AI Solutions, Inc.

LEGAL & BUSINESS TECHNOLOGY

MICROSOFT 365 ENVIRONMENT ASSESSMENT

Plan of Action & Budget

Remediation roadmap, phased effort estimate, and investment summary

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

48.5	4	8	$9,215
CONSULTING HOURS	REMEDIATION PHASES	WEEKS ELAPSED	EST. INVESTMENT

IN THIS DOCUMENT

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

1 · Purpose & How to Use This Plan

The Executive Summary described *what* is wrong and the Detailed Technical Analysis described *why* it matters. This Plan of Action & Budget answers the remaining three questions: in what order the work is done, how long each item takes, and what it costs.

Every task below traces to a numbered finding in the Detailed Technical Analysis and carries the same priority rating. Nothing new has been introduced; the 40–50 hour indicative range published in the Executive Summary is resolved here into **48.5 hours across 4 phases**, scheduled over **8 calendar weeks**.

Sequencing is driven by exploitability rather than by severity alone. Phase 1 and Phase 2 close the two pathways that are directly exploitable today — password-only sign-in and publicly reachable closing documents — before any effort is spent on classification, labeling, or compliance tooling. That order also front-loads the Secure Score gain, so the measurable improvement lands in the first three weeks.

Priority legend

PRIORITY	MEANING IN THIS PLAN
CRITICAL	Active or imminent risk of breach, data loss, or compliance failure. Scheduled in Phase 1 or 2; not deferrable.
HIGH	Significant exposure remediated within this engagement.
MEDIUM	Meaningful gap scheduled into the roadmap, typically Phase 3 or 4.
LOW	Minor hardening or hygiene item; grouped with related work to avoid separate mobilization.

2 · Remediation Strategy at a Glance

1 WEEKS 1–2

Identity Hardening

Close the wire-fraud pathway: MFA coverage, Conditional Access baseline, legacy authentication block. 8.0 h · $1,520

2 WEEKS 2–3

Sharing & Exfiltration Containment

Retire 67 anonymous links, reset tenant sharing defaults, stop external auto-forwarding. 11.5 h · $2,185

3 WEEKS 3–6

Data Protection & Endpoint Compliance

DLP for financial identifiers, sensitivity labels, retention, Intune compliance and app protection. 19.5 h · $3,705

4 WEEKS 6–8

Governance, Visibility & AI Readiness

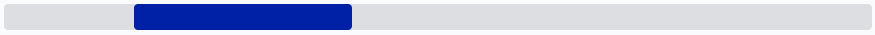
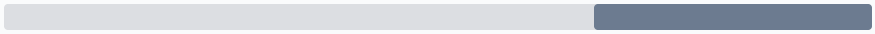
Audit logging, legal hold, admin-role reduction, license reclamation, Copilot readiness gate. 9.5 h · $1,805

DESIGN PRINCIPLE

Controls are deployed in report-only or test mode first wherever the platform supports it — Conditional Access, DLP, and Intune compliance all ship with an evaluation mode. Meridian sees the impact on real traffic before enforcement, which is what keeps a 42-seat firm working while the tenant is hardened.

3 · Schedule & Sequencing

Eight elapsed weeks assumes remote delivery, one change window per week, and client decisions returned within two business days. Effort is not evenly distributed: Phase 3 is the longest in calendar time because DLP and labeling require a monitoring period between pilot and enforcement, not because it consumes proportionally more hours.

PHASE	HOURS	WEEK 1 2 3 4 5 6 7 8
1 · Identity Hardening	8.0	
2 · Sharing & Exfiltration	11.5	
3 · Data & Endpoint Protection	19.5	
4 · Governance & AI Readiness	9.5	
Total programme	**48.5**	**8 weeks from kickoff to closeout report**

Milestones and decision points

WEEK	MILESTONE	DECISION REQUIRED FROM MERIDIAN
Week 0	Kickoff & access	Global Administrator access granted; break-glass account agreed; staff change-notice approved.
Week 1	Conditional Access in report-only	Confirm the exclusion list (service accounts, break-glass) before enforcement.
Week 2	MFA enforced tenant-wide	Sign-off that all 42 users are registered; approve enforcement date.
Week 3	Anonymous links retired	Approve the exception list for links that must remain active for active closings.
Week 4	DLP in test mode	Confirm which financial identifiers are in scope and who receives policy-match alerts.
Week 5	Label taxonomy published	Approve the three-tier label names and the closing/escrow libraries to be defaulted.
Week 6	DLP enforced; Intune compliance live	Approve blocking of non-compliant devices via Conditional Access.
Week 8	Closeout & Secure Score review	Decide on ongoing monitoring cadence and whether to open the Copilot readiness workstream.

