

Helhetlig styring og kontroll

Informasjonssikkerhet

Katrine Aam Svendsen
Seniorrådgiver
17.11.21 – NIFS

Agenda

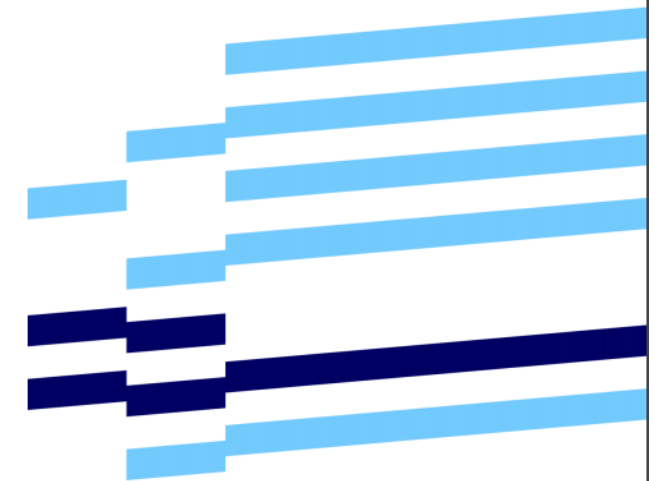
- Bakgrunn
- Hva vil det si å jobbe helhetlig?
- Ulike perspektiver gir ulikt fokus
- Fellestrekk ved styring og kontroll
- Ha oversikt – viktig utgangspunkt for helhetlig arbeid

Difi rapport 2018:4

- Kartlegging av statsforvaltningens arbeid med:
 - Styring og kontroll, og risikostyring
 - Beredskap, øvelser og hendelseshåndtering
 - Nasjonale felleskomponenter
 - Sikkerhetskultur
 - Kompetanse
 - Etatsstyringsdialogen
- Hovedfunn:
 - en av tre statlige virksomheter har ikke tilstrekkelig styring og kontroll på informasjonssikkerhet
 - departementer etterspør i liten grad status på arbeidet med informasjonssikkerhet hos underliggende virksomheter

Arbeidet med informasjonssikkerhet i statsforvaltningen

Kunnskapsgrunnlag



Andre forutsetninger

- IKT-sikkerhetsutvalget 2018 – «IKT-sikkerhet i alle ledd»:
 - «(...) brukerne er usikre på hvor de skal henvende seg for å få råd og veiledning om IKT-sikkerhet.»
 - «Fra et brukerperspektiv kan det være krevende å forholde seg til mange aktører»
- Tiltaksoversikt til nasjonal strategi for digital sikkerhet – Tiltak 5: «Sikker digitalisering i offentlig sektor»
 - «Virksomhetene i offentlig sektor skal få et mer samordnet og helhetlig tilbud om veiledning om digital sikkerhet»

Samarbeid mellom



NASJONAL
SIKKERHETSMYNDIGHET



Direktoratet for forvaltning
og økonomistyring



Dialog med



Datatilsynet



Hva vil det si å jobbe helhetlig?

Å se sammenhengen mellom viktige områder og aktiviteter i virksomheten.

Ved å se aktiviteter, risikoer og tiltak på tvers av fagområder og avdelinger kan virksomheten oppnå bedre styring og kontroll.

