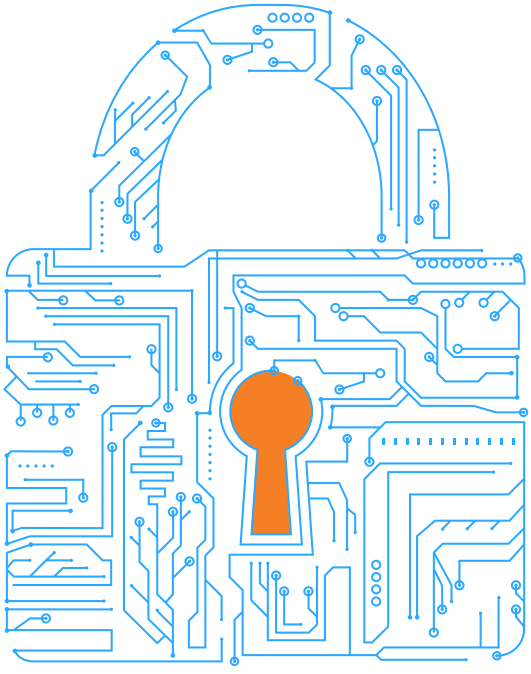
Cayosoft

CHECKLIST

10 Best Practices for Securing and Simplifying Hybrid Identity Management

How to secure, simplify, and scale your Microsoft identity infrastructure



Published:
2025

Sponsored by:
Cayosoft

+1 (614) 423-6718

IT Identity and Architecture Team Checklist

Best Practice	Status			Notes/Action Items
Zero standing administrative privileges	◯ Done	◯ In Progress	◯ Not Started	
Automated user onboarding, updating, and deprovisioning	◯ Done	◯ In Progress	◯ Not Started	
Policy-driven, no-code automation (no scripts)	◯ Done	◯ In Progress	◯ Not Started	
Unified hybrid identity console in place	◯ Done	◯ In Progress	◯ Not Started	
Delegated and audited LAPS/BitLocker access	◯ Done	◯ In Progress	◯ Not Started	
Dynamic group management and certification workflows	◯ Done	◯ In Progress	◯ Not Started	
Microsoft 365 license optimization is automated	◯ Done	◯ In Progress	◯ Not Started	
Attribute and naming standard enforcement is active	◯ Done	◯ In Progress	◯ Not Started	
Attribute-driven (dynamic) role-based access controls	◯ Done	◯ In Progress	◯ Not Started	
HR integration for lifecycle management	◯ Done	◯ In Progress	◯ Not Started	

If you checked fewer than eight best practices as "Done," it's time to modernize.

Explore how Cayosoft Administrator can help you:

- Strengthen security
- Eliminate manual errors
- Save time and money

For More Detailed Information Check Page 3

The 10 Best Practices

1. Eliminate Standing Privileges

Implement zero-native-permission delegation using Role-Based Access Control (RBAC) and Virtual OUs to minimize insider risk and lateral movement attacks. Ensure admin roles are scoped to specific objects or attributes without granting full domain or tenant-wide permissions.

2. Automate the Entire User Lifecycle

Automate user onboarding, modification, and deprovisioning with HR-driven provisioning (via Workday, SQL, or CSV integrations). Automatically assign and revoke group memberships, licenses, and mailboxes based on HR status changes.

3. Replace Scripts with Policy-Driven Automation

Deploy a no-code rule engine for group membership enforcement, license assignment, and mailbox provisioning tasks. Eliminate reliance on brittle PowerShell scripts that lack auditability and scalability.

4. Centralized Hybrid Identity Management

Use a unified, web-based console that connects on-premises AD, Entra ID, Exchange, and Microsoft 365 without requiring agents on domain controllers. Manage all hybrid tasks in real-time, without jumping between tools or relying on sync cycles.

5. Secure Access to Sensitive Credentials

Implement delegated, audited retrieval of Local Administrator Password Solution (LAPS) credentials and BitLocker recovery keys. Enforce strict access policies and maintain immutable audit trails of who accessed credentials and when.

6. Automate Group Governance

Enable dynamic, attribute-based membership updates for security and distribution groups. Implement attestation workflows where group owners must periodically certify membership lists. Support time-bound group memberships to automatically expire access.

7. Optimize Microsoft 365 Licensing

Auto-assign licenses based on user attributes (e.g., department, location, role). Detect and reclaim unused licenses automatically. Manage quota pools and delegate license visibility at the business unit or department level to optimize spend.

8. Enforce Naming Standards and Attribute Validation

Automate enforcement of naming conventions for users, groups, and devices (e.g., First.Last@company.com, Location-Dept-DeviceType). To prevent directory inconsistencies, validate key attributes like department, title, and manager.

9. Attribute-Based Access Controls

Define role assignment policies based on user attributes such as department, office location, or job title. Dynamically update access rights as user attributes change, ensuring least privilege without manual intervention.

10. Integrate Identity Management with HR Systems

Direct integrations with Workday, Oracle HR, or flat files drive identity management processes. Trigger provisioning, group assignments, license application, and deprovisioning based on real-time HR events.