CHECKLIST

Hardening Active Directory Tiered Administration Model Checklist

A practical checklist for validating and hardening a tiered administration model in Active Directory before production rollout.

Hardening Active Directory Tiered Administration Model Checklist

Use this checklist to verify that your tiered administration model is operationally enforceable, not just documented. Mark each item complete only when it is implemented, tested, and reviewed.

1) Define the tier model clearly

- [ ] Tier 0, Tier 1, and Tier 2 definitions are documented and approved.
- [ ] Identity infrastructure, security control points, and domain-level administration are assigned to Tier 0.
- [ ] Server, application, and infrastructure administration are assigned to Tier 1.
- [ ] Endpoints, help desk operations, and user support activities are assigned to Tier 2.
- [ ] Exceptions to the tier model are explicitly documented with business justification.
- [ ] The model includes a clear statement of what is not allowed, not just what is allowed.

2) Inventory privileged identities and paths

- [ ] All privileged accounts are inventoried by role, tier, and owner.

- [ ] Separate administrative identities exist for each tier where needed.
- [ ] Shared admin accounts are eliminated or tightly controlled.
- [ ] Service accounts with privileged access are identified and reviewed.
- [ ] Standing rights are documented for all privileged accounts.
- [ ] All sign-in paths for privileged accounts are mapped, including interactive, remote, scheduled, and delegated access.

3) Enforce logon boundaries

- [ ] Tier 0 accounts cannot sign in to Tier 1 or Tier 2 systems except for approved, audited exceptions.
- [ ] Tier 1 accounts cannot sign in to Tier 2 systems unless explicitly required.
- [ ] Tier 2 accounts have no path to Tier 0 resources.
- [ ] Interactive logon is restricted by tier using policy and local configuration.
- [ ] Remote desktop, SSH, PowerShell remoting, and other administrative channels are tier-restricted.
- [ ] Privileged credentials are not stored in browsers, password managers, scripts, or tools on lower-trust systems.

4) Use dedicated management endpoints

- [ ] Tier 0 administration uses dedicated Tier 0 workstations or jump hosts.
- [ ] Tier 1 administration uses separate management endpoints from Tier 0.
- [ ] Tier 2 administration uses endpoints appropriate to lower trust.
- [ ] Privileged management endpoints are hardened, patched, and monitored.
- [ ] Email, web browsing, chat, and general-purpose productivity use are prohibited on Tier 0 admin workstations.
- [ ] Management endpoints are not shared with general user activity.

5) Reduce credential exposure

- [ ] Tier 0 credentials never appear on lower-trust systems during normal operations.
- [ ] Cached credentials are minimized or disabled where feasible.
- [ ] Credential delegation is constrained to approved workflows only.
- [ ] LSASS protection, credential guard, or equivalent protections are enabled where supported.
- [ ] Admin tools that can expose credentials are reviewed and restricted.
- [ ] Copy-paste and file transfer paths between tiers are limited or controlled.

6) Review delegation and service account usage

- [ ] Unnecessary constrained and unconstrained delegation is removed.
- [ ] Service accounts are reviewed for cross-tier authentication rights.
- [ ] Service accounts are assigned the minimum permissions required.
- [ ] Password rotation or managed identity mechanisms are in place where possible.
- [ ] Tier-crossing service dependencies are justified and documented.
- [ ] Backup, monitoring, deployment, and automation accounts are treated as privileged assets.

7) Remove excessive standing privilege

- [ ] Local administrator rights are reduced to the minimum required.
- [ ] Domain admin membership is limited and reviewed regularly.
- [ ] Tier 0 privileges are time-bound or otherwise just-in-time where possible.
- [ ] Temporary elevation has an approval and expiration process.
- [ ] Break-glass accounts exist, are protected, and are tested.

- [ ] Emergency access procedures do not bypass logging or review.

8) Separate admin tooling and workflows

- [ ] Tier 0 tools are used only from Tier 0 management systems.
- [ ] Tier 1 tools are isolated from Tier 0 operations.
- [ ] Administrative scripts are stored, signed, and reviewed appropriately.
- [ ] Tooling does not reuse the same credentials across tiers without justification.
- [ ] Browser-based admin portals are accessed only from approved management systems.
- [ ] Automation jobs are executed from the correct tier and with least privilege.

9) Validate logon and session controls

- [ ] Authentication logs show that cross-tier logons are blocked or rare and approved.
- [ ] Failed logon attempts are monitored for privileged accounts.
- [ ] Remote sessions are traceable to an approved source device and account.
- [ ] Session timeout, lock, and disconnect behavior is defined for privileged access.
- [ ] Administrative sessions do not persist longer than necessary.
- [ ] Test logons confirm that the intended restrictions are actually enforced.

10) Improve monitoring and detection

- [ ] Privileged activity is logged centrally.
- [ ] Tier 0 administrative actions are separately reviewed.
- [ ] Cross-tier logon attempts generate alerts or reviewable events.
- [ ] Abnormal privileged movement is detectable from event logs and endpoint telemetry.
- [ ] Changes to privileged group membership are monitored.
- [ ] Service account authentication patterns are baselined and reviewed.

11) Test for common failure modes

- [ ] Tier 0 admins can work without signing in to Tier 1 or Tier 2 systems.
- [ ] Tier 1 admins cannot access Tier 0 resources through convenience paths.
- [ ] A compromised lower-tier endpoint cannot capture usable Tier 0 credentials.
- [ ] Shared jump hosts do not collapse tier boundaries.
- [ ] Monitoring, backup, and deployment tools do not create hidden cross-tier bridges.
- [ ] Phishing and browser-based compromise scenarios have been considered for privileged users.

12) Review exceptions and rollback plan

- [ ] Every exception has an owner, expiration date, and approval record.
- [ ] Exceptions are reviewed after implementation, not left indefinitely.
- [ ] There is a rollback plan if a control breaks critical operations.
- [ ] The rollback plan preserves the ability to detect and contain risk.
- [ ] Production rollout is gated on successful validation of the control set.

Production readiness questions

Answer these before trusting the model in production:

- [ ] Can a Tier 0 credential ever reach a lower-trust system during normal operations?
- [ ] Can a compromised Tier 2 endpoint plausibly lead to Tier 0 control?
- [ ] Are admin identities, devices, and tools truly separated by tier?
- [ ] Are service accounts and automation paths included in the same review as human admins?
- [ ] Can you prove boundary enforcement with logs, not just policy documents?

Final sign-off

- [ ] Tier boundaries are documented, enforced, and tested.
- [ ] Logon paths are restricted and verified.
- [ ] Delegation and standing rights are minimized.
- [ ] Monitoring is in place for privileged movement and exceptions.
- [ ] The environment is ready for controlled production rollout.

Notes

Use this checklist during design review, implementation, and periodic revalidation. A tiered administration model is only effective when it is consistently enforced across people, devices, credentials, and tooling.