



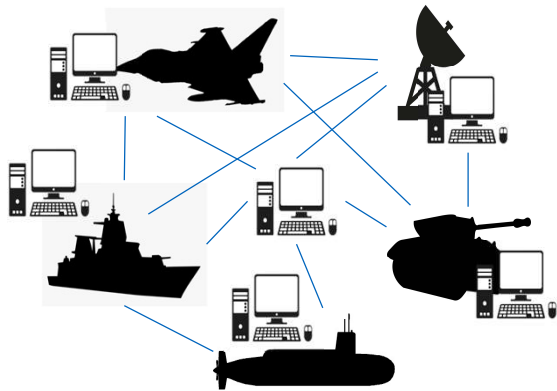
FFI Forsvarets
forskningsinstitut

Hva gjør en risikovurdering for tilsiktede handlinger god?

Erfaringer fra FoU innen risiko og forsvarlig sikkerhet for Forsvarets digitale systemer

Monica Endregard, sjefsforsker (Monica.Endregard@ffi.no)
Havtil's fagseminar om sikring
Stavanger, 13. september 2024

Motivasjon: Et digitalisert forsvar



- IKT-infrastrukturen og –applikasjonene er **integratoren** for militære evner
- Rask teknologiutvikling og –anvendelse
 - Sivil og militær IKT veves tettere sammen
 - Nye løsninger for nettverk, applikasjoner og datalagring (kunstig intelligens og maskinlæring)
- Komplexitet og usikkerhet
- Sikkerhet skal være risikobasert
- **Hvordan forstå og styre risiko og sikkerhet i denne nye konteksten?**



Foto: Forsvaret



Foto: Forsvaret



Foto: Forsvaret

Forsvaret har fått kritikk

«Vi har funnet mangler i informasjonssystemene Forsvaret bruker i operasjoner. Det er sårbarheter i sikkerheten og systemene fungerer for dårlig sammen. Dette er svært alvorlig.»

Riksrevisjonen, 4.10.2022



Riksrevisjonens undersøkelse
av Forsvarets informasjons-
systemer for kommunikasjon og
informasjonsutveksling i
operasjoner

Ugradert versjon av Dokument 3:3 (2022–2023)

