SACSF/G9.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline 9.0 – Essential Eight: Reporting and use in SA Government

Purpose

This guideline sets out the implementation and reporting requirements for the South Australian (SA) Government in relation to the Essential Eight. It also provides guidance and resources to support agencies with their Essential Eight obligations.

Scope

This guideline applies to:

- South Australian Government public sector agencies, that is, administrative units, bodies corporate, statutory authorities and instrumentalities of the Crown as defined in the *Public Sector Act 2009*.
- Suppliers to the SA Government and non-government personnel providing services to agencies.

Background

In response to the growing cyber threat, the Australian Cyber Security Centre (ACSC) has developed a prioritised set of strategies to mitigate cyber security incidents[1] and help organisations protect themselves against various cyber threats. The eight most effective of these strategies are known as the Essential Eight.

The Essential Eight Maturity Model supports the implementation of the Essential Eight, with maturity levels based upon mitigating increasing levels of adversary tradecraft.

The Essential Eight has been designed as a baseline set of mitigation strategies to protect Windows-based internet connected networks. While the principles behind the Essential Eight may be applied to cloud services, enterprise mobility, or other operating systems, it was not primarily designed for such purposes and alternative mitigation strategies may be more appropriate to mitigate unique cyber threats to these environments.[2]

[1] Strategies to Mitigate Cyber Security Incidents | Cyber.gov.au

[2] Essential Eight Explained | Cyber.gov.au

In South Australia , the South Australian Cyber Security Framework (SACSF)[3] is the whole of government, Cabinet approved approach to ensure that cyber security is adequately managed in each SA Government agency. Some of the Essential Eight mitigation strategies are incorporated into the SACSF at high-level.[4]

Reporting

Each year, SA Government agencies are required to complete an attestation on their security maturity and capability against the SACSF expectations. Reporting Essential Eight maturity is included in the attestation process.

Reporting against the Essential Eight Maturity Model provides a strategic benchmark for SA Government, highlighting improvement and training opportunities, areas of risk, and standardising the reporting approach across Commonwealth, state and territory governments, and industry.

Essential Eight adoption by the South Australian Government

While there is no expectation or requirement that agencies meet a certain maturity level against the Essential Eight, target maturity levels should be considered based on the levels of adversary tradecraft and targeting likely for their environment.

As a minimum, it is recommended that agencies plan to achieve Maturity Level One across all mitigation strategies.

Guideline detail

Maturity Levels[5]

The ACSC have defined four levels of maturity to assist with implementation of the Essential Eight (Maturity Level Zero through to Maturity Level Three). Except for Maturity Level Zero, the levels are based on mitigating increasing levels of adversary tradecraft (i.e., tools tactics, techniques, and procedures).

The ACSC generally recommends that Maturity Level One may be suitable for small to medium enterprises, Maturity Level Two may be suitable for large enterprises, Maturity Level Three may be suitable for critical infrastructure providers and other organisations in high threat environments.

Agencies need to consider that the likelihood of being targeted is influenced by their desirability to adversaries, and the consequences of a cyber security incident will depend on their requirement for the confidentiality, integrity and availability of their systems and data. This, in conjunction with the maturity level descriptions below, can help inform the target maturity level to implement.

It is important to note that while the selection of a Maturity Level is based on risk, the risk of not implementing a mitigation strategy or control associated with a Maturity Level cannot be accepted by the agency to achieve that Maturity Level. All mitigation strategies must be implemented in full, or adequate compensating controls must be in place.

[3] South Australian Cyber Security Framework | Security SA

[4] The SACSF Implementation Toolkit available to agency security staff includes control mapping between the SACSF and Essential Eight.

[5] Essential Eight Maturity Model | Cyber.gov.au

Essential Eight Maturity Model – Maturity level descriptions (from the Essential Eight Maturity Model)

