



id: SI_002

model: deepseek/deepseek-v3.2

seeds:

04_risiko: sårbarhet

03_relasjon: tillit

05_handling: vent

01_perspektiv: bruker

02_tidhorisont: kortsiktig

Instans SI_002

Seeds: bruker | kortsiktig | tillit | sårbarhet | vent

Din **kortsiktig** fokus på å «oppgradere» kan underminere **tillit** hvis swarm blir et uforståelig orakel. I et strengt helsemiljø er **sårbarhet** ved dataleakage fatal. **Vent** derfor med proprietære rammeverk (CrewAI) — de krever lokal kjøring og nytt governance.

Konkrete valg:

1. **Arkitektur:** Bruk Azure OpenAI (GPT-4) + Azure Logic Apps som orkester. Unngå Copilot Studio for swarm—den er for **bruker**-sentrert automasjon, ikke tung agent-orkestrering. Bygg Python-agenter i Azure Container Instances (serverless) for Case 2. Dette bevarer Microsoft-investering og sikkerhet.
2. **Spesialisering (Case 1):** Ikke lag 100 agenter. Start med 5-7 roller (f.eks. «Regelverksfortolker», «Pasientsikkerhetsvurderer», «Kostnadsanalytiker»). Gi hver en unik systemprompt og tilgang til forskjellige datakilder (SharePoint-mapper, Dataverse-tabeller) via søk med Azure AI Search (data forblir i miljøet). Aggreger med en «synteser»-agent som prioriterer konsensus og flagger dissens.
3. **Inbox (Case 2):** Bruk Azure Service Bus som kø. Hver agent-instans henter en case, prosesserer med en felles, parametrisert systemprompt (variabler for kompleksitet), og skriver til en results-tabell i Dataverse. Implementer et «quality gate»-script som sjekker resultatkonsistens for de 10% mest varierende casene.

Failure mode: Swarm er ikke riktig for enkle, lineære oppgaver eller der forklarbarhet er lovpålagt. Kompleksiteten skyter i været.



Neste steg:

1. Sett opp en pilot med 3 spesialiserte Azure OpenAI-agenter som analyserer én konkret problemstilling med data fra en begrenset SharePoint-mappe (kun indeksert søk, ingen raw data-utlevering).
2. Implementer detaljert logging av token-forbruk og feilrater per agent i Azure Monitor for å kvantifisere kostnad og pålitelighet før skaling.
3. Etabler en godkjenningssøknad for dataflyt mellom Dataverse og Azure OpenAI-tjenesten med juridisk avdeling for å adressere **sårbarhet**.