Sources and References

Understanding Security Roles in AI Transformation

InnoviaCon 2026 | S. David Brown | PacificaOne

Microsoft Learn - Business Central

- **Copilot in Business Central Overview** - Core principle: Copilot inherits user data permissions
  https://learn.microsoft.com/en-us/dynamics365/business-central/copilot-overview
- **Configure Copilot and AI Capabilities** - How to enable, disable, and manage Copilot features per user
  https://learn.microsoft.com/en-us/dynamics365/business-central/enable-ai
- **Payables Agent Overview** - How the Payables Agent works end-to-end
  https://learn.microsoft.com/en-us/dynamics365/business-central/payables-agent
- **Payables Agent Setup** - Dedicated agent identity, PAYABLES AGENT - RUN permission set
  https://learn.microsoft.com/en-us/dynamics365/business-central/payables-agent-setup
- **Payables Agent FAQ** - Safety model: creates drafts only, never posts automatically
  https://learn.microsoft.com/en-us/dynamics365/business-central/faqs-payables-agent
- **Assign Permissions to Users and Groups** - Permission sets, effective permissions, and granular access control
  https://learn.microsoft.com/en-us/dynamics365/business-central/ui-define-granular-permissions
- **Security Groups in Business Central** - Linking Entra ID security groups to BC permission sets
  https://learn.microsoft.com/en-us/dynamics365/business-central/ui-security-groups
- **Security Filters** - Row-level security: restricting which records a user or agent can access
  https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/security/security-filters
- **Change Log Setup** - Configuring audit trails for security-sensitive tables
  https://learn.microsoft.com/en-us/dynamics365/business-central/across-log-changes
- **BC 2026 Release Wave 1 (v28)** - New features including Permissions Overview page and Agent Designer templates
  https://learn.microsoft.com/en-us/dynamics365/release-plan/2025wave2/smb/dynamics365-business-central/
- **BC 2026 Release Wave 1 Planned Features** - Detailed feature list for BC v28
  https://learn.microsoft.com/en-us/dynamics365/release-plan/2025wave2/smb/dynamics365-business-central/planned-features

Microsoft Learn - Entra ID and Agent Identity

- **What Are Agent Identities** - Microsoft Entra Agent ID: first-class identities for AI agents
  https://learn.microsoft.com/en-us/entra/agent-id/identity-platform/what-are-agent-identities
- **Entra Agent Identities for AI Agents** - Implementing agent identity governance in Entra
  https://learn.microsoft.com/en-us/entra/agent-id/identity-professional/microsoft-entra-agent-identities-for-ai-agents
- **Agent Identity Governance Overview** - Governance framework for AI agent identities
  https://learn.microsoft.com/en-us/entra/id-governance/agent-id-governance-overview

- **Conditional Access for Agent Identities** - Applying Conditional Access policies to agents
  https://learn.microsoft.com/en-us/entra/identity/conditional-access/agent-id
- **Conditional Access for Copilot and AI Security** - Security policies specifically for AI workloads
  https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-copilot-ai-security

Microsoft Learn - M365 Copilot and SharePoint

- **M365 Copilot Oversharing Blueprint** - Microsoft's phased guidance for fixing oversharing before Copilot deployment
  https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-blueprint-oversharing
- **M365 Copilot Architecture, Data Protection, and Auditing** - How M365 Copilot handles data security and audit trails
  https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture-data-protection-auditing
- **SharePoint Advanced Management for Copilot Readiness** - Preparing SharePoint permissions for Copilot deployment
  https://learn.microsoft.com/en-us/sharepoint/get-ready-copilot-sharepoint-advanced-management

Microsoft Security Blogs

- **Four Priorities for AI-Powered Identity and Network Access Security in 2026** - Make every AI agent a first-class identity
  https://www.microsoft.com/en-us/security/blog/2026/01/20/four-priorities-for-ai-powered-identity-and-network-access-security-in-2026/
- **Detecting and Analyzing Prompt Abuse in AI Tools** - Microsoft's approach to prompt injection detection
  https://www.microsoft.com/en-us/security/blog/2026/03/12/detecting-analyzing-prompt-abuse-in-ai-tools/
- **From Oversharing to Optimization: Deploying M365 Copilot with Confidence** - Tech Community guidance on Copilot deployment
  https://techcommunity.microsoft.com/blog/microsoft365copilotblog/from-oversharing-to-optimization-deploying-microsoft-365-copilot-with-confidence/4357963

