PREPARED FOR

Ironbark Legal Pty Ltd

IT Audit Risk Report April 2026

A half-day on-site assessment of Ironbark Legal's IT environment, conducted on Thursday 9 April 2026. This report sets out what was found, the risks it creates for the practice, and a prioritised plan to close the gaps.

AUDIT DATE	DELIVERED	CONDUCTED BY	AUDIT ID
9 April 2026	14 April 2026	Birender Chahal	AUD-2026-0042

01 · EXECUTIVE SUMMARY

An exposed posture with three critical gaps. The most urgent is open to the internet today.

CIO Tech conducted a half-day on-site assessment of Ironbark Legal on Thursday 9 April 2026, covering the Microsoft 365 tenant, 22 endpoints, the on-premise file server, backup arrangements, and the network. Some controls are already in place: the firm has a managed firewall, a real endpoint security product, and a professional backup tool. Those investments are not being fully used.

The assessment identified **15 findings across four severity levels, including three critical gaps that expose the practice to ransomware, trust account fraud, and loss of legal professional privilege**. The most urgent finding is that the office's on-premise server can be reached directly from the public internet on the Remote Desktop port. This is the single most exploited attack path against Australian SMBs in 2026. It should be closed today.

The second and third critical findings are that the current backup is not immutable and has not been tested, and that multi-factor authentication is incomplete with significant admin sprawl. Each of these is addressable without a full rebuild. This report sets out a 90-day remediation roadmap, prioritised by risk.

OVERALL IT POSTURE

Exposed

The firm holds client trust account data, conveyancing files, family law records, and privileged legal communications on systems that are partially reachable from the public internet. The investments already made (managed firewall, SentinelOne EDR, Veeam backup) are not being actively administered. This is a common pattern: the right tools, not enough attention.

3	5	4	3
CRITICAL FINDINGS	HIGH FINDINGS	MEDIUM FINDINGS	LOW FINDINGS

TOP THREE TO ADDRESS FIRST

C1	**Remote Desktop is open to the internet.** The on-premise server has TCP port 3389 accessible from any IP address. This should be closed today. Fix within 24 hours.
C2	**Backups are not immutable and not tested.** Veeam writes to a NAS that is on the same domain and same network. A ransomware attack would destroy the backup. Fix within 14 days.
C3	**MFA incomplete and admin sprawl.** Six accounts without MFA; five admin accounts across two identity systems; one domain admin shared with the prior IT provider. Fix within 14 days.

02 · ENVIRONMENT OVERVIEW

What was assessed.

A half-day, on-site assessment at Ironbark Legal, Level 3, 12 Atchison Street, St Leonards. The environment below reflects the state at the time of the audit.

