# Example Essential Eight Assessment Test Plan – Maturity Level One

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mitigation Strategy** | **Test ID** | **Control Description** | **Test Methodology** | **Test Findings** |
| **Patch applications** | ML1-PA-01 | An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. | Review the method of automated asset discovery being used to identify assets such as workstations, servers and network devices.  Request evidence of previous vulnerability scans and review the date/time stamp and scope. |  |
| ML1-PA-02 | A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | Request evidence of when the vulnerability database was last updated and compare to vulnerability scan history to determine whether updates occurred within 24 hours of vulnerability scans taking place. |  |
| ML1-PA-03 | A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services. | Observe a vulnerability scan, or request evidence of previous vulnerability scans, and note the date/time stamp and scope. Check whether the list of scanned online services match the list of online services that are known to be used. |  |
| ML1-PA-04 | 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. | Observe a vulnerability scan, or request evidence of previous vulnerability scans, and note the date/time stamp and scope. Check whether the list of scanned applications includes the list of applications that should have been scanned. |  |
| ML1-PA-05 | 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 vulnerability scanner to identify online services within the environment and check that they have been patched against a critical vulnerability or known working exploit. Determine the date the patch was installed and compare to when the patch was made available. Check that the gap between is not greater than 48 hours. |  |
| ML1-PA-06 | 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. | Use a vulnerability scanner to identify online services within the environment and check that they have been patched against a non-critical vulnerability that has no known working exploits. Determine the date the patch was installed and compare to when the patch was made available. Check that the gap between is not greater than two weeks. |  |
| ML1-PA-07 | Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release. | Use a vulnerability scanner to identify the listed applications within the environment. Check the date applications were updated and compare to the dates patches were released. Check that the gap between is not greater than two weeks. |  |
| ML1-PA-08 | Online services that are no longer supported by vendors are removed. | Use a vulnerability scanner to identify online services within the environment and check they are still vendor supported. |  |
| ML1-PA-09 | 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 a vulnerability scanner to identify the listed applications within the environment and check they are still vendor supported. |  |
| **Patch operating systems** | ML1-PO-01 | An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. | Review the method of automated asset discovery being used to identify assets such as workstations, servers and network devices.  Request evidence of previous vulnerability scans and review the date/time stamp and scope. |  |
| ML1-PO-02 | A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | Request evidence of when the vulnerability database was last updated and compare to vulnerability scan history to determine whether updates occurred within 24 hours of vulnerability scans taking place. |  |
| ML1-PO-03 | 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. | Observe a vulnerability scan, or request evidence of previous vulnerability scans, and note the date/time stamp and scope. Check whether the list of scanned devices includes the list of devices that should have been scanned. |  |
| ML1-PO-04 | 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. | Observe a vulnerability scan, or request evidence of previous vulnerability scans, and note the date/time stamp and scope. Check whether the list of scanned devices includes the list of devices that should have been scanned. |  |
| ML1-PO-05 | 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 vulnerability scanner to check whether operating systems for internet-facing servers and internet-facing network devices have been patched against a critical vulnerability or known working exploit. Determine the date the patch was installed and compare to when the patch was made available. Check that the gap between is not greater than 48 hours. |  |
| ML1-PO-06 | 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. | Use a vulnerability scanner to check whether operating systems for internet-facing servers and internet-facing network devices have been patched against a non-critical vulnerability that has no known working exploits. Determine the date the patch was installed and compare to when the patch was made available. Check that the gap between is not greater than two weeks. |  |
| ML1-PO-07 | 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. | Use a vulnerability scanner to check whether operating systems for workstations, non-internet-facing servers and non-internet-facing network devices have been patched against a vulnerability. Determine the date the patch was installed and compare to when the patch was made available. Check that the gap between is not greater than one month. |  |
