Oslo

Forum for informasjonssikkerhet og personvern

Onsdag 26. januar

Sendingen starter 09:00

Photo by OLEG PLIASUNOV on Unsplash

Program

09:00 - 09:05	**Velkommen og introduksjon til dagens program**
09:05 - 09:15	**Hva skjer på personvernområdet?** Maryke Silalahi Nuth
09:15 - 09:25	**Hva skjer på informasjonssikkerhetsområdet?** Åsmund Skomedal
09:25 - 09:50	**Skytjenesteveilederen** Ivar Aasgaard og Lars Martin Undhjem
09:50 – 10:00	Pause til å fylle kaffekoppen
10:00 – 10:35	**Grunnprinsipper for IKT-sikkerhet 2.0** Seniorrådgiver Are Søndenaa fra NSM
10:35 - 11:00	**Koordinatorundersøkelsen og avslutning** Cecilie Bergh

Praktisk info

- Mange deltagere i dag, skru av mikrofonen og rekk opp hånda eller skriv spørsmål eller kommentarer i chatten.
- Ha gjerne på kameraet!
- Vi vil stoppe noen ganger underveis for å svare på spørsmål. Noen spørsmål kan også bli besvart i chatten.
- 10 minutter pause ca. kl. 09:50

Oslo

Hva skjer på personvernområdet?

Maryke S. Nuth
Fagsjef personvern
maryke.nuth@byr.oslo.kommune.no

Forum for informasjonssikkerhet og personvern
26. januar 2022

Photo by Fabio on Unsplash

Hva er nytt på personvernområdet?

Personvernvurderinger

- Generelt kurs i bruken av malene for alle

Kurs for alle ansatte	
Gjennomført	01.12.2021
Kommende	feb, april og september (dato kommer)

- Spesielt kurs tilpasset enkeltsektorer

HEL	
Gjennomført	13.12.2021 (Del I)
Kommende	22.03.2022 (Del II)

BFE	
Gjennomført	05.01.2022 (Innføring)
Kommende	03.03.2022 (Gjennomgang av vurderinger)

Det er i tillegg planlagt flere kurs i HEI-sektoren

Løsning for behandlingsoversikt

- Planlagt utvikling og innføring innen 2022
- UKE er prosjekteier
- Skal innføres trinnvis

Vurdering av Facebook – Hva skal virksomhetene gjøre?

- Skaffe oversikt over virksomhetenes Facebook-side(r) og hva de bruker den til (formål)
- Kartlegge den faktiske bruken av Facebook:
  - Hvor mange er det som følger sidene?
  - Hvilken type informasjon samles inn som følge av kommunens bruk av Facebook?
  - Brukes Facebook-sidene til enveis kommunikasjon til innbyggere, eller legges det opp til dialog eller respons?
- Gjennomgå alle Facebook-sidene med den hensikt å
  - vurdere personvernvennlige innstillinger som tilbys av Facebook
  - begrense behandling av personopplysninger (dataminimering)
- Gjennomgå tidligere personvernvurderinger av Facebook. Hvis det ikke finnes slike vurderinger, bør det gjennomføres personvernvurderinger nå!

Bruk av apper

«Eierskaps»-/ansvarsforhold

- Hvem «eier» appen (som en løsning) og dataene (inkl. anonymiserte data og bruksmønstre)?
- Hvem er databehandler, underdatabehandler og behandlingsansvarlig?
- Hvem er ansvarlig for å gjennomføre personvernvurderinger?

Photo by Neil Soni on Unsplash

Har du spørsmål? Ta kontakt med din sektorkontakt i FIN/ISI team personvern

	BLK	FIN	NOE	BYU	MOS	KIF	OVK	AIS	HEI	BYD
Sektorkontakt	Siri P. Johansen			Christina M. Grønli			Linda M. Knutsen	Siril Jonassen		Linda M. Knutsen

Generelle henvendelser sendes til fagsjef for personvern Maryke S. Nuth

Oslo

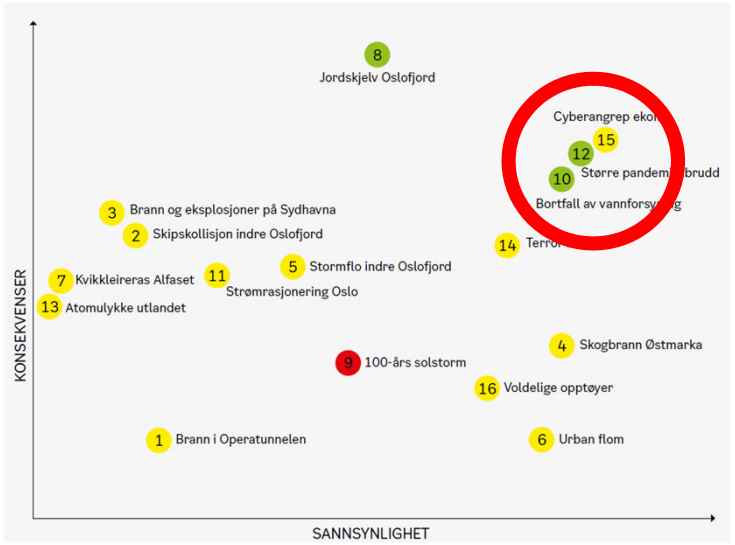
Informasjonssikkerhet

Hva skjer for tiden …

26. januar 2022

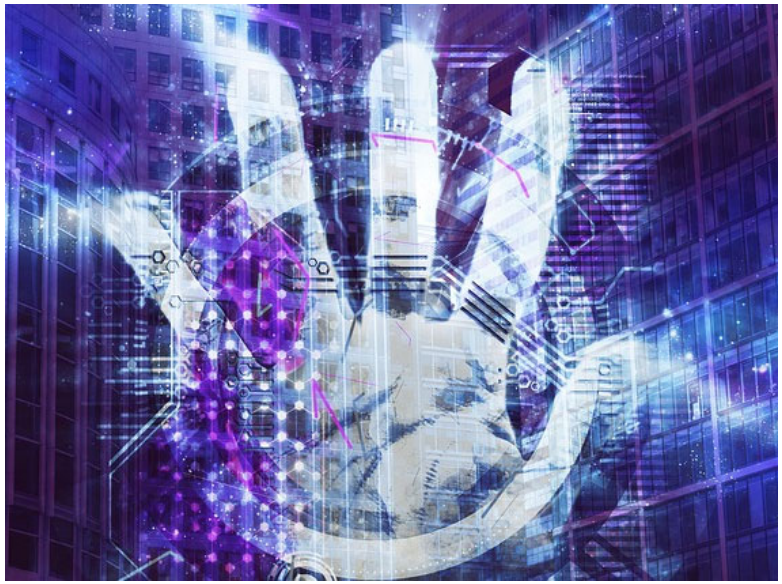
Åsmund Skomedal
Fagsjef informasjonssikkerhet
asmund.skomedal@byr.oslo.kommune.no

Utviklingen i 2021



- **Kommunalt Risikobilde** (KRB) for Oslo Kommune;
  et Cyberangrep er den mest sannsynlige alvorlige hendelsen
- Et skjerpet trusselbilde
  - **NSM** Oslo kommune er et attraktivt mål
  - **Digi.no** «I Norge har nettkriminaliteten det siste året økt med 72 prosent»
  - **NHO** «1 av 5 bedrifter rammet av dataangrep siste 12 månedene»
- Flere alvorlige hendelser den siste tiden; Amedia, Nortura, Nordic Choice, …
- Angrepet på Stortinget i 2020
  - **Datatilsynet** varslet 24. jan. et overtredelsesgebyr på 2 millioner kroner til Stortingets administrasjon

Informasjonssikkerhet i 2022 (i)



Noen aktuelle tema

- **Skytjenester** – ny veileder
- Virksomhetens eget **styringssystem**
  - Forankring hos virksomhetsledelsen !
  - Er organiseringen internt fortsatt egnet ?
- Oppfølging av faste **rutiner**
  - Er systemoversikten oppdatert (kartoteket) ?
  - Hvordan varsles og håndteres hendelser ?
- **Beredskapsplaner**
  - Revider ved behov
  - Gjennomfør en øvelse !
- Husk at *alle* systemer har sårbarheter; de er bare ikke oppdaget enda

Informasjonssikkerhet i 2022 (ii)

Tiltak det jobbes med sentralt:

- **Felles IKT-plattform**
  - Planlegger anskaffelse av 2-faktor autentisering (eget brev sendt)
    - Digitalt informasjonsmøte; 1. februar kl 13.30 - 15:00
    - Påmelding til lise.arneberg@byr.oslo.kommune.no
  - Innrullert og administrert sluttbrukerutstyr (PC og mobil)
- Flere funksjoner i felles **CSIRT**
- Ett felles styringsrammeverk (**ISMS**) for alle virksomheter
  - Minimumskrav og behovsprøvde krav
  - Veiledning og verktøystøtte til virksomhetenes styringssystem
- Oppfølging av alvorlige hendelser og **sårbarheter**
  - Log4j; eget brev til alle virksomhetene om oppfølging


Let's be careful out there!
Foto: irpp.org, Creativ

Oslo

Ny veileder: Sikker etablering av skytjenester

Forum 26. januar 2022

Lars Martin Undhjem, FIN/ISI
Ivar Aasgaard, FIN/ISI

Foto: Roman Odintsov (Pexels)

Agenda

- Bakgrunn og formål
- Målgrupper og anvendelsesområde
- Ansvar
- Risikostyring
- Fremgangsmåte
- Avrop

Bakgrunn og formål

- Veilederen ble besluttet utarbeidet for å veilede virksomheter i kommunen som har begrenset kunnskap og erfaring med egen utvikling, eller flytting, av applikasjoner i/til skyen.
- Formålet med veilederen er å bidra til å sikre at det ikke tas i bruk infrastruktur eller plattform i skyen som medfører uakseptabel risiko for kommunens virksomhet når det gjelder informasjonssikkerhet og personvern.
- I veilederen får du hjelp til oppgaver som bør eller må utføres i vurderingsprosessen rundt etablering av infrastruktur og plattform i sky.

Målgrupper og anvendelsesområde

- Målgruppen er ledere og medarbeidere som er systemeiere eller er involvert i arbeidet med etablering, utvikling, forvaltning og drift av skytjenester.
- Denne utgaven er rettet mot plattform som en tjeneste (PaaS) og infrastruktur som en tjeneste (IaaS), og etablering av kommunens egne tjenester basert på disse.

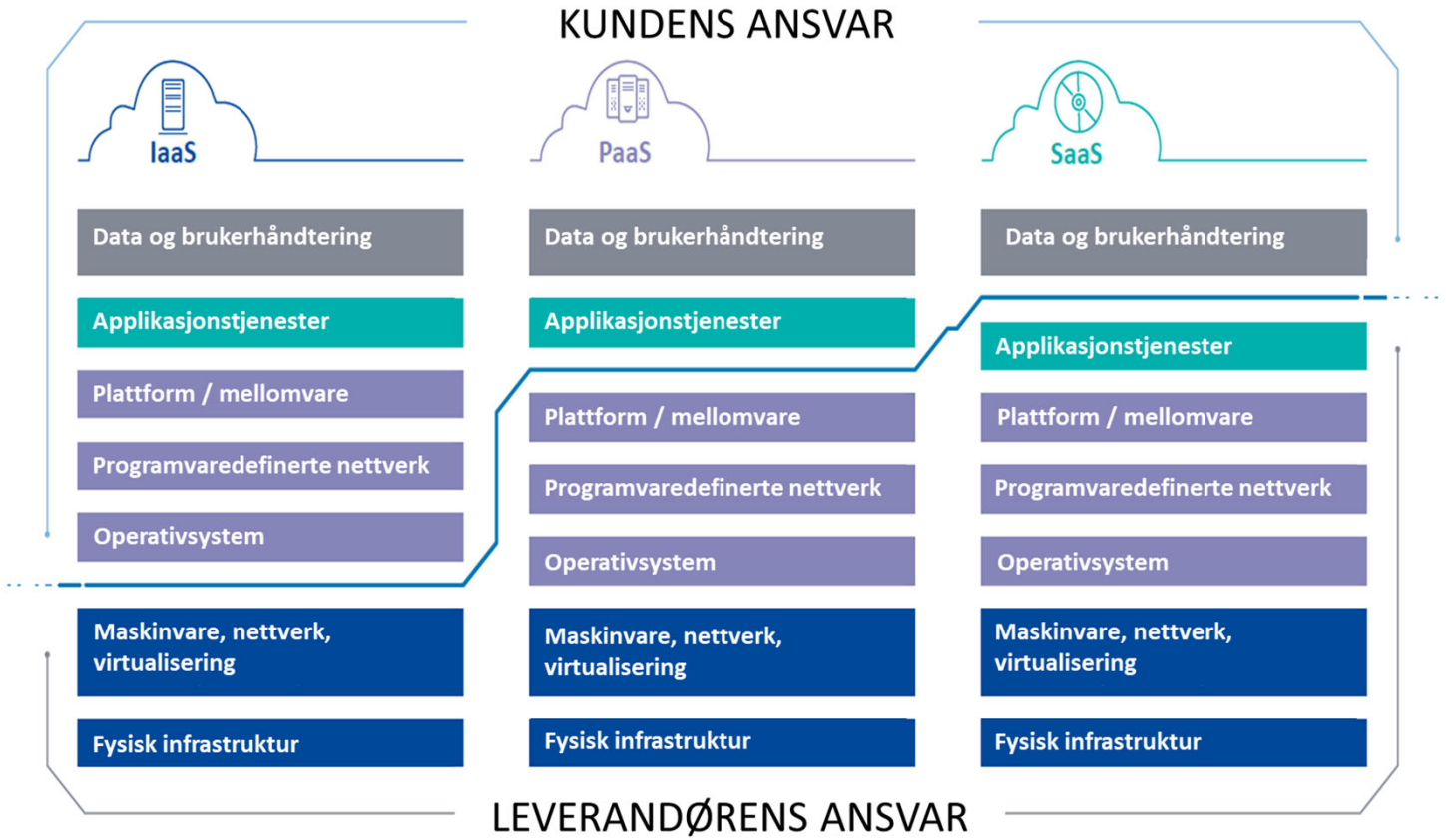
Rene applikasjonstjenester i skyen (SaaS) er ikke dekket av veilederen i nåværende versjon.