Å jobbe helhetlig innebærer at

alle relevante områder
er inkludert

prosesser er
gjenkjennbare på tvers
av fagområder

ledelsen og ansatte forstår
sammenhengen mellom områdene

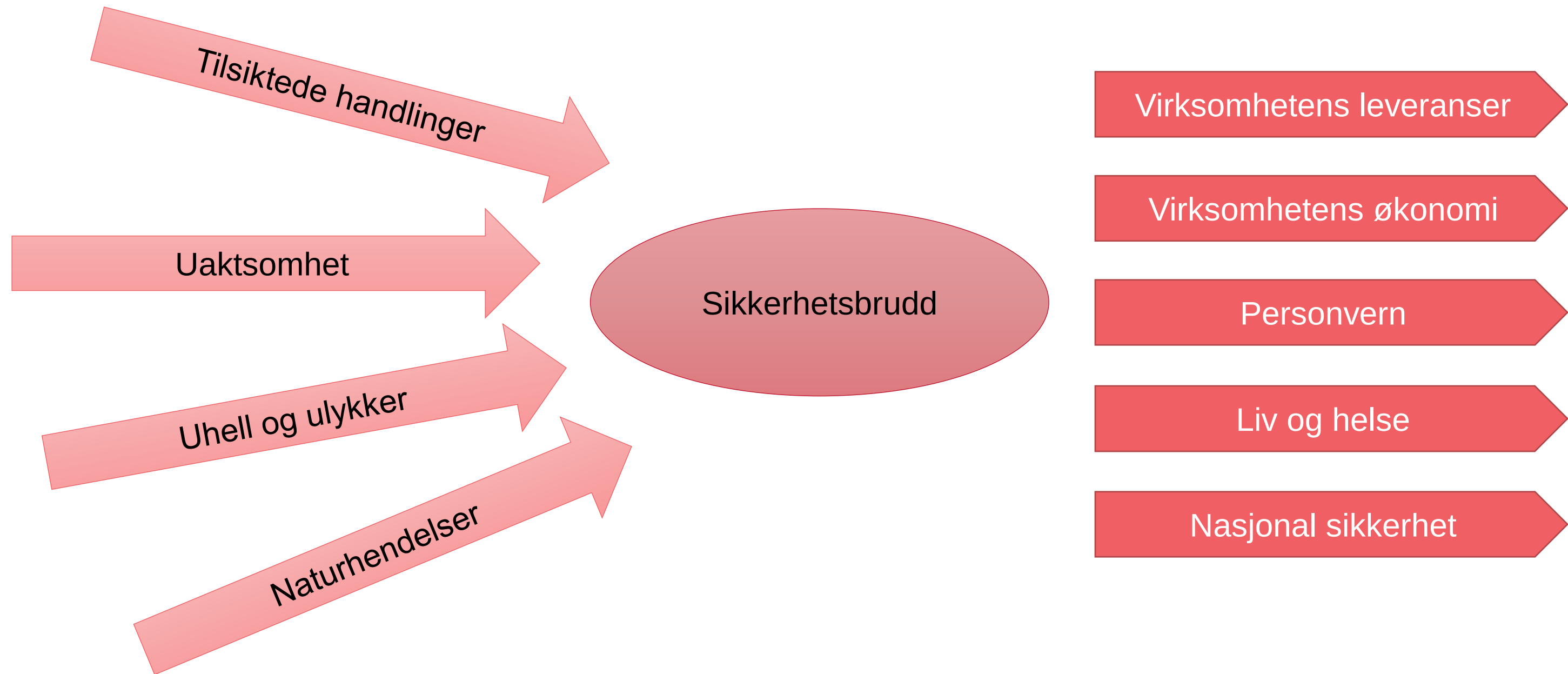




