



id: SI_005

model: deepseek/deepseek-v3.2

seeds:

04_risiko: sårbarhet

03_relasjon: makt

05_handling: vent

01_perspektiv: økonomisk

02_tidhorisont: langsiktig

Instans SI_005

Seeds: økonomisk | langsiktig | makt | sårbarhet | vent

Arkitektur: Cloud-only med streng helsedata gir makt via Azure OpenAI-agenter direkte i Python på Azure Container Instances (ACI). **Trade-off:** Copilot Studio er “locked-in” og saknar swarm-sårbarhet ved kost-kontroll. Proprietære rammeverk (CrewAI) gir fleksibilitet, men øker økonomisk risiko ved eksterne APIer. Microsoft-preservering krever Azure-basert orkestering med Azure Functions som dispatcher og Entra ID-autentisering.

Spesialisering: For Case 1, ikke dupliser prompt. Gi hver agent en “seed”-rolle med kontekst fra Dataverse via SQL-injection (f.eks., `SELECT regulatory_clauses WHERE topic=@problem`). Aggreger output med en “sentinel”-agent som bruker clustering-algoritme for å identifisere konsensus og dissens – dette motvirker kaos.

Inbox-modell: For Case 2, bruk Azure Queue Storage. Hver agent tar en case, men alle deler en core prompt-template med dynamisk parameter-fylling (`{{case_specifics}}`) fra databasen. Consistency sikres med en valideringsagent som scorer outputs før aggregering.

Data-injection: Bruk Azure AI Search med indekserte SharePoint-/Dataverse-data. Agentene spør indeksen via Azure OpenAI’s grounding features. **Kritisk sikkerhet:** All data forblir i tenant; bruk privat endpoint til Azure OpenAI og audit logging.

Observerbarhet: Track med Application Insights for hver agent-container. Mål: token/agent, latency, error rate. **Cost-ROI:** Batch-scheduling på timer (ikke real-time). Cache felles kontekst i Azure Redis. Fallback til GPT-3.5-Turbo for mindre kritiske agenter.

Transition: Fra Copilot til swarm er en langsiktig prosess. **Fase 1** (3 måneder): Bygg en 5-agent pilot for en analyse-case med konkret ROI-måling. **Quick win:** Automatiser compliance-check av 100 dokumenter parallelt, demonstrer tid- og kostbesparing.

**Neste steg:**

1. Utfør en 2-weeks proof-of-concept med 3 spesialiserte Azure OpenAI-agenter på en isolert helsedataset.
2. Design og implementer en Azure AI Search-indeks for valgt SharePoint-compliance-dokumentasjon.
3. Sett opp Application Insights-dashboard for token-forbruk og agent-latency i POC-en.