SEQUENCING CONSTRAINT

Device-compliance blocking (Phase 3) depends on the Conditional Access framework built in Phase 1, and safe Copilot evaluation (Phase 4) depends on both sharing remediation and labeling being complete. Phases can be descoped from the end of the plan, but not reordered.

4 · Phase 1 — Identity Hardening

1
WEEKS 1-2

Identity & Access

Addresses findings: Incomplete MFA coverage (Critical) · Legacy authentication enabled (High) · No Conditional Access baseline (High)

ID	TASK	PRIORITY	HRS	COST
P1-01	**Register all 42 users for Microsoft Authenticator.** Prioritize the 11 accounts with no registered method, starting with the two in the closing/finance group. Includes assisted enrollment sessions and a fallback method for shared/reception accounts.	CRITICAL	3.0	$570
P1-02	**Deploy Conditional Access MFA baseline.** Build the policy set in report-only, review sign-in impact for five business days, then enforce. Includes a documented break-glass exclusion and a legacy-service-account inventory.	HIGH	2.5	$475
P1-03	**Block legacy authentication tenant-wide.** Identify any remaining basic-auth clients from sign-in logs, remediate or exempt them, then apply the block policy.	HIGH	1.5	$285
P1-04	**Validation, staff communication and runbook.** Post-enforcement sign-in verification, a one-page user guide, and the identity section of the handover runbook.	MEDIUM	1.0	$190
Phase 1 subtotal			**8.0**	**$1,520**

Outcome. A phished password alone no longer grants mailbox access. This single phase removes the pathway used in real-estate wire-fraud schemes and delivers the largest Secure Score movement in the plan (approximately +14 points).

Risk of deferral. Highest in the plan. Every day this remains open, 11 accounts — two with finance authority — are protected by a password alone.

5 · Phase 2 — Sharing & Exfiltration Containment

2
WEEKS 2-3

Collaboration & External Sharing

Addresses findings: Anonymous "anyone" links active (Critical) · Tenant default sharing too permissive (High) · Mailbox auto-forwarding to external (High)

ID	TASK	PRIORITY	HRS	COST
P2-01	**Reset tenant sharing default to "Specific people."** Applied at tenant level with per-site review for the libraries that legitimately share externally.	HIGH	1.0	$190
P2-02	**Remediate 67 anonymous links.** Triage the full set, expire or re-scope each one, and handle the 9 links containing buyer financial data first with same-day revocation and a record of exposure window.	CRITICAL	4.0	$760
P2-03	**Stop external auto-forwarding and investigate.** Transport rule blocking external forwarding, plus review of the three flagged mailboxes for rule origin, sign-in history, and indicators of compromise.	CRITICAL	1.5	$285

ID	TASK	PRIORITY	HRS	COST
P2-04	**Sharing governance controls.** Default link type and expiry, restrict "anyone" links to opt-in sites only, and stand up a monthly external-sharing report to the firm's designated owner.	MEDIUM	2.0	$380
P2-05	**Change communication and exception handling.** Notice to staff explaining the new sharing workflow, plus a defined path for closings that require external access.	MEDIUM	1.5	$285
P2-06	**Validation and documentation.** Re-run the sharing report to confirm zero unreviewed anonymous links; document exceptions and the remediation record.	MEDIUM	1.5	$285
Phase 2 subtotal			11.5	$2,185

POSSIBLE CHANGE ORDER

If the review in P2-03 finds evidence that any of the three forwarding rules was created by an attacker rather than a user, incident response is outside this plan. An indicative allowance of 8–12 hours would be raised as a separate change order and actioned immediately.