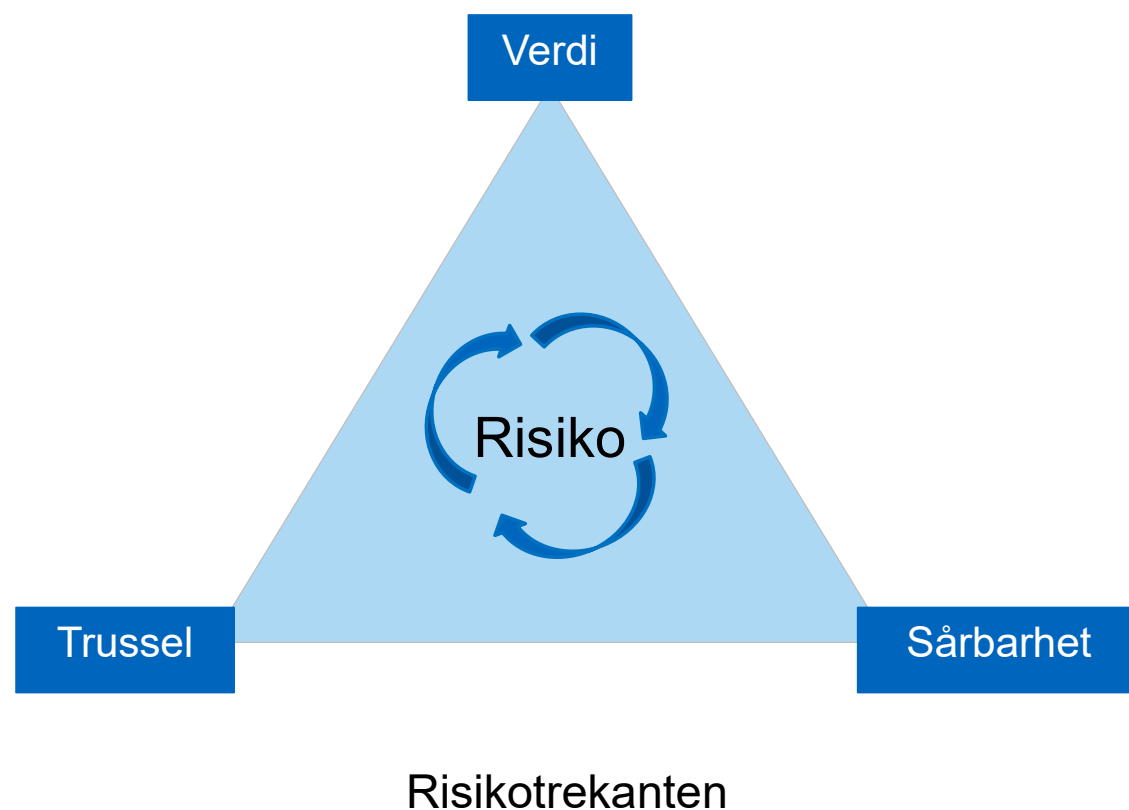


Regelbasert og risikobasert sikkerhetsstyring – hvordan finne den riktige balansen?

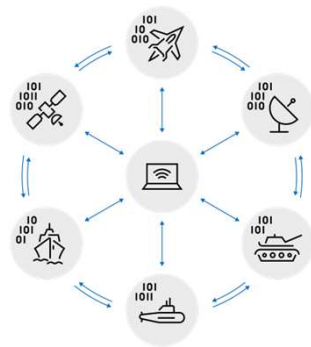
	Regelbasert	Risikobasert
Egenskaper	• Toppstyrt og kontrollbasert • Detaljerte, spesifikke og ofte tekniske krav • Sjekklistor	• Sikkerhet er virksomhetens ansvar • Risikovurdering som basis for sikkerhetstiltak • Systembaserte tilsyn
Fordeler	• Enhet på tvers av skiller • Uniforme sikkerhetsnivå og -tiltak • Enklere virksomhetsstyring • Forenkler tilsyn	• Virksomhetens egen kunnskap • Fleksibilitet • Tilpassede sikkerhetstiltak • Proaktiv og dynamisk
Utfordringer	• Regler i fokus • Detaljerte og rigide krav • Mindre lokale tilpasninger • Kan gi høyere sikkerhetskrav enn nødvendig • Mer reaktivt	• Ikke praktisk veiledning • Forutsetter kunnskap • Krever innsats, metodekompetanse og ressurser • Ingen benchmark for valg av tiltak • Mer ansvar og usikkerhet

Risikobaserte vurderinger og forsvarlig sikkerhetsnivå

- Et **forsvarlig sikkerhetsnivå** oppnås når kritiske verdier er beskyttet mot aktuelle trusler slik at den totale risikoen er akseptabel
- **Risikovurderinger** brukes til å identifisere verdier, tilhørende trusler, sårbarheter, usikkerhet og samlet risiko
 - Skal bidra til et godt beslutningsunderlag
- **Sikkerhetstiltak** endrer restrisiko



Hva er et akseptabelt (forsvarlig) sikkerhetsnivå, og hvorfor er det viktig?