Staff & scope	20 staff (2 principals, 11 solicitors, 2 paralegals, 3 administration, 2 reception). Practice areas: commercial, property / conveyancing, wills & estates, family law.
Microsoft 365	Tenant: ironbarklegal.onmicrosoft.com. 20 × Business Standard licences. 4 shared mailboxes (info, reception, accounts, conveyancing). Secure Score 36%, reviewed once 2 years ago.
Identity	Hybrid: on-premise Active Directory (ironbark.local) synced to Entra ID. 5 privileged accounts total: 2 on-prem Domain Admins, 3 Microsoft 365 Global Administrators. One Domain Admin shared with the prior IT provider.
Endpoints	22 devices: 18 laptops, 4 desktops. All running Windows 11 Pro. Joined to the on-prem domain. Average age 2.1 years. Not enrolled in Intune.
Server	One on-premise server: HPE ProLiant ML350 Gen10 running Windows Server 2019 Standard. Roles: File server, Print server, Active Directory Domain Controller, Hyper-V host for a legacy scan-to-folder tool. Last OS patch November 2025.
Line-of-business apps	Leap (cloud practice management and trust accounting), InfoTrack (searches and settlements), SettleIt (e-conveyancing), DocuSign, Xero (firm accounts, not trust).
Backup	Veeam Backup & Replication writes daily backups to a local Synology RS1221+ NAS on the domain. USB rotation was started but last rotated January 2026. No cloud copy. No immutability. No Microsoft 365 backup. Last successful restore test 8 months ago.
Network	Ubiquiti UniFi Dream Machine Pro firewall, 2 × UniFi 24-port switches, 3 × UniFi access points. Segmented: staff Wi-Fi, guest Wi-Fi (separate VLAN), server VLAN. Default admin password still set on one of the switches. Inbound firewall rule "Remote Admin" forwards TCP 3389 from internet to the server.
Security tools	SentinelOne Control (20 device licences) installed on workstations. Management console: no one has logged in for 6 months. Two devices do not show in the console (agent not installed or stale).
IT governance	No written IT policies (0 of 4: backup, acceptable use, password, onboarding / offboarding). No documented incident response plan. Prior IT support: "Quick Fix IT", ad-hoc single engineer, break-fix only. Agreement ended December 2025.
Cyber insurance	Chubb Cyber Liability, $3M cover, renewal July 2026. Policy conditions require MFA on all accounts, managed EDR with active monitoring, immutable tested backup, and patching within 30 days. Current setup does not meet three of these conditions.
Compliance context	Legal Profession Uniform Law (NSW) Part 4.2 solicitor trust account rules apply. Legal professional privilege attaches to client communications. Australian Privacy Act and Notifiable Data Breaches scheme apply. Lawcover (compulsory PI insurer) security questionnaire due at renewal.

03 · FINDINGS SUMMARY

15 findings, ranked by risk.

Each finding is rated by severity. The severity rating drives the recommended timeframe for action. Detailed findings begin on the next page.

CRITICAL
Active exposure to data loss, ransomware, or regulatory breach.
FIX WITHIN 14 DAYS

HIGH
Significant gap that creates a clear path for attackers.
FIX WITHIN 30 DAYS

MEDIUM
Inconsistent control, should be closed in a structured plan.
FIX WITHIN 60 DAYS

LOW
Minor gap or best-practice improvement.
FIX WITHIN 90 DAYS

#	FINDING	SEVERITY	AREA	RECOMMENDED BY
C1	Remote Desktop port 3389 open to the public internet	CRITICAL	Network	10 Apr 2026 (24h)
C2	Backups are not immutable, not offsite, and not tested	CRITICAL	Backup & recovery	23 Apr 2026
C3	MFA incomplete and admin sprawl across two identity systems	CRITICAL	Identity & access	23 Apr 2026
H1	SentinelOne EDR installed but unmonitored	HIGH	Endpoint security	9 May 2026
H2	Default credentials still in place on one managed switch	HIGH	Network	9 May 2026
H3	All staff have local administrator rights on their devices	HIGH	Endpoint security	9 May 2026
H4	Windows Server 2019 not patched; broad antivirus exclusions	HIGH	Server	9 May 2026
H5	Email authentication weak (SPF soft-fail, no DKIM, no DMARC)	HIGH	Email security	9 May 2026
M1	No device management (Intune / MDM) across the fleet	MEDIUM	Endpoint security	8 Jun 2026
M2	No separate Microsoft 365 backup	MEDIUM	Backup & recovery	8 Jun 2026
M3	No written IT policies; no documented incident response plan	MEDIUM	Governance	8 Jun 2026
M4	Defender for Office 365 features not configured	MEDIUM	M365 security	8 Jun 2026
L1	No security awareness training or phishing simulation	LOW	Staff practices	8 Jul 2026
L2	Leap admin roles not segregated; too many full admins	LOW	LOB apps	8 Jul 2026
L3	No device disposal or certificate of destruction process	LOW	Governance	8 Jul 2026

04 · CRITICAL FINDINGS

Fix these within 14 days. C1 within 24 hours.

