# Microsoft 365 Adoption Baseline: *The 30-Minute Readiness Assessment for Secure, Successful Rollouts*

## Executive Summary

### The Challenge

Organizations investing in Microsoft 365, particularly AI capabilities like Copilot, face a critical gap: technical readiness does not equal adoption readiness. Without foundational configurations in place, rollouts generate user friction, security incidents, and helpdesk overload that undermine ROI and user confidence.

**The cost of poor preparation:**

- 30-40% of enablement budgets wasted on avoidable support issues
- User adoption stalls at 20-35% in the first 90 days
- Security incidents during rollouts erode trust and delay value realization
- IT teams spend 60% or more of their time firefighting instead of enabling

### The Solution: A 30-Minute Adoption Baseline

This assessment validates 12 high-impact configurations across security, provisioning, device management, and data protection. These are the foundations required for successful M365 and Copilot adoption.

**Delivered outcomes:**

- Reduce helpdesk volume by 40% during rollout windows
- Accelerate time-to-value: users productive on day 1, not day 30
- Lower security risk while enabling confident collaboration
- Make training stick by removing technical barriers

## 12 Checks, 4 Critical Domains

| Domain | Checks | Business Impact |
|---|---|---|
| Security & Identity | MFA enforcement, Legacy auth blocked, Self-service password reset | Prevents account takeovers and lockouts that destroy user trust during critical rollout phases |
| Provisioning & Access | Group-based licensing | New hires productive immediately with no delays waiting for IT to manually assign licenses |
| Device Health | Compliance policies, Update management | Stable devices mean fewer "it's broken" complaints and predictable change windows prevent chaos |
| Data & Collaboration | OneDrive folder redirection, SharePoint guardrails, Sensitivity labels, Email security, Backup validation | Files follow users, AI features work, collaboration is fast and safe, data is recoverable |
| Continuous Improvement | Adoption Score monitoring | Target training where it matters and stop wasting budget on blanket sessions |

## Why This Matters for Copilot Deployments

Without these baselines, Copilot becomes a $30+ per user/per month frustration:

- Files on local desktops? Copilot can't see them. Users wonder what they paid for.
- No sensitivity labels? Users fear AI will leak confidential data, so they don't use it.
- Devices out of compliance? Features fail unpredictably, generating support tickets.
- No backup validation? One accidental deletion or ransomware incident creates rollback demands and lost work.

With these baselines in place:

- Users experience "it just works" from day 1
- Helpdesk can focus on enablement, not firefighting
- Training delivers measurable behavior change
- Leadership sees adoption metrics improve within 60 days

## Investment Required

| Resource | Time Investment | Expected Outcome |
|---|---|---|
| IT Leadership | 30 min initial review, 30 min monthly follow-up | Identify gaps, prioritize fixes, track improvement |
| Technical Team | 2-4 weeks to remediate gaps (varies by current state) | Foundation for successful rollout and reduced support load |
| Budget Impact | Minimal (mostly configuration of existing licenses; backup may require third-party tool) | Avoid six-figure support costs and failed adoption |

**ROI Timeline:**

- Week 1: Critical security gaps closed
- Week 4: Provisioning and device health stable
- Day 1 of rollout: User friction reduced 40-60%
- 90 days post-rollout: Measurable adoption improvement, support tickets trending down

## What Success Looks Like

**Before Baseline:**

- "Why isn't Copilot finding my files?"
- "I got locked out again during the training session"
- "Our team can't collaborate because sharing is blocked"
- 300+ helpdesk tickets per 1,000 users in rollout month

**After Baseline:**

- Users experience seamless access and collaboration
- Security is invisible to users but visible to leadership
- Helpdesk tickets drop 40% compared to previous rollouts
- Adoption Score shows 10-15 point improvement in 60 days
- Training budget drives behavior change, not break/fix

## Questions for Leadership

1. When is the planned rollout for Copilot or next major M365 feature?
2. Have we validated these 12 configurations, or are we assuming they're in place?
3. What's the cost if 30% of users can't access new features on day 1?
4. Who owns ensuring readiness and do they have the authority to make changes?

