



The M365 Baseline Checklist

12 Configurations That Separate Healthy Environments from Struggling Ones

This isn't about getting ready for something—it's about knowing whether your M365 environment is operationally sound **right now**.

These 12 items represent the baseline every organization should maintain. They're not theoretical best practices; they're the configurations that consistently predict whether environments run smoothly or generate constant friction.

Time to complete: 15-20 minutes

Recommended frequency: Quarterly

✓ Your Current State

Security Foundations

Is your identity and access layer protecting users without creating friction?

- ☐ **Are 95%+ of sign-ins protected by multi-factor authentication?**

Why it matters: Compromised accounts are expensive and erode user trust

- ☐ **Have you blocked legacy authentication protocols?**

Why it matters: Legacy protocols bypass modern security controls

- ☐ **Can users reset their own passwords?**

Why it matters: Password resets shouldn't require helpdesk intervention

User Provisioning

Are access rights managed systematically or manually?

- ☐ **Are licenses assigned through groups instead of individually?**

Why it matters: Manual licensing creates delays and inconsistencies as you scale

Device Health

Do you have visibility and control over endpoint compliance?

- ☐ **Do you have compliance policies enforcing basic security standards?**

Why it matters: Inconsistent device states create unpredictable behavior and security gaps

- ☐ **Are Windows updates managed through rings or Autopatch?**

Why it matters: Unmanaged updates create support spikes and compatibility issues

Email Protection

Is your first line of defense configured?

- ☐ **Are Safe Links and Safe Attachments enabled for all users?**

Why it matters: Email remains the primary attack vector; basic protection should be non-negotiable

Data Access & Collaboration

Can users work from anywhere while data remains protected?

- ☐ **Are Desktop, Documents, and Pictures folders redirected to OneDrive?**

Why it matters: Local-only files create recovery nightmares and limit mobility

- ☐ **Do you have SharePoint external sharing rules defined?**

Why it matters: Undefined sharing policies lead to either over-restriction or over-exposure

- ☐ **Are sensitivity labels deployed and in use?**

Why it matters: Users need clear, visible guidance on data classification

Operational Visibility

Do you know what's working and what isn't?

- ☐ **Is someone reviewing Adoption Score or usage analytics monthly?**

Why it matters: You can't improve what you don't measure

- ☐ **Are M365 workloads backed up by a third-party solution?**

Why it matters: Microsoft's retention policies are not backups; recovery scenarios prove this

Understanding Your Score

10-12 Checked: Strong operational foundation. You're ahead of most organizations.

7-9 Checked: Solid core with gaps. Common for organizations that grew quickly or inherited environments.

4-6 Checked: Operational debt is building. These gaps are costing you in support time and user friction.

0-3 Checked: Significant operational risk. Your environment is likely generating preventable issues daily.

The Hidden Cost of Missing Baselines

These aren't just technical checkboxes—they're the difference between IT teams that enable vs. IT teams that firefight.

What Gaps Cost You:

Missing Baseline	What IT Experiences	What Users Experience
No MFA enforcement	Account takeover incidents	"Someone hacked my email"
Manual licensing	Hours spent on each new hire	"I still don't have access on day 3"
Unmanaged updates	Surprise support spikes	"My laptop broke overnight"
Files on local drives	Data recovery emergencies	"I lost everything when my drive died"
No sharing guardrails	Security incident investigations	"I can't share with our contractor"
No usage monitoring	Training budget spent blindly	Features sit unused

What Baselines Enable:

Baseline in Place	What IT Experiences	What Users Experience
MFA + SSPR	Minimal password support	Self-sufficient access management
Group-based licensing	Automated provisioning	Day 1 productivity
Managed updates	Predictable change windows	Stable, reliable devices
OneDrive KFM	No data recovery fires	Work from anywhere seamlessly
SharePoint guardrails	Confident collaboration	Appropriate sharing without tickets
Adoption monitoring	Targeted improvement	Features that actually help

When to Check Your Baseline

This isn't a one-time assessment. Environments drift, teams grow, and priorities shift.

Run this checklist:

- **Quarterly** as operational hygiene
- **After leadership changes** (new IT leaders should know current state)
- **Before major initiatives** (mergers, significant growth, new workload rollouts)
- **When support trends change** (unexplained ticket volume increases)

Think of this as your M365 "vital signs" check.

Why These 12?

Over hundreds of M365 environments, these 12 configurations consistently separate smooth operations from constant friction.

They're not exhaustive, they're foundational. The items that should be solid before anything else makes sense.

This is the floor, not the ceiling. If these aren't in place, advanced features and new workloads will underperform regardless of how well you implement them.

What's Next?

You now know your current operational state.

If you have gaps and need guidance on remediation priorities, timelines, or how to build this into your operational rhythm, let's talk.

This baseline helps you understand *what* needs attention. The next step is understanding *how* to close gaps efficiently while keeping the business running.

Run this quarterly. Share it with your team. Use it to validate vendor promises. This is what operationally sound M365 environments look like.

Alex@ModernWorkMindset.com