



Digitale trusler; ledelse og risiko

Temasamling for toppledere

Oslo 03.02.2023

Åsmund Skomedal,
informasjonssikkerhetssjef



Ytre krefter som påvirker behovet for endring

Det digitale trusselbildet er skjerpet

Sterk økning i bruk av teknologi

- Digitale
- Mobile
- KI/velferdsteknologi
- Sosiale medier
- Skytjenester



Lovverk og instruksjoner som krever etterlevelse



De store internasjonale aktørene utfordrer samfunnsutviklingen

Mer uforutsigbarhet og økt beredskap

Forventninger fra innbyggere og næringsliv øker.

Hvordan skal vi få bedre sikkerhet på tvers i hele kommunen?

Hvordan skal vi få en god sikkerhetskultur i kommunen?

Hvordan kan vi som er her i dag samarbeide for å møte disse utfordringene?

STORE ULYKKER

1. Brann i Operatunnelen
2. Skipskollisjon indre Oslofjord
3. Brann og eksplosjoner på Sydhavna
4. Skogbrann Østmarka

NATURHENDELSE

5. Stormflo indre Oslofjord
6. Urban flom
7. Kvikkleireskred Alfaset
8. Jordskjelv Oslofjord
9. 100-års solstorm

KRITISK INFRASTRUKTUR

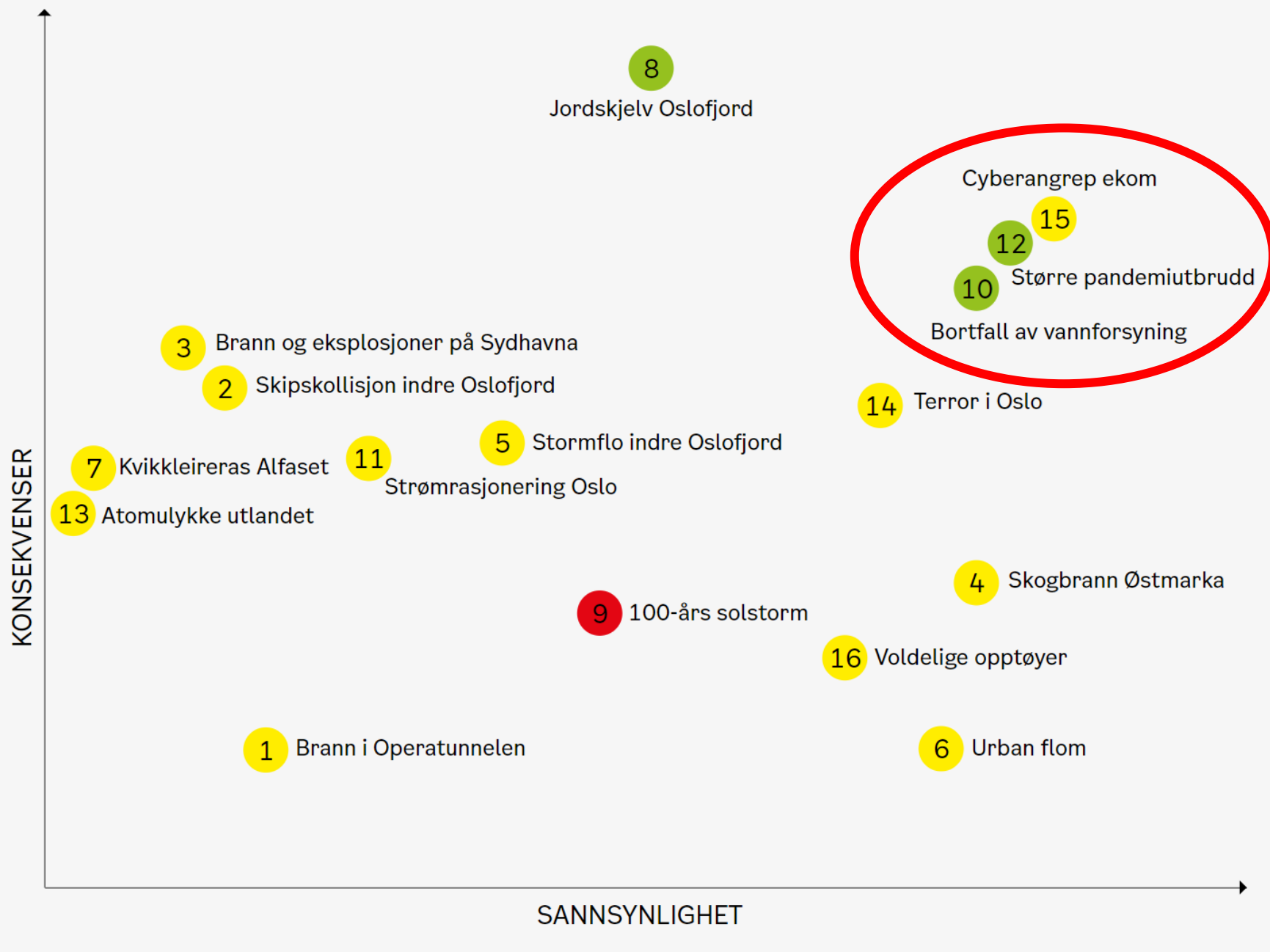
10. Bortfall av vannforsyning
11. Strømrasjonering Oslo