## How to Use This Assessment

**Time required:** 30 minutes for initial review

**Process:**

1. Gather your team (IT Leadership, Security representative, someone with backup system access)
2. Work through each check with the specified role
3. Mark each as Pass or Needs Action
4. Prioritize remediation: Security first (week 1), then provisioning (weeks 2-3), then device and data foundations (weeks 3-4)
5. Track progress monthly and re-run quarterly or before major rollouts

**Interpreting results:**

- 8+ Pass: Solid foundation, focus on gaps
- 4-7 Pass: Common for growing organizations, prioritize security and provisioning first
- 0-3 Pass: High risk for rollout failure, consider external help to accelerate remediation

# The 12 Critical Checks

## Check 1: MFA via Conditional Access (Tenant-Wide)

**Required Role:** Global Reader or Security Reader

**Where to Check:** Entra Admin Center > Entra ID > Protection > Conditional Access > Policies

**Pass Criteria:**

- Policy requires MFA for All users and All cloud apps
- Break-glass accounts properly excluded and documented
- Admin sign-ins use strong authentication (Authenticator or FIDO2)
- Policy is enabled (not report-only)

**Success Metrics:**

- 98% or more interactive sign-ins protected by MFA
- 100% admin sign-ins using strong auth
- Zero account takeover incidents during rollout period

**Status:** ___ Pass ___ Needs Action

**Notes:** ____________________________________________________

## Check 2: Block Legacy Authentication

**Required Role:** Security Reader or Reports Reader

**Where to Check:**

- Entra > Sign-in logs (filter: Client app = Legacy)
- Microsoft 365 Admin > Settings > Org Settings > Modern Authentication

**Pass Criteria:**

- Zero legacy sign-ins in last 7 days
- Modern authentication enforced organization-wide

- No service accounts or applications using basic auth

**Success Metrics:**

- 0% legacy sign-ins
- 95% or more Outlook clients using modern auth
- Reduction in authentication-related helpdesk tickets

**Status:** ___ Pass ___ Needs Action

**Notes:** ____________________________________________________________

### Check 3: Self-Service Password Reset and Combined Registration

**Required Role:** Global Reader or Security Reader

**Where to Check:**

- Entra > Protection > Password Reset
- Entra > Protection > Authentication Methods > Registration

**Pass Criteria:**

- SSPR enabled for all users (not just pilot groups)
- Combined registration enabled
- Multiple strong methods available (Authenticator app, phone, email)
- Users prompted to register on next sign-in if not already registered

**Success Metrics:**

- 80% or more users registered with 2+ strong methods
- Password reset tickets reduced by 40%
- Average time-to-resolution for lockouts under 5 minutes

**Status:** ___ Pass ___ Needs Action

**Notes:** ____________________________________________________________

## Check 4: Group-Based Licensing for New Users

**Required Role:** Global Reader or License Administrator

**Where to Check:**

- Entra > Groups > Licenses
- Users > Licenses (spot check recent hires)

**Pass Criteria:**

- New users receive licenses via security or dynamic groups
- Groups organized by role or department
- 10% or fewer direct license assignments (emergency cases only)
- Documentation exists for group-to-license mapping

**Success Metrics:**

- 90% or more users licensed via groups
- New-hire time-to-ready under 4 hours
- Zero "I don't have access" tickets on day 1 for new hires

**Status:** ___ Pass ___ Needs Action

**Notes:** ____________________________________________________________

## Check 5: Device Compliance Baseline (Intune)

**Required Role:** Intune Read Only Operator or Endpoint Security Reader

**Where to Check:**

- Intune Admin > Devices > Compliance Policies
- Reports > Device Compliance

**Pass Criteria:**

- At least one compliance policy assigned to user or device groups
- Policy includes OS version, encryption, password requirements

- Compliance reporting is active and reviewed regularly
- Non-compliant devices have clear remediation path

**Success Metrics:**

- 85% or more devices compliant
- Build-related incidents reduced 25% month-over-month
- Conditional Access policies can enforce device compliance

**Status:** ___ Pass ___ Needs Action

**Notes:** ______________________________________________________________

## Check 6: Windows Update Rings or Autopatch

**Required Role:** Intune Read Only Operator

**Where to Check:**

- Intune > Windows > Update Rings (Pilot and Broad)
- OR: Tenant Administration > Windows Autopatch

**Pass Criteria:**

- Pilot and Broad rings configured and assigned to device groups
- OR: Windows Autopatch enabled and reporting healthy
- Clear escalation path from Pilot to Broad with minimum 7-day soak time
- Update compliance tracked and reported

**Success Metrics:**

- 90% or more devices on target build within 14 days of release
- No unplanned "surprise update" incidents during rollout windows
- Predictable monthly patching cadence

