AI Solutions, Inc.

LEGAL & BUSINESS TECHNOLOGY

MICROSOFT 365 ENVIRONMENT ASSESSMENT

Detailed Technical Analysis

Findings by domain, evidence references, and recommended remediation

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

19	3	6	40.0
FINDINGS	CRITICAL	DOMAINS ASSESSED	CONFIG HOURS

IN THIS DOCUMENT

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

Priority Legend

PRIORITY	DEFINITION
CRITICAL	Active or imminent risk of breach, data loss, or compliance failure. Address immediately.
HIGH	Significant exposure that should be remediated within the current engagement.
MEDIUM	Meaningful gap to schedule into the remediation roadmap.
LOW	Minor hardening opportunity; address as capacity allows.
INFORMATIONAL	No action required; noted for awareness or as a positive control already in place.

1 · Identity & Access

Identity is the weakest area of the tenant and the source of the most urgent findings.

FINDING	PRIORITY	OBSERVATION	EFFORT
Incomplete MFA coverage	CRITICAL	11 of 42 users have no MFA method registered. Two are in the closing/finance group. *Evidence: 01-Identity-Access/mfa-status.csv*	3h
Legacy authentication enabled	HIGH	Basic auth protocols remain enabled tenant-wide, bypassing Conditional Access. *Evidence: 01-Identity-Access/authpolicies.json*	1.5h
No Conditional Access baseline	HIGH	No CA policies enforce MFA, device, or location controls. *Evidence: 01-Identity-Access/ca-policies.json — empty set*	2.5h
Excess Global Administrators	MEDIUM	4 Global Admins for a 42-seat tenant; no PIM or just-in-time elevation. *Evidence: 01-Identity-Access/admin-roles.csv*	2h

> **OBSERVATION**
>
> The combination of missing MFA, enabled legacy auth, and no Conditional Access means a single phished password grants an attacker full mailbox access — the exact pathway used in real-estate wire-fraud schemes.

RECOMMENDED REMEDIATION

Deploy a Conditional Access policy requiring MFA for all users; enable the "Block legacy authentication" policy; register all 42 users for the Microsoft Authenticator app; reduce Global Admins to two and enable Privileged Identity Management for just-in-time elevation.

2 · Device & Endpoint Compliance

FINDING	PRIORITY	OBSERVATION	EFFORT
No Intune compliance policies	HIGH	Devices enroll but no compliance policy evaluates encryption, OS version, or password posture. *Evidence: 02-Device-Compliance/intune-policies.json*	3h
BitLocker not enforced	MEDIUM	Disk encryption is left to user discretion on 19 managed laptops. *Evidence: 02-Device-Compliance/device-inventory.csv*	2h
No app protection policies	MEDIUM	Company data on personal mobile devices is unmanaged. *Evidence: 02-Device-Compliance/app-protection.json — none configured*	2.5h

RECOMMENDED REMEDIATION

Create an Intune compliance policy requiring BitLocker, a current OS build, and a device PIN; deploy an App Protection Policy to contain Outlook and Teams data on unmanaged mobile devices; mark non-compliant devices for Conditional Access blocking.

3 · Data Security & DLP

FINDING	PRIORITY	OBSERVATION	EFFORT
No DLP policies	CRITICAL	No Data Loss Prevention policy exists; SSNs and bank details can be emailed externally without detection. *Evidence: 03-Data-Security-DLP/dlp-policies.json — empty*	4h
No sensitivity labels	HIGH	No label taxonomy is published; closing documents are unclassified. *Evidence: 03-Data-Security-DLP/labels.json*	3.5h
Retention not configured	MEDIUM	No retention policy for transaction records against the firm's stated 7-year requirement. *Evidence: 03-Data-Security-DLP/retention.json*	2h

RECOMMENDED REMEDIATION

Publish a DLP policy targeting U.S. financial identifiers (SSN, bank account, routing numbers) across Exchange, SharePoint, and OneDrive, in test mode first; create a three-tier sensitivity label set (Public / Internal / Client-Confidential) and auto-apply Client-Confidential to closing folders; configure a 7-year retention policy for transaction libraries.

