Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

# Helhetlig styring og kontroll av informasjonssikkerhet

Katrine Aam Svendsen
4. februar 2020

# Agenda

| Tid | Tema |
|---|---|
| 10:00 | Velkommen og nytt fra Digitaliseringsdirektoratet |
| 10:10 | Innledning v/Digitaliseringsdirektoratet |
| 10:50 | Pause |
| 11:00 | Gruppeoppgaver<br>1.Hva gjør at veiledningstilbudet oppleves som lite helhetlig nå?<br>2.Hvordan ser det ut når det er et samordnet og helhetlig tilbud om veiledning? |
| 12:00 | Lunsj |
| 12:45 | Presentasjon av sammenhenger mellom eksisterende veiledning og føringer |
| 13:45 | Pause |
| 14:00 | Videre diskusjon i grupper |
| 14:30 | Oppsummering og avslutning |
| 15:00 | Slutt |

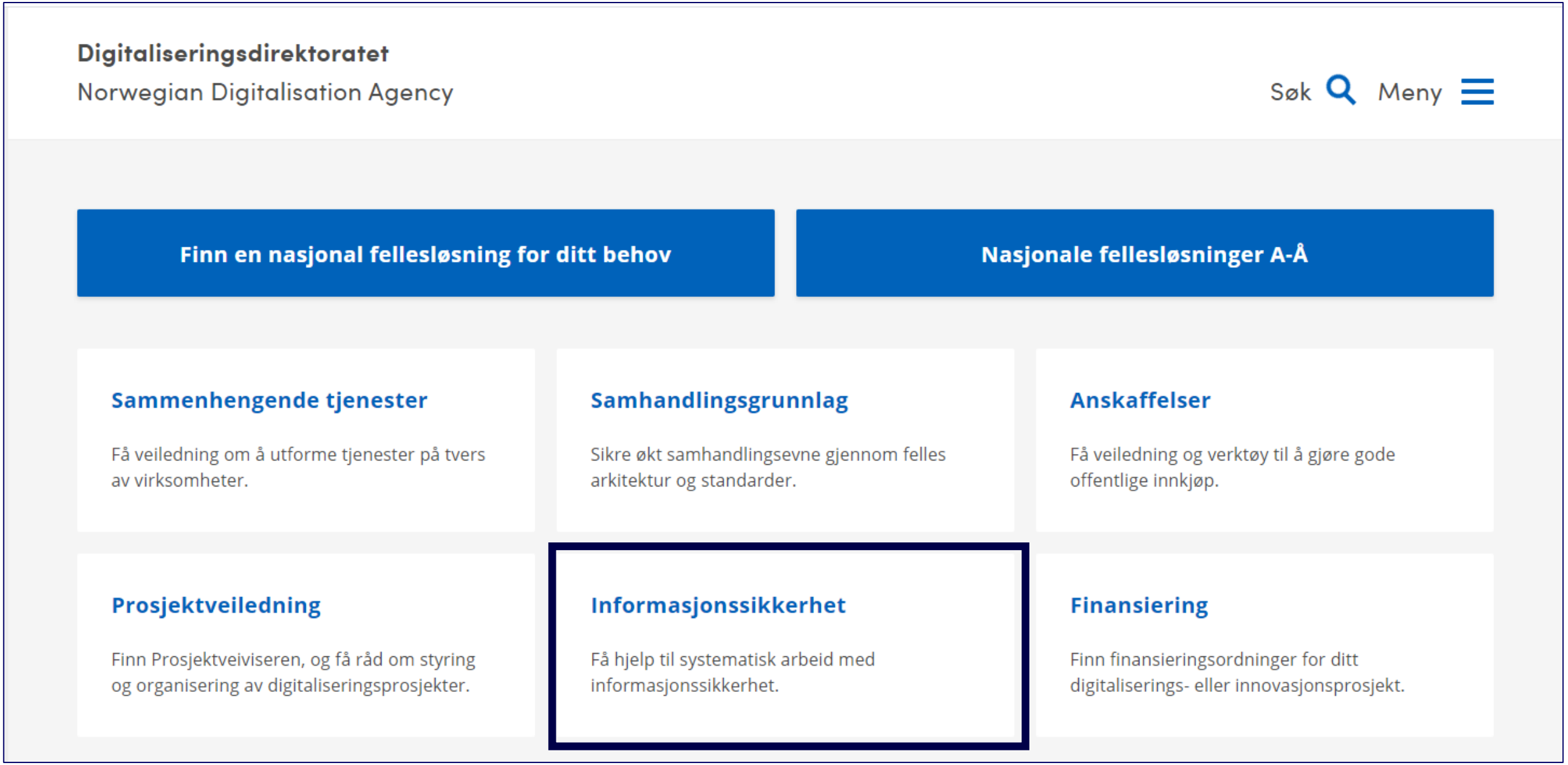
# Nytt fra Digitaliseringsdirektoratet

Difi
Direktoratet for forvaltning og ikt

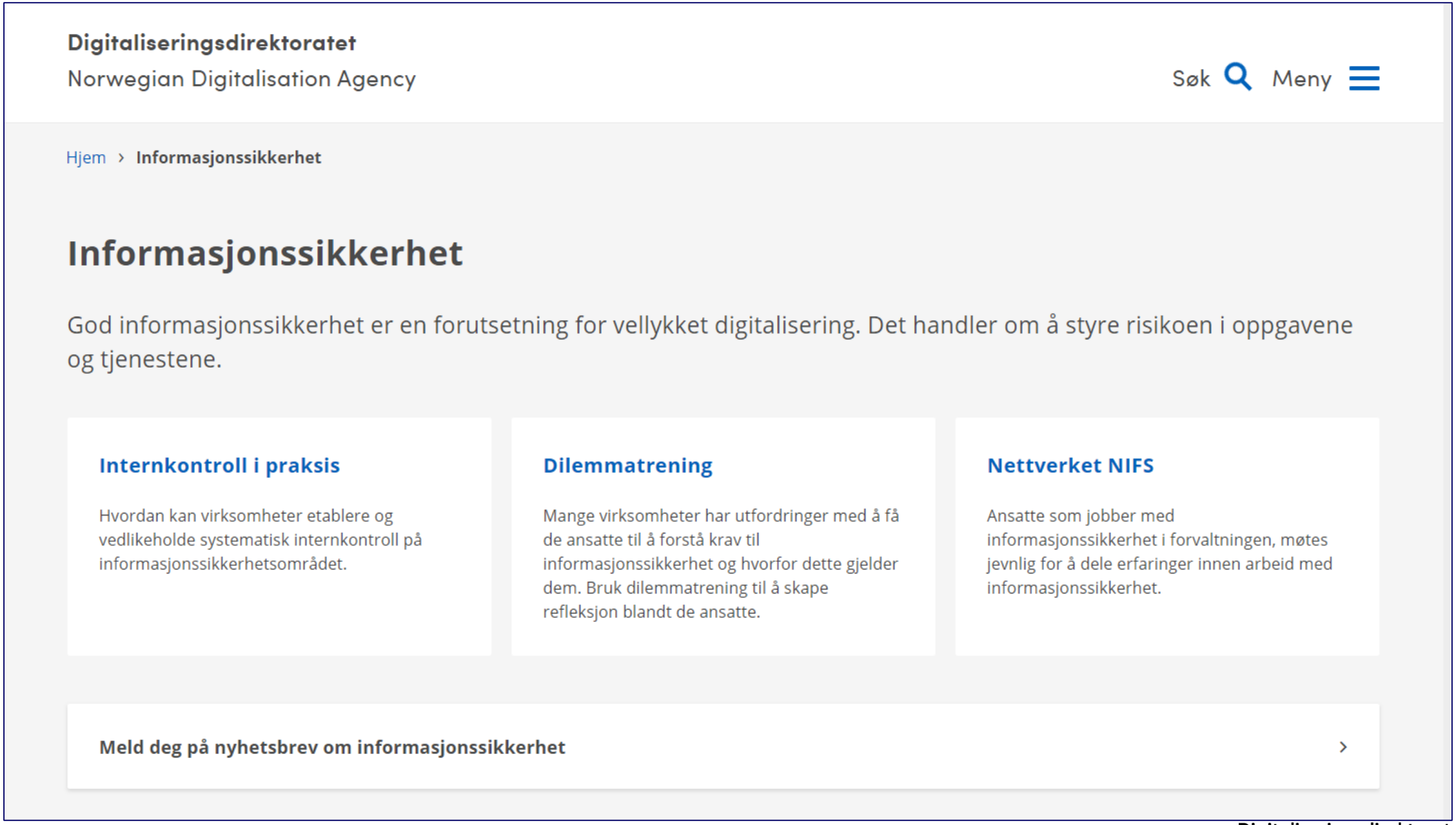
altinn

Deler av informasjons-forvaltningsmiljøet i Brønnøysundregistrene

**Digitaliseringsdirektoratet**
Norwegian Digitalisation Agency




https://www.digdir.no




https://www.digdir.no/infosikkerhet/882

# Publisert siden sist …

# Veileder for etterlevelse av forvaltningsstandardene

**Denne veilederen beskriver formålet med hver av fire sikkerhetsrelaterte forvaltningsstandarder og hvordan de bør iverksettes på systemene hvor de skal brukes.**

*Publisert: 17. des 2019, Sist endret: 18. des 2019*

De fire standardene er:

- Anbefalte standarder for sikker datak
- Anbefalt standard for transportsikrin
- Anbefalte standarder for å motvirke f
- Anbefalte standarder for sikker bruk

Vi kaller standardene i referansekatalog
at de fire forvaltningsstandardene viser
standarder og har gjerne en kort beskriv
standardene skal brukes sammen.

# Veileder for testing av etterlevelse

**Denne veilederen beskriver hvordan man kan teste etterlevelse av de fire forvaltningsstandardene som er anbefalt i Referansekatalogen for IT-standarder.**

*Publisert: 17. des 2019, Sist endret: 02. jan 2020*

I denne veilederen har vi plukket ut fire verktøy som kan brukes til testing. De to første verktøyene, **hardenize** og **internet.nl**, er noenlunde likeverdige og gir svar som er relevante for alle standardene med unntak av DKIM. Hardenize.com sjekker ikke DKIM i det hele tatt, og internet.nl

https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet/veiledere/veileder-testing-av-etterlevelse

Difi
Direktoratet for forvaltning og ikt

# Kompetansebeskrivelser

Ansvar, oppgaver og ønsket kompetanse for roller knyttet til styring og kontroll av informasjonssikkerh

Difi
Direktoratet for forvaltning og ikt

## Fagansvarlig informasjonssikkerhet

### Ansvar og oppgaver

Fagansvarlig informasjonssikkerhet har som hovedansvar å være pådriver og støtte til ledelsen og organisasjonen for øvrig i informasjonssikkerhetsarbeidet.

Hvilken stilling den fagansvarlige har i virksomheten vil variere avhengig av virksomhetens organisering og behov. Dersom fagansvarlig har en stilling som leder i virksomheten vil oppgavene og ansvaret komme i tillegg til oppgaver og ansvar vedkommende har som følger stillingsbeskrivelsen.

Difi
Direktoratet for forvaltning og ikt

## Rådgiver informasjonssikkerhet

### Ansvar og oppgaver

I denne forbindelsen mener vi personer som er støtteressurser i fagansvarlig informasjonssikkerhets arbeide i organisasjonen. Dette trenger ikke være fulltidsressurser.

Hovedansvaret til vedkommende er å støtte fagansvarlig i det arbeidet vedkommende gjør – bistå i tilknytning til ledelsens styring og oppfølging, gi råd og delta som informasjonssikkerhetsressurs i prosjekter og oppgaver i virksomheten, bistå i gjennomføring av risikovurderinger og -håndtering, planlegge og gjennomføre opplæring

### Ønsket kompetanse

Kompetansebehovet for en støtteressurs i

arbeidsoppgaver vedkommende har.

Ofte vil det være hensiktsmessig at en slik

fagansvarlig, men vedkommende kan ha n

Avhengig av virksomhetens evne og muligh

liten erfaring ha denne rollen. Det er da vik

risikostyring og internkontroll, og at de gje

fagområdene.

I noen virksomheter vil støtteressursene a

hensiktsmessig om de har mer spisskompe

risikovurderinger/-håndtering, revisjon, he

### Tema for intervju/medarbeidersamtale

Når man skal vurdere kompetansen til per

er det viktig at man tar utgangspunkt i hva

kompetanse som er vesentlig. Noen aspek

Forståelse for at informasjonssikkerhet ha

tilgjengelighet, og at det handler om mye

sikkerhetsloven.

Forståelse for at risikobildet er i stadig end

Forståelse av de aktivitetene vedkommen

informasjonssikkerhet understøtter virkso

Forståelse for at informasjonssikkerhet er

formidle dette til de ansatte.

Difi
Direktoratet for forvaltning og ikt

## Systemeier

### Ansvar og oppgaver

Med systemeier mener vi i denne forbindelsen ansatte som har et særskilt ansvar for et gitt IKT-system. Dette kan variere fra en virksomhet til en annen.

Systemeiere vil ha ansvaret for risiko knyttet til systemet de er ansvarlige for, og vil derfor også være risikoeiere. De har derfor også ansvar og oppgaver som beskrevet under «Risikoeier». Dersom et system benyttes i kun én arbeidsoppgave/prosess, bør vurdering og håndtering av risiko for arbeidsoppgaven og systemet sees i sammenheng.

Noen systemeiere er imidlertid ansvarlig for systemer som også benyttes av andre risikoeiere – vi kaller dem systemeier fellessystem. I slike tilfeller er det systemeiers ansvar å ivareta interessene til de som benytter systemene i sin oppgaveløsning og tjenesteutføring. Systemeierne må derfor involvere risikoeierne i risikovurderingsarbeid og andre internkontrollaktiviteter som utføres på fellessystemene.

### Ønsket kompetanse

Systemeiere bør ha grunnleggende kunnskap om informasjonssikkerhet, og hvordan sikkerhetshendelser kan påvirke systemet de er ansvarlig for.

Systemeier bør ha grunnleggende kunnskap arbeidsoppgaven(e)/prosessen(e) systemet inngår i.

Systemeier fellessystemer bør ha evnen til å kommunisere og koordinere med ulike risikoeiere, og vurdere deres behov. De bør kunne inkludere dem i gjennomføring av risikovurdering og -håndtering, og hensynta deres vurdering av hvilke konsekvenser som kan oppstå dersom ulike hendelser inntreffer.

### Tema for intervju/medarbeidersamtale

Systemeier må ha forståelse for at man må se sammenhengen mellom system og arbeidsoppgave når man gjennomfører risikovurderinger. Det er ikke tilstrekkelig å gjøre en teknisk risikovurdering av systemet, det må også sees i sammenheng med hvordan arbeidsoppgaven(e) gjennomføres.

Systemeier fellessystem må ha forståelse for at det er de ulike risikoeierne som best kan si hvilke konsekvenser ulike hendelser kan få for virksomhetens måloppnåelse. Disse må derfor involveres i gjennomføringen av risikovurderinger.

Difi
Direktoratet for forvaltning og ikt

## Risikoeier (Linjeleder – operativt ansvarlig)

### Ansvar og oppgaver

Alle med mål- og resultatansvar på operativt nivå i virksomheten er ansvarlig for å håndtere den risikoen som er tilstede for de arbeidsoppgavene de er ansvarlige for. Dette innebærer også informasjonssikkerhetsrisiko.

Risikoeiere har ansvar for å ha tilstrekkelig oversikt over sitt ansvarsområde, for å kunne prioritere risikovurderinger slik at arbeidet med risikovurdering og -håndtering gjøres på en effektiv måte. Vedkommende er også ansvarlig for at nødvendige risikovurderinger gjennomføres, at identifiserte risikoer håndteres, blant annet ved at tiltak iverksettes. Beslutninger knyttet til risiko som vedkommende ikke har tilstrekkelig fullmakt til å håndtere, enten fordi risikonivået er for høyt, eller fordi kostnaden av eventuelle tiltak er for høy, må løftes i linjen på

Difi
Direktoratet for forvaltning og ikt

## Toppleder

### Ansvar og oppgaver

Toppleder er ansvarlig for at virksomheten har velfungerende styring og kontroll. Dette innebærer at arbeidet med informasjonssikkerhet gjennom

måte rundt om i hele virksomheten, tilpasset

Toppleder, med sin ledergruppe, må gi føring

informasjonssikkerhetsområdet skal være: h

være ansvarlig, beskrivelse av nivåer for kons

etc. Føringer forankrer ledelsens ansvar.