FINDING C1

Remote Desktop (port 3389) open to the public internet

CRITICAL

NETWORK

WHAT WE FOUND

The UniFi Dream Machine Pro has an inbound firewall rule named "Remote Admin" forwarding TCP port `3389` from any public IP address to `10.0.0.5` (the on-premise server). The rule was created in 2022, likely by the previous IT provider for after-hours access. It is still active. A public IP scan against the firm's static IP returns an open RDP service on port 3389.

WHY IT MATTERS

Internet-exposed RDP is the single most exploited attack path against Australian SMBs in 2026. Automated bots scan every Australian IP range continuously, brute-force passwords, and drop ransomware within hours of finding a weak account. Behind the server sit 20 solicitors' mailboxes, the domain controller, and the file share holding client files across every practice area. A successful compromise would constitute a data breach under the Notifiable Data Breaches scheme and almost certainly a waiver of legal professional privilege for the documents accessed.

ACTION

Close the rule today. Remove the "Remote Admin" inbound rule on the UniFi firewall. If after-hours server access is needed, deploy a VPN (e.g. UniFi Teleport, WireGuard) with MFA. Verify closure with an external port scan after the change.

EFFORT

15 minutes to remove the rule. 2 to 3 hours to stand up a proper MFA-gated VPN if required.

FINDING C2

Backups are not immutable, not offsite, and not tested

CRITICAL

BACKUP & RECOVERY

WHAT WE FOUND

Veeam Backup & Replication runs nightly backups of the server to a Synology RS1221+ NAS. The NAS is domain-joined using a local admin credential. USB rotation was designed but last performed in January 2026. There is no cloud copy. No immutability. Microsoft 365 data is not backed up separately. Last successful restore test was 8 months ago.

WHY IT MATTERS

Because the NAS is domain-joined and accessible over SMB, a ransomware attack that reaches the server will also encrypt the Veeam backups. The firm would lose the live data and the recovery copies in the same incident. In a law firm context this means losing in-flight matter files, trust account records (required for Part 4.2 compliance), and privileged communications. Chubb's cyber policy requires tested, immutable, offsite backup as a condition of cover. Current arrangements do not meet that condition.

ACTION

Reconfigure Veeam to write to an **immutable** hardened Linux repository (or replace with Veeam Cloud Connect) and add a cloud offsite copy (Wasabi, Backblaze, or Azure Blob with immutability). Add a separate Microsoft 365 backup (e.g. Veeam for Microsoft 365, Dropsuite, Keepit). Document RTO of 4 hours for trust account data, 8 hours for working files. Automate monthly restore test with email alerting.

EFFORT

10 to 14 hours for the full rebuild. No downtime to live systems.

04 · CRITICAL FINDINGS (CONTINUED)

Identity and admin sprawl.

FINDING C3

MFA incomplete and admin sprawl across two identity systems

CRITICAL

IDENTITY & ACCESS

WHAT WE FOUND

Six Microsoft 365 accounts do not have MFA enabled: two paralegals, two reception, one shared conveyancing account, one shared accounts mailbox. Five privileged accounts exist in total: 2 on-premise Domain Admins (one shared with the prior IT provider, "Quick Fix IT") and 3 Microsoft 365 Global Administrators. No dedicated break-glass admin. No Conditional Access policies. Legacy authentication not blocked. Several solicitors use the same account for daily work and privileged tasks in Leap.

WHY IT MATTERS

Law firms are a high-value target for business email compromise focused on conveyancing settlement redirection: one phished email to a client before settlement, with altered bank details, can move six or seven figures in minutes. One of those six non-MFA accounts handles reception and accounts correspondence. The shared Domain Admin with a former IT provider means someone outside the firm still has full control of the server. A credential from any of those accounts gives an attacker a direct path to trust account data and privileged client communications.