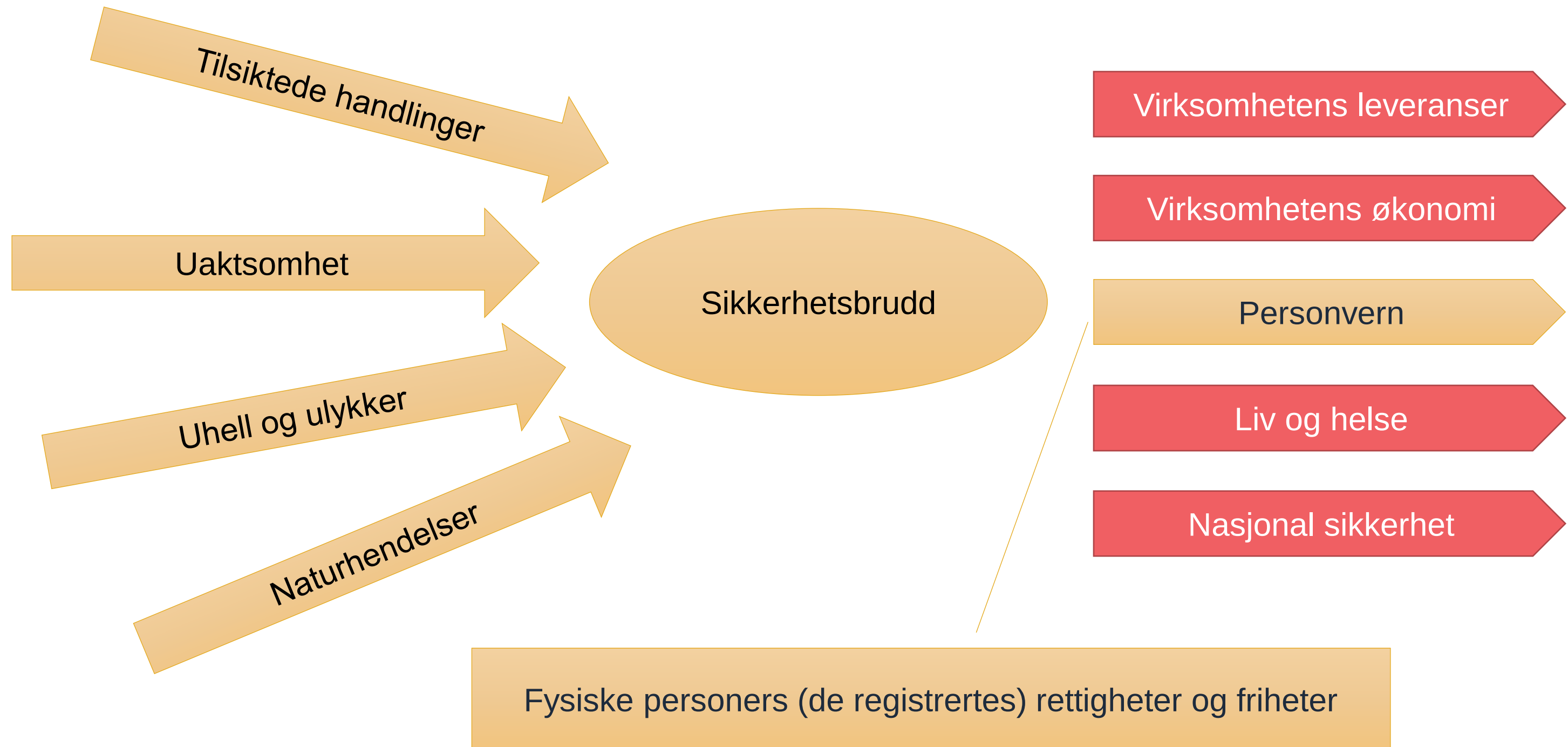
Ulike perspektiver gir ulikt fokus

Årsaker

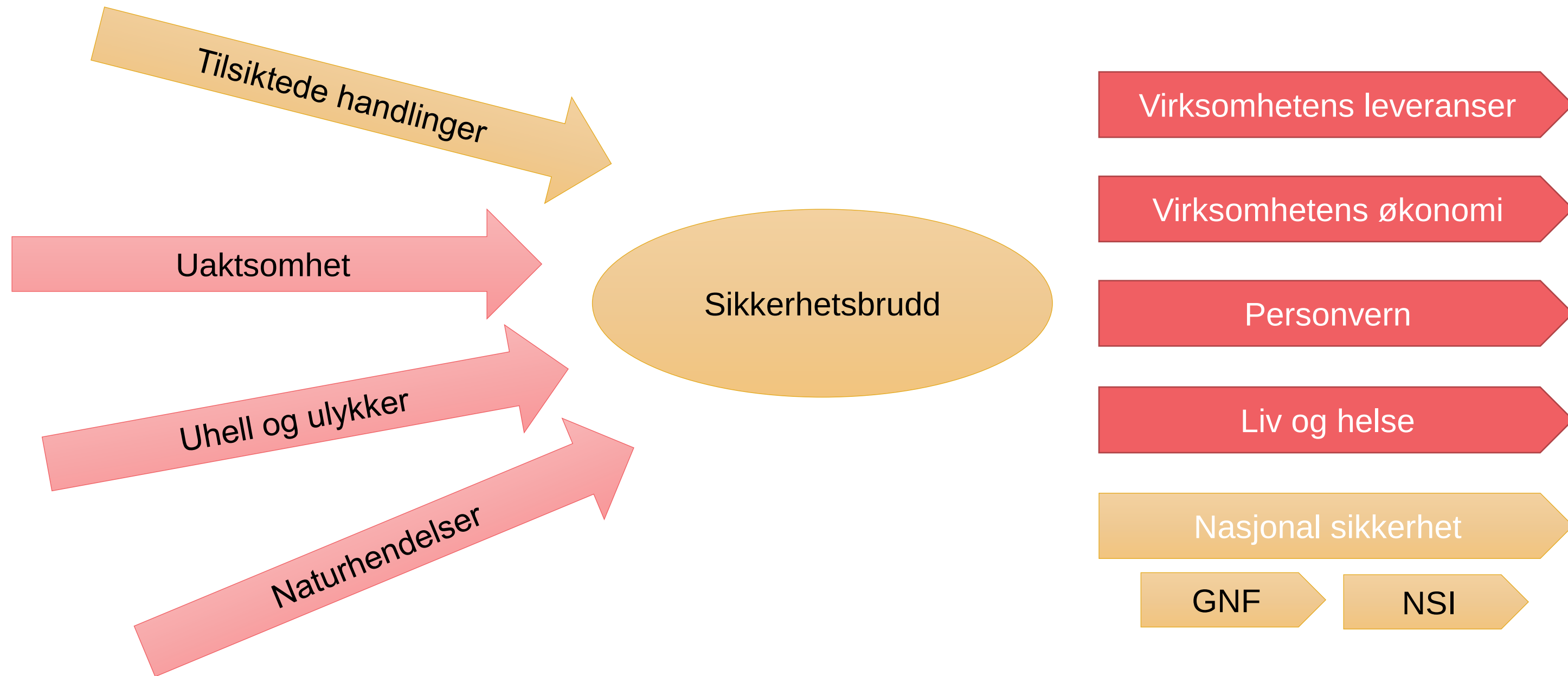
Konsekvenskategorier



Personopplysningsloven m/personvernforordningen



Lov om nasjonal sikkerhet (sikkerhetsloven)