Toppleder

aktivitete

informasj

I det dagli

sette «to

vurdere o

aksepter

Toppleder

gjennom

tilstrekke

virksomh

### Ønsket kompetanse

Toppleder må forstå at det er ledelsens ansv

virksomheten er hensiktsmessig, og at ledels

Det er nødvendig med tilstrekkelig kunnskap

informasjonssikkerhet i den helhetlige virkso

Toppleder bør ha forståelse for at styring av

fra annen virksomhetsstyring og internkontro

ligger det også å forstå at styringssystem/int

aktiviteter, ikke en samling dokumenter.

Toppleder eier risikoen for at virksomheten i

arbeidet med styring og kontroll av informas

Effektiv risikostyring er viktig. Noe risiko må

definerte kriterier for å akseptere risiko, mer

Toppleder må også forstå hvordan informasj

informasjonsbehandlingen som gjennomføre

mål. For å forstå dette, må vedkommende o

om å sikre både konfidensialitet, integritet o

mer enn personopplysninger og beskyttelse

Informasjonssikkerhetsbrudd kan få konsekv

kan få konsekvenser for innbyggere, andre v

I tillegg er det viktig med forståelse for at ris

for eksempel dersom man velger å tjenesteu

Difi
Direktoratet for forvaltning og ikt

## Øvrig ledergruppe

### Ansvar og oppgaver

***Toppledergruppen*** bør ha forståelse for at de må være involvert i føringer for hvordan internkontrollen på informasjonssikkerhetsområdet skal være: hvilke aktiviteter som s gjennomføres, hvem som skal være ansvarlig, beskrivelse av nivåe konsekvens og sannsynlighet, kriterier for å akseptere risiko etc.

***Ledere på alle nivåer*** er ansvarlig for å følge opp arbeidet med informasjonssikkerhet på sine ansvarsområder, på samme måte som de følger opp annet arbeid er ansvarlige for.

I tillegg er de ansvarlig for at det blir gjennomført tilstrekkelige risikovurderinger og håndtering a risiko på sine ansvarsområder.

På samme måte som risikoeiere må også ledere på alle nivå minst en gang årlig systematisk vurd status på informasjonssikkerhetsarbeidet innenfor sine ansvarsområder. De har også ansvar for deres medarbeidere har tilstrekkelig kompetanse innen informasjonssikkerhet til å utføre sine oppgaver på en god måte.

### Ønsket kompetanse

På samme måte som toppleder bør øvrig ledergruppe ha grunnleggende kunnskap om hva informasjonssikkerhet er, hva internkontroll handler om, og hva som er sammenhengen mellom to. De må vite hva som er ledelsens ansvar, kjenne til hvilke aktiviteter som skal gjennomføres, o hvem som har ansvaret for de ulike aktivitetene.

Alle ledere må også forstå hvordan informasjonssikkerhet, gjennom å understøtte den informasjonsbehandlingen som gjennomføres i virksomheten, bidrar til at virksomheten når sine mål. For å forstå dette, må vedkommende også ha forståelse for at informasjonssikkerhet handle om å sikre både konfidensialitet, integritet og tilgjengelighet på informasjonen, og at det gjelder mer enn personopplysninger og beskyttelse i henhold til sikkerhetsloven. Informasjonssikkerhetsbrudd kan få konsekvenser får virksomhetens økonomi og tjenesteniv kan få konsekvenser for innbyggere, andre virksomheter og samfunnet.

Det er nyttig med forståelse for at styring av informasjonssikkerhetsarbeidet ikke skiller seg vese fra annen virksomhetsstyring og internkontroll på andre områder (f.eks. HMS og personvern). I d ligger det også å forstå at styringssystem/internkontroll (generelt) er et sett av systematiske aktiviteter, ikke en samling dokumenter.

Alle ledere må også ha forståelse for at de er ansvarlig for å akseptere risiko på noen nivåer, base på definerte kriterier for å akseptere risiko, mens annen risiko enten må helt opp til toppleder, e kan aksepteres på operativt nivå.

De må også forstå at risikobildet endrer seg når man tar ulike strategiske valg, for eksempel ders man velger å tjenesteutsette oppgaver, eller ta i bruk skytjenester.

### Tema for intervju/medarbeidersamtale

Det vil variere mye hvor naturlig det er å snakke om informasjonssikkerhet i en intervjusituasjon eller en medarbeidersamtale, avhengig av hva slags lederstilling det er snakk om. Det kan imidle være nyttig å snakke med kandidaten om hvilken informasjon som behandles i arbeidsoppgaven vedkommende skal ha ansvar for, hvordan vedkommende ser på informasjonssikkerhet og anne internkontroll, og vedkommendes tanker om punktene under «ønsket kompetanse».

11

Difi
Direktoratet for forvaltning og ikt

## IT-leder e.l.

### Ansvar og oppgaver

IT-leder har mange oppgaver relatert til informasjonssikkerhet. Vedkommende vil være ansvarlig for flere tekniske sikkerhetstiltak (tiltaksleverandør), og er ansvarlig for å sørge for IT-faglig kompetanse inn i vurdering og håndtering av risiko[9]. I tillegg er det ofte IT-avdelingen som er ansvarlig for overvåking og hendelseshåndtering, og IT-leder vil derfor være ansvarlig for å styre denne aktiviteten.

IT-leder vil også være risikoeier for de arbeidsoppgavene som vedkommende er ansvarlig for.

### Ønsket kompetanse

Avhengig av hva slags IT-miljø virksomheten har, må IT-leder ha god kunnskap om løsningene de benytter, og hvilke trusler og sårbarheter som kan påvirke virksomhetens risikobilde. Vedkommende bør også ha god kunnskap om hvilke tiltak som kan gjennomføres for å redusere risiko, og kunne gi en beskrivelse av et kost/nytte perspektiv.

IT-leder må også kjenne organisasjonen, og ha evnen til å formulere IKT-tekniske problemstillinger på en forståelig måte til ledelse og øvrige i organisasjonen, gjerne i samarbeid med fagansvarlig informasjonssikkerhet.

IT-leder må ha kompetanse til å forklare toppleder og øvrig ledergruppe hvordan ulike valg kan påvirke risikobildet. Eksempler kan være dersom man vurderer tjenesteutsetting, eller vurderer å ta i bruk skytjenester.

### Tema for intervju/medarbeidersamtale

Forståelse for forholdet mellom tiltaksleverandør og virksomhetens risikoeiere. En tiltaksleverandør er ansvarlig for visse sikkerhetstiltak risikoeiere har behov for. Dette vil normalt inkludere utforming, iverksetting og vedlikehold av sikkerhetstiltakene.

Difi
Direktoratet for forvaltning og ikt

## Alle ansatte

### Ansvar og oppgaver

Alle ansatte har et ansvar for å bidra til at virksomheten når sine samlede mål på en best mulig måte. De skal ha et bevisst forhold til målene for eget arbeid, hvilken informasjon de behandler, og hvilke krav som stilles til arbeidet deres. Dette gjelder også for fagområdet informasjonssikkerhet.

### Ønsket kompetanse

Alle ansatte bør ha kunnskap om hvilken betydning informasjonssikkerhet har for sine arbeidsoppgaver, og hvordan de kan utføre arbeidet sitt på en måte som ivaretar behovet for informasjonssikkerhet. De bør blant annet ha tilstrekkelig forståelse for trusler og risiko til at de utfører arbeidsoppgavene på en sikker måte.

De må også ha forståelse for hvordan uønskede hendelser kan hindre dem i å få gjort jobben sin slik de skal, eller få konsekvenser for andre parter.

Alle ansatte må også kjenne til virksomhetens interne rutiner for varsling av informasjonssikkerhetshendelser.

### Tema for intervju/medarbeidersamtale

Det vil variere mye hvor naturlig det er å snakke om informasjonssikkerhet i en intervjusituasjon eller en medarbeidersamtale, avhengig av hva slags stilling det er snakk om. Det kan imidlertid være nyttig å snakke med kandidaten om hva arbeidsoppgaven innebærer, og hvordan vedkommende reflekterer med tanke på hvilken informasjon som behandles, og hvordan dette kan påvirke enhetens måloppnåelse.

https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet/veiledere/kompetansebeskrivelser-styring-og-kontroll-av-informasjonssikkerhet

14

# Samarbeidsprosjektet

| Delprosjekt | Leder | Bidrar |
|---|---|---|
| Informasjonssikkerhet i styringsdialogen | Direktoratet for forvaltning og økonomistyring | Digitaliseringsdirektoratet<br>Norwegian Digitalisation Agency<br>NSM |
| Øvelser for bedre informasjonssikkerhet | dsb | Digitaliseringsdirektoratet<br>Norwegian Digitalisation Agency<br>NSM |
| Sikkerhetskultur | NorSIS | Digitaliseringsdirektoratet<br>Norwegian Digitalisation Agency |
| Kompetanse | Digitaliseringsdirektoratet<br>Norwegian Digitalisation Agency | NorSIS |
| Styring og kontroll | Digitaliseringsdirektoratet<br>Norwegian Digitalisation Agency | Direktoratet for forvaltning og økonomistyring<br>NSM |

# Informasjonssikkerhet i styringsdialogen

- Veileder med tilhørende dialogverktøy
- Justert veiledning til årsrapport


- Publiseres på DFØs nettsider – www.dfo.no

# Styring og kontroll for informasjonssikkerhet

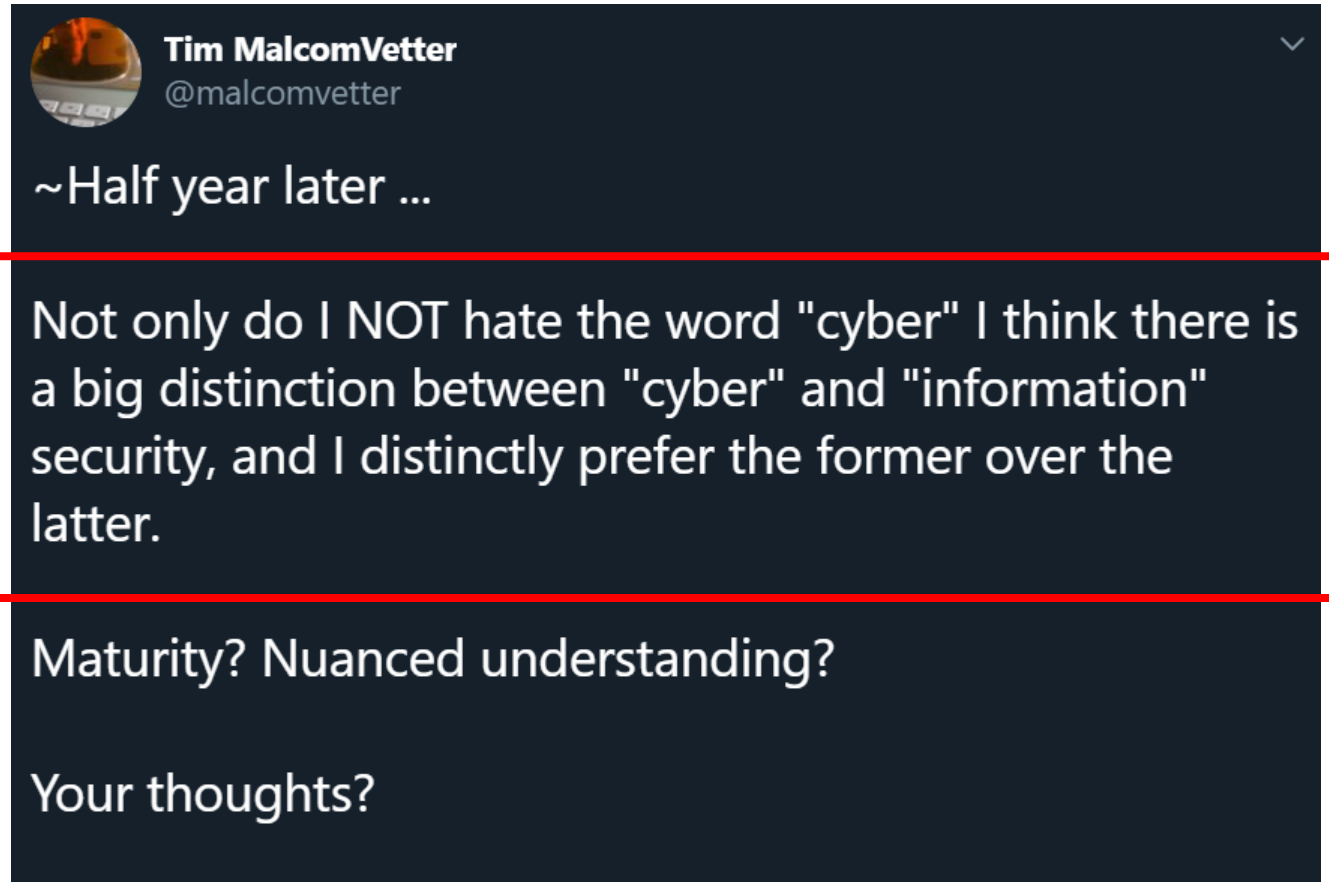
Delprosjektet har som hovedmål å styrke styringen av informasjonssikkerhet i virksomheter, og vise hvordan dette henger sammen med helhetlig styring og kontroll.

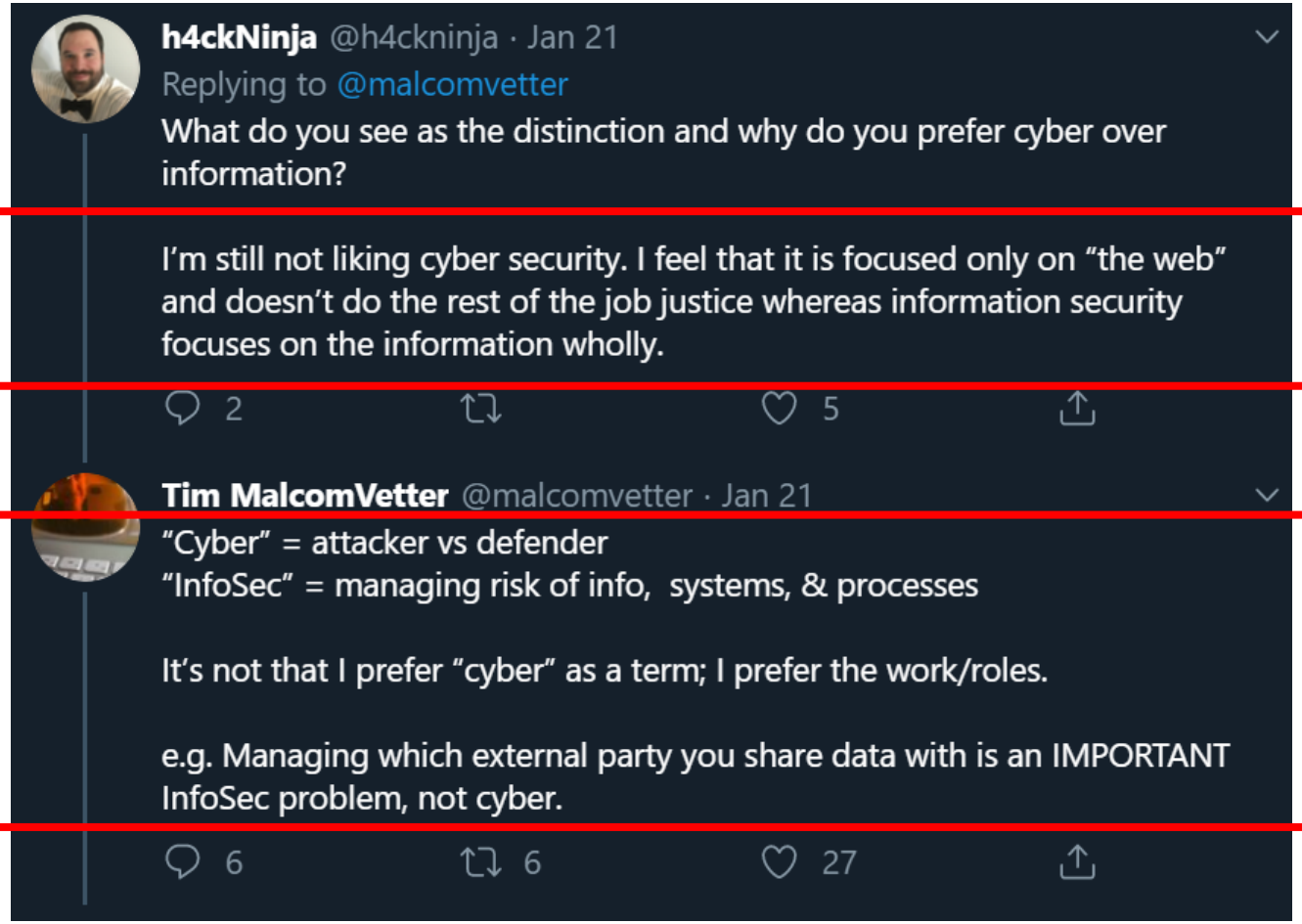
Et delmål: Tydeliggjøre sammenhenger mellom veiledningen fra Digitaliseringsdirektoratet, DFØ, NSM

