Privasec GRC
GOVERNANCE
AND INFORMATION
SECURITY PARTNERS

ACSC Essential Eight Assessment Services

A CISO's Thoughts, by Prashant Haldankar, Privasec's CISO

Australian Cyber Security Centre's (ACSC) Strategy to Mitigate Cyber Security Incidents provides a prioritised list of mitigation strategies to assist organisations in protecting their systems and their crown jewels against a range of adversaries. The mitigation strategies advised by ACSC vary and can be customised based on the risk profile, the industry sector and the adversaries the organisation is most concerned with.

The Essential Eight

While all organisations operate differently and have different risk profiles, no single mitigation strategy is guaranteed to prevent cyber-security incidents from occurring. ACSC's recommendation of implementing the Essential Eight mitigation strategies as a baseline effectively makes it harder for adversaries to compromise systems. ACSC found that an Effective implementation of Essential Eight strategies can mitigate 85% of cyber threats. Proactive approaches to implementing these strategies are cost-effective solutions in terms of time, money and effort than simply being reactive to responding to large scale cyber-security incidents.

NSW Government Cyber Security Policy requires the implementation, amongst others, of the Australian Cyber Security Centre's (ACSC) Essential Eight security controls. The policy requires (Requirement 3.1 and 3.2) an independent annual assessment of all mandatory requirements in the policy for the previous financial year, including a maturity assessment (referred to by Privasec as 'gap and maturity assessment') against the ACSC Essential Eight.

ACSC's recommended implementation order for each adversary can assist organisations in building a strong cyber-security posture for their business and the support systems, which are critical to an organisation's success in delivering business objectives, i.e., no business interruption due to a cyber-security incident.

ASCS Essential Eight Controls and their Importance:

The Essential Eight strategies focus on three key objectives for mitigation strategy. The table below sourced from ACSC explains each of the mitigation strategies, the controls, and the importance of these controls:

Mitigation Strategies to Prevent Malware Delivery and Execution

Application Control to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g., Windows Script Host, PowerShell and HTA) and installers.

Why: All non-approved applications (including malicious code) are prevented from executing.

Configure Microsoft Office Macro Settings to block macros from the internet, and allow only vetted macros either in 'trusted locations' with limited write access or digitally signed in with a trusted certificate.

Why: Microsoft Office macros can be used to deliver and execute malicious code on systems.

Patch Applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.

Why: Security vulnerabilities in applications can be used to execute malicious code on systems.

User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g., OLE), web browsers and PDF viewers.

Why: Flash, ads and Java are popular ways to deliver and execute malicious code on systems.

Mitigation Strategies to Limit the Extent of Cyber-Security Incidents

Restrict Administrative Privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.

Why: Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.

Multi-Factor Authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.

Why: Stronger user authentication makes it harder for adversaries to access sensitive information and systems.

Patch Operating Systems. Patch/mitigate computers (including network devices) with ‘extreme risk’ vulnerabilities within 48 hours. Use the latest operating system version. Don’t use unsupported versions.

Why: Security vulnerabilities in operating systems can be used to further compromise the systems.

Mitigation Strategies to Recover Data and System Availability

Daily Backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.

Why: To ensure information can be accessed following a cyber-security incident (e.g., a ransomware incident).

Effective implementation of these controls is a starting point, and continual improvement to bring maturity is key in keeping up with the changing cyber threat landscape. Once the baseline controls are implemented, organisations should focus on increasing the maturity of their implementation such that they eventually reach full alignment in keeping the intent of each mitigation strategy.

ACSC has defined three maturity levels to assist organisations in determining the maturity of their implementation. The maturity criteria defined in ACSC Maturity Model includes:

- Maturity Level One - Partly aligned with intent of mitigation strategy.
- Maturity Level Two - Mostly aligned with intent of mitigation strategy.
- Maturity Level Three - Fully aligned with intent of mitigation strategy.

Privasec’s ACSC Essential Eight Maturity Assessment Approach

Privasec follows a mature assessment and auditing approach to provide organisations with assurance on its effective alignment with the Essential Eight controls and roadmap to achieve the highest level of maturity.

Our assessment process leverages the people, process, and technology aspects with a combination of advanced auditing tools to provide an objective assessment of risk and compliance to the Essential Eight controls.

Our Assessment adheres to the following steps. A Privasec consultant will be a key part of this process to ensure you achieve the desired outcome:

- Scope Assessment: Validation of the assessment scope and confirmation that the scope and the identified services are appropriately covered by the system components that are defined in the scope. This includes systems and business applications.
- Gap Assessment and Risk Reporting: An initial review of the documentation and technology controls for the in-scope system and applications will be conducted. This includes a gap analysis of people, process and technology control against the Essential Eight's stipulated controls and strategies. Your consultant will keep you updated with any early findings and areas of non-compliance to give you as much time to remediate them as possible.
- We will also conduct an audit leveraging our tools and assessment process to perform an objective measure of cyber-risk exposure and cyber maturity for the in-scope systems and applications.
- A risk-based review of the organisation's IT security processes and supporting technologies and controls to draw a baseline of current compliance and maturity.
- An assessment of the likely effectiveness of the controls in place to protect the organisation against any cyber-security threats.
- Once a clear understanding of the risks impacting an organisation have been identified, the Privasec consultant will work with your process, key stakeholders, and asset owners to:

  A. Identify, at a high level, practical solutions and remediation options,
  B. Create a tailored mitigation approach to effectively reduce risks and align with your business objectives.
  C. Prepare a detailed roadmap to reach the desired maturity level in comparison to the current maturity level.

- Risk Remediation: Your consultant will provide guidance and support during the remediation process to ensure your compliance/risk objectives are met.
- Once the report is finalised, Privasec will prepare and deliver the presentation to your organisation's key stakeholders and to its board (as required). Our presentation will be tailored to the audience and will address business and technical stakeholders.

Deliverables:

Our reports provide a holistic and detailed view of the organisation's current compliance to the Essential Eight, cyber-risk exposure profile and the current maturity. We also deliver a detailed compliance roadmap against each of the mitigation strategies, with recommendations of ways to achieve the highest level of maturity.

These reports form a baseline for the Annual Compliance Reporting and can be used to support the organisation's cyber-security reporting, for example, NSW Cyber Security Policy Annual reporting and attestations submissions to relevant governance bodies including the Cyber Security Senior Officers Group (CSSOG) and the ICT and Digital Leadership Group (IDLG).

Privasec
GRC GOVERNANCE AND INFORMATION SECURITY PARTNERS
RED RED TEAMING & ADVANCED ETHICAL HACKING
DRONE SEC UAS HACKING, HARDENING & DEFENCE

1800 996 001 (AUS)
+65 6631 8375 (SG)
+603 2788 3709 (MY)
+64 9 222 4725 (NZ)

info@privasec.com.au
www.privasec.com

Australia | Level 2, 64 Clarence St, Sydney, NSW 2000
Level 6, 276 Flinders St, Melbourne, VIC 3000
Level 6, 200 Adelaide St, Brisbane, QLD 4000
Singapore | 5 Shenton Way, UIC Building #10-01 Singapore 068808
Malaysia | L9, Unit 3 Wisma UOA II - 6, Changkat Semantan 50490 KL
New Zealand | Level 4, 17 Albert St Auckland 1010