

SUCCESS STORY



# Canadian Credit Union

A Case Study By Synchronworks

Editor: Tania Ramkumar

[synchronworks.net](https://synchronworks.net)

[info@synchronworks.net](mailto:info@synchronworks.net)

1.866.960.9409



 **SYNCHROWORKS**

## CONTENTS

<b>1</b>	Facts at a Glance	3
<b>2</b>	Synopsis	4
<b>3</b>	The Challenge	5
<b>4</b>	Business Impact	6
<b>5</b>	Opportunities and Solutions	9
<b>6</b>	The Result	10

# Facts at a Glance

2025 | Financial Services (Credit Union)

## Synopsis

Secure AI adoption initiative to introduce Microsoft 365 Copilot in a regulated environment - supported by governance, training, and workflow automation

## Scope

- Environment Assessment
- Microsoft 365 Copilot Deployment & Enablement
- AI Policy Creation
- Security & Governance Controls
- Change Management & Training
- Post-Deployment Review
- Power Automate Configuration (HR/IT forms)



# TAKING CONTROL OF AI

## From Shadow Use to a Governed Microsoft 365 Copilot Deployment

Synchroworks turned AI risk into AI readiness through a security-first Microsoft 365 Copilot deployment.

### Synopsis

A Canadian credit union noticed growing interest among employees in using AI tools to work more efficiently, along with concern about the use of unapproved, external AI platforms that operate outside organizational security and compliance controls. To address this, the organization wanted a safe, approved way for employees to use AI - without risking sensitive information or creating unmanaged usage.

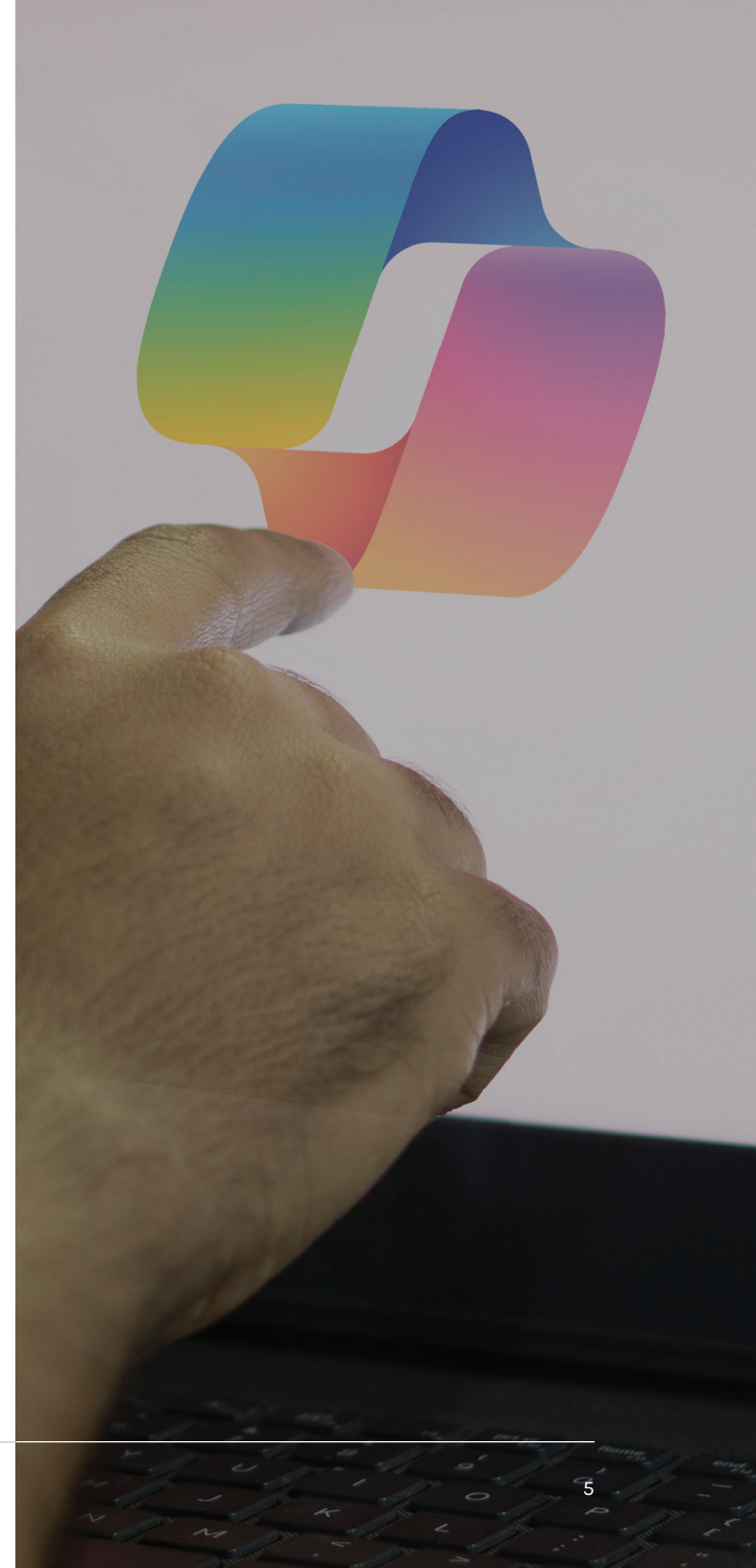
The credit union partnered with Synchroworks to guide the adoption of Microsoft 365 Copilot as a secure, enterprise-approved alternative. Through a structured, security-first rollout that included a clear AI policy, user training, and targeted workflow improvements using Power Automate, Synchroworks helped the organization enable everyday AI use while maintaining control, compliance, and user confidence.