Militære evner er helt avhengig av IKT

Tilgjengelig

Tilstrekkelig beskyttet

Til å stole på



Nasjonal sikkerhet

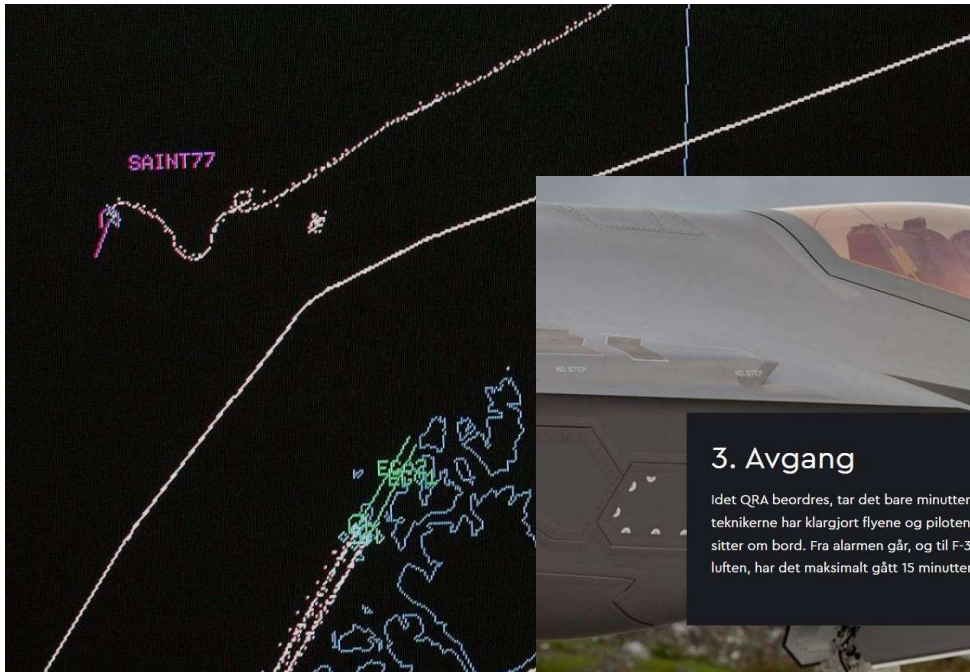


Foto: Forsvaret

Skape sammenheng mellom overordnede oppgaver og IKT



Eksempel: Hurtig reaksjonsvarsel (QRA)



[Dette er QRA – Quick Reaction Alert - Forsvaret](#)

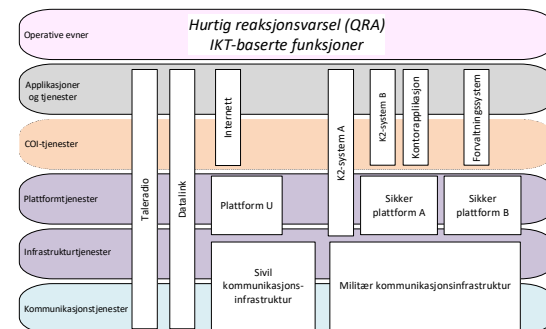
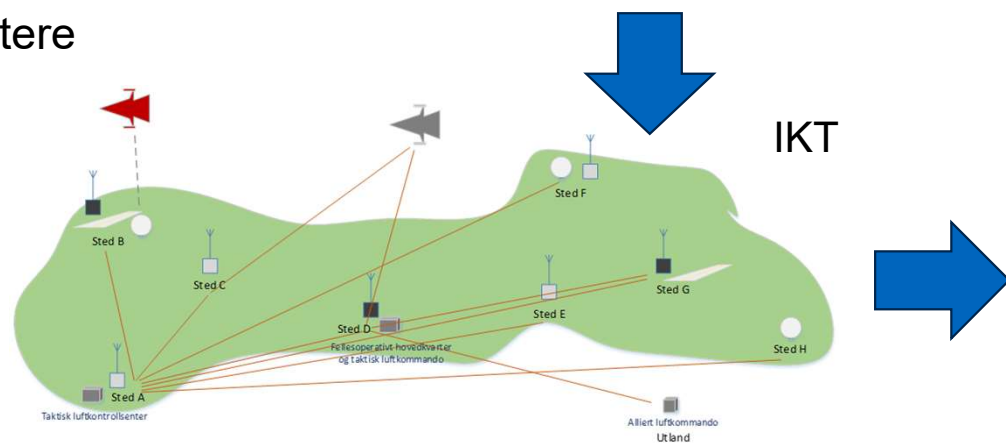
Evne til å markere norsk suverenitet og håndtere episoder i fred

- **Prosesser**

- Overvåke luftrom og oppdage
- Gi ordre om oppdrag
- Ta av (scramble)
- Identifisere
- Avskjære/eskortere
- Returnere
- Rapportere

