



id: SI\_001

model: openai/gpt-5.4-mini

seeds:

04\_risiko: sårbarhet

03\_relasjon: konkurranse

05\_handling: implementer

01\_perspektiv: strategisk

02\_tidhorisont: kortsiktig

## Instans SI\_001

**Seeds:** strategisk | kortsiktig | konkurranse | sårbarhet | implementer

**Min vurdering:** Magnus bør ikke velge mellom «kjør» og «vent». Den strategiske, kortsiktige og forsvarlige tredjeveien er en **begrenset, reverserbar pilot** med tydelig politisk risikoeierskap, stram datakontroll og dokumentert kollektiv beslutning. I offentlig sektor er «akseptert risiko» forsvarlig først når den er **bevisst, avgrenset, tidsbundet, sporbar og besluttet på rett nivå** – ikke når den bare er “tatt”.

### 1) Risikostyring i grånyanser

Kategoriser risiko i fire nivåer:

- **R0: Uakseptabel** – stopp.
- **R1: Høy, men begrensbart** – kan bare kjøres som pilot.
- **R2: Moderat** – kan produseres med kontrolltiltak.
- **R3: Lav** – normal drift.

Lag en 1-side **risikomatrise** med: sannsynlighet, konsekvens, kompenserende tiltak, rest-risiko, beslutningstaker. «Akseptert risiko» blir forsvarlighet når rest-risikoen er **forankret i politisk ledelse**, og når man har en **exit-klausul** hvis avvik oppstår.

### 2) Ansvarsfordeling og dokumentasjon

Krev en formalisert **tverrfaglig beslutningssløyfe**:

1. Juridisk + IT-sikkerhet skriver hver sin vurdering i samme dokument.
2. Magnus samler dem i en **beslutningsnotat** med tydelig uenighet.
3. Ledergruppen/politisk nivå signerer på valgt risiko.
4. Arkiver alt i sak-/arkivsystem.



Formulering til avdelingene:

«Jeg ber ikke om garanti, men om en eksplisitt faglig vurdering av rest-risiko og hvilke vilkår som gjør pilot mulig.»

### 3) Leverandørkontrakt

Krev minst:

- **Databehandleravtale / rolleavklaring**
- **Revisjonsrett / sikkerhetsdokumentasjon**
- **Plikt til å varsle modellendringer og underleverandører**
- **Sletting/tilbakelevering ved avslutning**
- **Ansvarsfordeling for brudd som skyldes leverandørens forhold**
- **Skadesløsholdelse for IP-/sikkerhetsbrudd der det er realistisk**
- **Exit-rett ved manglende kontrolltiltak**

### 4) Minimalstandard for pilot

Absolutt minimum:

- Ikke-prod-data eller sterkt anonymiserte data der mulig
- Begrenset brukergruppe, begrenset formål
- Human-in-the-loop før vedtak/utsendelse
- Loggføring av alle AI-forslag og overstyringer
- 4-8 ukers pilot med tydelig stoppkriterier
- DPIA / sikkerhetsvurdering / beslutningsnotat før oppstart

### 5) Politisk samtale

Si:

«Valget er ikke om vi tar risiko, men hvem som eier den. Jeg kan anbefale en pilot med kontrollert rest-risiko; hvis dere vil ha rask effekt, må dere også eie usikkerheten og godkjenne rammene.»

### 6) Tidskompromiss

Midtveien er: **pilot i sandkasse + juridisk avklaringsspor parallelt**. Politikerne får noe å vise, men kommunen låser ikke full utrulling før læring og avklaring foreligger.

**Norske kommunale mønstre å se etter:** sandkasse-/pilotregimer i digitale innbyggertjenester, ofte med egne styringsgrupper og avgrenset dataflyt.

**Neste steg:**

1. Lag en 1-sides risikoprofil med R0-R3 og forslag til pilotgrense.



2. Sett opp et felles møte med juridisk, IT-sikkerhet og linjeleder for å signere rest-risiko.
3. Forhandle kontrakt med minimumskrav og exit-rett før pilotstart.