Implementing AI-Ready Security Roles in Business Central

A Complete Step-by-Step Guide

Easiest to Most Involved

For Microsoft Dynamics 365 Business Central
and the Microsoft Ecosystem

S. David Brown, JD
PacificaOne
InnoviaCon 2026

Why This Guide Exists

Every AI feature in Business Central inherits your existing security roles. Copilot Chat queries data using the logged-in user's permission set. The Payables Agent processes invoices under its own dedicated identity. Custom agents built in Agent Designer operate within whatever permissions you assign. MCP connections pass through the authenticated identity's role. Power Automate flows execute with the connection identity's access.

None of these tools bypass your security model. None create their own elevated access. They simply use the roles you already defined, at machine speed, with the ability to traverse and correlate data across every table those roles can access.

If your roles are clean, tight, and aligned with least privilege, AI becomes a powerful tool that operates safely within well-defined boundaries. If your roles are messy, sprawling, and full of accumulated excess access, AI becomes a force multiplier for every gap in your security posture.

This guide walks you through fixing that, starting with the simplest actions you can take today and progressing to the most involved architectural decisions. Each step includes exactly what to do, where to find it in BC, and why it matters for AI readiness.

How This Guide Is Organized

The steps are ordered from least effort to most effort. The first steps require no budget, no new tools, and less than thirty minutes. The later steps involve planning, governance decisions, and potentially partner engagement. You do not need to complete every step before enabling AI features, but you should complete at least steps 1 through 5 before expanding AI access beyond read-only Copilot Chat.

Each step follows the same format:

- **What:** The specific action
- **Where in BC:** Exact navigation or page name
- **Time required:** Realistic estimate
- **Why it matters for AI:** The specific connection to AI risk
- **How to do it:** Detailed walkthrough
- **What to do with what you find:** Decision framework
- **Common pitfalls:** Mistakes to avoid

STEP 1: AUDIT YOUR SUPER USERS

Effort: Low | Time: 15-30 minutes | Budget: None

What

Identify every user in your Business Central environment who has the SUPER permission set assigned, and determine whether each one actually needs it.

Where in BC

Search for "User Security Status" in the BC search bar. This page shows all users and their assigned permission sets. You can also go to the Users page, select a user, and view their Permission Sets section.

Alternatively, search for "Permission Set by User" which lets you look up a specific permission set and see every user who has it assigned.

Time Required

15 minutes to pull the list. Another 15 minutes to document your findings and determine next steps.

Why It Matters for AI

SUPER grants unrestricted access to every table, every object, every function in Business Central. There are no boundaries. When Copilot Chat runs in the context of a SUPER user, it can query any data in the system. When a Power Automate flow authenticates as a SUPER user, it can read and modify anything. If an MCP connection or Copilot Studio agent authenticates with a SUPER identity, that agent has the equivalent of unrestricted database access.

SUPER was tolerable when humans interacted with BC one page at a time. A SUPER user still had to navigate to specific pages, apply filters, and manually process data. The complexity of the interface was itself a barrier. AI removes that barrier entirely. A SUPER-credentialed AI can traverse and correlate your entire database in seconds.

Microsoft recognized this risk at the API layer: applications connecting through API registrations in Entra ID cannot be assigned the SUPER permission set. Microsoft enforces this guardrail programmatically. But the same guardrail does not exist for human user accounts, and those accounts can be used as connection identities for Power Automate flows, Power BI datasets, and other tools.