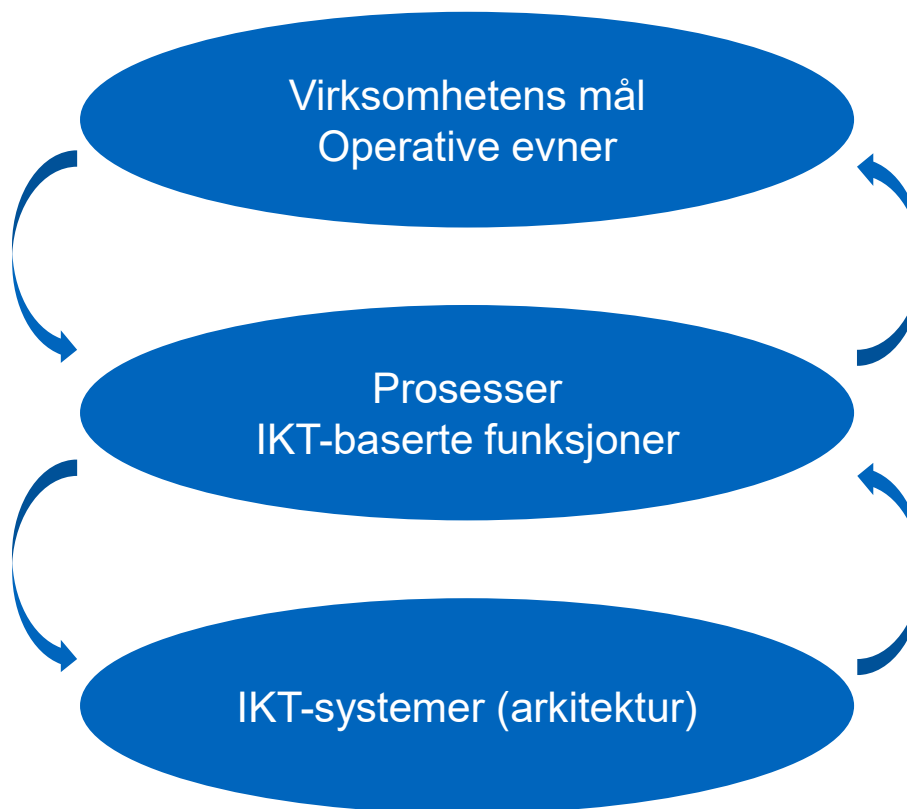
- **IKT-baserte funksjoner**

- Detektere, behandle og formidle data fra sensorer i radarkjeden
- Etablere, presentere og formidle luftbilde
- Kontakt med og innhenting av informasjon fra sivile luftfartsmyndigheter



Anbefaling: Verdisentrisk funksjonell systemkartlegging

- Top down kartlegging / modellering av virksomheten
 - Mål og kjerneverdier
 - Leveranser
 - Prosesser
 - IKT-systemer og arkitektur
- Krever bred involvering og samarbeid
 - Ledelse, operative miljøer, IKT-ekspertise, ...
- Helt nødvendig utgangspunkt for å kunne vurdere risiko



