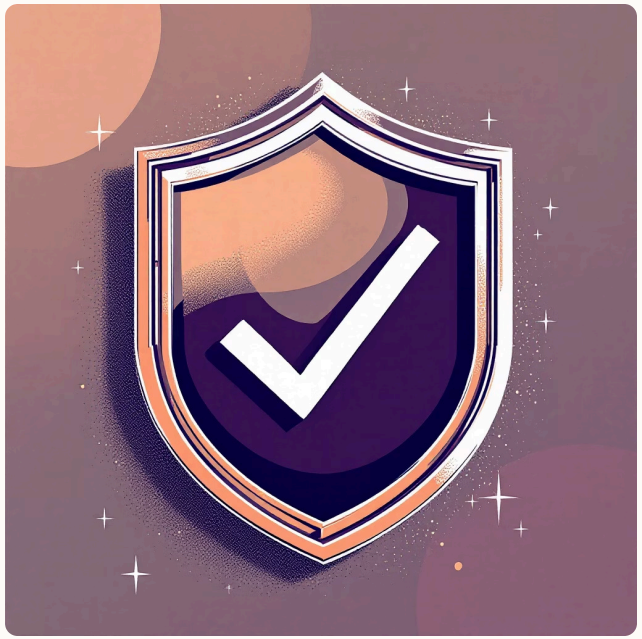
SECURITY AUDIT

M365 Permission Audit Checklist

Microsoft 365 Permissions Audit - Quick Reference Guide

A comprehensive guide to securing your Microsoft 365 environment before Copilot reveals what's been hidden in plain sight. This practical checklist helps IT administrators and security teams identify oversharing risks, lock down sensitive data, and establish ongoing governance - all within a manageable 1-2 weekend timeline.

Disclaimer



Important Legal Notice

This checklist is general guidance for a Microsoft 365 permissions audit and is not legal, compliance, or security advice. Every Microsoft 365 tenant is different. Use this as a starting point and validate all changes with your IT/security/compliance team or a qualified advisor.

Test changes in a safe environment before broad rollout. AdaptSphere NextGen AI assumes no responsibility for losses or impacts resulting from the use of this material.

Your organization's specific requirements, regulatory obligations, and risk tolerance should guide all implementation decisions. When in doubt, consult qualified professionals before making changes to production environments.

AdaptSphere is independent and not endorsed or affiliated with Microsoft Corporation.

Overview

This checklist helps you spot and fix the most common Microsoft 365 oversharing issues before Copilot surfaces something awkward—or expensive. The goal is simple: confirm that access is intentional, sensitive data is protected, and you can prove "who saw what" when questions come up.

Timeline

1-2 weekends for initial implementation

Skill Level

IT Administrator or Security Lead

Scope

Teams, Groups, SharePoint, OneDrive, Entra ID, Purview

This audit focuses on the highest-impact security wins with minimal disruption to daily operations. You'll establish baseline controls, remove obvious risks, and create a sustainable governance framework that scales with your organization.

What You'll Need

To run this checklist effectively, ensure you have the right access, stakeholders, and mindset before diving in. Success requires both technical permissions and organizational buy-in.

1

Admin Access

- Microsoft 365 Admin Center
- Teams Admin Center
- SharePoint Admin Center
- Microsoft Entra ID
- Microsoft Purview

2

Documentation

- List of top 10-20 Teams
- SharePoint site inventory
- Current sharing policies
- Organizational chart

3

Stakeholders

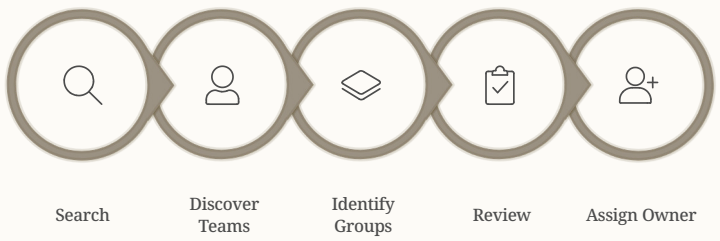
- IT Security Lead / Microsoft 365 Admin
- Business owners (HR, Finance, Operations)
- Department leads
- Executive sponsor

4

Mindset

Willingness to delete stale access - kindly, but firmly. This audit only works if you're prepared to make tough calls and communicate changes clearly.