**Status:** ___ Pass ___ Needs Action

**Notes:** ______________________________________________________________

## Check 7: Safe Links and Safe Attachments (Preset Policies)

**Required Role:** Security Reader

**Where to Check:** security.microsoft.com > Email and Collaboration > Policies and Rules > Threat Policies > Preset Security Policies

**Pass Criteria:**

- Standard preset policy applied tenant-wide
- Strict preset assigned to pilot or high-risk groups (optional but recommended)
- Safe Links URL rewriting enabled with click tracking on
- Safe Attachments dynamic delivery enabled for unknown attachments

**Success Metrics:**

- 95% or more mailboxes covered by Safe Links and Safe Attachments
- Phishing or mail-security tickets reduced 30% quarter-over-quarter
- User-reported phishing incidents trending down

**Status:** ___ Pass ___ Needs Action

**Notes:** ______________________________________________________

## Check 8: OneDrive Known Folder Move

**Required Role:** Intune Read Only Operator or Global Reader with OneDrive admin access

**Where to Check:**

- Intune > Devices > Configuration Profiles (Windows Settings Catalog > OneDrive ADMX)
- OneDrive Admin Center > Reports > OneDrive usage

**Pass Criteria:**

- Desktop, Documents, Pictures redirected to OneDrive for target users

- Policy deployed via Intune (not manual user setup)
- Sync health visible in reports
- Users notified before KFM enabled (change management)

**Success Metrics:**

- 80% or more target users with KFM enabled
- Sync error rate under 2% weekly
- Reduced "I lost my files" helpdesk tickets
- Improved Copilot usage (files accessible to AI)

**Status:** ___ Pass ___ Needs Action

**Notes:** ____________________________________________________________

## Check 9: SharePoint External Sharing Guardrails and Site Templates

**Required Role:** Global Reader (org sharing) or SharePoint Administrator (site-level)

**Where to Check:**

- SharePoint Admin > Policies > Sharing (organization level)
- Active Sites > select site > Policies > Sharing (site level)

**Pass Criteria:**

- Organization sharing posture defined (e.g., "New and existing guests" or "Existing guests only")
- Sharing settings consistent across sites or intentionally varied by sensitivity
- Approved site templates exist for Department sites, Project sites, External collaboration
- Site creation workflow includes security and classification decision

**Success Metrics:**

- Project site creation time under 1 day
- External sharing violations reduced 25%
- Users can self-service site creation without IT bottleneck

- Zero "accidentally shared with everyone" incidents

**Status:** ___ Pass ___ Needs Action

**Notes:** ____________________________________________________________

## Check 10: Sensitivity Labels

**Required Role:** Compliance Data Administrator or Global Reader with Purview access

**Where to Check:** Microsoft Purview > Solutions > Information Protection > Sensitivity Labels > Label Policies

**Pass Criteria:**

- 3-5 labels published to target groups (e.g., Public, Internal, Confidential, Restricted)
- Default label recommendation configured (e.g., "Internal" as default)
- Labels applied to files, emails, Teams, SharePoint sites
- Auto-labeling rules configured for known sensitive content (optional but recommended)

**Success Metrics:**

- 60% or more of new content labeled in pilot groups
- Accidental external shares of confidential content reduced 20%
- Users understand label meanings without calling IT
- Copilot respects label-based permissions

**Status:** ___ Pass ___ Needs Action

**Notes:** ____________________________________________________________

## Check 11: Adoption Score and Usage Reviews

**Required Role:** Reports Reader or Global Reader

**Where to Check:**

- Microsoft 365 Admin > Reports > Adoption Score
- Usage reports for Teams, SharePoint, OneDrive, Outlook

**Pass Criteria:**

- Named owner assigned to monitor Adoption Score monthly
- Monthly or bi-weekly review cadence established with stakeholders
- Two focus areas identified with active improvement plans
- Metrics tracked over time (baseline, target, actual)

**Success Metrics:**

- 10 point or more increase in chosen Adoption Score categories over 60 days
- Targeted feature usage increase measurable
- Training adjusted based on data, not assumptions
- Leadership receives quarterly adoption report

**Status:** ___ Pass ___ Needs Action

**Notes:** ____________________________________________________________

## Check 12: Validate Third-Party M365 Backups

**Required Role:** View-only access to backup provider portal (no M365 role required)

**Where to Check:** Backup provider portal or reports (coverage, last backup, retention, restore tests)

Examples: Veeam Backup for Microsoft 365, AvePoint Cloud Backup, Barracuda Cloud-to-Cloud Backup

