CYBER ASSURANCE SUMMARY

Halcyon Advisory Group

Issued for the purpose of demonstrating cyber security maturity to insurers, clients, and regulators.

Organisation	**Halcyon Advisory Group**
Registered domain	halcyonadvisorygroup.com.au
Director	Mitchell Chen
Security Lead	Sarah Blackwood
Monitoring period	**December 2025 — March 2026**
Report prepared by	Beacon Monitoring Platform
Issued by	Sicarius Pty Ltd
Report date	**16 March 2026**

OVERALL SECURITY POSTURE

94 / 100

Demonstrated

Continuous monitoring active since 20 December 2025 · 0 open findings · 4 resolved during monitoring period

CYBER RESILIENCE STATUS (DDRR)

The following assessment reflects Halcyon Advisory Group's security capability across four pillars: Defend, Detect, Respond, and Recover. Each pillar has been evaluated against continuous monitoring signals and verified evidence throughout the monitoring period.

Capability	Score	Status	What this confirms
Defend	**96 / 100**	**Demonstrated**	Endpoint protection, patch compliance, identity security, and access controls are fully implemented and actively monitored.
Detect	**95 / 100**	**Demonstrated**	Continuous monitoring is operating across credential exposure, domain surveillance, and external attack surface signals.
Respond	**91 / 100**	**Demonstrated**	Incident response plan is documented, signed, and current. Escalation procedures are in place and the Director has been briefed.
Recover	**94 / 100**	**Demonstrated**	Backup capability is verified. A restore test was completed in March 2026. Business continuity planning is documented and signed.

✓ No findings open — all identified issues have been resolved

4 findings were identified and resolved during the monitoring period (December 2025 — March 2026). Mean time to resolution: 11 days. No items require attention at the date of this report.

ESSENTIAL EIGHT ALIGNMENT

The Australian Cyber Security Centre's Essential Eight Mitigation Strategies form the foundation of Australia's cyber security baseline. The following assessment maps Beacon's monitored signals to each control. Ratings reflect observed alignment — not formal certification.

Control	Alignment	Est. Maturity	Evidence & Notes
Application Control Evidence: Device posture monitoring	**Moderate**	Level 1–2	Partial signal coverage. Manual assessment recommended to confirm alignment.
Patch Applications Evidence: Device monitoring, patch telemetry	**Strong**	Level 2–3	Signals indicate the control is broadly implemented.
Patch Operating Systems Evidence: Device monitoring, OS telemetry	**Strong**	Level 2–3	Signals indicate the control is broadly implemented.
Restrict Admin Privileges Evidence: Identity review, admin account audit	**Strong**	Level 2–3	Signals indicate the control is broadly implemented.
Multi-Factor Authentication Evidence: Identity posture checks, credential monitoring	**Strong**	Level 2–3	All accounts confirmed MFA-enabled as of 4 February 2026.
User Application Hardening Evidence: Browser security signals, email configuration	**Strong**	Level 2–3	Signals indicate the control is broadly implemented.
Regular Backups Evidence: Backup verification, restore test record	**Strong**	Level 2–3	Restore test completed 3 March 2026. Pass confirmed by Technical Coordinator.
Office Macro Settings Evidence: Email protection config, M365 configuration	**Moderate**	Level 1–2	Partial signal coverage. Manual assessment recommended to confirm alignment.

About this assessment. This assessment reflects observations from Beacon monitored signals only. The ACSC Essential Eight Maturity Model requires human assessment of controls that Beacon cannot fully observe. This assessment uses 'observed alignment' and 'estimated maturity' — never 'certified' or 'assessed at Level X'.

COMMON UNDERWRITING QUESTIONS — EVIDENCE INDEX

The following index addresses questions commonly asked by cyber insurers and client procurement teams during security due diligence. Each question is answered with reference to evidence collected by Beacon during continuous monitoring.

Question	Beacon Evidence	Status
Multi-Factor Authentication		
Is MFA enforced for all users?	MFA confirmed active for all 13 staff accounts on Microsoft 365. Verified by identity posture monitoring as of 4 February 2026.	**Demonstrated**
Is MFA enforced for remote and privileged access?	Administrative accounts confirmed MFA-enabled. No MFA gaps detected across monitored identity signals.	**Demonstrated**
Patch Management		
Are critical application patches applied within 30 days?	Patch telemetry signals indicate consistent application patch compliance. No overdue critical patches detected during the monitoring period.	**Demonstrated**
Are operating system patches applied within 30 days?	OS telemetry signals indicate consistent OS patch compliance across monitored endpoints. No overdue OS patches detected.	**Demonstrated**
Endpoint Protection		
Is endpoint detection and response (EDR) deployed on all devices?	SentinelOne EDR agent confirmed active on all monitored endpoints. Full coverage verified throughout monitoring period.	**Demonstrated**
Is endpoint protection actively monitored?	SentinelOne integration performs automated 4-hourly health and coverage checks. Gaps trigger immediate findings.	**Demonstrated**
Email Security		
Is DMARC configured and enforced?	DMARC policy confirmed as active on primary domain halcyonadvisorygroup.com.au. Email authentication configuration monitored continuously.	**Demonstrated**
Are SPF and DKIM records correctly configured?	SPF and DKIM records verified present and valid. No email authentication gaps detected during the monitoring period.	**Demonstrated**
Backups		
Are backups performed regularly?	Backup capability confirmed active. Backup verification signals monitored by Beacon throughout the period.	**Demonstrated**
Have backups been tested for successful restoration?	Restore test completed 3 March 2026. Pass result confirmed by Technical Coordinator David Wu (Pinnacle IT). Acknowledged by Director Mitchell Chen. Data sets tested: client document archive, email PST archive, financial system backup.	**Demonstrated**
Are backups isolated from the live environment?	Backup isolation confirmed via Security Lead review. Backup environment separated from production systems.	**Demonstrated**
Admin Privilege Restriction		
Is administrative access restricted to named accounts?	Admin account audit signals indicate privileges are restricted. No unexpected privilege escalation detected during the monitoring period.	**Demonstrated**
Are privileged accounts separate from standard user accounts?	Identity security review confirms separation of privileged and standard accounts across monitored identity systems.	**Demonstrated**
Application Control		
Is application control or whitelisting implemented?	Partial signal coverage from device posture monitoring. Manual assessment recommended to confirm full implementation. Beacon observes no signals inconsistent with application control being in place.	**Partial**
Macro Settings		

