Aligning information technology and supply chain management through decision governance

Information technology and supply-chain management need a shared way to govern operational decisions. IT protects architecture, access, data and system integrity. Supply-chain leaders own service, cost, inventory and operating policy. When AI agents begin recommending or initiating actions, both sides need to agree what the agent may do, what evidence is required and when a person must decide.

Why shadow automation appears

Teams often introduce scripts, copilots or agent workflows to reduce manual work. These experiments can solve a local problem while leaving unanswered questions: Which data may the agent use? Who owns the rule? Can it change a purchase order, inventory allocation or transport booking? Where is the approval recorded? What happens when connected systems disagree?

If those questions are addressed only after a pilot succeeds, the organisation may discover that a useful prototype cannot pass security, controls or operational review. Shared decision governance brings those considerations into the workflow design from the start.

Define decision authority as an operational control

A workable framework separates four concerns:

- Identity and access: which person or service may connect to which system.
- Decision authority: which role may approve which business choice, within what limits.
- Execution scope: which specific action may be sent to a protected workflow after approval.
- Evidence and outcome: what context, policy, approval, execution response and result are retained.

These controls complement one another. System access does not automatically grant authority to make every business decision. Likewise, a model evaluation or AI policy does not by itself identify the person accountable for changing an operational commitment.

Build a joint operating model

For each candidate use case, appoint an operational owner and a technical owner. The operational owner defines the decision, constraints, escalation paths and success measures. IT and security assess data access, identity, deployment boundaries, integration patterns and monitoring. Finance, quality, procurement or customer service joins where the decision affects its controls or commitments.

Document the decision envelope in plain language: permitted inputs, excluded data, applicable policies, approval thresholds, execution endpoint, failure behaviour and evidence retained. Include a manual fallback. Test normal cases, policy exceptions, missing evidence, stale data and rejected execution requests. Only widen an agent’s scope after the pilot’s evidence and approvals support doing so.

What to measure

Measure process performance and control quality together. Useful indicators include decision cycle time, percentage routed to human review, policy overrides, incomplete evidence, failed hand-offs and outcome reconciliation. A faster process that bypasses the right owner is not a successful control design.

Where Aidecis fits

Aidecis keeps one authority model and one decision record across your people, your own algorithms and every vendor’s agents. Aidecis never writes into your systems: your people, systems or bots execute the approved action, and Aidecis reads each execution back and reconciles it against the approval, so SAP stays your single source of truth. With enforced control, your own integration checks Aidecis's single-use grant before it executes. Agents and algorithms that write in their own systems are checked against their registered role and limits afterwards, and flagged within minutes if they went outside them: observed control, which does not prevent an action but shows it. It does not replace identity management, ERP permissions or an organisation’s AI governance programme. A pilot can help IT and supply-chain leaders test one decision path and agree the controls before scaling.

See how the Aidecis workflow is designed and discuss a pilot.

Copyright 2026 Aidecis