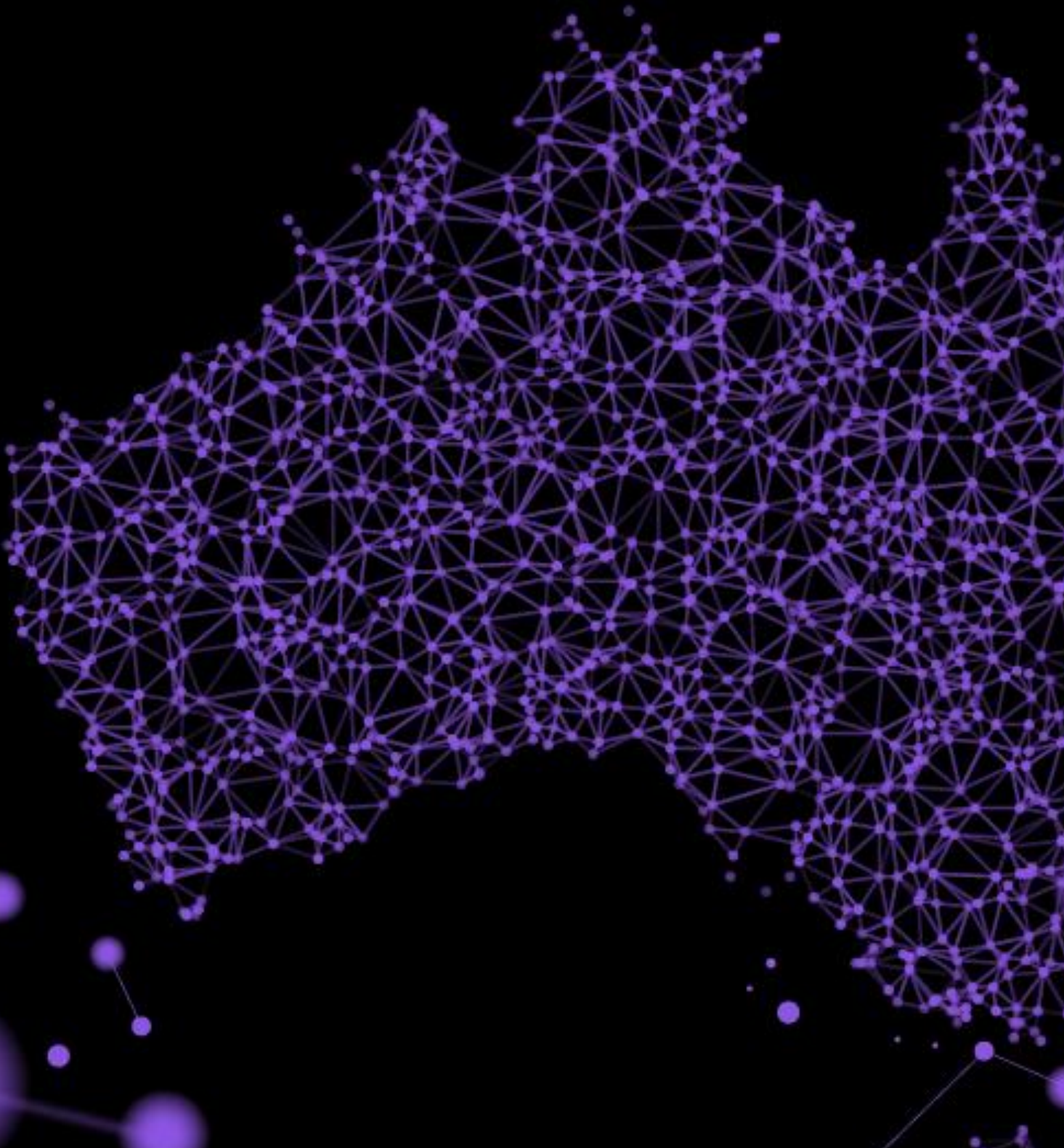
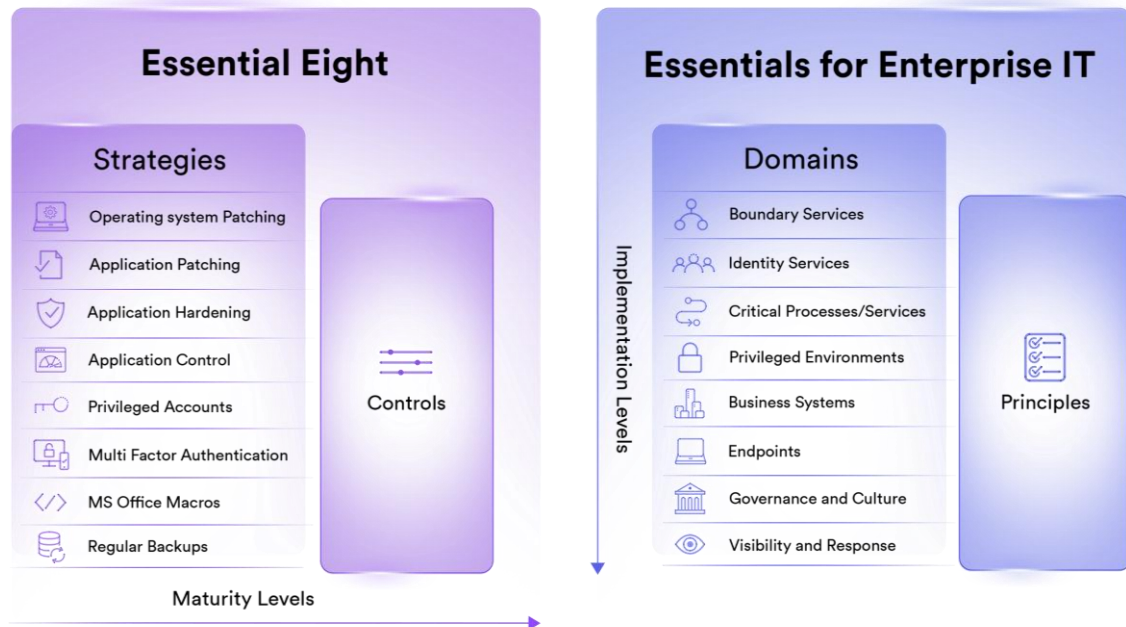