Are Microsoft Office macros restricted or disabled?	Partial signal coverage from M365 configuration monitoring. Manual assessment recommended to confirm macro restriction policy. No macro-based threat signals detected.	**Partial**
Incident Response		
Is there a documented incident response plan?	Data Breach Response Plan signed by Director Mitchell Chen on 5 February 2026. Documented and current. Stored in Beacon Policy Register.	**Demonstrated**
Has the incident response plan been reviewed in the past 12 months?	Policy signed and reviewed within the current monitoring period. Next review scheduled in accordance with policy review cycle.	**Demonstrated**
Security Awareness Training		
Do all staff complete security awareness training?	100% completion confirmed. All 13 staff completed all 12 training modules. Final module completed 1 March 2026.	**Demonstrated**
Does training cover phishing, passwords, ransomware, and incident response?	Training programme covers: Phishing & Scams, Passwords & Authentication, Incident Response Basics, Ransomware Basics, and 8 additional modules. Completion records held in Beacon.	**Demonstrated**
Credential Exposure		
Is credential exposure monitored against known breach databases?	Continuous credential monitoring active via HIBP Enterprise. No active credential exposures detected during the monitoring period.	**Demonstrated**
Domain & Exposure		
Is the organisation's domain monitored for impersonation or lookalike threats?	Domain surveillance and certificate transparency monitoring active for halcyonadvisorygroup.com.au. No impersonation signals detected.	**Demonstrated**
Incident History		
Has the organisation experienced a cyber incident or data breach in the past 3 years?	No incidents or data breaches detected or reported during the Beacon monitoring period. Monitoring active since 20 December 2025.	**Demonstrated**

STAFF SECURITY TRAINING

Security awareness training is delivered to all staff through the Beacon platform. Completion is tracked per employee and per module. The following records cover the monitoring period.

Organisation	Halcyon Advisory Group
Reporting period	**December 2025 — March 2026**
Total staff	**13**
Overall completion	**13 / 13 staff — 100% — all 12 modules complete**

Module	Completion	Avg Completion Date
1.1 Phishing & Scams	**13 / 13 (100%)**	5 Jan 2026
1.2 Passwords & Authentication	**13 / 13 (100%)**	10 Jan 2026
1.3 Incident Response Basics	**13 / 13 (100%)**	15 Jan 2026
1.4 Safe Device Use	**13 / 13 (100%)**	20 Jan 2026
1.5 Data Protection & Privacy	**13 / 13 (100%)**	25 Jan 2026
1.6 Ransomware Basics	**13 / 13 (100%)**	30 Jan 2026
1.7 Remote Work Security	**13 / 13 (100%)**	4 Feb 2026
1.8 Mobile & Cloud Safety	**13 / 13 (100%)**	9 Feb 2026
1.9 Social Engineering	**13 / 13 (100%)**	14 Feb 2026
1.10 Protecting Family & Friends	**13 / 13 (100%)**	19 Feb 2026
1.11 Compliance & Regulations	**13 / 13 (100%)**	24 Feb 2026
1.12 Building a Cyber Resilient Culture	**13 / 13 (100%)**	1 Mar 2026

MONITORING COVERAGE STATEMENT

Throughout the monitoring period, Beacon maintained continuous automated monitoring across the following coverage domains: endpoint protection status and agent coverage, identity security and multi-factor authentication posture, credential exposure via known breach datasets, patch compliance for applications and operating systems, email authentication configuration (DMARC, SPF, DKIM), domain surveillance and certificate transparency, and backup verification and restore test records. Monitoring was active from 20 December 2025 through the report date with 47 automated syncs completed.

Monitoring active since	20 December 2025
Monitoring syncs completed	**47**
Findings identified	4
Findings resolved	**4 (100%)**
Findings open at report date	**0**

APPENDIX A — ABOUT THIS REPORT

About This Report

Beacon monitors a defined set of external exposure signals and selected security posture indicators. These include: domain reputation and impersonation signals, credential exposure in known breach datasets, identity security posture, device protection status, email authentication configuration, and selected system hygiene indicators. Beacon monitoring does not replace penetration testing, comprehensive vulnerability scanning, or a formal security audit. This report summarises observations derived from monitored signals during the stated period and should be read accordingly.

About Sicarius Pty Ltd

Sicarius Pty Ltd (ABN 92 664 916 241) operates the Beacon cyber monitoring platform and provides cyber investigation and incident response support services. Beacon monitoring outputs may be reviewed by Sicarius investigators to assist in identifying significant security signals and to support incident response when required. Sicarius does not operate, administer, or manage the organisation's IT systems, networks, or security controls.

Important Notice

This report is intended to assist organisations in demonstrating ongoing cyber risk monitoring practices to clients, insurers, and regulators. It does not constitute a formal security audit, penetration test, Essential Eight maturity assessment, or guarantee of protection against cyber threats. Responsibility for implementing and maintaining security controls remains with the organisation.