Essential Eight Self Assessment Guide

A Handbook for Organisations Conducting Their Own Maturity Level One Assessment

www.computerone.com.au

Understanding the Essential Eight Maturity Levels

The Australian Cyber Security Centre (ACSC) outlines the full criteria for Maturity Levels One, Two and Three within the Essential Eight framework. We've included a simplified overview in this brochure to help you achieve Maturity level One.

You can access the complete criteria on the ACSC website.

What This Guide Covers

This brochure walks you through assessing each Essential Eight attribute at Maturity Level One, based on guidance current as of 02 October 2024.

A Note on Product References

Some sections mention specific products or brands. These references are not endorsements by Computer One or the ASD/ACSC.

They are included only as practical examples. Some products mentioned do reflect tools we use ourselves, including Microsoft security products and Airlock Digital.

Readers will also note that most of the content is written from the perspective of testing and assessing a Windows environment. Linux and IOS environments can also be assessed, of course, but to keep the intent simple and focused on the majority of users, we have restricted references to just Windows.

Contents

There are four Mandatory Stages of an Essential Eight Assessment

Plan & Prepare **4**
Determine Scope & Approach **5**
Assessment of Controls **6**
Developing the Security Assessment Report **24**

These stages ensure consistency, accuracy, and evidence based maturity outcomes.

Why the Essential Eight Matters

The Australian Signals Directorate (ASD) developed the Essential Eight to help organisations reduce cyber-risk through eight prioritised mitigation strategies. Assessing your maturity ensures you understand how effectively these controls are implemented and where uplift is needed.

The most recent Essential Eight Assessment Process Guide outlines how assessments must be planned, executed, and reported.

This brochure helps you conduct a clear, structured self-assessment against Maturity Level One, targeting threats using widely available tools and techniques.

Plan & Prepare

Understanding Maturity Levels

Every organisation must first assess itself against all aspects of Level One. This step ensures you build a complete and stable security foundation before progressing to higher maturity levels.

Because the Essential Eight must be assessed as a complete package, an organisation cannot progress to a higher maturity level unless it has already demonstrated achievement of each element of the previous level. If any control is ineffective, the strategy is not implemented, preventing maturity achievement.

Maturity Level One focuses on threats using commodity tradecraft. This includes readily available exploits, stolen credentials, or simple attack techniques.

At Level One the focus is on mitigating:

- common vulnerabilities
- weak credentials
- human error

Before assessing, confirm:

- *Required access: systems, accounts, documentation, personnel, and facilities*
- *Approval to run scripts and tools*
- *Engagement with stakeholders from across the organisation*
- *Evidence collection and protection, incl. post-assessment storage / circulation*
- *Report use, retention and marketing permissions*
- *Stakeholder engagement and consultation*

Determine Scope & Approach

Outline the scope of the assessment (the maturity level you are targeting) in the security assessment report.

Define what systems are in scope and select your testing methods.

An effective assessment uses both qualitative and quantitative techniques, including:
- Qualitative: Documentation reviews, policy inspections, and interviews.
- Quantitative: Scripts, configuration reviews, scanning tools

> *Note: The ACSC strongly prefers automated tools and scripts over manual inspection.*

Final scope decisions, and anything deemed as out of scope, must be recorded in the assessment report, as they influence timelines, resources, and sampling requirements.

Consult with the system owner to determine sample sizes for testing. You should aim to assess a reasonable representative sample of workstations (including laptops), servers and network devices.

Document any limitations, such as reduced sample sizes or restrictions on tool use.

Evidence Quality Levels

To be confident of your findings, use the highest quality evidence you can gather.

Evidence types include:

Excellent
Simulated tests confirming control effectiveness

Good
Direct configuration inspection

Fair
Screenshots, exported reports

Poor
Policies or verbal statements

Aim for Excellent or Good evidence wherever possible. This gives readers more confidence in your report.

Assessment of Controls

At this stage, the assessor reviews and tests how effectively each control within the Essential Eight mitigation strategies is implemented.