HELSE

12. Større pandemiutbrudd
13. Atomulykke utlandet

TILSIKTEDE HANDLINGER

14. Terror i Oslo
15. Cyberangrep ekom
16. Voldelige opptøyer



Utvikling på sikkerhetsområdet

Tekniske sårbarheter
1999: **894** nye
2022: ca **25 000** nye

Sosial manipulering

Hacktivisme

Tyveri av
personopplysninger

Kommersialisering
av skadevare

Løsepengevirus

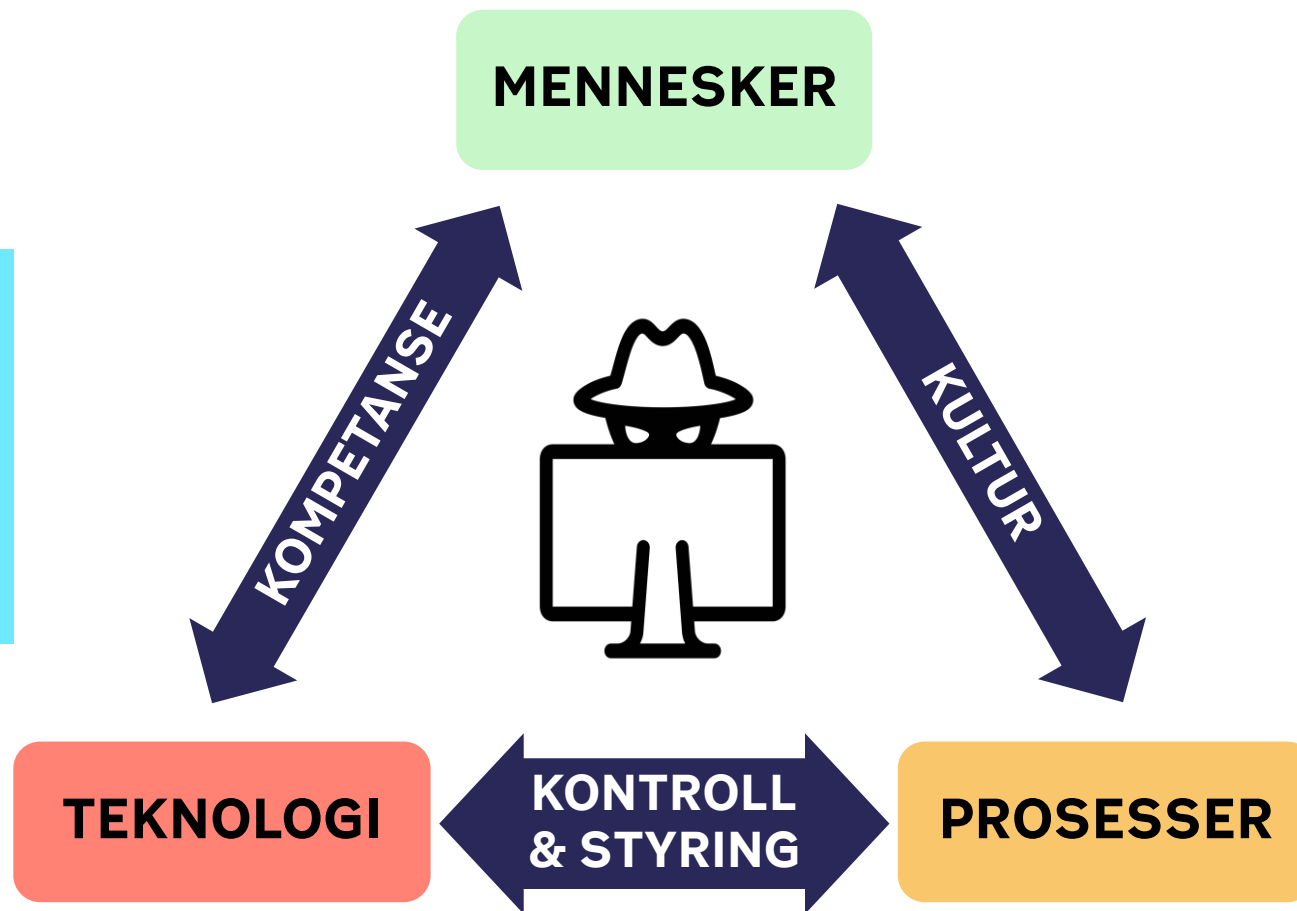
Angrep på
leverandørkjeder

Kunstig
intelligens



Angriperne utnytter våre svakheter

Teknologi har innebygde sårbarheter
Prosesser/tiltak har variabel kvalitet
Menneskelige feil forsvinner ikke



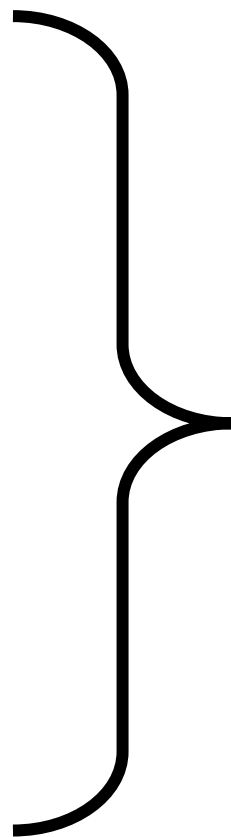
Vi har en jobb å gjøre ...

Sårbarheter