ACTION

Enforce MFA on all user and admin accounts via Conditional Access. Create one dedicated cloud-only **break-glass Global Admin** with sealed credentials. Separate daily-use accounts from admin accounts. Rotate the shared Domain Admin password and remove the former provider's access. Block legacy authentication. Reduce privileged accounts from 5 to 3 (2 admins + 1 break-glass).

EFFORT

6 to 8 hours. MFA rollout requires 15 minutes per staff member. No downtime.

05 · HIGH FINDINGS

Fix these within 30 days.

FINDING H1

SentinelOne EDR installed but unmonitored

HIGH

ENDPOINT SECURITY

WHAT WE FOUND

The firm pays for 20 SentinelOne Control licences (approximately $120 per month). The management console has not been logged into for 6 months. Two workstations do not appear in the console (agent not installed or stale). No alert routing is configured. No one is responsible for reviewing detections.

WHY IT MATTERS

An unmanaged EDR provides some protection (the agent still detects and blocks known threats) but misses most of the value. A real attack triggers alerts that nobody reads, which is indistinguishable from having no alerts at all. The firm is paying for visibility it is not consuming. Chubb's cyber policy requires "managed EDR with active monitoring" as a condition of cover.

ACTION

Either (a) transfer the SentinelOne tenant to a managed provider who actively monitors detections with documented SLAs, or (b) migrate to Microsoft Defender for Business (included in Business Premium) and monitor it centrally. Reconcile coverage to 22 of 22 devices. Configure email alerts to a monitored address. Document response procedures.

EFFORT

4 to 6 hours to reconcile and transfer. Ongoing monitoring becomes part of managed IT.

05 · HIGH FINDINGS (CONTINUED)

Network and endpoint privilege.

FINDING H2

Default credentials still in place on one managed switch

HIGH

NETWORK

WHAT WE FOUND

Of the two UniFi 24-port switches, one (USW-24-POE, MAC ending `...A3:7F`) still has the factory default credentials. The other switch and the UDM Pro have been changed. The switch manages the server VLAN.

WHY IT MATTERS

Any device on the network (including a visitor who joins guest Wi-Fi and then pivots, or a compromised workstation) could log into that switch and reroute traffic, disable ports, or mirror the server VLAN to an attacker-controlled port. Default credentials are the first thing an automated attacker tries after gaining a foothold.

ACTION

Change the admin password on the affected switch. Set a new strong password for all network equipment, stored in a team password manager. Confirm all network device management interfaces are on the management VLAN, not the staff VLAN.

EFFORT

30 minutes.

FINDING H3

All staff have local administrator rights on their devices

HIGH

ENDPOINT SECURITY

WHAT WE FOUND

On every device we checked (sample of six across four staff members), the primary user is a member of the local Administrators group via a domain group policy that grants "Domain Users" local admin. Staff can install any software, disable SentinelOne, change system settings, and run scripts without approval.

WHY IT MATTERS

Local admin rights are the single largest multiplier of damage in a ransomware incident. A phishing email landing on a non-admin account can usually be contained. The same email on an admin account ends with the device encrypted, security tools disabled, and pivot to the domain controller. Restricting admin rights is one of the Essential Eight controls and appears on Lawcover's security questionnaire.

ACTION

Remove the "Domain Users is a local admin" group policy. Create a single per-device local admin account used only when elevation is genuinely needed. Document the approved software list for solicitors (Leap, InfoTrack, DocuSign, Office, Teams, Chrome, Edge, Adobe Reader, team password manager). Anything outside goes through a request.

EFFORT

1 to 2 hours to change the policy. 2 to 3 hours to resolve individual "software breakage" requests in the first week.

05 · HIGH FINDINGS (CONTINUED)

Server hygiene and email authentication.

