verovia

The Fastest Path To Industrial AI

Governance & Security



Controlled execution: AI agents that do real work in your systems, inside limits you set.

An agent that can change records and send messages can also make costly mistakes. Operations leaders worry about changes nobody approved and about company data quietly leaving the building. When an auditor asks who signed off on a purchase, someone has to have the answer. Verovia puts a governance gate in front of every agent action. Each action is recorded before it runs and checked against your rules, and anything risky waits for a person you name.

Large purchases go to the right approver

Set limits on amounts and bulk deletes. Anything over the line waits for a named person in Teams, and the record shows who said yes.

Work keeps moving

Checks are designed to add under 30 ms per action. Only what your rules mark as risky stops for a person.

You decide what each agent can touch

One set of rules covers Business Central, Outlook, Teams and MCP clients. Start in monitor-only mode and enforce one rule at a time when you're ready.

Records your auditor can verify

Each action is sealed in a tamper-evident chain and mapped to 19 frameworks, including OSHA PSM, ISO 45001 and ISO/IEC 42001.

Every agent action is recorded and decided before it runs

Agent asks to act — in chat, Teams or MCP → **Recorded first** — no record, no change → **Your rules decide** — deny, hold or check → **Mentor check** — can flag or block

- **Allowed** — runs as asked
- **Flagged** — reviewed, or held for approval
- **Denied** — not run, and the agent is told

Sealed in the tamper-evident audit chain
Verify it in one click. Export it for your auditor.

insidesales@verosoftdesign.com

Verosoft

verovia

What's in the governance layer

Audit trail

Each agent action is recorded as it happens: the agent, the person it acted for, the tool, the data and the result.

Records outlive deleted conversations and users. Kept 2 years by default, adjustable from 1 to 10.

Tamper-evident chain

Every record is sealed to the one before it with a SHA-256 hash. **Verify chain** confirms nothing was changed or removed.

The database refuses edits and deletes of audit records.

Policies

Admins write rules in plain words, such as "hold deletes of more than 10 records".

Monitor-only mode shows what a rule would catch before you enforce it. Each version keeps its author and reason.

Verovia check

An AI reviewer screens risky actions as they happen and flags requests nobody made or data heading outside the company.

It can flag or block. Approval stays with a person. It never reads tool outputs, where injected instructions hide.

Holds & approvals

Sensitive actions wait for a named approver, who gets a Teams message.

When an action is routed to someone else, the person who asked for it can't approve it.

Suggestions

The assistant reads the audit trail and proposes rule changes with the evidence attached.

Nothing goes live until an admin publishes it.

Compliance

Requirements from 19 frameworks map to live platform controls. Each one shows Met or Gap, with a one-click Fix.

Statuses come from your real settings and can't be set by hand.

Pause, export and auditor access

Pause an agent in one click, or let it pause itself after repeated denials. Export the trail as CSV or JSON with personal details removed.

Auditors get a read-only role.

Evidence for the frameworks your auditors use

19 frameworks, 14 platform controls

Pick the frameworks that apply to you. Each requirement shows as Met, Gap, Yours or Not applicable. Verovia supplies the controls and the evidence. Certification belongs to your organization and its auditor.

Industrial safety & quality

OSHA PSM · OSHA lockout/tagout
MSHA Part 56 · ISO 45001
ISO 9001 · ISO 55001

Manufacturing, mining, energy, asset-heavy operations

AI governance

ISO/IEC 42001 · NIST AI RMF
OWASP Top 10 for Agentic Applications
Verovia AI governance baseline

Any team putting agents to work

Security

ISO/IEC 27001 · SOC 2 · IEC 62443
Saudi NCA ECC, including OT controls

IT, security and OT teams

Works inside the Microsoft tools you already run

Governance sits where your teams already work. Nothing new to learn, and no separate security product to buy.

Dynamics 365 · Microsoft 365 · Copilot · Azure · Microsoft Entra ID

Business Central & Mobi

Work orders, assets, purchases and users are governed first. Rules on amounts and bulk deletes protect your ERP data.

Outlook & Teams

Mail leaving your domains is flagged as external. Approval requests arrive in Teams.

MCP clients

Agents connected from other clients pass through the same gate.

Bought with your licences

Verosoft is a tier-one Microsoft CSP and can bundle governed AI with the licences you already buy.

insidesales@verosoftdesign.com

Verosoft