| ML1-PO-08 | Operating systems that are no longer supported by vendors are replaced. | Use a vulnerability scanner to identify operating systems within the environment and check they are still vendor supported. |  |
| **Multi-factor authentication** | ML1-MF-01 | Multi-factor authentication is used to authenticate users to their organisation’s online services that process, store or communicate their organisation’s sensitive data. | Identify the organisation’s use of their own online services to process, store or communicate their sensitive data. Attempt to logon, or observe a user logon, to the online services. Verify that the user is presented with an MFA challenge. |  |
| ML1-MF-02 | Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation’s sensitive data. | Identify the organisation’s use of third-party online services to process, store or communicate their sensitive data. Attempt to logon, or observe a user logon, to the online services. Verify that the user is presented with an MFA challenge. |  |
| ML1-MF-03 | 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. | Identify the organisation’s use of third-party online services to process, store or communicate their non-sensitive data. Attempt to logon, or observe a user logon, to the online services. Verify that the user is presented with an MFA challenge. If not, confirm that the online service provider does not offer MFA functionality. |  |
| ML1-MF-04 | 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. | Identify the organisation’s use of their own online customer services to process, store or communicate their customers’ sensitive data. Attempt to logon, or observe a user logon, to the online customer services. Verify that the user is presented with an MFA challenge. |  |
| ML1-MF-05 | 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. | Identify the organisation’s use of third-party online customer services to process, store or communicate their customers’ sensitive data. Attempt to logon, or observe a user logon, to the online customer services. Verify that the user is presented with an MFA challenge. |  |
| ML1-MF-06 | Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data. | Identify the organisation’s use of online customer services (both their own and third party) to process, store or communicate their customers’ sensitive data. Attempt to logon as a typical customer, or observe a customer logon, to the online customer services. Verify that the customer is presented with an MFA challenge. |  |
| ML1-MF-07 | 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. | When observing users and customers performing MFA, determine whether it uses either of the below approaches:  Something users have (e.g. look-up secrets, out-of-band devices, single-factor OTP devices, single-factor cryptographic software or single-factor cryptographic devices) AND something users know (e.g. memorised secrets).  OR  Something users have that is unlocked by something users know or are (e.g. multi-factor OTP devices, multi-factor cryptographic software and multi-factor cryptographic devices). |  |
| **Restrict administrative privileges** | ML1-RA-01 | Requests for privileged access to systems, applications and data repositories are validated when first requested. | Confirm the organisation has documented, approved and enforced privileged access processes and procedures that outline the requirements for provisioning privileged accounts. Confirm the organisation has a list of systems, applications and data repositories that require privileged access.  Review documented privileged access processes and procedures. Request forms, support tickets or emails provided by users requesting privileged access to systems, applications or data repositories along with approvals. This can be compared to screenshots of accounts with privileged access to determine if there are any discrepancies. |  |
| ML1-RA-02 | Privileged users are assigned a dedicated privileged account to be used solely for duties requiring privileged access. | Discuss whether privileged users are assigned separate unprivileged and privileged accounts or whether they use a single privileged account for all their duties. Request a privileged user show you the accounts they use for privileged actions and unprivileged actions. |  |
| ML1-RA-03 | Privileged accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services. | While logged in as a privileged user, attempt to browse to an internet website. Review the configuration preventing internet access and attempt to change this as a privileged user not responsible for administering that system. Privileged accounts not responsible for administering these systems should not be able to change settings to access the internet.  Attempt to open Microsoft Outlook on a system using the privileged account.  Run the following PowerShell command to check if privileged accounts have access to mailboxes and email addresses:  *Get-ADUser -Filter {(admincount -eq 1) -and (emailaddress -like "\*") -and (enabled -eq $true)} -Properties EmailAddress | Select samaccountname, emailaddress* |  |
| ML1-RA-04 | Privileged accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties. | Confirm the organisation has a documented and approved list of privileged accounts that require access to online services. It should specify which account has access to which online service.  Determine whether these accounts are appropriately limited from accessing all other online services over the internet. |  |
