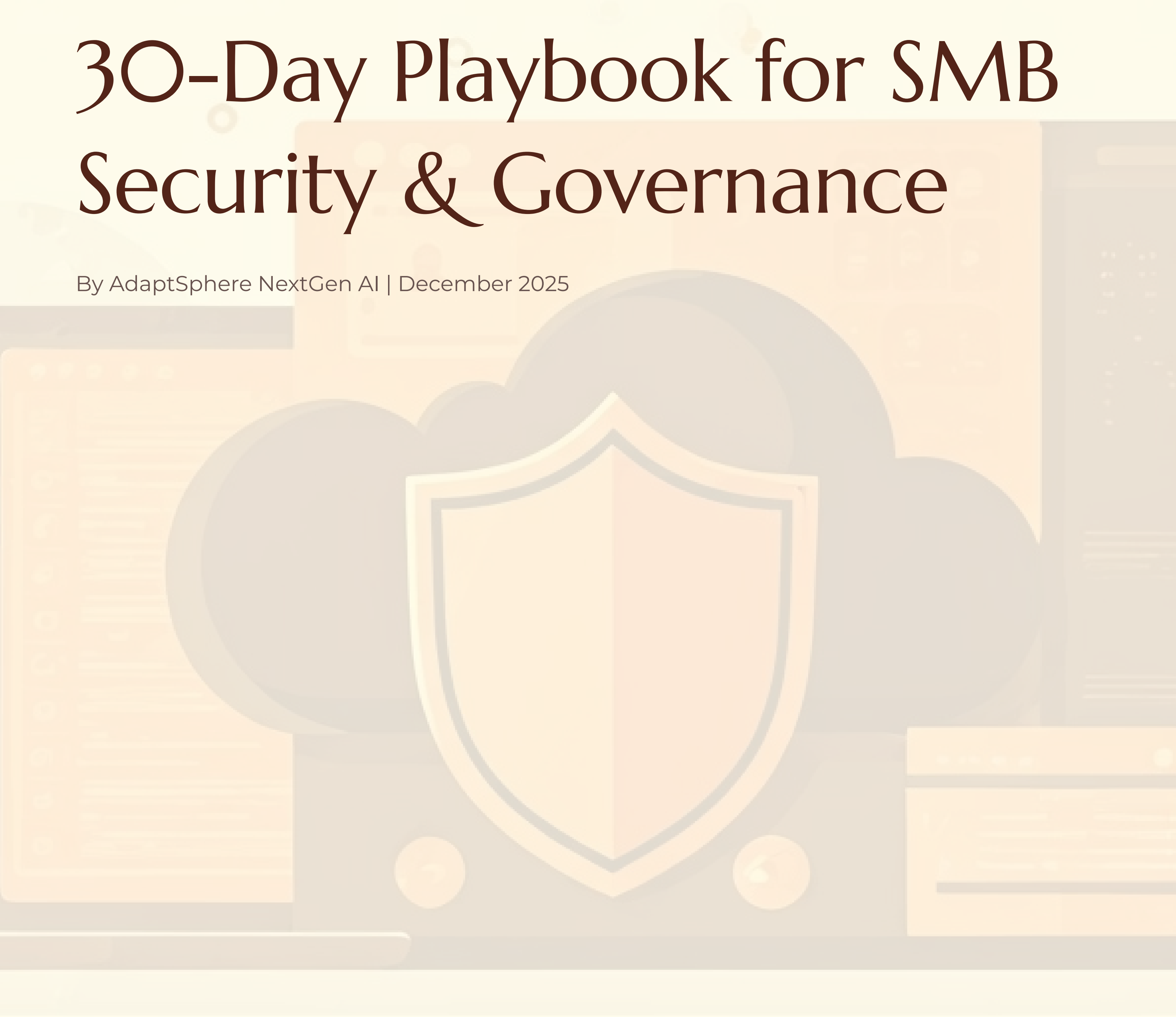
Copilot Control System Implementation Checklist

30-Day Playbook for SMB Security & Governance

By AdaptSphere NextGen AI | December 2025



Important Guidance:

While this checklist reflects Microsoft's official security recommendations and governance frameworks as of December 2025, every organization's infrastructure, compliance requirements, and risk profile is unique. Additionally, Microsoft's Copilot platform and governance capabilities evolve frequently - new features, policy options, and best practices may emerge that supersede elements of this guide.

