

Copyl Papers

Architectural thinking for enterprise AI.

POSITION PAPER 03

Your Team Built 50 AI Apps. Who Owns Them?

AI has made software easier to create. Organisations now need to make it easier to take responsibility for that software.

Rolf Bäck · Founder & Chief Architect, Copyl

6 minute read

Published October 2026

v0.1

Download PDF

WHY THIS PAPER EXISTS

A working app can now start with a prompt.

It can be ready to demonstrate that afternoon. Organisations should welcome that. The harder questions begin when someone starts relying on it.

Who owns it? What can it access? Who supports it when the person who built it leaves?

Building is solved. *Owning* is not.

AI has made software easier to create. Organisations now need to make it easier to take responsibility for that software.

THE SECOND PROBLEM

A useful experiment quietly becomes part of the working day.

A caseworker builds a case board. A controller creates a dashboard. A project lead puts together an agent that drafts replies.

The people closest to the work can turn their ideas into useful tools without waiting for a development project. They can test an approach, learn from colleagues and improve it while the problem is still fresh.

That is worth protecting.

But a working prototype leaves operational questions unanswered. An app may run under a personal account. Its connections may depend on the builder's credentials. Colleagues may start using it before anyone has agreed who maintains it.

The transition can happen quietly. A useful experiment becomes part of the working day. Then its creator changes roles, an integration fails or someone asks for a record of what happened.

By then, the organisation depends on something it has never formally taken ownership of.

Fifty apps can mean fifty separate decisions about access, hosting, integrations and support. Without shared rules, every new app adds another set of responsibilities to discover later.

AN APP AND AN AGENT NEED DIFFERENT CONTROLS

Displaying information is not the same as taking action.

An app that displays information needs appropriate access controls, reliable operation and a named owner.

An agent that takes action needs more. It may update a record, send a message or trigger a process across several systems. The organisation

needs to define what it may do, whose authority it acts under and when a person must approve the next step.

Consider an agent that helps process invoices. Reading an invoice, suggesting an account code and authorising a payment carry different responsibilities. Access to one step should not automatically grant access to the others.

Those boundaries need to be enforced when the action happens. They also need to remain visible afterwards.

A log should help someone establish what the agent accessed, what action it took, which permissions applied and whether a person approved it. Where a decision requires an explanation, the workflow needs to capture the relevant evidence and rationale.

BUILD ANYWHERE. GOVERN EXECUTION IN ONE PLACE.

Keep the builders' tools. Share the way into production.

People should be able to keep using the tools that help them build. The organisation should provide a shared way to connect those tools to business systems, control their actions and operate them over time.

That requires:

Named ownership. Someone is accountable for the app or agent, with an agreed support and handover process.

Separate agent identities. Agents act through assigned identities and permissions instead of inheriting unrestricted access from a builder.

Controlled integrations. Access to business systems is managed through shared connections with defined boundaries.

Approval at the right steps. Actions with significant consequences require human review before execution.

Traceable activity. Records make it possible to investigate actions, approvals and failures.

Explicit data handling. Storage, processing locations and external services are understood and approved.

These controls give builders a clearer route into production. They also reduce the work required to assess each new solution from scratch.

WHERE COPYL FITS

A shared operating layer for AI agents.

[Copyl](#) provides a shared operating layer for AI agents, with identity, permissions, integrations, approval controls and audit trails. Agents can be built in Copyl or with other tools, then connected to business systems through governed execution.

That gives organisations a common foundation for running agents across departments. Teams can develop solutions around their own work while IT manages access and operational controls centrally.

Deployment and data handling still need to be assessed for each solution, including any external model providers or services it uses. A shared platform provides controls; the organisation remains responsible for how they are configured and used.

FIVE QUESTIONS BEFORE AN AI APP GOES LIVE

Before an app or agent touches real business data, ask:

01 Who owns it? Who is accountable now, who supports it and what happens when its creator leaves?

02 What can it access? Which systems and data can it reach, through which identity and with what permissions?

03 What can it do? Which actions may it take independently, and which require approval?

04 Can we reconstruct its activity? If someone asks what happened last Tuesday, can we show the relevant actions, approvals and outcomes?

05 Where does the data go? Where is it stored and processed, and which external services receive it?

If an answer is “we don’t know”, assign an owner to resolve it before the solution becomes part of daily operations.

The ability to build fifty apps is an *opportunity*.

Making ownership, access and support clear is how an organisation gets to keep using them.

Already running a growing collection of AI apps or agents? [Talk to Copyl](#) about bringing them into governed operation.

RELATED READING

AI Agents Are Users, Not Features

The Deployment Lifecycle of AI Agents

Agent-as-a-User Pattern

ABOUT THE AUTHOR



Rolf Bäck

Founder & Chief Architect, Copyl

Rolf has spent more than 30 years building enterprise software platforms. Since 2011 he has led the development of Copyl, an enterprise platform for business applications, automation and AI. His current work focuses on how AI agents become governed participants in enterprise systems rather than isolated assistants.

- Founder of Copyl
- Enterprise software architect
- Working on enterprise AI architecture since 2022
- Based in Sweden

ABOUT COPYL

Copyl is an Enterprise AI Operating System that enables organizations to deploy, govern and orchestrate AI agents alongside business applications, APIs and automations on a single platform.

[copyl.com](#) · [Why Copyl](#) · [Design Patterns](#)

[Other papers](#)

[Design Patterns](#)

[Why Copyl](#)

[Download PDF](#)

The Operating System for Autonomous Organizations.

Building Trusted Autonomy™

Product

[Agent Hub](#)

[Solutions](#)

[Marketplace](#)

[AI transformation](#)

[Why Copyl](#)

[Enterprise Agent Operating System](#)

[AI Execution Platform](#)

[Digital Workforce Platform](#)

[AI Agent Governance](#)

[AI Integration Platform](#)

Insights

[Position Papers](#)

[AI Agents Are Users, Not Features](#)

[Design Patterns](#)

[Blog](#)

[ROI Calculator](#)

[Compliance](#)

[Sovereign & On-Prem](#)

[Developers & Companies](#)

Company

[Pricing](#)

[About us](#)

[Why Copyl](#)

[Become a partner](#)

[Contact](#)

[LinkedIn](#)

Legal

[Terms & Conditions](#)

[Privacy Policy](#)

[Cookie settings](#)

Enterprise Agent Operating System, AI execution platform, digital workforce, agent governance, multi-agent orchestration, Copyl.

Thoughts on AI

A short weekly note on enterprise AI, agent governance, and operational context—not hype.

Name

Work email

Language

☐ SV ☒ EN

► What interests you? (optional)

I agree to receive Thoughts on AI by email up to twice a month. I can unsubscribe anytime. See our [Privacy Policy](#) for how we handle your data.

Subscribe

Helsingborg, Sweden

© 2007–2026 Copyl AB. All rights reserved.