How to Do It

1. Open BC and search for "User Security Status"
2. Look at the Super User column, which shows Yes or No for each user
3. Export this list to Excel for documentation (use the Share icon or copy and paste)

4. For each SUPER user, document their name, email, actual job function, when SUPER was assigned, who assigned it and why, and whether they use SUPER for daily work or only for occasional admin tasks

What to Do with What You Find

Legitimate SUPER users (keep, but minimize)

- One or two BC administrators who perform system configuration, extension installation, and user management
- Even these users should consider having a separate non-SUPER account for daily work and switching to SUPER only when performing admin tasks

SUPER users who do not need it (remove or replace)

- Users who received SUPER during implementation for convenience
- Users who received SUPER during a month-end crisis and it was never removed
- Users who inherited SUPER from a copied permission set
- Users who left the company but their account is still active
- For each of these: create or assign appropriate permission sets that cover their actual job functions, then remove SUPER

Service and integration accounts with SUPER (critical to address)

- Any non-human account with SUPER is a high-priority issue
- These accounts are the most likely identities for AI connections
- See Step 4 for detailed guidance on service accounts

Common Pitfalls

- **"But they need SUPER for month-end close."** They do not. They need specific posting and adjustment permissions. Identify exactly which tables and operations they need during close and create a dedicated Month-End Close permission set.
- **"Removing SUPER will break things."** It might, temporarily. This is actually useful information. Each permission error tells you exactly what access the user actually needs. Add those specific permissions to a custom set.
- **"We will do it later."** Every day SUPER remains on accounts that do not need it is a day those accounts could be used as AI connection identities with unrestricted access. The risk increases as more AI features activate.
- **"We only have three SUPER users, it is fine."** Three SUPER users means three potential unrestricted AI access points. The number that is fine is the minimum required for system administration, which is usually one or two.

STEP 2: CHECK WHAT AI FEATURES ARE ACTIVE

Effort: Low | Time: 10 minutes | Budget: None

What

Determine which Copilot and AI capabilities are currently enabled in your Business Central environment and understand what each one does.

Where in BC

Search for "Copilot & AI Capabilities" in the BC search bar. This page shows every AI feature available in your environment, its status (Active, Inactive, Preview), and configuration options.

Time Required

10 minutes to review the page and understand what is active.

Why It Matters for AI

In BC SaaS, Microsoft can activate AI features through updates without requiring explicit customer approval. Some features may already be active in your environment without anyone having deliberately enabled them. You need to know what is on before you can assess whether your roles are ready for it.

The COPILOT SYS FEATURES permission set (introduced in BC v26) controls whether individual users can access Copilot functionality. But this is an all-or-nothing switch per user. If a user has the COPILOT SYS FEATURES permission set and Copilot Chat is active in the environment, they can use Copilot Chat to query any data their underlying permission set allows. There is no way to say this user can use Copilot for sales data but not financial data. The access boundary is always the user's full permission set.

How to Do It

1. Search for "Copilot & AI Capabilities" in BC
2. Review each listed capability including its status, description, and data movement settings
3. For each active feature, ask: Do we want this active right now? Do our users' permission sets appropriately scope what this feature can access? Have we communicated to users that this feature exists?
4. Document the current state: which features are active, which are inactive
5. Check the Copilot data movement settings to understand where your data flows for AI processing

What to Do with What You Find

- **If features are active that you did not deliberately enable:** This is normal in SaaS BC. Microsoft activates features through updates. Decide whether to leave them active or disable them while you complete the role cleanup in the remaining steps.

- **If you want to limit which users can use Copilot:** Search for Permission Sets and find COPILOT SYS FEATURES. Remove it from users who should not have Copilot access. Add it to users who should.
- **If agents are available:** These have their own configuration pages (search for Agents in BC). They require deliberate setup. See Step 8 for detailed agent configuration guidance.

Common Pitfalls

- **"We did not turn anything on, so nothing is active."** Check anyway. SaaS updates can activate features.
- **"We will just disable everything."** This is an option, but it means you lose the productivity benefits. A better approach: complete the role cleanup (Steps 1-5) and then enable features strategically.
- **"Our users do not know about Copilot."** They may discover it on their own. The Copilot icon appears in the BC interface when features are active. Proactive communication is better than reactive surprise.

