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 user accounts that malicious actors compromise have special privileges they will exploit it, otherwise they will seek user accounts with special privileges. Depending on their intent, malicious actors may also destroy all data (including backups) accessible to a user 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.

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

Mitigation Strategy	Description
	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.
	Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.
	Online services that are no longer supported by vendors are removed.
	Office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.
Patch operating systems	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.
	Operating systems that are no longer supported by vendors are replaced.
Multi-factor authentication	Multi-factor authentication is used to authenticate users to their organisation’s online services that process, store or communicate their organisation’s sensitive data.
	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation’s sensitive data.
	Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation’s non-sensitive data.
	Multi-factor authentication is used to authenticate users to their organisation’s online customer services that process, store or communicate their organisation’s sensitive customer data.

Mitigation Strategy	Description
	Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.
	Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.
	Multi-factor authentication is used to authenticate privileged users of systems.
	Multi-factor authentication is used to authenticate unprivileged users of systems.
	Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.
	Multi-factor authentication used for authenticating users of online services is phishing-resistant.
	Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.
	Multi-factor authentication used for authenticating users of systems is phishing-resistant.
	Successful and unsuccessful multi-factor authentication events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict administrative privileges	Requests for privileged access to systems, applications and data repositories are validated when first requested.
	Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.
	Privileged access to systems and applications is disabled after 45 days of inactivity.
	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.
	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.
	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.
	Privileged users use separate privileged and unprivileged operating environments.

Mitigation Strategy	Description
	Privileged operating environments are not virtualised within unprivileged operating environments.
	Unprivileged user accounts cannot logon to privileged operating environments.
	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.
	Administrative activities are conducted through jump servers.
	Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.
	Privileged access events are centrally logged.
	Privileged user account and security group management events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Application control	Application control is implemented on workstations.
	Application control is implemented on internet-facing servers.
	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.
	Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.
	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.
	Microsoft’s recommended application blocklist is implemented.
	Application control rulesets are validated on an annual or more frequent basis.
	Allowed and blocked application control events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.

Mitigation Strategy	Description
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict Microsoft Office macros	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.
	Microsoft Office macros in files originating from the internet are blocked.
	Microsoft Office macro antivirus scanning is enabled.
	Microsoft Office macros are blocked from making Win32 API calls.
	Microsoft Office macro security settings cannot be changed by users.
User application hardening	Internet Explorer 11 is disabled or removed.
	Web browsers do not process Java from the internet.
	Web browsers do not process web advertisements from the internet.
	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	Web browser security settings cannot be changed by users.
	Microsoft Office is blocked from creating child processes.
	Microsoft Office is blocked from creating executable content.
	Microsoft Office is blocked from injecting code into other processes.
	Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.
	Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	Office productivity suite security settings cannot be changed by users.
	PDF software is blocked from creating child processes.
	PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	PDF software security settings cannot be changed by users.
	PowerShell module logging, script block logging and transcription events are centrally logged.
	Command line process creation events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.

Mitigation Strategy	Description
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Regular backups	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.
	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.
	Backups of data, applications and settings are retained in a secure and resilient manner.
	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.
	Unprivileged user accounts cannot access backups belonging to other user accounts.
	Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.
	Unprivileged user accounts are prevented from modifying and deleting backups.
	Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.

MATURITY LEVEL 2 – DEEP DIVE

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 user 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.

Control	Assessment Guidance (ordered by effectiveness)
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).

Control	Assessment Guidance (ordered by effectiveness)
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 user accounts that have not been used within 45 days can indicate that they are no longer required. Rather than user accounts remaining active, and a possible target for malicious actors to exploit, inactive user 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 user 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 expiry date is set for privileged user accounts in Active Directory under user account profiles and whether a mechanism exists to disable such user accounts after 12 months unless revalidated beforehand. Ask for a screenshot of the output of the following PowerShell commands that check for user 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 user 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 user 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.

Control	Assessment Guidance (ordered by effectiveness)
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 user 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'.

Control	Assessment Guidance (ordered by effectiveness)
	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 user account and security group management events are centrally logged.	Leveraging related Windows Event IDs, check whether changes to privileged user accounts and groups are logged. In addition, determine if these event logs are being centrally stored. More information on security operations for privileged user 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	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.

Control	Assessment Guidance (ordered by effectiveness)
one of their delegates, as soon as possible 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).

Control	Assessment Guidance (ordered by effectiveness)
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 a user 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 a user 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 a user account that is allowed to execute Microsoft Office macros.

Control	Assessment Guidance (ordered by effectiveness)
	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 a user 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.

Control	Assessment Guidance (ordered by effectiveness)
	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).

Control	Assessment Guidance (ordered by effectiveness)
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 user 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 user accounts increases the chance that they will be compromised. Should this occur for these user 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 user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.	Use the guidance provided in Maturity Level One of this guide but apply the more restrictive access control requirements. Specifically, privileged user 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 user accounts including backup administrator accounts.
Privileged user 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 user 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 user accounts including backup administrator accounts.