FINDING H4

Windows Server 2019 not patched; overly broad antivirus exclusions

HIGH
SERVER

WHAT WE FOUND

The HPE ProLiant server was last patched in November 2025. Five months of security updates are missing, including fixes for known exploited vulnerabilities. SentinelOne is installed on the server with exclusions for the entire `C:\Data`, `C:\Leap`, and `C:\Scans` directories, set by the prior IT provider to resolve a performance complaint that has since been resolved by an application update. Windows Server 2019 mainstream support ends January 2029, so the OS itself is still viable with patching.

WHY IT MATTERS

Unpatched servers are the lowest-hanging fruit for ransomware operators, particularly when combined with C1 (RDP exposed) or any phished admin credential. The broad antivirus exclusions mean that if an attacker drops tooling into `C:\Data`, SentinelOne will not see it. Excluding directories where client files live is the exact opposite of what the exclusion is for.

ACTION

Apply all outstanding Windows updates in a planned maintenance window. Review SentinelOne exclusions and remove the three directory-wide entries. Replace with narrow file or process exclusions only where genuinely required. Document exclusions with justification and review annually.

EFFORT

3 to 4 hours, plus a 1 hour planned outage for reboot.

FINDING H5

Email authentication weak: SPF soft-fail, no DKIM, no DMARC

HIGH
EMAIL SECURITY

WHAT WE FOUND

The `ironbarklegal.com.au` domain has SPF in soft-fail (`~all`) instead of hard-fail (`-all`). DKIM not configured. No DMARC record. External email tagging is off.

WHY IT MATTERS

An attacker can send email that appears to come from the firm's own domain, instructing a client about to settle a property transaction to pay into a different bank account. Conveyancing settlement redirection is one of the most common and costly attacks against Australian law firms. A successful fraud creates exposure for the firm under trust account obligations and can trigger Lawcover claims. The firm's reputation is staked on every invoice it sends.

ACTION

Configure SPF hard-fail, enable DKIM signing, publish DMARC. Begin DMARC at `p=none` for reporting, review reports for 2 weeks, then escalate to `p=quarantine` and `p=reject`. Enable external sender warning banners in Outlook.

EFFORT

3 to 4 hours configuration. 2 weeks DMARC monitoring before hardening.

06 · MEDIUM FINDINGS

Fix these within 60 days.

FINDING M1

No device management (Intune / MDM) across the fleet

MEDIUM

ENDPOINT SECURITY

WHAT WE FOUND	No devices enrolled in Microsoft Intune or any other device management platform. Policies are applied via on-premise Group Policy, but with 18 laptops that leave the office regularly, GPO only applies when a device is on the corporate network or VPN. Patching of workstations is left to Windows Update defaults. No remote wipe capability.
WHY IT MATTERS	A lost or stolen solicitor's laptop today contains cached copies of client files, browser saved passwords for Leap and InfoTrack, and domain credentials. Without central management, most recommendations in this report cannot be enforced over time as the fleet changes.
ACTION	Enrol all 22 devices in Intune. Baseline policy: BitLocker required, screen lock after 10 minutes, SentinelOne or Defender enabled, remote wipe capable, patching deadline 14 days. Intune is included with Microsoft 365 Business Premium.
EFFORT	Initial setup 6 to 8 hours. 15 minutes per device enrolment. Ongoing enforcement automatic.

FINDING M2

No separate Microsoft 365 backup

MEDIUM

BACKUP & RECOVERY

WHAT WE FOUND	The firm relies on Microsoft's native 30-day deleted-item retention for email and 93-day retention for deleted OneDrive / SharePoint files. No third-party Microsoft 365 backup in place. Solicitors store email threads as the authoritative record of advice given.
WHY IT MATTERS	Microsoft's shared responsibility model makes the firm responsible for long-term retention and recovery from accidental or malicious deletion. For a law firm, the consequence is not just operational: the firm may have retention obligations for client records for 7 years or more, and the ability to produce correspondence from 5 years ago on discovery is a professional requirement.
ACTION	Add a Microsoft 365 backup (e.g. Veeam for Microsoft 365, Dropsuite, Keepit) with 10-year retention minimum. Addressed alongside the C2 backup rebuild.
EFFORT	Included in C2.

