PREPARED FOR

Harbourline Advisory Pty Ltd

# IT Audit Risk Report April 2026

A half-day on-site assessment of Harbourline Advisory's IT environment, conducted on Wednesday 8 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 |
|---|---|---|---|
| 8 April 2026 | 14 April 2026 | Birender Chahal | AUD-2026-0041 |

01 · EXECUTIVE SUMMARY

# A mixed posture with two critical gaps. Addressable in 90 days.

CIO Tech conducted a half-day on-site assessment of Harbourline Advisory on Wednesday 8 April 2026, covering the Microsoft 365 tenant, 15 endpoints, the Synology file server, backup arrangements, and the network. The foundations are in place: Microsoft 365 is set up, staff are productive, client work is getting done.

The assessment identified **14 findings across four severity levels, including two critical gaps that expose the practice to data loss and account compromise**. The most urgent finding is that the current backup can be encrypted or deleted in a ransomware event, so a single attack could destroy the firm's client files and the recovery copies at the same time. The second critical finding is that multi-factor authentication is missing on four staff accounts and the principal's daily-use account is a Global Administrator, which hands an attacker who compromises one password the keys to the whole tenant.

None of these gaps are unusual for a 15-person practice without a dedicated IT provider, and all of them are fixable. This report sets out a 90-day remediation roadmap, prioritised by risk, so the practice knows what to do first, what to do next, and what can wait.

OVERALL IT POSTURE

## At Risk

The practice is exposed to the two most common threats facing Australian SMBs in 2026: ransomware and business email compromise. Both are addressable. None of the findings require a full rebuild. They require focused remediation over the next 90 days.

| 2 | 5 | 4 | 3 |
|---|---|---|---|
| CRITICAL FINDINGS | HIGH FINDINGS | MEDIUM FINDINGS | LOW FINDINGS |

TOP THREE TO ADDRESS FIRST

| | |
|---|---|
| C1 | **Backups can be destroyed by ransomware.** The Synology to USB backup is not immutable, not tested, not offsite. Fix within 14 days. |
| C2 | **MFA gaps and admin sprawl.** Four accounts without MFA; three Global Admins; the principal's daily account holds full tenant control. Fix within 14 days. |
| H1 | **No managed endpoint security.** Microsoft Defender Free only, no central visibility. An infection would be invisible until damage is done. Fix within 30 days. |

02 · ENVIRONMENT OVERVIEW

# What was assessed.

A half-day, on-site assessment at Harbourline Advisory, Level 5, 30 Phillip Street, Parramatta. The environment below reflects the state at the time of the audit.

| | |
|---|---|
| **Staff & scope** | 15 staff (12 accountants, 1 office manager, 1 reception, 1 principal). Mixed office and work-from-home. Two partners. |
| **Microsoft 365** | Tenant: harbourlineadvisory.onmicrosoft.com. 15 × Business Standard licences. 3 shared mailboxes (reception, accounts, smsf). Secure Score 28%, never reviewed. |
| **Identity** | Entra ID only (no on-premise Active Directory). 3 Global Administrator accounts. Principal's daily-use account holds Global Admin. No break-glass account. |
| **Endpoints** | 15 devices: 12 laptops, 3 desktops. 13 on Windows 11, 2 on Windows 10 22H2 (end of support October 2025, currently unsupported). Average age 3.2 years. Not enrolled in Intune. |
| **Servers** | No on-premise servers. One Synology DS220+ NAS (NAS-HA-01) used for shared document archive and as the current backup target. |
| **Line-of-business apps** | Xero (practice and multiple client files), MYOB AccountantsEnterprise (practice management), CAS360 (ASIC corporate compliance), FYI Docs (document management), Practice Ignition (engagements). |
| **Backup** | Scheduled script copies Synology NAS to an external USB drive weekly. USB permanently connected. No offsite copy. No immutability. No separate Microsoft 365 backup. Last successful restore test unknown (> 14 months). |
| **Network** | Consumer-grade Netgear Nighthawk router (over 5 years old, firmware 18 months out of date). Single flat network. Guest Wi-Fi shares the VLAN with business devices. No DNS filtering. |
| **Security tools** | Microsoft Defender Free on each device, locally managed. No EDR. No central security dashboard. No managed patching. No Intune, no Defender for Business. |
| **IT governance** | No written IT policies (0 of 4: backup & recovery, acceptable use, password, onboarding / offboarding). No documented incident response plan. Previous IT support was informal, by a partner's nephew. |
| **Cyber insurance** | CGU Cyber Liability, $2M cover. Policy conditions require MFA on all accounts, managed EDR, and patching within 30 days. Current setup does not meet these conditions. |
| **Compliance context** | Tax Practitioners Board registration. APES 325 risk management standard applies. Australian Privacy Act and Notifiable Data Breaches scheme apply (firm holds personal tax and financial data). |

