to identify cyber security incidents.	Discuss how security events are analysed by SOC analysts to determine whether a cyber security incident has occurred. Reviewing an organisation's cyber security incident register may also provide evidence of the analysis of cyber security events in order to identify cyber security incidents.
Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.	Discuss to what extent cyber security incidents are reported to an organisation's Chief Information Security Officer, or one of their delegates, after they occur or are discovered. Determine whether typical reporting timeframes are reasonable (i.e. is reporting occurring as soon as possible).
Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Discuss to what extent cyber security incidents are reported to ASD after they occur or are discovered. Determine whether typical reporting timeframes are reasonable (i.e. is reporting occurring as soon as possible).
Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Request access to a copy of the cyber security incident response plan for the system. Discuss to what extent it is followed following a cyber security incident.

Restrict Microsoft Office macros

Context

At this maturity level, a 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.

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.

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 packages. This maturity level requires Microsoft Office to be configured to prevent activation of these packages.

The implementation of ASD and vendor hardening guidance can assist in reducing the attack surface of applications. This is particularly important for applications that are commonly targeted by malicious actors such as web browsers, office productivity suites and PDF software. In cases where ASD hardening guidance and vendor hardening guidance conflict, the most restrictive guidance should take precedence.

At this maturity level, event logs for PowerShell should be centrally collected and analysed as often the lack of sufficient logging can impact the ability of an organisation to identify or determine the extent of a cyber security 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)
Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	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. 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 (Windows)*.
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 Object Linking and Embedding 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)'.

Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	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. ASD 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.
Office productivity suite 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 ASR 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 file, change the view to show all files, right click on an .exe file and select Open. The ASR rule if implemented will block this. 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).
PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Generally, hardening guidance for PDF software can be configured via registry settings. This will be included as part of any RSoP reports. 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.
PowerShell module logging, script block logging and transcription events are centrally logged.	ASD's E8MVT can assist in determining the implementation of this control. Within the RSoP report, look for the 'Turn on Module Logging', 'Turn on PowerShell Script Block Logging' and 'Turn on PowerShell Transcription' settings at 'Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell'. They should all be enabled. In addition, module logging should ideally be configured to log all modules (i.e. '*'), although an organisation may tailor this setting. Finally, determine if these event logs are being centrally stored.

Command line process creation events are centrally logged.	ASD's E8MVT can assist in determining the implementation of this control.
	Within the RSoP report, look for the 'Audit Process Creation' setting at 'Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\'. It should be enabled with a value of 'Success'. In addition, look for the 'Include command line in process creation events' setting at 'Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation'. It should be enabled. Finally, determine if these event logs are being centrally stored.
Event logs are protected from unauthorised modification and deletion.	Discuss whether a SIEM, or equivalent solution, is used to protect event logs from unauthorised modification and deletion.
Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).
Cyber security events are analysed in a timely manner to identify cyber security incidents.	Discuss how security events are analysed by SOC analysts to determine whether a cyber security incident has occurred. Reviewing an organisation's cyber security incident register may also provide evidence of the analysis of cyber security events in order to identify cyber security incidents.
Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.	Discuss to what extent cyber security incidents are reported to an organisation's Chief Information Security Officer, or one of their delegates, after they occur or are discovered. Determine whether typical reporting timeframes are reasonable (i.e. is reporting occurring as soon as possible).
Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Discuss to what extent cyber security incidents are reported to ASD after they occur or are discovered. Determine whether typical reporting timeframes are reasonable (i.e. is reporting occurring as soon as possible).
Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Request access to a copy of the cyber security incident response plan for the system. Discuss to what extent it is followed following a cyber security incident.

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 but apply the more restrictive 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 but apply the more restrictive 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 software 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, malicious actors may be more focused on particular targets and, more importantly, are willing and able to invest some effort into circumventing the idiosyncrasies and particular policy and technical controls implemented by their targets. For example, this includes socially engineering a user to not only open a malicious document but also to unknowingly assist in bypassing controls. This can also include circumventing stronger multi-factor authentication by stealing authentication token values to impersonate a user. Once a foothold is gained on a system, malicious actors will 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.