STEP 3: USE THE PERMISSIONS OVERVIEW PAGE (BC V28)

Effort: Low | Time: 30-60 minutes | Budget: None

What

Use the new Permissions Overview page in BC v28 to get a comprehensive, unified view of all permission sets in your environment, including those from ISV extensions.

Where in BC

Search for "Permissions Overview" in the BC search bar. This page was introduced in BC v28, which began rolling out April 1, 2026. Also useful: the "Effective Permissions" page, which shows the combined effective permissions for a specific user across all their assigned permission sets.

Time Required

30 minutes for an initial review. Up to an hour if you want to document findings for specific users or roles.

Why It Matters for AI

In a modern BC environment, your permission sets come from three sources: Microsoft's base application (System permission sets like D365 BASIC, D365 PURCH DOC EDIT), your own custom permission sets (User-defined), and ISV extensions (Insight Works, Continia, Lanham, and others each bring their own permission sets). Until BC v28, getting a unified view across all three sources required manual work.

The Permissions Overview page gives you that unified view for the first time. This matters for AI because Copilot and agents do not distinguish between permissions from the base app, your custom sets, or ISV extensions. They see the combined effective permissions. An ISV extension might grant broader access than you realized, and that broader access becomes part of what AI can query.

How to Do It

Using Permissions Overview (BC v28 and later)

1. Search for "Permissions Overview" in BC
2. Browse permission sets by source: System (Microsoft), User (your custom sets), Extension (ISV)
3. For each permission set, review which objects it grants access to, what level of access, and which app or extension it belongs to
4. Look specifically for permission sets that grant Modify or Delete on sensitive tables, ISV extension permission sets with broader access than expected, and permission sets you do not recognize

Using Effective Permissions

1. Search for "Effective Permissions" in BC
2. Select a specific user
3. Review their combined effective permissions across all assigned permission sets
4. Key understanding: permissions from different sets combine. The system takes the highest access level. If Set A grants Read on the Customer table and Set B grants Modify on the Customer table, the user gets Modify access.
5. Check the Source column to understand which permission set is granting each permission

Priority users to check

- Users you identified as having SUPER in Step 1
- Users in sensitive roles: AP clerks, controllers, anyone who processes payments
- Service and integration accounts (see Step 4)
- Users who will be early adopters of Copilot or agents

Common Pitfalls

- **"This is overwhelming."** Focus on your highest-risk users first: SUPER users, payment processors, service accounts. You do not need to review everything at once.
- **"I do not understand what these objects are."** Focus on table names you recognize: Customer, Vendor, Item, Employee, G/L Entry. If you do not recognize a table, it is probably a system table, still worth noting but lower priority.
- **"Our ISV extensions need all those permissions."** Maybe. But verify. Some ISV permissions were designed broadly for compatibility, not because every user needs every permission.

STEP 4: DOCUMENT AND REVIEW SERVICE/INTEGRATION ACCOUNTS

Effort: Medium | Time: 1-2 hours | Budget: None

What

Identify every non-human account in your BC environment (service accounts, integration accounts, API connections), document their permission sets, and determine whether those permissions are appropriately scoped.

Where in BC

Users page in BC for BC-side accounts. Microsoft Entra admin center (entra.microsoft.com) for App registrations and Enterprise applications. Power Automate (make.powerautomate.com) for Power Platform connections.

Time Required

1-2 hours for initial inventory and documentation. May require follow-up with your IT team or partner to understand what each account is used for.

Why It Matters for AI

Service accounts are the most likely identities that AI connections will authenticate with. When you build a Copilot Studio agent that connects to BC through MCP, it needs an identity. When a Power Automate flow connects to BC, it authenticates as someone. These non-human accounts are the natural choice for these connections.

The problem: service accounts in most BC environments have dramatically broader permissions than necessary. They were set up during implementation with the goal of making the integration work, not minimizing access. The typical pattern is assigning D365 FULL ACCESS or even SUPER to a service account because troubleshooting permission errors for an integration is time-consuming and the path of least resistance is broad access.

