MICROSOFT ENTRA OPTIMIZATION CHECKLIST

Most organizations pay for Microsoft Entra but use only a fraction of it. 14 decision points to unlock the full value of your investment, close security gaps, and activate the governance features you are already paying for. Estimated timeline: 4-8 weeks for full optimization.

Microsoft Entra is not a product you deploy once and forget. It is a platform that rewards attention and punishes neglect. Organizations that activated Entra ID five years ago and never revisited their configuration are running on defaults that no longer match their security posture, their compliance requirements, or the features Microsoft has shipped since.

This checklist is not about buying Entra. It is about getting what you already own. Check off the items you have completed to track your progress. Expand each item for details and common mistakes.

01

These six decisions establish the identity foundation of your Entra ID tenant. Most tenants defaulted to convenience years ago and never revisited.

1

Conditional Access Policy Audit

CRITICAL 1-2 WEEKS (DEPENDS ON SCOPE) *Security*

Review every Conditional Access policy in your tenant. Most organizations have 5-10 policies created years ago that no longer reflect their current risk posture. Policies should cover legacy authentication blocking, device compliance, location-based restrictions, and high-risk sign-in response.

> **Common mistake:** Assuming existing policies are sufficient because they were "best practice at the time." Microsoft ships new Conditional Access features quarterly. Your 2021 policy set does not cover 2026 threats.

2

Conditional Access Naming Convention

CRITICAL 2-4 HOURS (SINGLE WORKSHOP) *Governance*

Establish a consistent naming convention for Conditional Access policies before you have 50 of them. A clear convention (e.g., [Priority]-[Target]-[Action]-[Exception]) makes policy review, troubleshooting, and auditing dramatically easier.

> **Common mistake:** Creating policies with descriptive names like "Block legacy auth" and "MFA for admins" that become impossible to manage when you have 30+ policies with overlapping scopes.

3

MFA Coverage Gap Analysis

CRITICAL 1-2 WEEKS (DEPENDS ON SCOPE) *Security*

Map which users and applications have MFA enforced versus which do not. Entra ID reports this in the Per-User MFA status blade. Most organizations discover 10-20% of privileged accounts are not MFA-enforced due to legacy service accounts or emergency bypass policies that were never removed.

> **Common mistake:** Enforcing MFA for all users without exception policies for service accounts, causing authentication failures in automated workflows.

4

Legacy Authentication Blocking

CRITICAL 2-4 HOURS (SINGLE WORKSHOP) *Security*

Legacy authentication protocols (IMAP, POP3, SMTP AUTH, older Office protocols) bypass Conditional Access entirely. Entra ID can block these protocols via Conditional Access, but most tenants have not enabled this control.

> **Common mistake:** Leaving legacy authentication enabled because "some old app might need it," without testing whether any application in the environment actually does.

5

Entra Connect to Cloud Sync Migration

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Operations*

If your organization is still running Entra Connect (formerly Azure AD Connect) for hybrid identity synchronization, migrate to Entra Cloud Sync. Cloud Sync is Microsoft's recommended path forward, with simpler configuration, agent-based architecture, and no sync server to maintain.

> **Common mistake:** Staying on Entra Connect because "it works," missing the security patches, feature improvements, and operational simplification that Cloud Sync provides.

6

Sign-in Risk Policy Activation

STANDARD 2-4 HOURS (SINGLE WORKSHOP) *Security*

Entra ID Protection can detect risky sign-ins (impossible travel, unfamiliar locations, leaked credentials) and force password resets or MFA challenges. Most organizations have this feature available in their license tier but have not activated the sign-in risk policies.

> **Common mistake:** Having Entra ID Protection licensed but not configured, paying for threat detection that never fires.

02

These five decisions activate the governance features that most organizations are paying for but not using. Entra ID Governance is included in Entra ID P2 licenses, but the features must be configured to deliver value. If you are on Entra ID P1, items 7-11 require a license upgrade.

7

Access Reviews (Access Certifications)

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Entra ID Governance includes automated access reviews that certify whether users still need access to applications and groups. Organizations without active reviews accumulate stale access at a rate of 3-5% per quarter. After one year, 12-20% of access grants are no longer justified.

> **Common mistake:** Having access review licenses but no active campaigns, leaving stale access unchallenged for years.

