# CISO Tenant Migration Checklist

Compliance-Safe M&A Microsoft 365 Tenant Migration Framework

For Executive Steering Committee and Board Briefings

## Executive Summary

Microsoft 365 tenant migrations during M&A transactions present significant compliance and legal risks that require executive-level oversight. This checklist provides a structured framework to ensure regulatory obligations are met while maintaining business continuity during the integration process.

## 1. Clarify Regulatory and Legal Anchors Before Design

- ✓ Map all active litigation, investigations, and regulatory matters
  - Identify every Microsoft 365-dependent legal or regulatory obligation
- ✓ Inventory eDiscovery cases, holds, retention policies, and data residency commitments
  - Document current compliance posture in both source and target tenants
- ✓ Align with legal on source tenant preservation requirements beyond TSA
- ✓ Define timeline and scope for maintaining legacy tenant access

## 2. Decide the Compliance Operating Model for TSA

- ✓ Define which tenant acts as "system of record" for legal and regulatory purposes
  - Clarify authority during transition period to avoid confusion
- ✓ Establish explicit guidance on which tenant to use for new matters
  - New eDiscovery cases, retention policies, and DLP rules
  - Document minimum compliance capabilities before user cutover
  - Baseline DLP, key retention labels, core sensitivity labels

## 3. Design Migration Waves Around Compliance Constraints

- [ ] Segregate held users and critical investigations into dedicated waves
  - Users under Litigation Hold require specialized tooling and legal oversight
- [ ] Plan eDiscovery export and case recreation timeline
  - Complete before decommissioning any source workloads
- [ ] Sequence high-risk workloads after controls are in place
  - Teams, SharePoint, OneDrive move only after labels, DLP, barriers ready

## 4. Rebuild and Validate Purview Controls in Target

- [ ] Recreate retention and DLP policies using documented baselines
  - Avoid ad-hoc manual clicks during cutover night
- [ ] Reimplement communication compliance and information barriers
- [ ] Obtain specific signoff from risk and legal teams
- [ ] Validate private channels, Teams storage models, and multi-geo flows
- [ ] Verify alignment with updated Purview policies before and after migration



## 5. Preserve Evidence and Observability Across Boundary

- [ ] Export and archive unified audit logs before source tenant sunset
  - Store in external SIEM or evidence repository for forensic continuity
- [ ] Define SOC procedures for cross-tenant incident correlation
  - Alert routing, investigation playbooks, and reporting across boundaries
  - Document any unavoidable "gap windows" in telemetry
- [ ] Include in risk register and board-level reporting

## 6. Align Executive Communication and Governance

- [ ] Build concise "Compliance in Tenant Migration" briefing
  - Highlight red-flag areas and key decision points for steering committee
- [ ] Tie migration milestones directly to regulatory outcomes
  - E.g., "Cannot deprecate Tenant A until cases X, Y, Z recreated in Tenant B"
- [ ] Agree on escalation paths when compliance blockers threaten TSA dates

Avoid negotiating hold removal on weekend before cutover

## Recommended Next Steps

1. Schedule working session with CISO, General Counsel, CIO, and M&A integration lead

2. Commission focused Microsoft 365 compliance due diligence on both source and target tenants

3. Identify where native Microsoft tools stop and third-party migration solutions are needed

4. Present comprehensive risk register to integration steering committee with clear escalation criteria

5. Establish regular compliance checkpoint meetings throughout migration timeline