



Professional Services

Secure, compliant IT infrastructure
for businesses with serious data
governance obligations

CMTG.COM.AU



The Reality of IT in This Sector

Professional services firms, including law practices, financial advisers, accountants, and management consultants, hold sensitive client information as a matter of course. That information includes legal advice, financial positions, commercial strategies, and personal data that clients have shared under an expectation of confidentiality. The obligations around how that data is stored, protected, and handled are both professional and legal. A data breach in a professional services context is not just an IT incident. It is a professional conduct issue, a regulatory matter, and a reputational event that can end client relationships.

The Pressure Points

- Client confidentiality is a professional obligation, not just a privacy policy requirement. The technology environment that stores client data must be able to withstand scrutiny from the regulator and the client
- Many professional services firms are subject to sector-specific data obligations beyond the Privacy Act, including obligations under the Legal Profession Uniform Law, ASIC requirements, and the Tax Practitioners Board standards
- The consequences of a ransomware incident in a professional services environment extend to the clients whose data was held, creating notification obligations, potential liability, and significant reputational damage
- Remote and hybrid working models mean that confidential client data is being accessed from a range of devices and locations that need to be secured consistently
- Growing firms taking on larger clients and more complex engagements need infrastructure that reflects the seriousness of the work they are doing
- Many professional services firms are still running IT that was appropriate when the business was smaller and that is no longer adequate for the obligations they now carry

Why Standard IT Falls Short

Many professional services firms have IT arrangements that look adequate on the surface but would not survive a serious incident or a detailed

A backup that has never been tested, a Microsoft 365 tenant that has never been hardened, and a support agreement that responds rather than prevents are common in this sector. The question for a law firm or financial adviser is not whether their IT is convenient. It is whether it is defensible.

What CMTG Brings to This Sector

1



SOVEREIGN, AUDITABLE DATA STORAGE:

Client data hosted on CMTG's private cloud platform stays in Western Australia on infrastructure CMTG owns. A clear, auditable answer to where client data lives, who can access it, and what would happen in the event of a breach. No foreign jurisdiction exposure.

2



MICROSOFT 365 HARDENED AND PROPERLY MANAGED:

CMTG manages the Microsoft 365 environment that most professional services firms depend on: security hardening, Secure Score uplift, conditional access policies, and cloud backup covering email, OneDrive, SharePoint, and Teams. The platform as it should be, not as it comes out of the box.

3



RANSOMWARE PROTECTION AND RAPID RECOVERY:

Immutable backup with sub-1-hour recovery capability means that in the event of a ransomware incident, the firm can recover client data and resume operations quickly. The notification obligation is uncomfortable. An extended outage while recovering from an attack is worse.

4



COMPLIANCE ADVISORY:

CMTG provides Essential Eight advisory and implementation, helping professional services firms demonstrate a defensible security posture to clients, regulators, and professional bodies that are increasingly asking the question.

What It Looks Like in Practice

A Perth-based legal practice with a mix of commercial and private client work engaged CMTG to review and upgrade an IT environment that had not been substantially updated since the firm grew from five to twenty-five practitioners.

CMTG hardened the Microsoft 365 environment, migrated matter management and client document storage to the sovereign cloud platform, implemented Fortinet endpoint protection across all devices and remote workers, and provided quarterly reporting that gave the managing partners clear visibility of the firm's security posture. The firm subsequently included CMTG's security credentials in a response to a commercial client's supplier security questionnaire.

Relevant Credentials

1  DATA SOVEREIGNTY: Private cloud hosting exclusively in Western Australia, under Australian law, on infrastructure CMTG	2  MICROSOFT 365: Gold Microsoft Datacenter Partner and Gold Cloud Mid-Market Partner with full M365 management capability	3  COMPLIANCE: Essential Eight advisory and implementation, supporting professional obligations to clients and regulators	4  RECOVERY: Sub-1-hour RTO with immutable backup and quarterly DR testing
--	---	--	---

If your firm has not had its Microsoft 365 environment independently reviewed, cannot clearly articulate where client data is stored and how it is protected, or is facing increasing expectations from larger clients about your security posture, a conversation with CMTG is a practical starting point.