Patch applications

Context

At this maturity level, patches, updates or other vendor mitigations should be applied within 48 hours for office productivity suites, web browsers and their extensions, email clients, PDF software, and security products when vulnerabilities are assessed as critical by vendors or when working exploits exist. In addition, all applications that are no longer supported by vendors should be removed from systems.

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 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Use the relevant guidance provided in Maturity Level One of this guide but apply 48 hour timeframes when vulnerabilities are assessed as critical by vendors or when working exploits exist.
Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Use the relevant guidance provided in Maturity Level One of this guide when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

Applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	Use the relevant guidance provided in Maturity Level One of this guide and extend it to all applications.

Patch operating systems

Context

At this maturity level, patches, updates or other vendor mitigations should be applied within 48 hours for operating systems of workstations, servers and network devices when vulnerabilities are assessed as critical by vendors or when working exploits exist. In addition, vulnerabilities in drivers and firmware should be mitigated at this maturity level.

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 of operating systems 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 other operating systems 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)
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers.	Use the relevant guidance provided in Maturity Level One of this guide but apply vulnerability scanning activities to drivers.
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware.	Use the relevant guidance provided in Maturity Level One of this guide but apply vulnerability scanning activities to firmware.

Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Use the relevant guidance provided in Maturity Level One of this guide but apply 48 hour timeframes when vulnerabilities are assessed as critical by vendors or when working exploits exist.
Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Use the relevant guidance provided in Maturity Level One of this guide when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Use the relevant guidance provided in Maturity Level One of this guide and apply 48 hour timeframes when vulnerabilities are assessed as critical by vendors or when working exploits exist.
Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Use the relevant guidance provided in Maturity Level One of this guide when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.	Use the relevant guidance provided in Maturity Level One of this guide and apply 48 hour timeframes when vulnerabilities are assessed as critical by vendors or when working exploits exist.
Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Use the relevant guidance provided in Maturity Level One of this guide when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
The latest release, or the previous release, of operating systems are used.	A network-based vulnerability scanner 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 this command for servers and workstations (assuming a SOE is used for workstations). For Linux workstations and servers, the 'cat /etc/os-release' command can be run to determine the version of the operating system. Request a screenshot of the output of running this command for servers and workstations (assuming a SOE is used for workstations). This version can then be checked against release information for the Linux distribution being used to determine whether it is a supported version or not.

Multi-factor authentication

Context

At this maturity level, users of data repositories should be using phishing-resistant multi-factor authentication. In addition, customers of online customer services should be using phishing-resistant multi-factor authentication, rather than just being offered it as an option.

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 data repositories.	Request a list of 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 used for authenticating customers of online customer services is phishing-resistant.	Observe a customer account authenticating to any of the organisation's online customer services that process, store or communicate sensitive customer data, as well as any third-party online customer services that process, store or communicate sensitive customer data. Check whether they are required to use a phishing-resistant form of multi-factor authentication, such as a security key, smart card or passkey.
Multi-factor authentication used for authenticating users of data repositories is phishing-resistant.	Observe both unprivileged and privileged users authenticating to a data repository. Check whether they are required to use a phishing-resistant form of multi-factor authentication, such as a security key, smart card or passkey.
Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).
Event logs from workstations are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).

Restrict administrative privileges

Context

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

While lower maturity levels required the use of privileged operating environments for administrative activities, they did not require Secure Admin Workstations (SAWs) to be implemented for such environments. However, at this maturity level, a concerted effort should be made to apply the principles associated with SAWs to such environments to ensure that their attack surface is reduced as much as possible. This includes hardening operating systems, including removing all unnecessary functionality. Note, this does not necessarily require separate physical machines to be used for privileged operating environments.

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. Local Security Authority protection functionality and Credential Guard are designed to assist in protecting this process. Remote Credential Guard provides a similar functionality for remote access. In addition, memory integrity helps protect the overall integrity of systems.

