



id: SI_008

model: qwen/qwen3.6-plus

seeds:

04_risiko: sårbarhet

03_relasjon: tillit

05_handling: implementer

01_perspektiv: operasjonell

02_tidhorisont: langsiktig

Instans SI_008

Seeds: operasjonell | langsiktig | tillit | sårbarhet | implementer

1. Arkitektur: Azure OpenAI + Azure Functions + Service Bus er eneste rasjonelle valg. Copilot Studio er locked til dialogflyt; eksterne rammeverk bryter tillit og dataresidens. Azure-native gir Entra ID, private endpoints og operasjonell kontroll. Trade-off: høyere dev-kost vs. langsiktig compliance.

2. Spesialisering: Unngå prompt-duplikering. En router-agent dispatch-oppgaver til spesialiserte sub-swarms.

```
roles = {"regulatory": SYS_REG, "cost": SYS_COST}
tasks = [f"{prompt}\nKontekst:{filtered_context}" for prompt in
roles.values()]
results = await asyncio.gather(*[aopenai.chat(m=[{"role":"system","content":t}])
for t in tasks])
```

Aggreger via synthesizer-agent med streng JSON-schema validering og vektet konsensus. Eliminerer meningskaos.

3. Inbox-modell: Service Bus queue + Azure Container Apps (scale 0→100). Base-systemprompt + dynamisk context-injection per case-kompleksitet. Idempotent prosessering og retry-policy sikrer consistency. Batch-kjøring er optimalt for operasjonell stabilitet.

4. Data & Kontekst: Azure AI Search + Managed Identity. RAG med strict RBAC. Sårbarhet: Aldri eksporter PHI fra helsevesenet. Bruk CMK (kunde håndtert nøkkel) og Entra ID row-level security i Dataverse. All injeksjon skjer innenfor Microsoft-trust boundary.



5. Observerbarhet & Kost: Application Insights med correlation IDs. Cost-optimering: GPT-4o-mini for routing/validering, GPT-4o for syntese. Redis-cache + hard token-budsjett per swarm-run. Fail-fast ved overshoot.

6. Transition: Mnd 1-2: RAG-pipeline + orchestrator. Mnd 3-4: Service Bus-distribusjon + 5 spesialiserte agenter. Quick win: Automatisert compliance-sjekk for journalføring. Mnd 5-6: Skalér til 100 agenter. Swarm feiler ved høy interaktivitet eller flytende kontekst – da er Copilot riktig verktøy.

Neste steg:

1. Kartlegg SharePoint/Dataverse metadata for RAG-indeksering og PHI-maskering.
2. Implementer PoC orchestrator (Azure Function + Service Bus) med 5 agenter og mock-helsedata.
3. Definer output-JSON-skjema, sett opp Application Insights og test fail-fast grenser før produksjon.