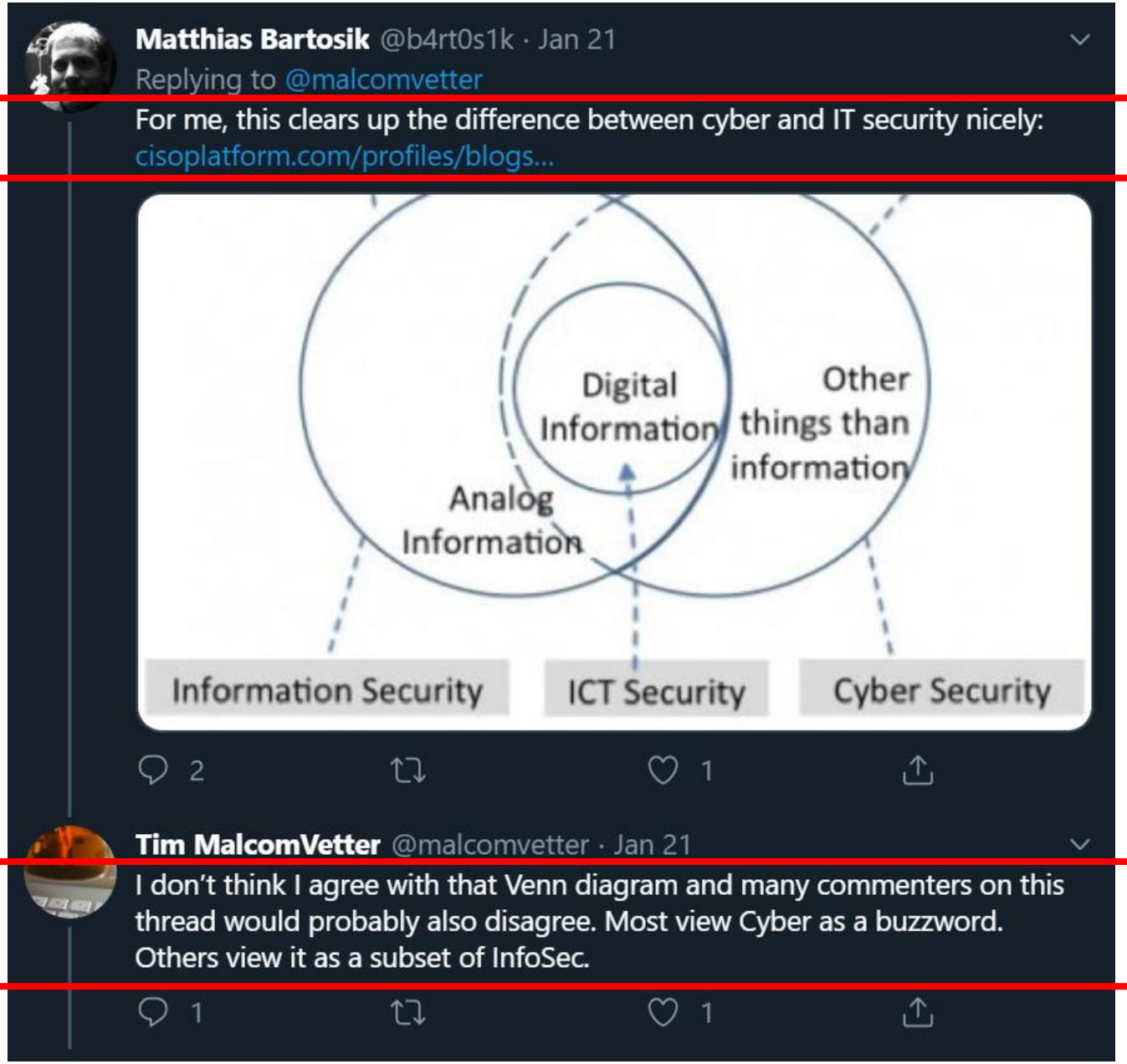
Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

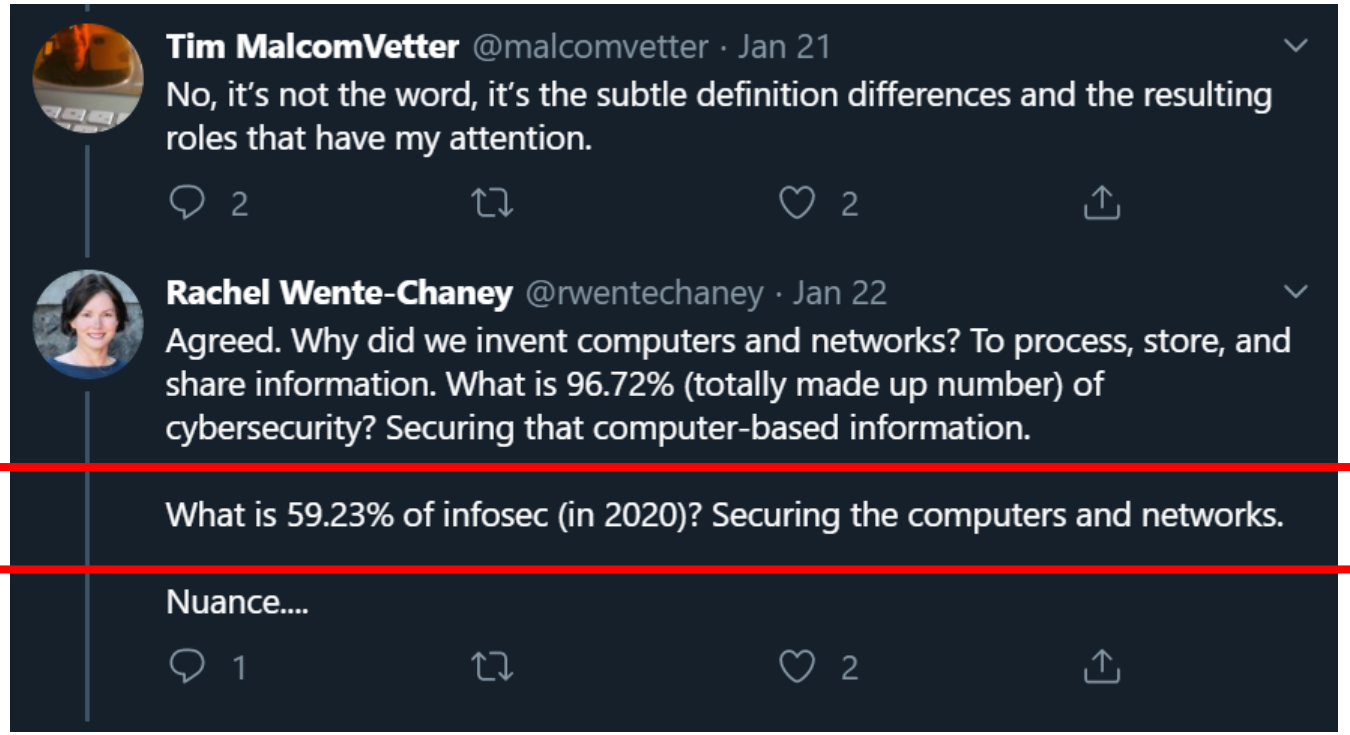
# Styring og kontroll med… Noe™

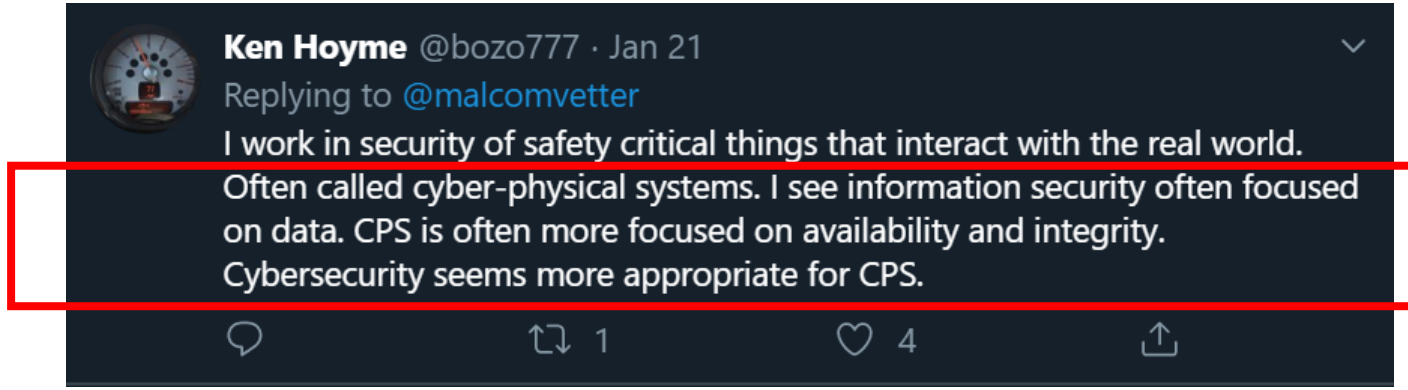
Remi Longva
Seniorrådgiver
2020-02-04

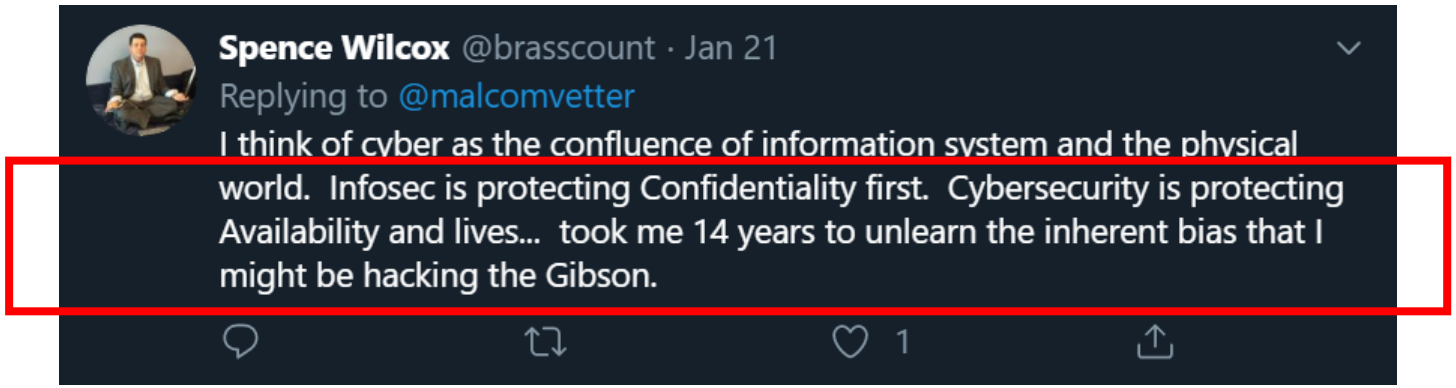

Tim MalcomVetter
@malcomvetter
~Half year later ...
Not only do I NOT hate the word "cyber" I think there is a big distinction between "cyber" and "information" security, and I distinctly prefer the former over the latter.
Maturity? Nuanced understanding?
Your thoughts?


h4ckNinja @h4ckninja · Jan 21
Replying to @malcomvetter
What do you see as the distinction and why do you prefer cyber over information?
I'm still not liking cyber security. I feel that it is focused only on "the web" and doesn't do the rest of the job justice whereas information security focuses on the information wholly.
2
5
Tim MalcomVetter @malcomvetter · Jan 21
"Cyber" = attacker vs defender
"InfoSec" = managing risk of info, systems, & processes
It's not that I prefer "cyber" as a term; I prefer the work/roles.
e.g. Managing which external party you share data with is an IMPORTANT InfoSec problem, not cyber.
6
6
27


Matthias Bartosik @b4rt0s1k · Jan 21
Replying to @malcomvetter
For me, this clears up the difference between cyber and IT security nicely:
cisoplatform.com/profiles/blogs...
Digital Information
Other things than information
Analog Information
Information Security
ICT Security
Cyber Security
2
1
Tim MalcomVetter @malcomvetter · Jan 21
I don't think I agree with that Venn diagram and many commenters on this thread would probably also disagree. Most view Cyber as a buzzword. Others view it as a subset of InfoSec.
1
1


Tim MalcomVetter @malcomvetter · Jan 21
No, it's not the word, it's the subtle definition differences and the resulting roles that have my attention.
2
2
Rachel Wente-Chaney @rwentechaney · Jan 22
Agreed. Why did we invent computers and networks? To process, store, and share information. What is 96.72% (totally made up number) of cybersecurity? Securing that computer-based information.
What is 59.23% of infosec (in 2020)? Securing the computers and networks.
Nuance....
1
2


Ken Hoyme @bozo777 · Jan 21
Replying to @malcomvetter
I work in security of safety critical things that interact with the real world. Often called cyber-physical systems. I see information security often focused on data. CPS is often more focused on availability and integrity. Cybersecurity seems more appropriate for CPS.
1
4


Spence Wilcox @brasscount · Jan 21
Replying to @malcomvetter
I think of cyber as the confluence of information system and the physical world. Infosec is protecting Confidentiality first. Cybersecurity is protecting Availability and lives... took me 14 years to unlearn the inherent bias that I might be hacking the Gibson.
1

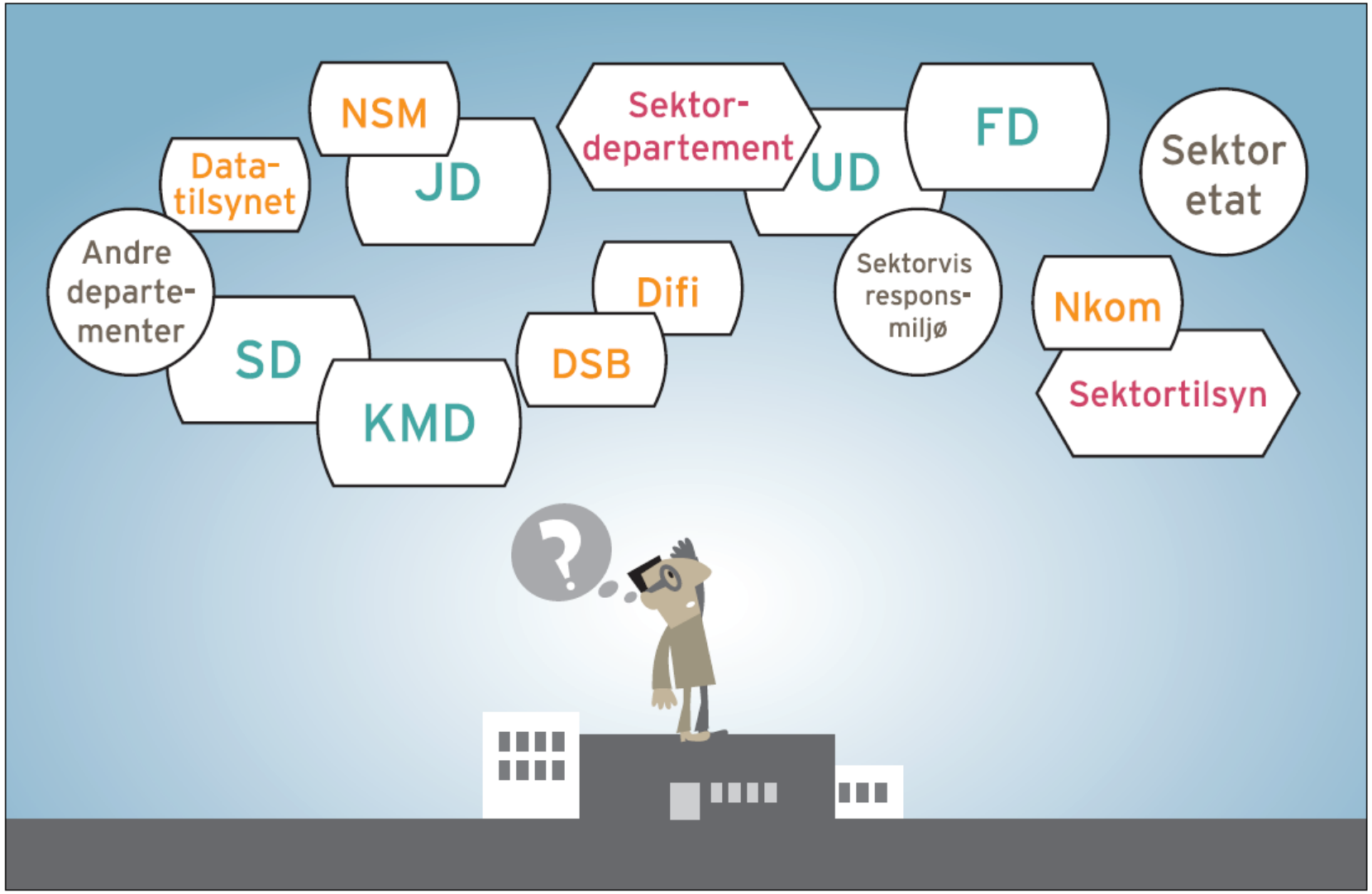
# Ulike perspektiver

# Perspektiver

- Offentlige oppgaver og tjenester
- «Sektor»
  - tjenestevertikal – f.eks. «helse»
- Digital teknologi – tverrsektorielt
- Virksomhet – toppleder | leder
- Virksomhet – virksomhets- eller IT-arkitekt
- Virksomhet – IT-sikkerhetsekspert

# IKT-sikkerhetsutvalget

**NOU 2018: 14 IKT-sikkerhet i alle ledd**


NSM
Sektor-
departement
FD
Data-
tilsynet
JD
UD
Sektor
etat
Andre
departe-
menter
Sektorvis
respons-
miljø
Difi
Nkom
SD
DSB
KMD
Sektortilsyn

«brukerne er usikre på hvor de skal henvende seg for å få råd og veiledning om IKT-sikkerhet»

«det er uklart for brukerne hva de ulike etatene har ansvaret for»

«rådene kan være basert på ulike standarder og bransjepraksis eller lover og forskrifter»

«…peker også på at rådene ikke er koordinerte og enhetlige. Dette knytter seg særlig til en-til-en-veiledningen og ikke det skriftlige materialet etatene gir ut.»