06 · MEDIUM FINDINGS (CONTINUED)

Governance and email security features.

FINDING M3

No written IT policies; no documented incident response plan

MEDIUM
GOVERNANCE

WHAT WE FOUND	No written backup and recovery policy. No acceptable use policy. No password and access control policy. No documented onboarding / offboarding procedure. No incident response plan setting out who to call and in what order if an incident occurs out of hours. IT practices exist informally.
WHY IT MATTERS	Lawcover's security questionnaire at policy renewal asks explicitly for written IT policies and an incident response plan. Chubb will do the same. Beyond insurance, the firm has obligations under the Legal Profession Uniform Law and Privacy Act to demonstrate reasonable steps; an undocumented practice is hard to defend in a privacy complaint. If an incident happens at 7pm on a Friday, the worst time to decide who to call is at 7pm on a Friday.
ACTION	Draft five short documents (1 to 2 pages each): backup & recovery, acceptable use, password & access, onboarding / offboarding, and a 1-page incident response playbook (phone tree, first-24-hour actions, notification decision tree). Review annually at partner meeting.
EFFORT	6 to 8 hours using standard SMB templates.

FINDING M4

Defender for Office 365 features not configured

MEDIUM
M365 SECURITY

WHAT WE FOUND	Safe Links, Safe Attachments, impersonation protection, and anti-phishing policies in Microsoft Defender for Office 365 are not configured. Business Standard does not include Defender for Office 365 by default; the features would be unlocked by an upgrade to Business Premium.
WHY IT MATTERS	Safe Links rewrites URLs so a phishing link that passes initial scanning can still be blocked at click-time. Safe Attachments detonates attachments in a sandbox before delivery. Impersonation protection flags email that pretends to be from a principal or from a settling party. All three are the first line of defence for a law firm targeted by settlement redirection fraud.
ACTION	As part of the Business Premium upgrade recommended in H1, configure Safe Links, Safe Attachments, anti-phishing, and impersonation protection. Enable quarantine notifications so users can self-release false positives.
EFFORT	3 to 4 hours, bundled with the Business Premium rollout.

07 · LOW FINDINGS

Address these within 90 days.

Best-practice improvements. They do not create immediate risk but should be closed once the critical, high, and medium findings are handled.

FINDING L1

No security awareness training or phishing simulation

LOW
STAFF PRACTICES

WHAT WE FOUND	Staff have not received formal security awareness training. No phishing simulation has been run. No "Report phishing" button in Outlook. Solicitors are the primary target for settlement redirection but have no specific training on the pattern.
WHY IT MATTERS	The majority of incidents start with a staff member clicking a link or opening an attachment. Conveyancing-focused phishing is a known, specific pattern that staff can be trained to recognise.
ACTION	Roll out a short quarterly awareness programme (10 minute video each quarter) including a dedicated module on settlement redirection. Run two phishing simulations per year. Add a one-click "Report phishing" button in Outlook.
EFFORT	Setup 2 to 3 hours. Approx 1 hour per quarter per staff member.

FINDING L2

Leap admin roles not segregated; too many full admins

LOW
LOB APPS

WHAT WE FOUND	Both principals, the office manager, and one paralegal have full administrator rights in Leap (including trust accounting administration). Four admins for a 20-person firm is more than needed and creates trust account audit questions.
WHY IT MATTERS	Part 4.2 of the Legal Profession Uniform Law and the associated Uniform Rules require appropriate segregation of duties around trust accounting. Multiple full admins means no single-person accountability for trust account entries and complicates the annual external examination.
ACTION	Reduce full Leap administrators to two (both principals). Office manager and paralegal roles moved to specific role-based permissions. Document who can create, approve, and reconcile trust transactions.
EFFORT	1 to 2 hours.

