novaeon

THE CHECKLIST · 40 CHECKPOINTS

Taking AI agents to production

Novaeon Studio · Maik Buchenau · As of November 2026

An AI agent acts inside finance, HR, procurement or sales, with real authorizations and real consequences. This checklist treats every agent like any other change in SAP: inventoried, rated, tested, approved, monitored and reversible, like a transport. It works for SAP Joule agents (used as the example throughout), custom agents on SAP BTP and agents from other vendors that touch your SAP data. 40 checkpoints in 9 blocks. Tick them off, flag the gaps, name an owner for each.

> Note: SAP is evolving Joule and Joule Studio very fast. Check dates, prices and availability (GA/EA/roadmap) against current SAP documentation and your own contract before any decision. General information, not legal advice. Drafted with AI.

1 Inventory & ownership

- [ ] Every agent has a **business owner** (process accountability) and a technical owner (operations).
- [ ] Every agent is in **one inventory**, including the models, skills, sub-agents and MCP servers it uses. For SAP landscapes this is the **SAP AI Agent Hub** (from LeanIX), which also lists agents from other vendors.
- [ ] Purpose, process, affected systems and data categories are documented in one sentence ("What may this agent do, and what not?").
- [ ] Agents outside SAP that access SAP data (Copilot, custom agents via A2A/MCP) are in the same inventory.

2 Risk & autonomy

- [ ] Each agent has a risk rating (e.g. low / medium / high) based on impact: money, people, customers, compliance.
- [ ] The **autonomy level** is a deliberate decision: suggest only · act with approval · act autonomously.
- [ ] **Human-in-the-loop** is configured for every high-risk step (a person approves, not just a log entry).
- [ ] Checked whether the use case falls under **EU AI Act Annex III** (e.g. hiring, promotion, performance evaluation). High-risk obligations apply from 2 Dec 2027.

3 Identity & authorizations

- [ ] The agent acts only with the requesting user's permissions (intersection of user and agent); autonomous agents have their **own technical identity**.
- [ ] The agent's roles and authorizations are described in the authorization concept and approved. No "SAP_ALL for the bot".
- [ ] Outbound connections (destinations, OAuth) follow the pattern client credentials (machine-to-machine) or JWT bearer (user propagation); no secrets in code.
- [ ] Custom agents running on BTP Cloud Foundry are secured with IAS. Otherwise they are reachable from the internet by default.
- [ ] Only **verified MCP servers** are called in production.

4 Data & grounding

- [ ] Uploaded grounding documents reviewed: in Joule they are visible to **all users of the tenant** (no per-document permissions). Upload nothing confidential.
- [ ] Master data quality for the process assessed (an agent working on bad data just makes wrong decisions faster).
- [ ] Decision taken on the vendor's use of customer data (for SAP: opt-out in SAP for Me); logging opt-in set deliberately.
- [ ] Data protection: records of processing, DPIA where needed, and data center region (e.g. EU Access) documented.

5 Testing & evaluation

- [ ] Test cases exist for the main flows **and** for edge cases (missing data, conflicting instructions, aborted runs).
- [ ] Security tests: prompt injection, tool misuse, data leakage through answers.
- [ ] Evaluation scenarios with expected results; acceptance criteria agreed up front (e.g. hit rate, error tolerance).
- [ ] Tests check not only that tools are **discovered** but that they are actually **invoked** (discovery ≠ invocation): a tool that shows up in the list is no proof the agent can call it, so test real calls end to end.
- [ ] Regression test planned after every SAP release update and every agent change.

6 Transport & approval

- [ ] Separate development → test → production environments; no building directly in production.
- [ ] Transport path defined: Joule Studio classic via **Cloud Transport Management** (MTA); new Joule Studio via Git-based deployments; custom agents through your own CI/CD pipeline.
- [ ] Every change (prompt, instructions, tools, model switch) is **versioned** and goes through the same approval as code.
- [ ] Formal approval before go-live (change request, approver, date), e.g. in **SAP Cloud ALM**.
- [ ] Release dependencies clarified: Joule features only arrive with current releases. Your upgrade calendar is your AI calendar.

7 Operations & monitoring

- [ ] Ongoing monitoring: usage, error rate, response times, aborts (Agent Hub / Cloud ALM where available).
- [ ] Traceability: audit trail per session showing who triggered what, with which result.
- [ ] Behavioral drift watched (e.g. process/agent mining in Signavio, spot checks by the owner).
- [ ] Incident process: a named person is alerted when an agent acts wrongly, and a named person (usually the business owner) is allowed to switch it off.

8 Cost

- [ ] Consumption estimated per agent: SAP agents **0.02 AI Units per agent action** (2026); custom agents by resource consumption.
- [ ] End of free runtime for custom Joule agents (**31 Dec 2026**) included in the 2027 budget.
- [ ] Budget **per agent**, not per user; warning threshold and hard cap defined (AI Units expire after 12 months).
- [ ] Contract terms negotiated: price per AI Unit, allowance, overage rate, and whether unused units can be carried forward (by default they expire after 12 months).
- [ ] Deterministic steps built as **skills** rather than agent steps (Joule skills aren't charged per call).

9 Works council, rollback & retirement

- [ ] **Works council** involved early where co-determination applies. In Germany: § 90 BetrVG (explicitly covers AI) and § 87(1) no. 6 BetrVG (systems able to monitor behavior or performance). Usually this needs a works agreement.
- [ ] Rollback plan tested: restore the previous version or switch the agent off without stopping the process (manual fallback).
- [ ] Retirement criteria defined (value, cost, error rate) and a regular review date set per agent.
- [ ] Retirement cleans up: authorizations, destinations, inventory entry, grounding documents.

Novaeon Studio — SAP release and change management meets AI agents.
Want to walk through your agents against this list? Book a 30-min call: https://novaeon.studio/#contact · office@novaeon.studio