Step 1: Hunt Down Public Teams & Ownerless Groups



What to Look For

- Teams set to "Public" that should be "Private"
- Teams with no active owner
- Inactive Teams that still allow joins
- Groups with 100+ members and unclear purpose

Action Items

01

Identify all public Teams – List teams, document business purpose

02

Identify ownerless Teams/Groups – Cross-reference with team registry

03

Convert public → private (if needed) – Notify members before change

04

Assign 2+ owners per team – Verify new owners accept responsibility

05

Archive inactive Teams – Confirm with content owner first

Owner: _____ **Target Date:** _____

Deliverable: List of public Teams (categorized as "keep public" or "convert to private") and all Teams with active owners assigned.

Step 2: Scrub Guest Access & External Sharing Rules

Inactive Guest Accounts

Last logged in more than 90 days ago—prime candidates for removal to reduce attack surface.

"Anyone" Sharing Links

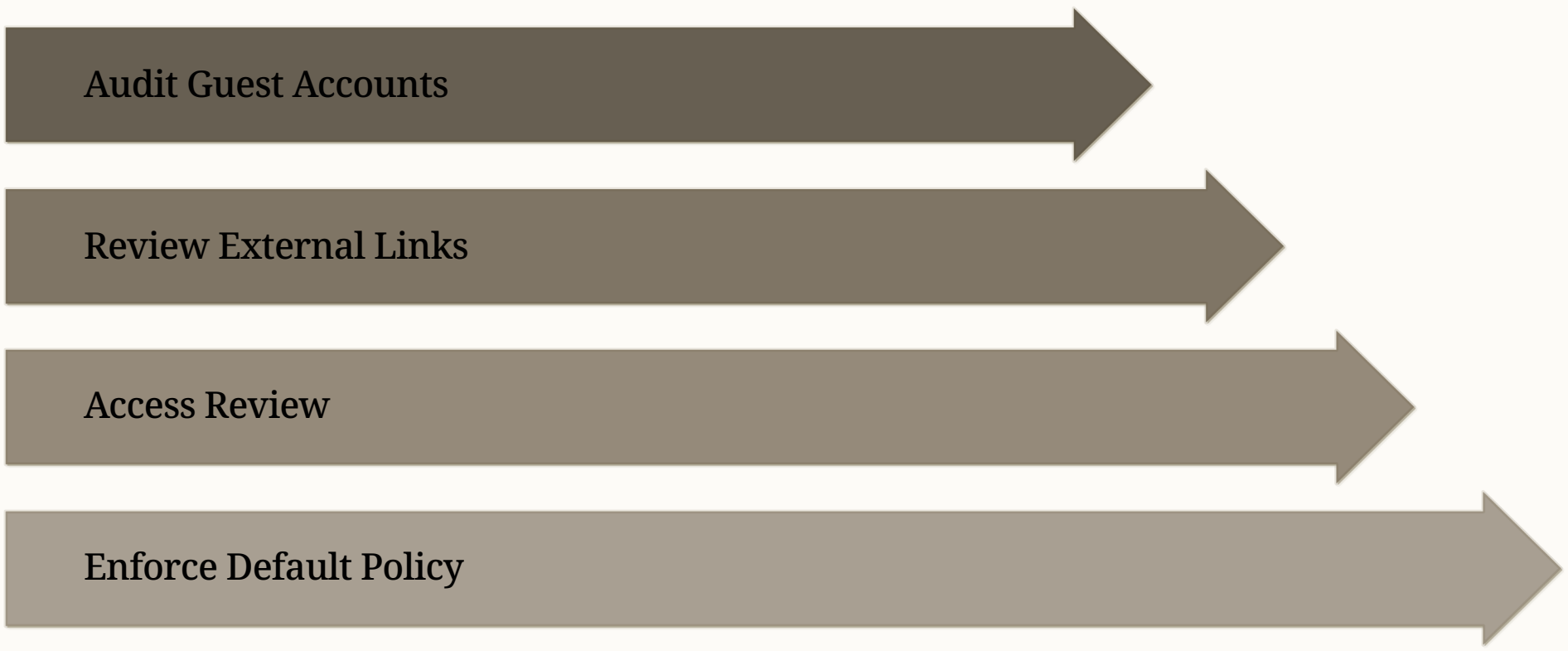
The riskiest sharing option that creates untrackable access to your content.