FINDING L3

No device disposal or certificate of destruction process

LOW
GOVERNANCE

WHAT WE FOUND	Three retired laptops are stored in a cupboard at reception. No documented process for secure wipe or destruction. No certificate of destruction retained for previously disposed devices.
WHY IT MATTERS	Devices used by solicitors contain cached client files, email, and credentials. Unsecured retired devices are a slow-burn data breach risk. Chubb and Lawcover expect a documented disposal process.
ACTION	Wipe the three retired devices using a verified method (BitLocker key destruction on a full disk, then factory reset). Define a standard disposal process going forward: secure wipe, certificate of destruction from a provider, retention of certificates for 7 years.
EFFORT	1 to 2 hours for the three devices; standing process thereafter.

08 · ESSENTIAL EIGHT ALIGNMENT

How the firm measures against the ACSC baseline.

The Essential Eight is the set of mitigation strategies recommended by the Australian Cyber Security Centre. Level 1 is the minimum recommended for all organisations. Ironbark Legal currently meets zero of eight controls at Level 1 (three are partially implemented).

CONTROL	STATUS	NOTES
Multi-factor authentication	PARTIAL	Enabled for 14 of 20 accounts. Six missing. Not enforced by Conditional Access. Addressed by C3.
Regular backups	PARTIAL	Veeam backup exists but is not immutable, not offsite, not tested, and excludes Microsoft 365. Addressed by C2 and M2.
Patch operating systems	PARTIAL	Workstation patching ad-hoc via Windows Update. Server 5 months behind. Addressed by H4 and M1.
Patch applications	NOT IMPLEMENTED	No central patching of Office, browsers, PDF readers, or helper apps across the fleet. Addressed by M1.
Restrict administrative privileges	NOT IMPLEMENTED	Domain Users group is local admin. Five privileged accounts with no break-glass. Addressed by C3 and H3.
Application control	NOT IMPLEMENTED	No restrictions on software installation. Addressed by Intune rollout (M1) and H3.
Configure Microsoft Office macros	NOT IMPLEMENTED	Default macro settings. Internet-originated macros are not blocked. Addressed by M1.
User application hardening	NOT IMPLEMENTED	Flash, Java, ads, and auto-run are not hardened. Legacy browser settings in place. Addressed by M1.

Essential Eight Level 1: 0 of 8 fully met, 3 partially met.

Implementing the findings in this report moves the firm from 0 to 7 of 8 at Level 1 within 90 days. Full Level 1 alignment requires the Intune rollout (M1) to be operational, at which point macro and application hardening can be enforced centrally and patch management becomes consistent.

Essential Eight alignment is not a legal requirement for private-sector SMBs. It is increasingly cited in cyber insurance questionnaires (Chubb, Lawcover) and is an accepted defensible baseline if the firm ever faces a privacy complaint under the Notifiable Data Breaches scheme. Meeting Level 1 on all eight controls materially reduces exposure to the most common attack patterns affecting Australian businesses and demonstrates reasonable steps under the Privacy Act.

09 · REMEDIATION ROADMAP

The plan, in order.

A 90-day sequenced plan to close every finding in this report. The order reduces risk first and avoids rework: emergency closure of the internet-facing exposure, then identity, then endpoints, then policies.

PHASE 0 · BY 10 APRIL (24 HOURS) Close the front door

One action. Today.

1	C1	Remove the "Remote Admin" inbound rule on the UniFi firewall; verify with external scan	15 minutes

PHASE 1 · BY 23 APRIL Stop the bleeding (14 days)

The other two criticals. Identity and backup.

2	C2	Rebuild backup with immutable repository + cloud offsite + M365 backup; test restore	10 to 14 hours
3	C3	Enforce MFA; break-glass admin; rotate shared Domain Admin; block legacy auth; reduce privileged accounts 5 to 3	6 to 8 hours

PHASE 2 · BY 9 MAY Fix the visible layer (30 days)

Endpoint, server, network, email authentication.