ASD Essentials for Enterprise IT Explained



ASD have just published the “Essentials for Enterprise IT, a new cybersecurity framework. It’s intended to be the first in a series, covering different IT environments such as Cloud and Operational Technology (OT).

Essentials differs significantly from the longstanding Essential Eight. It’s broader and more comprehensive with several key differences:



- ✓ The **8 Strategies**, primarily focused on endpoints, have been replaced by **8 Domains**, covering the entire enterprise IT environment.
- ✓ **Maturity Levels**, deployed in order of adversary capability, have been replaced by **Implementation Levels**, deployed in order of priority.
- ✓ Rather than proscriptive **controls**, often applicable only to Microsoft Windows endpoints, **Principles** define what the expected outcome should look like.
- ✓ **Actions** guide how those outcomes can be met across the applicable domains

Essentials for Enterprise IT also reflects a significantly changed threat landscape to the one that Essential Eight was designed to mitigate. The risk from opportunistic attacks targeting users like ransomware remains the same, but increasingly sophisticated and motivated adversaries are targeting privileged systems on the edge to launch attacks while remaining undetected.

Looking at Essentials for the first time can feel overwhelming, especially if you are accustomed to – or only just getting your head around – Essential Eight. The reality is a practical and flexible framework that can be easily “chunked” into manageable deployment actions that result in meaningful and measurable uplift.

The purpose of this article is to provide guidance based on our own experience preparing our transition to Essentials for Enterprise from our current Essential Eight Maturity Level 3 operations, while also leveraging our alignment with other Commonwealth and international frameworks.

