



id: SI_002

model: anthropic/claude-opus-4.6

seeds:

04_risiko: mulighet

03_relasjon: makt

05_handling: vent

01_perspektiv: strategisk

02_tidhorisont: langsiktig

Instans SI_002

Seeds: strategisk | langsiktig | makt | mulighet | vent

Dissens: Dere bør IKKE innføre agentisk KI nå.

Mitt perspektiv, formet av **vent** og **strategisk**, bryter med mainstream-entusiasmen: En mellomstor offentlig virksomhet med fragmentert logging, ufullstendig ABAC, ingen OPA, ingen Zero Trust og begrensede DevSecOps-ressurser har ikke den institusjonelle **makten** til å kontrollere autonome agenter. Å pilotere innenfor 6–9 måneder er ikke en **mulighet** — det er en felle.

Hvorfor vente er den strategisk overlegne posisjonen

Maktanalyse: Agentisk KI omfordeler beslutningsmakt fra mennesker til programvare. I et system uten konsolidert audit-pipeline og med legacy-monolitter uten deterministiske API-kontrakter, gir dere makt til aktører dere ikke kan observere, begrense eller reversere. Det er ikke innovasjon — det er abdikasjon.

Langsiktig kostnad vs. kortsiktig gevinst: En mislykket pilot med datakorupsjon, runaway agents eller GDPR-brudd via ukontrollerte eksterne API-kall vil sette organisasjonens KI-ambisjon tilbake 3–5 år. Den politiske og omdømmemessige risikoen i offentlig sektor er asymmetrisk — nedsiden er katastrofal, oppsiden er inkrementell.

Emergent behavior i svake systemer: Systemer uten idempotens, uten transaksjonsgarantier og med latent kobling mellom fagsystemer er designet for uforutsette kjedereaksjoner. Å slippe autonome agenter inn her er å teste worst-case i produksjon.



Den strategiske muligheten: Bygg fundamentet først

I stedet for å pilotere agentisk KI, bruk de 6–9 månedene til å bygge **infrastrukturen som gjør agentisk KI mulig langsiktig**:

1. **Konsolidert audit-pipeline** (OpenTelemetry + event-sourcing til sentralt lager) — dette har selvstendig verdi uavhengig av KI.
2. **Policy-motor** (OPA/Styra) med policy-as-code for eksisterende tjenester — bygg muskelminne før agenter trenger det.
3. **IAM-oppgradering** til full ABAC med støtte for ephemeral credentials og token-scoping — dette er gjeld dere uansett må betale.

Disse tre tiltakene gir dere **makt** til å kontrollere agenter når dere er klare, og de leverer umiddelbar sikkerhetsverdi.

Neste steg

1. **Deklarer en “Foundation First”-strategi** overfor ledelsen: Agentisk KI er målet for 2026, men 2025 brukes til å bygge kontrollplanet. Sett konkrete KPI-er (100% sentralisert logging, ABAC-dekning >80%, OPA i produksjon).
2. **Kjør en skygge-pilot** — la en agent foreslå handlinger som mennesker utfører, uten autonom eksekveringsrett. Dette gir data om agentadferd og emergent behavior uten risiko. Sett opp i et isolert miljø med syntetiske data.
3. **Kartlegg API-modenhet** for alle integrasjonspunkter: klassifiser hvert API etter idempotens, kontraktsstyrke og sideeffektrisiko. Kun APler som scorer “grønt” på alle tre blir kandidater for fremtidig agenttilgang.

Kjernebudskap: Den største strategiske muligheten er å ikke være først. Vent, bygg makt gjennom infrastruktur, og innfør agentisk KI fra en posisjon av kontroll — ikke håp.