03 · FINDINGS SUMMARY

# 14 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 | Backups are not immutable, not offsite, and not tested | CRITICAL | Backup & recovery | 22 Apr 2026 |
| C2 | MFA gaps and daily-use Global Admin account | CRITICAL | Identity & access | 22 Apr 2026 |
| H1 | No managed endpoint detection and response (EDR) | HIGH | Endpoint security | 8 May 2026 |
| H2 | All staff have local administrator rights | HIGH | Endpoint security | 8 May 2026 |
| H3 | Consumer-grade firewall with outdated firmware; flat network | HIGH | Network | 8 May 2026 |
| H4 | Email authentication weak (SPF soft-fail, no DKIM, no DMARC) | HIGH | Email security | 8 May 2026 |
| H5 | Two endpoints on unsupported Windows 10 | HIGH | Endpoint security | 8 May 2026 |
| M1 | No device management (Intune / MDM) across the fleet | MEDIUM | Endpoint security | 7 Jun 2026 |
| M2 | Defender for Office 365 features not configured | MEDIUM | M365 security | 7 Jun 2026 |
| M3 | No written IT policies (0 of 4) | MEDIUM | Governance | 7 Jun 2026 |
| M4 | No separate Microsoft 365 backup | MEDIUM | Backup & recovery | 7 Jun 2026 |
| L1 | No security awareness training or phishing simulation | LOW | Staff practices | 7 Jul 2026 |
| L2 | Shared mailbox passwords stored in spreadsheet | LOW | Identity & access | 7 Jul 2026 |
| L3 | Inconsistent device build; no standard operating environment | LOW | Endpoint security | 7 Jul 2026 |

04 · CRITICAL FINDINGS

# Fix these within 14 days.

FINDING C1

## Backups are not immutable, not offsite, and not tested

CRITICAL

BACKUP & RECOVERY

**WHAT WE FOUND**

A weekly scheduled script copies files from the Synology DS220+ NAS to an external USB drive attached to the NAS. The USB drive is permanently connected. No offsite or cloud copy. Backup has no immutability (it can be overwritten or deleted). Microsoft 365 data is not backed up separately from Microsoft's native retention. Last successful restore test more than 14 months ago. No documented recovery time or recovery point objective.

**WHY IT MATTERS**

If ransomware reaches the NAS, it will also reach the USB backup (same network, same credentials). The practice would lose live client files and the recovery copies at the same time. A single incident could force Harbourline to choose between paying the attacker or rebuilding files from email attachments. Insurer CGU requires a tested, offsite, immutable backup as a condition of cover; current arrangements do not meet that condition.

**ACTION**

Implement **immutable, offsite, tested backup** covering both the Synology file store and Microsoft 365 (mail, SharePoint, OneDrive, Teams). Target: daily backups, 30 day immutability minimum, geographically separate storage, automated monthly restore test with email alert on failure. Document RTO 8 business hours, RPO 24 hours.

**EFFORT**

8 to 12 hours to configure and seed the initial backup. No downtime. One test restore to validate.