Controls are assessed by:

- Reviewing configuration settings
- Running scripts or tools
- Testing control behaviour
- Inspecting system outputs

The following sections summarise Level One requirements for each Essential Eight strategy. They reflect the Nov 2023 maturity model.

At each mitigation strategy, review and test the effectiveness of controls. Guidance on determining the effectiveness of controls within each mitigation strategy has been provided.

Assessors must also evaluate compensating controls when applicable, ensuring that they provide protection equivalent to the original control.

More details on assessment guidance can be found on the Australian Signals Directorate website, if required.

Using Compensating Controls

If your organisation cannot meet a control directly:

- Implement strong compensating controls
- Document the justification for applying a compensating control, the scope of the control, risk rating of the issue, the control's lifecycle (when it applies or will be reviewed) and the review date
- Importantly, risk acceptance cannot replace a mitigation strategy – you cannot state that you are compliant with a particular maturity level of the Essential Eight just by documenting and accepting a risk.

Applying and Assessing the Essential Eight

Patch Applications

Ensure vulnerabilities in applications are identified and patched within required timeframes.

Vendors frequently update online services and applications to fix vulnerabilities. By using release dates and patch notes, you can compare applications in use with the latest versions from vendors and check if they are up to date.

Helpful resources

- SANS Internet Storm Centre
- Microsoft Security Response Centre
- CISA Known Exploited Vulnerabilities Catalogue

Level One Requirements

- Use automated asset discovery at least fortnightly
- Use a vulnerability scanner with up to date databases
- Scan online services daily
- Scan productivity software weekly
- Apply patches for critical vulnerabilities within 48 hours
- Apply non critical patches within two weeks
- Remove unsupported software

How to Assess for Level One Maturity

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.	■ View a demonstration of the asset discovery method. If a third party provides IT support, confirm their service addresses this asset discovery requirement ■ Verify recent scan dates and scope. ■ Check for unauthorised assets on the network. ■ Consider aligning asset discovery timing with vulnerability scans.
A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	■ Review a vulnerability scan demonstration and confirm the scanner has all the online services known to be in use, in scope. ■ Confirm the database's most recent update (ideally within the previous 24 hours of the scan).
A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in services.	■ Review a vulnerability scan in action and its results. ■ Review recent scans for date/time and scope. Confirm they are happening daily. ■ Ensure scanned services match the organisation’s known used 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.	■ Review a vulnerability scan and confirm inclusion of all applications that match the control description. ■ Check previous scans for date/time and the scanned applications to confirm frequency is compliant.
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.	■ Use a network-based scanner to identify online services, their versions and install dates. Compare this information to release date of patches then determine if patching timeframe of 48 hours has been met. (!) Note: a scanner may not identify missing vendor mitigations such as configuration changes ■ There are several free tools available, such as: 🌐 Nessus Essentials 🌐 Nexpose Community Edition 🌐 OpenVAS 🌐 Qualys Community Edition The ASD also provides several tools, but you must be a network partner like Computer One to access them. ■ Manually check versions (screenshots of versions for online services) if a scanner is unavailable.
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.	■ Similar to critical vulnerability patching. Use network-based scanning or manual checks. You can use the same applications described above to identify unpatched applications. ■ Consider the potential for overlooked or unknown services. An automated scanner is likely to deliver more exhaustive results.
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.	■ Review the list of installed applications within ‘Programs and Features’ in Windows or ‘Applications’ in iOS systems. ■ Employ vulnerability scanners or PowerShell to further build out the list of installed applications. (!) Note: The ACSC offers a Powershell script that can be used to output installed applications with registered uninstall functionality. You can find it on this page. Search for “Powershell”. This list should be reviewed in conjunction with the list of installed applications to ensure no applications are missed. ■ Review installed applications against patch release dates. ■ For manual checks, demonstrate application versions and install dates.

