



id: SI_004

model: google/gemma-4-26b-a4b-it

seeds:

04_risiko: mulighet

03_relasjon: avhengighet

05_handling: vent

01_perspektiv: økonomisk

02_tidhorisont: kortsiktig

Instans SI_004

Seeds: økonomisk | kortsiktig | avhengighet | mulighet | vent

Analysen identifiserer en kritisk mismatch mellom ambisjon og infrastruktur. Implementering av agentisk KI i et deterministisk miljø er en **økonomisk** risiko som kan eskalere eksponentielt ved systemsvikt.

Arkitektur og sikkerhetsmekanismer Dere må gå bort fra RBAC til en **ABAC (Attribute-Based Access Control)**-modell styrt av en sentralisert policy-motor (f.eks. OPA - Open Policy Agent). Siden IAM-plattformen er mangelfull, må dere bygge en "Policy Proxy" mellom agenten og de eldre fagsystemene.

- **Sandboxing:** Ikke implementer agenter direkte i produksjonsmiljøet. Bruk isolerte containere med streng egress filtering.
- **Rate-limiting:** Sett harde grenser på antall API-kall per minutt for å hindre "looping-kaos" som kan krasje eldre fagsystemer.

Tekniske blindsoner og undervurderte risikoer Den største faren er **avhengighet** av usikre integrasjoner. Eldre systemer forventer forutsigbare input; agents probabilistiske natur vil skape "støy" som fragmentert logging ikke kan fange opp. En uforutsett beslutning kan utløse en kjedereaksjon i datakilder som ikke har rollback-kapasitet. Dette er en **kortsiktig** gevinst som kan føre til langvarig operasjonell lammelse.

Kontrollmodell: "Human-in-the-loop" vs. "Human-on-the-loop" Mainstream foreslår full autonomi for effektivitet. Mitt perspektiv er en streng **vent**-strategi: Implementer en "Shadow Mode" i 6 måneder hvor agenten kun foreslår handlinger uten å utføre dem. Dette transformerer risiko til en **mulighet** for å trene policy-motoren uten faktiske tap.



Kritiske risikoer som ignoreres:

1. **State-drift:** Agenten endrer data i system A, men system B (som er eldre) forstår ikke endringen, noe som skaper inkonsistente datastatuser.
2. **Credential Exhaustion:** Automatisert nøkkelrotasjon for agenter er ekstremt komplekst når systemene ikke støtter moderne protokoller.

Neste steg:

1. **Etabler en "Policy Proxy":** Utvikle et mellomlag som validerer agentens forespørsler mot et sett med uforanderlige regler (f.eks. "Aldri endre felt X i system Y uten menneskelig godkjenning").
2. **Shadow Pilot:** Start piloten utelukkende i "observe-only" modus for å kartlegge logg-fragmentering.
3. **Kostnadsanalyse av feil:** Beregn den økonomiske kostnaden ved en fullstendig rollback av datakorupsjon i de eldste fagsystemene før første API-nøkkel tildeles agenten.