Essential 8 Maturity Model

ACSC
Australian
Cyber Security
Centre

Essential 8 Maturity Model Version October 2021

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies, in the form of the Strategies to Mitigate Cyber Security Incidents, to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight.

To assist organisations in determining the maturity of their implementation of the Essential Eight, three maturity levels have been defined for each mitigation strategy. The maturity levels are defined as:

- **Maturity Level One:** Partly aligned with the intent of the mitigation strategy
- **Maturity Level Two:** Mostly aligned with the intent of the mitigation strategy
- **Maturity Level Three:** Fully aligned with the intent of the mitigation strategy

As a baseline organisations should aim to reach Maturity Level Three for each mitigation strategy. Where the ACSC believes an organisation requires a maturity level above that of Maturity Level Three, the ACSC will provide tailored advice to meet the specific needs of the organisation.

Mitigation Strategy	Maturity Level 1	Maturity Level 2	Maturity Level 3	Exclaimer Statement
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	Application control is implemented on workstations and internet-facing servers to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set. Allowed and blocked executions on workstations and internet-facing servers are logged.	Application control is implemented on workstations and servers to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers to an organisation-approved set. Microsoft's 'recommended block rules' are implemented. Microsoft's 'recommended driver block rules' are implemented. Application control rulesets are validated on an annual or more frequent basis. Allowed and blocked executions on workstations and servers are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	Exclaimer operate an application whitelist and admin control policy to restrict the applications which are able to run on workstations and servers. We also operate conditional access to block rooted devices. Where we are able we use defender to block the applications and drivers from their recommended lists. Some applications such as WSL.exe are required in limited use on workstations and are therefore allowed. As part of our annual access review we also review our application lists to ensure that they are relevant, up to date and complete. All activities on servers are centrally logged, these logs are analysed in real time by our automated security monitoring tool. If the tool detects a security issue the on-call team is alerted.

Mitigation Strategy	Maturity Level 1	Maturity Level 2	Maturity Level 3	Exclaimer Statement
Patch applications	Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release. A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. 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.	Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release. Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month. A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications. 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.	Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month. A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications. Applications that are no longer supported by vendors are removed.	Exclaimer operate a number of different programs in parallel to manage patching. We operate automatic package management tools to both automatically upgrade packages consumed by our application. At every PR we scan the code for vulnerabilities including OWASP T10 and SANS T25, this way we ensure that there are no known vulnerabilities within our production code. Further to this we also scan the currently released artifacts daily for the same vulnerabilities, this ensures that if a zero-day vulnerability is detected we do not need to wait for a PR to identify it. Critical vulnerabilities are aimed to be remediated within 48h, High within 14 days, Medium within 90 days.

Mitigation Strategy	Maturity Level 1	Maturity Level 2	Maturity Level 3	Exclaimer Statement
Configure Microsoft Office macro settings	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. Microsoft Office macros in files originating from the internet are blocked. Microsoft Office macro antivirus scanning is enabled. Microsoft Office macro security settings cannot be changed by users	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. Microsoft Office macros in files originating from the internet are blocked. Microsoft Office macro antivirus scanning is enabled. Microsoft Office macros are blocked from making Win32 API calls. Microsoft Office macro security settings cannot be changed by users. Allowed and blocked Microsoft Office macro executions are logged.	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute. Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations. Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View. Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis. Microsoft Office macros in files originating from the internet are blocked. Microsoft Office macro antivirus scanning is enabled. Microsoft Office macros are blocked from making Win32 API calls. Microsoft Office macro security settings cannot be changed by users. Allowed and blocked Microsoft Office macro executions are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	Exclaimer's application whitelist and admin control system also controls the enablement and running of Office macros. This technical policy stops users from running un-approved, unsigned or un-trusted macros. Exclaimer's macro whitelist is controlled using a group to allow users who have a business requirement to be excluded, this group is reviewed as part of our access review policy. Our system logs any attempts for macros to be run and sends these logs to our IT team for review.

Mitigation Strategy	Maturity Level 1	Maturity Level 2	Maturity Level 3	Exclaimer Statement
User application hardening	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 does not process content from the internet. Web browser security settings cannot be changed by users.	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 does not process content from the internet. Microsoft Office is blocked from creating child processes. Microsoft Office is blocked from creating executable content. Microsoft Office is blocked from injecting code into other processes. Microsoft Office is configured to prevent activation of OLE packages. PDF software is blocked from creating child processes. ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented. Web browser, Microsoft Office and PDF software security settings cannot be changed by users. Blocked PowerShell script executions are logged.	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 is disabled or removed. Microsoft Office is blocked from creating child processes. Microsoft Office is blocked from creating executable content. Microsoft Office is blocked from injecting code into other processes. Microsoft Office is configured to prevent activation of OLE packages. PDF software is blocked from creating child processes. A CSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented. Web browser, Microsoft Office and PDF software security settings cannot be changed by users. .NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed. Windows PowerShell 2.0 is disabled or removed. PowerShell is configured to use Constrained Language Mode. Blocked PowerShell script executions are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected	Exclaimer's application blocking policy excludes all unapproved software from executing on workstations, we specifically block all software from running unless it is being executed from a specifically allowed path. This includes blocking any processes which start to run from temp. We only allow users to install a subset of approved browsers and ensure via automated deployments that these are up to date and secure. We harden our operating systems however the security hardened OS is not benchmarked. While it overlaps with CIS benchmarks, the goal is not to be CIS-compliant Our system logs any attempts for blocked applications to be run and sends these logs to our IT team for review.