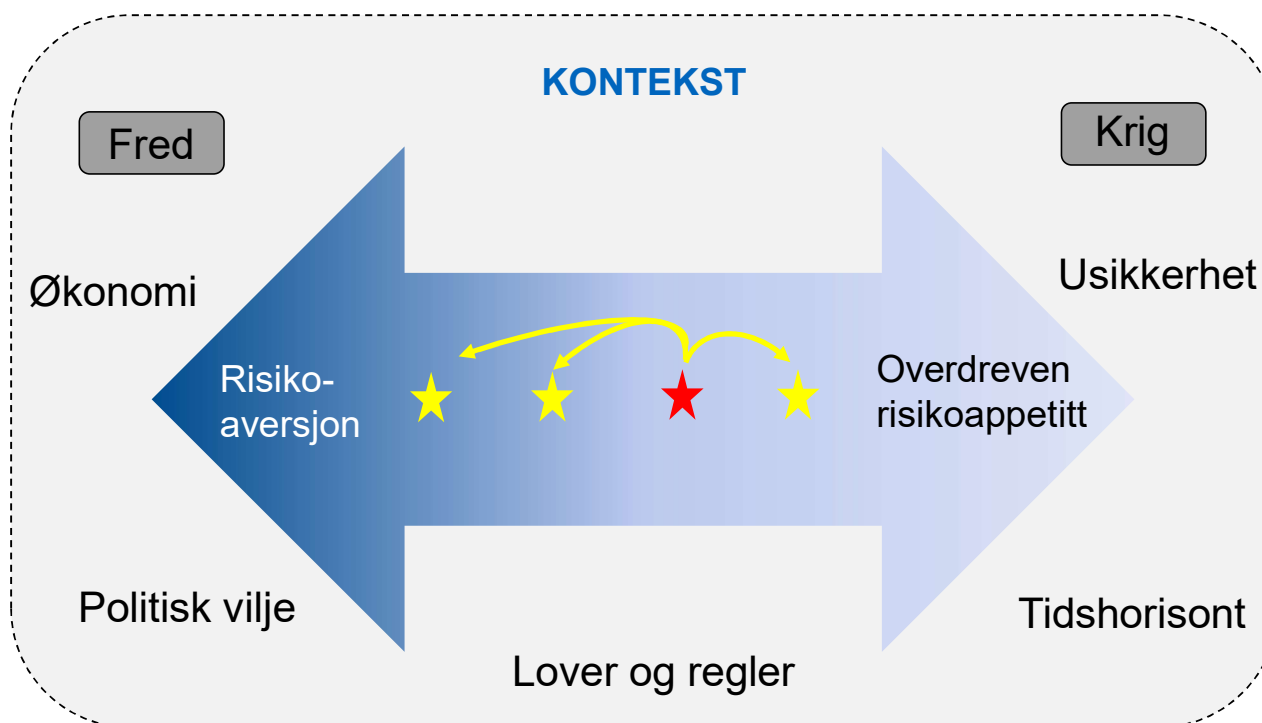
Utfordringer ved tilsiktede handlinger

- Dynamisk risiko
 - handlinger med lav frekvens, men potensielt store konsekvenser
 - strategisk tenkende aktør som tilpasser seg og endrer mål og operasjonsmønster
- Ikke nok ressurser til å sikre alt
- Stort antall mulige angrepsscenarioer og sikringsmuligheter
- Begrenset med historiske data
- Subjektiv vurdering av hva akseptabel risiko er

Dillon et al. (2009). *Risk Analysis* 29 (3), 321 – 335.

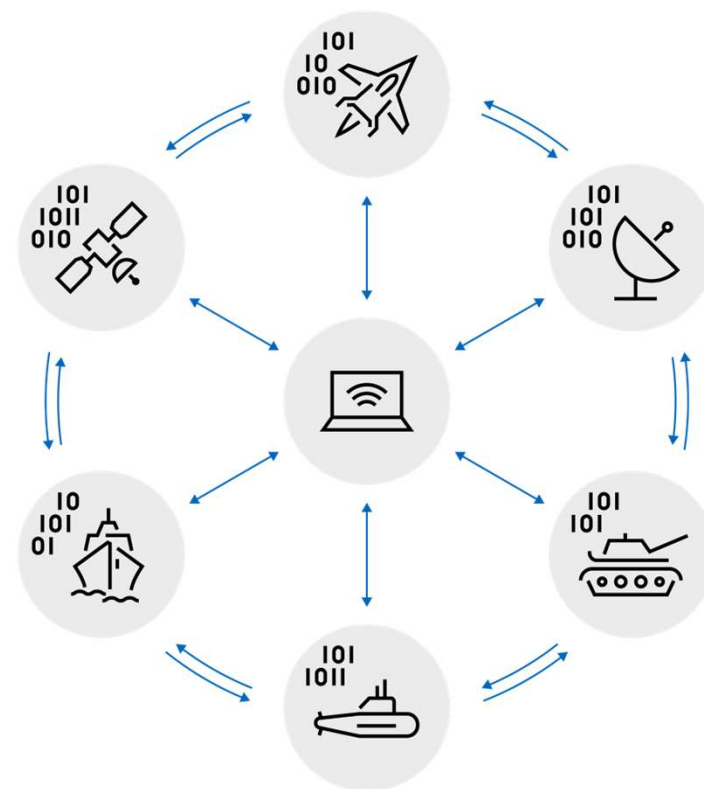
Kontekst og dynamikk påvirker forsvarlig sikkerhetsnivå

- Et **forsvarlig sikkerhetsnivå** oppnås når kritiske verdier er beskyttet mot aktuelle trusler slik at den totale risikoen er akseptabel
- **Risikovurdering**
 - Identifisere verdier
 - Tilhørende trusler og sårbarheter
 - Usikkerhet
 - Risikobilde
 - Anbefalinger
- **Risikohåndtering**
 - Kost/nytte vurderinger
 - Andre hensyn
 - Risikovilje
 - **Sikkerhetstiltak** endrer restrisiko
- **Konteksten** påvirker vurderingene som utgjør hva som er et forsvarlig sikkerhetsnivå til enhver tid