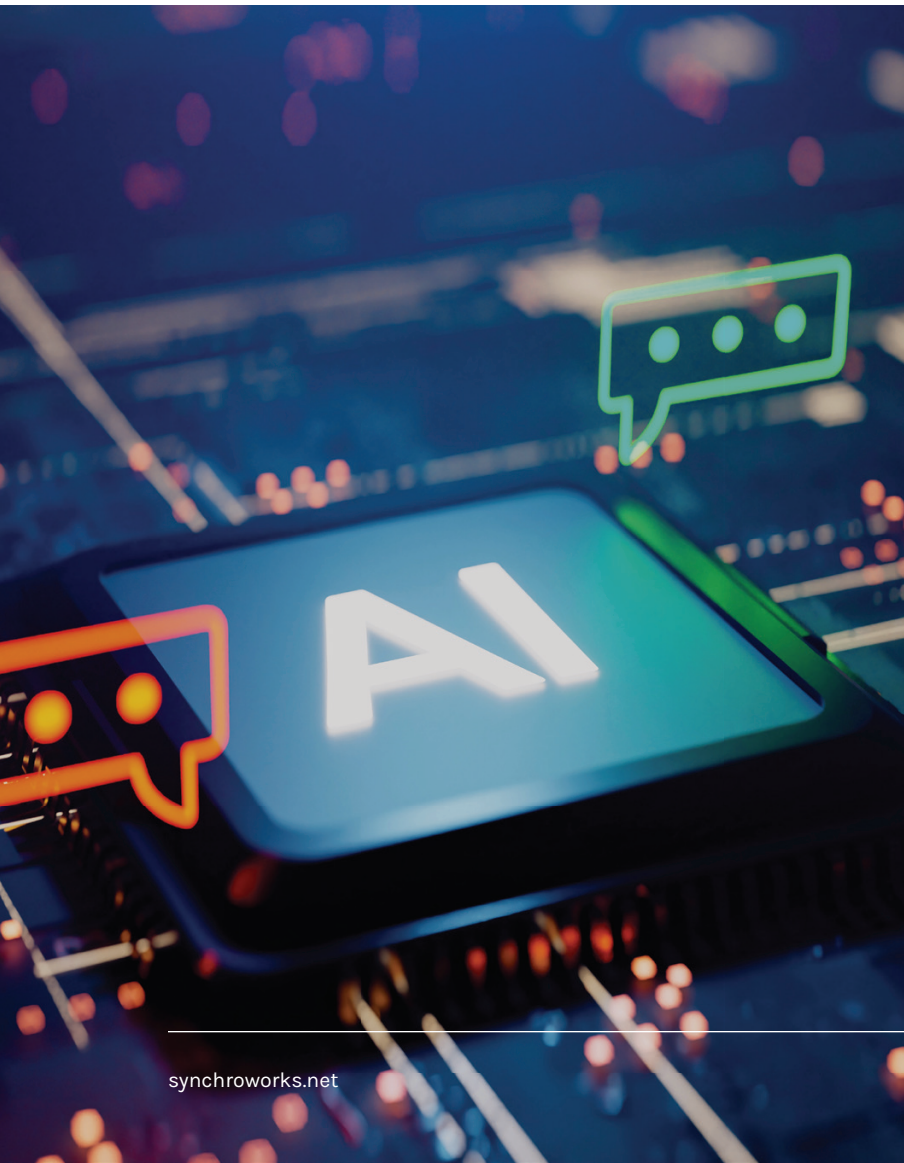
# The Challenge

As AI becomes embedded in everyday productivity tools, the credit union recognized both the opportunity and the responsibility that comes with adoption in a financial services context. Key challenges included:

- Enabling AI in a way that protects member information, financial data, and confidential business information
- Ensuring AI use aligns with regulatory, legal, and contractual obligations
- Preventing inconsistent usage and “shadow AI” tools outside approved platforms
- Establishing accountability so AI supports productivity without replacing professional judgment or internal controls
- Driving adoption through practical enablement to avoid underutilized licenses and uncertainty around “what’s allowed”

The organization required more than a technical rollout - it needed a governance framework, enforceable controls, and user training that would meet financial-industry expectations.





## Business Impact

Without clear governance and structured enablement, AI adoption can introduce:

- 1 Increased risk of sensitive data exposure through prompts or generated content
- 2 Inconsistent use of AI tools across departments and roles
- 3 Reduced trust and adoption due to uncertainty or perceived risk
- 4 Audit and compliance concerns related to retention, oversight, and incident handling

A deliberate approach was required to ensure AI delivered real, day-to-day value while maintaining the same standards of oversight applied to core enterprise systems.