4 · Compliance Posture

FINDING	PRIORITY	OBSERVATION	EFFORT
Unified audit log gaps	HIGH	Mailbox auditing is on, but unified audit search shows inconsistent coverage; some service plans never enabled. *Evidence: 04-Compliance-Purview/audit-config.json*	1.5h
No eDiscovery / legal hold readiness	MEDIUM	No hold policies; relevant for a firm handling escrow disputes. *Evidence: 04-Compliance-Purview/holds.json — none*	2h

FINDING	PRIORITY	OBSERVATION	EFFORT
Compliance Manager unreviewed	LOW	Default assessment present but never actioned; score 41%. *Evidence: 04-Compliance-Purview/compliance-manager.csv*	1h

RECOMMENDED REMEDIATION

Enable unified audit logging across all workloads; create a baseline legal-hold capability; assign an owner to the Compliance Manager improvement actions aligned to the firm's stated obligations.

5 · Collaboration & External Sharing

FINDING	PRIORITY	OBSERVATION	EFFORT
Anonymous "anyone" links active	CRITICAL	67 files shared via anonymous links; sampling found 9 containing buyer financial data. *Evidence: 05-Collaboration-Sharing/sharing-report.csv*	4h
Tenant default sharing too permissive	HIGH	Default SharePoint and OneDrive setting is "Anyone with the link". *Evidence: 05-Collaboration-Sharing/sharing-settings.json*	1h
Mailbox auto-forwarding to external	HIGH	3 mailboxes auto-forward externally — a classic exfiltration and BEC indicator. *Evidence: 05-Collaboration-Sharing/forwarding-rules.csv*	1.5h

RECOMMENDED REMEDIATION

Change the tenant default to "Specific people"; expire and re-scope existing anonymous links; disable external auto-forwarding via a transport rule and investigate the three flagged mailboxes immediately.

6 · Licensing & AI Readiness

FINDING	PRIORITY	OBSERVATION	EFFORT
Copilot prerequisites unmet	HIGH	Oversharing and absent labels make Copilot deployment unsafe today. *Evidence: synthesis of sections 3 and 5*	1h
Underused licensing	LOW	7 Business Premium licenses assigned to disabled or never-signed-in accounts. *Evidence: 06-Licensing-AI-Readiness/license-usage.csv*	1.5h
Secure Score baseline low	MEDIUM	Current Secure Score 38% vs. 52% peer median. *Evidence: 07-Secure-Score/secure-score.json*	0.5h

RECOMMENDED REMEDIATION

Defer Copilot until external sharing is controlled and Client-Confidential labeling is live; reclaim the 7 unused licenses; treat a Secure Score of 65% as the readiness gate for Copilot.

7 · Microsoft Secure Score Analysis

Meridian's current Secure Score is **38%** (evidence: 07-Secure-Score/secure-score.json). The highest-value improvement actions, in order of impact-to-effort:

IMPROVEMENT ACTION	POINTS	PRIORITY	EFFORT
Require MFA for all users	+9.1%	CRITICAL	3h
Block legacy authentication	+4.8%	HIGH	1.5h
Enable DLP for financial data	+4.2%	CRITICAL	4h
Restrict anonymous sharing	+3.9%	CRITICAL	2h
Enforce device compliance	+3.3%	HIGH	3h

QUICK WINS — UNDER 2 HOURS EACH

Block legacy authentication, restrict the tenant default sharing setting, and disable external auto-forwarding. Together these raise the score by roughly 9 points for under 4 hours of combined effort.

TOTAL ASSESSED REMEDIATION EFFORT

DOMAIN	FINDINGS	EFFORT
1 · Identity & Access	4	9.0h
2 · Device & Endpoint Compliance	3	7.5h
3 · Data Security & DLP	3	9.5h
4 · Compliance Posture	3	4.5h
5 · Collaboration & External Sharing	3	6.5h
6 · Licensing & AI Readiness	3	3.0h
Configuration effort across all findings	**19**	**40.0h**

Figures above are configuration effort only. The accompanying Plan of Action & Budget adds validation, pilot, communication, and documentation time and schedules the work into phases.

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