CHECKLIST

Active Directory Tiering Model for Privileged Access Control Checklist

A practical checklist for validating and implementing an Active Directory tiering model to reduce blast radius, separate privileged access by trust level, and verify cross-tier controls before production use.

Active Directory Tiering Model for Privileged Access Control

Implementation and Validation Checklist

Use this checklist to assess whether your Active Directory tiering model is ready for production use and whether the trust boundaries are actually enforced.

Purpose

An Active Directory tiering model separates administrative privilege by trust level so one compromised account cannot automatically reach every critical system. This checklist helps you validate the design, confirm the controls, and identify weak points before rollout.

---

1) Define the tier model

- [ ] Tier 0 is defined for identity and trust infrastructure.
- [ ] Tier 1 is defined for servers, virtualization, backup, and infrastructure services.
- [ ] Tier 2 is defined for workstations, help desk support, and lower-trust endpoints.
- [ ] The organization has documented what belongs in each tier.
- [ ] Exceptions and special cases are explicitly documented.

Verify

- [ ] Domain controllers are assigned to Tier 0.
- [ ] PKI, federation, directory synchronization, and identity management systems are assigned to Tier 0.
- [ ] Infrastructure servers are assigned to Tier 1.
- [ ] End-user endpoints are assigned to Tier 2.
- [ ] No system is left in an undefined trust category.

---

2) Separate privileged identities

- [ ] Administrative accounts are separated by tier.
- [ ] Tier 0 admins do not use the same account for Tier 1 or Tier 2 tasks.
- [ ] Tier 1 admins have accounts that are not used for Tier 0 administration.
- [ ] Tier 2 support accounts cannot administer higher-tier systems.
- [ ] Shared admin accounts are eliminated or formally justified.

Verify

- [ ] Each privileged user has distinct accounts for each approved tier.
- [ ] Naming standards clearly distinguish privileged account purpose.
- [ ] MFA or equivalent strong authentication is enforced where feasible.
- [ ] Emergency access accounts are controlled, monitored, and tested.

---

3) Restrict where privileged accounts can log on

- [ ] Tier 0 accounts can only log on from Tier 0 workstations or equivalent hardened endpoints.
- [ ] Tier 1 accounts are restricted to Tier 1 management devices.
- [ ] Tier 2 support accounts are restricted to approved Tier 2 admin devices where applicable.
- [ ] Interactive logon paths are blocked across tiers.
- [ ] Remote logon rules match the tier policy.

Verify

- [ ] Tier 0 accounts cannot sign in to mixed-use laptops.
- [ ] Tier 0 accounts cannot sign in to lower-tier servers or workstations.
- [ ] Tier 1 accounts cannot authenticate to Tier 0 systems.
- [ ] Admin consoles are not accessible from standard user devices.

---

4) Harden administrative devices

- [ ] Privileged access workstations or hardened admin endpoints are deployed.
- [ ] Administrative devices are dedicated to admin use.

- [ ] Email, web browsing, and general productivity tasks are not performed from Tier 0 admin sessions.
- [ ] Administrative devices are patched, monitored, and baselined.
- [ ] Local admin rights on privileged devices are tightly controlled.

Verify

- [ ] Browser use on Tier 0 endpoints is minimized or blocked where practical.
- [ ] Removable media controls are in place.
- [ ] Endpoint security is enforced consistently.
- [ ] Credential caching and token exposure are reduced as much as possible.

---

5) Constrain management paths

- [ ] Jump hosts are defined and approved for privileged access.
- [ ] Direct administrative access is blocked where a jump path is required.
- [ ] Remote Desktop, PowerShell remoting, SSH, and vendor tools are restricted by tier.
- [ ] Management protocols are limited to approved source and destination pairs.
- [ ] No lower-tier system can initiate an approved path into a higher tier.

Verify

- [ ] Tier 2 endpoints cannot reach Tier 0 management ports.
- [ ] Tier 1 hosts cannot be used as a bridge to Tier 0 systems.
- [ ] Jump hosts are treated as privileged assets and monitored accordingly.
- [ ] Firewall and network segmentation support the tier policy.

---

6) Review group membership and delegation

- [ ] Privileged group memberships are documented and reviewed.
- [ ] Nested group usage is understood and intentionally configured.
- [ ] Local administrator assignments are not broader than necessary.
- [ ] Delegation settings do not create cross-tier trust paths.
- [ ] Service accounts are reviewed for privilege creep.

