What? We are fortunate to have assisted lots of clients with the Australian Signals Directorate (ASD) Essential 8 Maturity Model (E8). The ASD update the E8 model on a regular basis, the last change was November 2023. In recent conversations, many were not aware of the update, so we thought it would be of value to highlight the salient issues.

What do I really need to know? Like most updates, there are several changes that, in all likelihood, will only marginally improve your organisation's ability to mitigate against various cyber threats – for example, some controls have been split to provide finer definition, and some have been moved to different categories.

Some of the key changes focus on faster patching, improved multi-factor authentication, and enhanced logging and monitoring – we can assist with the details if you are interested.

However, the main issues worth considering fall into two main categories:

1) The first is the inclusion of a **new group of six (6) discrete 'universal controls'** that fall into several of the "maturity 2" categories.

   Essentially these controls stress the need to have, protect and analyse event logs, timely analyse events, and report to appropriate parties on cyber incidents.

   Most did not exist prior to this update (one moved from Maturity 3 to 2), so it is worth having a look to make sure you have got yourself covered.

2) The second issue is a subtle but important **nuanced word change** from "internet-facing services" to "online services" (in 58 locations throughout the model).

   It is reasonable to assume that many might have missed that little change, but it could have a big impact to you depending on your technology environment.

   a. **Online Services** covers any service that is accessible over the internet, includes applications, email, cloud storage, social media etc.

   b. **Internet-facing services** refers to services that are intentionally exposed and accessible to anyone on the public internet, includes public websites, applications etc.

   This wording change has been made throughout the entire model in controls involving patching, vulnerability scanning, using Multi-factor Authentication, Privileged / Administrative Accounts, etc.

Consider doing a quick 'delta comparison' between your older Essential 8 assessment to the new model. As always, if you would like help or would value an independent assessment, please do not hesitate to reach out.

Do not forget… While the E8 is a great step in the right direction, it is primarily a 'technically-focused' maturity model which neglects the broader cyber risks associated with your people, and other key considerations such as incident planning and simulation. It also excludes some non-Microsoft technologies – do not be lulled into thinking that if you have the E8 covered, you are safe!

If you would like to take the next step using a more holistic cyber security framework (people, process, technology perspective), we do it all of the time and could assist there too.