Trusselbildet

Stor kompleksitet

Økt digitalisering



Og utfordringene er flere ...

- ▶ Vi har ikke nok kompetanse om informasjonssikkerhet
- ▶ Hvordan skal vi få tak i folk som kan noe om dette?
- ▶ Hvordan skal vi få til dette innenfor de rammene vi har?
- ▶ Kan vi la dette gå utover vår kjernevirksomhet?
- ▶ Hvem gjør egentlig hva?
F.eks. FIN, UKE, HEL, Origo og virksomhetene som bruker felles- og sektorsystemer



Målsetninger

Overordnede målsetninger

- ▶ Tillit i befolkningen
- ▶ Tjenester som er sikre og har god kvalitet
- ▶ Effektiv utvikling av tjenester

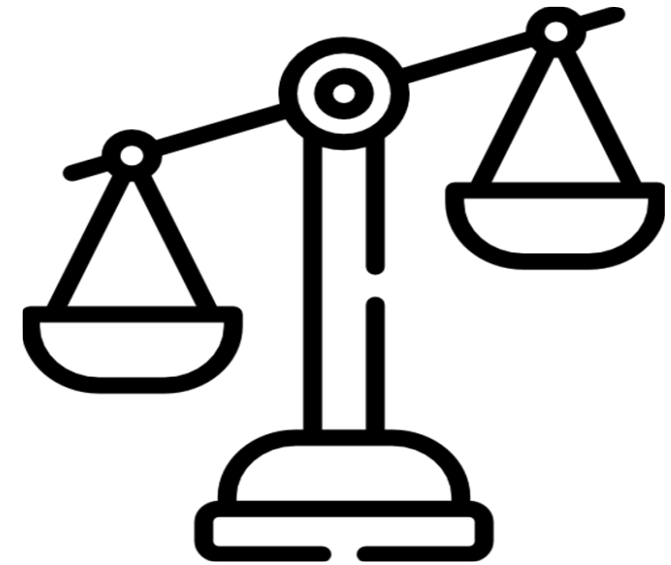
Målsetninger for **informasjonssikkerhetsarbeidet**