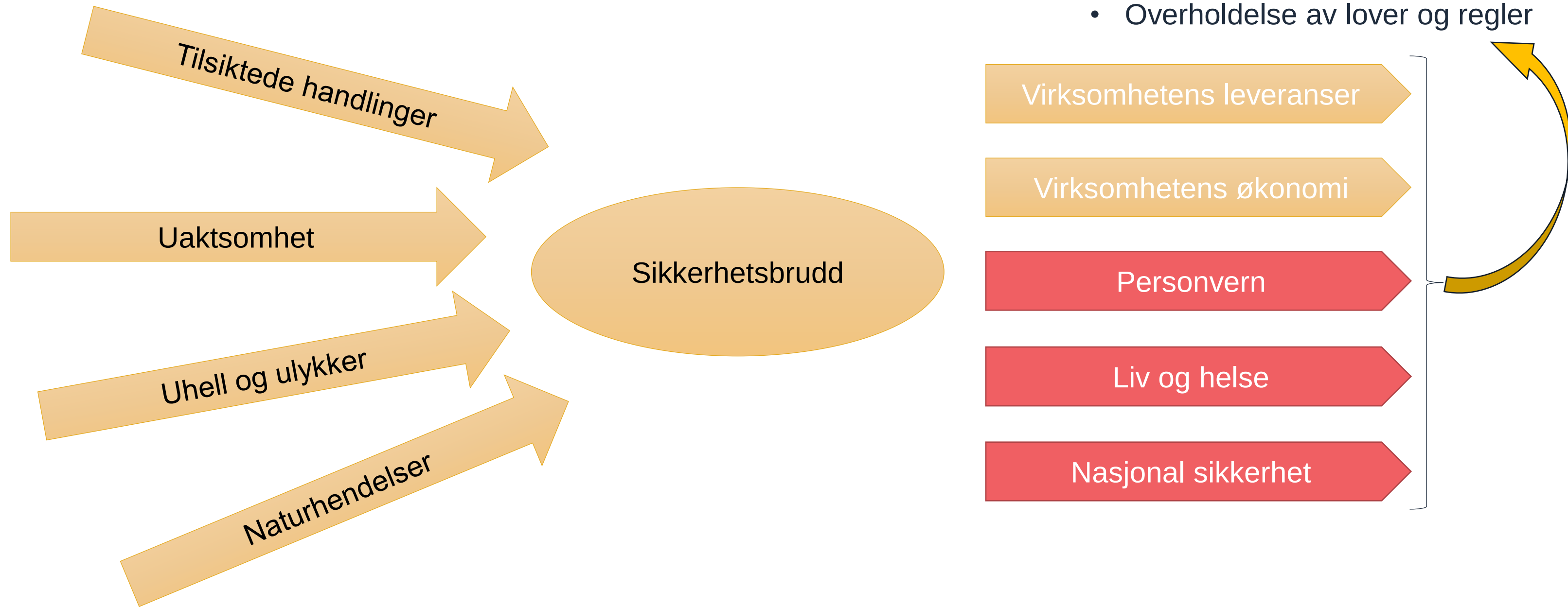


Obs: konseptuell forståelse. Det er f.eks. krav om å sikre at informasjonssystem fungerer slik de skal i sl § 6-2 a.