| ML1-RA-05 | Privileged users use separate privileged and unprivileged operating environments. | Attempt to access the administrative network environment using a standard account. Attempt to access the standard environment using a privileged account. Look for evidence of administrative access to unprivileged environments using tools such as BloodHound. |  |
| ML1-RA-06 | Unprivileged accounts cannot logon to privileged operating environments. | Attempt to logon to a privileged operating environment using a standard account. Use BloodHound to analyse Active Directory data and any unprivileged accounts that have connected to privileged operating environments by looking for cached credentials. |  |
| ML1-RA-07 | Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. | Request a demonstration of a privileged account attempting to logon to a standard user workstation. Check group policy settings for ‘Deny logon locally’ and ‘Deny log on through Remote Desktop Services user rights’ to workstations for privileged accounts.  While logged in as a standard user, attempt to use ‘runas’ to open an application as an administrator. Attempt other ways (e.g. WinRM, Computer Management or RDP) to escalate privileges to an administrator. |  |
| **Application control** | ML1-AC-01 | Application control is implemented on workstations. | Check whether an in-built or third-party application control solution has been implemented for workstations. |  |
| ML1-AC-02 | Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients. | If a path-based approach is used for application control, check that it covers user profiles and temporary folders used by operating systems, web browsers and email clients. Note, hash-based and publisher-based approaches are system-wide and automatically meet the intent of this control. |  |
| ML1-AC-03 | Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set. | Compare the application control policy to the organisation’s approved set of applications. Confirm the application control policy is functioning as expected by using ACVT.  E8MVT can be used to perform limited (single folder) testing for file execution in user profiles and temporary directories.  The tester should attempt to execute a benign executable (EXE or COM) file inside of the user profile directory. The tester should be aware that subfolders within the user profile may have different behaviour depending on the configuration.  The tester should attempt to execute a benign software library (DLL or OCX) file inside of the user profile directory. The tester should be aware that subfolders within the user profile may have different behaviour depending on the configuration.  The tester should attempt to execute multiple benign script (PS, VBS, BAT or JS) files inside of the user profile directory. The tester should be aware that subfolders within the user profile may have different behaviour depending on the configuration.  The tester should attempt to execute a benign installer (MSI, MST or MSP) file inside of the user profile directory. The tester should be aware that subfolders within the user profile may have different behaviour depending on the configuration.  The tester should attempt to execute a benign compiled HTML (CHM) file inside of the user profile directory. The tester should be aware that subfolders within the user profile may have different behaviour depending on the configuration.  The tester should attempt to execute a benign HTML application (HTA) file inside of the user profile directory. The tester should be aware that subfolders within the user profile may have different behaviour depending on the configuration.  The tester should attempt to execute a benign control panel applet (CPL) file inside of the user profile directory. The tester should be aware that subfolders within the user profile may have different behaviour depending on the configuration. |  |
| **Restrict Microsoft Office macros** | ML1-RM-01 | Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. | Run RSOP on workstations to identify the Microsoft Office macro security settings applied by group policy settings. This should typically be set to ‘Disable without notification’. Note ‘Disable with notification’ (the default setting) allows users to bypass this control and does not meet the intent. Check for Active Directory security groups that enforce Microsoft Office macro blocking.  Test running Microsoft Office macros on a user in the disallowed group. E8MVT will attempt to execute a Microsoft Office macro within a document.  Confirm a list of approved users who can execute Microsoft Office macros is maintained and matches the technical implementation. Typically, this means the Active Directory Security Group that permits Microsoft Office macro use should match the list of users who have been approved to run Microsoft Office macros. |  |