6 · Phase 3 — Data Protection & Endpoint Compliance

3
WEEKS 3-6

Data Security, DLP & Device Compliance

Addresses findings: No DLP policies (Critical) · No sensitivity labels (High) · No Intune compliance policies (High) · Retention not configured (Medium) · BitLocker not enforced (Medium) · No app protection policies (Medium)

ID	TASK	PRIORITY	HRS	COST
P3-01	**Data Loss Prevention for U.S. financial identifiers.** Policy covering SSN, bank account and routing numbers across Exchange, SharePoint, OneDrive and Teams. Deployed in test mode with policy tips, tuned against two weeks of real matches, then enforced.	CRITICAL	4.0	$760
P3-02	**Sensitivity label taxonomy.** Three-tier set (Public / Internal / Client-Confidential), published to all users, with Client-Confidential set as the default label on closing and escrow libraries and mandatory labeling enabled.	HIGH	3.5	$665
P3-03	**Seven-year retention policy.** Retention configured for transaction record libraries and the associated mailboxes, aligned to the firm's stated obligation.	MEDIUM	2.0	$380
P3-04	**Intune compliance policy.** Requires BitLocker, a current OS build, and a device PIN; non-compliant devices marked for Conditional Access blocking once the grace period expires.	HIGH	3.0	$570
P3-05	**BitLocker enforcement across 19 managed laptops.** Disk-encryption profile with key escrow to Entra ID, staged rollout, and exception handling for any device that fails silent encryption.	MEDIUM	2.0	$380
P3-06	**App Protection Policies for personal mobile devices.** Containment of Outlook and Teams data — PIN, copy/paste restriction, save-as block, selective wipe — without enrolling personal handsets.	MEDIUM	2.5	$475
P3-07	**Pilot, tuning, user guidance and documentation.** Pilot group management, false-positive tuning on DLP, labeling guidance for closing staff, and policy documentation.	MEDIUM	2.5	$475
Phase 3 subtotal			**19.5**	**$3,705**

Outcome. Client financial data can no longer leave the firm by email unnoticed, closing documents carry a classification that travels with the file, and firm data on laptops and personal phones is protected at rest. Completion of this phase clears the 65% Secure Score readiness gate for Copilot.

7 · Phase 4 — Governance, Visibility & AI Readiness

4
WEEKS 6-8

Compliance, Licensing & Copilot Readiness

Addresses findings: Unified audit log gaps (High) · Copilot prerequisites unmet (High) · Excess Global Administrators (Medium) · No eDiscovery/legal hold readiness (Medium) · Secure Score baseline low (Medium) · Compliance Manager unreviewed (Low) · Underused licensing (Low)

ID	TASK	PRIORITY	HRS	COST
P4-01	**Enable unified audit logging across all workloads.** Close the service-plan gaps identified in the audit configuration and verify searchability end to end.	HIGH	1.5	$285
P4-02	**Baseline legal-hold capability.** eDiscovery permissions, a documented hold procedure, and one tested hold — relevant to a firm handling escrow disputes.	MEDIUM	2.0	$380
P4-03	**Compliance Manager ownership.** Assign an internal owner, select the improvement actions aligned to the firm's obligations, and set a review cadence.	LOW	1.0	$190
P4-04	**Reduce Global Administrators from 4 to 2 and enable just-in-time elevation.** Right-size role assignments to least privilege; see the licensing note in section 9 regarding PIM.	MEDIUM	2.0	$380
P4-05	**Reclaim 7 unused Business Premium licenses.** Confirm the accounts are genuinely dormant, preserve mailbox data where required, then release the licenses.	LOW	1.5	$285
P4-06	**Secure Score monitoring cadence and Copilot readiness gate.** Scheduled review, alerting on score regression, and a documented 65% gate for Copilot adoption.	MEDIUM	0.5	$95
P4-07	**Closeout report and handover.** Before/after posture summary, evidence pack, runbook, and the recommended ongoing-support scope.	MEDIUM	1.0	$190
Phase 4 subtotal			**9.5**	**$1,805**

8 · Budget Summary & Commercial Options

PHASE	WINDOW	HOURS	RATE	COST
1 · Identity Hardening	Weeks 1–2	8.0	$190	$1,520
2 · Sharing & Exfiltration Containment	Weeks 2–3	11.5	$190	$2,185
3 · Data Protection & Endpoint Compliance	Weeks 3–6	19.5	$190	$3,705
4 · Governance, Visibility & AI Readiness	Weeks 6–8	9.5	$190	$1,805
Programme subtotal		**48.5**		**$9,215**
Contingency allowance (10%, drawn only against approved change)		4.85	$190	$922
Not-to-exceed ceiling		**53.35**		**$10,137**

Blended senior consulting rate of $190/hour, illustrative for this sample. Time is recorded in 0.25-hour increments. Remote delivery; no travel or expenses are included.