Anbefaling: Dynamisk risikostyring

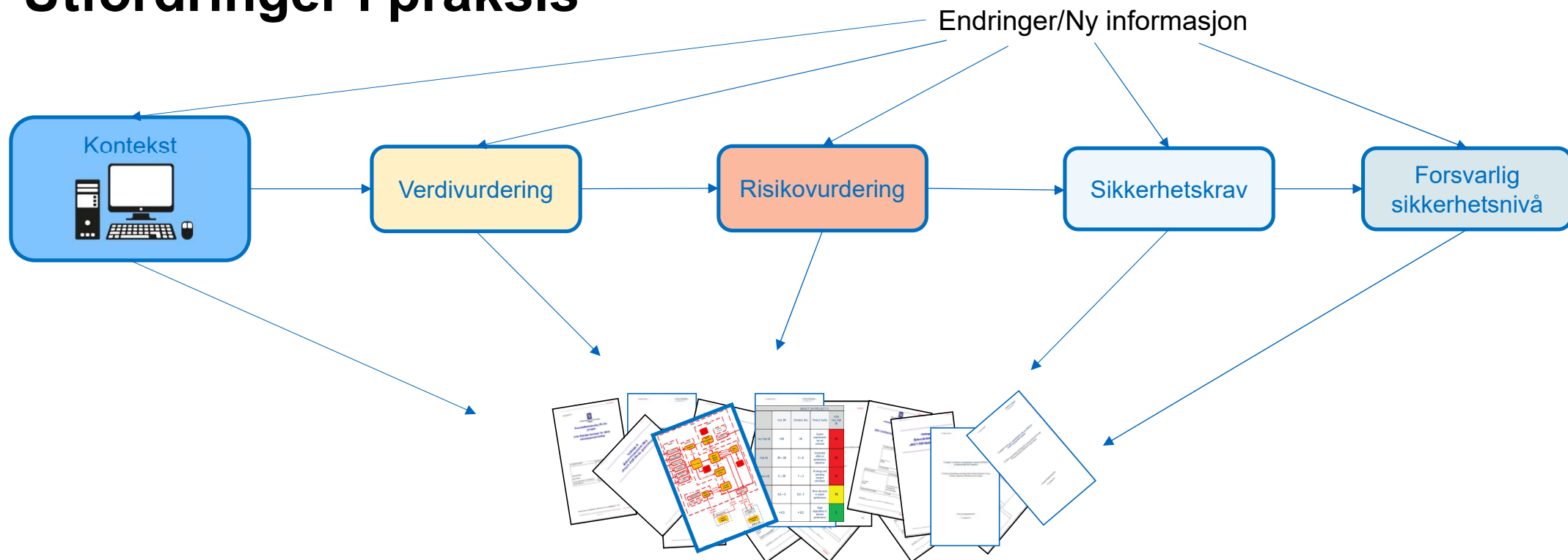
- Operativ kontekst og dermed operative behov er dynamiske
 - IKT-tjenestene skal dekkes i det daglige, i øvelser, og i krise og væpnet konflikt
- Teknologiske oppdateringer og endringer i IKT-tjenestene i seg selv
- Endringer i digitale verdikjeder som endrer risikobildet
- Endringer i trusselbildet som påvirker behovet for sikkerhetstiltak



Utfordringer i praksis - usikkerhet, sannsynlighet og kommunikasjon av risiko

- Kunnskapsgrunnlaget kan være ufullstendig eller skjevt
 - Kombinasjon av relevante data, erfaringer, eksperimenter, modelldata og ekspertvurderinger
 - Variasjon og uenighet i tolkninger og ekspertvurderinger
- Usikkerhet knyttet til trusler og sannsynligheter for hva som kan skje
 - Dynamisk bilde som kan endre seg raskt pga politisk klima, aktørers evne og nye sårbarheter
 - Utvalg av tenkbare hendelser (scenarier)
- Usikkerhet knyttet til systemforståelse, verdier og konsekvenser
 - Komplekse sosio-tekniske systemer med integrerte fysiske og digitale komponenter
 - Avhengigheter, både andres avhengighet av virksomheten og virksomhetens avhengigheter av andre
 - Verdiers kontekst og tidsvariasjon
- **Anbefaling: Utføre og presentere en usikkerhetsanalyse for beslutningstakere**
 - Unngå overforenkling

Utfordringer i praksis



- Mye ustrukturert informasjon
- Lite sporbarhet/sammenheng
- Statisk prosess



Anbefaling: Strukturering, digitalisering og automatisering må til for å håndtere kompleksiteten og muliggjøre fortløpende vurderinger

Oppsummering av anbefalinger

- **Verdisentrisk og funksjonell systemkartlegging som grunnlag for risikovurdering**
 - IKT i seg selv skaper ikke verdi, men det er hvordan IKT brukes som gir verdi
 - «Så enkelt som mulig, men som komplekst som nødvendig»
 - **En god risikovurderingsprosess er tverrfaglig**
 - Militærfaglig kompetanse, teknologisk kompetanse og risiko- og sikkerhetsfaglig kompetanse
- **Dynamisk risikostyring** som hensyntar endringer i operativ kontekst, teknologi og trusselbildet
- **Utføre og presentere en usikkerhetsanalyse for beslutningstakere**
- Strukturering, digitalisering og automatisering er nødvendig for å sikre dokumentasjon, gjennomsiktighet, sporbarhet og etterprøvbarehet



FFI

Forsvarets
forskningsinstitutt

**Vi gjør kunnskap og ideer
til et effektivt forsvar**