An MCP connection authenticating with a service account that has D365 FULL ACCESS gives the connected AI agent read and write access to nearly everything in your database. Microsoft provides a guardrail: applications connecting through API registrations in Entra ID cannot be assigned the SUPER permission set. This is enforced programmatically. But D365 FULL ACCESS is not SUPER and can still be assigned.

How to Do It

Inventory BC Users

- Go to the Users page in BC and look for accounts not associated with current employees
- Look for naming patterns like Integration, Service, API, Connector, Sync, or the name of an external system

- For each account, document: account name, what system it serves, all assigned permission sets, when created, who manages it, when permissions were last reviewed

Inventory Entra ID App Registrations

- Go to Microsoft Entra admin center and navigate to Applications then App registrations
- Look for applications that connect to Business Central
- Check API permissions granted, whether it has BC permissions assigned, who created it, and last sign-in activity

Inventory Power Platform Connections

- Go to Power Automate and navigate to Data then Connections
- Look for connections to Business Central
- Note what identity it authenticates as, what flows use this connection, and whether it uses a personal account or a service principal

What to Do with What You Find

- For each service account with broad permissions: determine exactly what the integration needs, create a custom permission set granting only those specific permissions, test in sandbox, apply in production, and document
- For accounts whose purpose you cannot determine: check the Change Log for recent activity, ask your implementation partner, and if genuinely unused, disable the account
- For Power Automate connections using personal accounts: consider migrating to service principal authentication with a dedicated, narrow permission set

Common Pitfalls

- **"I do not want to break our integration."** Test in sandbox first. Always. Never change service account permissions in production without testing.
- **"Our partner set this up."** Contact your partner. They should be able to tell you which BC tables and operations the integration uses.
- **"It has worked fine for years with FULL ACCESS."** Yes, because FULL ACCESS includes everything. The goal is to give only the access that is actually needed.
- **"We use the same account for multiple integrations."** Each integration should have its own dedicated service account with its own scoped permission set.

STEP 5: IDENTIFY AND FIX SEGREGATION OF DUTIES VIOLATIONS

Effort: Medium-High | Time: 2-4 hours | Budget: None

What

Review user permission sets for segregation of duties (SoD) conflicts, where a single user has the combined ability to perform an entire transaction without oversight.

Where in BC

This requires reviewing each user's Effective Permissions and cross-referencing against SoD rule sets you define. BC does not have a built-in SoD engine (unlike Dynamics 365 Finance and Operations, which has SoD rule sets and automatic violation detection).

Why It Matters for AI

Segregation of duties violations that exist in your permission structure are inherited by AI. If a user can create a vendor, enter a purchase invoice, and post a payment, Copilot Chat can help them do all three faster. An agent operating under that user's permissions could theoretically do all three autonomously. AI makes SoD violations easier to exploit by reducing the friction of manual navigation.

For organizations subject to SOC 2 audits, financial audits, or regulatory compliance, SoD violations documented in your BC environment could become audit findings, especially as auditors begin asking about AI controls.

Accounts Payable SoD Rules

Duty A	Duty B	Why They Conflict
Create/modify vendor records	Enter purchase invoices for vendors	User could create a fictitious vendor and enter fake invoices
Enter purchase invoices	Approve/post purchase invoices	User could enter and approve their own invoices without oversight
Enter purchase invoices	Process payments/post payment journals	User could enter invoices and pay them without approval
Create/modify vendor records	Process payments	User could create a fictitious vendor and route payments to themselves
Modify vendor bank account details	Process payments	User could redirect legitimate payments to a different bank account

General Ledger SoD Rules

Duty A	Duty B	Why They Conflict
Create journal entries	Post journal entries	User could create and post unauthorized adjustments

Modify chart of accounts	Post transactions	User could create accounts and post to them without oversight
Modify posting setup tables	Post transactions	User could change where transactions post and then post transactions