8

Privileged Identity Management (PIM) Activation

CRITICAL 1-2 WEEKS (DEPENDS ON SCOPE) *Security*

PIM provides just-in-time access to privileged roles, replacing standing admin access with time-limited, approval-gated elevation. A typical enterprise has 10-20 Global Admins with standing access. PIM eliminates that standing privilege, reducing your attack surface by orders of magnitude.

> **Common mistake:** Activating PIM for a few roles but leaving Global Admin permanent because "it is easier," defeating the purpose of just-in-time privileged access.

9

Lifecycle Workflows

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Entra ID Governance includes lifecycle workflows that automate joiner, mover, and leaver events based on HR system signals. Most organizations handle these manually or through scripts.

> **Common mistake:** Building custom PowerShell scripts for onboarding when Entra lifecycle workflows can automate the same process with built-in audit trails.

10

Entitlement Management (Access Packages)

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Access packages bundle application access, group membership, and role assignments into self-service requestable packages. Instead of manually provisioning access, users request a package and the access is automatically provisioned and time-bound.

> **Common mistake:** Creating access packages for every application individually instead of grouping access by role or function, producing package sprawl that nobody manages.

11

Tenant Restrictions and Collaboration Controls

STANDARD 2-4 HOURS (SINGLE WORKSHOP) *Security*

If your organization collaborates with external partners, Entra ID B2B collaboration and tenant restrictions control what external users can access and from where. Most organizations have B2B enabled but have not configured tenant restrictions, allowing external users to access resources from any device or location.

Common mistake: Enabling B2B collaboration without device compliance requirements, letting partner users access your resources from unmanaged devices.

03

These four decisions move your Entra deployment from baseline security to advanced posture. They require the Entra ID P2 license and deliberate configuration.

12

Continuous Access Evaluation (CAE)

STANDARD 2-4 HOURS (SINGLE WORKSHOP) *Security*

CAE forces real-time token revocation when risk signals change, instead of waiting for the token to expire (up to 1 hour). Most organizations have CAE available but have not enabled it for all applications. Without CAE, a compromised token remains valid for up to 60 minutes after the risk signal fires.

Common mistake: Enabling CAE for only Microsoft applications and not third-party SaaS apps, leaving a window where compromised tokens remain valid after risk changes.

13

Workload Identity Configuration

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Entra Workload ID governs service principals, managed identities, and app registrations (requires Entra Workload ID license). Most organizations have hundreds of workload identities with no governance, no access reviews, and no lifecycle management.

Common mistake: Focusing exclusively on human identity governance while ignoring workload identities, which often have higher privilege and weaker controls.

14

Identity Protection Tuning

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Security*

Entra ID Protection uses machine learning to detect compromised accounts, risky users, and risky sign-ins. The default policies are conservative. GCA tunes detection thresholds, configures automated remediation (force password reset, block access), and integrates alerts with SIEM.

> **Common mistake:** Accepting default Identity Protection policies without tuning, producing either too many false positives (alert fatigue) or too few detections (false security).

These 14 decisions are Entra-specific in execution. When GCA is involved, here is how we approach them differently.

We audit your existing Entra configuration before recommending changes. Most Entra optimization engagements start with a gap analysis that maps your current policies, features, and license utilization against Microsoft's best practices and your compliance requirements. GCA is rated 4.8 / 5.0 on Gartner Peer Insights based on 32 verified reviews. GCA also uses Microsoft's own Identity Secure Score to baseline your current posture before recommending changes. See our full Microsoft Entra partner page for the broader Entra practice.

DOWNLOAD ENTRA CHECKLIST (PDF)

ENTRA PARTNER PAGE

BOOK A CONSULTATION

Need help with your Microsoft Entra Optimization Checklist?

GCA Technology Services — gca.net — Book a consultation: gca.net/book-a-consultation

MANAGING YOUR DIGITAL IDENTITIES

SERVICES

Managed IAM

Implementation

Assessment & Strategy

General IAM

SOLUTIONS

Identity Management

Web Access Management

Identity Governance

Privileged Access

PARTNERS

SailPoint

Microsoft Entra

Okta

OpenText

Netwrix

Ping Identity

COMPANY

About GCA

Careers

Contact Us

Privacy Policy

MANAGING **YOUR** DIGITAL IDENTITIES