



id: SI\_005

model: openai/gpt-5.4-mini

seeds:

04\_risiko: sårbarhet

03\_relasjon: tillit

05\_handling: forhandle

01\_perspektiv: strategisk

02\_tidhorisont: kortsiktig

## Instans SI\_005

**Seeds:** strategisk | kortsiktig | tillit | sårbarhet | forhandle

Den reelle adopsjonsbarrieren er sjelden “manglende forståelse” alene. I norsk juridisk praksis er det oftere en **kortsiktig normalisering av risiko**: man vet at åpne KI-verktøy er utrygge, men risikoen oppleves som diffus, usynlig og foreløpig ustraffet. Det blir en stilltiende forhandling: “Vi vet dette ikke er ideelt, men ingen har blitt tatt ennå.” Det er en sårbarhetslogikk, ikke en kunnskapslogikk.

### 1. Bevissthet vs. risiko

Mange vet nok til å være urolige, men ikke nok til å endre adferd. Gapet ligger i at konsekvensen oppleves som **lav sannsynlighet, høy abstraksjon**. For at bevissthet skal bli handling, må risiko konkretiseres: klientspesifikke klausuler, sikkerhetsbrudd, eller spørsmål fra revisjon/forsikring. “Det kan gå galt” virker svakt; “det kan bryte taushetsplikt i en konkret sak” virker.

### 2. Tillit til teknologien

SikkerKI møter et høyere tillitskrav fordi den ber om **ny tillit** til et mindre kjent system, mens ChatGPT/Claude allerede har sosial legitimitet. Profesjonelle aksepterer ofte kjent usikkerhet bedre enn ukjent sikkerhet. De spør ikke bare “er det sikkert?”, men “kan jeg forklare dette for partner, klient og tilsyn?” Blind compute/on-prem må derfor bevises, ikke bare påstås.

### 3. Regulatorisk press

Datatilsynet og GDPR er ikke fraværende; de er bare ikke omsatt til operativ frykt. Mange antar at håndheving kommer “senere” eller “mot de store”. I Norge blir ofte ansvar forvaltet gjennom intern praksis før tilsyn. Uten eksplisitt klientkrav eller forsikringssignal forblir regulering en teoretisk brems.

### 4. Sosiale dynamikker

Bransjen er sterkt normdrevet: hvis de største firmaene bruker åpne verktøy, blir det en



standard. Sikker KI blir normalt først når den blir **kollegialt risikoreduserende**, ikke teknologisk bedre. En enkelt aktør som går foran, tar første-mover-sårbarhet; derfor trengs koalisjon, ikke sololøp.

## 5. Pris og friksjon

Kostnaden ved ikke å bytte er skjult, men reell: klienttap, omdømme, forsikring, intern lekkasje. Samtidig er byttefriksjonen konkret: integrasjon, vane, fart, “det funker jo allerede”. SikkerKI må derfor vinne på **lav friksjon i dag**, ikke på langsiktig compliance alene.

## 6. Konkrete byttebarrierer

De som vil bytte stopper ofte ved: manglende integrasjon med dokumentflyt, uklare kostnader, usikker feature-paritet, og frykt for tregere arbeidshverdag. Strategisk sett er det ikke nok å være trygg; løsningen må være **trygg nok uten å koste kortsiktig produktivitet**.

### Neste steg

1. Kartlegg 10–15 norske advokat-/revisorhus: hvilke konkrete hendelser, ikke meninger, utløser bytte?
2. Utform en “bevispakke” for tillit: teknisk attestasjon, databehandleroppsett, revisjonsspor og enkel forklaring til partner/klient.
3. Test én lav-friksjon integrasjon i et reelt arbeidsløp og mål hvor byttet faktisk stopper: vane, hastighet eller dokumentflyt.