Veilederen finner du på felles intranett, her:
https://felles.intranett.oslo.kommune.no/informasjonssikkerhet-og-personvern/informasjonssikkerhet/skytjenester/

Ansvar

- Kommunens styrende dokumenter innenfor IKT og informasjonssikkerhet/personvern gjelder ved etablering og bruk av skytjenester på samme måte som for etablering og bruk av tradisjonell IKT.
- En virksomhet som setter ut tjenester til skyleverandører, setter ut oppgaver og kan ikke fraskrive seg ansvaret for IKT-tjenester som leveres til innbyggere, næringsliv eller ansatte.

Tjenestemodeller:



- Det kan være en utfordring å forstå og håndtere oppgavefordelingen mellom skytjenesteleverandør og virksomheten (kunden), spesielt fordi denne varierer med tjenestemodell.

Dette er alltid kundens (virksomhetens) ansvar

- Informasjonssikkerhet og personvern
- Eierskap til informasjonen i tjenesten
- Brukerautorisering
- Systemeierskap
- Akseptabel risiko
- Leverandøroppfølging
- Etterlevelse av lover, regelverk og styrende dokumenter

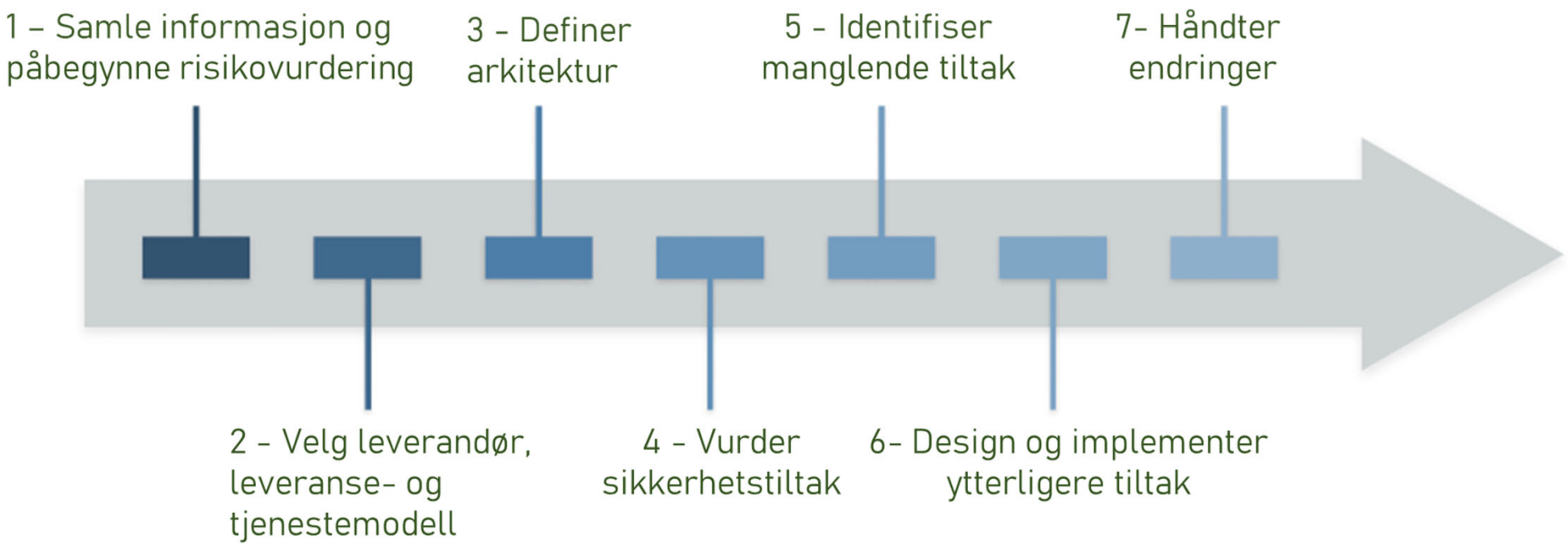
Risikostyring

- Risikostyring omfatter blant annet:
  - identifisering og verdivurdering av verdier
  - kartlegging av trusler, sårbarheter og uønskede hendelser som kan ramme verdiene
  - analyse av sannsynlighet og konsekvens av slike hendelser og vurdering mot akseptabel risiko
  - håndtering av risikoer som ikke er akseptable, gjennom å henholdsvis redusere, overføre, akseptere eller unngå risiko,
  - og deretter identifisere og iverksette nødvendige tiltak, samt følge opp at planlagte tiltak har blitt gjennomført

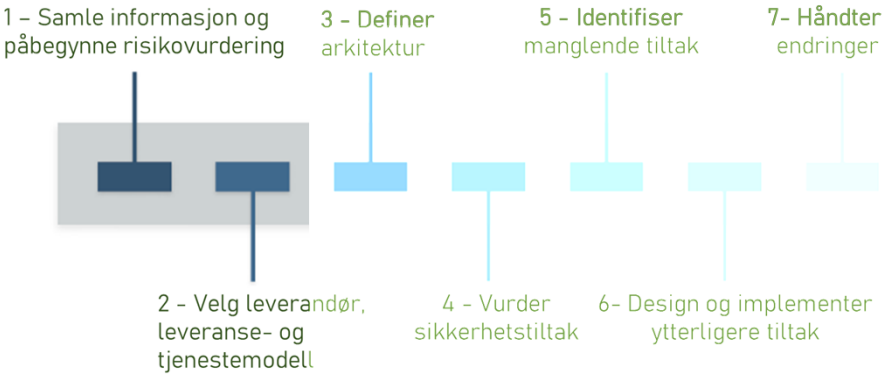
Risikostyring, forts

- *Hvordan påvirkes risikovurderinger ved bruk av skytjenester?*
  - det kan være ulike sårbarheter med tilhørende risikoer og tiltak avhengig av hvor informasjonen behandles.
  - Innhenting av data/underlag
- *Eksempler på risikoer ved skytjenester*
  - Kompleksitet av totalløsninger
  - Kompetanse
  - Avtaler og endringer i vilkår
  - Avhengighet til leverandør
  - Kostnader
  - Leverandørs tilgang til data
  - Lovpålagt utlevering av data til myndigheter

Fremgangsmåte

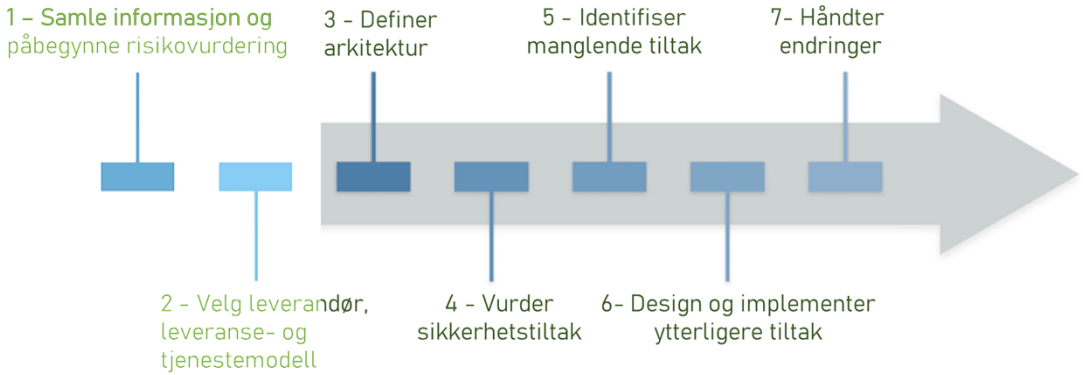


Fremgangsmåte



- Kort om Cloud Security Alliance (CSA)
- Steg 1: Samle informasjon og påbegynne risikovurdering
  - Kartlegging av informasjon som skal behandles
  - Kartlegging av lover og regelverk som får anvendelse
  - Klassifisering
  - Oppstart risikovurdering
- Steg 2: velg leverandør, leveranse- og tjenestemodell
  - Valg av tjenestemodell og leveransemodell (privat, offentlig, gruppe eller hybrid)
  - Exitstrategi
  - Avtaleoppfølging
  - Risikovurdering – steg 2

Videre steg



- Etter at man har gjort de overordnede vurderingene og kommet frem til at løsningen som skal realiseres er egnet for sky, begynner arbeidet med den tekniske løsningen.
- Arkitektur utarbeides, sikkerhetstiltak utformes og risikovurdering oppdateres.
- Valg av skytjenesteleverandør vil påvirke hvilke muligheter man har
- Veilederen dekker i nåværende utgave ikke disse stegene, kun steg 1 og 2.

Kort om lovgiving og skytjenesteavtaler

- Det kan finnes juridiske hindre for å gå til skyen, og veilederen tar for seg de vanligste:
  - Arkivloven
  - Bokføringslovgiving
  - Personopplysningsregelverket
  - Mm
- Ettersom avtaler er en essensiell del av skyleveranser sier veilederen også noe om
  - Varianter av skytjenesteavtaler
  - Vilkår i avtalene

Avrop

- Systemdriftsavtalen med Sopra Steria
- Samkjøpsavtalen «Lisenser Bredde» med Crayon
- Samkjøpsavtalen «Lisenser Microsoft» med Atea

Råd:
Snakk med din kundekontakt i UKE om egenskaper ved de ulike avtalene

Spørsmål?