- ▶ At vi opererer innenfor en akseptabel risiko
 - ▶ Gjøre prioriteringer som gir effektiv bruk av tid og penger
- => vi må **snakke om risiko** på en enhetlig måte



Risikobasert **styring** av informasjonssikkerhet

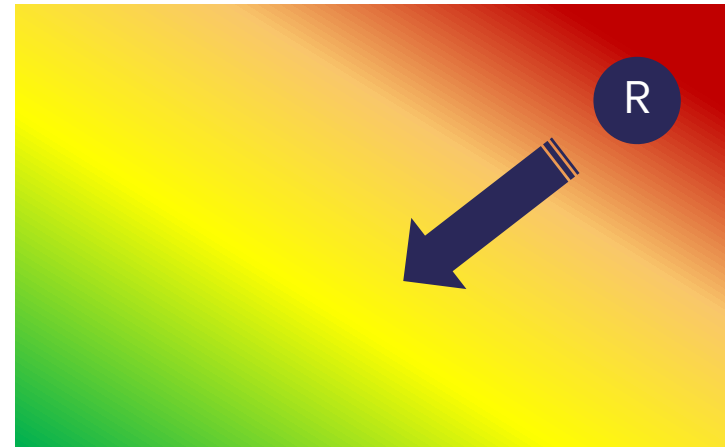
- Risikostyringen sikter mot akseptabel risiko
- Ta hensyn til økonomi
 - Gjennomførbart innenfor eksisterende rammer
 - En må ikke gjennomføre alle tenkelige sikkerhetstiltak, men en må ha gjort vurderingene
- Støtter prioritering
 - Hva må gjennomføres og hva kan prioriteres ned?
 - Beslutningsstøtte for endrede rammer
- Følger opp tiltakene
 - planlegge, prioritere og følge opp tiltak
 - eskalere/informere overordnet styringsnivå ved uakseptabel risiko som ikke lar seg håndtere



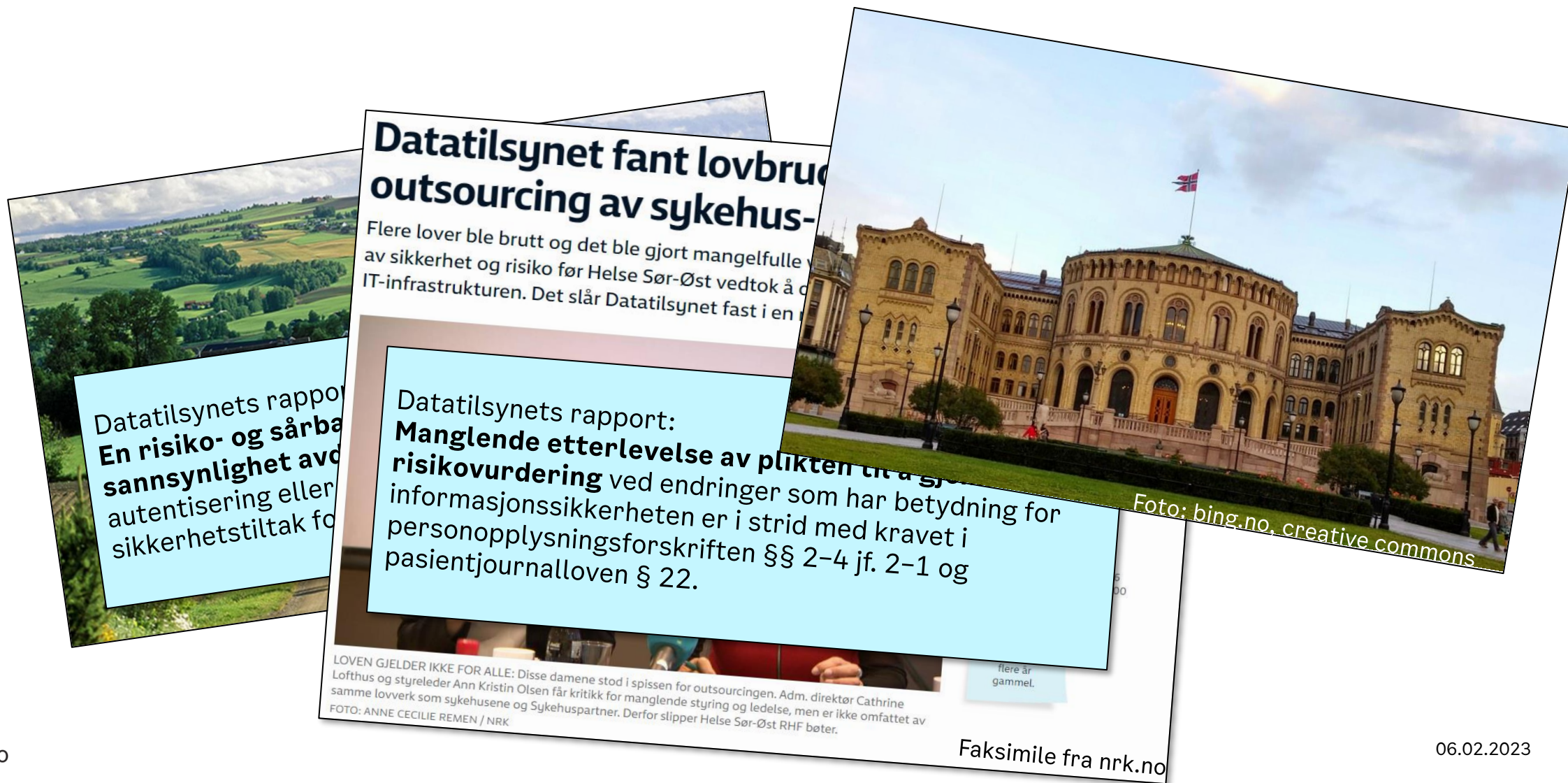
Risikovurderinger legges til grunn for risikostyringen