# Opportunities and Solutions

Synchroworks led the organization through an evaluation of available AI options, with a focus on security, governance, and practical integration into existing workflows. Given the credit union's established Microsoft 365 environment, data residency requirements, and need for enterprise-grade controls, Synchroworks recommended Microsoft 365 Copilot as the most appropriate solution. This approach allowed the organization to enable AI productivity quickly while maintaining oversight, auditability, and regulatory alignment.

## OPPORTUNITIES & SOLUTIONS #1

### Environment Assessment & Readiness

Synchroworks assessed the existing Microsoft 365 tenant to confirm Copilot could be deployed securely and effectively, including:

- Review of licensing readiness and rollout approach
- Assessment of information architecture and access controls
- Identification of governance needs for regulated operations
- Alignment of AI usage with existing security, privacy, and records practices

## OPPORTUNITIES & SOLUTIONS #2

### Microsoft 365 Copilot Pilot Deployment & Configuration

Synchroworks delivered a controlled Copilot rollout to a licensed pilot group, ensuring it operated within Microsoft 365 security boundaries:

- Provisioning Copilot access for approved users
- Ensuring Copilot respected existing controls, including:
  - SharePoint, OneDrive, and Exchange permissions
  - Sensitivity labels and Data Loss Prevention (DLP) rules
  - Retention and legal hold policies
- Designing the pilot to support future scaling while maintaining governance maturity

## Change Management & Training

Recognizing that successful AI adoption depends on user understanding and confidence, Synchronworks delivered targeted change management and training to support responsible Copilot use:

- Role-based training focused on practical, day-to-day Copilot use
- Guidance on safe prompting, data handling, and output review
- Clear explanation of approved vs. prohibited AI use
- Reinforcement of human accountability and decision ownership



## AI Policy Creation (Governance Framework)

Synchroworks developed a comprehensive AI governance policy to support responsible, compliant AI adoption aligned with financial industry expectations.

### Approved Use

- Only AI tools approved by IT, Risk, and Compliance may be used
- AI must not make autonomous decisions affecting members
- AI-generated content requires human review and approval before external use

### Data Protection

- Sensitive data may not be entered into AI tools unless formally approved, including:
  - Member personal or financial information
  - Account, transaction, lending, or credit data
  - HR/payroll records
  - Legal privileged materials
  - Security credentials or incident response data
- Permitted use requires data minimization and anonymization where possible

### Governance & Compliance

- Treats AI tools as enterprise systems subject to oversight, auditability, and risk management
- Aligns AI usage with regulatory, legal, privacy, cybersecurity, and records retention requirements
- Complements existing Information Security, Privacy, Acceptable Use, and Incident Response policies

### Scope

- Applies to employees, executives, contractors, consultants, and third parties
- Covers both direct AI use and AI embedded within enterprise platforms

### Microsoft 365 Copilot Controls

- Access limited to licensed, approved, and trained users
- Operates within existing Microsoft 365 permissions and compliance controls
- Users may not access or infer information beyond their role
- Copilot output must be reviewed and is not authoritative legal or financial guidance

### Audit & Oversight

- AI prompts and outputs are corporate records subject to retention and legal hold
- AI usage may be logged and monitored for audit or investigation
- AI-related incidents follow established incident response procedures
- Policy enforcement, ownership, and annual review are defined

### Purpose and Policy Intent

- Enable secure, ethical AI use to improve efficiency and service quality
- Protect member, financial, and confidential business information
- Reinforce that AI supports productivity and analysis - not professional judgment or accountability

### Guiding Principles

- Human accountability
- Least data use
- Security first
- Transparency through review of AI-generated content
- Compliance by design

# The Result

With Synchroworks' structured approach, the credit union established a secure, scalable foundation for AI adoption while delivering practical improvements to everyday work.

Key outcomes included:

- Responsible AI adoption grounded in a formal governance policy aligned to regulated financial services expectations
- Controlled Copilot rollout with clear access rules, training requirements, and output review standards
- Reduced risk of misuse through prohibited data inputs, least-data guidance, and security-first controls
- Improved productivity by enabling AI-assisted drafting, summarization, and internal knowledge work within approved boundaries
- Modernized HR and IT workflows through standardized intake forms and routing, reducing manual effort and improving consistency
- Internal capability uplift through documentation, training, and knowledge transfer to support long-term maintainability

Rather than adopting AI informally, the organization implemented Copilot as an enterprise capability - with governance, accountability, and operational readiness built in.

The credit union is now positioned to expand Copilot usage responsibly and continue modernizing operations through Microsoft 365 and the broader Power Platform.



Microsoft  
Copilot



# Interested in working together?

Let's talk about how we can help  
you harness the power of digital –  
and deliver real results.

---

[synchronworks.net](https://synchronworks.net)  
[info@synchronworks.net](mailto:info@synchronworks.net)  
1.866.960.9409