Commercial options

OPTION	STRUCTURE	INVESTMENT
A · Fixed fee, full programme Recommended	All four phases committed up front at a fixed price. Scope is the 24 tasks listed in sections 4–7; change orders handled per section 12. Billed 40% at kickoff, 30% at end of Phase 2, 30% at closeout.	**$8,900** saves $315
B · Phased, time and materials	Each phase authorized separately at the estimate above and invoiced monthly on actual hours. Maximum flexibility; no commitment beyond the current phase.	$9,215 estimated
C · Critical-only	Phases 1 and 2 only — the directly exploitable exposures. Leaves DLP, labeling, retention, device compliance, and audit gaps open; Copilot remains out of reach. Offered as a budget-constrained starting point, not as a recommendation.	$3,705

Ongoing support (optional, post-engagement)

Hardening decays without maintenance: new users are added, links get shared, policies drift. A monthly managed-posture retainer covering Secure Score review, sharing-report triage, DLP alert handling, device compliance monitoring, and quarterly reporting is available at **$725/month (4 hours)**. Quoted separately and not included in the totals above.

9 · Licensing Implications & Cost Offsets

Meridian's existing Microsoft 365 Business Premium licensing covers nearly all of this plan. Two items are exceptions and are called out so there are no surprises.

CAPABILITY REQUIRED BY THIS PLAN	COVERED BY BUSINESS PREMIUM	ACTION
MFA, Conditional Access, block legacy auth	Yes (Entra ID P1)	No additional cost.

CAPABILITY REQUIRED BY THIS PLAN	COVERED BY BUSINESS PREMIUM	ACTION
Intune compliance & app protection policies	Yes	No additional cost.
DLP across Exchange, SharePoint, OneDrive, Teams	Yes	No additional cost.
Sensitivity labels, default library label, mandatory labeling	Yes	No additional cost.
Retention policies; eDiscovery (Standard) and legal hold	Yes	No additional cost.
Service-side auto-labeling of files at rest	**No**	Requires a Purview add-on. This plan achieves the same practical result for closing and escrow content using default library labels plus mandatory labeling — revisit only if volume justifies it.
Privileged Identity Management (just-in-time admin)	**No**	Requires Entra ID P2 on the admin accounts only — approximately $18/month for two administrators. If declined, P4-04 still reduces Global Admins to two with dedicated, MFA-enforced admin accounts and a monitored break-glass account.
Microsoft 365 Copilot	**No**	Deliberately deferred until the readiness gate is met. Not budgeted here.

COST OFFSET

Reclaiming the 7 Business Premium licenses assigned to disabled or never-signed-in accounts (task P4-05) removes roughly **$154/month — about $1,848 per year** from Meridian's subscription. Over the first year that offsets approximately 20% of this programme's cost. Licensing figures are list prices in USD and should be confirmed against the firm's current agreement.

10 · Secure Score Trajectory

Meridian begins at 38%, against a 52% median for comparable professional-services tenants. The projection below is built from the point values published by Microsoft for each improvement action and shown cumulatively by phase.

STAGE	PROJECTED SCORE	GAIN	PRINCIPAL CONTRIBUTORS
Baseline (assessment date)	38%	—	Below the 52% peer median.
After Phase 1	~52%	+13.9	Require MFA for all users (+9.1), block legacy authentication (+4.8).
After Phase 2	~57%	+5.4	Restrict anonymous sharing (+3.9), sharing defaults and forwarding controls (+1.5).
After Phase 3	~66%	+9.0	DLP for financial data (+4.2), device compliance (+3.3), labeling and retention (+1.5).
After Phase 4	**~71%**	**+4.5**	**Audit logging, admin-role reduction, license hygiene.**

Scores are projections. Microsoft periodically revises point weightings and adds improvement actions, so the absolute figure at closeout may differ; the relative gain is the meaningful measure.