- JD: nasjonal digital sikkerhet
  - nasjonal IKT-sikkerhet
- Nasjonal strategi for digital sikkerhet
- Nasjonalt cybersikkerhetssenter
- Sikkerhetsloven kap. 5 Informasjonssikkerhet
- Sikkerhetsloven kap. 6 Informasjonssystemsikkerhet

- KMD: IT-politikk | IKT-politikk
- Digitaliseringsstrategi for offentlig sektor
  - => Nasjonal strategi for digital sikkerhet
- Statens kompetansemiljø for informasjonssikkerhet
- Instruks og tildelingsbrev til Digitaliseringsdirektoratet:
  - forebyggende IT-sikkerhet
  - IKT-sikkerhet i anskaffelser

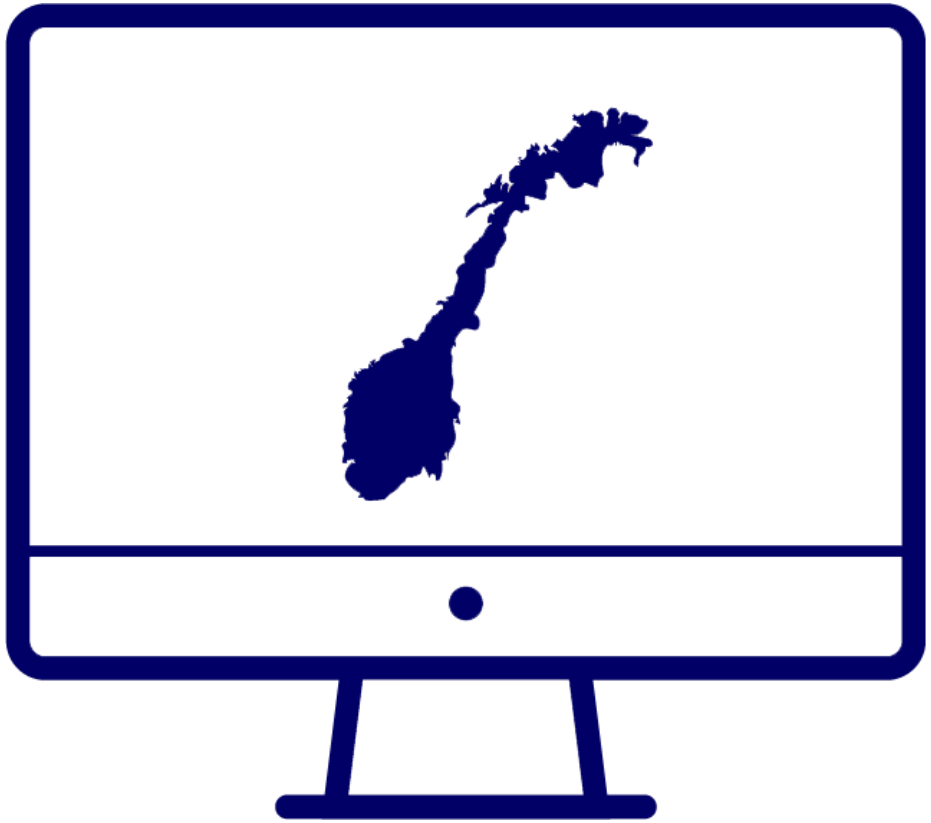
# Menneskets evne til å resonnere?

- Språk
- Språklig presisjon
  - må være tilstrekkelig til å være egnet til å arbeide med «problemdomenet»
- Ett eller flere «problemdomener»?
  - Åpenbart snakk om ulike perspektiver
  - Men hvordan er det fornuftig å dele opp i «problemdomener»?

# Realitetsorientering

- Flere fagområder møtes i ny «digital» verden
  - De har med seg ulike begreper
- Varierende begrepsbruk i regelverk
  - Sjekk «information system» i NIS-direktivet og «informasjonssystem» i sikkerhetsloven (forarbeidene)
- I blant mangler vi ord for ting
  - Jf. Digitaliseringsdirektoratets bruk av «styringsaktiviteter», «tiltaksbanker» og «tiltaksleverandører»
- Ulike, delvis overlappende begreper vil være i bruk i lang tid fremover
  - Og nye vil komme til
- Ved behov
  - vi bør beskrive | avklare hva vi legger i begrepene vi bruker
  - vi bør være obs på **kontekst** og **perspektiv**

# Offentlig sektor



**Arbeids- og sosialdepartementet**
Torbjørn Røe Isaksen (H)

**Barne- og familiedepartementet**
Kjell Ingolf Ropstad (KrF)

**Finansdepartementet**
Jan Tore Sanner (H)

**Forsvarsdepartementet**
Frank Bakke-Jensen (H)

**Helse- og omsorgsdepartementet**
Bent Høie (H)

**Justis- og beredskapsdepartementet**
Monica Mæland (H)

**Klima- og miljødepartementet**
Sveinung Rotevatn (V)

**Kommunal- og moderniseringsdepartementet**
Nikolai Astrup (H) Linda Hofstad Helleland (H)

**Kulturdepartementet**
Abid Q. Raja (V)

**Kunnskapsdepartementet**
Trine Skei Grande (V) Henrik Asheim (H)

**Landbruks- og matdepartementet**
Olaug Vervik Bollestad (KrF)

**Nærings- og fiskeridepartementet**
Iselin Nybø (V) Geir Inge Sivertsen (H)

**Olje- og energidepartementet**
Tina Bru (H)

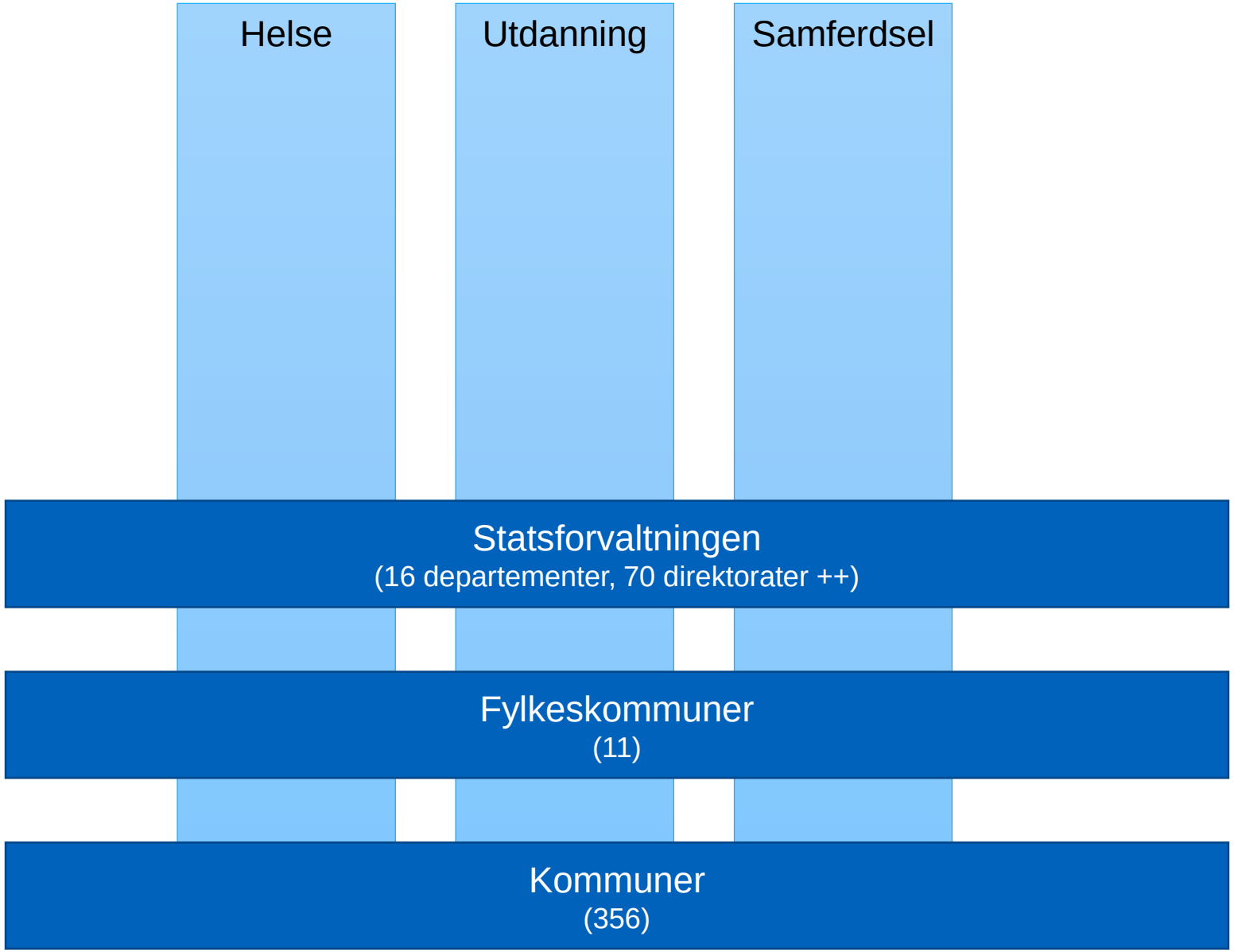
**Samferdselsdepartementet**
Knut Arild Hareide (KrF)

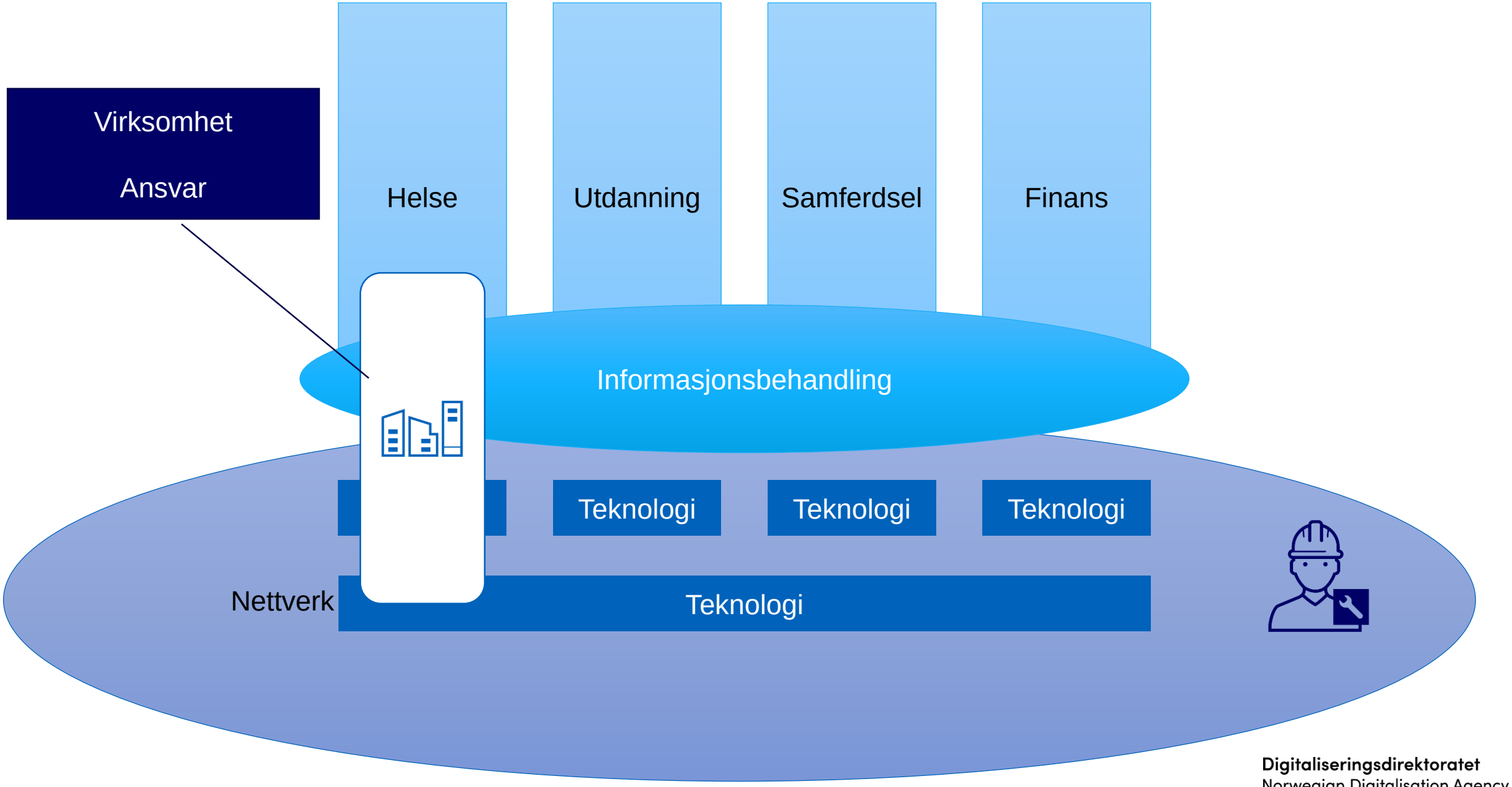
**Utenriksdepartementet**
Ine Eriksen Søreide (H) Dag-Inge Ulstein (KrF)

## Statsforvaltningen
(16 departementer, 70 direktorater ++)

## Fylkeskommuner
(11)

## Kommuner
(356)


Helse
Utdanning
Samferdsel
Statsforvaltningen
(16 departementer, 70 direktorater ++)
Fylkeskommuner
(11)
Kommuner
(356)


Virksomhet
Ansvar
Helse
Utdanning
Samferdsel
Finans
Informasjonsbehandling
Teknologi
Teknologi
Teknologi
Nettverk
Teknologi

