MCP-readiness checklist

12 vragen voor uw IT-leverancier vóór u investeert in agentic AI

Agentic AI staat of valt met de koppeling naar uw bedrijfssystemen. Model Context Protocol (MCP) is de open standaard die die koppeling de afgelopen 18 maanden heeft gedefinieerd. Gebruik deze twaalf vragen om in één gesprek vast te stellen of een leverancier daar serieus mee bezig is — of dat ze "agentic AI" verkopen met de aanpak van 2023.

Sectie A — Architectuur & standaarden

- [ ] 1. Werkt jullie agent-implementatie via Model Context Protocol (MCP), of via maatwerk-API-koppelingen per systeem?
  Waarom: maatwerk-koppelingen zijn duurder en kortlevender dan MCP-servers. Een leverancier zonder MCP-aanpak in mei 2026 is niet bijgebleven.
- [ ] 2. Welke MCP-servers gebruiken jullie standaard, en welke onderhouden jullie zelf?
  Waarom: zelf onderhouden klinkt sterk maar betekent ook risico. Open-source community-servers zijn meestal de veiligste keus.
- [ ] 3. Op welk agentplatform draait jullie oplossing (Claude, OpenAI, Microsoft, lokaal model)? Kan ik later wisselen zonder de koppellaag te vervangen?
  Waarom: dit toetst of de leverancier daadwerkelijk standaarden gebruikt of doet alsof.
- [ ] 4. Hebben jullie ervaring met MCP-implementaties in Nederlandse boekhoud- of ERP-systemen (Exact, AFAS, Twinfield, Yuki)?
  Waarom: het MCP-landschap voor de Nederlandse stack is dun. Eerlijk antwoord (of het wel/niet eerder is gedaan) is meer waard dan een geruststelling.

Sectie B — Uw systemen & data

- [ ] 5. Welke van mijn systemen kunnen vandaag via een bestaande MCP-server worden aangesproken, en welke vragen om maatwerk?
  Waarom: dwingt de leverancier om concreet over úw landschap na te denken, niet alleen over generieke demo's.
- [ ] 6. Hoe stellen jullie vast welke acties de agent mag uitvoeren — lezen, schrijven, goedkeuren — en op welk niveau?
  Waarom: een agent met onbeperkte schrijftoegang is een productie-incident dat staat te wachten.
- [ ] 7. Krijg ik een auditlog van alle acties die de agent via MCP-servers uitvoert? Met welk detailniveau?
  Waarom: zonder logs is governance fictief. AVG/GDPR maakt dit verplicht.
- [ ] 8. Hoe gaan jullie om met persoonsgegevens die door de agent worden gelezen of geschreven? Welke modellen draaien waar, en wat is jullie verwerkersovereenkomst?
  Waarom: dit raakt direct aan AVG-compliance. Vermijd partijen die hier vaag op blijven.

Sectie C — Beheer & continuïteit

- [ ] 9. Wat gebeurt er als een MCP-server (van jullie of van een derde partij) een breaking change doorvoert? Wie patcht, op welke termijn?
  Waarom: open-source servers worden onderhouden door derden. Wie hangt aan welke server is een operationele vraag.
- [ ] 10. Is er een testomgeving waarin we de agent eerst kunnen laten "droog draaien" tegen een kopie van onze systemen voordat hij in productie schrijft?
  Waarom: een leverancier die dit niet aanbiedt, verwacht dat u op vertrouwen produceert.
- [ ] 11. Hoeveel kost een typische uitbreiding (een extra systeem aansluiten) ná de eerste implementatie? Geef een richtbedrag.
  Waarom: marge op uitbreidingen is waar slechte deals zich verstoppen. Een eerlijk antwoord is een open antwoord.
- [ ] 12. Welke afhankelijkheden creëren we door voor jullie te kiezen? Wat hebben we nodig om over twee jaar moeiteloos van leverancier te kunnen wisselen?
  Waarom: de meest informatieve vraag van de twaalf. Een partij die hier helder antwoord geeft, weet wat ze doen.

De juiste antwoorden klinken concreet, met namen van systemen en versies. De verkeerde klinken als "dat regelen we wel". U weet zelf welke kant van die scheidslijn u in uw kantoor wilt hebben.

> Vragen of een tweede mening over de antwoorden die u krijgt?
> Wij denken vrijblijvend mee.
> spiescreations.nl