Stale External Access

External users who completed projects months ago but still have full access.

Permissive Defaults

Sharing policies that default to broad access instead of requiring intentional sharing.



Action Items

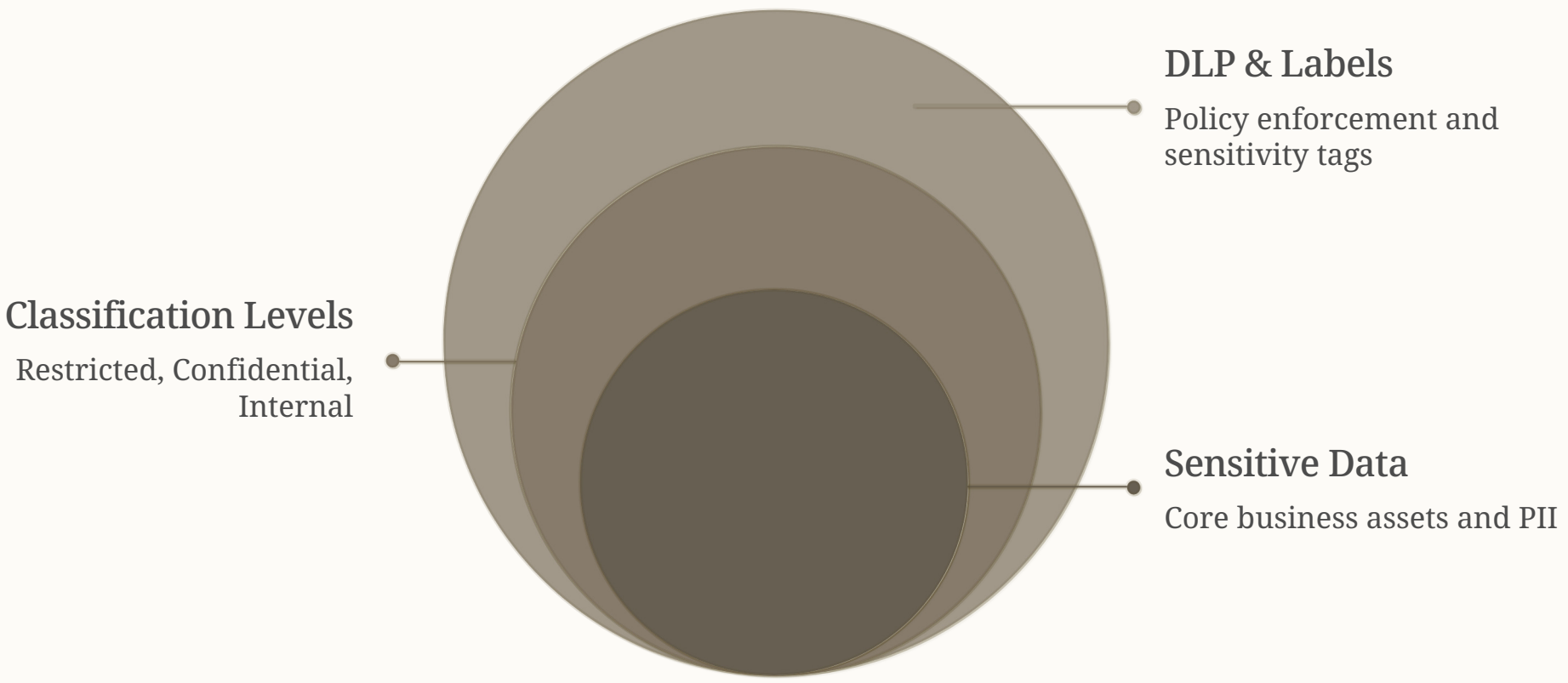
- **Audit all active guest accounts** – Export from Entra ID, check last login
- **Remove stale guests** – Document removed accounts for audit trail
- **Disable "Anyone" sharing links** – SharePoint Admin Center → Sharing settings
- **Set link expiration** – Default 30-90 days to prevent zombie links
- **Switch default to "Specific People"** – Require intentional sharing decisions
- **Set up guest access reviews** – Quarterly cadence using Entra ID Access Reviews if licensed