Inventory SoD Rules

Duty A	Duty B	Why They Conflict
Adjust inventory quantities	Modify item costs	User could inflate inventory values through cost and quantity manipulation
Create purchase receipts	Post inventory adjustments	User could create phantom receipts and adjust inventory to cover shortages
Process warehouse shipments	Modify sales orders	User could modify orders after shipment to cover diversion of goods

How to Fix Violations

- **Option 1: Split responsibilities across users.** Assign Duty A permissions to User 1 and Duty B permissions to User 2. This is the cleanest fix.
- **Option 2: Add compensating controls via approval workflows.** Configure BC approval workflows to require a different user to approve the sensitive action. Note: workflows are a compensating control, not a fix for the underlying permission issue.
- **Option 3: Create time-limited elevated access.** User normally has restricted permissions. For specific tasks like month-end close, temporarily assign additional permissions. Set a calendar reminder to remove the elevated access.

Common Pitfalls

- **"We are too small to segregate duties."** When you cannot split duties across people, compensating controls become essential. Document the constraint and the controls you have in place.
- **"Nobody has ever committed fraud here."** SoD is not just about fraud. It is about preventing mistakes: duplicate payments, wrong accounts, unverified invoices.
- **"Our approval workflows already catch this."** Verify the workflows cover all scenarios. Many are configured for invoices above a dollar threshold but not for all invoices.

STEP 6: CONFIGURE THE CHANGE LOG FOR AI-RELEVANT TABLES

Effort: Medium | Time: 1 hour | Budget: None

What

Configure the BC Change Log to track modifications to security-sensitive tables, so you have an audit trail for permission changes, user management, and sensitive data modifications.

Where in BC

Search for "Change Log Setup" in the BC search bar. To view logged changes, search for "Change Log Entries".

Why It Matters for AI

The Change Log is your primary audit trail in BC. There is a critical gap: the Change Log tracks modifications (inserts, updates, deletes) but does NOT track what Copilot reads or queries. If Copilot summarizes 500 vendor records in response to a question, the Change Log shows nothing. Despite this gap, configuring it for sensitive tables is essential because it tells you when the security configuration itself changed.

Security and User Management Tables to Monitor

Table	Why Monitor
Access Control	Tracks when permission sets are assigned to or removed from users
User	Tracks when user accounts are created, modified, or disabled
Permission Set	Tracks when permission sets themselves are created or modified
User Property	Tracks changes to user properties
Tenant Permission Set	Tracks changes to tenant-level (custom) permission sets

Financial Sensitivity Tables to Monitor

Table	Why Monitor
Vendor	Tracks vendor record creation and changes
Vendor Bank Account	Tracks changes to where vendor payments are sent
Customer	Tracks customer record changes
Payment Terms	Tracks changes to payment terms, which rarely should change after setup
General Posting Setup	Tracks changes to how transactions post
Employee	Tracks changes to employee records including salary data

STEP 7: REVIEW AND TIGHTEN PERMISSION SETS FOR KEY ROLES

Effort: High | Time: 4-8 hours | Budget: None (may want partner help)

What

Review the permission sets assigned to your most sensitive user roles and replace overly broad sets with narrower, purpose-built ones that grant only the access each role actually needs.

Why It Matters for AI

This is the direct application of the principle: "Your employees ignore 96% of their permissions. Agents will not." (Oso/Cyera research: 2.4 million workers, 3.6 billion permissions, 96% unused). When humans have overly broad permissions, they do not exercise the excess because they do not navigate to pages they do not need. When AI operates under those same permissions, it can access everything the permissions allow, because natural language queries bypass the need to know where data lives.