Collaborate with your IT, security, and compliance leaders to adapt these steps to your specific environment and regulatory needs. Use a pilot group or test environment first to validate that each control works as intended in your tenant configuration, and customize the 30-day timeline based on your organization's complexity and readiness. Stay current with Microsoft Learn, TechCommunity blogs, and Ignite sessions for the latest CCS features, DLP capabilities, and governance changes. Document which controls you implement, when, and why—this creates accountability and helps with future audits. If you're implementing in a highly regulated industry (healthcare, finance, public sector) or have complex compliance requirements, consider working with a governance specialist familiar with the latest Microsoft updates.

This checklist is a starting point, not a substitute for professional security or legal advice specific to your organization's needs and jurisdiction. Given the rapid pace of Microsoft product evolution, we recommend reviewing and updating your implementation strategy quarterly.

Overview

The **Copilot Control System (CCS)** is Microsoft's unified governance framework for Copilot and AI agents. It combines:

Security & Governance

Purview DLP for Copilot (new), DSPM, sensitivity labels, audit logging

Management Controls

Copilot policies, Teams/SharePoint settings, agent governance

Measurement & Reporting

Usage analytics, adoption dashboards, safety metrics

This 10-page checklist helps you implement all three pillars in 30 days.

Pre-Implementation Requirements

Admin Access Required

- Microsoft 365 Admin Center (Global or Service Admin)
- Purview Compliance Portal (Compliance Admin)
- Entra ID admin access (Identity Admin)
- Microsoft 365 Audit Logs enabled
- Copilot Studio (if building agents)

Documentation Needed

- Teams inventory (names, owners, public/private status)
- SharePoint site list (purpose, sensitivity level)
- OneDrive and shared mailbox patterns
- Current sensitivity label strategy
- Active DLP policies
- Custom apps, connectors, agents list

Key Stakeholders

IT/Security Lead

owns CCS implementation

Microsoft 365 Administrator

tenant configuration

Business Owner/Dept Leads

data classification

Finance

licensing and Copilot Business cost

Executive Sponsor

approves rollout

Week 1: Map & Assess

Task 1.1: Inventory High-Risk Data

List your 10-20 most sensitive locations:

> **Example High-Risk Locations:**
>
> Finance SharePoint: Budgets, forecasts, GL - High risk - CFO owner - Label as Confidential
>
> HR SharePoint: Salary, reviews, policies - High risk - HR Lead owner - Restrict to HR
>
> Legal/Contracts: NDAs, IP, agreements - High risk - Counsel owner - Label Highly Confidential
>
> Executive Team: Board prep, strategy - High risk - CEO owner - Verify membership
>
> Finance Mailbox: AR, AP, payroll - High risk - Controller owner - Audit access

Action Items:

- Identify top 10-20 repositories
- Rate each High/Medium/Low risk
- Assign owner for each
- Note which Copilot experiences can access each (Outlook, Teams, SharePoint, Chat, Search)

Week 1: CCS Readiness Assessment

Task 1.2: CCS Readiness Assessment

Rate yourself 0-2 for each control (0=not in place, 2=fully implemented):

1

Pillar 1: Security & Governance

- Sensitivity labels (Public/Internal/Confidential/Highly Confidential): __/2
- Label enforcement (auto or mandatory): __/2
- Encryption & external share block: __/2
- DLP policies active: __/2
- Purview audit logging enabled: __/2
- DSPM for AI visibility: __/2

Total Score (0-12): __

Guidance: 9-12 = Mature | 5-8 = Partial | 0-4 = At Risk

2

Pillar 2: Management Controls

- Copilot licenses assigned: __/2
- Copilot Outlook/Teams policy: __/2
- Teams public vs private: __/2
- Guest access reviewed: __/2
- Agent governance in place: __/2
- MFA and device compliance: __/2

Total Score (0-12): __

Guidance: 9-12 = Strong | 5-8 = Building | 0-4 = Weak

3

Pillar 3: Measurement & Reporting

- Copilot adoption tracked: __/2
- Content labeling tracked: __/2
- DLP blocks logged: __/2
- Oversharing incidents tracked: __/2
- Guest reviews completed: __/2
- Time-saved metrics captured: __/2

Total Score (0-12): __

Guidance: 9-12 = Mature | 5-8 = Partial | 0-4 = Minimal

Week 2: Deploy Core Controls

Task 2.1: Enable DSPM for AI (Visibility)

Goal: See where sensitive data sits and what Copilot can access.