| ML1-RM-02 | Microsoft Office macros in files originating from the internet are blocked. | Check if the following group policy setting is enabled. Do this for all installed Microsoft Office applications that can execute macros.  *User Configuration/Policies/Administrative Templates/Microsoft <Application><Version>/Application Settings/Security/Trust Center/Block macros from running in Office files from the internet*  Check if the following registry value exists and is set to 1. Do this for all installed Microsoft Office applications.  *Computer\HKCU\SOFTWARE\Policies\Microsoft\office\<version>\<Application>\security\blockcontentexecutionfromInternet*  E8MVT will check that these registry settings are configured to the correct setting. |  |
| ML1-RM-03 | Microsoft Office macro antivirus scanning is enabled. | Check if the following group policy setting is enabled for all Microsoft Office applications.  *User Configuration/Policies/Administrative Templates/Microsoft Office <Version>/Security Settings/Macro Runtime Scan Scope*  E8MVT will check the registry to confirm that the policy setting is configured.  Attempt to run a pseudo malicious Microsoft Office macro that contains an EICAR test string. E8MVT will open a test file containing a Microsoft Office macro that will write the EICAR test string to a file. |  |
| ML1-RM-04 | Microsoft Office macro security settings cannot be changed by users. | Open Microsoft Office applications and attempt to change the Microsoft Office macro security settings in the Trust Center. |  |
| **User application hardening** | ML1-AH-01 | Internet Explorer 11 is disabled or removed. | E8MVT will perform a check of the group policy setting to disable Internet Explorer 11. In addition, check that the folder containing Internet Explorer 11 in Program Files and Program Files (x86) has been removed and that the iexplore.exe binary does not exist on the system.  E8MVT will check for the existence of the iexplore.exe binary in Program Files locations*.*  Note, even in Microsoft Windows 11, the iexplore.exe binary may still exist and various methods can be used to open Internet Explorer 11 as a standalone browser. To prevent this from occurring, either the iexplore.exe binary should be removed or an application control block rule implemented to block its execution. |  |
| ML1-AH-02 | Web browsers do not process Java from the internet. | Load a website in Microsoft Edge with known Java content and check if it renders in the web browser. Check the following registry keys.  *HKLM:\SOFTWARE\Oracle\JavaDeploy\WebDeployJava*  *HKLM:\SOFTWARE\JavaSoft\Java Plug-in\*  Alternatively, the following PowerShell commands can be used.  *Get-ItemProperty -Path "HKLM:\SOFTWARE\Oracle\JavaDeploy\WebDeployJava"*  *Get-ItemProperty -Path "HKLM:\SOFTWARE\JavaSoft\Java Plug-in"*  Load a website in Google Chrome with known Java content and check if it renders in the web browser.  Load a website in Mozilla Firefox with known Java content and check if it renders in the web browser. |  |
| ML1-AH-03 | Web browsers do not process web advertisements from the internet. | Load the Can You Block It? website in Microsoft Edge.  Load the Can You Block It? website in Google Chrome.  Load the Can You Block It? website in Mozilla Firefox. |  |
| ML1-AH-04 | Web browser security settings cannot be changed by users. | Check that group policy settings are configured for Microsoft Edge. Open the web browser configuration panel and look for existence of a ‘Managed by organisation’ message or similar. Attempt to change a security-related setting.  Check that group policy settings are configured for Google Chrome. Open the web browser configuration panel and look for existence of a ‘Managed by organisation’ message or similar. Attempt to change a security-related setting.  Check that group policy settings are configured for Mozilla Firefox. Open the web browser configuration panel and look for existence of a ‘Managed by organisation’ message or similar. Attempt to change a security-related setting. |  |
| **Regular backups** | ML1-RB-01 | Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements. | Request the current business continuity plan (BCP). Note when the BCP was last modified as old BCPs often don’t reference the current environment. Confirm the organisation has a defined list of data, applications and settings.  Verify data, applications and settings are backed up and retained in accordance with business criticality and business continuity requirements. |  |
| ML1-RB-02 | Backups of data, applications and settings are synchronised to enable restoration to a common point in time. | Verify data, applications and settings are backed up in a synchronised manner using a common point in time. |  |
| ML1-RB-03 | Backups of data, applications and settings are retained in a secure and resilient manner. | Verify data, applications and settings are backed up and retained in a secure and resilient manner. |  |
| ML1-RB-04 | Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises. | Verify the organisation has conducted a disaster recovery exercise. Verify the organisation has successfully restored data, applications and settings as part of this exercise. Confirm the existence of a disaster recovery plan (DRP) and ensure it is appropriate, relevant and followed during major cyber security incidents and exercises. |  |
| ML1-RB-05 | Unprivileged accounts cannot access backups belonging to other accounts. | Verify access controls restrict access to backups to only the owner of the backup and privileged accounts. |  |
| ML1-RB-06 | Unprivileged accounts are prevented from modifying and deleting backups. | Verify access controls restrict the modification and deletion of backups to only privileged accounts. |  |