Key Roles to Review First

1. Accounts Payable Clerk -- processes vendor invoices, handles payments
2. Accounts Receivable Clerk -- processes customer payments, handles collections
3. Controller / Accounting Manager -- financial reporting, month-end close, journal entries
4. Purchasing Agent -- creates purchase orders, manages vendors
5. Sales Order Processor -- enters sales orders, manages customer relationships
6. Warehouse Worker -- picks, packs, ships, receives
7. Warehouse Manager -- manages warehouse operations, inventory adjustments
8. IT Administrator -- system configuration, user management

Process for Each Role

- **Document current state:** List all permission sets currently assigned. Use Effective Permissions to see the combined result.
- **Determine actual needs:** Talk to the people doing the job. What pages do they use? What reports do they run? Compare actual needs to current permissions.
- **Design the target permission set:** Start with least privilege. Create custom User-type permission sets with descriptive names. For each table, determine whether Read, Insert, Modify, or Delete access is needed.
- **Test in sandbox:** Apply new permission sets to test users. Have actual users test their daily workflows. Document permission errors and add specific missing permissions.
- **Deploy to production:** Replace old broad sets with new narrow ones. Keep documentation. Monitor for issues.

Example: AP Clerk Permission Set

An AP clerk in a food distribution company needs to: view vendor records (Read on Vendor table), enter purchase invoices (Insert on Purchase Header and Purchase Line), view purchase order history, view item information for invoice matching, and run AP aging reports.

An AP clerk does NOT need to: create or modify vendor records, post purchase invoices, access employee records, modify payment terms or posting setup, access sales data, or modify item costs.

The resulting custom permission set might grant access to 30-40 objects instead of the 91 or more objects in D365 PURCH DOC EDIT.

STEP 8: CONFIGURE AGENTS WITH DEDICATED IDENTITIES AND NARROW ROLES

Effort: High | Time: 2-4 hours per agent | Budget: None

What

When deploying BC agents (Payables Agent, Sales Order Agent, custom agents via Agent Designer), configure each with its own dedicated identity and the narrowest possible permission set.

Why It Matters for AI

Agents are autonomous. Unlike Copilot Chat where a human types each query, agents operate continuously and make decisions without real-time human oversight. If the agent's permission set is broader than necessary, every action the agent takes has a larger blast radius. A permission error during testing is a signal that the agent is trying to access data it should not have. The correct response is to add the specific permission it needs, not to assign a broad set like D365 FULL ACCESS.

Payables Agent Setup

- Review the agent card and note the Agent Permission Sets section
- The default permission set is PAYABLES AGENT RUN, a system set designed by Microsoft specifically for this agent
- Do NOT add D365 FULL ACCESS, D365 BASIC, or other broad sets to the agent
- Configure a dedicated email mailbox, not a shared human mailbox
- Configure the supervisor who reviews and approves draft invoices
- Test in sandbox with sample invoices before enabling in production

Agent Designer (Custom Agents, BC v28)

- Define the agent's purpose narrowly
- Assign permission sets starting from zero and adding only what is needed. Never copy a human user's permission sets to an agent.
- Test extensively in sandbox before production deployment
- Export the agent definition as JSON and store it in version control

Entra ID Agent Identity (for Copilot Studio Agents)

- Register a dedicated service principal in Entra ID for the agent
- Use Microsoft Entra Agent ID (preview 2026) if available in your tenant
- Apply Conditional Access policies to the agent identity if appropriate
- In BC, create a user record for the service principal and assign a narrow, purpose-built permission set

- Document the agent's purpose, its Entra ID identity, its BC permission sets, who created it, and when it was last reviewed

STEP 9: REVIEW M365 AND SHAREPOINT PERMISSIONS

Effort: Medium-High | Time: 2-4 hours | Budget: None

What

Review permissions in Microsoft 365, SharePoint, and OneDrive alongside your BC permissions, because AI tools can correlate data across these systems.

Why It Matters for AI

Business Central is not an island. A Copilot Studio agent with MCP connections can connect to BC and M365 simultaneously. BC roles might appropriately restrict access to customer financial data, but if someone saved a customer profitability spreadsheet on a SharePoint site that is shared too broadly, an AI agent connected to both could combine data from both sources.