GNF = Grunnleggende nasjonale funksjoner

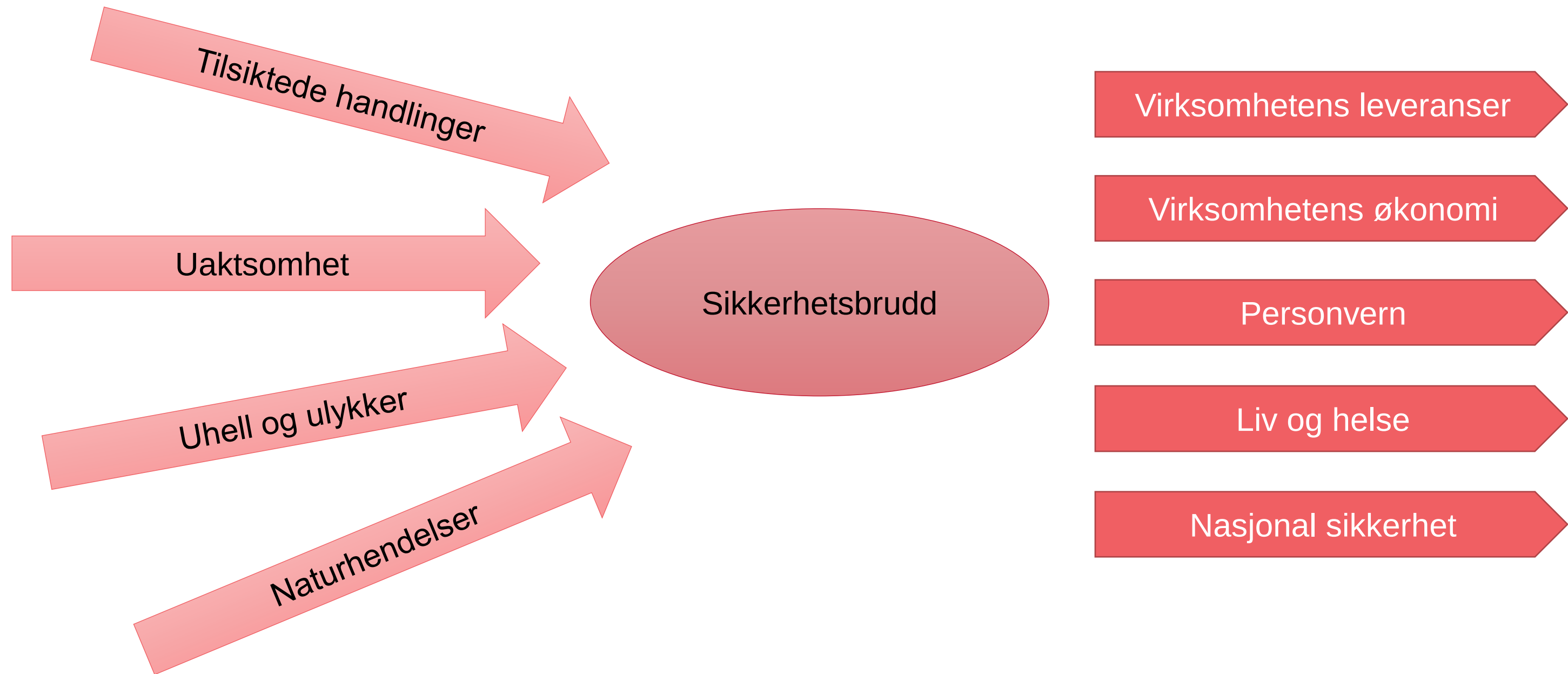
NSI = Nasjonale sikkerhetsinteresser

Økonomiregelverket i staten



Årsaker

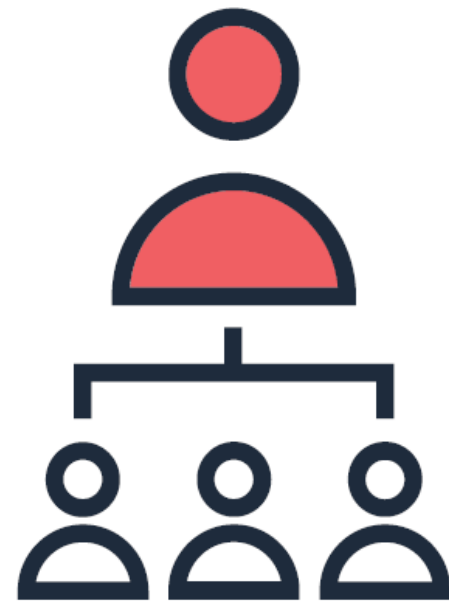
Konsekvenskategorier

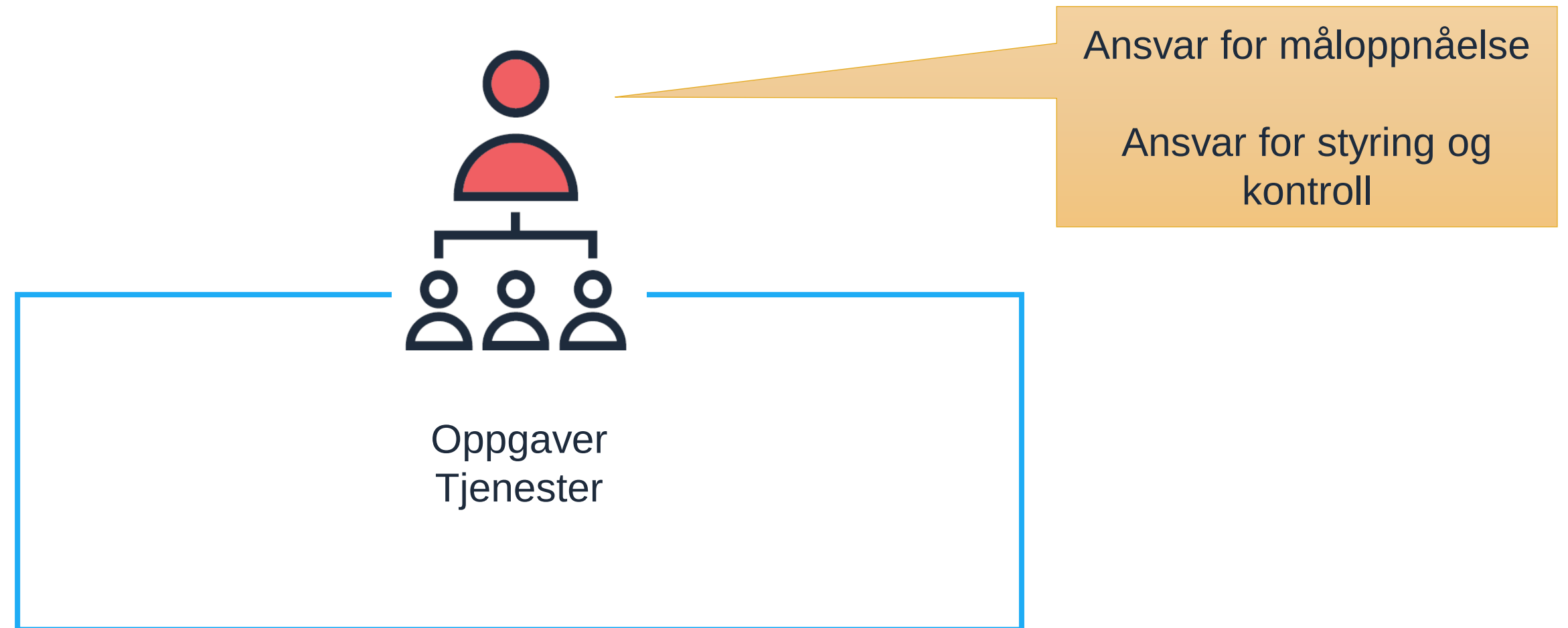


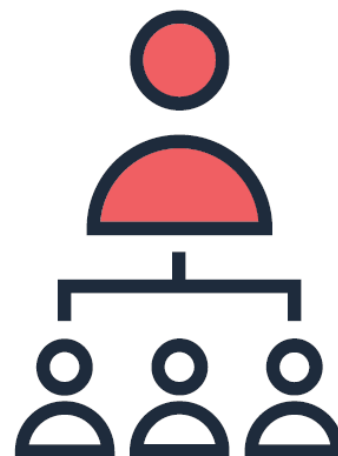


Fellestrekk ved styring og kontroll

Ledelsen må lede an







Oppgaver
Tjenester

Overordnet ansvar for at arbeidet med informasjonssikkerhet gjennomføres på en hensiktsmessig måte

Sørge for at
styringsaktivitetene
blir etablert

Følge opp slik at de
gjennomføres på en
god måte

Ha tydelige roller og ansvar



Risikoeier



- Linjeledere og andre med operativt ansvar
 - Ansvar for mål og resultater
 - Ansvar for risiko innen sitt område
- må kjenne sin rolle, og vite hva som ligger i den



Samme person skal forstå, vurdere og ta beslutninger om risiko innen ulike områder – for eksempel informasjonssikkerhet, personvern, HMS og økonomi.

Toppleder med ledergruppe

- Gi føringer
- Ansvarlig for at aktiviteter for etablering/forbedring gjennomføres
- Kommunisere viktighet – «Tonen på toppen»
- Virksomhetsledelsens gjennomgang



- Hvilke aktiviteter skal gjennomføres?
- Hvem skal være ansvarlig?
- Nivåer for konsekvens og sannsynlighet
- Kriterier for å akseptere risiko
- Etc.

Tiltaksleverandør

- Ansvarlig for sikkerhetstiltak
- Utforming, etablering, forvaltning
- Felles tiltaksleverandører
 - IT-avdeling
 - Bygningsansvarlig
 - Personalfunksjon/HR
- Ekstern tjenesteleverandør