> **COPILOT READINESS GATE**
>
> The 65% gate is cleared at the end of Phase 3 — but the score is the proxy, not the requirement. The real prerequisites are that external oversharing is remediated (Phase 2) and that closing and escrow content carries a Client-Confidential label (Phase 3), because Copilot surfaces whatever a user can already reach. Deploying it before both are true would broadcast confidential client information across the firm.

11 · Client Responsibilities & Prerequisites

- **Named point of contact** with authority to approve change windows and policy exceptions, available for a weekly 30-minute checkpoint.
- **Global Administrator access** for the duration of the engagement, plus agreement on a break-glass account excluded from Conditional Access and monitored.
- **Staff communication** issued from firm leadership ahead of the MFA and sharing changes — adoption is materially smoother when the notice comes from Meridian rather than from us.
- **Decisions returned within two business days** at each milestone in section 3; the eight-week schedule assumes this.
- **Confirmation of the 7-year retention obligation** and identification of the record types it applies to.
- **Access to the closing/escrow team** for approximately two hours total, for labeling guidance and DLP false-positive review.
- **Device availability** — the 19 managed laptops must connect during the BitLocker rollout window.

12 · Assumptions, Exclusions & Change Control

ASSUMPTIONS

- Remote delivery during standard business hours, U.S. Central Time.
- The tenant remains on Business Premium with 42 seats; no migration, merger, or office move occurs mid-engagement.
- All 19 laptops are Intune-enrolled and healthy, as reported in the device inventory.

- Findings reflect the tenant as assessed on March 14, 2026; material configuration drift may alter effort.

EXCLUSIONS

- Incident response or forensic investigation, including any arising from task P2-03.
- Third-party application remediation, line-of-business software changes, and title-production system integration.
- Email or file migration, tenant-to-tenant work, and network or firewall changes.
- End-user training beyond the change communications and one-page guides listed in the task tables.
- Copilot licensing, deployment, or adoption work.
- Legal review of retention obligations — we implement the firm's stated requirement; we do not advise on it.

CHANGE CONTROL

Any work outside the 24 tasks in sections 4–7 is estimated in writing and requires written approval before it begins. The 10% contingency is drawn only against approved change, is reported monthly, and is refunded if unused under Option A. Hours are tracked in 0.25-hour increments and reported at each milestone.

13 · Deferred & Optional Work

Identified during the assessment but deliberately outside this plan — listed so that deferral is a recorded decision rather than an omission.

ITEM	EST. HRS	RATIONALE FOR DEFERRAL
Attack-simulation and phishing awareness programme	8–12	High value for a firm exposed to wire fraud, but only meaningful once MFA and Conditional Access are enforced. Recommended for the quarter following closeout.
Purview auto-labeling at rest	6–8	Requires additional licensing; default library labels achieve the practical result at 42 seats.
Insider risk and communication compliance policies	10–14	Requires E5-tier licensing. Revisit only if headcount or regulatory exposure grows.
Copilot pilot and adoption programme	12–16	Gated on Phase 3 completion and a 65% Secure Score. Scoped separately once the gate is cleared.
Backup and recovery review for Microsoft 365 data	4–6	Outside the assessment scope but a common gap at this size; flagged for a future conversation.

14 · Approval to Proceed

Selecting an option below authorizes AI Solutions, Inc. to begin the work described in this plan, subject to the assumptions, exclusions, and change-control terms in section 12.

SELECT	OPTION	INVESTMENT	SCOPE
☐	**A · Fixed fee, full programme**	$8,900	Phases 1–4, all 24 tasks, fixed price.
☐	**B · Phased, time and materials**	$9,215 est.	Phase-by-phase authorization at $190/hour.
☐	**C · Critical-only**	$3,705	Phases 1–2 only.
☐	**Add: managed posture retainer**	$725/month	Ongoing monitoring and maintenance, 4 hours monthly.

Authorized signature — Meridian Title & Escrow, LLC

Name and title

Date

Questions before you decide?

We are happy to walk through any task, estimate, or assumption in this plan line by line — including the trade-offs behind Option C — before anything is signed.

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

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