Online services that are no longer supported by vendors are removed.	■ Use vulnerability scanners to check for end-of-life services. ■ Review evidence of removal of unsupported services.
Office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	■ Use vulnerability scanners to check for end-of-life services. ■ Demonstrate current versions and check against supported versions. ■ Verify Adobe Flash Player has been removed from the network.

Patch Operating Systems

Reduce exposure from OS level vulnerabilities.

Operating system vendors frequently issue updates to fix vulnerabilities. Unsupported systems, particularly those connected to the internet, are highly targeted by cyber attackers.

While internal systems like workstations and non-internet-facing servers are less exposed, they still need timely patching to mitigate risks from sophisticated attacks.

Helpful resources

- SANS Internet Storm Centre
- Microsoft Security Response Centre
- CISA Known Exploited Vulnerabilities Catalogue

Maturity Level One Requirements

- Automated asset discovery at least fortnightly
- Use vulnerability scanners with updated databases
- Scan internet facing servers daily
- Scan internal systems at least fortnightly
- Apply critical OS patches within 48 hours
- Apply non critical OS patches within two weeks
- Replace unsupported operating systems

How to Assess for Level One Maturity

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.	■ Review the performance of the automated asset discovery tool. This may be a standalone tool or integrated with a vulnerability scanner and may be provided by a third party such as Computer One. ■ Verify past asset discovery scans for frequency and coverage. ■ Consider aligning discovery scan frequency with vulnerability scans for efficiency. ■ Use asset discovery tool to spot any unauthorised assets connected to the system between scheduled scans and investigate them.
A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	■ Witness and review the vulnerability scanning process. ■ Ensure you see evidence of the vulnerability database having been updated recently, preferably within the last 24 hours.
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.	■ Review the process of daily vulnerability scanning and confirm it is taking place. ■ Acquire and review recent scan logs, focusing on timestamps and event details, looking to confirm the daily nature of the scan.

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.	■ Review the process of the fortnightly scanning and confirm it is taking place. ■ Acquire and review logs of recent scans, highlighting dates and coverage. Look for evidence of the fortnightly or earlier scan frequency.
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.	■ Use a network-based vulnerability scanner to verify up-to-date operating systems. ■ There are several free tools available, such as: 🌐 Nessus Essentials 🌐 Nexpose Community Edition 🌐 OpenVAS 🌐 Qualys Community Edition The ASD also publishes a free tool, but it is only available to ASD partners like Computer One. (!) Note from the ASD site: 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). ■ Utilize WMIC or PowerShell to produce a list of hotfixes and when they were applied. 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.	■ Assess using the same process as above
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.	■ As above
Operating systems that are no longer supported by vendors are replaced.	■ Utilize scanners to identify the OS version. ■ Use ‘winver’ command for Windows or ‘cat /etc/os-release’ for Linux to check OS versions. ■ Acquire screenshots of these outputs to compare with vendor support lists.

Multi Factor Authentication (MFA)

Prevent misuse of credentials by adding a second verification factor.

Multi-factor authentication significantly enhances security by making it harder for malicious actors to misuse credentials. It's particularly effective against brute force attacks that can easily breach single-factor methods like passwords.

At Maturity Level One, the focus is on securing online services with multi-factor authentication. The permitted forms include a combination of something the user has (like a device or OTP) and something they know (like a password).

Biometrics must not be used as a primary authentication factor. They may be used only as a secondary factor to unlock a “something you have” factor (for example, device-bound cryptographic credentials). For online services, ensure MFA is phishing-resistant. Avoid SMS one-time codes (and similar) as they are considered weaker and do not meet the phishing-resistant intent.

Maturity Level One Requirements

- MFA for all organisational online services storing or processing sensitive data
- MFA for third party services that store or process sensitive organisational or customer data
- MFA for online customer facing services with sensitive information

How to Assess for Level One Maturity

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.	■ Test login to all the organisation’s services and observe if multiple factors (password, OTP) are needed whether they are presented at once or in sequence after the first is verified. ■ If you are assessing a less familiar department in the organisation, investigate for other non-disclosed internet-facing portals lacking MFA.
Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation’s sensitive data.	■ Try logging into third-party services handling sensitive data and verify MFA presence. ■ If MFA is missing, verify if it is unavailable or simply unimplemented.
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.	■ Test login to the third-party services. ■ If MFA is missing, verify if it is unavailable or simply unimplemented.