FINDING C2

## MFA gaps and daily-use Global Administrator account

CRITICAL

IDENTITY & ACCESS

**WHAT WE FOUND**

Four Microsoft 365 accounts do not have MFA enabled: reception, two junior accountants, and the shared smsf@ mailbox. Three Global Administrator accounts exist, and the principal uses one of them as a daily working account. No dedicated break-glass admin account. No Conditional Access policies. Legacy authentication is not blocked.

**WHY IT MATTERS**

Accountants are a priority target for business email compromise because they approve payments and hold client banking details. One phished password on a non-MFA account gives an attacker inbox access and the ability to redirect invoices. A phished password on the principal's Global Admin account gives the attacker the entire tenant: all staff mailboxes, all client files, password resets. The firm's cyber insurer requires MFA on all accounts as a policy condition.

**ACTION**

Enforce MFA on all user and admin accounts via Conditional Access (not per-user MFA). Create one dedicated cloud-only **break-glass Global Admin** with a stored, sealed password. Remove Global Admin from the principal's daily account; replace with a separate admin-only login used only when privileged action is required. Block legacy authentication. Reduce Global Admins from 3 to 2.

**EFFORT**

4 to 6 hours. MFA rollout requires a short staff communication and 15 minutes per person to set up Authenticator. No downtime.

05 · HIGH FINDINGS

# Fix these within 30 days.

FINDING H1

## No managed endpoint detection and response (EDR)

HIGH

ENDPOINT SECURITY

**WHAT WE FOUND**

Every device runs the free Microsoft Defender that ships with Windows. No central management console, no behaviour-based detection, no automated isolation, no cross-fleet visibility. If one laptop is infected tomorrow, nobody is alerted. There is no dashboard to check whether antivirus is active and up to date across the 15 devices; that check must be done manually, device by device.

**WHY IT MATTERS**

Free Defender blocks known malware but does not detect the behaviours that define a real attack (credential theft, lateral movement, ransomware staging). A single undetected infection gives an attacker time to pivot to the Synology NAS, the Xero logins stored in browsers, and the principal's mailbox. CGU's policy requires managed EDR as a condition of cover.

**ACTION**

Deploy **Microsoft Defender for Business** (included in Microsoft 365 Business Premium) or an equivalent managed EDR across all 15 devices. Central dashboard, behaviour-based detection, automated isolation of compromised devices, monthly alert review. This triggers a licence review: Business Premium is typically $6 to $8 per user per month above Business Standard.

**EFFORT**

6 to 8 hours to configure centrally. Agent deployment automatic once devices are enrolled. No downtime.

FINDING H2

## All staff have local administrator rights on their devices

HIGH

ENDPOINT SECURITY

**WHAT WE FOUND**

On every device we checked (sample of five across four staff), the primary user is a member of the local Administrators group. Staff can install any software, disable Defender, change system settings, and run scripts without approval. No standard user model.

**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 often ends with the whole device encrypted and tools disabled. Restricting admin rights is one of the Essential Eight controls and appears on most cyber insurance questionnaires.

**ACTION**

Move all staff to standard user accounts. Create one separate local admin account per device, used only when software genuinely requires elevation. Document the approved software list (Xero, MYOB AE, CAS360, FYI, Office, Teams, Chrome, Edge, team password manager). Anything outside that list goes through a request.

**EFFORT**

1 to 2 hours per device manually (20 to 30 hours total). Drops to a single policy change once Intune is deployed (see M1).

05 · HIGH FINDINGS (CONTINUED)

# Network, email authentication, and unsupported operating systems.

FINDING H3

## Consumer-grade firewall with outdated firmware; flat network

HIGH

NETWORK

| | |
|---|---|
| WHAT WE FOUND | Office runs on a Netgear Nighthawk R7000 (a home router, over 5 years old). Firmware 18 months out of date. No separate guest network; visitors given the Wi-Fi password sit on the same flat network as business devices and the Synology NAS. No DNS filtering. No remote access VPN. |
| WHY IT MATTERS | Consumer equipment is not built for continuous business use or rapid patching against new exploits. A flat network means any compromised device (including a visitor's phone) is one hop from the NAS holding client files. Old firmware means known vulnerabilities remain open. |
| ACTION | Replace with a managed business firewall (e.g. Fortinet FortiGate 40F), segment the network (guest Wi-Fi on a separate VLAN with no path to the Synology or office devices), enable DNS filtering, subscribe to automatic firmware updates. |
| EFFORT | 4 to 6 hours on-site. One 30-minute outage for the switchover. Hardware $600 to $900 plus $30 to $50 / month for subscriptions. |