Oslo

PAUSE

Sendingen starter igjen kl. 10:00

Photo by OLEG PLIASUNOV on Unsplash

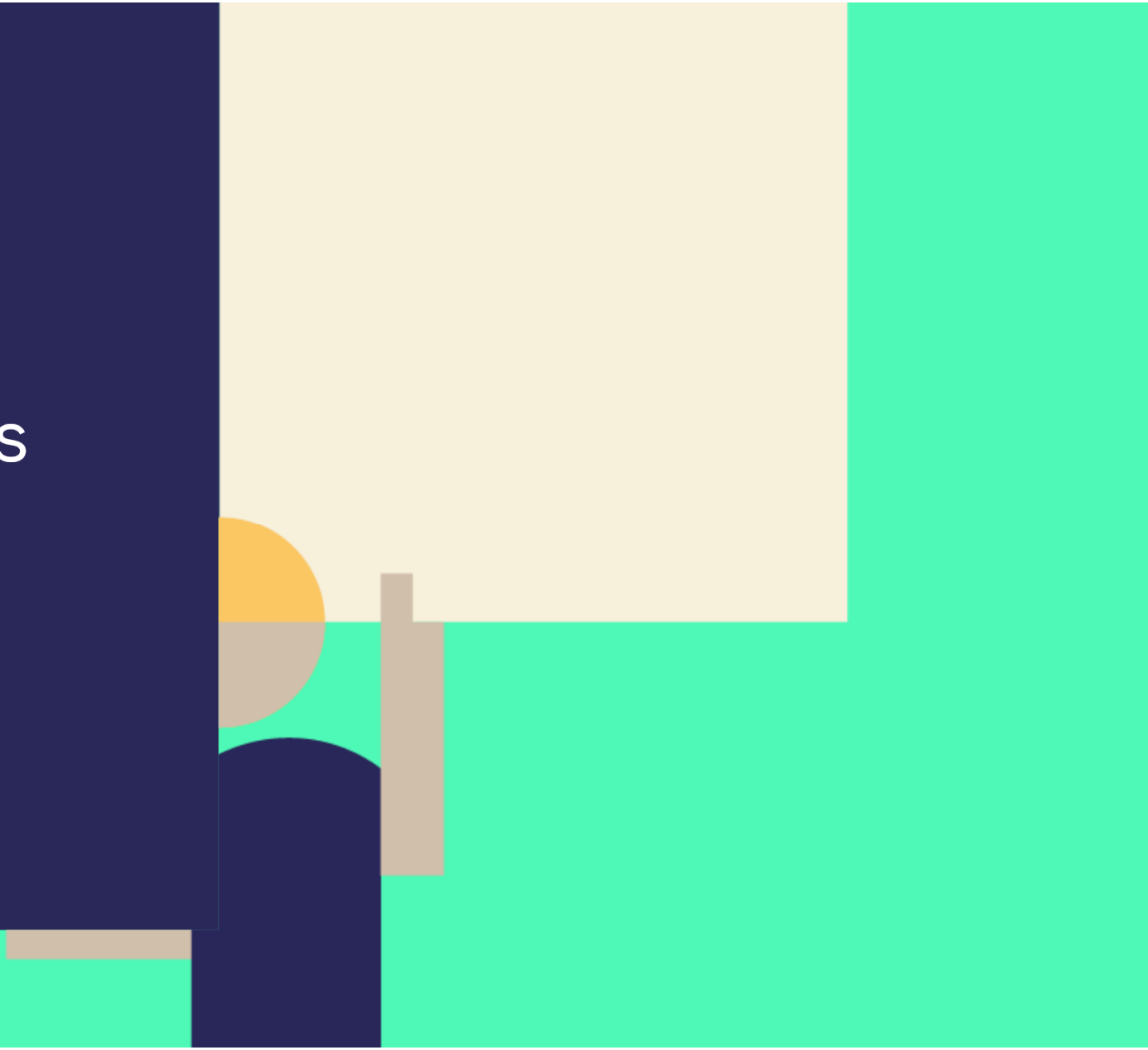
For mer informasjon se:
nsm.no/grunnprinsipper-ikt

Are Søndenaa
Seniorrådgiver (Nasjonalt cybersikkerhetssenter)
Nasjonal sikkerhetsmyndighet

Oslo

Innsikt om læringsbehov hos koordinatorene

Wenche Hagan
Maylén Mago Pedersen
Cecilie Bergh



Nye rollekort...

- Tildelingsbrev
- Rollene utpekes i virksomhetene
- 30 ISKer
- 27 PKOer
- 21 PISKer

Oslo

Oslo

Informasjonssikkerhets-koordinator (ISK)

Rollekortene er veiledninger, basert på relevante styrende dokumenter i Oslo kommune. Det er ikke obligatorisk å ta i bruk rollekortene, med mindre dette er besluttet i den enkelte sektor/virksomhet.

Rollekortene beskriver typiske oppgaver for informasjonssikkerhet og/eller

ROLLE

Informasjonssikkerhetskoordinator (ISK) skal bistå virksomhetsleder i arbeidet med å sikre etterlevelse av regelverket. Koordinatoren vil også være en sentral rådgiver for virksomhetsleder og øvrig ledelse. Av denne grunn er det viktig at informasjonssikkerhetskoordinator får rapportere direkte til virksomhetsleder.

Informasjonssikkerhetskoordinatoren må samarbeide med virksomhetens personvernkoordinator (PKO), dersom denne rollen ivaretas av en annen ansatt. Det er også nødvendig å samarbeide med andre relevante roller, f.eks. systemeiere, systemforvaltere, sikkerhetsledere mv., både internt i virksomheten og ellers i kommunen.

Koordinatoren er virksomhetens kontaktpunkt innen informasjons- og IKT-sikkerhet for overordnet byrådsavdeling og for kommunens sentrale fagmiljø innen personvern og informasjonssikkerhet i Byrådsavdeling for finans.

Informasjonssikkerhetskoordinatoren er *ikke ansvarlig for*

Informasjonssikkerhetskoordinator (ISK) Oslo

PLANLEGGE
- Utarbeide årsplan for virksomhetens oppgaver innen informasjonssikkerhet.
- Bistå virksomhetsleder i oppfølgingen av årsplanen.
- Utarbeide og vedlikeholde styrende dokumenter for informasjonssikkerhet for virksomheten, i tråd med kommunens styrende dokumenter.
- Forvalte oversikt over gjeldende myndighetskrav for å ivareta taushetsplikt og informasjonssikkerhet.

RÅDGIVNING OG KONTAKTPERSON
- Gi råd og veiledning innen informasjonssikkerhet til ledelsen og ansatte, både generelt og i prosjekter og anskaffelser.
- Bistå med å implementere informasjonssikkerhet i arbeidsprosesser.
- Være virksomhetenes kontaktperson innen spørsmål og oppgaver relatert til informasjonssikkerhet overfor overordnet byrådsavdeling, Byrådsavdeling for finans og kommunens personvernombud.

KOMPETANSE
- Vedlikeholde egen kompetanse på fagområdet.
- Delta på kommunens arrangementer og kurs for koordinatorene.
- Tilrettelegge for nødvendig og målrettet opplæring i informasjonssikkerhet til alle ansatte i virksomheten, inkludert ledelsen.
- Koordinere og delta i felles kampanjer for informasjonssikkerhet i virksomheten.

RISIKOSTYRING
- Bistå ved gjennomføring av overordnet risikovurdering for informasjonssikkerhet.
- Koordinere gjennomføringen av risikovurderinger og oppfølging av status.
- Bistå i å fasilitere virksomhetens risikovurderinger etter behov.
- Oppfølging av uakseptabel risiko.

RUTINER
- Bidra til å etablere og vedlikeholde rutiner innen informasjonssikkerhetsområdet, bl.a. for autorisering og tilgangskontroll, og for beredskap.
- Følge opp at etablerte rutiner etterleves.
- Bidra til å gjennomføre beredskapsøvelser for å sikre kontinuitet i virksomhetens tjenester.

HENDELSER OG AVVIK
- Bidra til å håndtere informasjonssikkerhetshendelser- og brudd.
- Bidra til oversikt over alle avvik og sikkerhetsbrudd.
- Rapportere alvorlige sikkerhetsbrudd til virksomhetsleder.

RAPPORTERING
- Bistå ved rapportering av alvorlige sikkerhetsbrudd til overordnet byrådsavdeling og til Byrådsavdeling for finans.
- Bistå virksomhetsleder med rapportering av informasjonssikkerhetstilstand gjennom virksomhetsleders egenerklæring, ledelsens gjennomgang og en oppsummering av hendelser og avvik.

Oslo

Personvernkoordinator (PKO)

Rollekortene er veiledninger, basert på relevante styrende dokumenter i Oslo kommune. Det er ikke obligatorisk å ta i bruk rollekortene, med mindre dette er besluttet i den enkelte sektor/virksomhet.

Rollekortene beskriver typiske oppgaver for informasjonssikkerhet og/eller

ROLLE

Personvernkoordinator (PKO) skal bistå virksomhetsleder i arbeidet med å sikre etterlevelse av regelverket. Koordinatoren vil også være en sentral rådgiver for virksomhetsleder og øvrig ledelse. Av denne grunn er det viktig at personvernkoordinator får rapportere direkte til virksomhetsleder.

Personvernkoordinatoren må samarbeide med virksomhetens informasjonssikkerhetskoordinator (ISK), dersom denne rollen ivaretas av en annen ansatt. Det er også nødvendig å samarbeide med andre relevante roller, f.eks. personvernombud, systemeiere, systemforvaltere, sikkerhetsledere mv., både internt i virksomheten og ellers i kommunen.

Koordinatoren er virksomhetens kontaktpunkt innen personvern for overordnet byrådsavdeling, for kommunens sentrale fagmiljø innen personvern og informasjonssikkerhet i Byrådsavdeling for finans, samt for personvernombudet.

Personvernkoordinatoren er *ikke ansvarlig for* virksomhetens

Personvernkoordinator (PKO) Oslo

PLANLEGGE
- Utarbeide årsplan for virksomhetens oppgaver innen personvern.
- Bistå virksomhetsleder i oppfølgingen av årsplanen.
- Utarbeide og vedlikeholde styrende dokumenter for personvern for virksomheten, i tråd med kommunens styrende dokumenter.
- Forvalte oversikt over gjeldende krav innen personvern.

RÅDGIVNING OG KONTAKTPERSON
- Gi råd og veiledning innen personvern til ledelsen og ansatte ved behandling av personopplysninger.
- Bidra med råd og veiledning knyttet til personvern i prosjekter og anskaffelser, herunder ved inngåelse av databehandleravtaler og ved kravstilling.
- Bistå med å implementere personvern i arbeidsprosesser.
- Være virksomhetenes kontaktperson innen personvernrelaterte spørsmål og oppgaver overfor overordnet byrådsavdeling, Byrådsavdeling for finans og kommunens personvernombud.

KOMPETANSE
- Vedlikeholde egen kompetanse på fagområdet.
- Delta på kommunens arrangementer og kurs for koordinatorene.
- Tilrettelegge for nødvendig og målrettet opplæring innen personvern til ledelsen og ansatte i virksomheten.
- Koordinere og delta i felles kampanjer for personvern i virksomheten.

OVERSIKT OG VURDERINGER
- Bistå ved utfylling og vedlikehold av behandlingsoversikt for personopplysninger.
- Bistå ved overordnede vurderinger av personvern i de enkelte behandlingsprosessene.
- Bistå i vurderingen av om det er behov for å gjennomføre personvernkonsekvensvurderinger (DPIA).
- Bistå i, og eventuelt fasilitere, virksomhetens DPIAer.
- Bistå ved gjennomføring av eventuelle forhåndsdrøftelser med Datatilsynet.

RUTINER
- Bidra til å etablere og vedlikeholde rutiner innen personvernområdet.
- Følge opp at etablerte rutiner etterleves.

HENDELSER OG AVVIK
- Bidra til å håndtere personvernhendelser og brudd på personopplysningssikkerheten.
- Bidra til oversikt over alle hendelser og avvik.
- Rapportere alvorlige hendelser og avvik til virksomhetsleder.

RAPPORTERING
- Bistå ved rapportering av hendelser og avvik til Datatilsynet, til overordnet byrådsavdeling, til Byrådsavdeling for finans og til personvernombudet.
- Bistå virksomhetsleder med årlig rapportering av tilstand på personvernområdet gjennom virksomhetsleders egenerklæring og ledelsens gjennomgang, samt oppsummering av hendelser og avvik.