Maturity Level Zero (ML0)	Maturity Level One (ML1)	Maturity Level Two (ML2)	Maturity Level Three (ML3)
This maturity level signifies that there are weaknesses in an organisation's overall cyber security posture. When exploited, these weaknesses could facilitate the compromise of the confidentiality of their data, or the integrity or availability of their systems and data, as described by the tradecraft and targeting in Maturity Level One.	The focus of this maturity level is to address the threat of malicious actors who are content to simply leverage commodity tradecraft that is widely available in order to gain access to, and likely control of, systems. For example, malicious actors opportunistically using a publicly-available exploit for a vulnerability in an internet-facing service which had not been patched, or authenticating to an internet-facing service using credentials that were stolen, reused, brute forced or guessed. Generally, malicious actors are looking for any victim rather than a specific victim and will opportunistically seek common weaknesses in many targets rather than investing heavily in gaining access to a specific target. Malicious actors will employ common social engineering techniques to trick users into weakening the security of a system and launch malicious applications, for example via Microsoft Office macros. If accounts that malicious actors compromise have special privileges they will exploit it. Depending on their intent, malicious actors may also destroy data (including backups).	The focus of this maturity level is to address the threat of malicious actors operating with a modest step-up in capability from the previous maturity level. These malicious actors are willing to invest more time in a target and, perhaps more importantly, in the effectiveness of their tools. For example, these malicious actors will likely employ well-known tradecraft in order to better attempt to bypass controls implemented by a target and evade detection. This includes actively targeting credentials using phishing and employing technical and social engineering techniques to circumvent weak multi-factor authentication. Generally, malicious actors are likely to be more selective in their targeting but still somewhat conservative in the time, money and effort they may invest in a target. They will likely invest time to ensure their phishing is effective and employ common social engineering techniques to trick users to weaken the security of a system and launch malicious applications, for example via Microsoft Office macros. If accounts that malicious actors compromise have special privileges they will exploit it, otherwise they will seek accounts with special privileges. Depending on their intent, malicious actors may also destroy all data (including backups) accessible to an account with special privileges.	The focus of this maturity level is to address the threat of malicious actors who are more adaptive and much less reliant on public tools and techniques. These actors can exploit the opportunities provided by weaknesses in their target's cyber security posture, such as the existence of older software or inadequate logging and monitoring. Malicious actors do this to not only extend their access once initial access has been gained to a target, but to evade detection and solidify their presence. Malicious actors make swift use of exploits when they become publicly available as well as other tradecraft that can improve their chance of success. Generally, malicious actors may be more focused on particular targets and, more importantly, are willing and able to invest some effort into circumventing the idiosyncrasies and particular policy and technical controls implemented by their targets. This can also include circumventing stronger multi-factor authentication by stealing authentication token values to impersonate a user. Once a foothold is gained on a system, malicious actors will seek to gain privileged credentials or password hashes, pivot to other parts of a network, and cover their tracks. Depending on their intent, malicious actors may also destroy all data (including backups).

Implementation

The steps below can be followed to develop an Essential Eight implementation strategy.

Implementation step	Description
1. Determine the target maturity level	• In conjunction with the advice on maturity levels above, consider conducting a cyber security threat intelligence assessment to assist in determining the maturity level that your agency should aim for. • Consider your agency’s risk appetite. • The ultimate maturity level you are aiming to achieve may influence the way that strategies are implemented at a lower level (e.g. an application control tool is not required to meet maturity level 1 (ML1), but if you are aiming for ML2 or ML3 it will be needed, so you should aim to implement it to achieve ML1).
2. Assess current maturity level	• Conduct a gap analysis against the Essential Eight to understand current controls in place. The reporting that has been conducted as part of the annual SACSF attestation will provide an overview of current state. • Each maturity level is designed to be implemented as a package. Aim to implement the lower-level controls across all eight strategies before moving to a higher level, to reduce the risk of control gaps and exposure. • Implementing one maturity level at a time will provide a more secure baseline for your agency than achieving higher maturity levels in a few mitigation strategies to the detriment of others. • For example, if your agency is currently ML0 in four strategies, and ML1 in four strategies, it is recommended to aim for ML1 in all eight strategies before focussing on ML2.
3. Develop a plan to reach the next maturity level	a. Define the scope • Are all systems in scope? Is the scope limited to the corporate environment? Are any cloud services included or excluded? Does your agency have any OT (Operational Technology) or Linux environments, and are they in scope? • Try to minimise exceptions to the scope if possible, remembering that the Essential Eight is designed for Windows based internet-connected environments. b. Ensure it is realistic • Implementing the Essential Eight is a big piece of work that will likely include project management, change management, risk assessment, business analysis, procurement, and communications. • Ensure the resources that you need are available. Consider having a roadmap that stretches over several years if needed. • Identify any legacy systems or technical debt that may impact implementation. These can hamper implementation of the strategies, although strong risk management processes may address this.

	c. Consider a roll-out strategy • Identify any quick-wins to reduce organisational risk exposure and gain momentum for the project. • Consider first implementing a control for high-risk users and computers such as those with access to important (sensitive or high-availability) data and exposed to untrustworthy internet content, and then implement it for all other users and computers. • Incorporate your organisation's change management processes and ICT roll-out strategies into your project. d. Consider requirements for exceptions and compensating controls • Scope exceptions and compensating controls should be documented and approved. • Review any exceptions and compensating controls at regular intervals. e. Ensure management support • Seek support for your implementation strategy from the appropriate governance bodies. As well as needing approval for budget and resources, Essential Eight implementation will likely need involvement from all parts of the agency, so it is important that all stakeholders are identified and engaged to understand what is planned, why it is important, and how it may impact them.
4. Reassess maturity level	a. Conduct an assessment (see the next section) • Conduct a formal assessment against the maturity level that you are aiming to achieve to determine any gaps or improvements required. b. Plan to meet the next maturity level by repeating the process above.

