

Når kontrollbehovet går på bekostning av informasjonssikkerhet

Fra hemmer til fremmer: hvordan gode risikovurderinger driver innovasjon

Normkonferansen 2026

Aleksander Hausmann · CloudNorway AS

Hvem er jeg?

2009–2016

Forsvaret og NATO

Ingeniørutdanning så Head of Cyber Security Section

2016–2017

Sunnaas sykehus HF

Informasjonssikkerhetsleder og personvernombud

2017–2020

PwC

Teamleder i avdeling for Cybersecurity & Privacy

2020–2026

Diffia

CISO for leverandør av digital hjemmeoppfølging

2026–

CloudNorway

Leder for Informasjonssikkerhet og Personvern



“

*Robusthet bygges ikke gjennom
å eliminere risiko, men gjennom
evne til å håndtere den.*

— Lærdom fra Forsvaret



Et eksempel fra min tid i helsesektoren

En sykepleier tar bilde av et sår med sin private telefon for å dokumentere status før henvisning.
Det fantes ingen godkjent løsning for klinisk foto, bildet havner i personlig kamerarull.

Pasientbilde · Privat enhet · Kommersiell sky · Ingen sporbarhet

NØKKELINNSIKT

Avvik som dette blir **sjelden logget**. Risikovurderinger måler systemene vi har, ikke arbeidet som gjøres utenfor dem.
Skyggepraksis synes ofte ikke før den gjør skade.

Den metodiske asymmetrien

Kontrollbehovet skaper en asymmetri i risikostyringen:



Den nye løsningen

Granskes i detalj

- Trusselmodellering
- Sårbarhetsanalyse
- Konsekvensvurdering
- Krav om full modenhet



o-tiltaket

Dagens praksis, sjelden vurdert

- Ingen trusselmodellering
- Kjent, men ikke analysert
- Akseptert som «status quo»
- Stabilitet $\neq$ lav risiko

Resultatet: et beslutningsgrunnlag som mangler halve bildet.

“

*Vi krever at det nye skal være
perfekt, mens vi aksepterer at
det gamle bare er kjent.*

Konservatisme uten sammenligning er ikke forsiktighet.
Det er blindhet.

o-tiltaket: risikoen vi allerede lever med

Disse risikoene lever videre i daglig drift, uten systematisk vurdering:



Kommersielle meldingstjenester

Pasientopplysninger på Messenger, SMS og privat e-post. Utenfor virksomhetens kontroll.



Ikke-godkjent AI-teknologi

Helsepersonell limer pasientdata inn i ChatGPT og Claude fordi godkjente alternativer mangler.



Manuelle rutiner uten sporbarhet

Lokale Excel-ark, telefonrunder og individuelle noteringer som aldri ble risikovurdert.

Felles kjennetegn: reelle, utbredte og ikke systematisk risikovurdert.

Hva risikovurderingen faktisk måler

Og hva den burde måle:

✗ Dagens metodikk

Restrisiko ved endring = **negativ vurdering**

0-tiltaket behandles som risikofritt. Oppsiderisikoen ignoreres.

✓ Komplett risikovurdering

Restrisiko ved endring – eksisterende restrisiko (0-tiltak) – oppsiderisiko = **samlet risiko**

Samlet risiko kan gå ned selv om endringen introduserer nye risikoer.

Uten alle tre måles risikoen mot et vakuum.

“

*Det er som å stå i en lekk båt
og være bekymret for at den nye båten
kanskje kan få riper i lakken.*



Konsekvensene for risikobildet

Når 0-tiltaket ikke vurderes, skjer følgende:

Skjevt beslutningsgrunnlag

Samlet risiko overvurderes

Skjult restrisiko

Dagens risiko forblir uhåndtert

Tap av faglig tillit

Magefølelse overstyrer prosess

Skygge-IT vokser

Fagfolk omgår formelle kanaler

Informasjonssikkerhet har i praksis gått på bekostning av informasjonssikkerhet.

Å stå i ro er også en risiko

Samfunnet beveger seg, detaljkontroll forutsetter at det ikke gjør det



*Treghet er ikke nøytralt. I et samfunn som beveger seg, blir **stillstand sin egen risiko**.*

Oppdragsbasert sikkerhet

Prinsippet fra militær ledelse, anvendt på informasjonssikkerhet

Forsvaret

Definer oppdraget og rammene.

Gi frihet til å operere innenfor dem.

Resultat: tempo og tilpasningsevne.

Informasjonssikkerhet

Definer sikkerhetskravene og
akseptabel risiko. La fagmiljøene
finne veien. Resultat: raskere
innføring, lavere samlet risiko.

Eksempel: Norsk skyplattform med todelt infrastruktur, hoveddelen på norsk helsenett, kommuniserte med sykehusene uten å være eksponert mot internett. Kun det som **måtte** være internett-vendt, var det. Rammene var strenge, men klare og innenfor dem kunne fagmiljøene gjøre flere endringer med lav risiko og høyere tempo.



Én kulturendring

Krev vurdering av 0-tiltaket og oppsiderisikoen
i enhver risikovurdering.

*Fra hemmer til fremmer. Risikovurderingen blir et
beslutningsverktøy som gjør oss trygge og bevegelige,
ikke bare forsiktige.*



Takk for oppmerksomheten

Ta kontakt for å diskutere videre.

Aleksander Hausmann | aleksander@cloudnorway.no | +47 99 51 47 96