Human risk as a compliance driver

Cybercrime is getting more expensive for Australian businesses, averaging $97,200 per report for mid-sized organisations. Human-risk management is now a practical way to evidence Essential Eight maturity progress and demonstrate “reasonable steps” under the Privacy Act.

What’s driving requirements

Australian regulators, auditors, and insurers increasingly expect continuous evidence, not annual check-box activity:

- **Essential Eight (ASD):** Maturity Levels 1–3 require demonstrable progress, with evidence of implementation over time.
- **Privacy Act and OAIC guidance:** Organisations must take “reasonable steps” to protect personal information, supported by documented policies and staff awareness.
- **Cyber insurance and audits:** Proof of training, phishing outcomes, and policy acknowledgement is increasingly requested during renewals and assessments.

Where organisations struggle

- Limited IT time to manage ongoing training, policy sign-off, and reporting alongside day-to-day operations
- Outdated annual training that doesn’t stand up to audits or customer reviews
- Policy acceptance scattered across inboxes and folders, making proof hard to produce on demand
- Evidence spread across tools, creating manual work and slowing audits and assurance requests

How We Support Your Compliance Evidence

Ongoing training + phishing	Centralised policy management	Human Risk Score + reporting	Quick cloud deployment
Automated programmes with measurable participation and improvement	Distribute policies and capture eSign acknowledgement in one place	Exportable, board-ready outputs for auditors and evidence logs for auditors and stakeholders	Microsoft 365 or Google Workspace sync, no installs

Begin your human-risk review
A short assessment to benchmark your evidence posture and define next steps.

Schedule Your Risk Review