FINDING H4

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

HIGH

EMAIL SECURITY

| | |
|---|---|
| WHAT WE FOUND | The `harbourlineadvisory.com.au` domain has SPF in soft-fail ( `~all` ) instead of hard-fail ( `-all` ). DKIM not configured. No DMARC record. External email tagging off. |
| WHY IT MATTERS | An attacker can send email that appears to come from the firm's own domain ("domain spoofing"). Clients receive what looks like a message from a partner, instructing them to pay into a different bank account. The practice's reputation is staked on every invoice it sends; a successful spoof damages long-standing client relationships even when no money is lost. Domain spoofing of accountants around BAS and end of financial year is a recurring attack pattern in Australia. |
| ACTION | Configure SPF hard-fail, enable DKIM signing, publish DMARC. Begin DMARC at `p=none` for reporting, review reports for two weeks, then escalate to `p=quarantine` and `p=reject` . Enable external sender warning banners. |
| EFFORT | 3 to 4 hours configuration. 2 weeks DMARC monitoring before hardening. |

FINDING H5

## Two endpoints running unsupported Windows 10

HIGH

ENDPOINT SECURITY

| | |
|---|---|
| WHAT WE FOUND | Two devices still on Windows 10 22H2. Microsoft ended mainstream security updates for Windows 10 on 14 October 2025. Both devices are hardware-capable of Windows 11. |
| WHY IT MATTERS | Any vulnerability discovered in Windows 10 from October 2025 onwards is not being patched on these two devices. Over time they become the weakest link on the network. Insurers and external auditors increasingly check OS support status. |
| ACTION | In-place upgrade both devices to Windows 11 24H2. Back up each before the upgrade. Schedule outside working hours. |
| EFFORT | 1 to 2 hours per device, after hours. No user data loss expected. |

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 are enrolled in Microsoft Intune or any other device management platform. No way to enforce policies centrally, push patches, require encryption, or remote-wipe a lost or stolen laptop. |
| WHY IT MATTERS | A lost laptop today means the finder has full local admin access to client files. Without central management, most recommendations in this report require going device by device, which does not scale and does not stay enforced over time. |
| ACTION | Enrol all 15 devices in Intune. Baseline policy: BitLocker required, screen lock after 10 minutes, Defender for Business enabled, remote wipe capable. Intune is included with Microsoft 365 Business Premium. |
| EFFORT | Initial setup 4 to 6 hours. 15 minutes per device enrolment. Ongoing enforcement automatic. |

FINDING M2

## 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 a licence upgrade to Business Premium. |
| WHY IT MATTERS | Safe Links rewrites URLs in email 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 pretending to be from the principal. All three are the first line of defence for a firm targeted by business email compromise. |
| 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. |

06 · MEDIUM FINDINGS (CONTINUED)

# Governance and Microsoft 365 backup.

FINDING M3

## No written IT policies (0 of 4)

MEDIUM

GOVERNANCE

| | |
|---|---|
| WHAT WE FOUND | No written backup and recovery policy. No acceptable use policy. No password and access control policy. No documented staff onboarding / offboarding procedure. IT practices exist informally. |
| WHY IT MATTERS | APES 325 (Tax Practitioners Board) requires risk management and documented controls for registered tax agents. Cyber insurers increasingly ask for evidence of written policies alongside technical controls. Without documented policies, new staff have no standard to follow and there is no evidence of due diligence if an incident occurs. |
| ACTION | Draft four short policies (one to two pages each): backup and recovery, acceptable use, password and access, onboarding / offboarding. Review annually. |
| EFFORT | 4 to 6 hours using standard SMB templates. |