- In Microsoft 365 Admin Center, enable Copilot Control System dashboards
- In Purview, run data access governance reports for SharePoint
- Review DSPM reports to identify overshared sites and mislabeled files
- Prioritize top 20 files/sites for remediation

Task 2.2: Deploy Purview DLP for Copilot (Critical - New)

This new feature blocks sensitive data from being used in Copilot interactions.

DLP Rules to Create:

Financial Data

Credit cards, account numbers, SWIFT codes

PII/Privacy

SSNs, national IDs, passport numbers

Health Data

HIPAA-aligned content

Board/Legal

Confidential strategic/legal files

Internal Only

Prevent internal docs from leaving org

High Business Impact

Sensitive operations

Week 2: DLP Implementation & Testing

Implementation Steps:

01

In Purview > Data Loss Prevention > Policies, create or update rules

02

Start rules in **Audit Only** mode (learn phase, 1-2 weeks)

03

Move high-confidence rules to **Block** mode after tuning

04

Cover SharePoint, OneDrive, Exchange, Teams

Testing:

- Have test user ask Copilot to summarize file with fake credit card numbers - verify DLP blocks
- Confirm Finance users can still use Copilot on Finance-only sites
- Check Purview audit logs for DLP block entries

Week 2: Labels & Permissions

Task 2.3: Create Sensitivity Labels

Label Hierarchy:

1

Public

Share broadly (general info, marketing)

2

Internal

Company use only; no external sharing

3

Confidential

Finance/HR/contracts; restricted by department

4

Highly Confidential

Board, executive, strategic; auto-encrypt, no external share

Actions:

- In Purview > Information Protection > Labels, confirm labels exist
- Set Highly Confidential to auto-encrypt and block external sharing
- Enable auto-labeling for obvious cases (files with "salary," "SSN," "contract")
- Manually apply labels to top 20% of sensitive repositories

Task 2.4: Tighten Permissions & Sharing

Quick Wins:

- List all public Teams; convert any with sensitive data to Private
- In SharePoint Admin Center > Sharing, set external links to "Specific people" with 60-90 day expiry
- Remove "Anyone" sharing links from finance, HR, legal sites
- Ensure all Teams have 2 owners (no single point of failure)

Week 3: Enable Audit & Identity

Task 3.1: Comprehensive Audit Logging

- In Purview > Audit > Audit Search, confirm logging is On
- Set retention to minimum 90 days (prefer 1 year)
- Enable Purview Audit for Copilot and AI applications

Create Alerts For:

External sharing spikes

more than 10 new shares in 1 day

Bulk downloads

more than 50 files in 1 hour

New public Teams or Teams made public

DLP blocks on sensitive data

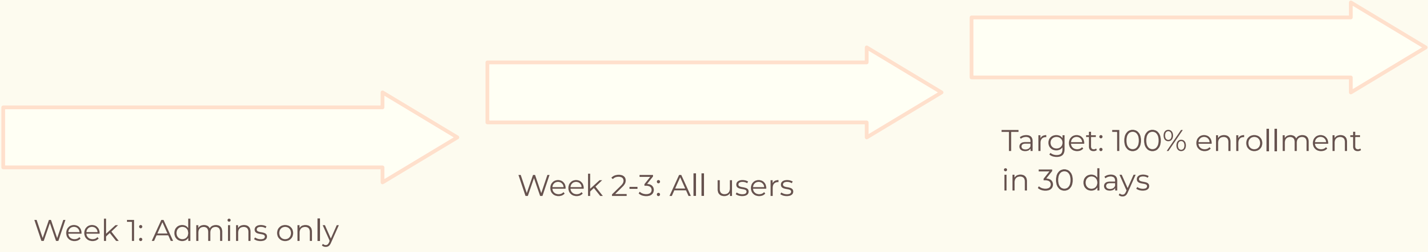
Alert Delivery:

- Daily digest to Security Lead
- Weekly summary to IT Lead

Week 3: MFA & Access Reviews

Task 3.2: MFA & Access Reviews

MFA Rollout:



Week 1: Admins only

Week 2-3: All users

Target: 100% enrollment in 30 days

- In Entra ID > Security > Multi-factor Authentication
- Require phone app or passwordless sign-in

Quarterly Access Reviews:

- Set up in Entra ID > Identity Governance > Access Reviews
- Assign dept leads as reviewers
- Auto-remove unused access after 30 days if not reviewed

Guest Access Cleanup:

- Audit all guest accounts and last login date
- Remove guests who completed projects more than 90 days ago
- Require explicit approval for new guest invites

Week 4 & Beyond: Measure & Maintain

Task 4.1: Monthly Scorecard (Key Metrics)

Track these metrics with Business, IT, and Ops leads monthly:

> **Key Metrics to Track:**
>
> Copilot adoption (% active weekly): Target 50% or more
>
> Labeled high-risk content: Target 100%
>
> DLP blocks logged: Stable/declining trend
>
> Oversharing incidents: Target 0 per month
>
> MFA enrollment: Target 100%
>
> Guest reviews completed: Target 100%
>
> Time-saved examples: Target 10+ per 100 users

Monthly Meeting (60 minutes):

1

Business (10 min)

Getting value? Compliance concerns?

2

IT/Security (20 min)

Any incidents? Noisy controls? Tuning needed?

3

Operations (10 min)

User friction? Training gaps?

4

All (20 min)

Priorities for next month?

Week 4: Extend Governance

Task 4.2: Extend Governance (Month 2)

Once foundational controls are stable:

Copilot Studio Agents

Register all agents, restrict data connections, require IT approval before publishing

Outlook Governance

Apply retention labels to sensitive mailboxes; test Copilot respects labels

Teams & SharePoint

Document all bots/webhooks; ensure service accounts have least-privilege access

Quick Rollback Reference

If you need to quickly reverse a control, use this reference:

Auto-label rules

Rollback: Disable auto; keep manual labels

Time: 2-4 hours

External link defaults

Rollback: Loosen expiry or type

Time: 1-2 hours

MFA for non-admins

Rollback: Pause; re-enable with phased plan

Time: 1 day

Public to Private Teams

Rollback: Revert within 30 days

Time: 1 day

DLP block rule

Rollback: Switch to audit or warn

Time: 1-2 hours

Copilot policy

Rollback: Disable for group while investigating

Time: Same day

Success Checklist (End of 30 Days)

By end of Week 4, you should have:

- □ Documented all sensitive data locations (10-20 sites)
- □ Deployed baseline DLP rules (in audit or block mode)
- □ Applied sensitivity labels to top 20% of sensitive content
- □ Tightened permissions on overshared sites
- □ Enabled Purview audit logging with alerts
- □ Achieved 90% or more MFA enrollment
- □ Completed first monthly scorecard with stakeholders
- □ Scheduled quarterly access reviews

By Month 2: Extend governance to custom agents, Outlook, and Teams.

Key Resources

Microsoft Ignite 2025: CCS Updates

techcommunity.microsoft.com

CCS Security & Governance

learn.microsoft.com/copilot

Purview DLP for Copilot

learn.microsoft.com/purview

Configure DLP & DSPM

Microsoft official documentation

Notes & Progress Tracking

Use this section to track your implementation progress:

Week	Task	Owner	Status
Week 1	Inventory & assess	______	[ ]
Week 2	Deploy DLP & labels	______	[ ]
Week 3	Enable audit & MFA	______	[ ]
Week 4	First scorecard	______	[ ]

Additional Notes:

____

____

____

____

____

____

____

____

Last Updated: December 2025

Contact: info@adaptsphere.ai