ARCH Cyber Discussion paper submission for Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

At ARCH Cyber, our mission is to support organisations in achieving a robust and resilient cyber security posture. Our team brings deep experience working across Federal and State Government agencies, as well as the private sector, including major Cloud Service Providers.

ARCH has played a central role in strengthening cyber security assurance across government and critical infrastructure. We have delivered multiple Info-sec Registered Assessors Program (IRAP) assessments for government agencies and critical infrastructure clients, and our team has contributed directly to the evolution of the program.

ARCH has also contributed significantly to the development and maturation of the Essential Eight (E8) framework and undertaking control mappings across jurisdictions to understand security classification equivalency.

Through this we've observed a desire at a business and executive level for compliance models. This is because they provide structure and direction and a sense of 'complete' or 'done'. But, they often fail to capture the nuanced operational realities of an environment, risk tolerances, and sectoral priorities of the organisations they are applied to.

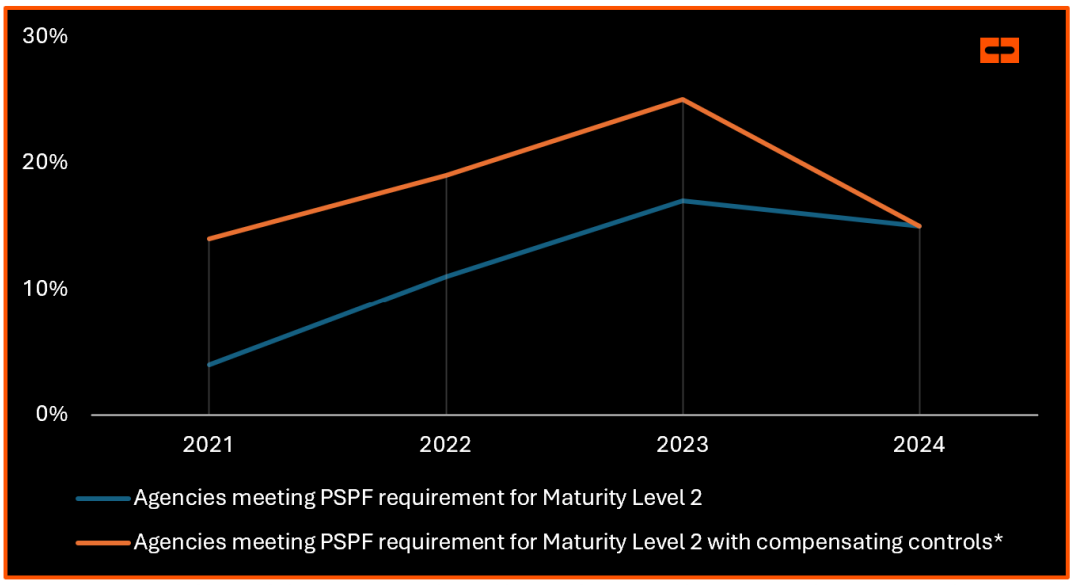
The multi-framework approach adopted under the Security of Critical Infrastructure (SOCI) legislation begins to address this by encouraging alignment to risk, but in a compliance-driven culture it can also incentivise organisations to choose the least demanding option rather than the most appropriate one.

We have also observed the growing challenge of "framework fatigue," where the proliferation of overlapping regulatory models creates unnecessary overhead, confusion, and ultimately disengagement. Without strong assurance mechanisms, even the most robust frameworks risk being reduced to a paper exercise.

At ARCH Cyber we believe there is need to harmonise and simplify cyber regulation. A streamlined and outcome-focused approach would both improve efficiency and promote best practice across sectors. This aligns directly with the Australian Cyber Security Strategy's "Horizon Two" challenge that "Australian entities find the cyber regulatory framework complex and difficult to navigate."

This should also be underpinned by a risk-based approach. IRAP, for example, does not have a pass failure outcome. Instead, an authority for each government agency determines what is acceptable for their organisation. Comparatively, the Protective Security Policy Framework (PSPF) has required government entities attain maturity level two (ML2) of the Essential Eight Maturity Model for nearly a decade, with little progress. In 2023/24 a perceived deterioration in the technical hardening of systems was actually reported in the Commonwealth Cyber Security Posture Report (see Graph 1).

Graph 1: Number of Commonwealth agencies implementing technical controls to meet minimum cyber security maturity requirements



*The 2024 reported a single statistic of 15% for agencies meeting Maturity Level 2. This has been applied to both trend lines

On its face, this appears to be 'bad'. Contextually, this does not account for the fact that the E8 maturity model updates annually to reflect the evolutions in threat actor tactics, techniques and procedures, and the challenges that may exist with legacy systems, implementation costs to support uplift or remediation timeframes. Neither does it consider the compensatory arrangements that could be in place providing adequate or better security outcomes.

Ultimately security outcomes are driven by informed choices, risk tolerances and technical work to implement. To that end **we believe the following opportunities include:**

Key opportunities include:

- Mapping framework equivalence to preserve flexibility while ensuring regulatory intent is met.
- Incentivising demonstrable security uplift and continuous improvement over minimum compliance.
- Reducing duplication through outcome-based regulatory measures that are easier to implement and verify.

And we believe the key risks going forward are:

- Continued proliferation of frameworks leading to disengagement.
- Inconsistent application of controls without robust assurance and accountability.