Microsoft 365 + Entra ID + Azure Hardening Checklist

917SOLUTIONS
DELIVERING THE FUTURE

Most Microsoft 365 environments aren't badly configured — they're just unfinished.

Tenants evolve.
Admins change.
Defaults linger longer than they should.

What starts as "good enough" slowly becomes risky — not because anyone did something wrong, but because no one ever stopped to audit what quietly accumulated over time.

This checklist exists for one reason: **To help you see what actually matters before something goes wrong.**

What This Checklist Is
This is a practical, field-tested starting point for auditing and hardening Microsoft 365, Entra ID, and Azure, based on what we consistently see when reviewing real-world tenants.

It focuses on:
- Identity and access controls that quietly expand risk
- MFA configurations that look enabled but aren't effective
- Legacy paths and permissions that rarely get revisited
- Azure and Entra settings that extend blast radius when left unchecked

Every item here is included because we've seen what happens when it isn't.

What This Checklist Is Not
- Not a scare tactic
- Not a "turn everything on" guide
- Not theoretical best practices pulled from documentation

Security isn't about enabling every toggle. It's about enabling the right controls, in the right order, for the right reasons.

Use this checklist to:
- Audit your current posture
- Validate assumptions
- Identify gaps that deserve attention now versus later

The goal isn't perfection. The goal is clarity.

Stay proactive — these small steps **make a big impact**.

For full configuration guides or Microsoft 365 support, contact Gerty at gerty@917solutions.com

Entra ID + Microsoft 365 + Azure Auditing Checklist

1 Entra ID > Overview	
1.1 Document Secure Score for Identity	
1.2 Document Microsoft Secure Score	
1.3 Document Total # of Global Adminstrators	
1.4 Document Total # of Users	
1.5 Document Total # of Groups	
1.6 Document Total # of Apps	
1.7 Document Total # of Devices	

2 Entra ID > Overview > Properties	
2.1 'Microsoft 365 audit log search' is 'Enabled'	
2.2 'Technical contact’ is 'Updated'	
2.3 'Access Management for Azure Resources’ is enabled	
2.4 'Security Defaults’ is disabled	

3 Entra ID > Users > Per-User MFA	
3.1 'Per-User MFA' is 'Disabled'	
3.2 'Authentication Methods are Migrated	

4 Entra ID > Users > User Settings	
4.1 'Users Can Register Applications' Is Set to 'No'	
4.2 'Restrict non-admin users from creating tenants' is set to 'Yes'	
4.3 'Users Can Create Security Groups' Is Set to 'No'	
4.4 'Guest user access' is set to "Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)"	
4.5 'Restrict access to Microsoft Entra admin center' is Set to 'Yes'	
4.6 'Allow users to connect their work or school account with LinkedIn' is is set to 'No'	
4.7 'Show keep user signed in' is set to 'No'	

5 Entra ID > Users > User Settings > External Collaboration	
5.1 Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)'	
5.2 'Guest invite restrictions' is set to "Only users assigned to specific admin roles can invite guest users"	
5.3 'Allow external users to remove themselves from your organization (recommended) is set to 'Yes'	

6 Entra ID > Users > User Settings > User Features	
6.1 'Users can use preview features for My Apps' set to None	
6.2 'Administrators can access My Staff' set to None	
7 Entra ID > Users > Password reset	
7.1 'Self service password reset enabled' is set to 'All'	
7.2 'Number of days before users are asked to re-confirm their authentication information' is not set to '0'	
7.3 'Notify users on password resets?' is set to 'Yes'	
7.4 'Notify all admins when other admins reset their password?' is set to 'Yes'	
7.5 'Customize helpdesk link' is set to 'Yes'	
8 Entra ID > Groups > General	
8.1 'Owners can manage group membership requests in My Groups' is set to 'No'	
8.2 'Restrict user ability to access groups features in My Groups. Group and User Admin will have read-only access when the value of this setting is 'Yes''	
8.3 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No'	
8.4 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No'	

9 Entra ID > Groups> Expiration	
9.1 'Adjust group lifetime to 180 days'	

10 Entra ID > Protection > Authentication Methods	
10.1 Policies > Microsoft Authenticator > 'Ensure Microsoft Authenticator is configured to protect against MFA fatigue'	
10.2 Policies > 'Ensure weak authentication methods are disabled'	
10.3 Password Protection > 'Lockout threshold' is less than or equal to '10'	
10.4 Password Protection > 'Lockout duration in seconds' is greater than or equal to '60'	
10.5 Password Protection > 'Enforce custom banned password list '	
10.6 Password Protection > 'Ensure password protection is enabled for on-prem Active Directory'	
10.7 Registration Campaign > Is Configured	
10.8 Settings > 'System-preferred multifactor authentication' is 'enabled'	
10.9 User registration details > Ensure all member users are 'MFA capable'	