Verify

- [ ] No Tier 2 support group is indirectly granting Tier 0 access.
- [ ] No server admin group has unintended rights on domain controllers.
- [ ] Delegation is approved, minimized, and monitored.
- [ ] Legacy service accounts are not silently bypassing tier boundaries.

---

7) Validate that credentials cannot be reused across tiers

- [ ] Credential reuse is tested and blocked where possible.
- [ ] Cached credentials on lower-trust systems are minimized.
- [ ] Sessions are isolated by device and purpose.
- [ ] Privileged users do not perform non-admin activity in admin sessions.
- [ ] Session hijacking risk is considered in the endpoint design.

Verify

- [ ] A Tier 0 credential obtained on a lower-tier endpoint cannot be used to reach Tier 0 assets.
- [ ] A Tier 1 credential cannot authenticate to Tier 0 systems.
- [ ] Long-lived sessions and token exposure are controlled.
- [ ] Admins are not reusing the same workstation for daily and privileged activity.

---

8) Confirm service account boundaries

- [ ] Service accounts have the minimum required scope.
- [ ] Service accounts are not used as broad administrative identities.
- [ ] Service accounts are mapped to the tier of the systems they support.
- [ ] Password rotation and lifecycle management are defined.
- [ ] Interactive logon is disabled unless explicitly required and justified.

Verify

- [ ] No service account can administer systems outside its intended tier.
- [ ] No service account is exempt from review because it is ?legacy.?
- [ ] gMSA or equivalent managed identity options are considered where appropriate.
- [ ] Secrets are protected and access to them is logged.

---

9) Set monitoring and alerting for boundary violations

- [ ] Authentication events are logged for privileged accounts.
- [ ] Administrative logon sources are monitored.
- [ ] Alerts exist for impossible or unusual cross-tier access.

- [ ] Tier boundary violations are visible in SIEM or equivalent tooling.
- [ ] Incident response steps exist for suspected admin credential compromise.

Verify

- [ ] Tier 0 admin logons from Tier 2 endpoints generate alerts.
- [ ] Privileged account use from unexpected host classes is flagged.
- [ ] Delegation abuse indicators are monitored.
- [ ] Password spray and credential stuffing detections are in place for identity exposure scenarios.

---

10) Test the model before production enforcement

- [ ] A narrow validation workflow has been completed.
- [ ] Findings were recorded and remediated.
- [ ] The environment was retested after fixes.
- [ ] Rollout was staged rather than enforced all at once.
- [ ] Exception handling exists for business-critical edge cases.

Validation workflow

- [ ] Identify Tier 0 systems and accounts.
- [ ] Verify where each privileged account can log on interactively and remotely.
- [ ] Confirm the admin workstation or jump path is isolated from lower tiers.
- [ ] Test whether credentials can be reused across tiers.
- [ ] Review delegation, local admin, and service account paths for cross-tier exposure.
- [ ] Record violations, fix them, then retest before broad enforcement.

Production readiness checklist

Before moving to enforcement, confirm the following:

- [ ] Tier definitions are documented and agreed upon.
- [ ] Privileged accounts are separated by purpose and tier.
- [ ] Administrative devices are hardened and dedicated.
- [ ] Logon restrictions match the tier design.
- [ ] Management paths are restricted and monitored.
- [ ] Delegation and group membership do not cross trust boundaries.
- [ ] Service accounts have been reviewed.
- [ ] Alerting exists for boundary violations.
- [ ] The design has been tested and retested.
- [ ] Exceptions have owners, expiry dates, and compensating controls.

Common warning signs

- [ ] One admin account works everywhere.
- [ ] Jump hosts exist but are not the only admin path.
- [ ] Server administration and workstation support happen from the same endpoint.
- [ ] Local admin rights are broadly delegated for convenience.
- [ ] Service accounts have broad reach without clear justification.
- [ ] Tier labels exist, but logon paths do not reflect them.

If several of these are true, the environment likely has a naming convention, not a real tiering model.

Decision checkpoint

Use a tiering model when you need stronger containment of privileged access, especially if identity compromise would create broad lateral movement risk. If the environment cannot support separate accounts, devices, and management paths, the model is incomplete and should not be treated as enforced.

Notes

- This checklist is vendor-neutral and intended for operational use.
- Adapt the tier definitions to your environment, but keep the separation principle intact.
- The model only works when accounts, devices, and access paths all follow the same trust boundary.