Risiko- og sårbarhets (ROS) vurderinger handler om å

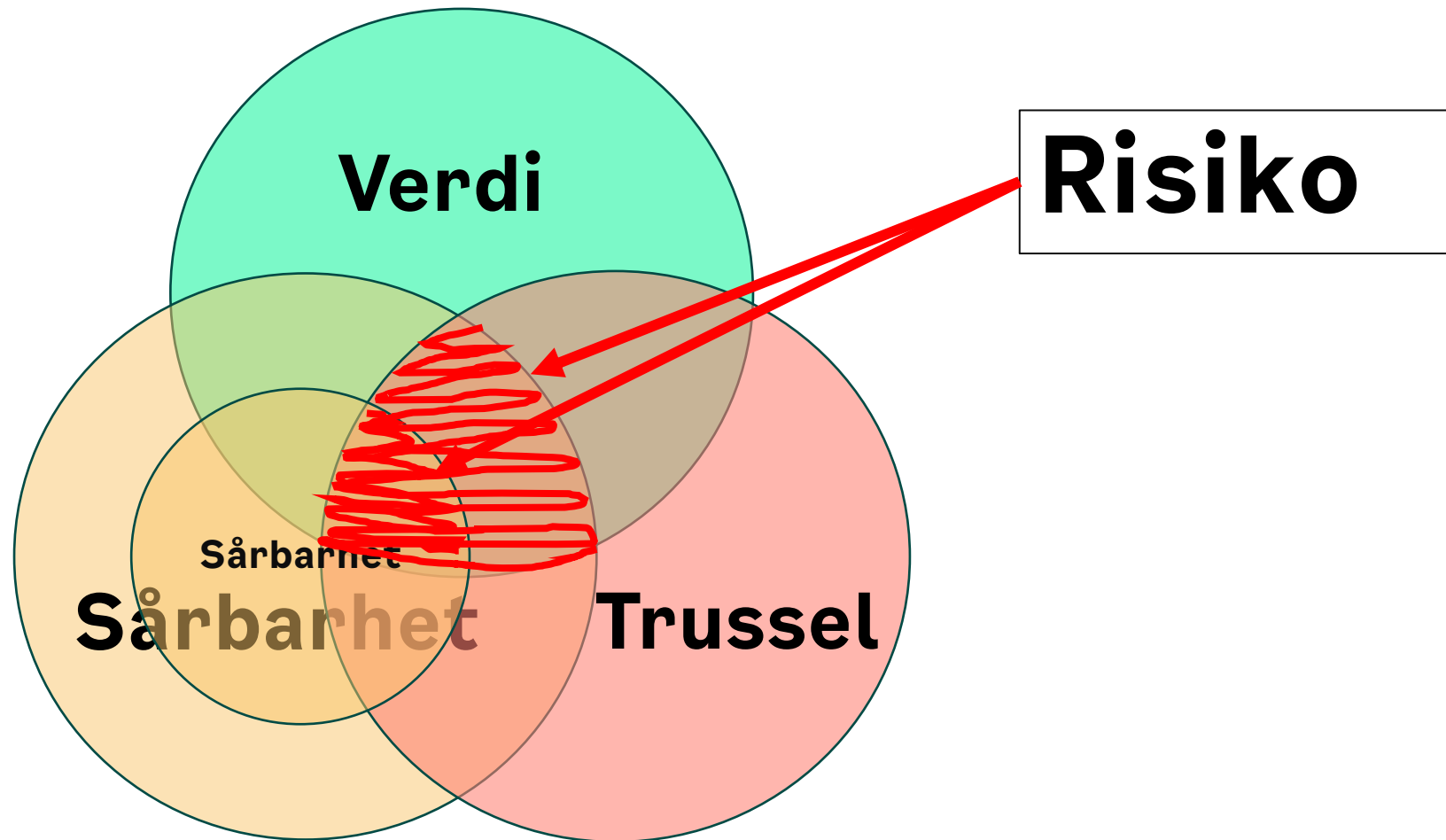
- ▶ avgjøre om verdiene er godt nok beskyttet i det trusselbildet vi har
- ▶ identifisere og foreslå tiltak
- ▶ vurdere risiko etter gjennomførte tiltak
- ▶ dokumentert beslutningsunderlag