FINDING M4

## No separate Microsoft 365 backup

MEDIUM

BACKUP & RECOVERY

| | |
|---|---|
| WHAT WE FOUND | The practice 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. |
| WHY IT MATTERS | Microsoft's shared responsibility model makes the customer (not Microsoft) responsible for long-term data retention and recovery from accidental or malicious deletion. Recovery becomes impossible outside native retention windows. ATO record-keeping obligations extend to 5 or 7 years depending on the record type. |
| ACTION | Add a Microsoft 365 backup (e.g. Dropsuite, Keepit, Barracuda Cloud-to-Cloud Backup) with 7-year retention minimum. Addressed as part of the C1 backup rebuild. |
| EFFORT | Included in C1. |

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. Staff do not have a clear reporting channel for suspicious email. |
| WHY IT MATTERS | The majority of incidents start with a staff member clicking a link or opening an attachment. Technical controls reduce exposure; trained staff close the gap. |
| ACTION | Roll out a short quarterly awareness programme (10 minute video each quarter) and run two phishing simulations per year. Add a "Report phishing" button in Outlook. |
| EFFORT | Setup 2 to 3 hours. Approx 1 hour per quarter per staff member. |

FINDING L2

## Shared mailbox passwords stored in spreadsheet

LOW
IDENTITY & ACCESS

| | |
|---|---|
| WHAT WE FOUND | Three shared mailboxes (reception, accounts, smsf) configured as licensed user accounts with passwords shared via a spreadsheet on the NAS. MFA is not possible in this configuration. |
| WHY IT MATTERS | Shared passwords rotate slowly, travel via email when new staff join, and survive in old document copies. A compromise gives undetected access to mailboxes that handle invoice replies and BAS correspondence. |
| ACTION | Convert the three accounts to proper Microsoft 365 shared mailboxes (no licence, no password). Delegate access. Retire the shared spreadsheet; move residual passwords into a team password manager (e.g. 1Password Teams, Keeper Business). |
| EFFORT | 2 to 3 hours. |

FINDING L3

## Inconsistent device build; no standard operating environment

LOW
ENDPOINT SECURITY

| | |
|---|---|
| WHAT WE FOUND | Each device has been configured individually over time. No standard baseline. Different versions of browsers, PDF readers, helper apps across the fleet. Some devices carry leftover software from previous staff. |
| WHY IT MATTERS | Inconsistent builds make patching and troubleshooting slower; old software left on devices is a common compromise route. A standard build lets a new laptop be set up in an hour, not half a day. |
| ACTION | Once Intune is in place (M1), define a Harbourline Advisory standard operating environment: approved apps, baseline settings, patching schedule. Apply to all devices over 30 days. |
| EFFORT | Bundled into the Intune rollout. |

08 · ESSENTIAL EIGHT ALIGNMENT

# How the practice 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. Harbourline Advisory currently meets zero of eight controls at Level 1 (four are partially implemented).

| CONTROL | STATUS | NOTES |
|---|---|---|
| **Multi-factor authentication** | PARTIAL | Enabled for 11 of 15 accounts. Four missing. Not enforced by Conditional Access. Addressed by C2. |
| **Regular backups** | PARTIAL | Backup exists but is not immutable, not offsite, not tested, and excludes Microsoft 365 data. Addressed by C1 and M4. |
| **Patch operating systems** | PARTIAL | Updates happen ad-hoc when Windows prompts. Two devices still on unsupported Windows 10. Addressed by H5 and M1. |
| **Patch applications** | PARTIAL | Core apps (Office, browsers) mostly current. No central patching of helper apps (PDF readers, Zoom, Adobe). Addressed by M1. |
| **Restrict administrative privileges** | NOT IMPLEMENTED | All staff are local admins. Three Global Admins in Microsoft 365. Addressed by C2 and H2. |
| **Application control** | NOT IMPLEMENTED | No restrictions on software installation. Addressed by Intune rollout (M1) and H2. |
| **Configure Microsoft Office macros** | NOT IMPLEMENTED | Default macro settings. Internet-originated macros are not blocked. Addressed by Intune rollout (M1). |
| **User application hardening** | NOT IMPLEMENTED | Flash, Java, ads, and auto-run are not hardened. Legacy browser settings in place. Addressed by Intune rollout (M1). |

### Essential Eight Level 1: 0 of 8 fully met, 4 partially met.

Implementing the findings in this report moves the practice from 0 to 6 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.

