novaeon

检查清单 · 40 个检查点

AI 智能体投产

Novaeon Studio · Maik Buchenau · 2026 年 11 月版

AI 智能体在财务、人力资源、采购或销售中执行操作，拥有真实的权限，也会产生真实的后果。本清单将每个智能体视同 SAP 中的任何其他变更：纳入清册、评定风险、完成测试、获得审批、持续监控，并且像传输（Transport）一样可以回退。它适用于 SAP Joule 智能体（全文以其为例）、基于 SAP BTP 的自建智能体，以及访问您 SAP 数据的其他供应商的智能体。共 9 个模块、40 个检查点。请逐项勾选，标记缺口，并为每一项指定负责人。

> 注意：SAP 对 Joule 和 Joule Studio 的更新非常快。在做出任何决策之前，请对照最新的 SAP 文档和您自己的合同核实日期、价格和可用性（GA/EA/路线图）。本文为一般性信息，不构成法律意见。由 AI 辅助起草。

1 清册与责任归属

- [ ] 每个智能体都有一名**业务负责人**（对流程负责）和一名技术负责人（负责运维）。
- [ ] 每个智能体都登记在**同一份清册**中，包括其使用的模型、技能、子智能体和 MCP 服务器。对于 SAP 系统环境，这就是 **SAP AI Agent Hub**（源自 LeanIX），它同样会列出其他供应商的智能体。
- [ ] 用一句话记录用途、流程、涉及的系统和数据类别（“该智能体可以做什么，不可以做什么？”）。
- [ ] 访问 SAP 数据的 SAP 之外的智能体（Copilot、通过 A2A/MCP 接入的自建智能体）登记在同一份清册中。

2 风险与自主程度

- [ ] 每个智能体都根据影响范围（资金、人员、客户、合规）进行风险评级（例如低 / 中 / 高）。
- [ ] **自主级别**经过明确决策：仅提供建议 · 经审批后执行 · 自主执行。
- [ ] 每个高风险步骤都配置了**人工审批环节（human-in-the-loop）**（由人员审批，而不仅仅是一条日志记录）。
- [ ] 已核查该用例是否属于**欧盟《人工智能法》附件三**的范围（例如招聘、晋升、绩效评估）。高风险义务自 2027 年 12 月 2 日起适用。

3 身份与权限

- [ ] 智能体仅以发起请求的用户的权限执行操作（用户权限与智能体权限的交集）；自主运行的智能体拥有**独立的技术身份**。
- [ ] 智能体的角色和权限已在权限概念中描述并获得批准。不允许“给机器人分配 SAP_ALL”。
- [ ] 出站连接（Destination、OAuth）采用客户端凭据（机器对机器）或 JWT bearer（用户传播）模式；代码中不包含任何密钥。
- [ ] 运行在 BTP Cloud Foundry 上的自建智能体已通过 IAS 加以保护。否则它们默认可从互联网访问。
- [ ] 生产环境中只调用**经过验证的 MCP 服务器**。

4 数据与知识依据（Grounding）

- [ ] 已审查上传的 Grounding 文档：在 Joule 中，这些文档对**租户的所有用户**可见（不支持按文档设置权限）。请勿上传任何机密内容。
- [ ] 已评估该流程的主数据质量（基于劣质数据工作的智能体只会更快地做出错误决策）。
- [ ] 已就供应商使用客户数据的问题作出决定（对于 SAP：在 SAP for Me 中选择退出）；日志记录的选择加入（opt-in）经过审慎设置。
- [ ] 数据保护：已记录处理活动记录、必要时的数据保护影响评估（DPIA）以及数据中心区域（例如 EU Access）。

5 测试与评估

- [ ] 针对主要流程**以及**边界情况（数据缺失、指令冲突、运行中断）均有测试用例。
- [ ] 安全测试：提示词注入、工具滥用、通过回答造成的数据泄露。
- [ ] 具备带有预期结果的评估场景；验收标准已事先约定（例如命中率、容错度）。
- [ ] 测试不仅检查工具能否被**发现**，还检查工具是否真正被**调用**（发现 ≠ 调用）：工具出现在列表中并不能证明智能体能够调用它，因此请端到端测试真实调用。
- [ ] 已计划在每次 SAP 版本更新和每次智能体变更后进行回归测试。

6 传输与审批

- [ ] 开发 → 测试 → 生产环境相互分离；不直接在生产环境中构建。
- [ ] 传输路径已定义：经典版 Joule Studio 通过 **Cloud Transport Management**（MTA）；新版 Joule Studio 通过基于 Git 的部署；自建智能体通过您自己的 CI/CD 流水线。
- [ ] 每项变更（提示词、指令、工具、模型切换）都进行**版本管理**，并与代码经过相同的审批流程。
- [ ] 上线前有正式审批（变更请求、审批人、日期），例如在 **SAP Cloud ALM** 中。
- [ ] 已理清版本依赖关系：Joule 功能只随最新版本提供。您的升级日历就是您的 AI 日历。

7 运维与监控

- [ ] 持续监控：使用量、错误率、响应时间、中断情况（如可用，通过 Agent Hub / Cloud ALM）。
- [ ] 可追溯性：每个会话都有审计跟踪，记录谁触发了什么操作以及结果如何。
- [ ] 监测行为漂移（例如在 Signavio 中进行流程 / 智能体挖掘，由负责人进行抽查）。
- [ ] 事件处理流程：智能体执行错误操作时，会通知一名指定人员；并由一名指定人员（通常为业务负责人）有权将其关闭。

8 成本

- [ ] 已按智能体估算消耗：SAP 智能体**每次智能体操作 0.02 AI Units**（2026 年）；自建智能体按资源消耗计算。
- [ ] 自建 Joule 智能体免费运行期的结束（**2026 年 12 月 31 日**）已纳入 2027 年预算。
- [ ] 预算**按智能体**而非按用户编制；已定义预警阈值和硬性上限（AI Units 在 12 个月后过期）。
- [ ] 已谈定合同条款：每 AI Unit 的价格、额度、超额费率，以及未使用的额度能否结转（默认情况下 12 个月后过期）。
- [ ] 确定性步骤以**技能（Skill）**而非智能体步骤的形式构建（Joule 技能不按调用次数计费）。

9 职工委员会、回退与停用

- [ ] 在涉及共同决定权的情况下，尽早让**职工委员会（Betriebsrat）**参与。在德国：§ 90 BetrVG（明确涵盖 AI）和 § 87(1) no. 6 BetrVG（能够监控行为或绩效的系统）。通常需要签订一份企业协议。
- [ ] 回退计划已经过测试：恢复到上一版本，或在不中断流程的情况下关闭智能体（手动替代方案）。
- [ ] 已定义停用标准（价值、成本、错误率），并为每个智能体设定定期评审日期。
- [ ] 停用时进行清理：权限、Destination、清册条目、Grounding 文档。

Novaeon Studio — 当 SAP 发布与变更管理遇上 AI 智能体。
希望对照本清单逐一梳理您的智能体？欢迎预约 30 分钟通话：https://novaeon.studio/zh/contact/ · office@novaeon.studio