Konsekvenser av mangelfull risikostyring ...



Forholdet mellom **risiko**, trusler, sårbarheter og verdi



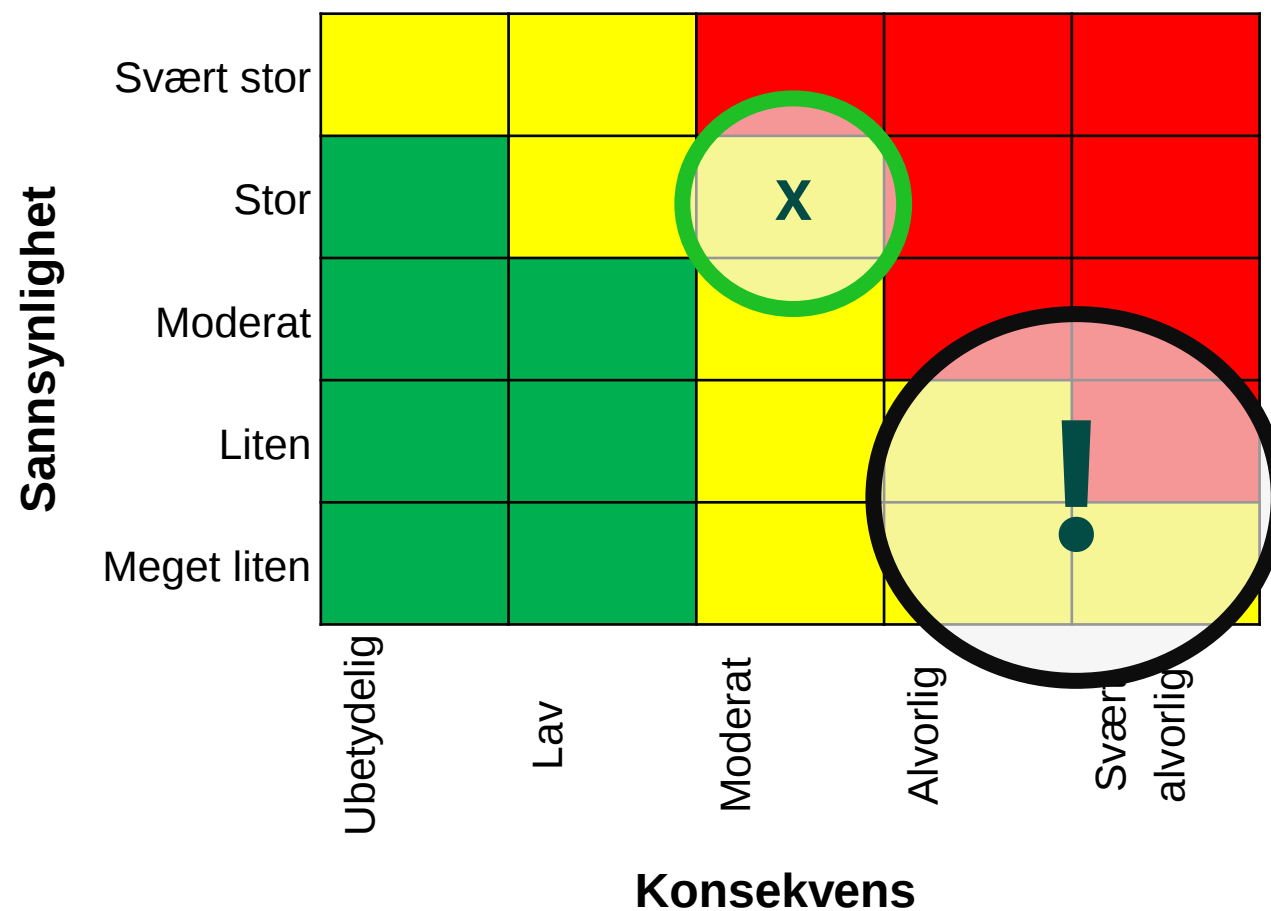
Verdier i tjenester og systemer

Informasjonsverdi vurderes ut fra **konsekvenser** av sikkerhetsbrudd.

Vi ser da på konsekvenser innen flere områder:



Hvordan uttrykkes **risiko** (innen informasjonssikkerhet)