...krever relevant kompetanse

KOMPETANSEMÅL for koordinator

- I stand til å planlegge og utarbeide årsplan for virksomhetens oppgaver innen personvern og informasjonssikkerhet.
- I stand til å gi råd og veiledning til ledelsen og ansatte, både generelt, i prosjekter og anskaffelser.
- Forstå hva det innebærer å være virksomhetens kontaktperson innen spørsmål og oppgaver relatert til personvern og informasjonssikkerhet overfor overordnet byrådsavdeling, Byrådsavdeling for finans og kommunens personvernombud.
- I stand til å tilrettelegge for nødvendig og målrettet opplæring innen personvern og informasjonssikkerhet til ledelsen og ansatte og koordinere og delta i felles kampanjer i sin virksomhet.
- I stand til å fasilitere arbeidsprosesser (ref. risikovurderinger, personvernkonsekvensvurderinger, DPIA)
- I stand til å etablere og vedlikeholde rutiner og følge opp at etablerte rutiner etterleves, herunder internkontroll.
- I stand til å håndtere personvern- og informasjonssikkerhetshendelser og brudd og ha oversikt over alle hendelser og avvik i virksomheten.
- Bistå med rapportering av alvorlige hendelser, sikkerhetsbrudd og avvik til Datatilsynet, overordnet byrådsavdeling og Byrådsavdeling for finans
- Bistå med virksomhetsleders årlige rapportering (ref. virksomhetsleders egenerklæring, ledelsens gjennomgang, oppsummering av hendelser og avvik)

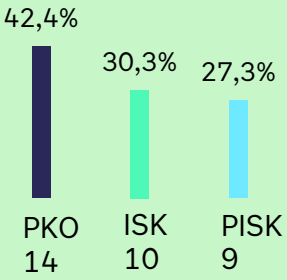
Om innsiktsarbeidet

DYBDEINTERVJUER

- 7 virksomheter
- 11 Koordinatorer
- 6 virksomhetsledere
+ 1 direktør i ledergruppa

- Organisering og forankring av arbeidet i virksomheten
- Hvordan virksomheten jobber med informasjonssikkerhet og personvern
- Samarbeid mellom koordinator og ledelse
- Virksomhetsleders syn på informasjonssikkerhet og personvern
- Utfordringer med arbeidet i Oslo kommune
- Utfordringer med arbeidet i virksomhetene
- Rollekortene
- Styringsdialog med overordnet byrådsavdeling
- Organisasjonsressurser for koordinatorene (tid, oppgaver, ansvar)
- Kompetansebehov hos koordinatorene
- Kompetansebehov hos ledere
- Kompetansebehov i virksomhetene

SPØRREUNDERSØKELSE



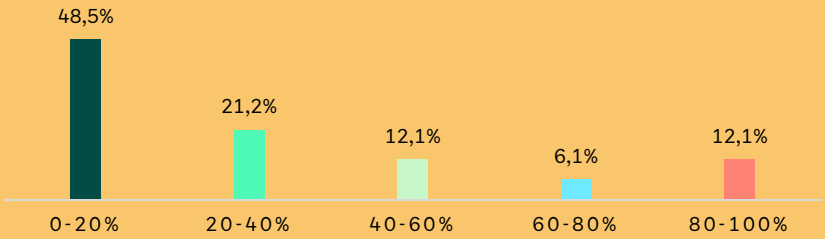
77 koordinatorer totalt i Oslo kommune
33 har svart - 43 %

- Om koordinatorenes kompetanse
- Om arbeidsoppgavene de ivaretar
- Om verktøy de bruker (verktøy, maler, sjekklister og veiledere)
- Om utkastet til læringskonsept
- Om samarbeid og støtte
- Bakgrunnsinformasjon om dem

Bakgrunnsinformasjon om koordinatorene

«Jeg sto på kopi i en e-post, der sto det at jeg var ny personvernkoordinator. Da jeg spurte sjefen min visste heller ikke sjefen hva rollen innebar (...)»

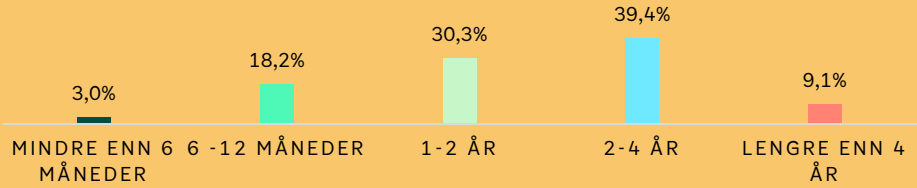
HVOR MYE TID BRUKER DU I ROLLEN DIN SOM KOORDINATOR?



«Skulle brukt mer tid på arbeidet. Jeg føler meg trygg i hva rollen min er, men ikke trygg på at jeg gjør det rollen sier.»

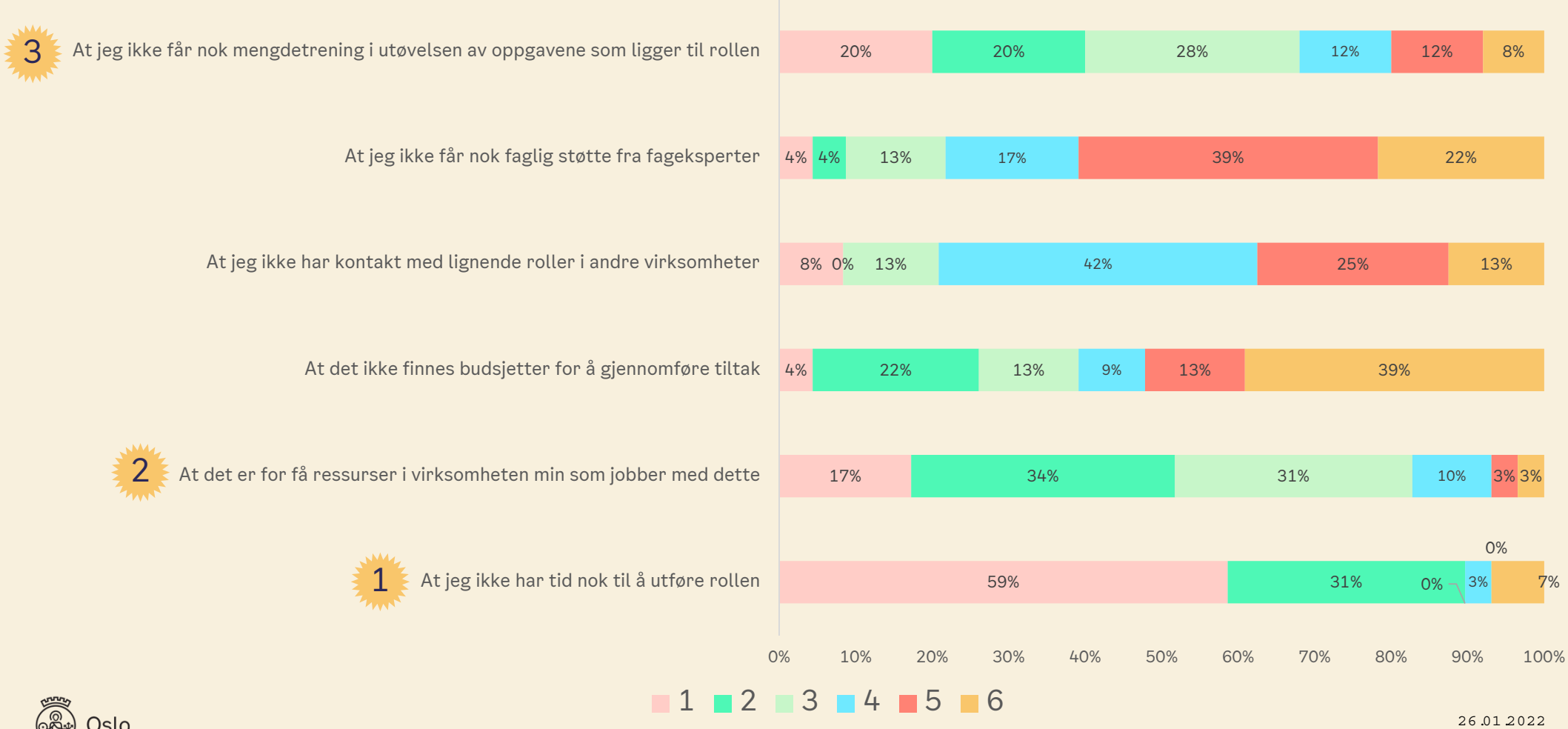
HVORDAN FIKK DU ROLLEN?

HVOR LENGE HAR DU HATT ROLLEN?



Organisatoriske utfordringer

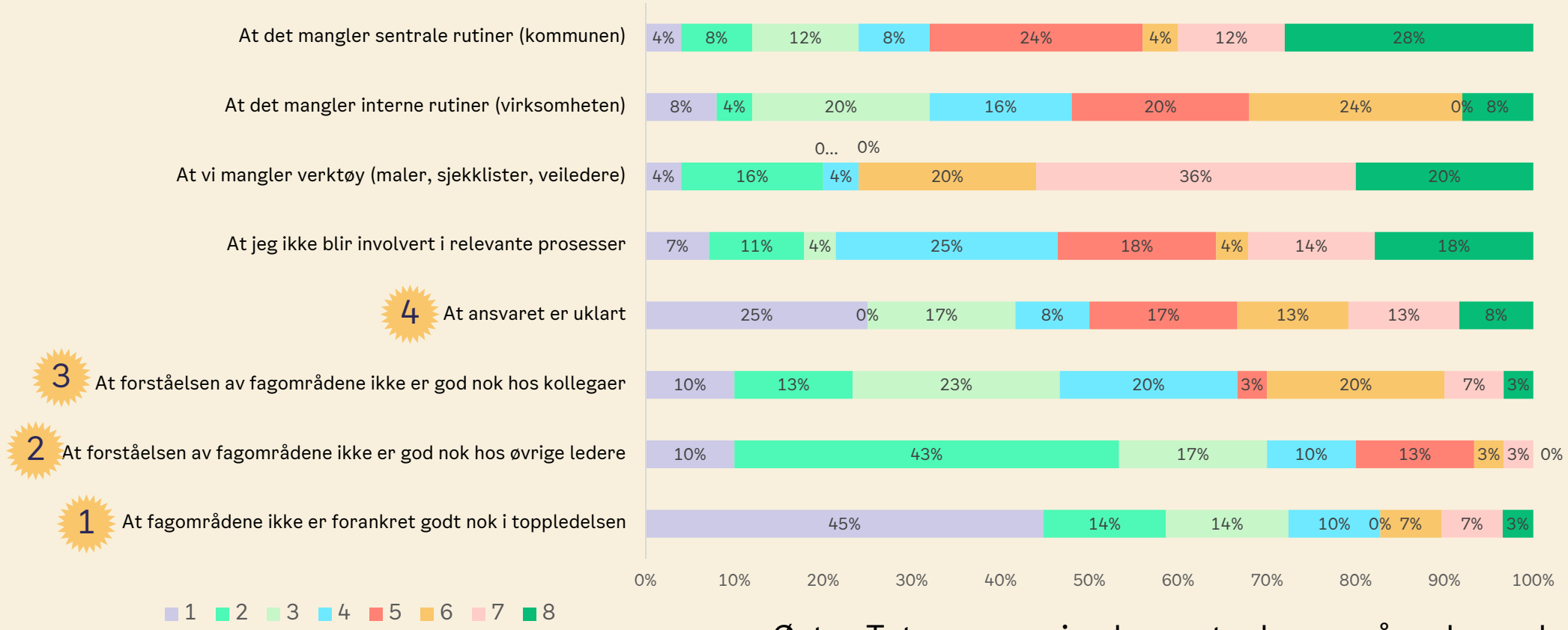
«Personvernoppgavene kommer fra alle kanter, kan bli litt bustete på håret av det.»



«Det føles litt ut som at om vi har det på papiret, så er det greit».

Organisatoriske utfordringer

«Føler jeg svømmer motstrøms uten at ledelsen støtter. Tenker at dersom det skjer noe, så får jeg også skylda.»



«Østre Toten er noe jeg kunne tenke meg å male med bred pensel til min ledelse.»

Oslo

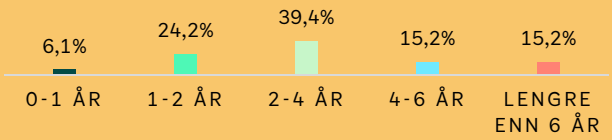
Organisering og forankring

- Rollene er etablert i de virksomhetene vi snakket med.
- Koordinatorene opplever at fagområdene er lite forankret i ledelsen.
- Koordinatorene opplever gjennomgående stor arbeidsbelastning
- Ulik organisering
  - en virksomhet har etablert et sikkerhetsforum som jobber bredt med sikkerhet, herunder informasjonssikkerhet.
  - de fleste mangler organisering rundt rollen.
  - varierer om rollene er samlet i en enhet eller i ulike avdelinger

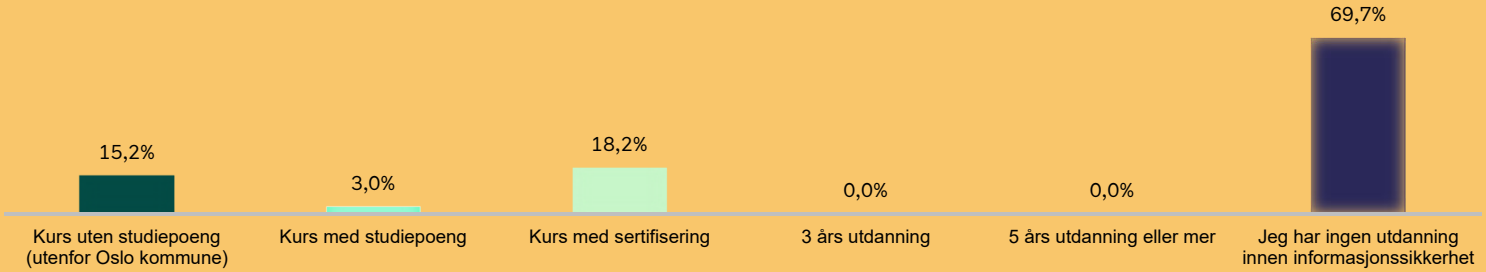
- Flere virksomhetsledere oppfatter personvern som krevende og til hinder for å sette i gang med prosesser.