Owner: _____ **Target Date:** _____

☐ **Deliverable:** Guest access cleanup plan with stale accounts removed, link-sharing settings locked down, and quarterly review cadence scheduled.

Step 3: Label & Lock Down Sensitive Data

Protecting your organization's crown jewels requires more than good intentions—it demands systematic classification and enforcement. Sensitivity labels and DLP policies work together to prevent data leaks before they happen.



HR Files

Salary data, performance reviews → auto-encrypt with "Highly Confidential" label

Finance Files

Budgets, projections, contracts → encrypt and restrict external sharing

Legal Files

IP, contracts, agreements → block external sharing completely

Implementation Checklist

Create Sensitivity Labels

Start with Confidential and Highly Confidential in Purview

Apply Protection

Auto-encrypt and restrict sharing based on classification

Deploy DLP

Create rules for credit cards, SSNs, and employee IDs

Train Department Owners

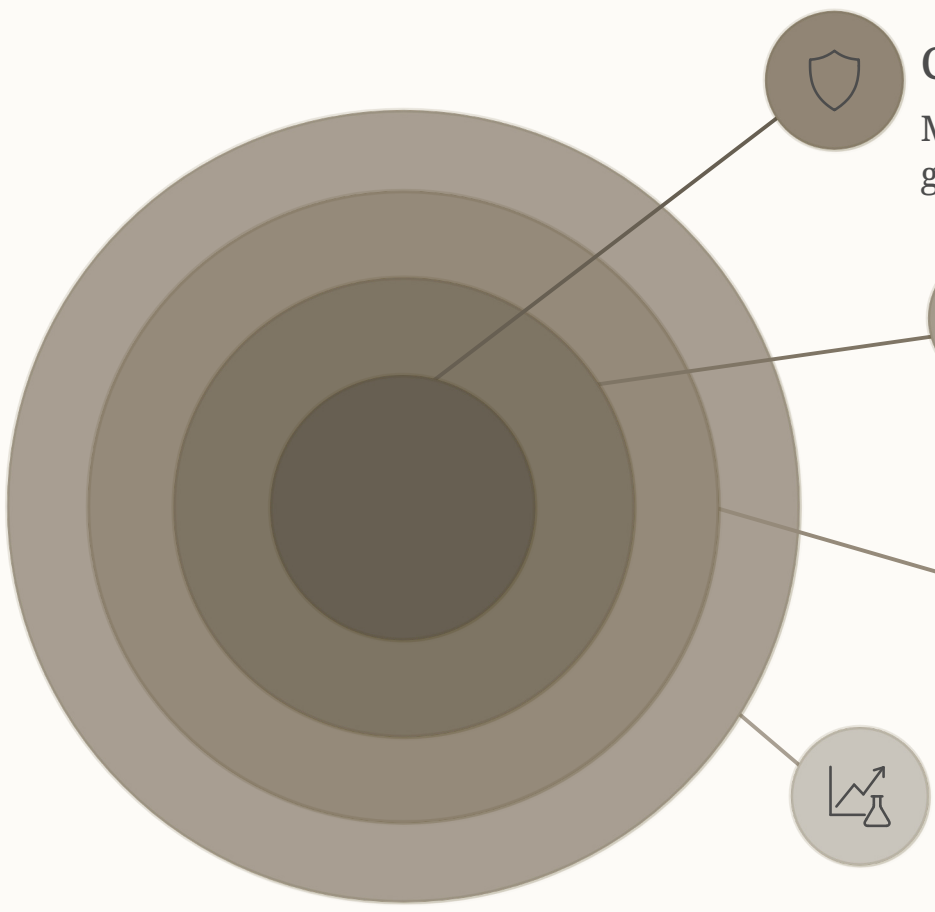
15-minute briefing on when and how to use labels

Owner: _____ **Target Date:** _____

Deliverable: Baseline labeling + DLP starter plan with at least 2-3 active DLP policies and labels applied to top 20% of sensitive files.