Research confirms this is widespread: 60-80% of enterprise SharePoint sites have at least one oversharing vulnerability (EPC Group). 16% of business-critical data is overshared (Concentric AI, 550 million records analyzed). The average company has 802,000 files at risk.

Key Areas to Review

- **SharePoint site permissions:** Review sharing settings for sites containing financial data, HR data, customer sensitive data, and vendor sensitive data. Check for sites shared with Everyone or Everyone except external users.
- **OneDrive sharing:** Review broadly shared files and folders. Check for files shared via Anyone with the link.
- **Microsoft 365 Groups:** Review group membership, especially groups tied to Teams channels where sensitive information is discussed.
- **Microsoft Purview (if available):** Use data classification and sensitivity labels to identify where sensitive data lives. Configure DLP policies to restrict how sensitive data is shared.

STEP 10: IMPLEMENT ROW-LEVEL SECURITY FILTERS

Effort: High | Time: 4-8 hours | Budget: None (may want partner help)

What

Configure BC security filters to restrict which records within a table each user or agent can access, adding a second dimension of control beyond table-level permissions.

Why It Matters for AI

Permission sets control which tables a user can access. Security filters control which records within those tables the user can see. Both apply equally to humans and AI. Without security filters, a sales user with read access to the Customer table can see every customer in the system. With a security filter restricting to their territory, the user and Copilot operating as that user can only see customers in their assigned area.

Common Filtering Dimensions

- **Multi-location distribution/manufacturing:** Location Code (filter by warehouse, plant, or distribution center) and Responsibility Center (filter by business unit)
- **Multi-territory sales:** Salesperson Code (filter by assigned salesperson/territory) and Customer Posting Group (filter by customer segment)

How to Configure

- Go to Permission Sets page and select the permission set you want to filter
- Click Permissions to view the table-level permissions
- Find the table you want to filter and enter a filter expression in the Security Filter column
- Example: Location Code=FILTER(WAREHOUSE-A) restricts to records for Warehouse A
- Filters apply to ALL access through that permission set, including API access, Power Automate, and AI
- Save and test with the affected user in a sandbox environment

STEP 11: ESTABLISH AN AGENT GOVERNANCE FRAMEWORK

Effort: High | Time: 4-8 hours for design | Budget: None

What

Create a formal process for reviewing, approving, and monitoring AI agents before they are deployed in your BC environment.

Why It Matters for AI

Agent Designer in BC v28 makes it easy to build custom agents using natural language instructions. That accessibility means the people building agents may not be the people who understand security implications. Without a governance framework, you will end up with agents deployed with broad permissions, no documentation, and no oversight.

Agent Deployment Checklist

- **1. Purpose Documentation:** What does this agent do? What business process does it support? Who requested it? Who built it?
- **2. Identity Review:** Does the agent have its own dedicated identity? Is it registered in Entra ID? Are Conditional Access policies applied?
- **3. Permission Review:** What permission sets are assigned? Were they designed from scratch or copied from a human user? Has Effective Permissions been reviewed?
- **4. Input Source Review:** What data does the agent read? Are any input sources exposed to external parties?
- **5. Output/Action Review:** What can the agent create, modify, or delete? Are destructive actions gated by human approval?
- **6. Testing Verification:** Was the agent tested in sandbox? Were edge cases and prompt injection resistance tested?
- **7. Monitoring Plan:** How will the agent's actions be audited? Who reviews agent activity and how often?

Agent Governance Responsibilities

- **Agent Sponsor:** The business user who requested the agent. Responsible for defining the business need and reviewing output.
- **Agent Builder:** The person who configures the agent. Responsible for technical configuration.
- **Security Reviewer:** Someone with BC security knowledge who reviews permission sets before production deployment.
- **Ongoing Monitor:** Someone responsible for periodic review of agent activity.