Fagkunnskap

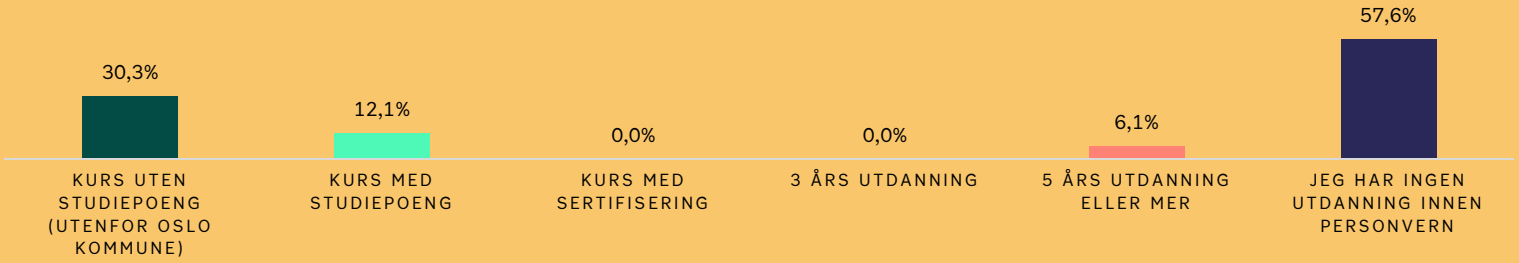
HVOR MANGE ÅR I LØPET AV DITT ARBEIDSLIV HAR DU JOBBET MED INFORMASJONSSIKKERHET ELLER PERSONVERN?



HAR DU NOEN UTDANNING INNEN INFORMASJONSSIKKERHET? (FLERVALG)



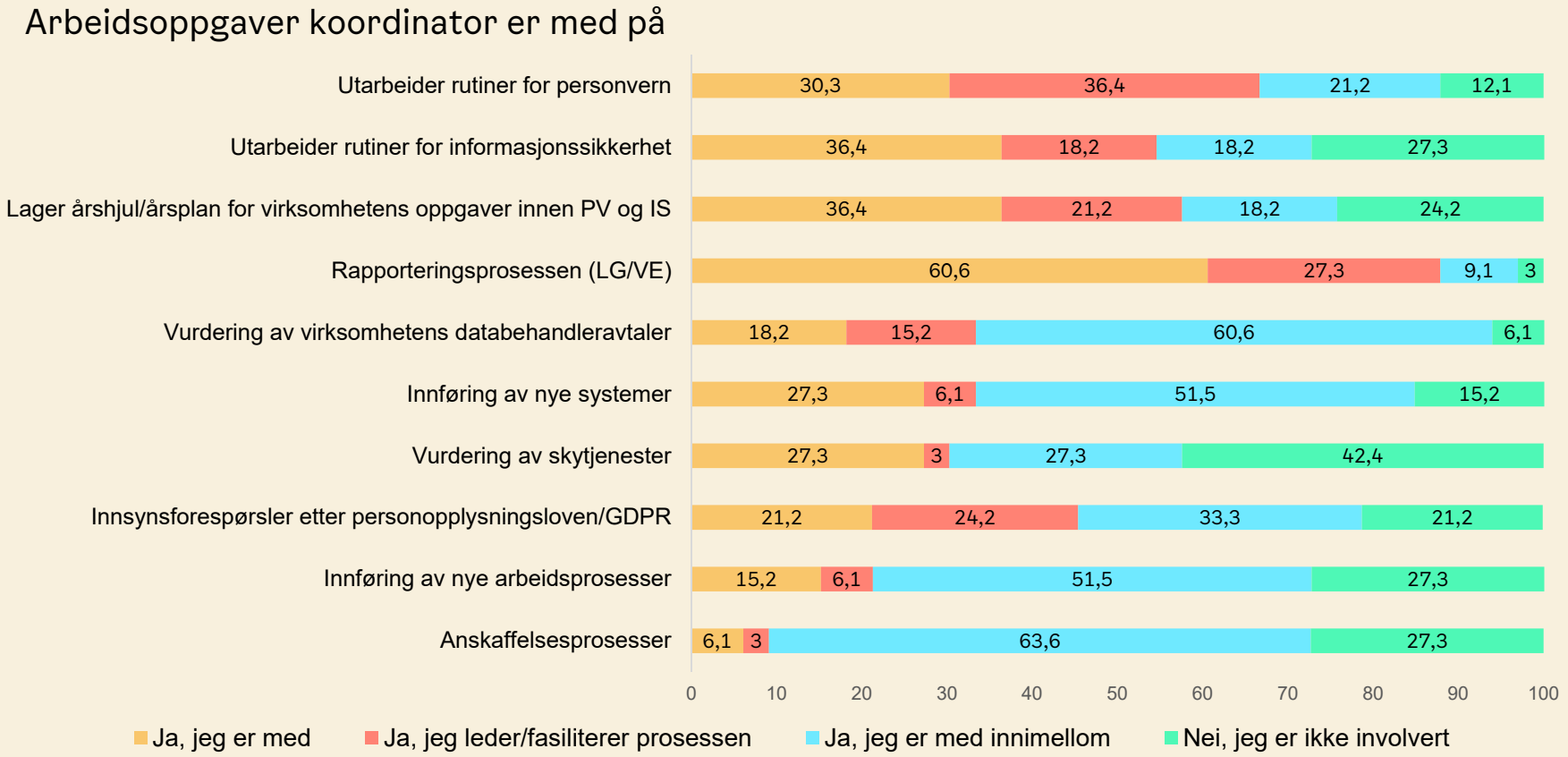
HAR DU NOEN UTDANNING INNEN PERSONVERN? (FLERVALG)



Oslo

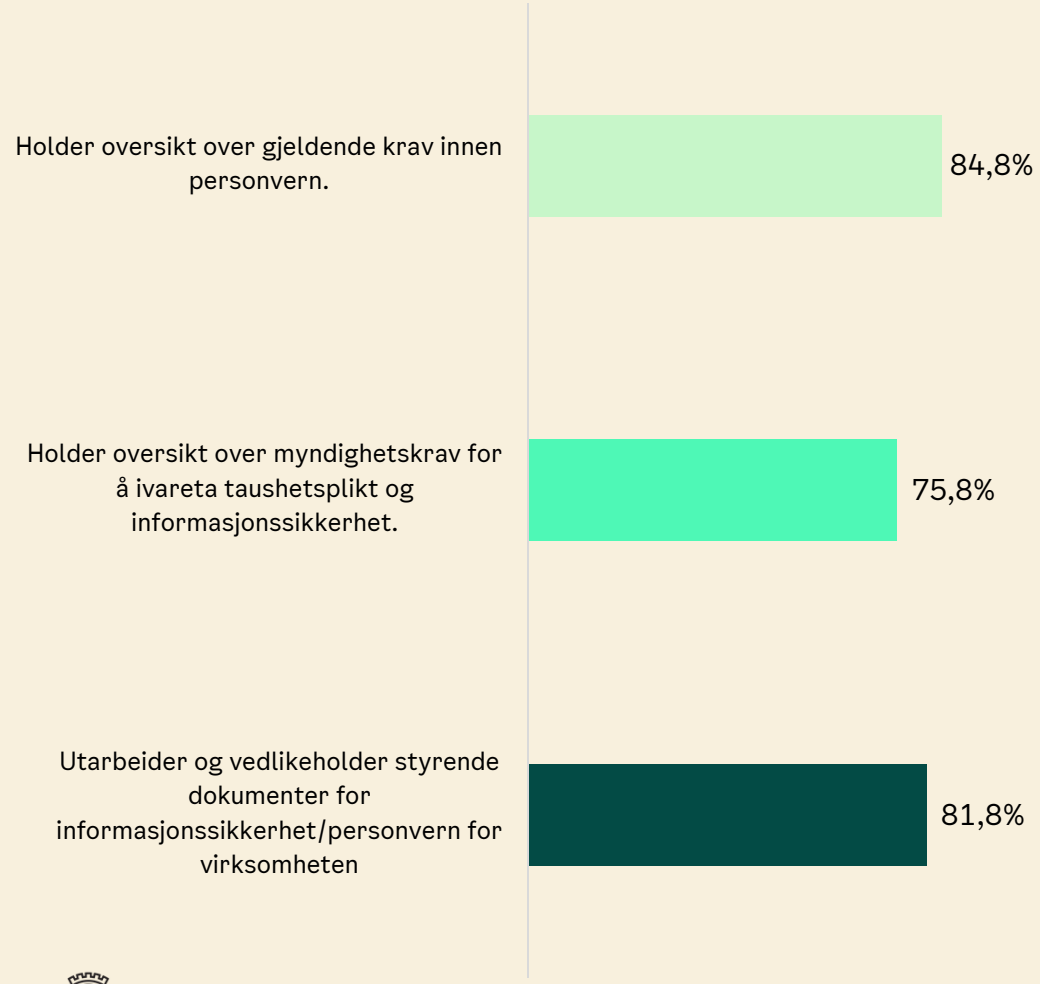
Om arbeidsoppgavene

«Jeg skulle ønske at flere oppgaver enn LG/VE var obligatoriske oppgaver, for da må man prioritere dem.»



6,1 % deltar ikke/bidrar ikke i nevnte oppgaver

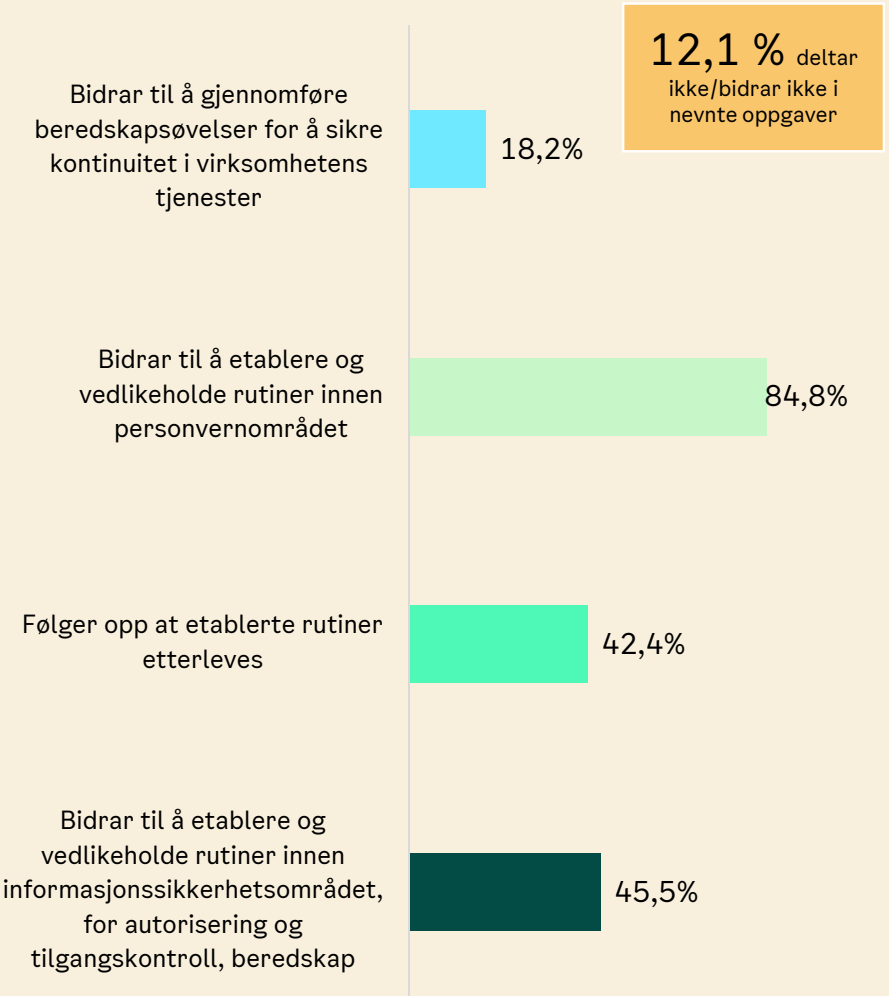
Krav og styrende dokumenter



«Hvis jeg skulle sette meg ned å skrive en rutine så hadde jeg trengt mye hjelp til den».

