AI Solutions, Inc.

LEGAL & BUSINESS TECHNOLOGY

MICROSOFT 365 ENVIRONMENT ASSESSMENT

Executive Summary

Overall posture, top risks, AI readiness, and recommended next steps

PREPARED FOR	PREPARED BY	DATE	DOCUMENT
Meridian Title & Escrow, LLC	AI Solutions, Inc.	March 14, 2026	EXEC v1.0

42	38%	5	40–50
USERS ASSESSED	SECURE SCORE	TOP RISKS	EST. HOURS

IN THIS DOCUMENT

SAMPLE · FICTIONAL DATA. This document accompanies the sample Executive Summary for a fictional client. Findings, hours, rates, and figures are illustrative and are not a quotation for any actual engagement.

1 · Overall Posture

Meridian Title & Escrow operates a Microsoft 365 Business Premium environment supporting 42 staff across two offices. The assessment found a functional but under-hardened tenant: the fundamentals of email and file collaboration are in place, yet several controls that protect client funds, closing documents, and personally identifiable information are either disabled or only partially deployed. The most urgent gaps concern multi-factor authentication coverage and external file sharing, both of which are directly exploitable today.

OVERALL RISK RATING	TENANT	SECURE SCORE	COPILOT READINESS
NEEDS ATTENTION	Business Premium · 42 seats	38% (peer median 52%)	Not ready — blocked by oversharing and absent labels

2 · Microsoft Secure Score Headline

Meridian currently sits at a Secure Score of **38%**, below the **52%** median for comparable professional-services tenants of this size. The score is dragged down primarily by incomplete identity protection and an absence of data-loss-prevention policies. A focused remediation effort can realistically lift this above **70%** within the first engagement phase. Secure Score is a useful trend line rather than a verdict — the underlying findings, not the number, are what carry the risk.

3 · Top Risks

#	RISK	WHAT IT MEANS FOR MERIDIAN
1	**Wire-fraud exposure** CRITICAL	11 of 42 accounts — including two with finance authority — have no multi-factor authentication, leaving the door open to the email-account takeover that drives real-estate wire fraud.
2	**Closing documents shared with the public internet** CRITICAL	67 files in SharePoint and OneDrive are reachable by anyone-with-the-link, several containing buyer financial data.
3	**No safety net for sensitive data** CRITICAL	With no Data Loss Prevention policies active, SSNs and bank details can leave the organization by email unmonitored.
4	**Legacy sign-in methods still permitted** HIGH	Older authentication protocols that bypass modern protections remain enabled tenant-wide.
5	**Limited visibility** HIGH	Unified audit logging gaps mean a security incident could not be fully reconstructed after the fact.

4 · AI Readiness Verdict

Meridian is **not yet ready** to deploy Microsoft 365 Copilot safely.

Because Copilot surfaces whatever a user already has access to, the current oversharing of closing files and the absence of sensitivity labels would let the tool expose confidential client information across the firm. Once external sharing is reined in, sensitivity labels are applied to closing and escrow records, and Secure Score clears roughly 65%, Meridian will be well positioned to adopt Copilot with confidence.

READINESS GATE	STATUS TODAY	CLEARED BY
External sharing controlled; anonymous links remediated	NOT MET	Sharing lockdown and link remediation.
Sensitivity labels applied to closing and escrow records	NOT MET	Publishing a label taxonomy and defaulting closing libraries.
Secure Score at or above roughly 65%	38%	Identity, sharing, and data-protection remediation combined.
Copilot licensing in place	NOT PURCHASED	Deliberately deferred until the gates above are met.

5 · Recommended Next Steps & Estimated Effort

STEP	ACTION	ESTIMATED EFFORT
1	**Enforce multi-factor authentication for all staff and block legacy authentication.** Closes the single most exploitable pathway in the tenant.	6–8 hours
2	**Lock down external sharing and remediate existing anonymous links.** Includes triage of all 67 links, prioritizing those containing buyer financial data.	10–14 hours
3	**Stand up baseline Data Loss Prevention and sensitivity labeling for client data.** Deployed in test mode first, then enforced.	16–20 hours
4	**Establish audit logging, alerting, and a Secure Score monitoring cadence.** Restores the visibility needed to reconstruct an incident.	6–9 hours
Indicative total for the initial hardening engagement		**40–50 hours**

IF NOTHING ELSE IS DONE THIS QUARTER

Steps 1 and 2 — roughly 16–22 hours — close the two exposures an attacker could use today. Everything else here can be scheduled; those two should not be.

6 · Next Steps

Ready to move forward?

Contact AI Solutions, Inc. to schedule your remediation engagement. A phased Plan of Action & Budget resolving these four steps into scheduled tasks, dates, and costs accompanies this summary, and we are happy to walk through any finding or estimate in it before you commit to anything.

Email: jeff@aisolutions.legal · **Web:** https://aisolutions.legal

This Executive Summary accompanies the Detailed Technical Analysis and the Plan of Action & Budget dated March 14, 2026. Sample document — Meridian Title & Escrow, LLC is fictional and all data is illustrative.