# Virksomhetskontekst

Perspektiv

Ledelse

# Informasjonssikkerhet?

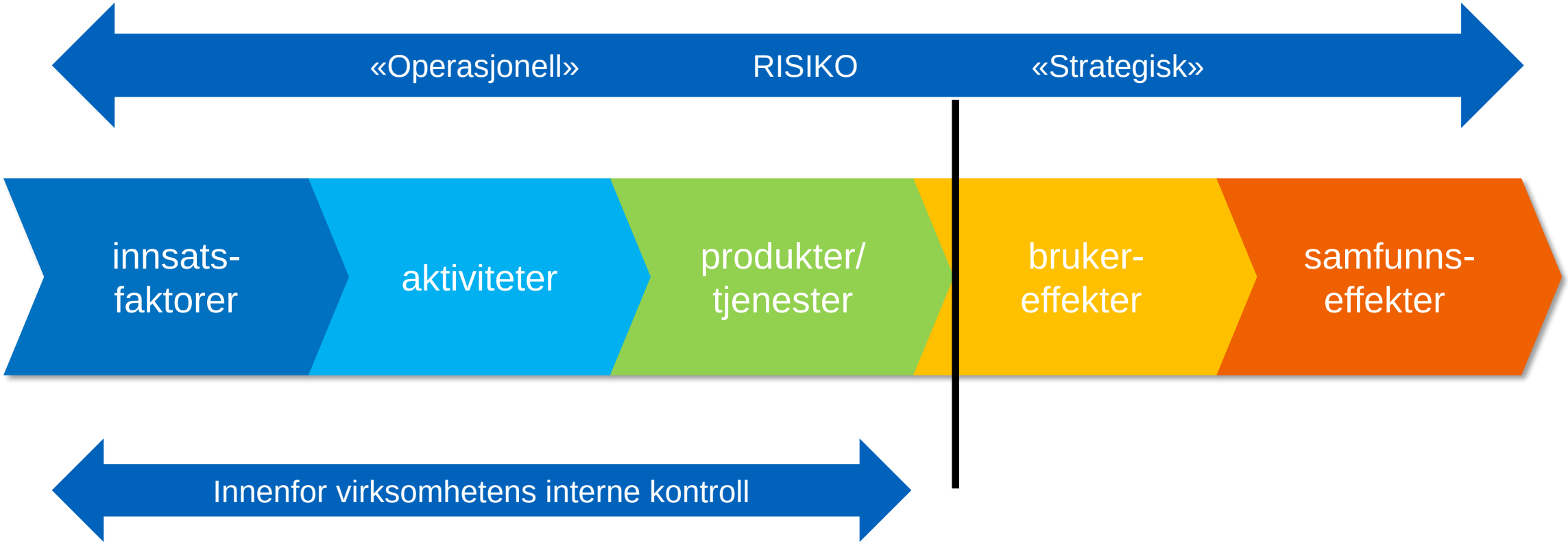
En offentlig virksomhet arbeider med informasjonssikkerhet for

- å utføre sine oppgaver og levere sine tjenester på en god måte
- å nå sine mål og ivareta lovpålagte forpliktelser

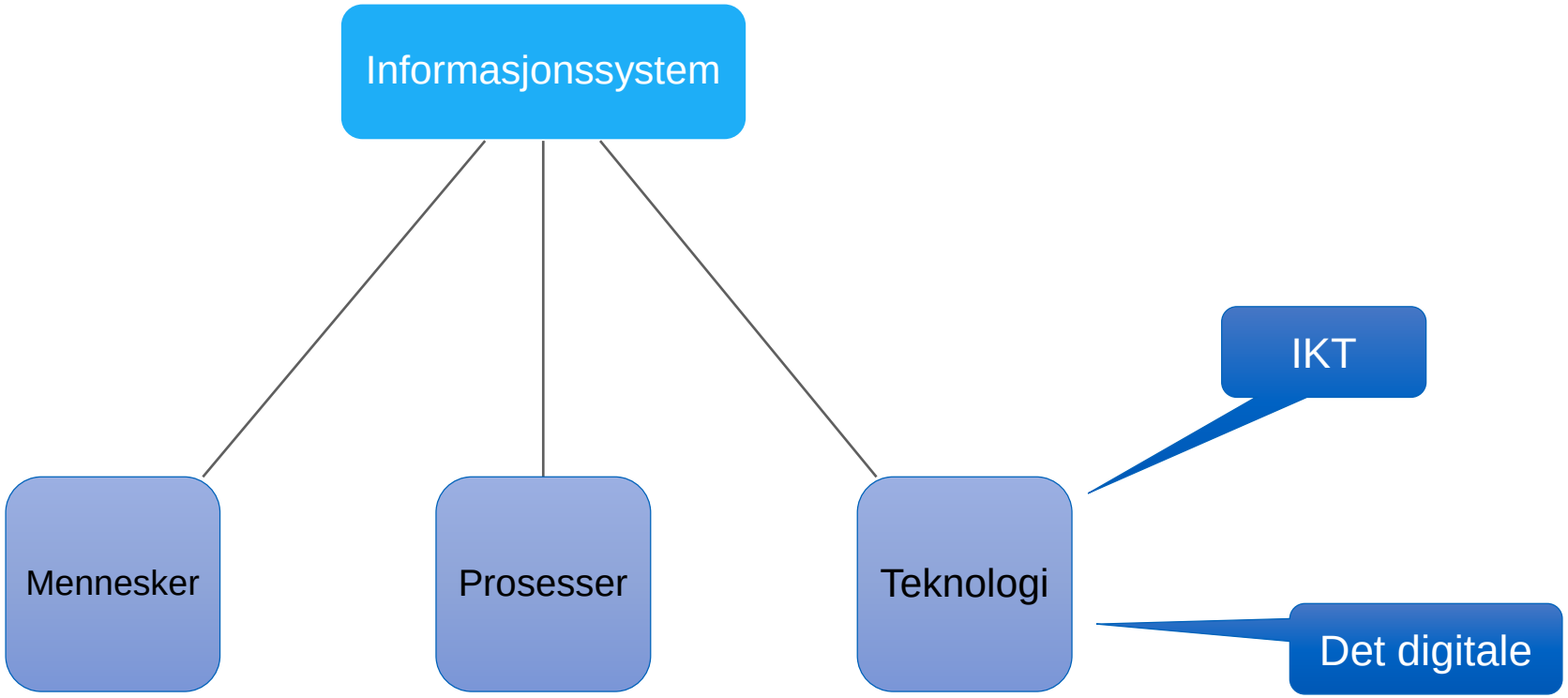
Informasjonssikkerhetsbrudd i en virksomhets oppgaver og tjenester kan få følger for tjenestenivå, økonomi og ansatte.

Det kan få konsekvenser utenfor virksomheten, for innbyggere, andre virksomheter, samfunnsfunksjoner eller nasjonale sikkerhetsinteresser.

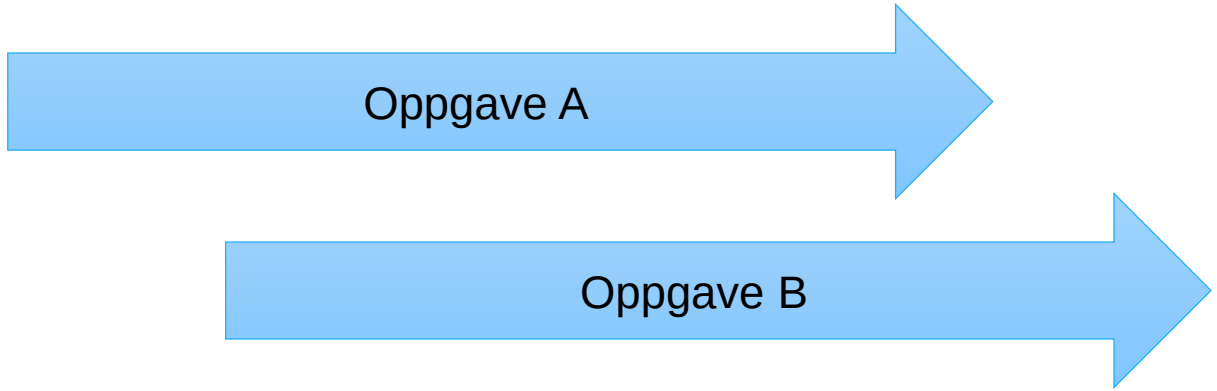
# Resultatkjeden



# Oppgaver og tjenester → Informasjonsbehandling


Informasjonssystem
Mennesker
Prosesser
Teknologi
IKT
Det digitale

Kjerneprosesser

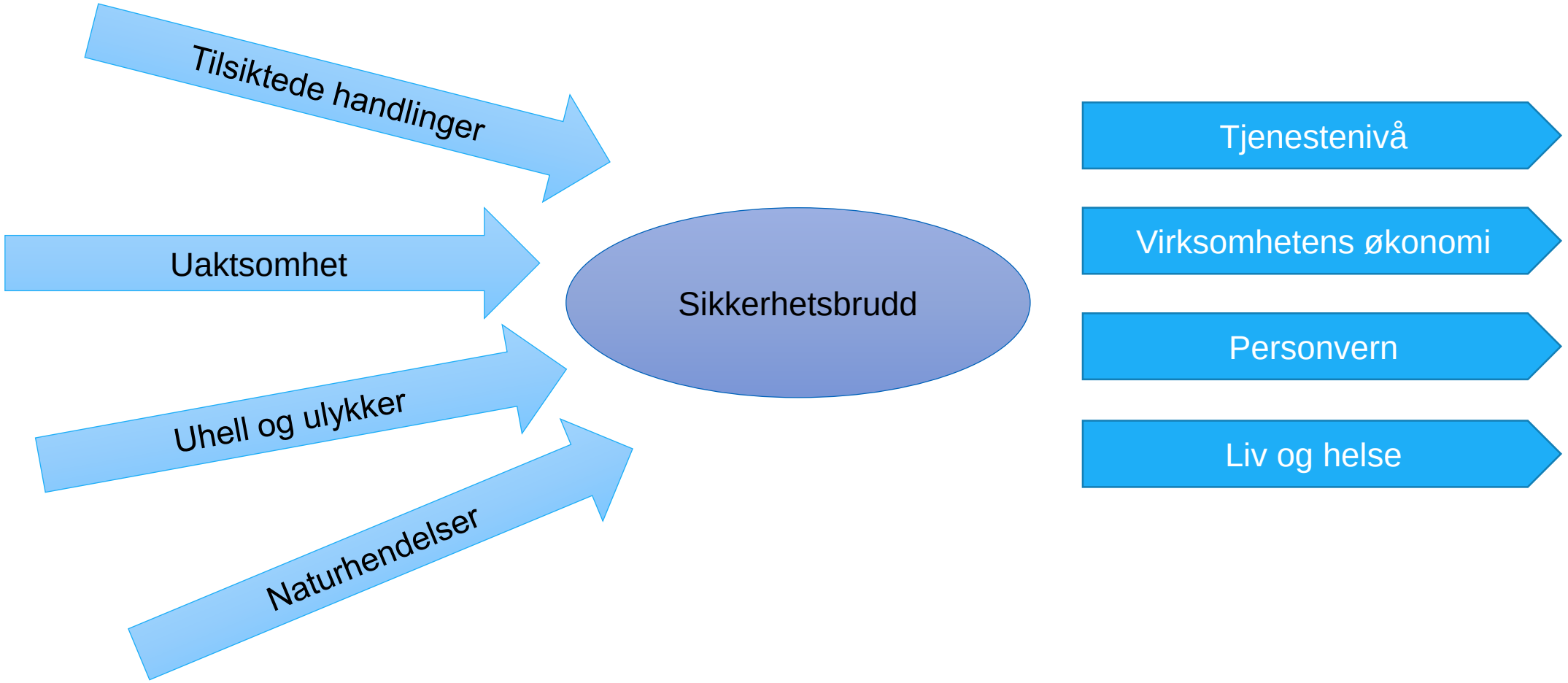



Støtteprosesser

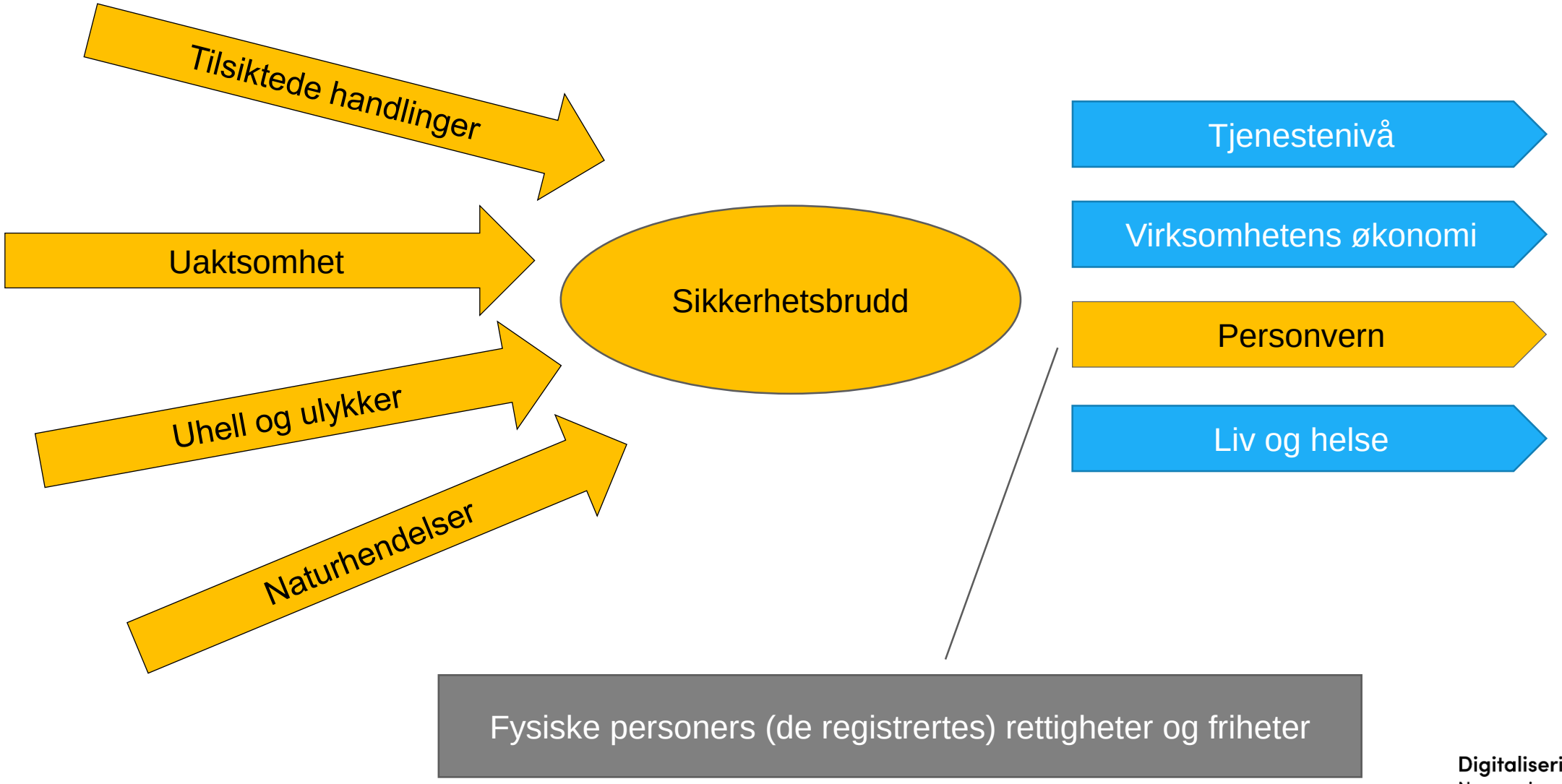

Virksomhetsstyring
Risikostyring | Internkontroll
Styring og kontroll
-
Informasjonssikkerhet