Rutiner og internkontroll

12,1 % deltar ikke/bidrar ikke i nevnte oppgaver

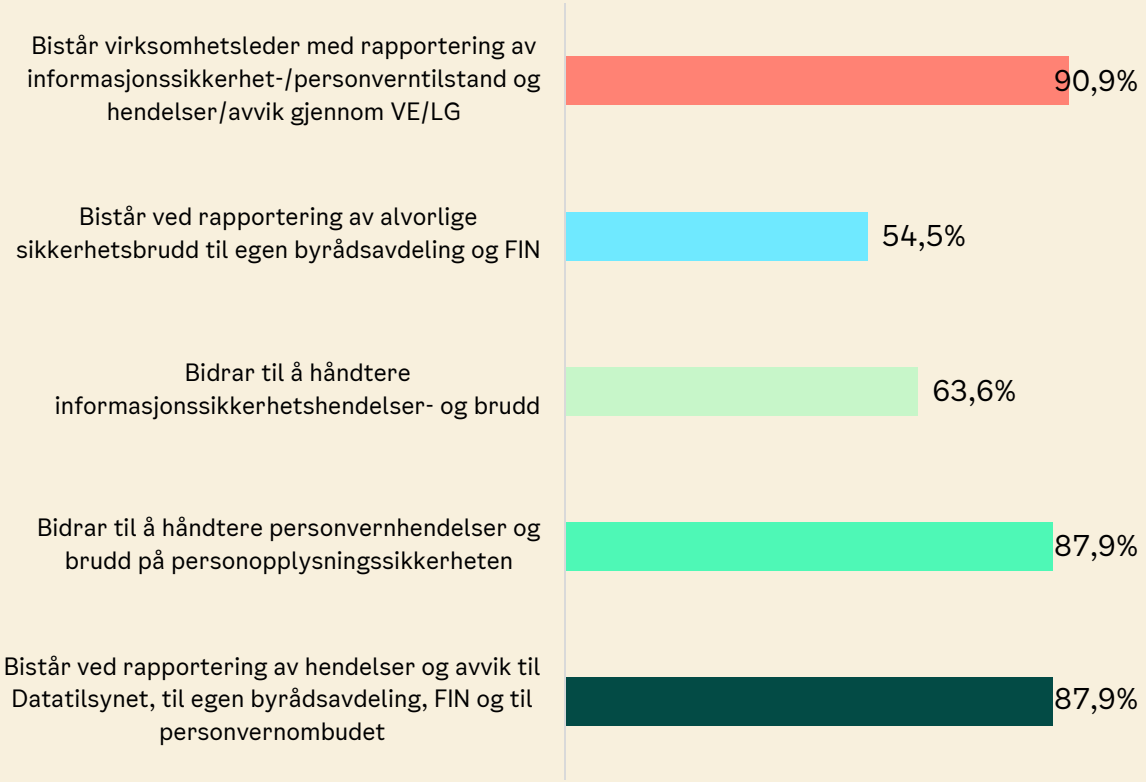


Oslo

3 % deltar ikke/bidrar ikke i nevnte oppgaver

«Jeg skulle ønske at styring av informasjonssikkerhet og personvern var en del av virksomhetsstyringen.»

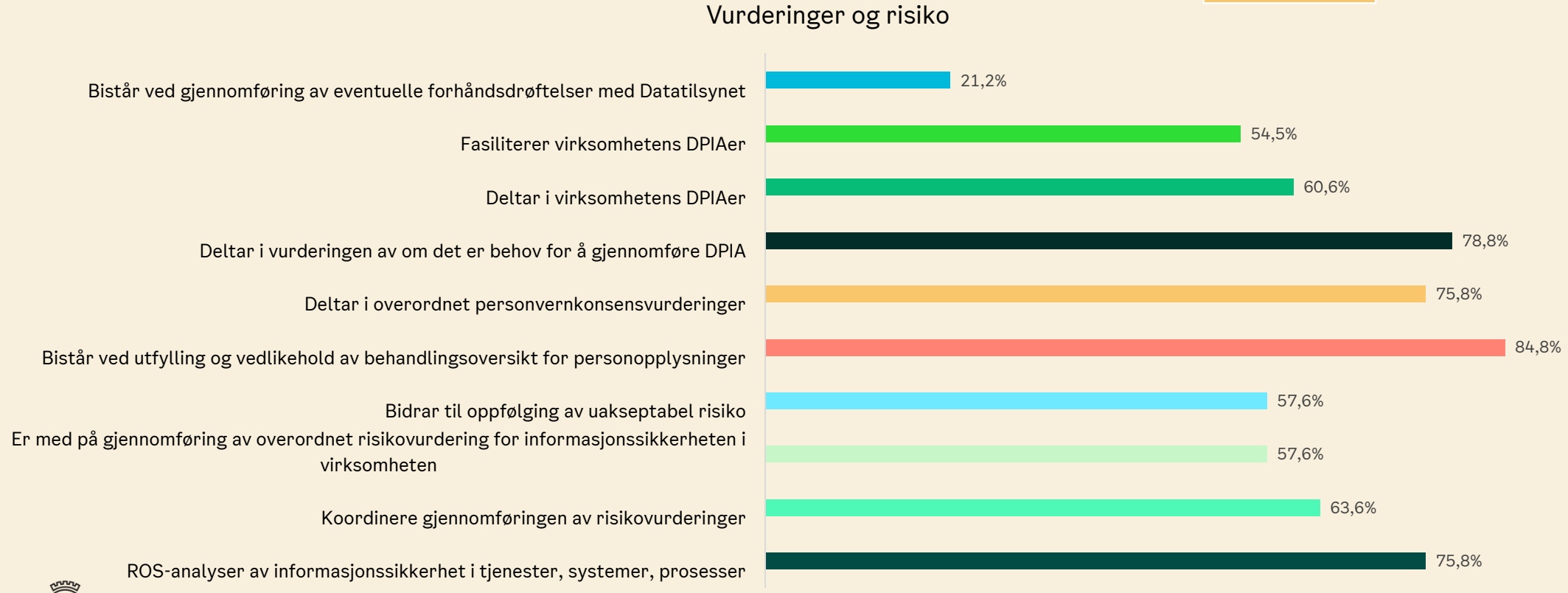
Rapportering og avvikshåndtering



- Ulike avvikssystem i virksomhetene
- Opplever få avviksmeldinger og tror det handler om underrapportering

«Jeg ønsker meg kurs og møtefora på ROS- og DPIA. Viktig å møte andre!»

3 % deltar ikke/bidrar ikke i nevnte oppgaver



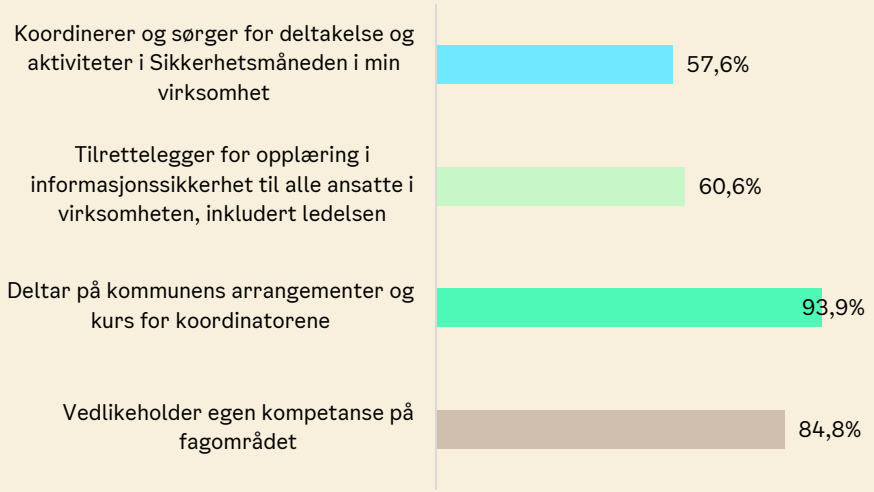
«Det er behov for å jobbe med holdningsendringer hos lederne, og da særlig de som jobber med mer sensitive opplysninger. Hva kan sendes på e-post og hva kan ikke sendes på e-post – hvordan få bort vanen hos ledere til å sende personopplysninger på e-post?»

3 % deltar ikke/bidrar ikke i nevnte oppgaver

Råd og veiledning

6,1 % deltar ikke/bidrar ikke i nevnte oppgaver

Kompetanseaktiviteter

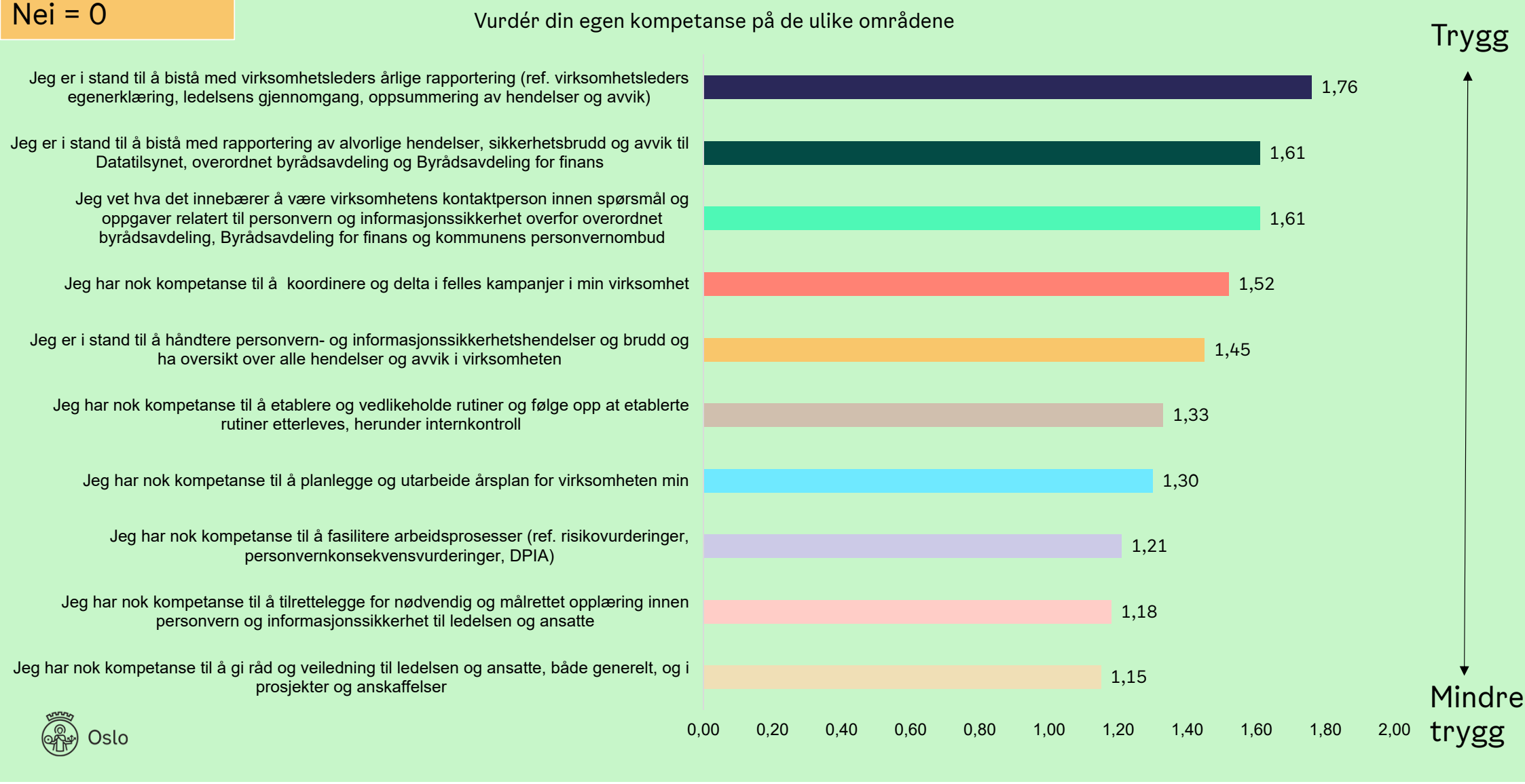


Ønskeliste fra koordinatorene:
- Utvikle verktøy for hvordan du holder opplæring i en virksomhet
- Metoder for å jobbe med sikkerhetskultur og atferdsendring i egen organisasjon.
- Dialogverktøy for hvordan koordinatorene kan snakke med ledelsen

