

Executive Brief — Microsoft 365 Security & Compliance Assessment

Sample Client (Regulated Multi-State Retail Group) · 3 September 2026 · Sample deliverable — identifiers redacted

IT Partner LLC completed a read-only security and compliance assessment of the Sample Client (Regulated Multi-State Retail Group) Microsoft 365 environment on 2 September 2026, with a verification pass on 3 September 2026. This note summarises what we found, what it means for the business, and what we recommend. The full report, findings tracker and presentation are attached.

In one sentence: Microsoft's built-in defaults have been adopted well, but almost nothing beyond them has been configured — detection is on, prevention and data governance are largely absent. Secure Score is 52.7% (Device 45%), Compliance Manager is 60%, and we raised 32 findings: 8 Critical, 13 High, 8 Medium, 3 Low. Twelve controls are working well and are credited in the report.

52.7% Secure Score	32 Findings	8 / 13 Critical / High	174 Can't do MFA	34 / 35 Domains w/o DKIM	0 Holds in open cases
------------------------------	-----------------------	----------------------------------	----------------------------	------------------------------------	---------------------------------

Five things that matter most

1	A Global Administrator account is flagged at risk right now Microsoft's risk engine has flagged one of the three Global Administrator accounts and 15 other users as at risk, and nobody has acted on it. Separately, the modern MFA policy has every strong method switched off (only email codes are enabled) and a Microsoft-driven migration is in progress that would leave the whole organisation without working MFA if it completed today. 174 users (24%) cannot perform MFA at all.
2	Every brand domain can be impersonated Email from 34 of 35 domains cannot be cryptographically verified (DKIM has never been turned on) and 21 domains have no DMARC policy at all — including the corporate domain and every state dispensary domain. Customers, patients, banks, regulators and outside counsel cannot tell genuine mail from forged mail. Impersonation attempts targeting a named executive were already observed in the week before the assessment.
3	Live legal matters with no preservation Three eDiscovery cases are open — one appears to involve litigation — yet not one mailbox in the tenant is under a hold, and there is no retention policy, data classification or custom data-loss-prevention rule anywhere. Preservation currently depends on people not deleting things.
4	Data can leave without anyone making a mistake Every external-sharing setting is at its most permissive and they compound: the default share link is anonymous, editable and never expires; anyone can invite anyone as a guest (143 guests exist, 112 never or no longer active); Teams is open to every domain on the internet; unmanaged devices have full access; sessions never time out.
5	Endpoints are running on defaults and drifting Only 21 devices are managed against 622 mailboxes. On those, there is no attack-surface-reduction, antivirus, disk-encryption or firewall policy; every user is a local administrator with unmanaged local-admin passwords; and 17 protections that were once on have silently regressed. Defender would see a ransomware intrusion — very little is configured to stop one.

What is working

Credit where due: the Standard email protection preset is on for everyone, MFA and legacy-authentication policies are tenant-wide, administrator MFA is complete, every device that is managed is fully onboarded to Defender, mailbox auditing is on everywhere, SPF is published on 33 of 35 domains and no external mail forwarding is occurring.

The structural constraint

One constraint shapes the plan. We verified that 365 of roughly 560 licensed users hold Business Basic or Business Standard, which include no Conditional Access, device management or advanced email protection entitlement. Only 195 users (Business Premium and E5) can be fully protected. Several fixes cannot be applied to everyone until this is decided; we recommend uplifting those users to Business Premium (or, at minimum, adding Entra ID P1), funded in part by reclaiming the ~190 licences currently assigned to accounts that have not signed in for 90 days or more.

Recommended plan

Phase 0 — Stabilise (weeks 1–2, configuration only, no licence cost)	Investigate and secure the at-risk administrator; enable Authenticator and passkeys before the MFA migration completes; place holds on the mailboxes in the open legal matters (with counsel); enable DKIM and publish DMARC on the domains in use; change the default share link to "specific people, view, expiring"; block external auto-forwarding; remove a mail rule that lets forged "box.com" mail bypass filtering; add executives and all 35 domains to impersonation protection; deploy attack-surface-reduction rules.
Phase 1 — Harden (to day 60)	Take the licensing decision; create break-glass accounts and move admin roles to just-in-time (PIM); enforce phishing-resistant MFA for admins; require healthy devices for access; deploy antivirus, BitLocker, firewall and local-admin-password policies; restrict guest invitations and Teams federation; clean up 190 dormant and 112 inactive guest accounts; replace two unsupported Windows 10 devices.
Phase 2 — Govern (to day 120)	Sensitivity labels, data-loss-prevention for card, patient and financial data, retention policies aligned with state record-keeping rules, mailbox archiving, Customer Lockbox, and an on-premises Active Directory assessment.
Phase 3 — Sustain (ongoing)	A monthly operating rhythm (Secure Score triage, alert review, inactive-account report) and a day-one security baseline for every acquired business, so future tenant-to-tenant migrations land securely instead of adding to the backlog.

What we need from you

1. Approve Phase 0 to start immediately — it is configuration only and needs a few hours of change windows over two weeks.
2. Nominate a legal contact so holds can be placed in the open matters this week.
3. Take the licensing decision (Business Premium uplift or Entra ID P1 add-on) within 30 days.
4. Agree a 30-minute readout with leadership and IT to walk through the findings presentation.

Prepared by Mike Mackey, Microsoft 365 Security Practice, IT Partner LLC. Full detail, evidence and verification status for every finding are in the accompanying report.