

INNER-CITY MELBOURNE LAW FIRM

From high risk to SMB1001 Gold. In four months.

A team of ten-plus, taken from shared passwords and an unsupported server to a recognised Australian cyber security standard. (Name withheld at the firm's request.)



4 mths

from high risk to certified Gold

Gold

SMB1001 Level 3, certified

24/7

security monitoring, beyond what Gold requires

Better

insurance outcome and experience

THE CLIENT

An **inner-city Melbourne law firm**, a team of ten-plus, holding confidential client matters on systems years behind on security.

THE JOB

Take the firm from high risk to SMB1001 Level 3 Gold, the recognised Australian cyber security standard, without disrupting a busy practice.

THE RESULT

Certified Gold in four months. A locked-down environment, trained staff, and their security status visible at any time.

THE CHALLENGE

When we first assessed this firm, the honest answer was: high risk, across the board.

- Multi-factor sign-in had gaps, so a stolen password could be enough to get in
- Passwords were shared and reused across accounts
- Remote access was open to attack
- An ancient server, no longer supported, hadn't seen a security update in years, and nothing kept the rest of the software patched either
- Behind all of it: years of no real investment in security, no roadmap, no strategy

For a law firm holding confidential client matters, that's not a technology problem. It's a trust problem waiting to surface. The partners wanted more than patch-up fixes: a standard they could stand behind.

WHAT WE DID

Four months, methodical, built around the five areas SMB1001 covers. In plain language:

- **Moved the firm to Microsoft 365** and locked it down to our best-practice baseline, which goes further than Gold requires
- **Closed the sign-in gaps:** multi-factor sign-in enforced everywhere through strict rules that check who's signing in, from where, on what device; the firm's main apps brought under one secure sign-in, covered by the same rules
- **Secured remote access** behind multi-factor-protected connections, and **contained what couldn't be replaced:** legacy systems separated from the working environment with tightly protected access
- **Hardened every computer:** local administrator rights removed, every firewall on and monitored, attack-detection software on each machine
- **Fixed the backups** (automated, tested annually), **wrote and verified the policies**, and **trained the whole team**
- **Then went past Gold:** continuous detection and response, with the Microsoft 365 environment monitored 24/7

THE RESULTS

- ✓ **Certified SMB1001 Level 3 Gold**, four months from a starting point years behind
- ✓ A secure environment that's **actually manageable**, instead of a collection of unknowns
- ✓ Legacy risk fenced in, not ignored
- ✓ Backups proven by testing, not assumed
- ✓ **An improved insurance outcome and experience** at renewal
- ✓ **Staff trained and aware** of the commitment the firm has made
- ✓ Local admin rights gone, firewalls monitored, every machine watched
- ✓ **Ongoing managed client:** their SMB1001 status visible at any time in Kevin, our client portal

THE TAKEAWAY

Four months is what it took to go from the worst starting position we see to a recognised standard. The certification wasn't the trick: it was the by-product of actually fixing things. And because the environment is managed all year with the status visible at any time, it stays fixed. Want to know where your firm would score today? Book a free assessment.