Mitigation Strategy	Maturity Level 1	Maturity Level 2	Maturity Level 3	Exclaimer Statement
Restrict administrative privileges	Requests for privileged access to systems and applications are validated when first requested. Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Requests for privileged access to systems and applications are validated when first requested. Privileged access to systems and applications is automatically disabled after 12 months unless revalidated. Privileged access to systems and applications is automatically disabled after 45 days of inactivity. Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Privileged operating environments are not virtualised within unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. Administrative activities are conducted through jump servers. Credentials for local administrator accounts and service accounts are unique, unpredictable and managed. Use of privileged access is logged. Changes to privileged accounts and groups are logged	Requests for privileged access to systems and applications are validated when first requested. Privileged access to systems and applications is automatically disabled after 12 months unless revalidated. Privileged access to systems and applications is automatically disabled after 45 days of inactivity. Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties. Privileged accounts are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Privileged operating environments are not virtualised within unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. Just-in-time administration is used for administering systems and applications. Administrative activities are conducted through jump servers. Credentials for local administrator accounts and service accounts are unique, unpredictable and managed. Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled. Use of privileged access is centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected. Changes to privileged accounts and groups are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	Exclaimer's IT control system is tightly linked to our HR systems to ensure that users are created and removed quickly as they start /leave. We also integrate heavily with SSO in order to ensure that there are a limited number of privileged logins to manage, this simplifies credential management, MFA and onboard /offboard. All privileged systems are controlled in this manner. Access to privileged systems is authorised as part of our change approval process - in the same manner to if a deployment of new code was being made to production - and must be approved by management. We complete at least a twice annual access review to ensure that the privileged access provided is still relevant and required. Any access which is deemed not to meet these requirements is removed. Access to machines is controlled through user specific administration accounts and provided through the use of jump boxes. with MFA enforced. Exclaimer store passwords using 1password vaults, the access for which is provided as though it were itself a privileged system. All admin logins and admin changes are logged and recorded, with sign-ins being sent to our log management and security monitoring tool - with security events being sent to our on-call team for investigation.

Mitigation Strategy	Maturity Level 1	Maturity Level 2	Maturity Level 3	Exclaimer Statement
Patch operating systems	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release. A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least fortnightly to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices. Operating systems that are no longer supported by vendors are replaced.	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release. A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices. Operating systems that are no longer supported by vendors are replaced.	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release, or within 48 hours if an exploit exists. A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices. The latest release, or the previous release, of operating systems are used for workstations, servers and network devices. Operating systems that are no longer supported by vendors are replaced.	Exclaimer operate a monthly standard patching cadence with vendor updates applied to all systems once per month. We update our pre-prod environment 1 week before production to ensure reliability, we also upgrade our 2 datacenters on separate days to further ensure that any potential instability introduced during patching is limited in scope. Any critical or zero-day vulnerabilities are treated as hotfixes and deployed within 48h. We partner with Microsoft Premier Support in order to get the latest Microsoft security information to help inform our patch management policy (for both Microsoft OS and Linux distributions provided by Microsoft) All systems are configured using centrally defined standards and deployed using Terraform and hardened images.

Mitigation Strategy	Maturity Level 1	Maturity Level 2	Maturity Level 3	Exclaimer Statement
Multi-facttor authentication	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services. Multi-factor authentication is used by an organisation's users if they authenticate to thirdparty internet-facing services that process, store or communicate their organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services.	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services. Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services. Multi-factor authentication is used to authenticate privileged users of systems. Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are. Successful and unsuccessful multi-factor authentications are logged.	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services. Multi-factor authentication is used by an organisation's users if they authenticate to thirdparty internet-facing services that process, store or communicate their organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services. Multi-factor authentication is used to authenticate privileged users of systems. Multi-factor authentication is used to authenticate users accessing important data repositories. Multi-factor authentication is verifier impersonation resistant and uses either: something users have and something users know, or something users have that is unlocked by something users know or are. Successful and unsuccessful multi-factor authentications are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	Exclaimer rely heavily on SSO in order to ensure that there are a limited number of privileged logins to manage, this simplifies credential management, MFA and onboard / offboard. All privileged systems are controlled in this manner. Any system which is able to be integrated with our identity provider is linked which forces MFA. Any system which cannot be integrated, but that offers 2FA is forced on - this is a process managed and controlled by our Internal IT team. All logins are tracked within our identity provider, signins are continuously monitored for 'risky signins' and reports are delivered to admins weekly.

Mitigation Strategy	Maturity Level 1	Maturity Level 2	Maturity Level 3	Exclaimer Statement
Regular backups	Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements. Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises. Unprivileged accounts can only access their own backups. Unprivileged accounts are prevented from modifying or deleting backups.	Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements. Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises. Unprivileged accounts, and privileged accounts (excluding backup administrators), can only access their own backups. Unprivileged accounts, and privileged accounts (excluding backup administrators), are prevented from modifying or deleting backups.	Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements. Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises. Unprivileged accounts, and privileged accounts (excluding backup administrators), cannot access backups. Unprivileged accounts, and privileged accounts (excluding backup break glass accounts), are prevented from modifying or deleting backups.	Exclaimer backup our customer signature and configuration data in a point-in-time manner. This means that we are able to restore back to any singular 5 minute window in the past 35 days. Backups are monitored and the on-call team are notified if there are failures which need to be investigated. Exclaimer also replicate our data between two regional datacenters, this occurs every 5s to ensure consistency. Both datacenters are hot and process mail. Our DR process to fail over between these two sites is tested at least every 6 months but in reality this occurs during most releases to ensure reliability of service. Access to the backups are limited to privileged users with access to the management system which is controlled through our change management policy.