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 login to organisation's customer services and check for MFA. ■ If MFA is missing, verify if it is unavailable or simply unimplemented.
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.	■ Log into third-party customer services with sensitive data to check MFA. ■ If MFA is missing, verify if it is unavailable or simply unimplemented.
Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.	■ Test login to customer-facing online services for MFA presence. These are things like customer portals, quote, project or document exchange portals, support ticket logs, warranty claim portals with sensitive information, payment portals and third-party services like software vendors. ■ Is multi-factor authentication set up as part of account creation or do users need to set it up themselves after initial account creation and a grace period? MFA set-up upon account creation is less risky.
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.	■ Discover and evaluate MFA implementations across different systems and services. ■ Differentiate between multi-step and multi-factor authentication. The latter is required to assess as Level One. ■ Compare and assess the security levels of various MFA methods (security keys, OTP devices, mobile apps, SMS codes).

Restrict Administrative Privileges

Limit the ability for attackers to escalate privileges.

Privileged access management in organisations should be well-documented and integrated into routine workflows.

Due to the high risk associated with privileged accounts, which are often targets for malicious actors, their internet, email, and web service access should be restricted and granted only under specific, necessary conditions.

Access requests for systems, applications, and data should be formally made through a form, service desk ticket, or email and must receive approval from a supervisor or the respective owner. Keeping a record of these requests and a list of all applications requiring privileged access is essential.

Maturity Level One Requirements

- Admin accounts used only for admin tasks
- Regular reviews of privileged access
- Grant privileges based on least privilege principles (Detailed controls available within ACSC maturity model)

How to Assess for Level One Maturity

Control	Assessment Guidance (Ordered by Effectiveness)
Privileged users are assigned a dedicated privileged account to be used solely for duties requiring privileged access.	■ Verify that privileged users have distinct privileged and unprivileged accounts ■ Ensure no one is set up to use a single account for all tasks.
Requests for privileged access to systems, applications and data repositories are validated when first requested.	■ Request and review submitted forms, tickets, or emails for privileged access requests, endorsed by a supervisor or relevant owner. ■ Compare these to actual privileged account access records to spot discrepancies that indicate the request process is not working as intended.
Privileged accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.	■ Test for internet access as a privileged user and check internet proxy settings on the network to determine if it is configured to block traffic from privileged accounts. ■ Use PowerShell to examine email access for privileged accounts. You can find an example script on this page – search for “Powershell”. ■ BloodHound can help identify overlooked privileged accounts that PowerShell may miss. ■ Verify if accounts, like those for cloud service management, have been permitted internet access through a formal application 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.	■ Discover and assess how access for privileged accounts authorised for online services, such as cloud management, is restricted from using other internet services. ■ This principle is about separating privilege from general internet access.
Privileged users use separate privileged and unprivileged operating environments.	■ Discuss the implementation of distinct privileged and unprivileged environments for system management. Note: at this level of Essential Eight maturity, there are no constraints on how this is to be implemented beyond establishing that separate privileged and unprivileged environments have been set up.
Unprivileged accounts cannot log-on to privileged operating environments.	■ Try logging into a privileged environment with a standard account. ■ Use BloodHound to check for any unprivileged accounts accessing privileged environments by looking for cached credentials.
Privileged accounts (excluding local administrator accounts) cannot log-on to unprivileged operating environments.	■ Undertake an attempt as a privileged account trying to access an unprivileged environment, using a test account which should be removed post-testing. ■ BloodHound can be used to assess if any privileged accounts have accessed unprivileged environments by looking for cached credentials.

Application Control

Prevent unauthorised code execution.

At this level, using an application control solution is essential – see list below.