Risikovurdering - et reelt eksempel

Scenario

- ▶ Falske innsynsforespørsler (10.000)

Aktør (og formål)

- ▶ Statlig støttet gruppe / Hacktivist
(Sabotasje eller etterretning ?)

Sårbarhet

- ▶ Ubegrenset med anonyme forespørsler

Verdi

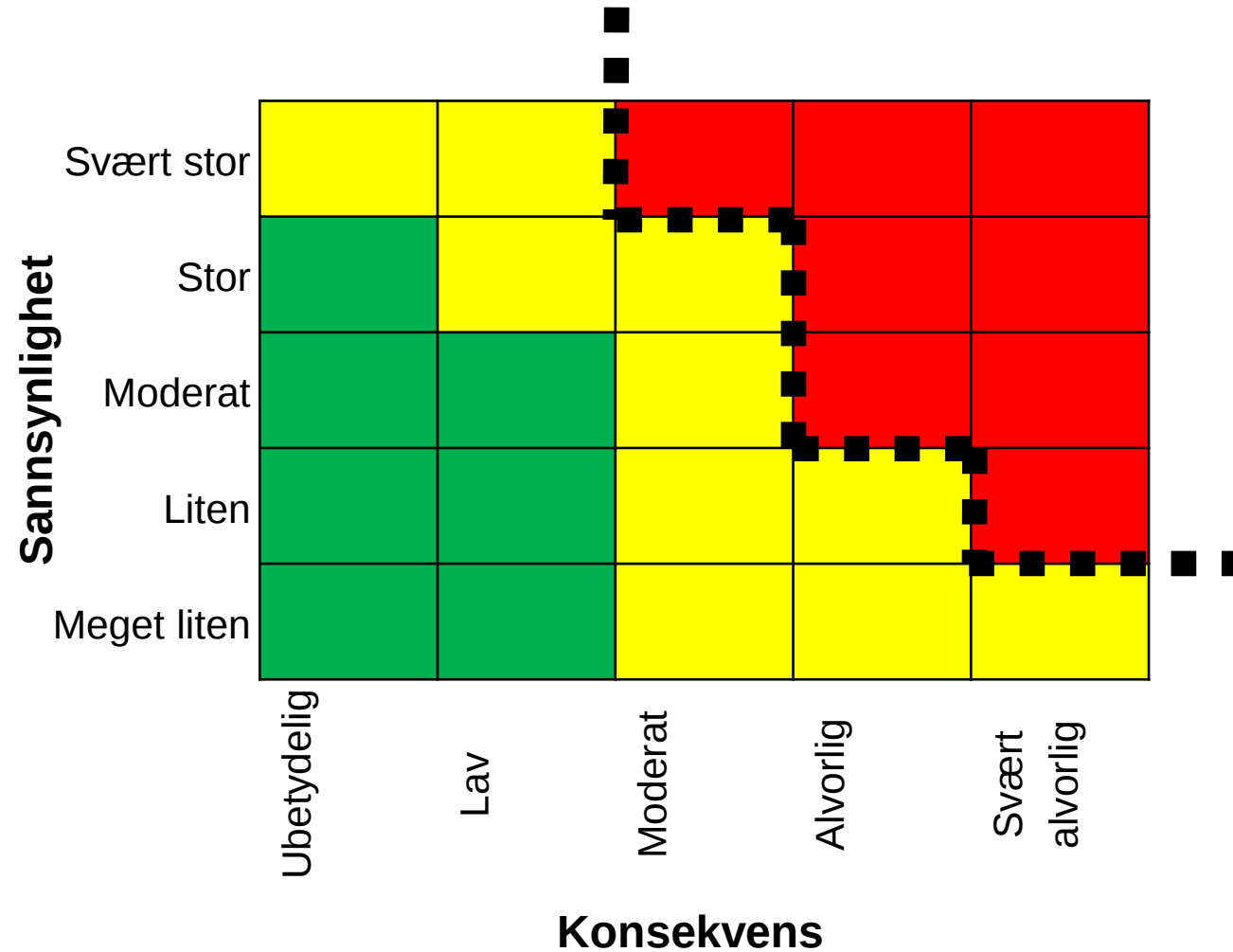
- ▶ Saksbehandlingsskapasitet;
misbrukte årsverk, overholde svarfrist