Security Research and Vulnerability Disclosures

- **EchoLeak (CVE-2025-32711) - Aim Security** - Zero-click Copilot data exfiltration via embedded document instructions, CVSS 9.3
  https://www.hackthebox.com/blog/cve-2025-32711-echoleak-copilot-vulnerability
- **Reprompt (CVE-2026-24307) - Varonis Threat Labs** - One-click Copilot session hijack via URL parameter injection, patched January 2026
  https://www.varonis.com/blog/reprompt
- **Copilot Studio Security Risk - Tenable** - Prompt injection leaked credit card data and modified prices to zero
  https://www.tenable.com/blog/microsoft-copilot-studio-security-risk-how-simple-prompt-injection-leaked-sensitive-data
- **Prompt Injection Attacks in Copilot - Mindgard** - Analysis of prompt injection techniques targeting Microsoft Copilot
  https://mindgard.ai/blog/prompt-injection-attacks-in-copilot

MCP Security Research

- **State of MCP Security - Pynt (Primary Research)** - Analysis of 281 MCP configurations: 9%, 52%, 92% exploit probability at 1, 3, 10 MCPs
  https://www.pynt.io/blog/llm-security-blogs/state-of-mcp-security
- **MCP Stacks Have a 92% Exploit Probability - VentureBeat** - Coverage of Pynt research on MCP security risk multiplication
  https://venturebeat.com/security/mcp-stacks-have-a-92-exploit-probability-how-10-plugins-became-enterprise
- **We Scanned 1,000 MCP Servers - Enkrypt AI** - Independent scan finding 33% of MCP servers had critical vulnerabilities
  https://www.enkryptai.com/blog/we-scanned-1-000-mcp-servers-33-had-critical-vulnerabilities

Data Exposure and Permissions Research

- **96% Unused Permissions - Oso and Cyera (March 2026)** - 2.4 million workers, 3.6 billion permissions analyzed: 96% of granted permissions never exercised
  https://www.osohq.com/research
- **IBM Cost of a Data Breach Report 2025** - 97% of organizations with AI-related security incidents lacked AI access controls
  https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai
- **IBM Press Release - AI Breach Findings** - 13% reported AI breaches, 97% lacked controls, shadow AI added $670K to breach costs
  https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls
- **Too Much Access: Microsoft Copilot Data Risks - Concentric AI** - 16% of business-critical data overshared across 550 million records analyzed
  https://concentric.ai/too-much-access-microsoft-copilot-data-risks-explained/

Business Central Security Guides

- **Is Copilot in Business Central Secure? - Sikich** - Copilot is not ChatGPT for your ERP. It IS your ERP, with copiloting.
  https://www.sikich.com/insight/is-copilot-in-business-central-secure-what-smbs-need-to-know-and-what-they-dont-need-to-fear/
- **Business Central Security: Complete Guide - Rand Group** - Comprehensive BC security guide covering identity, permissions, and governance
  https://www.randgroup.com/insights/microsoft/dynamics-365/business-central/business-central-security-a-complete-guide-to-identity-permissions-and-governance/
- **Segregation of Duties in Business Central - Rand Group** - SoD principles and implementation in BC
  https://www.randgroup.com/insights/microsoft/dynamics-365/business-central/microsoft-dynamics-365-business-central-segregation-of-duties/
- **Segregation of Duties in Business Central - ERP Software Blog** - Practical SoD guidance for BC environments
  https://erpsoftwareblog.com/2025/05/making-sense-of-segregation-of-duties-in-business-central/
- **BC Permission Management Guide - ERP Software Blog** - Step-by-step permission set management
  https://erpsoftwareblog.com/2025/07/business-central-permission-management-guide/