# Kilder

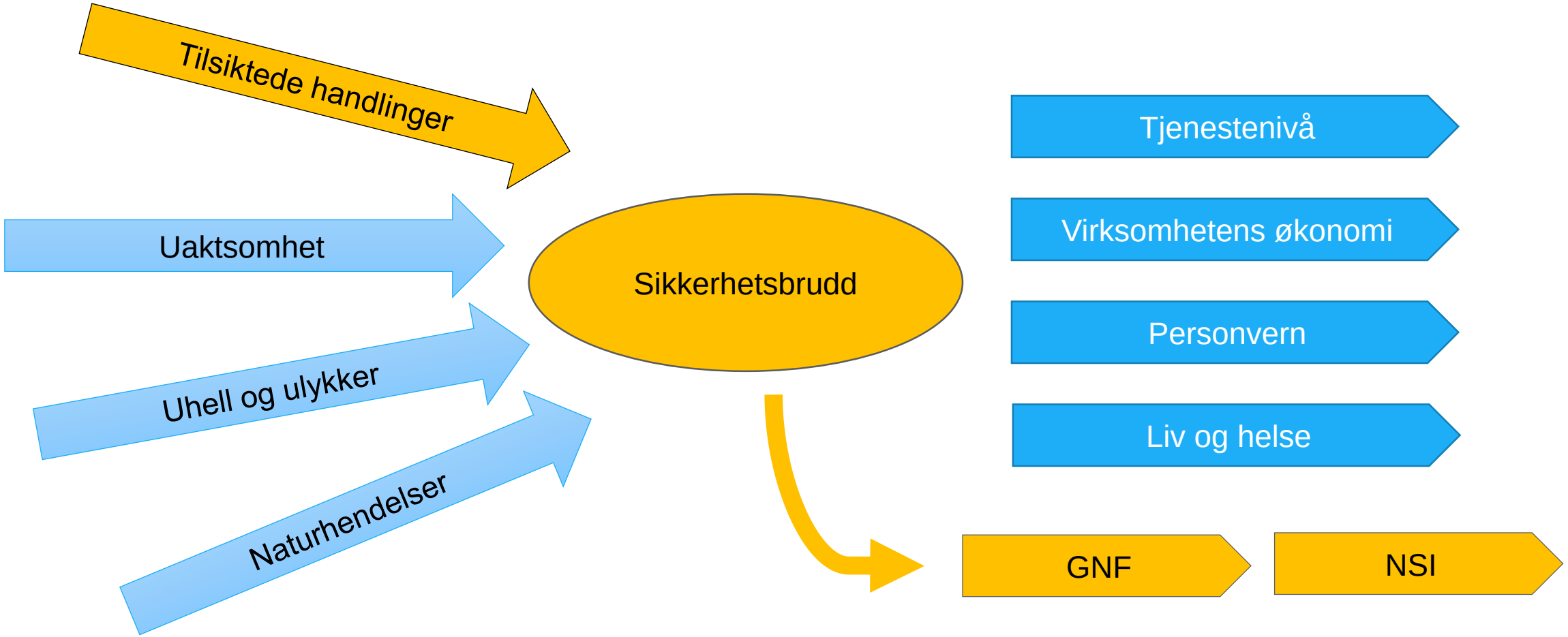
# Konsekvenskategorier



# Informasjonssikkerhet i personvernforordningen

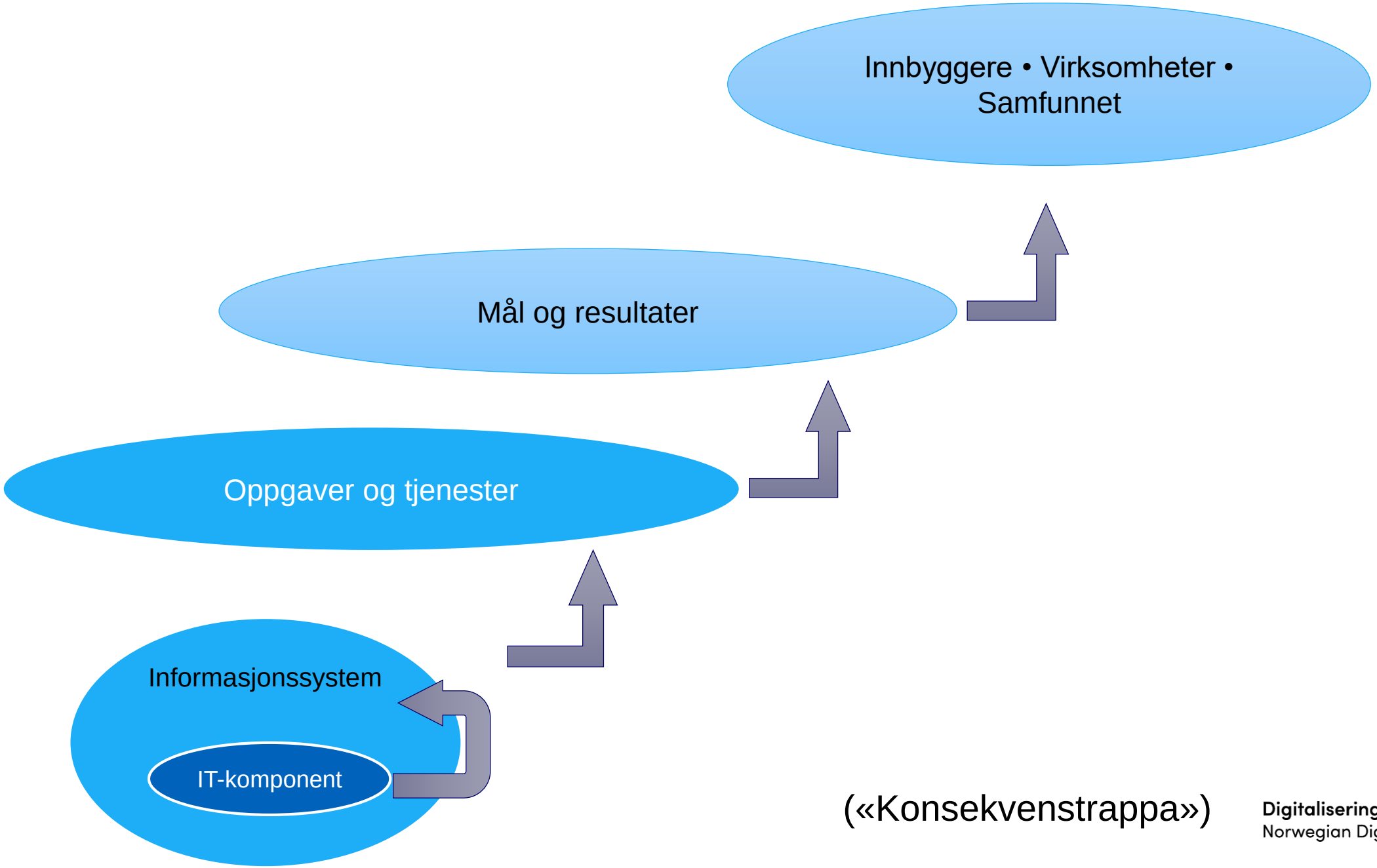


# Informasjonssikkerhet i sikkerhetsloven



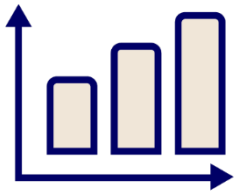

Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

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



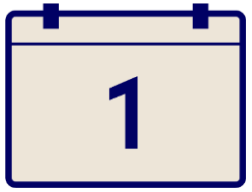

(«Konsekvenstrappa»)

# Egne interesser



- Mål og resultater

Jf. DFØs internkontrollmål ☺

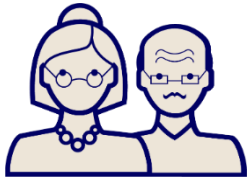



- Pålitelig rapportering

- Overholdelse av lover og regler

OBS!
Mange bruker «internkontroll» om bare dette

# Andres interesser



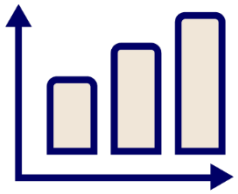
- Individer | Innbyggere

- Andre virksomheter

- Samfunnet for øvrig

# Kan også sies sånn

Informasjonssikkerhet har betydning for:

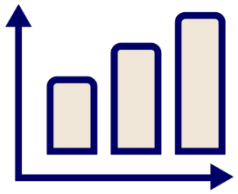


- Egne oppgaver og tjenester

- Lovpålagte forpliktelser

# Eller sånn

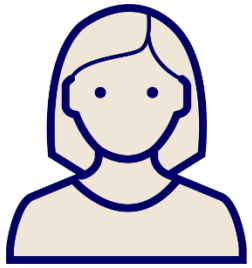
Informasjonssikkerhetsbrudd kan få konsekvenser for:



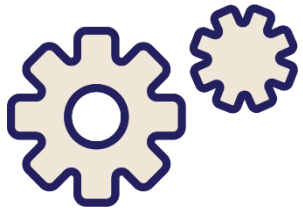
- Virksomhetens oppgaver og tjenester

- Andre (utenfor virksomheten)

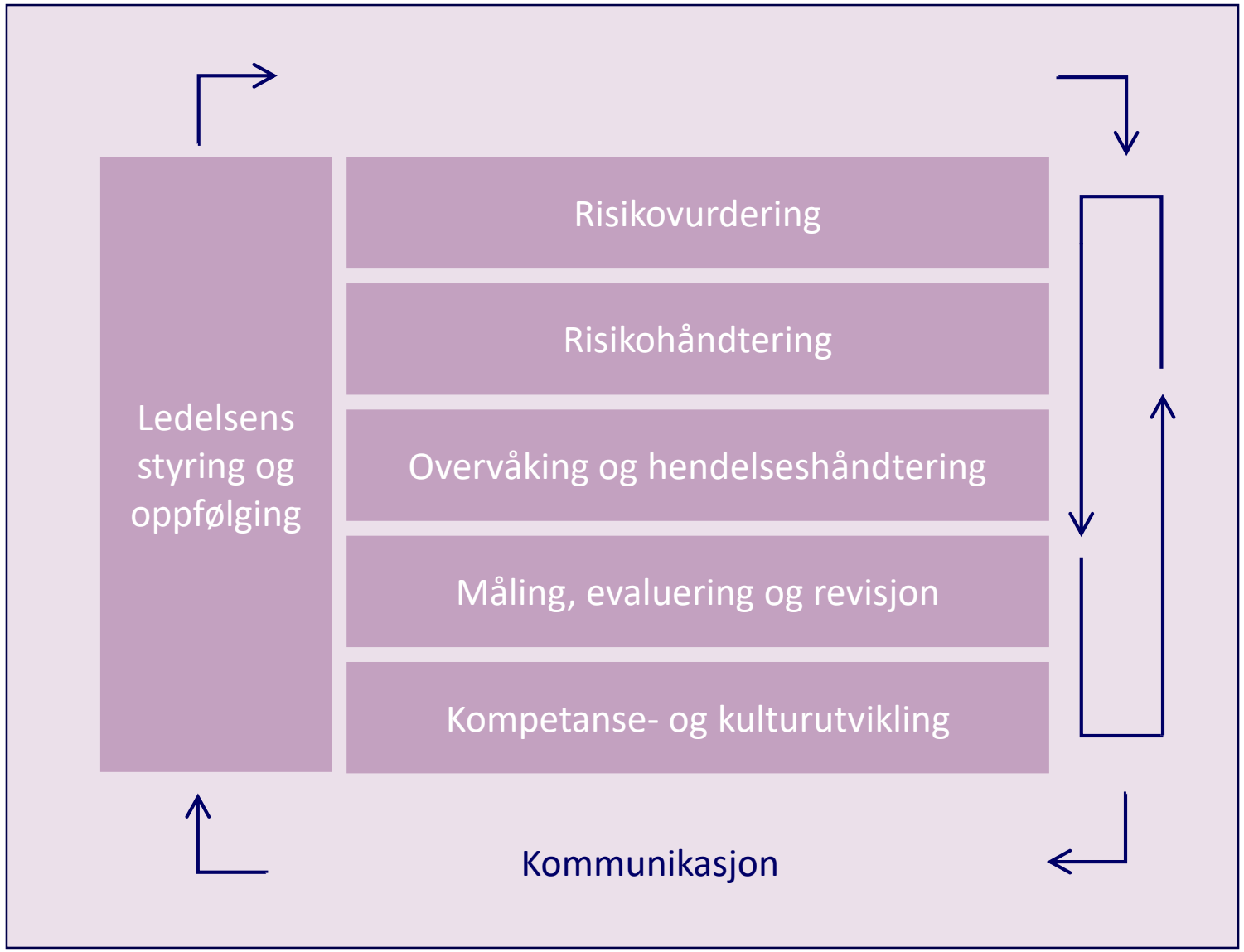
# Hvordan arbeide med informasjonssikkerhet?



- En god toppleder styrer gjennom et system

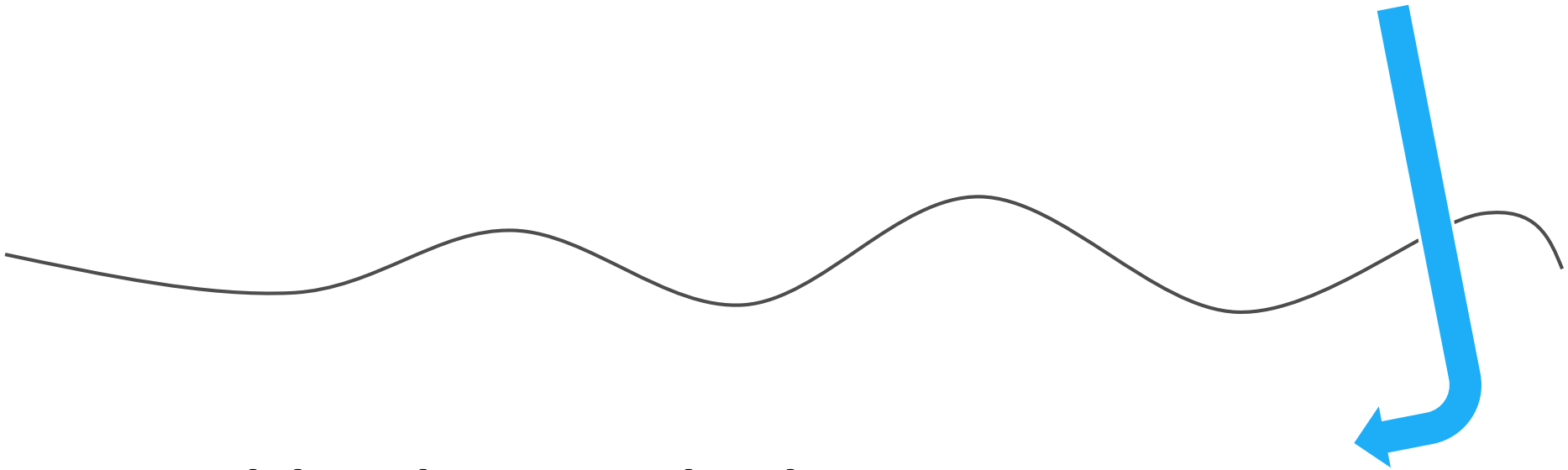


- En del av helhetlig styring og kontroll


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

«Styringsaktiviteter»

- Vurdering av risiko
- Håndtering av risiko



«Sikkerhetsstiltak»

# «Styringsaktiviteter»

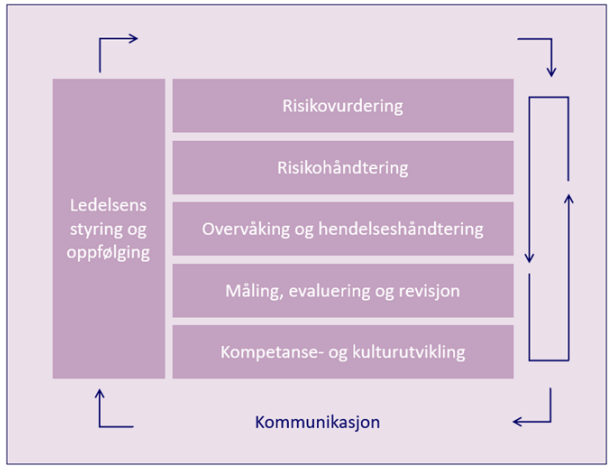
- ISO/IEC 27001 (kap. 4 til 10)

# «Sikkerhetsstiltak»

## Tiltaksbanker

- ISO/IEC 27002 = 27001 Annex A
- NIST SP 800-53
- NSMs grunnprinsipper for IKT-sikkerhet
- Normen kap. 5

# «Styringsaktiviteter»




# «Sikkerhetsstiltak»

## Tiltaksbanker

- ISO/IEC 27002 = 27001 Annex A
- NIST SP 800-53
- NSMs grunnprinsipper for IKT-sikkerhet
- Normen kap. 5

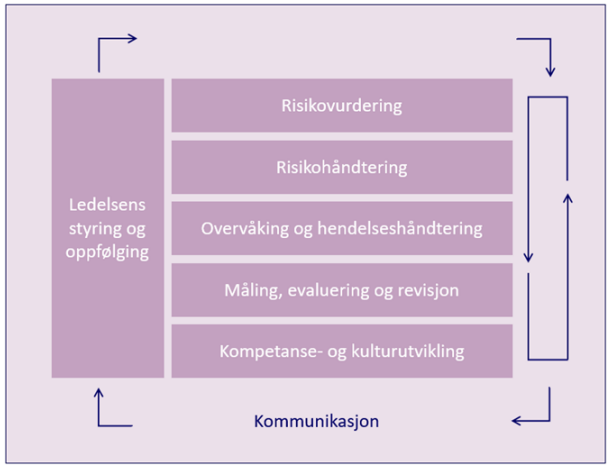
## Risikoeier

- Ansvar for oppgaver og tjenester
- Ansvar for mål og resultater
- Ansvar for risiko innen sitt område
- Som regel: linjeleder

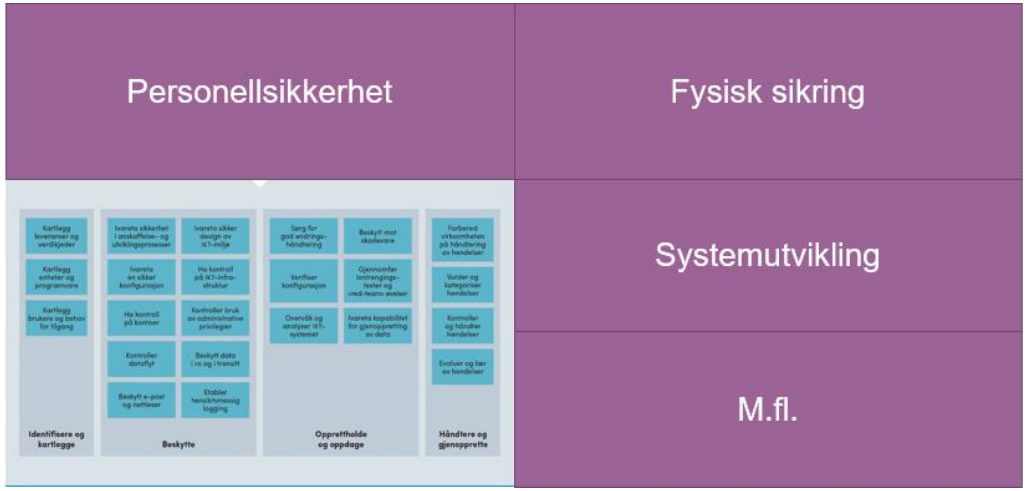
## Tiltaksleverandør

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

# «Styringsaktiviteter»




# «Sikkerhetsstiltak»




Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

Obs: konseptuell forståelse. Det virkelige verden er, som alltid, kompleks.