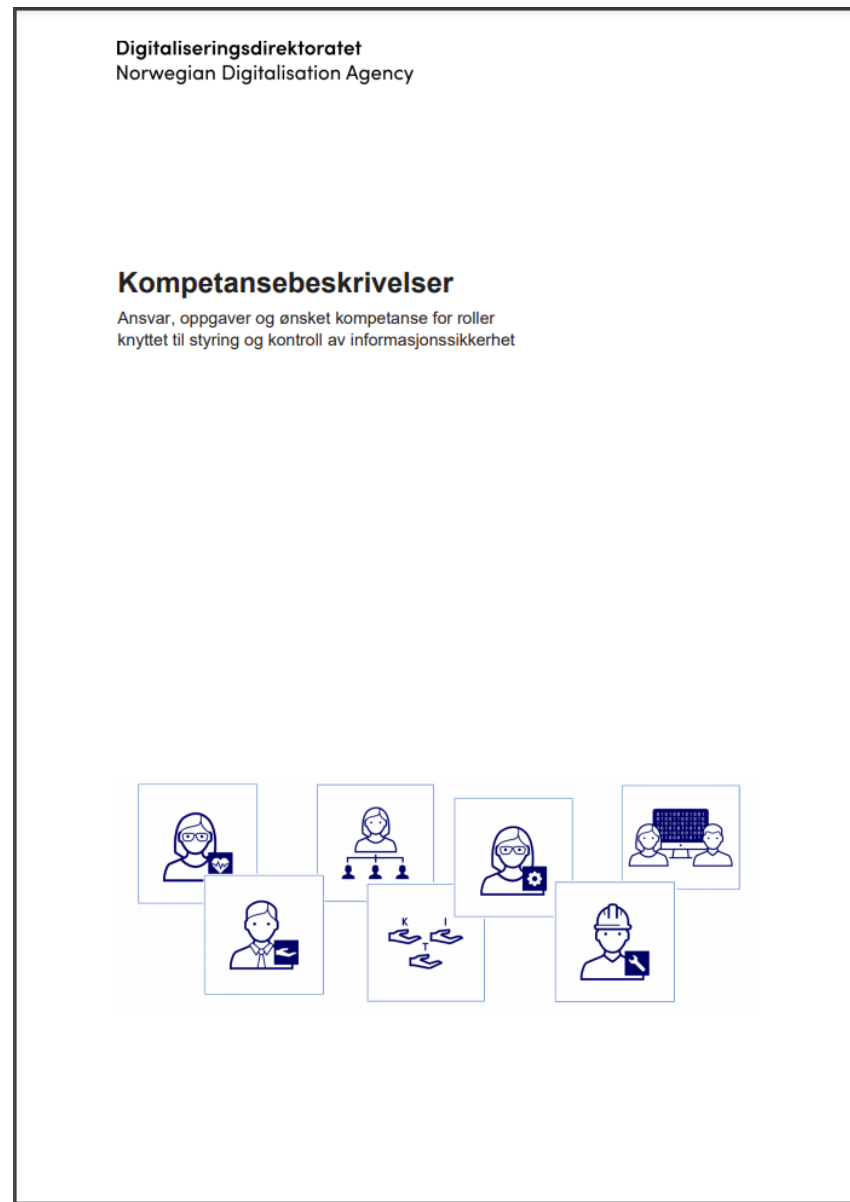
Fagansvarlig informasjonssikkerhet



- Har hovedansvaret for å støtte ledelsen i arbeidet med styring av informasjonssikkerhet
 - Tilrettelegge for god gjennomføring av styringsaktivitetene
 - Andre ofte brukte titler:
 - Informasjonssikkerhetsansvarlig
 - Informasjonssikkerhetsleder
 - CISO



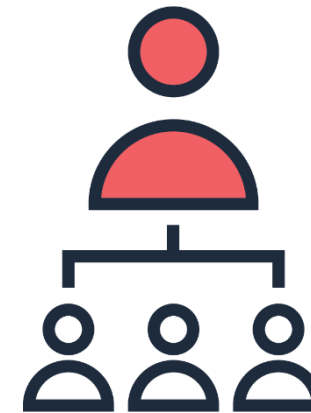
Kompetansebeskrivelser



<https://www.digdir.no/1107>

Fire historier om styring

Turid Toppleder



Linus Linjeleder



Fridtjof
Fagansvarlig

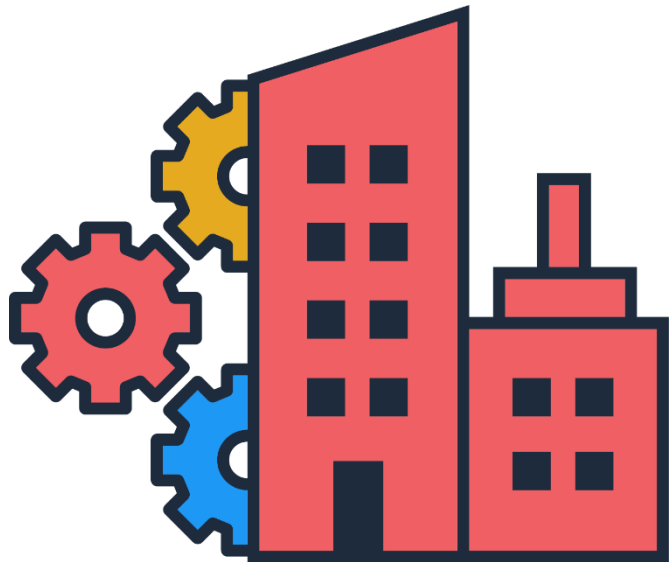


Trine
Tiltaksleverandør

<https://www.digdir.no/2647>

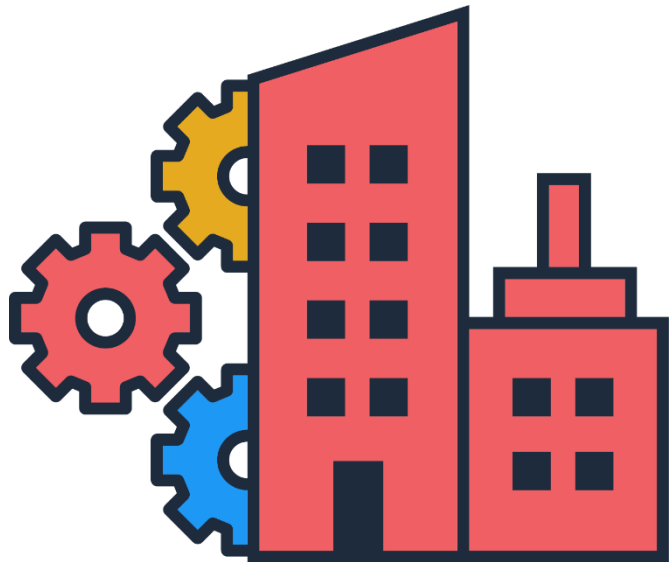
Jobb systematisk

Jobb risikobasert



Styring og kontroll:

En prosess, eller et sett med systematiske aktiviteter, som er nødvendige for å oppnå og opprettholde tilstrekkelig sikkerhet.