Sannsynlighet	Svært stor					
	Stor					
	Moderat					
	Liten					
	Meget liten					
		Ubetydelig	Lav	Moderat	Alvorlig	Svært alvorlig

Konsekvens

A green circle with a blue 'X' is centered on the cell corresponding to 'Moderat' probability and 'Moderat' consequence.

Hva er «akseptabel risiko» ?



Risikostyring og lederrollen

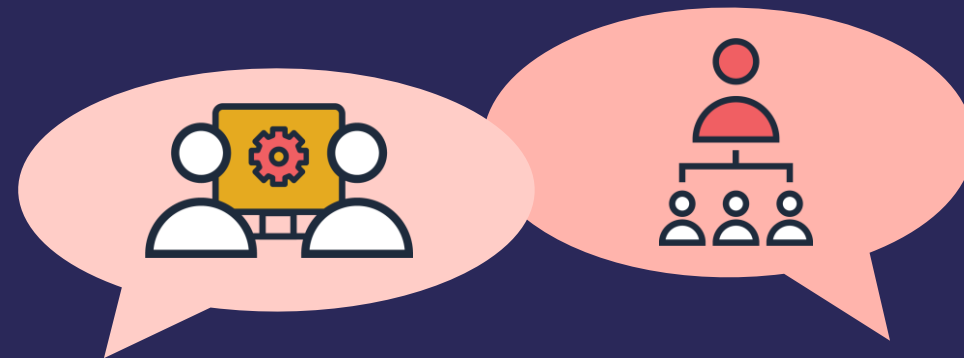
- ▶ Sørge for at risikovurderinger gjennomføres for virksomhetens tjenester
- ▶ Utøve risikostyring ved å vurdere, prioritere, beslutte og følge opp tiltak
- ▶ Utvikle og integrere risikostyring i eksisterende prosesser
- ▶ Utvikle en god sikkerhetskultur



For toppledere er ikke nødvendigvis dette arbeidet tidkrevende, men tiden er avgjørende !



Risikostyring



Risikoanalyser

- På hvilke områder bruker vi risikoanalyser hos oss?
- Hvordan bruker vi risikovurderinger som beslutningsstøtte i prioriteringer?
- Har jeg noen gode eksempler fra min virksomhet hvor risikostyring har gitt merverdi?