



Government And Compliance-Adjacent Organisations

Sovereign infrastructure for organisations where Australian data jurisdiction is non-negotiable



The Reality of IT in This Sector

Government bodies, government-adjacent organisations, and businesses working within the Australian public sector supply chain face IT requirements that are categorically different from most commercial environments. Data must stay onshore. Infrastructure must be auditable. Compliance with the ACSC Essential Eight is increasingly mandatory rather than aspirational. And the organisations responsible for these environments are accountable to regulators, funding bodies, and the public in ways that make IT risk genuinely consequential.

The Pressure Points

- Australian data jurisdiction is a hard requirement. Data hosted on US-based hyperscalers is subject to foreign government access legislation regardless of where the servers are physically located
- Essential Eight maturity requirements are being enforced more rigorously, with real consequences for organisations that cannot demonstrate compliance
- IRAP assessment and Official Protected status are becoming prerequisites for certain government contracts and grants
- Procurement processes require demonstrable credentials, independent verification, and a clear audit trail for all technology decisions
- Internal IT teams are often under-resourced and need a partner who can take on full accountability rather than just providing tools
- Cyber incidents involving government-adjacent organisations attract regulatory scrutiny and public attention that makes recovery more complex than in a private sector environment

Why Standard IT Falls Short

Most MSPs can provide an Essential Eight gap assessment and some remediation activity. Very few can offer the combination of sovereign infrastructure, active IRAP assessment, ACSC founding membership, and the technical depth to actually deliver a compliant, auditable environment end to end.

The difference between an organisation that claims compliance and one that can demonstrate it under scrutiny is the difference between passing an audit and explaining a failure.

What CMTG Brings to This Sector

1



SOVEREIGN CLOUD INFRASTRUCTURE:

CMTG's private cloud platform hosts client data exclusively within Western Australia on infrastructure CMTG owns. No hyperscaler exposure. No foreign jurisdiction risk. Full audit trail available on request.

2



ESSENTIAL EIGHT ADVISORY AND IMPLEMENTATION:

CMTG provides gap assessment, implementation guidance, and ongoing compliance monitoring across the ACSC Essential Eight Maturity Model. Practical, evidence-based uplift rather than checkbox compliance.

3



IRAP ASSESSMENT SUPPORT:

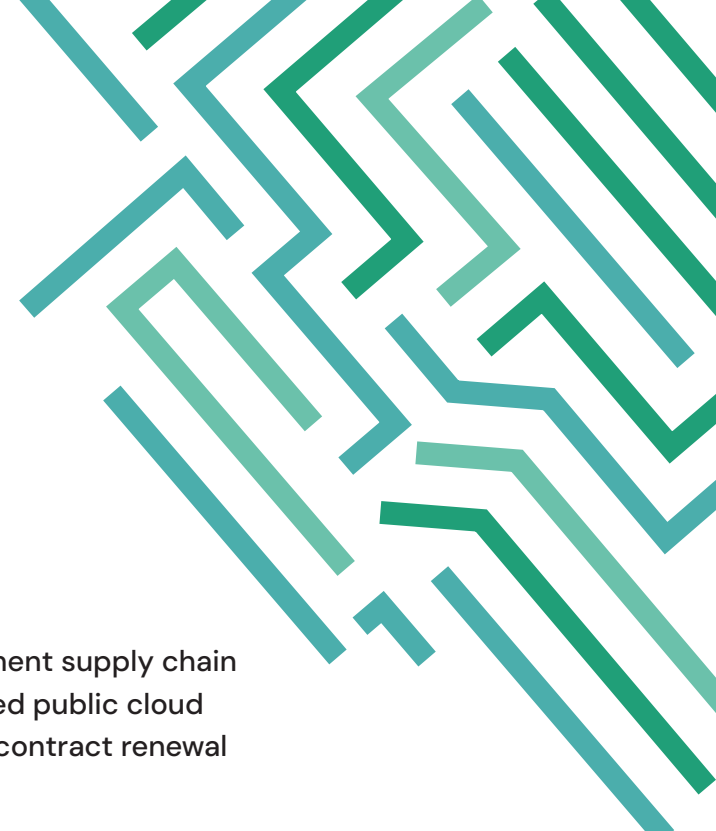
CMTG is actively progressing its own IRAP assessment targeting Official Protected status. That means the team understands the assessment process from the inside and can provide substantive support to clients on the same journey.

4



FOUNDING ACSC NETWORK PARTNER:

CMTG is a founding member of the Australian Cyber Security Centre Network Partner programme, providing direct access to threat intelligence and early visibility of emerging requirements.



What It Looks Like in Practice

A WA-based organisation operating within the government supply chain engaged CMTG to migrate its environment from a shared public cloud arrangement to CMTG’s sovereign platform ahead of a contract renewal that required demonstrable data sovereignty.

CMTG completed the migration, implemented the Fortinet security stack, initiated an Essential Eight uplift programme, and provided quarterly reporting that gave the organisation clear evidence of its compliance posture. The contract was renewed and the organisation had a documented path to a higher Essential Eight maturity level.

Relevant Credentials

1



ACSC FOUNDING MEMBERSHIP:

Founding member of the Australian Cyber Security Centre Network Partner programme

2



IRAP:

Active IRAP assessment in progress, targeting Official Protected status

3



SOVEREIGN INFRASTRUCTURE:

Dual WA data centres, private dark fibre, 100% Australian-owned and operated

4



ESSENTIAL EIGHT:

Compliance advisory and implementation across all eight mitigation strategies

If your organisation needs to demonstrate Australian data sovereignty, progress its Essential Eight maturity, or prepare for an IRAP assessment, CMTG has the infrastructure, the credentials, and the experience to support that work practically. It is worth a direct conversation about where you are and what needs to happen next.