- **BC Audit Trail in a Real Audit - ERP Software Blog** - How Change Log performs in actual audit scenarios
  https://erpsoftwareblog.com/2026/02/business-central-audit-trail-in-a-real-audit/
- **BC Permission Sets and Security Groups - ArcherPoint** - Permission sets and security groups explained (Part 1)
  https://archerpoint.com/business-central-permission-sets-and-security-groups-pt-1/
- **Permissions, Security, and Security Filters - ArcherPoint** - Security filters and row-level access (Part 2)
  https://archerpoint.com/permissions-security-and-security-filters-in-bc-part-ii/
- **Understanding Permission Sets - Stoneridge Software** - Permission set fundamentals for BC administrators
  https://stoneridgesoftware.com/understanding-permission-sets-in-dynamics-365-business-central/
- **Segregation of Duties in BC - 2-Controlware** - SoD implementation patterns for BC
  https://www.2-controlware.com/blogs/2024/segregation-of-duties-in-business-central/

Copilot Readiness and Governance Guides

- **Microsoft Copilot Enterprise Deployment Guide - EPC Group** - 60-80% of SharePoint sites have oversharing vulnerabilities
  https://www.epcgroup.net/microsoft-copilot-enterprise-deployment-guide-2026
- **Stop Copilot Oversharing in M365 - AdaptSphere** - Practical steps to fix oversharing before Copilot deployment
  https://adaptsphere.ai/stop-copilot-oversharing-microsoft-365/
- **Fix Oversharing Before Copilot Deployment** - SharePoint and OneDrive permission cleanup guidance
  https://helloitsliam.com/2025/12/10/fix-oversharing-in-sharepoint-and-onedrive-before-copilot-deployment/
- **Copilot Governance Checklist 2026 - AltiaTech** - Practical governance checklist using Microsoft Copilot Control System
  https://www.altiatech.com/copilot-in-2026-a-practical-governance-checklist-using-microsofts-copilot-control-system
- **Copilot Readiness Assessment - SysKit** - Assessment framework for Copilot deployment readiness
  https://www.syskit.com/blog/copilot-readiness-assessment/
- **Copilot Security Best Practices - CloudEagle** - Security best practices for Microsoft Copilot
  https://www.cloudeagle.ai/blogs/microsoft-copilot-security-best-practices

AI Agent Security

- **Entra Agent ID Deep Dive - Cloud Partner** - Detailed analysis of Microsoft Entra Agent ID for AI agents
  https://learn.cloudpartner.fi/posts/microsoft-entra-agent-id-agentic-identity-ai-agents
- **AI Agents vs Identity - Petri** - How AI agents challenge traditional identity management
  https://petri.com/ai-agents-vs-identity/
- **Emerging Agentic AI Security Vulnerabilities - Security Boulevard** - Identity-based attack patterns targeting agentic AI systems
  https://securityboulevard.com/2025/07/emerging-agentic-ai-security-vulnerabilities-expose-enterprise-systems-to-widespread-identity-based-attacks/
- **AI Agent Security Best Practices 2026** - Current best practices for securing AI agents in enterprise environments
  https://swarmsignal.net/ai-agent-security-2026/

BC v28 and 2026 Release Coverage

- **What's Coming to BC in 2026 - MSDynamicsWorld** - Comprehensive coverage of BC 2026 features including Agent Designer
  https://msdynamicsworld.com/blog-post/whats-coming-dynamics-365-business-central-2026
- **BC 2026 Release Wave 1 (BC28) Overview** - BC v28 feature summary and analysis
  https://visicnblog.wordpress.com/2026/03/21/dynamics-365-business-central-2026-release-wave-1-bc28/
- **Payables Agent Practical Guide - 4Sight** - Practical implementation guide for the Payables Agent
  https://4sight.cloud/blog/the-payables-agent-in-business-central-a-practical-guide-for-finance-leaders-and-partners
- **Activate and Configure Payables Agent - Crestwood** - Step-by-step Payables Agent activation guide
  https://www.crestwood.com/blog/how-to-activate-and-configure-the-payables-agent-in-dynamics-365-business-central/

Segregation of Duties Reference

- **SoD Examples, Roles, and Violations - Pathlock** - Comprehensive SoD examples across ERP environments
  https://pathlock.com/learn/segregation-of-duties-examples-of-roles-duties-and-violations/
- **Least Privilege for SOC 2 - Konfirmity** - Implementing least privilege for SOC 2 compliance
  https://www.konfirmity.com/blog/soc-2-least-privilege-for-soc-2