Let's start by understanding the scope of each Domain:

1. **Governance and Culture:** Ensuring specific people are accountable, properly resourced and supported to implement and sustain the required processes, technology and – most importantly – mindset across the organisation.
2. **Visibility and Response:** Having effective line-of-sight of your Enterprise IT Environment and a consistent ability to detect, contain and eradicate threats against it. This requires an accurate inventory, ability to analyse activity logs and other telemetry, and Security Operations people, processes and technology.
3. **Boundary Services:** The parts of your IT environment that sit next to the public internet, and therefore the most accessible by adversaries. Traditionally this included firewalls, remote access (e.g.: VPN) appliances, public facing web servers and apps. Nowadays cloud services (SaaS, PaaS & IaaS) and API gateways are common.
4. **Identity Services:** These are the components that determine who can access what and how. For most organisations these include Active Directory/Entra ID and other identity, credential and access management solutions.
5. **Critical Processes and Services:** The “crown jewels”, those applications and data that the organisation depends on to function. It differs from organisation to organisation but typically includes customer data, intellectual property, email, payment systems and ERP platforms.
6. **Privileged Environments:** Where the IT Team live and breathe; the tools, admin accounts and platforms that underpin the other domains. Administrative workstations, jump servers and cloud management portals.
7. **Business Systems:** The apps and data that most people in the organisation are using most of the time. Office Productivity -documents/spreadsheets/presentations etc., Line of Business applications – including SaaS, collaboration and messaging tools.
8. **User Devices:** Those “endpoints” that were the primary focus of Essential Eight but expanded to explicitly include corporate managed mobile devices and other non-Microsoft devices.

Essentials for Enterprise recommends prioritizing cybersecurity uplift across these Domains in the following order, known as Implementation Levels:

- **Implementation Level 1:** Start with the Boundary Services and Identity Services Domains, as they form the point of entry and basis of trust, akin to the doors, locks and keys of a building.
- **Implementation Level 2:** Move on to the Critical Processes and Services and Privileged Environments Domains, as they are high-value targets to adversaries due to both their ability to damage you and the extent of the damage caused.
- **Implementation Level 3:** The Business Systems and User Devices Domains are the last in line, primarily as hardening the other domains have already significantly reduced the ability for adversaries to compromise these two Domains.

The Governance and Culture, Visibility and Response Domains are not included in the Implementation Levels as they need to be deployed and continually improved on an ongoing basis.



Cyber Security Principles

What is actually implemented on the Domains in the Implementation Level priority is a series of Cyber Security Principles, drawn from ASD's Information Security Manual (ISM). There are 27 of these Principles in Essentials for Enterprise IT, but not every Principle is applicable for every Domain.



Principles and Actions

The Principles describe an outcome rather than an action. An example is "Data communicated between different security domains for systems (infrastructure and applications) is controlled and subject to inspection and verification".

The move to outcome-based Principles allows organisations to implement them technology-agnostically across the typically diverse systems that make up their Domains.

Each Principle has several Actions to assist in achieving the outcomes of each Principle. These are still technology-agnostic, but guide the actions required.

An example of an Approach supporting the previous Principle example is "Inspect outbound content flows to detect unauthorised transfer of sensitive or high-value data."



How to Get Started

Understanding what your organisation needs to do to implement Essentials for Enterprise is more straightforward than may appear.

You can start with a simple "table-top" deployment exercise. Bring the key stakeholders together and go through each of the Principles to understand how much of their outcomes are met in your Enterprise IT Environment. "Stakeholders" aren't limited to the Security and IT Teams, but should include business function owners as it's the workloads they manage that define many of the systems in place and how they function.

The table-top exercise does not need to be onerous. There are only 27 Principles and not every Principle applies to every domain. By focussing on the outcomes without having to – at this point – look for supporting evidence will allow you to quickly identify the biggest gaps.



Use Existing Frameworks

You can also draw on any other cyber security framework – such as NIST or ISO 27001 – that your organisation is aligned to. This is one of the benefits – and was the intent – of the shift to outcome-based Principles in Essentials for Enterprise.



Key Takeaway

ASD creating this new Essentials series is an important step in Australia lifting our collective cyber-posture. It should not be seen as yet another compliance responsibility, but instead a set of tools to guide you in safeguarding your organisation from the threats that unfortunately keep increasing in volume and capability.