Assessment

Assessment step	Description
1. Plan the assessment	• Plan the scope of your assessment, including what you will assess and which mitigation strategies you will assess against. You may choose to assess a single system, or the entire corporate environment. • If you are assessing against a certain maturity level, ensure that you have previously assessed against the lower level/s. For example, if your target maturity level is ML2, ensure that you first assess against ML1 and successfully meet those requirements before assessing against ML2. • Consider who will conduct the assessment. It can be done by internal staff, or by an external party. Ensure they have some experience, such as completing the TAFE Cyber Essential Eight Assessment course. • Be aware that even if an external party is used, they will require access to your systems and resources, especially your system administration staff. Include these resource considerations in your planning. • Use the Essential Eight Assessment Process guide to plan and prepare for your assessment. It describes specific assessment methods for each control at each maturity level, and their effectiveness.

2. Assessment tools	• The ACSC have developed a set of tools that can be used to conduct an initial assessment across your environment. The Essential Eight assessment toolkit can be downloaded from the ACSC Partner Portal[6]. • The toolkit includes the Application Control Verification Tool (ACVT) which tests the effectiveness of application control in your environment. • It also includes the Essential Eight Maturity Verification Tool (E8MVT) which tests the implementation of many Essential Eight controls and reports on if they meet the requirements of each maturity level. • Not all controls or mitigation strategies can be tested by the tools (for example Regular Backups is not included), so ensure that you understand what is and isn't being tested. • Ensure that any impact the tools may have on your environment is understood. The tools may be 'noisy' and use compute resources. The ACSC recommend using them on a test environment, rather than in production.
3. Assessing compensating controls	• Compensating controls can be adopted instead of specific Essential Eight requirements. However, they should provide an equivalent level of protection and meet the same intent as the Essential Eight requirement. • For example, a compensating control for application control would still need to prevent unauthorised applications from running. If an assessor can run an unauthorised application in a manner that should be prevented by the Essential Eight requirement, then the compensating control is not effective. • For this reason, compensating controls are most often applied to mitigation strategies such as Patching Applications and Patching Operating Systems where compensating controls can be wrapped around the unpatched system to reduce risk. • All exceptions and compensating controls must be documented, approved by an appropriate authority, and have a review date. • Risk acceptance without adequate compensating controls cannot be accepted as justification for not implementing a control in order to meet the corresponding maturity level. The risk to agency systems still exists, so the control is considered not to be implemented.
4. Reporting	• The findings of the assessment and recommendations can be documented in a formal report. The ACSC provide an example template that can be used. • Consider providing the report to internal stakeholders, and relevant governance committees including your agency cyber security governance committee and audit and risk committee.

[6] SA Government agencies can email <jcsc.adelaide@defence.gov.au> to request access to the ACSC Partner Portal.

Suppliers

Supplier considerations	Description
1. Procurement considerations	• The South Australian Government does not have a policy requirement that suppliers must be assessed against the Essential Eight. • However, the Essential Eight is becoming widely adopted by government and industry across Australia, and evidence of a supplier having and maintaining Essential Eight compliance to a certain maturity level may be a useful form of assurance to be considered in the procurement process in the same way that other cyber security certifications may be.
2. Contract considerations	• If considering incorporating Essential Eight compliance into a contract be sure to specify assessment requirements including that the assessment be completed by an independent third party, the frequency of assessments, and the maturity level to be maintained. • The Essential Eight is regularly updated by the ACSC to align with the changing cyber threat environment. The South Australian Government has no control over these changes. Ensure that the likelihood that the Essential Eight will change during the life of the contract is considered. • The Essential Eight is not a standard that organisations can achieve a globally recognised certification in such as ISO/IEC 27001 or SOC2. However, IRAP assessment will include the Essential Eight Maturity Model controls at a ML2 and ML3 level as specified in the ACSC Information Security Manual (ISM). • Ensure all contract clauses and requirements are reviewed by legal professionals.

Aboriginal Impact Statement

The needs and interests of Aboriginal people have been considered in the development of this guideline. There is no specific impact on Aboriginal people.

Related documents

- Essential Eight | Cyber.gov.au
- Strategies to Mitigate Cyber Security Incidents | Cyber.gov.au
- Essential Eight Maturity Model | Cyber.gov.au
- Essential Eight Maturity Model FAQ | Cyber.gov.au
- Essential Eight Assessment Process Guide | Cyber.gov.au

Definitions

Term	Definition
ISO/IEC 27001	International standard for Information Security Management Systems.
SOC 2	Service Organization Controls (SOC) 2. An auditable security framework for organisations that process, store or transmit data for their customers or partners.

Acronyms

Acronym	Words
ACSC	Australian Cyber Security Centre
E8	Essential Eight
IRAP	Infosec Registered Assessors Program
ISM	Information Security Manual
ML	Maturity Level (Essential Eight)
SACSF	South Australian Cyber Security Framework

DOCUMENT CONTROL

Approved by: CIO Steering Committee	
Contact: Chief Information Security Officer	
Division: Office of the Chief Information Officer	Compliance: Optional
Review number: V1.0	Date of original approval: November 2023
Next review date: November 2024	Most recent approval: November 2023

Licence