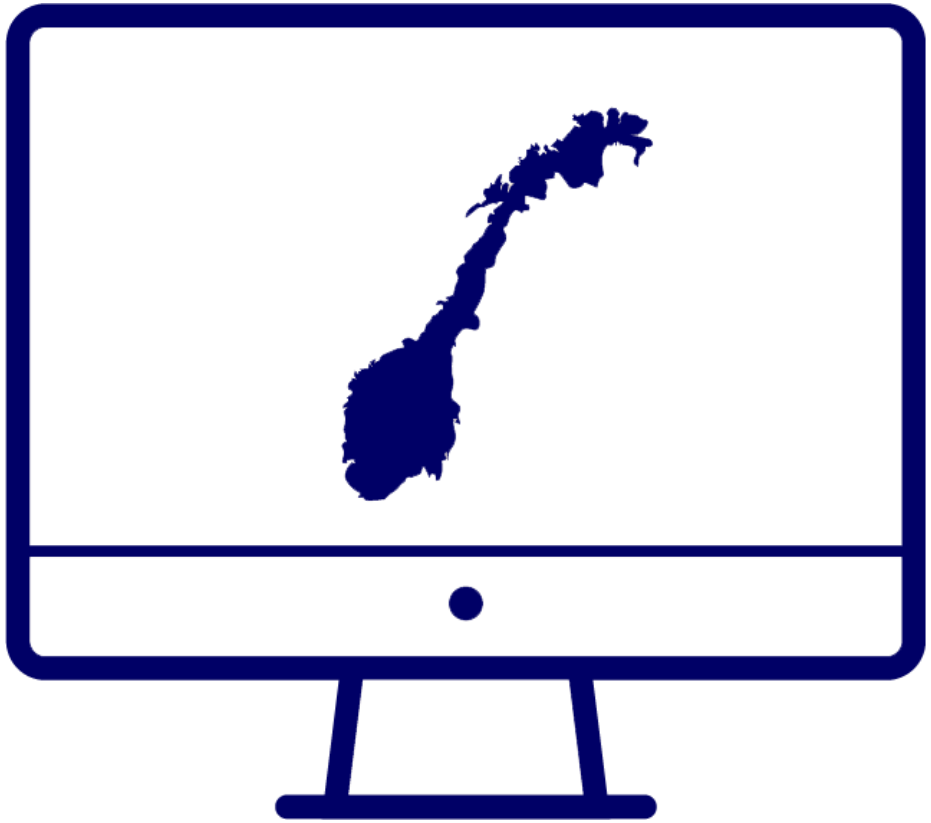
# Hva menes med helhetlig?

# Hvor helhetlig kan det bli?

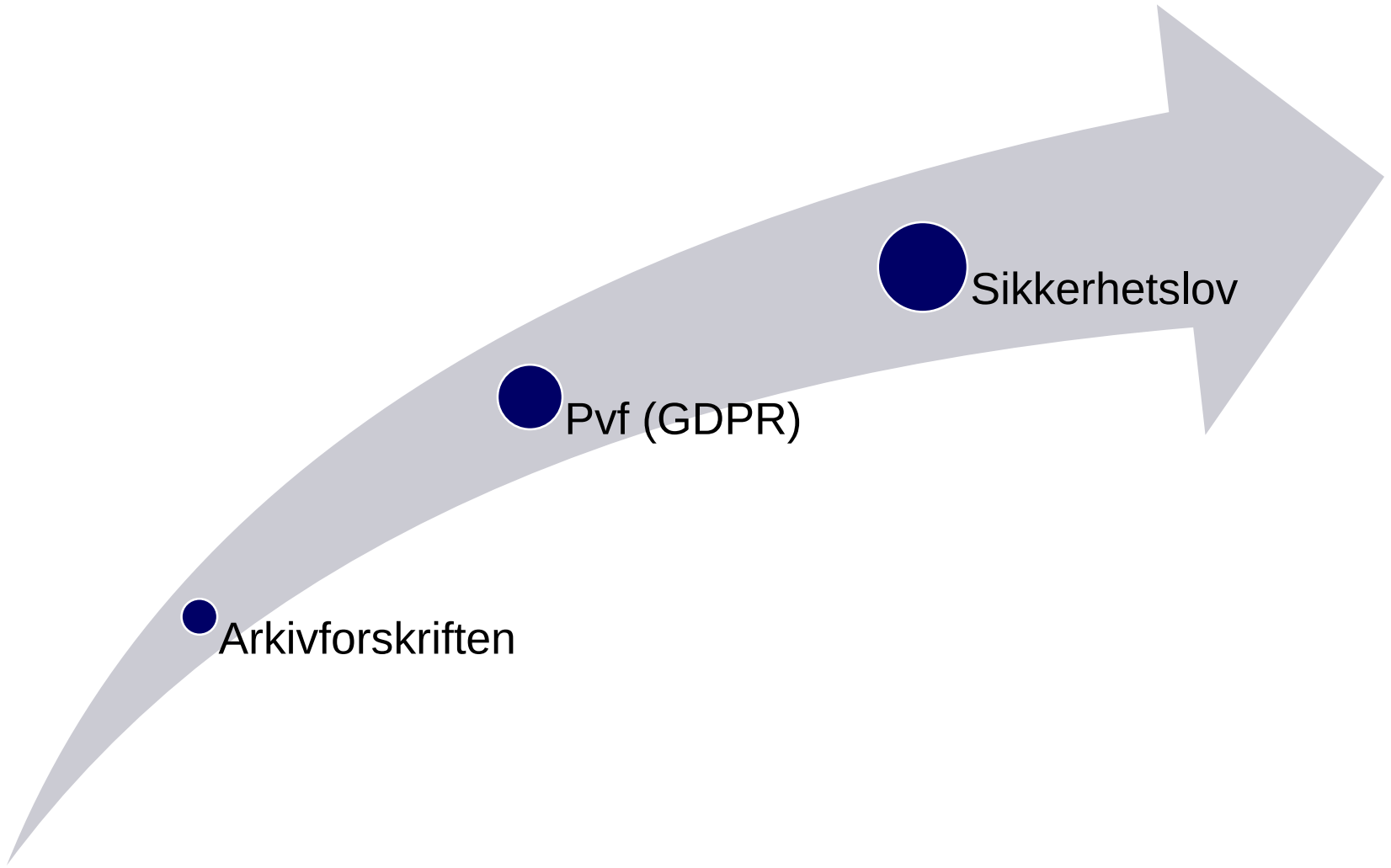
# Behov for helhetlig styring og kontroll

- På «informasjonssikkerhetsområdet»
  - Ulike regelverk stiller krav til forskjellige «deler» av det virksomheten skal ivareta innen informasjonssikkerhet
- Styring av hele virksomheten
  - Informasjonssikkerhet har stor betydning for primær måloppnåelse
  - **Styringsaktivitetene** har mye til felles uavhengig av «område» som skal ivaretas
    - Informasjonssikkerhet
    - Personvern (pol/pvf)
    - HMS (arbeidsmiljøloven)
    - Nasjonale sikkerhetsinteresser (sikkerhetsloven)
    - M.fl.

# Regelverk

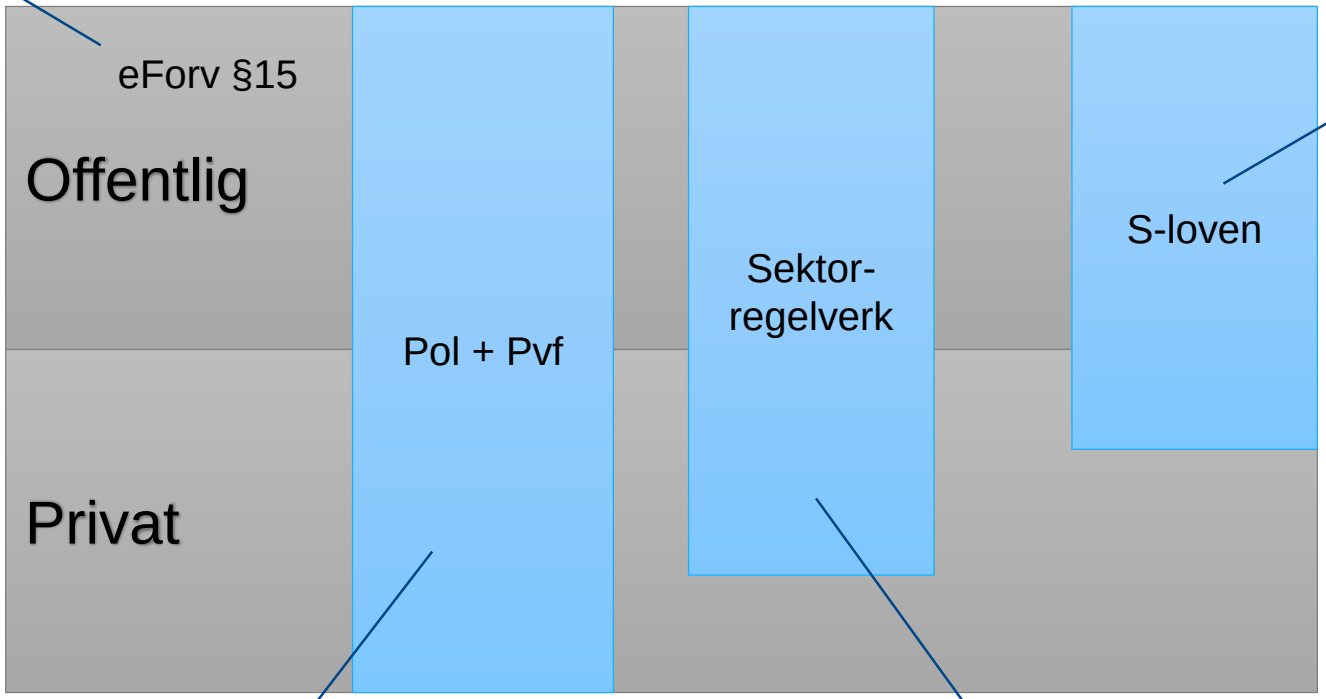


# Funksjonsbasert | Risikobasert | Fleksibelt



Styring og kontroll

Kilde: tilsiktede handlinger
Konsekvenser for
Nasjonale sikkerhetsinteresser (NSI)

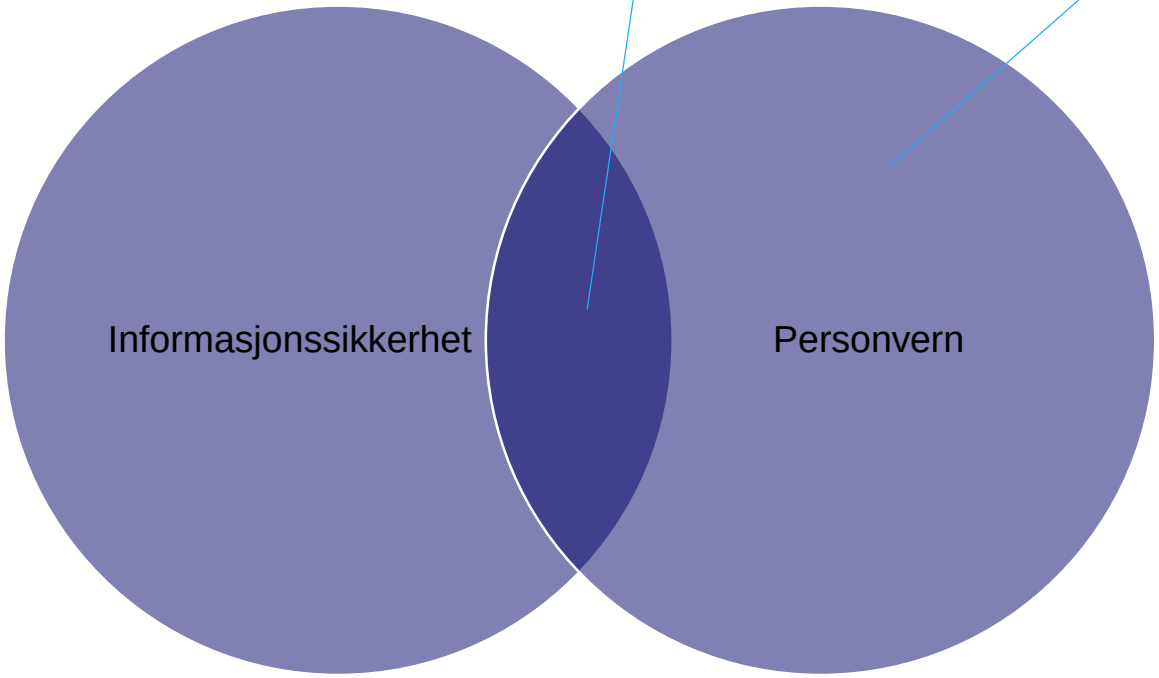



Informasjonstype: personopplysninger
Konsekvenser for fysiske personers
rettigheter og friheter