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, applications and data repositories 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.
Secure Admin Workstations are used in the performance of administrative activities.	Consider the extent to which the principles associated with SAWs have been applied to privileged operating environments. This includes whether ASD hardening guidance and vendor hardening guidance for operating systems has been applied. Furthermore, determine if a concerted effort has been made to reduce the attack surface of such environments as much as possible. Note, this does not necessarily require separate physical machines to be used for privileged operating environments.
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 this maturity level. Given the complex nature of JIT PAM, it will become apparent from discussions with system administrators 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.
Memory integrity functionality is 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 'Virtualization Based Protection of Code Integrity: Enabled with UEFI lock'.
Local Security Authority protection functionality is enabled.	Within the RSoP report, look for the 'Configure LSASS to run as a protected process' setting at 'Computer Configuration\Policies\Administrative Templates\System\Local Security Authority\'. It should be enabled with a value of 'Configure LSA to run as a protected process: Enabled with UEFI lock'.
Credential Guard functionality is 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'.

Remote Credential Guard functionality is enabled.	Within the RSoP report, 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'.
Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).
Event logs from workstations are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).

Application control

Context

At this maturity level, a requirement is introduced relating to the use of application control for non-internet-facing servers. In addition, the scope of application control implementations is expanded to include drivers. Note, while Microsoft AppLocker does not currently support the control of drivers, Windows Defender Application Control does. However, Microsoft AppLocker can be used if Microsoft's vulnerable driver blocklist is also enforced via Microsoft Window's memory integrity functionality, assuming an organisation is willing to accept the risk of all other drivers being able to execute.

Microsoft maintains a list of vulnerable drivers that have been discovered by security researchers. Implementing Microsoft's vulnerable driver blocklist can help to provide protection from malicious actors that would have sought to use these against an otherwise robust application control implementation in order to gain access to a system.

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 non-internet-facing servers.	Check whether an application control solution has been implemented on non-internet-facing servers.
Application control restricts the execution of 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 vulnerable driver blocklist is implemented.	Check whether memory integrity has been enabled via the Windows Security app as this will automatically enforce Microsoft's vulnerable driver blocklist.
	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 drivers. If driver rules are included, check whether Microsoft's vulnerable driver blocklist has been specified.
Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).
Event logs from workstations are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).

Restrict Microsoft Office macros

Context

Disabling the use of Microsoft Office macros represents an optimal security outcome, however, some users will have a demonstrated 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 using V3 signatures.

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 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 and validate the list on a regular basis for its correctness and 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 using V3 signatures, even if already signed by a third party. While introducing additional overhead, this mitigates the risk of potentially 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.
Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations.	Identify users that are responsible for the management of Microsoft Office macros. Discuss with them the processes and procedures that are used to check whether Microsoft Office macros are free of malicious code before they are either digitally signed to placed within Trusted Locations.
Only privileged users responsible for checking that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.	For each Trusted Location that is specified, review the effective file system permissions for that location. If able to, review file system permissions themselves rather than requesting a screenshot. Check the total number of users who are in user groups that have the relevant file system permissions to make changes to content in Trusted Locations.
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 2016\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 macros digitally signed by signatures other than V3 signatures cannot be enabled via the Message Bar or Backstage View.	Within the RSoP report, look for the 'Only trust VBA macros that use V3 signatures' setting at 'User Configuration\Policies\Administration Templates\Microsoft Office 2016\Security Settings\Trust Centre\'. It should be enabled.
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 validated, including what mechanisms are used to identify when/if these need to be removed due to compromise by malicious actors as part of cyber supply chain attacks.

User application hardening

Context

.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. 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)
.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'.
Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).
Event logs from workstations are analysed in a timely manner to detect cyber security events.	Discuss whether SOC analysts monitor event logs for signs of compromise (i.e. security events).

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 control over which accounts can access backups, and to what extent, progressively limits the damage that may be caused by a ransomware attack.

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 their own backups.	Use the guidance provided in Maturity Level One of this guide but apply the more restrictive access control requirements. Specifically, unprivileged accounts should no longer be able to access their own backups.

Privileged accounts (excluding backup administrator accounts) cannot access their own backups.	Use the guidance provided in Maturity Level One of this guide but apply the more restrictive 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.
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 but apply the more restrictive 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 and 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).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate