Example Essential Eight Assessment Test Plan – Maturity Level One

Mitigation Strategy	Control Description	Test ID	Test Description	Test Methodology	Test Findings
Application control	The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.	ML1-AC-01	(Workstations) Executable files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	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. ACVT can perform path enumeration tests to assist in identifying locations within the user directories that can execute executable files. E8MVT will perform limited testing for file execution in user profiles and temporary directories.	
		ML1-AC-02	(Workstations) Software library files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	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. E8MVT will perform limited (single folder) testing for file execution in user profiles and temporary directories.	
		ML1-AC-03	(Workstations) Script files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	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. E8MVT will perform limited (single folder) testing for file execution in user profiles and temporary directories.	
		ML1-AC-04	(Workstations) Installer files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	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. E8MVT will perform limited (single folder) testing for file execution in user profiles and temporary directories.	
		ML1-AC-05	(Workstations) Compiled HTML files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	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. E8MVT will perform limited (single folder) testing for file execution in user profiles and temporary directories.	
		ML1-AC-06	(Workstations) HTML applications files in the user profile directory and temporary folders used by the operating system, web browsers and email clients, cannot execute by a standard user.	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. E8MVT will perform limited (single folder) testing for file execution in user profiles and temporary directories.	
		ML1-AC-07	(Workstations) Control panel applet files in the user profile directory and temporary folders used by the operating system,	The tester should attempt to execute a benign control panel applet (CPL) file inside of the user profile directory. The tester	

			web browsers and email clients, cannot execute by a standard user.	should be aware that subfolders within the user profile may have different behaviour depending on the configuration. E8MVT will perform limited (single folder) testing for file execution in user profiles and temporary directories.	
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	ML1-PA-01	An automated method of asset discovery is run and reviewed at least fortnightly.	Confirm that a method of asset discovery is in place (such as an asset discovery tool or a vulnerability scanner with equivalent functionality) and that it is configured to be run in an automated manner at least every fortnight. Confirm that any anomalies that are identified are reviewed and actioned.	
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	ML1-PA-02	A vulnerability scanner with an up-to-date vulnerability database is being used for vulnerability scanning activities.	Confirm that a vulnerability scanner is in place and that the vulnerability database it uses is being updated within 24 hours prior to its use.	
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in internet-facing services.	ML1-PA-03	(Internet-Facing Services) A vulnerability scanner for internet-facing services is run and reviewed daily.	Confirm that a vulnerability scanner is in place, and it is configured to scan the organisation's internet-facing services. Confirm that reports from the vulnerability scanner are reviewed by the responsible staff daily, and that identified issues have been observed and actioned.	
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	ML1-PA-04	A vulnerability scanner is run and reviewed at least fortnightly to scan the organisation's office productivity suites, web browsers, email clients, PDF software and security products.	Confirm that a vulnerability scanner is in place, and it is configured to scan the organisation's applications listed, typically requiring a credentialed scan. Confirm that reports from the vulnerability scanner are reviewed by the responsible staff fortnightly, and that identified issues have been observed and actioned.	
	Patches, updates or other vendor mitigations for vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.	ML1-PA-05	(Internet-Facing Services) The organisation has a process for identifying vulnerabilities in internet-facing services within 48 hours and has an example of where an available exploit has been identified and patched within 48 hours.	Review the process in place for identifying vulnerabilities in internet-facing systems. Request evidence of the identification and patching of a system that contained an exploitable vulnerability within the environment.	
		ML1-PA-06	(Internet-Facing Services) Applications with an exploit that has been available for greater than 48 hours are patched or mitigated.	Use a vulnerability scanner to identify applications within the environment and check that they have been patched against a known exploit. Determine the date the patch was installed and compare to when the patch was made available.	
		ML1-PA-07	(Internet-Facing Services) Applications are patched or mitigated within two weeks.	Use a vulnerability scanner to identify applications within the environment and check that they have been patched against a known exploit. Determine the date the patch was installed and compare to when the patch was made available.	
	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions,	ML1-PA-08	The organisation has an effective process for patching office productivity suites, web browsers, email clients, PDF software and security products within one month.	Confirm the existence of a list of applications, and where the applications are installed. Ensure a process for identifying vulnerabilities for software in the list is consistently followed. Request evidence of the patching of these applications within one month.	

	email clients, PDF software, and security products are applied within one month of release.	ML1-PA-09	Office productivity suites, web browsers, email clients, PDF software and security products do not have vulnerabilities older than one month.	Use a vulnerability scanner to identify the listed applications within the organisation's environment, and check that they have been patched against a known exploit. Check the date the application was updated and compare to the date the patch was released. Ensure that the gap between is not greater than one month. E8MVT will perform basic checks of some Microsoft Office applications based on version numbers and file modification dates to determine if the software has been updated recently.	
	Internet-facing 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.	ML1-PA-10	The organisation has removed unsupported internet-facing services from the environment.	Confirm that the environment does not contain software on internet-facing systems that is no longer supported by the vendor. Use a vulnerability scanner to identify applications within the environment and check they are supported.	
		ML1-PA-11	The organisation has removed unsupported office productivity suites, web browsers, email clients, PDF software and security products from the environment.	Confirm that the environment does not contain any of the listed software that is no longer supported by the vendor. Use a vulnerability scanner to identify applications within the environment and check they are supported.	
Configure Microsoft Office macro settings	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	ML1-OM-01	A technical solution exists that blocks Microsoft Office macros for users who are not approved under the Microsoft Office macro policy.	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' 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.	
		ML1-OM-02	A record is kept of users that have been approved to allow Microsoft Office macro execution, and this list matches the list of users within the technical solution.	Confirm a repository of approved requests for users to execute Microsoft Office macros is maintained and up to date 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.	
	Microsoft Office macros in files originating from the internet are blocked.	ML1-OM-03	Microsoft Office files from the internet are unable to execute Microsoft Office macros.	Attempt to run Microsoft Office macros in Microsoft Office files from the internet. Confirm these files are blocked when received by download and email. Do this for all installed Microsoft Office applications. E8MVT will open a test file that contains a zone identifier to indicate it is from the internet.	
		ML1-OM-04	Microsoft Office has been configured to block Microsoft Office macros from running in Microsoft Office files from the internet.	Check if the following group policy setting is enabled. Do this for all installed Microsoft Office applications *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\HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\office\<version>\<Application>\security\blockcontentexecutionfromInternet. E8MVT will check that these registry settings are configured to the correct setting. *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\<version>\<application>\security\" | Select-Object -Property blockcontentexecutionfromInternet* Example: *Get-ItemProperty -Path "HKCU:\SOFTWARE\Policies\Microsoft\office\16.0\excel\security\" | Select-Object -Property blockcontentexecutionfromInternet*	
	Microsoft Office macro antivirus scanning is enabled.	ML1-OM-05	The system has macroruntimescope enabled for Microsoft Office applications in registry settings or has an alternative Microsoft Office macro scanning ability in place.	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.	
		ML1-OM-06	System anti-virus successfully detects a virus test signature inside of a Microsoft Office macro in a Microsoft Office file.	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.	
	Microsoft Office macro security settings cannot be changed by users.	ML1-OM-07	A standard user is unable to modify the security settings for Microsoft Office macros in all Microsoft Office applications.	Open the application and attempt to change the Microsoft Office macro security settings in the Trust Center. Do this for all installed Microsoft Office applications.	
User application hardening	Web browsers do not process Java from the internet.	ML1-AH-01	Java content does not execute in Microsoft Edge.	Load a website with known Java content and check if it renders in the web browser. Check the registry keys at *HKLM:\SOFTWARE\Oracle\JavaDeploy\WebDeployJava* and *HKLM:\SOFTWARE\JavaSoft\Java Plug-in*. *Get-ItemProperty -Path "HKLM:\SOFTWARE\Oracle\JavaDeploy\WebDeployJava"* *Get-ItemProperty -Path "HKLM:\SOFTWARE\JavaSoft\Java Plug-in"*	
		ML1-AH-02	Java content does not execute in Google Chrome.	Load a website with known Java content and check if it renders in the web browser.	
		ML1-AH-03	Java content does not execute in Mozilla Firefox.	Load a website with known Java content and check if it renders in the web browser.	
	Web browsers do not process web advertisements from the internet.	ML1-AH-04	Web ads do not display in Microsoft Edge.	Load a website in Microsoft Edge with known ads and check if it renders in the web browser. Check the 'Block ads on sites that show intrusive or misleading ads' setting is configured. Check if any ad blocking plugins are configured in the web browser.	

		ML1-AH-05	Web ads do not display in Google Chrome.	Load a website in Google Chrome with known ads and check if it renders in the web browser. Check the ‘Block ads on sites that show intrusive or misleading ads’ setting is configured. Check if any ad blocking plugins are configured in the web browser.	
		ML1-AH-06	Web ads do not display in Mozilla Firefox.	Load a website in Mozilla Firefox with known ads and check if it renders in the web browser. Check if any ad blocking plugins are configured in the web browser.	
	Internet Explorer 11 does not process content from the internet.	ML1-AH-07	Internet Explorer 11 is unable to connect to internet sites. Internet Explorer 11 may be allowed to access internal web applications only.	If Internet Explorer 11 is installed, access an external website using the web browser and ensure it is blocked. If it is not installed, use a manual request method (script, curl, proxy) with modified request headers to imitate IE (e.g. User-Agent) and check if the request is blocked. Review proxy or firewall configuration for the existence of rules to prevent IE specific browsing from reaching the internet.	
	Web browser security settings cannot be changed by users.	ML1-AH-08	Microsoft Edge settings cannot be changed by a standard user.	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 setting related to networking or security, such as blocking of ads, proxy settings or security level.	
		ML1-AH-09	Google Chrome settings cannot be changed by a standard user.	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 setting related to networking or security, such as blocking of ads, proxy settings or security level.	
		ML1-AH-10	Mozilla Firefox settings cannot be changed by a standard user.	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 setting related to networking or security, such as blocking of ads, proxy settings or security level.	
		ML1-AH-11	Internet Explorer 11 settings cannot be changed by a standard user.	Check that group policy settings are configured for Internet Explorer 11. Open the web browser configuration panel and look for existence of a ‘Managed by organisation’ message or similar. Attempt to change a setting related to networking or security, such as blocking of ads, proxy settings or security level.	
Restrict administrative privileges	Requests for privileged access to systems and applications are validated when first requested.	ML1-RA-01	A process exists and is enforced for granting privileged access to systems.	Confirm the organisation has a documented, approved and enforced privileged access process that outlines the requirements for provisioning a privileged account to a system or application. Confirm the organisation has a list of systems and applications that require privileged access. Review documented privileged access process and systems. Request evidence of process being followed (e.g. support tickets).	

	Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services.	ML1-RA-02	Privileged accounts (excluding privileged service accounts) cannot access the internet or web services via a web browser or other mechanism.	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. While privileged account policies should be reviewed, they do not satisfy this control without additional technical mechanisms.	
		ML1-RA-03	Privileged accounts are not configured with mailboxes and email addresses.	Attempt to open Microsoft Outlook on a system using the privileged account. Run the following PowerShell command *Get-ADUser -Filter {(admincount -eq 1) -and (emailaddress -like "*") -and (enabled -eq $true)} -Properties EmailAddress | Select samaccountname, emailaddress*	
	Privileged users use separate privileged and unprivileged operating environments.	ML1-RA-04	All administrative activities are performed in an administrative environment that is segmented from the standard user network environment. A separate environment is provisioned for the use of privileged access and is not used for any other purpose.	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. Check for the existence of workstations that exist solely for privileged access purposes. The privileged operating environment must not be virtualised within the unprivileged operating environment for Maturity Level Two or Maturity Level Three. However, it can be for Maturity Level One.	
	Unprivileged accounts cannot logon to privileged operating environments.	ML1-RA-05	Unprivileged accounts are not able to logon to systems in the privileged environment.	Use Bloodhound to analyse Active Directory data and look for which users and groups have RDP access to servers. Review group policy settings for RDP permissions.	
		ML1-RA-06	Unprivileged user prevented from using the PowerShell remote PSRemote windows feature.	Run the following PowerShell command *(Get-PSSessionConfiguration -Name Microsoft.PowerShell).Permission* Check the members of the built-in Active Directory Security Group Remote Management Users.	
	Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	ML1-RA-07	A privileged account cannot be used to authenticate and interactively login to standard user workstations, or other unprivileged environments. Limited-permission administrative accounts can be used to meet business requirements in unprivileged environments, such as for help desk personnel.	Attempt to login with a privileged account 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. Limited-permission administrative accounts can be used to meet business requirements in unprivileged environments, such as for help desk personnel. These accounts should not be highly privileged. Review list of administrative users who can login to unprivileged environments. None of the users should be highly privileged, for example Domain Administrators. These users should not be able to access the privileged environment.	

		ML1-RA-08	An unprivileged account logged into a standard user workstation cannot raise privileges to a privileged user.	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.	
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.	ML1-PO-01	An automated method of asset discovery is run and reviewed at least fortnightly.	Confirm that a method of asset discovery is in place (such as an asset discovery tool or a vulnerability scanner with equivalent functionality) and that it is configured to be run in an automated manner at least every fortnight. Confirm that any anomalies that are identified are reviewed and actioned.	
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	ML1-PO-02	A vulnerability scanner with an up-to-date vulnerability database is being used for vulnerability scanning activities.	Confirm that a vulnerability scanner is in place and that the vulnerability database it uses is being updated within 24 hours prior to its use.	
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing services.	ML1-PO-03	A vulnerability scanner is run and reviewed daily to scan the organisation’s internet-facing services.	Confirm that a vulnerability scanner is in place, and it is configured to scan the organisation’s internet-facing services. Confirm that reports from the vulnerability scanner are reviewed by the responsible staff daily, and that identified issues have been observed and actioned.	
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, servers and network devices.	ML1-PO-04	A vulnerability scanner is run and reviewed at least fortnightly to scan the organisation’s operating systems.	Confirm that a vulnerability scanner is in place, and it is configured to scan the organisation’s operating systems, typically requiring a credentialed scan. Confirm that reports from the vulnerability scanner are reviewed by the responsible staff fortnightly, and that identified issues have been observed and actioned.	
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.	ML1-PO-05	The organisation has an example of where an available exploit has been identified and patched within 48 hours.	If available, request evidence of the identification and patching of a system that contained an exploitable vulnerability within the environment.	
		ML1-PO-06	Internet-facing system that have a vulnerable operating system with an exploit that has been available for greater than 48 hours are patched or mitigated.	View vulnerability management solution, logon to server to verify patch applied successfully or review mitigation strategy. E8MVT will assesses based on most recently installed critical patch. Does not test for existing exploits or 48-hour timeframe requirements.	
		ML1-PO-07	Internet-facing systems that have a vulnerable operating system are patched or mitigated within two weeks.	Use vulnerability management solution to perform a patch audit of servers. Retrieve the update history of the workstation, noting the release date of the patch and the date it was installed. Look for differences greater than two weeks.	
	Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, servers	ML1-PO-08	The organisation has an effective process for patching operating systems within one month.	Confirm the existence of a list of managed operating systems, and where they are located. Ensure a process for identifying vulnerabilities for operating systems in the list is consistently followed. Request evidence of the patching of these systems within one month.	

	and network devices are applied within one month of release.	ML1-PO-09	Operating systems that have a vulnerability are patched or mitigated within one month.	Use a vulnerability management solution to perform a patch audit of all systems. Retrieve the update history of the systems in scope, noting the release date of the patch and the date it was installed. Look for differences greater than one month.	
	Operating systems that are no longer supported by vendors are replaced.	ML1-PO-10	The organisation has removed unsupported operating systems from the environment.	Confirm that the environment does not contain any operating systems no longer supported by the vendor. Use a vulnerability scanner to identify operating systems within the environment and check they are supported.	
Multi-factor authentication	Multi-factor authentication is used by an organisation's users when they authenticate to their organisation's internet-facing services.	ML1-MF-01	The organisation has a verified and approved list of internet-facing services operating within the organisation.	Confirm an approved list of internet-facing services exists and this list is regularly checked.	
		ML1-MF-02	The organisational remote access desktop solution presents a MFA challenge when attempting to authenticate.	Verify the user is presented with a MFA challenge when authenticating to the organisation's remote solution.	
		ML1-MF-03	Organisational internet-facing systems present a MFA challenge when attempting to authenticate.	Verify the user is presented with a MFA challenge when authenticating to the organisation's internet-facing systems.	
	Multi-factor authentication is used by an organisation's users when they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.	ML1-MF-04	Third-party internet-facing services that hold sensitive data are configured to require users to use MFA.	Verify the organisation's sensitive third-party internet-facing services are configured with MFA. Confirm the organisation has a policy that MFA will be implemented on all third-party internet-facing services that hold sensitive data.	
	Multi-factor authentication (where available) is used by an organisation's users when they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.	ML1-MF-05	Third-party internet-facing services that hold non-sensitive data are configured to require users to use MFA.	Verify the organisation's third-party internet-facing services are configured with MFA. Confirm the organisation has a policy that MFA will be implemented on all third-party internet-facing services that hold non-sensitive data.	
	Multi-factor authentication is enabled by default for an organisation's non-organisational users (but they can choose to opt out) when they authenticate to the organisation's internet-facing services.	ML1-MF-06	The organisational internet-facing services with non-organisational user presents a multi-factor challenge when attempting to authenticate by default.	Verify non-organisational users are presented with a MFA challenge when accessing organisational systems by default. Users may elect to opt out of this feature.	
Regular backups	Backups of important data, software and configuration settings are performed and retained with a frequency and	ML1-RB-01	The organisation has a business continuity plan (BCP) that outlines their important data, software and configuration settings that require backing up.	Request the current 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 important data, software and configuration settings.	

	retention timeframe in accordance with business continuity requirements.	ML1-RB-02	Important data, software and configuration settings are backed up and retained as per the timeframes outlined within the BCP.	Verify important data, software and configuration settings are backed up and retained in accordance with the BCP.	
	Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time.	ML1-RB-03	Important data, software and configuration settings are backed up in a synchronised manner using a common point in time.	Verify important data, software and configuration settings are backed up in a synchronised manner using a common point in time.	
	Backups of important data, software and configuration settings are retained in a secure and resilient manner.	ML1-RB-04	Important data, software and configuration settings are backed up and retained in a secure and resilient manner.	Verify important data, software and configuration settings are backed up and retained in a secure and resilient manner.	
	Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises.	ML1-RB-05	The organisation has documented evidence of a disaster recovery exercise being performed. This includes examples of where important data, software and configuration settings have been restored from backups.	Verify the organisation has conducted a disaster recovery exercise. Verify the organisation has successfully restored important data, software and configuration settings as part of this exercise. Confirm the existence of a disaster recovery plan (DRP), and ensure it is appropriate, relevant, and followed during incidents and exercises.	
	Unprivileged accounts cannot access backups belonging to other accounts.	ML1-RB-06	Unprivileged users are unable to access backups that do not belong to them.	Verify access controls restrict access to only the owner of the information.	
	Unprivileged accounts are prevented from modifying and deleting backups.	ML1-RB-07	Unprivileged users are unable to modify and delete backups.	Verify access controls restrict the modification and deletion of backups.	