Fagkunnskap og arbeidsoppgaver

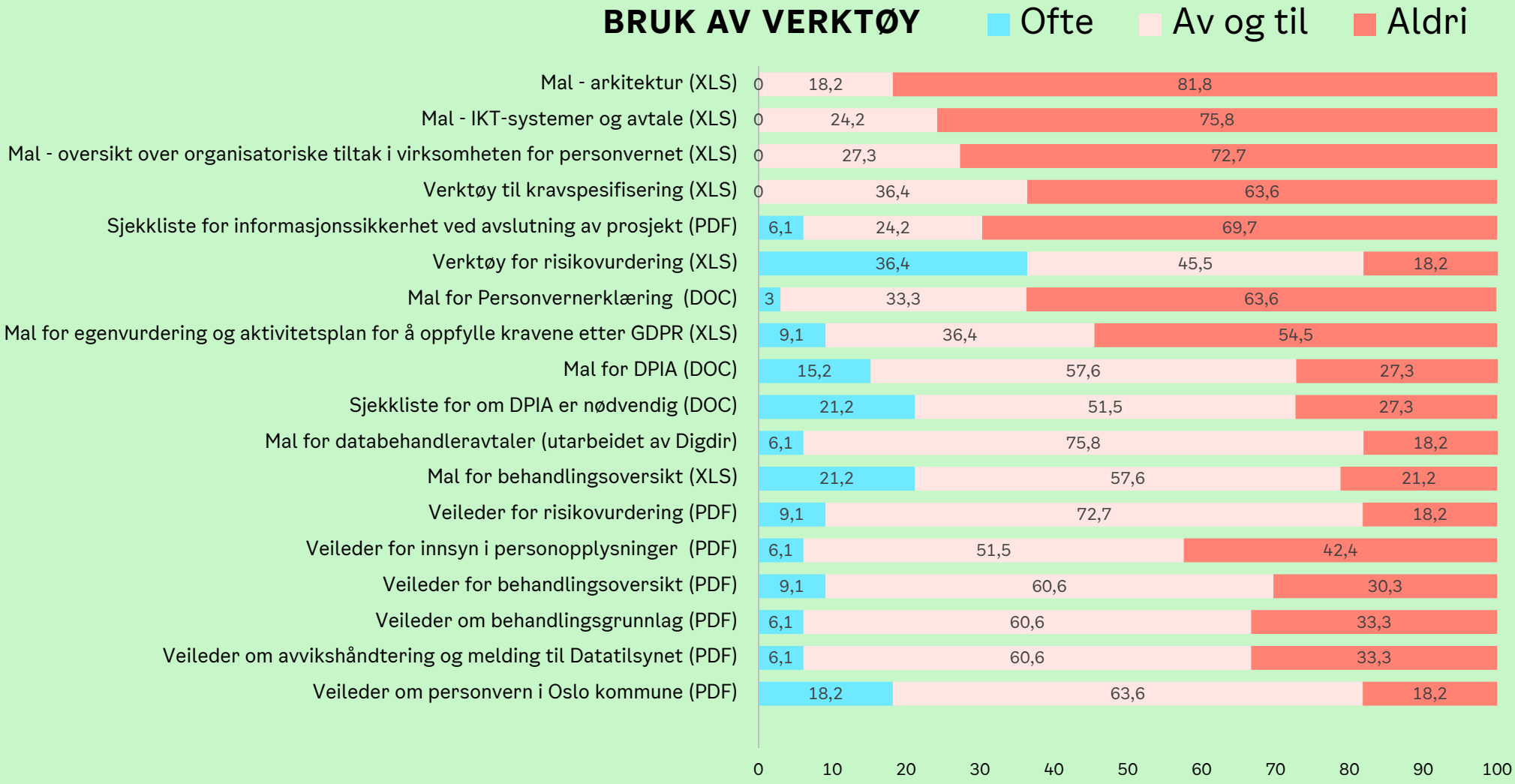
- Vedlikeholder egen kompetanse
- Mer kompetanse gjør at de ser tydeligere hva de ikke ivaretar av oppgaver
- Flere ønsker seg/trenger en kontrollerende funksjon
- Så å si alle er med på rapporteringsprosessen (LG/VE)
- Opplever generelt underrapportering av hendelser
- Jevnt over er det høy deltakelse i arbeidsprosesser.
- Tendensen vi ser er at deltakelsen er lavere på informasjonssikkerhetsbrudd, beredskap, oppfølging av rutiner. Så egentlig aktiviteter som handler om internkontroll.

Ja = 2
I noen grad = 1
Nei = 0



Oslo

BRUK AV VERKTØY



«Jeg kan ikke si at jeg kjenner til alle disse verktøyene. Usikker på om jeg har haket av riktig, da jeg kjenner igjen tema men ikke nødvendigvis med den tittelen. Ikke alt som er tilgjengelig heller, men som jeg har mottatt på epost fra andre som også som omhandler samme tema men usikker på om det er en av de nevnte over.»

DPIA-verktøy:

DPIA verktøy
Egen mal for DPIA i regi av BLK
Datatilsynets veileder for DPIA

Behandlingsprotokoll

Egen mal for system- og behandlingsoversikt, basert på sentral mal fra mange år tilbake, fordi Kartoteket var for lite oversiktlig og brukervennlig.

Andre kilder som nevnes:

Datatilsynet
Rettsdata
Filmer fra KINS
Digdir
NSM
ISF
Lærebøker i GDPR
Eksterne konsulenter

ROS-verktøy:

Andre maler for ROS-analyse

Egen mal for ROS, for å passe inn i vårt kvalitetssystem sin risikomodul (TKL), og for å forenkle prosessen for alskens småsystemer.

VERKTØY

«Ellers søker jeg en del på internett for å få tips og råd om hva andre har gjort og se på deres maler om det er noen jeg ser jeg kan benytte til vår virksomhet (gjerne fra statlige og kommunale virksomheter). Jeg har også fått maler fra andre virksomheter i kommunen som jeg har benyttet meg av.

Spesifikke maler:

Veileder om kontroll og overvåking i arbeidslivet 2019- Datatilsynet

Taushetserklæring for Oslo kommune (ansatte og innleide)

"Mal-intern kontroll GDPR-utviklet av undertegnede for UBF

Mal- risiko og mulighetsvurdering (oppside og nedside) - utviklet av undertegnede i samarbeid med Prosjektavdelingen for UBF«

Beredskapsplan informasjonssikkerhet

Egen sjekkliste ved endring av anlegg og system, brannmurer

Egen brukerinnmeldingsskjema

Egen risiko akseptmatrise, da risikoaksept er lik for konsekvenser forårsaket av informasjonssikkethetsbrudd, som for andre årsaker.

Eget ISMS dokument, basert på rådgivning fra Mnemonic, basert på ISO27001.

Egen egenvurdering/samsvarsvurdering ISO27001

Egen for ledelsens overordnede verdivurdering, basert på mal fra Mnemonic (15-20 overordnede tema).

Sikkerhetsregler - laget selv, basert på rådgivning fra Mnemonic for noen år siden

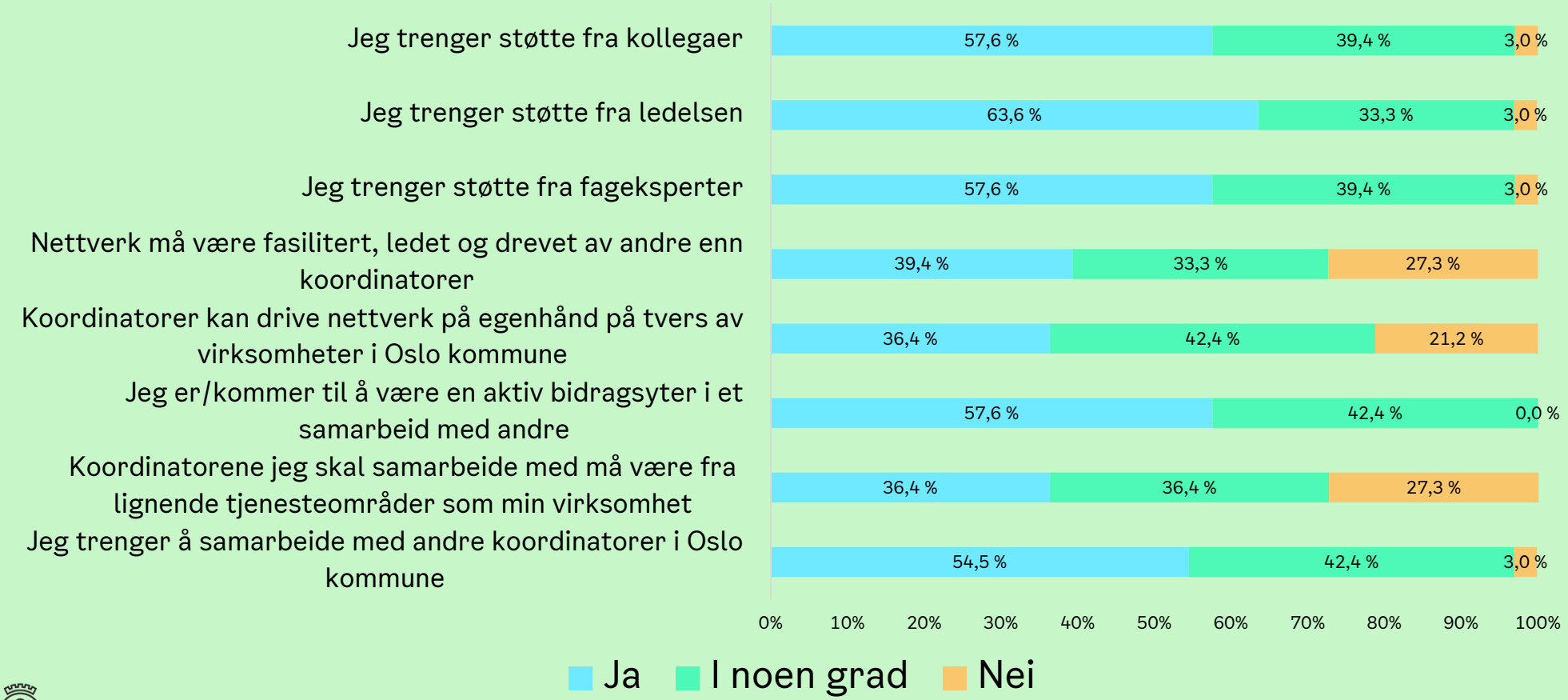
Etter at ISI ble opprettet og det kom nye koster til, ble det nevnt mal for DPIA som lå på internett og som var utarbeidet av en av de nyansatte. Denne har vi brukt internt for å se om den var bedre enn Oslo kommune sin.

Mal for databehandleravtale er henvist til mal på internett utarbeidet av direktoratet etter at Oslo kommune bestemte seg for å ikke ha egen mal. Da benytter vi den det er henvist til og ikke Oslo kommune sin som vi benyttet i begynnelsen.

Samarbeid, nettverk og støtte

«Synes nettverksmøtene er veldig fine, det er en fin arena for å dele. Problemstillingene gjelder jo alle.»

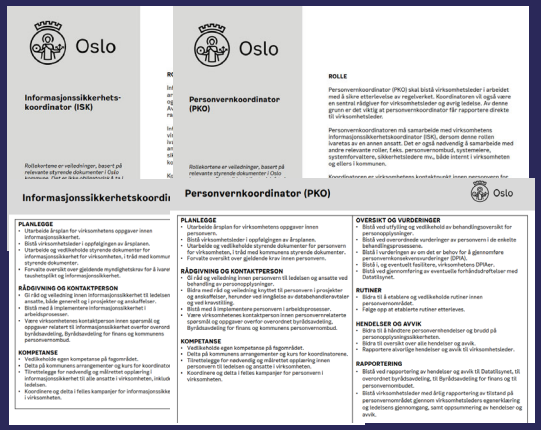
«Lærte masse da ressursperson fra FIN kom og risikovurderte med oss.»



Oppsummering av innsiktarbeidet

- Ulike behov for nye koordinatorer og blant de som har vært der en stund.
- Topplederne er ikke koblet på arbeidet
- Koordinatorrollen er ikke en fulltidsstilling
- Positive tilbakemeldinger på forum og nettverk – trenger mer av dette!
- Ønsker mer rådgivning fra ISI
- Sterkt ønske om at det som kan standardiseres, blir standardisert.
- Sterkt ønske om flere maler og verktøy
- Behov for høyere kompetanse hos lederne (Kommer fra ledere og koordinatorer)
- Tror at LG/VE-rapporteringen havner i et sort hull
- Informasjonssikkerhet og personvern er ikke en del av styringsdialogen (etterspør fokus på dette)
- Flere sier at de ikke har tatt rollekortene ordentlig i bruk

...vi fant et gap


Oslo

Informasjonssikkerhets-koordinator (ISK)

Rollekortene er veiledninger, basert på relevante styrende dokumenter i Oslo

Oslo

Personvernkoordinator (PKO)

Rollekortene er veiledninger, basert på relevante styrende dokumenter i Oslo

ROLLE

Personvernkoordinator (PKO) skal bistå virksomhetsleder i arbeidet med å sikre etterlevelse av regelverket. Koordinatoren vil også være en sentral rådgiver for virksomhetsleder og øvrig ledelse. Av denne grunn er det viktig at personvernkoordinator får rapportere direkte til virksomhetsleder.

