M365 COPILOT DEPLOYMENT CHECKLIST

September 2026

A Manager's Guide for Alternative Investment Funds

For alternative investment firms, Copilot is not just a productivity tool; it is a control-plane decision. The goal is to move from Shadow AI to a secure, auditable M365 safe zone before usage scales.

Phase 1: Enterprise Readiness

- **Licensing**: Use an eligible M365 base license (E5) plus Copilot (E7 adds adjacent controls, not more Copilot functionality).
- **Identity Baseline:** Enforce Entra SSO, MFA, Conditional Access, and managed-device access before go-live.
- **Platform Readiness:** Keep mailboxes in Exchange Online, keep M365 apps current, and allow required Microsoft endpoints and browser support.
- **Auto-Deploy Risk**: Review Microsoft's Copilot app rollout settings so Copilot does not simply appear before guardrails are in place.

Phase 2: Data Boundary & Permission Hygiene

- **Oversharing Audit:** Run Purview DSPM for AI and review broad SharePoint access before Copilot can ground on it.
- **Safe Zones:** Apply sensitivity labels, use No-AI exclusions where needed, and keep high-risk sites out of Copilot search.
- **Restricted Discovery:** Use SharePoint Restricted Content Discovery when a client wants Copilot without exposing all SharePoint content on day one.
- **Approved Tools Only**: Block unapproved plugins, browser extensions, and consumer AI paths.

Phase 3: Compliance & Defensibility

- **Audit & Logging:** Enable Purview Audit so prompts, responses, and policy events are reviewable for LP, ODD, and regulatory scrutiny.
- **DLP Guardrails:** Block or redact MNPI, investor PII, and compensation data in Copilot interactions.
- **Policy**: Publish an AI acceptable-use policy with approved use cases, off-limits data, and an exception path before rollout.
- **Retention**: Map Copilot activity into existing retention and eDiscovery workflows.

Phase 4: Controlled Rollout

- **Pilot Scope:** Start with a small low-risk user group and curated libraries; don't begin with trading, or investor data.
- **Sanctioning:** Sanction M365 Copilot and approved AI; monitor and block unsanctioned AI through Defender for Cloud Apps.
- **Teams Governance:** Set a deliberate stance on transcription and meeting AI features; several alt-invest clients are defaulting to tighter settings.
- **Prompt Playbooks:** Give users role-based prompts for research, IR, and recap workflows so adoption is useful, not random.
- **Agentic Features:** Treat Copilot Cowork and similar agentic modes as a separate decision with separate controls, not a default extension of chat Copilot.

If you cannot explain where the data goes, who can reach it, and what gets logged, you are not ready for tenant wide Copilot.