11 Entra ID > Enterprise Applications > Consent and Permissions	
11.1 'User consent for applications' is set to 'Do not allow user consent'	
11.2 'Admin consent requests' set to 'Yes'	
12 Azure > Subscriptions > Advanced Options	
12.1 'Subscription leaving Microsoft Entra ID directory' and 'Subscription entering Microsoft Entra ID directory' Is Set To 'Permit No One'	
12.2 'Use of the 'User Access Administrator' role is restricted	
12.3 'No custom subscription administrator roles exist	
13 Microsoft 365 admin center > Users > Role Assignments	
13.1 Ensure Administrative accounts are cloud-only	
13.2 Ensure two emergency access accounts have been defined	
13.3 Ensure that between two and four global admins are designated	
13.4 Ensure administrative accounts use licenses with a reduced application footprint	

14 Microsoft 365 admin center > Settings > Org Settings > Services	
14.1 Calendar > 'External sharing' of calendars is 'unchecked'	
14.3 Cortana > 'Allow Cortana' is 'unchecked'	
14.4 Microsoft 365 Groups > 'Let guest group members access group content' is 'unchecked'	
14.5 Microsoft 365 Installation Options > Feature Updates > 'As soon as they're ready (Current channel, recommended)' is 'checked'	
14.6 Microsoft 365 Installation Options > Installation > 'Skype for Business' is 'unchecked' for Windows and MacOS	
14.7 Microsoft 365 on the Web > 'Let users open files stored in third-party storage services in Microsoft 365 on the web' is 'unchecked'	
14.8 Forms > 'Add internal phishing protection' is 'checked'	
14.9 Microsoft Loop > 'Microsoft Loop workspaces are available to all users in my organization' is 'unchecked'	
14.10 Microsoft Planner > 'Allow iCalendar publishing' is 'unchecked'	
14.11 Modern Authentication > 'Authenticated SMTP' is 'unchecked'	
14.12 Office Scripts > Review the configured settings and disable / revoke	
14.13 Reports > 'Display concealed user, group, and site names in all reports' and 'Make report data available to M365 usage analytics for PowerBI' are unchecked	
14.14 Self-service trials and purchases > Review all applications that allow a trial and disable non-approved applications	
14.15 Sway >'Let people in your organization share their sways with people outside their organization' and 'Let people in your organization look up people and security groups' is unchecked	
14.16 User owned apps and services >'Office Store access' is unchecked	
14.17 User owned apps and services > ‘Starting trials on behalf of your organization’ is restricted	
14.18 User owned apps and services > ‘Auto-claim licenses’ is restricted	

Entra ID + Microsoft 365 + Azure Auditing Checklist

15 Microsoft 365 admin center > Settings > Org Settings > Security & Privacy	
15.1 Customer lockbox > 'Require approval for all data access requests' is 'checked' (REQUIRES E5)	
15.2 Password expiration policy > 'Password expiration policy' is set to 'Set passwords to never expire (recommended)'	
15.3 Idle session timeout > 'Password expiration policy' is set to '3 hours (or less)' for unmanaged devices	
16 Microsoft 365 admin center > Settings > Org Settings > Organization Profile	
16.1 Custom theme for Organization' is 'set	
16.2 Help desk information' is set	
16.3 Organization information' is set	
16.4 Release preferences' is set	
17 Microsoft 365 admin center > Settings > Domains	
17.1 Audit DNS health' for Domains	
17.2 Audit and Configure SPF	
17.3 Audit and Configure DKIM	
17.4 Audit and Configure DMARC	
17.5 Audit and Configure DNSSEC	
17.6 Audit and Configure Intune CNAME record	
18 Microsoft 365 admin center > Settings > Partner relationships	
18.1 Audit Partner relationships' for 'GDAP Privileges'	

Want the Full Version?
This PDF is part of our Microsoft 365 Hardening Series — a practical, ongoing effort to help teams secure Microsoft 365 intentionally, not reactively.

Newsletter subscribers receive:

- The full Excel-based hardening checklist
- Future checklists as new risk areas and configurations are released
- Invitations to hands-on webinars and walkthroughs focused on real implementation, not theory

This PDF is designed to give you clarity. Click here to subscribe to the Newsletter.

The full series is designed to help you act on it.

If you're responsible for the security of a Microsoft 365 environment and want a clear, repeatable way to audit, validate, and improve it over time — that's where the full series lives.

Where This Fits in the Hardening Series
This checklist represents Step 2 of our Microsoft 365 Hardening Series.

Each step in the series is intentionally sequenced. We focus on one area at a time so hardening efforts are measured, auditable, and sustainable — not rushed or reactive.

The Full Hardening Series Covers (Many More Areas to Cover)

1 Create Security Groups
2 Entra ID Tenant and Microsoft 365 Tuning (this checklist)
3 Audit Users / Mailboxes / Service Accounts
4 Exchange Mailflow Rules
5 MFA Audit + Baselining
6 Conditional Access Policies + Reporting
7 Organization Customization
8 Defender for Office 365
9 Intune Deployment & Configuration
10 Microsoft Defender for Endpoint
11 SharePoint + Microsoft Teams Review
12 Microsoft Purview Basics
13 Co-Pilot Enablement