Step 4: Tighten Microsoft Entra ID (Identity Gatekeeper)

Your identity layer is the first—and most critical—line of defense. A compromised user account can bypass every other control you implement. This step focuses on the non-negotiables that affect 99% of attack vectors.



Core Identity

Microsoft Entra ID user accounts and groups.

Authentication

Multi-factor and passwordless sign-in flows.

Access Controls

Conditional Access and least-privilege policies.

Monitoring & Recovery

Logging, risk detection, and account recovery.

Enable MFA for All Users

Non-negotiable security control. Start with admins, then roll out in waves to minimize user friction.

Verify Offboarding

Confirm ex-employee access removed on day 1. Run a retrospective check for the past 6 months.

Run Access Review

Department leads validate their users' access quarterly. Remove dormant accounts (6+ months inactive).

Limit Admin Accounts

Only necessary people with 2+ admins per critical role for redundancy and accountability.

Conditional Access (Optional Advanced)

Once baseline controls are in place, consider implementing Conditional Access policies to further fortify your identity layer. These policies evaluate various signals in real-time to make access decisions, mitigating risk before it impacts your organization.

- **Block Unusual Sign-in Locations:** Restrict access from untrusted geographies or IP ranges, preventing access attempts from suspicious origins.
- **Require Compliant Devices:** Ensure users can only access sensitive data from devices that meet your security standards (e.g., devices that are enrolled in Intune and are marked as compliant, have the latest OS updates, and antivirus software).
- **Risk-Based Policies:** Utilize Microsoft Entra ID's risk engine to trigger stronger authentication (like MFA) or block access entirely for users detected with high sign-in or user risk.
- **Implementation Best Practices:** Always start with policies in "report-only" mode to understand their impact and fine-tune them before enforcing. Roll out policies in phases, starting with a small pilot group.

Owner: _____ **Target Date:** _____

☐ **Deliverable:** 100% of users on MFA, current access review completed, and quarterly review cycle scheduled.

Step 5: Monitor Copilot Usage & Permission Events

Security isn't a one-time project - it's an ongoing conversation between your controls and your user's behavior. Monitoring helps you spot anomalies before they become incidents and proves your due diligence when auditors ask questions.

External Sharing Spikes

Alert when more than 10 external shares occur in a single day—often indicates compromised accounts or policy violations.

Public Teams Created

Flag new public Teams for immediate review to prevent accidental data exposure.

Copilot Usage Patterns

Monitor for unusual queries to sensitive data sources—watch for data exfiltration attempts.

Bulk Downloads

Track spikes in file access or downloads that deviate from normal user behavior patterns.