You can conduct an application control assessment without using any tools, but the effectiveness of your test will be severely limited. Manual application control assessments are generally ineffective and easily overlook edge vulnerabilities targeted by malicious actors.

It is important to note that some application control solutions might not support files like .chm, .hta, and .cpl. It is essential to assess paths used by standard user profiles and temporary folders in operating systems, web browsers, and email clients.

Common paths include:

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

To test application control effectiveness within these areas, try running benign executable files. The test should cover .exe, .com, .dll, .ocx, .ps1, .bat, .vbs, .js, .msi, .mst, .msp, .chm, .hta, and .cpl. If any executables run in the user profile directory or operating system temporary folders, the application control is not effective.

Helpful resources

- Microsoft's AppLocker,
- Windows Defender Application Control,
- or third-party tools like AirLock Digital, Ivanti, Trend Micro, or Carbon Black.

Maturity Level One Requirements

- Allow listing enforced for executables, scripts, installers, libraries
- Application control applied on workstations
- Prevent execution from user profile directories and temporary folders

How to Assess for Level One Maturity

Control	Assessment Guidance (Ordered by Effectiveness)
Application control is implemented on workstations.	• Verify the presence of an application control solution on workstations.
Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	• Ensure application control covers user profiles and temporary folders of the OS, web browsers, and email clients as a minimum. ! Note: this is relevant for path-based rules only, as publisher-based and hash-based rules are automatically applied system-wide.

Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.

- Test the effectiveness of application control by trying to write and execute files in accessible user areas. Utilise free tools like AirLock Digital's Application Whitelist Auditor, or CyberArk's Evasor for assessment.
- If restricted to Microsoft tools, use SysInternals AccessChk to analyse folder permissions. Run 'accesschk -dsuvw [path] > report.txt' for writable path permissions and 'whoami /groups' to determine user group permissions.
- To test and review AppLocker policy, use PowerShell cmdlets.
- In a tool-restricted system, you may have to acquire screenshots of 'effective access' permissions for critical folders to assess read/write/execute permissions, understanding this method has limitations and may not cover all folders and sub-folders - at any point in a path application control inheritance previously set by an operating system may be disabled by an application installer.

Restriction of Microsoft Office Macros

Limit macro based malware.

Users should only be allowed to run Microsoft Office macros if they have a proven business need.

Their use should be limited to essential applications, with their requirement and approvals recorded, aligning with their Active Directory group permissions.

If their business need ceases, their macro permission should be withdrawn.

Consider utilising ASD's E8MVT tool for evaluating the implementation of this control. This tool can accessed via an ACSC partner such as Computer One.

Maturity Level One Requirements

- Block macros from the internet
- Only allow digitally signed macros
- Prevent untrusted macro execution

How to Assess for Level One Maturity

Control	Assessment Guidance (Ordered by Effectiveness)
Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	■ To conduct your own assessment, generate an RSoP (Resultant Set of Policy) report with the 'gpresult' command to identify Microsoft Office macro settings applied via group policy settings. Within the RSoP report, look for the 'VBA Macro Notification Settings' at 'User Configuration\Policies\Administration Templates\<Microsoft Office Application>\Application Settings\Security\Trust Center\'. It should be enabled. ■ Within the RSoP report, look for 'VBA Macro Notification Settings' to be set to 'Disable all macros without notification' for the majority of users. In the absence of this configuration, while all Microsoft Office macros will be automatically disabled, users will be prompted through the Message Bar to decide if they wish to enable them. ■ For users who have a verified business need to use Microsoft Office macros, group policy setting can be left unconfigured, disabled, or enabled with any other setting. However, it is essential to ensure that antivirus scanning is active and that Microsoft Office macros from internet-sourced files are blocked. ■ Think about calculating the proportion of your organisation's users who are authorised to use Microsoft Office macros. This step is to make sure that the permissions for running these macros are not excessively generous.

