



id: SI_004

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

seeds:

04_risiko: mulighet

03_relasjon: makt

05_handling: implementer

01_perspektiv: operasjonell

02_tidhorisont: kortsiktig

Instans SI_004

Seeds: operasjonell | kortsiktig | makt | mulighet | implementer

Diagnose: Den asymmetriske risiko-kalkylen

Motstanden er ikke mangel på kunnskap, men en **operasjonell** kalkyle der gevinsten ved “skygge-KI” (ChatGPT/Claude) er umiddelbar, mens risikoen er diffus og fremtidig. Jurister opererer med et **kortsiktig** fokus på fakturerbar tid. Å bruke en åpen LLM er friksjonsfritt; å implementere SikkerKI krever en administrativ prosess som de ikke ser som en direkte **mulighet** for økt profitt, men som en kostnad.

Psykologisk og organisatorisk innsikt

- **Makt-dynamikk:** Advokaten eier klientens tillit. Bruk av usikre verktøy er en skjult maktforskyvning fra advokaten til teknologigigantene i USA. De fleste erkjenner dette intellektuelt, men i praksis vinner den operative bekvemmeligheten.
- **Sosial norm:** Det eksisterer en “silent consensus” om at alle andre tar risikoen. Å være den første som krever SikkerKI kan oppleves som en brems på effektivitet, ikke en profesjonell standard.

Leverage-punkter (Hva som faktisk flytter dem)

1. **Forsikring & Ansvar:** Ikke Datatilsynet (for tregt), men profesjonsansvarsforsikringen. Hvis forsikringsselskapene innfører klausuler om “godkjent databehandler for KI-verktøy”, endres spillereglene over natten.



2. **Klient-mandat:** Når store selskaper (Equinor, DNB, statlige aktører) i sine anbudskrav spesifiserer null datalekkasje til tredjepart, blir SikkerKI et verktøy for å vinne **makt** i markedet.
3. **Regulatorisk nådestøt:** Et konkret sanksjonsvarsel fra Datatilsynet rettet mot en profilert advokatfirma-partner vil skape en kjedereaksjon.

Skarpe dilemmaer

- **Feature-paritet vs. Sikkerhet:** Vil de velge en 90% like god modell som Claude, eller en 70% god modell som garanterer suverenitet? Per i dag vinner de 90%.
- **Friksjon vs. Compliance:** Hvert ekstra klikk i en sikker arbeidsflyt er et angrep på fakturerbar tid.

Implementerbare angrepsvinkler

- **Eliminer onboarding-friksjon:** Lag ferdige “Compliance-pakker” (dokumentasjon som kan sendes direkte til klienten/IT-avdelingen) slik at advokaten slipper å argumentere selv.
- **Mål “The Risk Manager”:** Ikke selg til partneren, selg til de som sitter med ansvaret for profesjonsansvar og IT-sikkerhet.

Neste steg:

1. **Kartlegg forsikringsvilkår:** Identifiser om norske ansvarsforsikringer har åpninger for sanksjonering ved bruk av usikre LLM-er.
2. **Produkt-modularisering:** Utvikle en “One-click Compliance”-modul som genererer juridisk holdbar dokumentasjon for klienten ved bruk av SikkerKI.
3. **Måltrettet lobby:** Knytt SikkerKI direkte opp mot krav i offentlige anbudsprosesser.