STEP 12: ESTABLISH CONTINUOUS SECURITY GOVERNANCE

Effort: Ongoing | Time: 30-60 min/quarter | Budget: None

What

Establish a recurring process for reviewing and maintaining your security posture as AI features evolve and your business changes.

Why It Matters for AI

Security is not a one-time project. BC updates every month in SaaS. New AI features activate. Agents are deployed. People change roles. Without recurring reviews, your carefully designed security architecture degrades over time, exactly the way it degraded before you started this guide.

Research from the AI Risk Report 2026: 73% of organizations have deployed AI tools, but only 7% have governance frameworks. The 93% gap is where incidents happen.

Quarterly Review Checklist (30-60 minutes)

- **SUPER User Review:** Pull the SUPER user list. Has anyone been added since the last review? Remove SUPER from any user who no longer needs it.
- **Agent Deployment Review:** What agents are deployed? Have any new agents been created? Review permission sets for broadening.
- **Service Account Review:** Have any new service accounts been created or permissions expanded?
- **MCP Connection Inventory:** What MCP connections exist? What identity does each authenticate with?
- **Permission Set Changes:** Review Change Log entries for Access Control and Permission Set tables.
- **Copilot Feature Status:** Check Copilot and AI Capabilities page for newly activated features.

OWASP Agentic AI Top 10 as an Audit Framework

5. Excessive Agency: Does each agent have only the permissions it needs?
6. Uncontrolled Autonomy: Are destructive actions gated by human approval?
7. Insecure Tool Use: Are MCP tools scoped narrowly?
8. Inadequate Guardrails: Are security filters and access boundaries in place?
9. Insufficient Logging: Is the Change Log configured? Are Entra sign-in logs monitored?
10. Unsafe Output Handling: Does the agent create drafts (safe) or post directly (risky)?
11. Vulnerable Supply Chain: Are ISV extensions and third-party MCP servers reviewed?
12. Improper Multi-Agent Trust: If agents communicate, are trust boundaries defined?
13. Data Leakage: Could agent actions expose sensitive data to unauthorized parties?
14. Lack of Human Oversight: Is there a human in the loop for irreversible actions?

Summary: The Implementation Sequence

Step	Action	Effort	Time	Do Before Enabling
1	Audit SUPER users	Low	15-30 min	Anything
2	Check active AI features	Low	10 min	Anything
3	Use Permissions Overview	Low	30-60 min	Expanding Copilot access
4	Document service accounts	Medium	1-2 hours	Any AI connections
5	Fix SoD violations	Med-High	2-4 hours	Agents that write data
6	Configure Change Log	Medium	1 hour	Agents in production
7	Tighten permission sets	High	4-8 hours	Broad Copilot rollout
8	Configure agents properly	High	2-4 hrs/agent	Each agent deployment
9	Review M365/SharePoint	Med-High	2-4 hours	Cross-system AI (MCP)
10	Implement security filters	High	4-8 hours	Multi-location AI access
11	Agent governance framework	High	4-8 hrs design	Custom agent deployments
12	Continuous governance	Ongoing	30-60 min/qtr	Always (never stop)

Minimum viable security posture for AI: Complete Steps 1 through 6 before expanding AI access beyond basic Copilot Chat. This takes approximately one working day spread across a week.

Recommended security posture for AI: Complete Steps 1 through 9 before deploying agents or MCP connections. This takes approximately two to three working days, potentially with partner assistance.

Comprehensive security posture for AI: Complete all 12 steps and maintain the ongoing governance cycle. This is the target state for organizations that are serious about AI-ready security.

Final Thought

The organizations that succeed with AI in Business Central will not be the ones with the perfect security architectures. They will be the ones that started. Every step in this guide uses tools you already have in BC and Entra. No new products are required. The only investment is time, attention, and the discipline to follow through.

Start now. Start small. But start.

Pull the SUPER list. Do it this week. Everything else follows from there.