The Zero-Trust RBAC Deployment Checklist

Use this functional checklist to audit your legacy environment, deploy dynamic identity management, and secure your Microsoft 365 tenant against AI data overexposure.

Phase 1: Legacy Architecture Audit (Discovery)

- [ ] **Identify Broken Inheritance:** Run a diagnostic script to flag all document libraries and folders where site-level inheritance has been manually disabled.
- [ ] **Locate Direct User Assignments:** Audit all site collections to find users who have been granted direct access to files rather than via group membership.
- [ ] **Inventory "Everyone" Group Usage:** Pinpoint all sensitive libraries where the default "Everyone except external users" group has been mistakenly applied.
- [ ] **Analyze External Guest Access:** Export a list of all active external sharing links and flag those without a 30-day auto-expiration policy.

Phase 2: Entra ID Identity Mapping (Restructuring)

- [ ] **Define Persona-Based Roles:** Map technical permission levels (Read, Contribute) to overarching business personas (e.g., "Financial Auditor", "Contractor") rather than individual names.
- [ ] **Create Centralized Security Groups:** Establish the required security groups directly within the Entra ID admin center, explicitly avoiding local SharePoint site groups.
- [ ] **Configure Dynamic Membership Rules:** Write Entra ID rules to automatically populate groups based on authoritative HR directory attributes (e.g., Department, Region, Job Title).
- [ ] **Implement Privileged Identity Management (PIM):** Revoke permanent Global Admin rights and require Just-In-Time (JIT) access approval for all administrative maintenance.

Phase 3: AI-Readiness & Advanced Governance (Hardening)

- [ ] **Deploy Microsoft Purview Labels:** Create and apply immutable sensitivity labels (e.g., "Highly Confidential") to encrypt files regardless of where they are moved within the tenant.
- [ ] **Enforce Conditional Access Policies:** Configure rules to block access from unmanaged devices or unexpected geographic locations.
- [ ] **Activate SharePoint Advanced Management (SAM):** Generate Data Access Governance (DAG) reports to identify overshared sites.
- [ ] **Restrict Semantic Indexing:** Utilize Restricted SharePoint Search to ensure legacy archives and sensitive sites are excluded from Microsoft 365 Copilot queries.