Styringsaktiviteter

- Ledelsens styring og oppfølging
- Risikovurdering
- Risikohåndtering
- Overvåking og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling
- Kommunikasjon



Omfang og innretning må stå i forhold til virksomhetens oppgaver og behov

Styringsaktiviteter

- Ledelsens styring og oppfølging
- Risikovurdering
- Risikohåndtering
- Overvåking og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling
- Kommunikasjon



Sikkerhetstiltak

Formål

- Forebygge
- Oppdage
- Håndtere og gjenopprette

Typer

- Organisatoriske
- Menneskelige
- Fysiske
- Teknologiske

Forutsetninger for å lykkes med å jobbe risikobasert

- Ulike typer kompetanse
- Gode føringer for å forstå, vurdere og håndtere risiko
- Gode, anvendbare kriterier for å akseptere risiko



Bygg riktig kompetanse og en god kultur



De ansatte må se arbeid med styring og kontroll i sammenheng med

Oppgaver/tjenester som utføres

Informasjonen som forvaltes

Virksomhetens målsetninger

De ansatte må vite

Hva de skal gjøre

Hvordan de skal gjøre det

Hvor de finner informasjon

Hvorfor dette er viktig for dem i deres arbeidshverdag



Gjennomfør ledelsens gjennomgang

Gjennomfør evalueringer

Sørg for kontinuerlig forbedring

Ledelsens gjennomgang

- Formål: vurdere status på virksomhetens arbeid med informasjonssikkerhet
- Resultat: beslutninger knyttet til kontinuerlig forbedring, og andre behov for endringer av det systematiske arbeidet

Evalueringer

- bør inkludere både styringsaktivitetene og sikkerhetstiltak som er iverksatt
- kan for eksempel kartlegge om det systematiske arbeidet med informasjonssikkerhet:
 - gjennomføres i henhold til de føringer som er satt
 - er hensiktsmessig organisert
 - er kostnadseffektivt

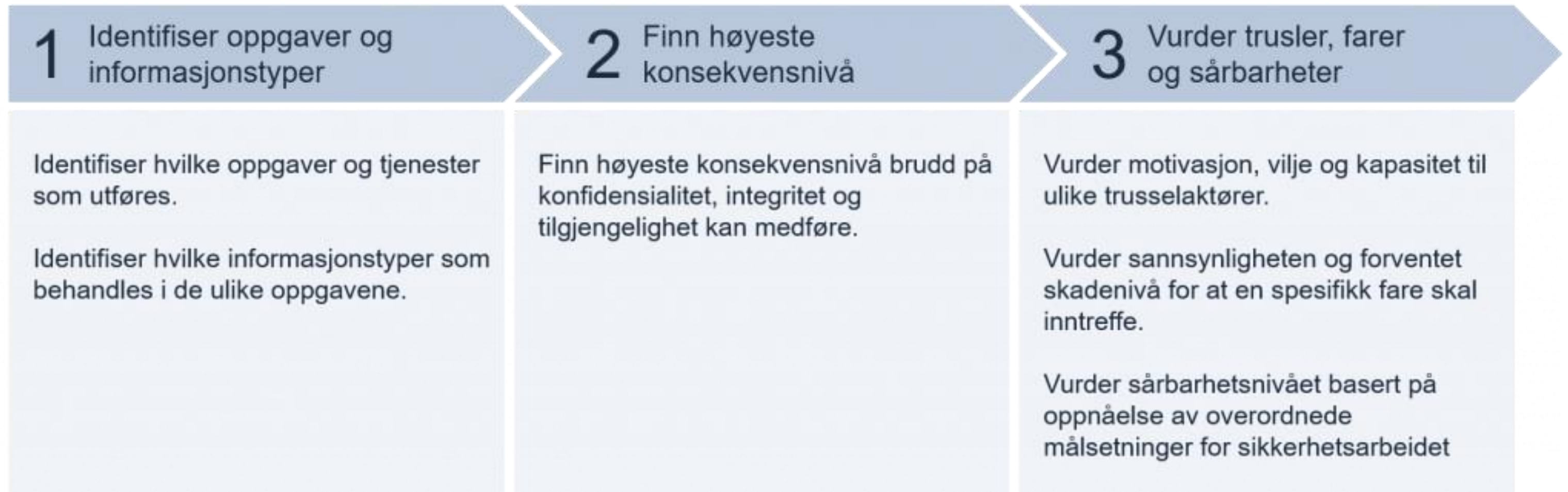
Kontinuerlig forbedring

- regelmessig og systematisk oppfølging, slik at svakheter og feil i styringsaktiviteter og sikkerhetstiltak korrigeres.
- benytte ulike kilder til informasjon om eget arbeid til å forbedre det
- gjøre arbeidet mer effektivt, slik at man får mest mulig ut av de ressursene som brukes



Ha oversikt –
viktig utgangspunkt for
helhetlig arbeid

Foranalyse



Foranalyse – bruk i helhetlig arbeid



Stifinneren



1 Hvor er vi, hvor skal vi?

2 Hvordan skal ting fungere hos oss?

3 Prøve ut og justere

4 Bygge et godt grunnlag

Hovedsaken **5**

6 Hvordan går det?

7 Forbedre og justere

SPØRSMÅL?

infosikkerhet@digdir.no
www.digdir.no/infosikkerhet



digdir.no

Digitaliseringsdirektoratet
postmottak@digdir.no
22 45 10 00
Postboks 1382 Vika, 0114 Oslo

Besøksadresser:
Industriveien 1, 8900 Brønnøysund
Skrivarevegen 2, 6863 Leikanger
Grev Wedels Plass 9, 0151 Oslo