Essential Eight alignment is not a legal requirement for private-sector SMBs, but it is increasingly cited in cyber insurance underwriting questionnaires and in the APES 325 risk management standard for registered tax agents. Meeting Level 1 on all eight controls materially reduces exposure to the most common attack patterns affecting Australian businesses.

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: identity before endpoints, endpoints before policies, foundations before fine-tuning.

## PHASE 1 · BY 22 APRIL Stop the bleeding (14 days)

Close the two critical gaps. Remove the paths an attacker or an accidental click can take tomorrow.

| | | | |
|---|---|---|---|
| 1 | C1 | Deploy immutable, offsite, tested backup (Synology + Microsoft 365) | 8 to 12 hours |
| 2 | C2 | Enforce MFA; break-glass admin; remove Global Admin from daily account; block legacy auth | 4 to 6 hours |

## PHASE 2 · BY 8 MAY Close the front doors (30 days)

The visible security layer: managed endpoint security, email authentication, business-grade firewall, modern operating systems.

| | | | |
|---|---|---|---|
| 3 | H1 | Deploy Defender for Business (licence upgrade to Business Premium) | 6 to 8 hours |
| 4 | H2 | Remove local admin rights; standard user model | Deferred into Intune (M1) |
| 5 | H3 | Replace router with managed business firewall; segment network; DNS filtering | 4 to 6 hours + hardware |
| 6 | H4 | Configure SPF, DKIM, DMARC; external email tagging | 3 to 4 hours + monitoring |
| 7 | H5 | Upgrade two Windows 10 devices to Windows 11 | 1 to 2 hours per device |

## PHASE 3 · BY 7 JUNE Make it stick (60 days)

Controls that hold the previous fixes in place and formalise governance.

| | | | |
|---|---|---|---|
| 8 | M1 | Enrol all devices in Intune; apply baseline policy | Setup 4 to 6 hours; 15 min / device |
| 9 | M2 | Configure Defender for Office 365 (Safe Links, Safe Attachments, anti-phishing) | 3 to 4 hours (bundled) |
| 10 | M3 | Draft four written IT policies; principal sign-off | 4 to 6 hours |
| 11 | M4 | Microsoft 365 backup (addressed as part of C1) | Included in C1 |

## PHASE 4 · BY 7 JULY Refine and maintain (90 days)

Best-practice items and a running review cycle.

| | | | |
|---|---|---|---|
| 12 | L1 | Roll out security awareness training and phishing simulation | 2 to 3 hours setup |
| 13 | L2 | Convert shared mailboxes; deploy team password manager | 2 to 3 hours |
| 14 | L3 | Define and apply standard operating environment via Intune | Bundled into M1 |

10 · WHAT HAPPENS NEXT

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

Harbourline Advisory 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 practice 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 practice to our managed service. Fixes get implemented, then we stay to keep them working: patching, monitoring, backup verification, security, and support. Based on the findings, the fit for a 15-person practice 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 two critical and five high findings, a cyber insurance policy with technical conditions, and line-of-business applications (Xero, MYOB AE, CAS360, FYI) that need active support. Business tier includes everything needed to execute this report and hold it in place over time: managed EDR, Intune, Microsoft 365 hardening, monthly security review, unlimited support.

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 practice. If Assured is the right fit, CIO Tech will produce a fixed-price proposal tailored to Harbourline Advisory, covering the findings in this report and ongoing managed IT from month one.

Book the walk-through | ciotech.com.au



**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-2026-0041.