Microsoft Office macros in files originating from the internet are blocked.	■ In the RSoP report, ensure 'Block macros from running in Office files from the Internet' is enabled at "User Configuration\Policies\Administration Templates\<Microsoft Office Application>\Application Settings\Security\Trust Center\." 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. Note: 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.	■ In the RSoP report, confirm 'Macro Runtime Scan Scope' is correctly set for each Office application. You can find it at: 'User Configuration\Policies\Administrative Templates\Microsoft Office 2016\Security Settings\Macro Runtime Scan Scope'. It should be set to either 1 - Macros in files with the Mark of The Web [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.
Microsoft Office macro security settings cannot be changed by users.	■ In the RSoP report, check that 'VBA Macro Notification Settings' are locked via group policy settings. Go to 'User Configuration\Policies\Administration Templates\<Microsoft Office Application>\Application Settings\Security\Trust Center\' Try altering macro settings in Office Trust Center with a user account to confirm settings are greyed out.

User Application Hardening

Reduce browser and document viewer attack surface.

Lacking modern security features and unsupported by Microsoft since 15 June 2022, Internet Explorer 11 is a frequent target for cyber-attacks. It should be replaced with Microsoft Edge or another up-to-date browser.

Blocking web ads with browser add-ons, extensions, or content filtering is recommended to guard against 'malvertising' used by malicious actors. For robust security, configure web browser settings through group policy settings, rather than relying on default settings which users might alter following malicious guidance.

Settings configured via group policy are typically unchangeable by users, indicated by a greyed-out appearance, a tooltip, or a padlock icon.

Level One Requirements

- Disable unnecessary features (Flash, ads, untrusted Java)
- Block risky content in browsers and PDF readers

How to Assess for Level One Maturity

Control	Assessment Guidance (Ordered by Effectiveness)
Internet Explorer 11 is disabled or removed.	■ In the RSoP report, verify if 'Disable Internet Explorer 11 as a standalone browser' is enabled. ■ Alternatively, take a look at the 'Windows Features' that are installed to check if Internet Explorer 11 is installed or removed. 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: standard users will still be able to launch IE11. Ensure 'iexplore.exe' is blocked through application control rules.
Web browsers do not process Java from the internet.	■ Compile a list of installed web browsers and test each by visiting a Java-based website – you can use this one: https://www.whatismybrowser.com/detect/is-java-installed. ■ Review browser plug-ins or extensions for Java components and ensure they are disabled. ■ If Java is needed for intranet use, assess compensating controls like web content filters for blocking internet-based Java.

Web browsers do not process web advertisements from the internet.	■ Verify if ad-blocking extensions or add-ins are installed in web browsers. ■ Check for ad-blocking via web content filters or proxies. ■ Conduct a test by visiting a known ad-heavy website using one of the organisation's PC's and take screenshots of the results. Note: browser settings for pop-up blocking alone do not suffice for this control.
Web browser security settings cannot be changed by users.	■ Review each installed web browser's security settings to see if they are unchangeable. ■ Look for indications like settings being greyed out or messages stating 'This setting is managed by your organisation/administrator'. ■ Check if Java Control Panel settings can be altered by users. Your organisation is compliant with this control if they cannot.

Regular Backups

Ensure resilience against data destruction.

Backups of data, applications, and settings should be regularly done and kept based on an organisation's critical needs and continuity plans.

It's crucial to test the restoration from these backups at least annually as part of disaster recovery practices, rather than waiting for a major security incident.

At this maturity level, it's important to ensure that regular users can't access others' backups but can access their own. However, privileged accounts may still have access to all users' backups.

Regular users should be able to read but not modify or delete their backups. This prevents ransomware, using regular user privileges, from altering or deleting backups. The risk of malicious actors with higher privileges compromising backups is considered at more advanced maturity levels.