4	H1	Transfer SentinelOne to managed monitoring or migrate to Defender for Business	4 to 6 hours
5	H2	Change default credentials on affected switch; rotate all network device passwords	30 minutes
6	H3	Remove "Domain Users = local admin" policy; standard user model	1 to 2 hours + support
7	H4	Apply outstanding Windows Server updates; remove over-broad AV exclusions	3 to 4 hours + 1h outage
8	H5	Configure SPF hard-fail, DKIM, DMARC; external email tagging	3 to 4 hours + monitoring

PHASE 3 · BY 8 JUNE Make it stick (60 days)

Central management, governance, insurance-aligned controls.

9	M1	Enrol 22 devices in Intune; apply baseline policy	Setup 6 to 8 hours; 15 min / device
10	M2	Microsoft 365 backup (addressed with C2)	Included in C2
11	M3	Draft IT policies and incident response plan; partner sign-off	6 to 8 hours
12	M4	Configure Defender for Office 365 (Safe Links, Safe Attachments, anti-phishing)	3 to 4 hours (bundled)

PHASE 4 · BY 8 JULY Refine and maintain (90 days)

13	L1	Security awareness programme; conveyancing-specific phishing simulation	2 to 3 hours setup
14	L2	Reduce Leap full admins to 2; define role-based permissions	1 to 2 hours
15	L3	Wipe retired devices; document disposal and certificate retention process	1 to 2 hours + process

10 · WHAT HAPPENS NEXT

This report is yours. How you act on it is up to you.

Ironbark Legal now has a written, prioritised view of what to fix and in what order. If a different provider implements this report, it is still a useful document. If CIO Tech implements it, here are the two shapes that takes.

OPTION 1

Project-based remediation

CIO Tech scopes the roadmap above as a fixed-price project. Once the fixes are in, the engagement ends. Suitable if the firm has a separate plan for ongoing IT support. Indicative project fee in the range of $15,000 to $30,000 plus hardware, software, and licences.

OPTION 2 · RECOMMENDED

CIO Tech Assured (managed IT)

CIO Tech delivers the roadmap as part of onboarding the firm to our managed service. Fixes get implemented, then we stay to keep them working: patching, monitoring, backup verification, security, EDR monitoring, and support. Based on the findings, the fit for a 20-person firm with an on-premise server is the **Business tier from $1,000 per month**.

Why Business tier, not Essentials. Essentials is sized for 1 to 15 users with a simpler risk profile. This audit identified three critical and five high findings, an on-premise server, a cyber insurance policy with technical conditions, and line-of-business applications (Leap, InfoTrack, SettleIt) that need active support. Business tier includes everything needed to execute this report and hold it in place over time: managed EDR monitoring, Intune, Microsoft 365 hardening, server management, monthly security review, unlimited support. Given the findings and the firm's compliance surface, the predictable monthly cost replaces the reactive spend pattern that produced the gaps this report has just documented.

NEXT STEP

A 30-minute walk-through of this report, and a tailored Assured proposal within 5 business days.

The natural next step is a short call to walk through the findings, answer questions, and decide whether Option 1 or Option 2 fits the firm. If Assured is the right fit, CIO Tech will produce a fixed-price proposal tailored to Ironbark Legal, covering the findings in this report and ongoing managed IT from month one.

Book the walk-through | ciotech.com.au

Limitations. CIO Tech identifies risks and recommends controls. Implementing these recommendations significantly reduces exposure to the most common threats facing Australian SMBs. No IT provider can guarantee prevention of all security incidents; effective security requires ongoing attention after the findings in this report are closed.

Prepared by. Birender Chahal, CIO Tech Pty Ltd · 217/14 Lexington Drive, Bella Vista NSW 2153 · birender@ciotech.com.au · ciotech.com.au · Audit ID AUD-2026-0042.