Informasjonstype:
sektorspesifikk

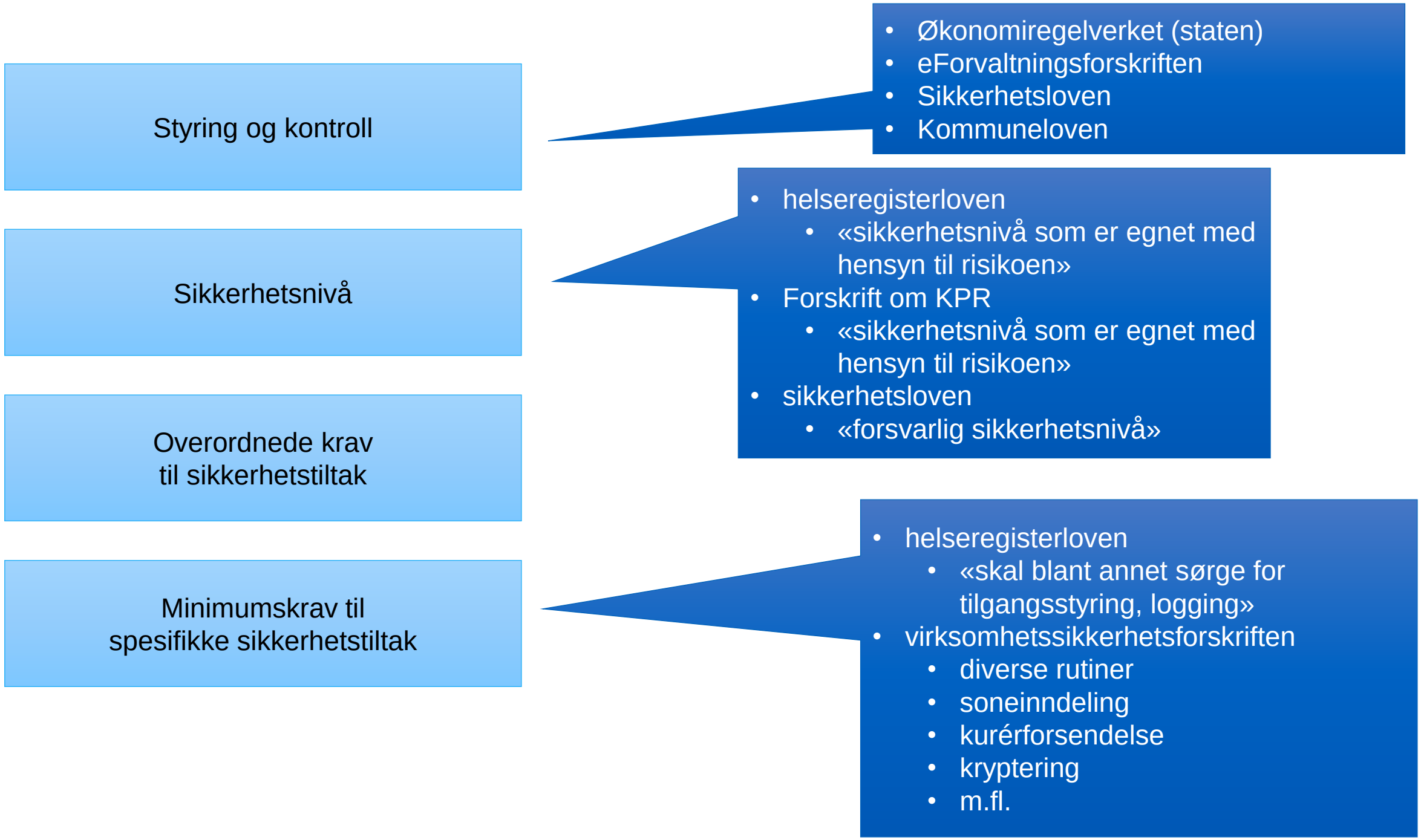
# Sammenheng med pol/pvf

K-I-T for personopplysninger




- Behandlingsansvarliges plikter
- Den registrertes rettigheter

- Personvernkonsekvenser ved lovlig, tiltenkt behandling


Styring og kontroll
Sikkerhetsnivå
Overordnede krav
til sikkerhetstiltak
Minimumskrav til
spesifikke sikkerhetstiltak
• Økonomiregelverket (staten)
• eForvaltningsforskriften
• Sikkerhetsloven
• Kommuneloven
• helseregisterloven
• «sikkerhetsnivå som er egnet med hensyn til risikoen»
• Forskrift om KPR
• «sikkerhetsnivå som er egnet med hensyn til risikoen»
• sikkerhetsloven
• «forsvarlig sikkerhetsnivå»
• helseregisterloven
• «skal blant annet sørge for tilgangsstyring, logging»
• virksomhetssikkerhetsforskriften
• diverse rutiner
• soneinndeling
• kurérforsendelse
• kryptering
• m.fl.

# Sikkerhetsloven
# Virksomhetsikkerhetsforskriften

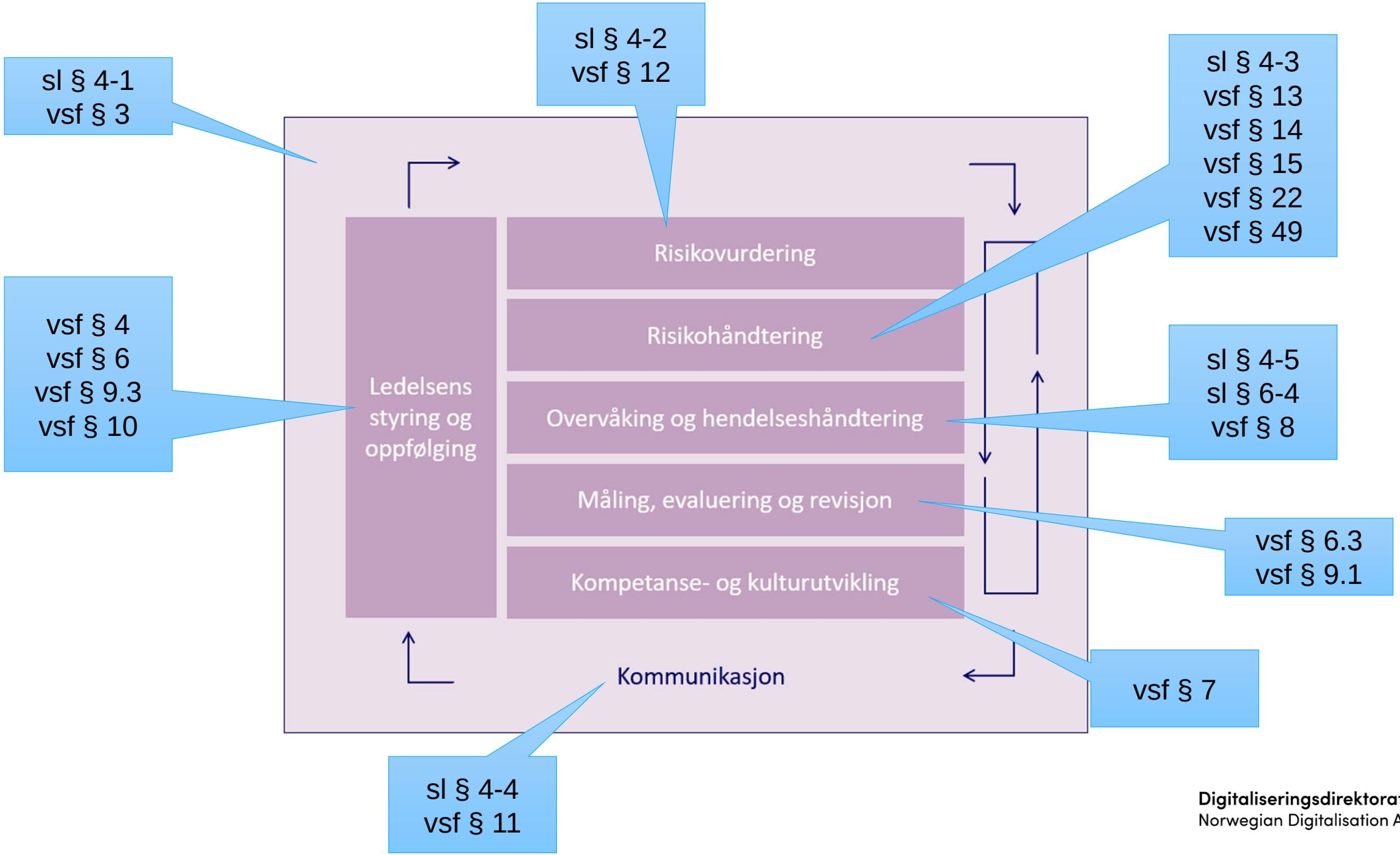
Styring og kontroll

Krav til innhold i styringsaktiviteter

Vurdering av behov

Forsvarlig sikkerhetsnivå

Minimumskrav til sikkerhetstiltak


sl § 4-1
vsf § 3
sl § 4-2
vsf § 12
sl § 4-3
vsf § 13
vsf § 14
vsf § 15
vsf § 22
vsf § 49
vsf § 4
vsf § 6
vsf § 9.3
vsf § 10
Ledelsens styring og oppfølging
Risikovurdering
Risikohåndtering
Overvåking og hendelseshåndtering
Måling, evaluering og revisjon
Kompetanse- og kulturutvikling
Kommunikasjon
sl § 4-5
sl § 6-4
vsf § 8
vsf § 6.3
vsf § 9.1
vsf § 7
sl § 4-4
vsf § 11

# Eksempel: internkontrollforskriften (HMS)

| Internkontroll innebærer at virksomheten skal: |
| --- |
| 1. sørge for at de lover og forskrifter i helse-, miljø- og sikkerhetslovgivningen som gjelder for virksomheten er tilgjengelig, og ha oversikt over de krav som er av særlig viktighet for virksomheten |
| 2. sørge for at arbeidstakerne har tilstrekkelig kunnskaper og ferdigheter i det systematiske helse-, miljø- og sikkerhetsarbeidet, herunder informasjon om endringer |
| 3. sørge for at arbeidstakerne medvirker slik at samlet kunnskap og erfaring utnyttes |
| 4. fastsette mål for helse, miljø og sikkerhet |
| 5. ha oversikt over virksomhetens organisasjon, herunder hvordan ansvar, oppgaver og myndighet for arbeidet med helse, miljø og sikkerhet er fordelt |
| 6. kartlegge farer og problemer og på denne bakgrunn vurdere risiko, samt utarbeide tilhørende planer og tiltak for å redusere risikoforholdene |
| 7. iverksette rutiner for å avdekke, rette opp og forebygge overtredelser av krav fastsatt i eller i medhold av helse-, miljø- og sikkerhets- lovgivningen |
| 8. foreta systematisk overvåkning og gjennomgang av internkontrollen for å sikre at den fungerer som forutsatt |

Kompetanse- og kulturutvikling

Risikovurdering

Risikohåndtering

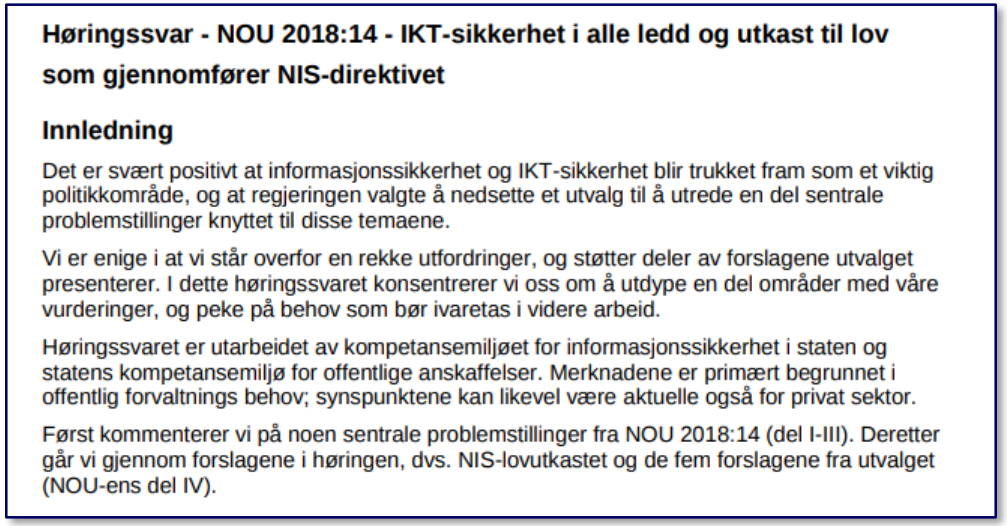
Måling, evaluering og revisjon

Overvåking og hendelseshåndtering

Ledelses styring og oppfølging

# ~~Difis~~ Høringssvar til NOU 2018:14 + NIS-lov

Digitaliseringsdirektoratets



**Høringssvar - NOU 2018:14 - IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet**

**Innledning**

Det er svært positivt at informasjonssikkerhet og IKT-sikkerhet blir trukket fram som et viktig politikkområde, og at regjeringen valgte å nedsette et utvalg til å utrede en del sentrale problemstillinger knyttet til disse temaene.

Vi er enige i at vi står overfor en rekke utfordringer, og støtter deler av forslagene utvalget presenterer. I dette høringssvaret konsentrerer vi oss om å utdype en del områder med våre vurderinger, og peke på behov som bør ivaretas i videre arbeid.

Høringssvaret er utarbeidet av kompetansemiljøet for informasjonssikkerhet i staten og statens kompetansemiljø for offentlige anskaffelser. Merknadene er primært begrunnet i offentlig forvaltnings behov; synspunktene kan likevel være aktuelle også for privat sektor.

Først kommenterer vi på noen sentrale problemstillinger fra NOU 2018:14 (del I-III). Deretter går vi gjennom forslagene i høringen, dvs. NIS-lovutkastet og de fem forslagene fra utvalget (NOU-ens del IV).

# PS: det svikter ikke alltid i det «digitale»

Bergens Tidende

## - Tilliten vår til byråden er tynnslitt

Bergens Tidende | 21 Jan 2020 | page 11 - 12 | 556 words

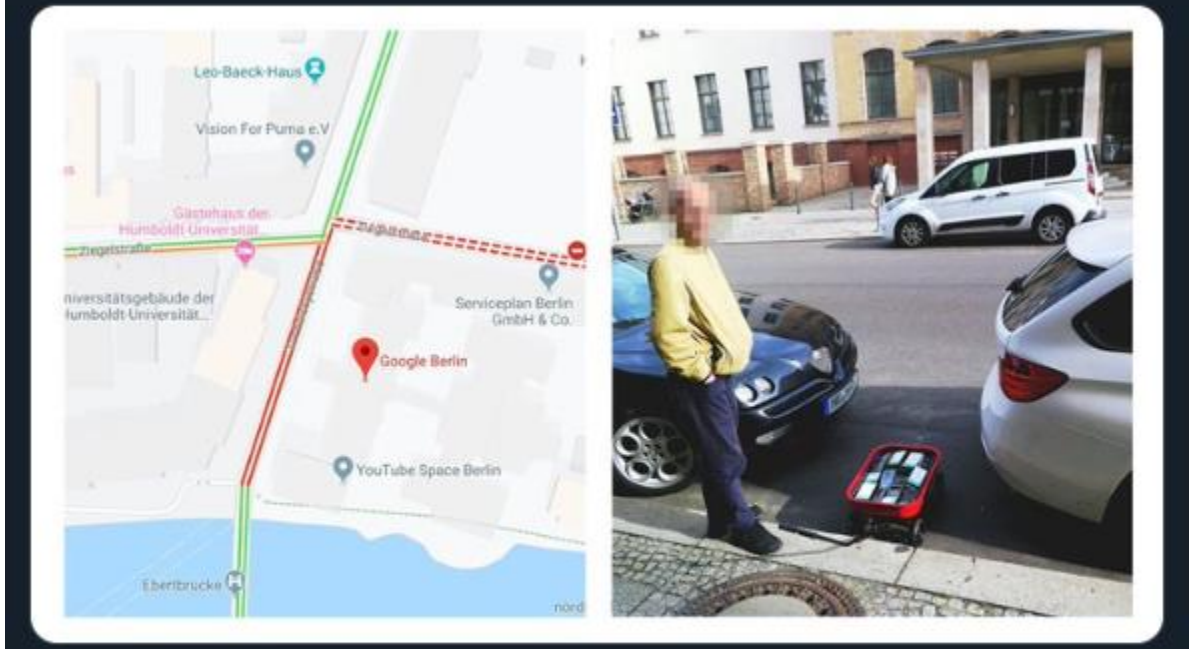
informasjonssikkerhet

Author: Gerd Margrete Tjeldflåt | Gerd Margrete Tjeldflåt

**Tirsdag svarer skolebyråd Linn Kristin Engø (Ap) for feilene kommunen har gjort i Vigilo-saken.**

**Simon Weckert**
@simon_deliver

99 smartphones are transported in a handcart to generate virtual traffic jam in Google Maps. Through this activity, it is possible to turn a green street red which has an impact in the physical world by navigating cars on another route! #googlemapshacks simonweckert.com/googlemapshack...




12:31 PM · Feb 1, 2020 · Twitter for iPhone

# Digitaliseringsdirektoratet

Digitaliseringsdirektoratet skal være en samordner og pådriver i offentlig sektors arbeid med [..] informasjonssikkerhet.

Digitaliseringsdirektoratet skal særskilt, bidra til at alle statlige virksomheter har et system for internkontroll av informasjonssikkerhet.

So, no pressure! 😉

Pressure is a privilege. 😬

Direktoratet for forvaltning og økonomistyring

Digitaliserings-direktoratet

NASJONAL SIKKERHETSMYNDIGHET

Digitaliseringsdirektoratet

Norwegian Digitalisation Agency