Maturity Level One Requirements

- Daily backups of important data
- Verify recoverability
- Protect backups from tampering

How to Assess for Level One Maturity

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 the specified backup frequencies with your IT team, particularly considering the importance of different data sets and applications. ■ Inspect the business continuity plan to verify documented frequencies and retention periods for backups. ■ With this item, you will be required to determine the degree of success of this control's implementation and compliance with the intent of this control.
Backups of data, applications and settings are synchronised to enable restoration to a common point in time.	■ Ensure backup processes are synchronised for seamless restoration to a common point in time. If not, restoration may prove challenging and result in potential data loss.
Backups of data, applications and settings are retained in a secure and resilient manner.	■ Assess the security and resilience of backup procedures. ■ Check if backups are encrypted and their effectiveness in quick recovery from ICT failures.

Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.	■ Review the results of disaster recovery drills, including their frequency, the date of the last drill, and whether they involved full or partial system restoration. ■ Confirm that post-exercise reports or reviews that detail the recovery process and any lessons learned have been produced. Note: for the purposes of this control, simple business-as-usual file recovery doesn't suffice; substantial system component restoration is key.
Unprivileged accounts cannot access backups belonging to other accounts.	■ Check if unprivileged accounts can alter or delete their own backups. ■ If backups are on network shares, use an unprivileged account to try and modify or delete a backup and take ownership of content to change permissions. The organisation is compliant if you cannot do this.

Developing the Security Assessment Report

The final stage of the assessment formalises all findings into a structured Security Assessment Report (SAR).

This report consolidates evidence, clarifies maturity outcomes, and provides the system owner with a practical roadmap for remediation. It is the authoritative output of the assessment process and must be written with accuracy, clarity, and traceability.

The SAR provides the system owner with a defensible record of their maturity, supporting governance, remediation planning, and audit readiness.

The outcomes determine whether the mitigation strategy can be claimed at the target maturity level.

Core Components of the Assessment Report

The ACSC requires the report to include the following elements:

- Assessment scope and boundaries
- Methods used (scripts, tools, interviews, configuration review)
- Evidence collected
- Outcome per control
- Identified exceptions & compensating controls
- Overall maturity level

Documenting Assessment Outcomes

Each control must be assigned one of the ACSC's standardised outcomes:

Effective	Alternate control	Ineffective	Not implemented	Not assessed	No visibility	Not applicable

If any required control is ineffective or not implemented, the entire strategy is considered not implemented.

Where exceptions exist, the report must include:

- Reason for the exception
- Associated risks
- Compensating controls implemented
- Assessment of whether compensating controls match the intent of the original control
- Expected lifetime and next review date
- Residual risk acceptance by an appropriate authority

Weak or poorly managed exceptions may prevent the organisation from being assessed at the target maturity level.

Recommendations & Roadmap for Improvement

The SAR should conclude with clear, prioritised recommendations to address gaps. Recommendations should be tied directly to control failures or gaps identified during the assessment.

These may include:

- Required technical configuration changes
- Process improvements
- Policy updates
- Implementation of stronger compensating controls
- Additional monitoring or validation steps

Report Handling & Retention

Security assessment reports often contain sensitive details and must be protected appropriately.

The assessor and system owner must confirm:

- How the report may be stored
- Who may access it
- How long it will be retained
- Any constraints on external sharing or referencing

A note on report use

To prove to an external body that your organisation is genuinely at a given level of maturity, it may be important to use an assessor engaged at arm's length.

Computer One is a skilled assessor of a variety of security frameworks, including the ASD Essential Eight. Our reports are prepared without cutting corners or obfuscating facts, to ensure your organisation is truly at the target level of ASD Essential Eight maturity.

The ASD Essential Eight is a set of practical cyber security strategies any organisation can aim at implementing successfully. It is one of the world's leading instruction sets for countering cyber threats.

Computer One can help your organisation achieve Maturity Level One, Two, or Three in a cost-effective, controlled manner.

For a genuinely independent assessment or assistance in raising your organisation's maturity level, contact us for a free and confidential discussion.

COMPUTER one

1300 667 871
sales@computerone.com.au
Brisbane | Sydney | Melbourne
computerone.com.au

ABN 47 010 486 209