Monitoring Cadence

Daily

Review automated alerts for high-priority events

1

Weekly

Check audit log summaries for trends

2

Monthly

Run Data Access Governance report

3

Quarterly

Department leads re-confirm user access

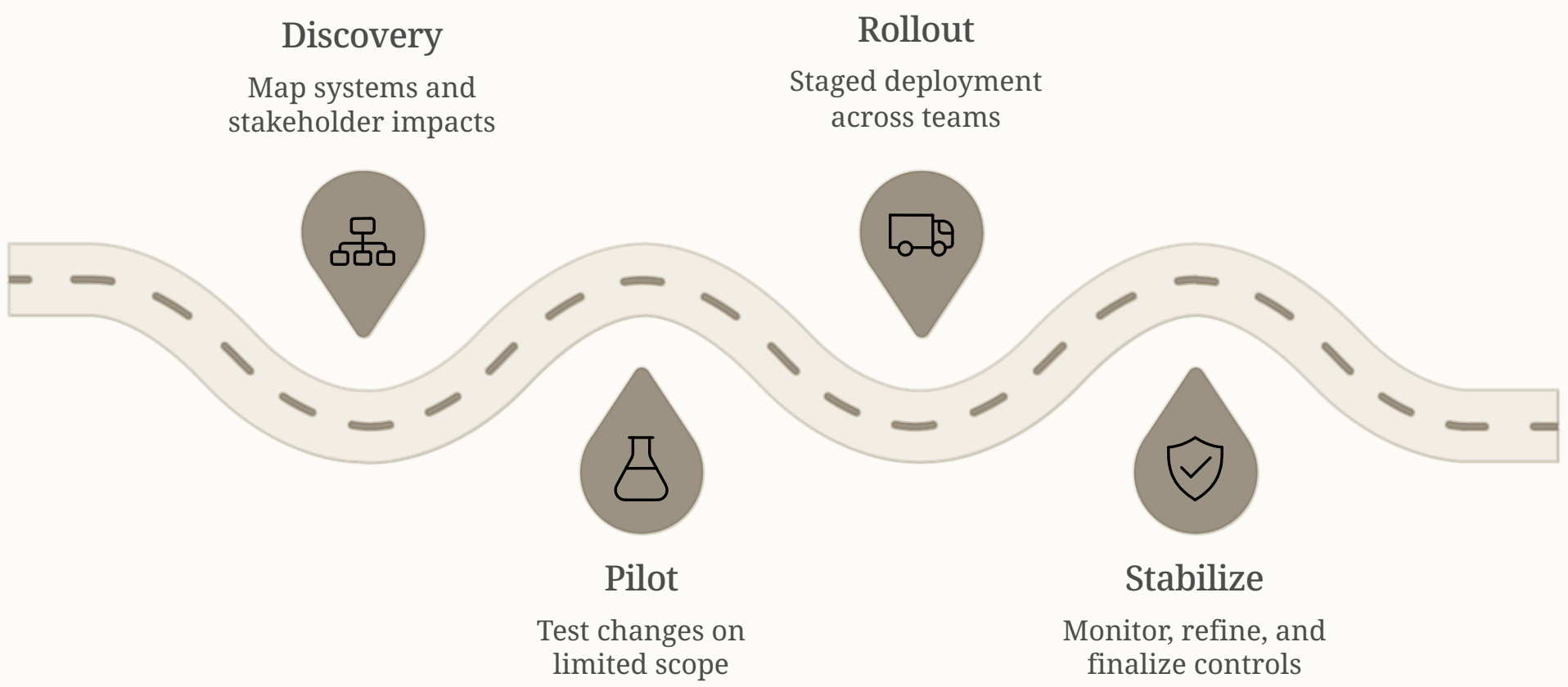
4

Owner: _____ **Target Date:** _____

Deliverable: Monthly audit log reviews scheduled, alerts configured, and dashboard/spreadsheet tracking permission events.

Step 6: Create Phased Rollout Plan

Change management separates successful audits from organizational chaos. This phased approach balances urgency with practicality, ensuring critical systems stay online while you progressively lock down permissions.



Implementation Timeline

Weeks	Phase	Owner	Status	Notes
1-2	Quick Wins	_____	☐	Disable "Anyone" links, remove stale guests, audit public Teams
3-4	Medium Effort	_____	☐	Convert public Teams, apply Sensitivity Labels, test DLP
5-8	Identity Hardening	_____	☐	MFA rollout, Entra ID access reviews, documentation
Month 3+	_____	☐		Monthly audit reviews, quarterly access reviews, Copilot monitoring

Communication Plan

- **Week 0:** Announce audit to leadership; explain "why now" (Copilot risk)
- **Week 1:** Notify Teams/Groups owners of changes coming; request input
- **Week 2-4:** Roll out changes in batches; address questions same day
- **Month 2+:** Share monthly audit summary; celebrate wins

Risk Mitigation

- Test all changes in dev/pilot tenant first
- Keep rollback plan documented for each change
- Assign owner for each step
- Schedule "go/no-go" review before major rollouts

Owner: _____ **Target Date:** _____

☐ **Deliverable:** Documented rollout plan, communication schedule, and risk register with owners assigned.

AdaptSphere NextGen AI, LLC | adaptsphere.ai | info@adaptsphere.ai