**Pass Criteria:**

- 95% or more mailboxes, OneDrive, SharePoint sites, and Teams protected
- Auto-protect enabled for new users and sites
- Last backup completed within 24 hours
- Retention policy meets organizational or regulatory requirements
- Last quarterly restore test passed with documented results

**Success Metrics:**

- Coverage percentage by workload tracked and reported monthly
- Backup age consistently under 24 hours
- Job success rate 98% or higher weekly
- Restore tests pass with RPO and RTO requirements met
- Zero data-loss incidents escalated to leadership

**Status:** ___ Pass ___ Needs Action

**Notes:** ____________________________________________________

# Assessment Summary and Action Plan

## Results Summary

| Check | Status | Priority | Owner | Target Date |
|---|---|---|---|---|
| 1. MFA via Conditional Access | | | | |
| 2. Block Legacy Authentication | | | | |
| 3. SSPR and Combined Registration | | | | |
| 4. Group-Based Licensing | | | | |
| 5. Device Compliance Baseline | | | | |
| 6. Windows Update Rings or Autopatch | | | | |
| 7. Safe Links and Safe Attachments | | | | |
| 8. OneDrive Known Folder Move | | | | |
| 9. SharePoint Sharing Guardrails | | | | |
| 10. Sensitivity Labels | | | | |
| 11. Adoption Score and Usage Reviews | | | | |
| 12. Third-Party M365 Backups | | | | |

**Total Pass:** _____ / 12

**Total Needs Action:** _____ / 12

## Recommended Remediation Timeline

**Week 1 (Critical Security)**

- Check 1: MFA via Conditional Access
- Check 2: Block Legacy Authentication
- Check 7: Safe Links and Safe Attachments

**Weeks 2-3 (User Access and Provisioning)**

- Check 3: SSPR and Combined Registration
- Check 4: Group-Based Licensing

**Weeks 3-4 (Device and Data Foundations)**

- Check 5: Device Compliance Baseline
- Check 6: Windows Update Rings or Autopatch
- Check 8: OneDrive Known Folder Move
- Check 9: SharePoint Sharing Guardrails
- Check 10: Sensitivity Labels
- Check 12: Third-Party M365 Backups

**Ongoing (Continuous Improvement)**

- Check 11: Adoption Score and Usage Reviews (monthly cadence)
- Re-run this assessment quarterly or before major rollouts

## Next Steps

**For IT Leadership:**

1. Schedule 60-minute review meeting with Security and Compliance leads
2. Identify "Needs Action" items and assign owners
3. Communicate timeline and expectations to stakeholders
4. Add monthly Adoption Score review to calendar

**For Technical Teams:**

1. Document current state for each "Needs Action" item
2. Estimate effort required for remediation
3. Identify dependencies or blockers
4. Create project plan with milestones
5. Schedule pilot testing before broad rollout

# Additional Resources

## Microsoft Documentation

### Identity and Security

- Conditional Access templates: https://aka.ms/CAtemplates
- Plan Conditional Access deployment: https://learn.microsoft.com/entra/identity/conditional-access/plan-conditional-access
- SSPR deployment guide: https://learn.microsoft.com/entra/identity/authentication/howto-sspr-deployment

### Device Management

- Intune device compliance: https://aka.ms/IntuneCompliance
- Windows Autopatch documentation: https://learn.microsoft.com/windows/deployment/windows-autopatch/

### Security and Compliance

- Microsoft Defender for Office 365: https://learn.microsoft.com/defender-office-365/
- Sensitivity labels: https://learn.microsoft.com/purview/sensitivity-labels
- Data Loss Prevention: https://learn.microsoft.com/purview/dlp-learn-about-dlp

### Adoption and Change Management

- Microsoft Adoption Hub: https://adoption.microsoft.com
- Copilot adoption resources: https://aka.ms/CopilotAdoption
- Microsoft 365 Adoption Score: https://learn.microsoft.com/microsoft-365/admin/adoption/adoption-score

## Assessment Frequency Recommendations

| Scenario | Frequency |
|---|---|
| Stable environment | Quarterly |
| Before major rollout (Copilot, E5, etc.) | 4-6 weeks in advance |
| After merger or tenant migration | Within 30 days |
| New IT leadership | First 30 days (baseline) |
| Unexpected helpdesk spike | Immediate |

*This document is provided for informational purposes. Organizations are encouraged to use and adapt it for their specific needs.*