Personvernkoordinatoren må samarbeide med virksomhetens informasjonssikkerhetskoordinator (ISK), dersom denne rollen ivaretas av en annen ansatt. Det er også nødvendig å samarbeide med andre relevante roller, f.eks. personvernombud, systemeiere, systemforvaltere, sikkerhetsledere mv., både internt i virksomheten og ellers i kommunen.

Informasjonssikkerhetskoordi

Personvernkoordinator (PKO)

Oslo

PLANLEGGE

- Utarbeide årsplan for virksomhetens oppgaver innen informasjonssikkerhet.
- Bistå virksomhetsleder i oppfølgingen av årsplanen.
- Utarbeide og vedlikeholde styrende dokumenter for informasjonssikkerhet for virksomheten, i tråd med kommune styrende dokumenter.
- Forvalte oversikt over gjeldende myndighetskrav for å ivare taushetsplikt og informasjonssikkerhet.

RÅDGIVNING OG KONTAKTPERSON

- Gi råd og veiledning innen informasjonssikkerhet til ledelsen ansatte, både generelt og i prosjekter og anskaffelser.
- Bistå med å implementere informasjonssikkerhet i arbeidsprosesser.
- Være virksomhetens kontaktperson innen spørsmål og oppgaver relatert til informasjonssikkerhet overfor overord Byrådsavdeling, Byrådsavdeling for finans og kommunens personvernombud.

KOMPETANSE

- Vedlikeholde egen kompetanse på fagområdet.
- Delta på kommunens arrangementer og kurs for koordinatorene.
- Tilrettelegge for nødvendig og målrettet opplæring innen informasjonssikkerhet til alle ansatte i virksomheten, inklud ledelsen.
- Koordinere og delta i felles kampanjer for informasjonssikke i virksomheten.

PLANLEGGE

- Utarbeide årsplan for virksomhetens oppgaver innen personvern.
- Bistå virksomhetsleder i oppfølgingen av årsplanen.
- Utarbeide og vedlikeholde styrende dokumenter for personvern for virksomheten, i tråd med kommunens styrende dokumenter.
- Forvalte oversikt over gjeldende krav innen personvern.

RÅDGIVNING OG KONTAKTPERSON

- Gi råd og veiledning knyttet til personvern i prosjekter og anskaffelser, herunder ved inngåelse av databehandleravtaler og ved kravstilling.
- Bistå med å implementere personvern i arbeidsprosesser.
- Være virksomhetenes kontaktperson innen personvernrelaterte spørsmål og oppgaver overfor overordnet byrådsavdeling, Byrådsavdeling for finans og kommunens personvernombud.

KOMPETANSE

- Vedlikeholde egen kompetanse på fagområdet.
- Delta på kommunens arrangementer og kurs for koordinatorene.
- Tilrettelegge for nødvendig og målrettet opplæring innen personvern til ledelsen og ansatte i virksomheten.
- Koordinere og delta i felles kampanjer for personvern i virksomheten.

OVERSIKT OG VURDERINGER

- Bistå ved utførling og vedlikehold av behandlingsoversikt for personopplysninger.
- Bistå ved overordnede vurderinger av personvern i de enkelte behandlingsprosessene.
- Bistå i vurderingen av om det er behov for å gjennomføre personvernkonsekvensvurderinger (DPIA).
- Bistå i, og eventuelt fasilitere, virksomhetens DPIAer.
- Bistå ved gjennomføring av eventuelle forhåndsdrøftelser med Datatilsynet.

RUTINER

- Bidra til å etablere og vedlikeholde rutiner innen personvernområdet.
- Følge opp at etablerte rutiner etterleves.

HENDELSER OG AVVIK

- Bidra til å håndtere personvernhendelser og brudd på personopplysningssikkerheten.
- Bidra til oversikt over alle hendelser og avvik.
- Rapportere alvorlige hendelser og avvik til virksomhetsleder.

RAPPORTERING

- Bistå ved rapportering av hendelser og avvik til Datatilsynet, til overordnet byrådsavdeling, til Byrådsavdeling for finans og til personvernombudet.
- Bistå virksomhetsleder med årlig rapportering av tilstand på personvernområdet gjennom virksomhetsleders egenerklæring og ledelsens gjennomgang, samt oppsummering av hendelser og avvik.

Oppdraget i rollekortet

Koordinatorenes ressurssituasjon og kompetanse

«Verdensbildet» –

informasjonssikkerhet og personvern

Ansatte

STØTTE FAGLIG

ISI

STØTTE FAGLIG

Kompetent koordinator

STØTTE FAGLIG

Ledere

STØTTE FAGLIG

STØTTE MED RESSURSER (TID OG KOMPETANSE)

STØTTE + GI MANDAT

RAPPORTERE

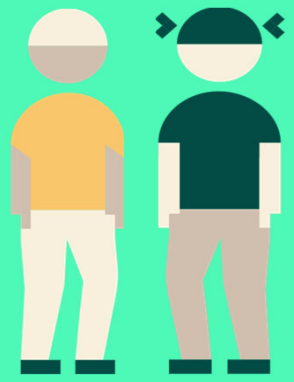
Virksomhets-leder

Byråds-avdeling (de som styrer)

STØTTE + STYRE

Oslo

Prinsipper for læringskonseptet



- Mulig for koordinator å gå ulike læringsstier – bygger opp modulært
- Stein på stein – utvikle over tid
- Praktisk, godt og relevant innhold
- Er skalerbart og kan lett tilpasses virksomheter på tvers
- Utforske nye læringsformer
- Pilotere læring sammen med dere

Avslutning

- Er du koordinator og har lyst til å svare på undersøkelsen, så blir vi superglade. :-D
  - https://response.questback.com/oslokommunebyrdsavd/cyok4ojkvy
- Det blir sendt ut en evaluering etter dette forumet som vi håper dere vil besvare.
  - https://response.questback.com/oslokommunebyrdsavd/suj40ebjxj
- Neste forum 23. mars – du kan melde deg på alle nå!
  - Se her: https://felles.intranett.oslo.kommune.no/informasjonssikkerhet-og-personvern/kompetanse/forum-for-informasjonssikkerhet-og-personvern/

Datoer for årets forum

26. januar
23. mars
8. juni
7. september
30. november

NSMs grunnprinsipper for IKT-sikkerhet

v 2.0

NASJONAL
SIKKERHETSMYNDIGHET

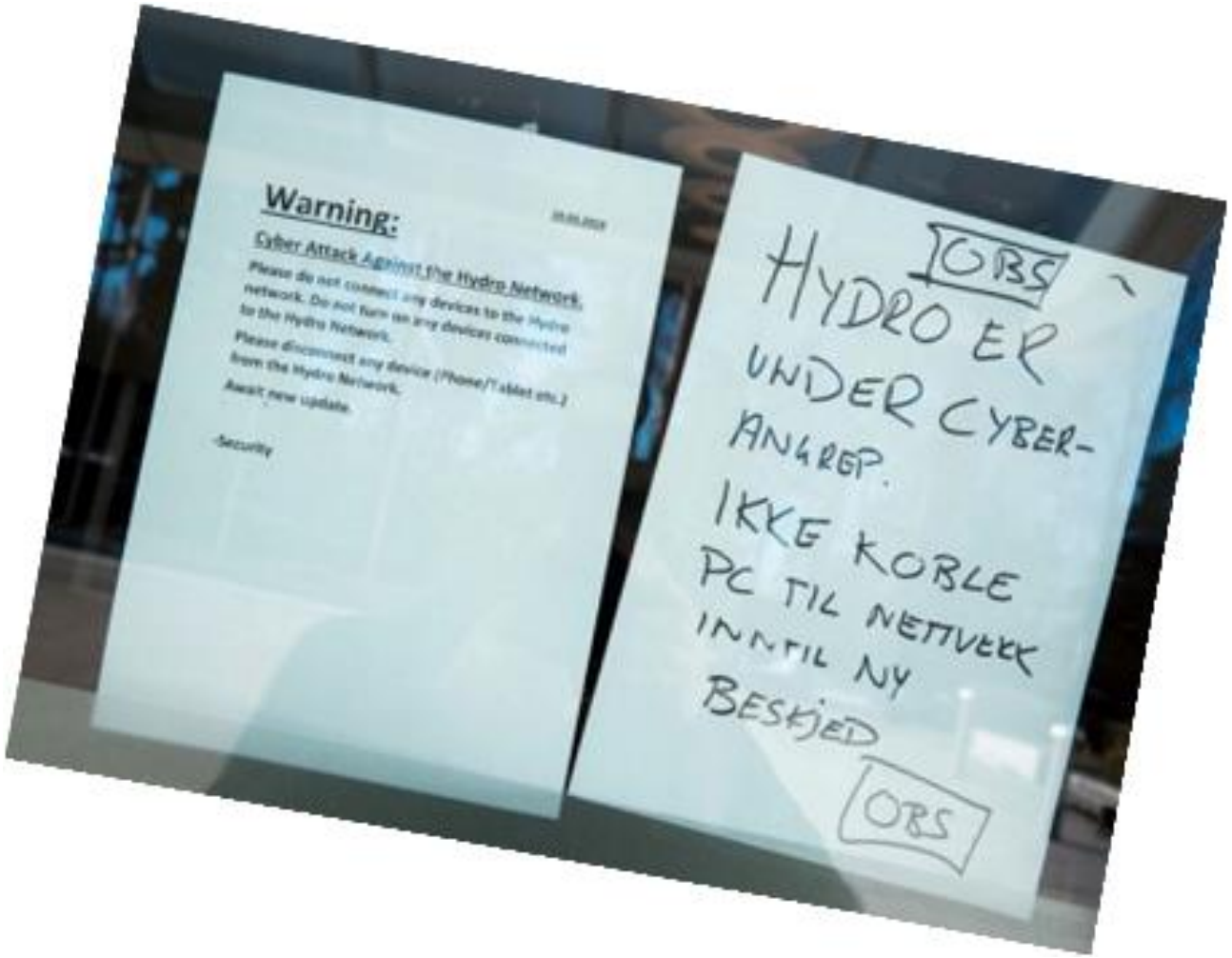
Are Søndenaa
Januar 2022

Innhold

- Introduksjon
  - Hvorfor trenger vi å tenke på sikkerhet?
  - Utfordringer for norske virksomheter
  - Utvikling av grunnprinsippene
  - Målgruppe – type virksomhet
- Oversikt og bruk av grunnprinsippene
  - Introduksjon til grunnprinsippene
  - Målgruppe – roller i virksomheten
  - Oversikt over grunnprinsippene
  - Oppbygning av hvert prinsipp
- Oppsummering og veien videre
  - Overordnet oppsummering av GP-IKT
  - Støtteprodukter
  - Prioritering av sikkerhetsarbeidet
  - Nyttige lenker

1 - Introduksjon

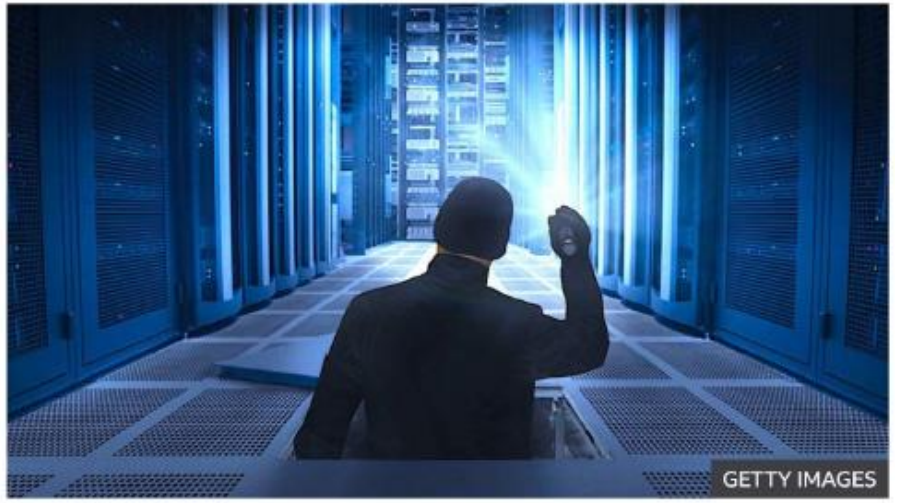
NASJONAL
SIKKERHETSMYNDIGHET



SolarWinds: Why the Sunburst hack is so serious

By Joe Tidy
Cyber reporter

16 December 2020



We've all seen the pop-ups on our laptops or phones: "Update is available, click here to download."

Østre Toten har vært uten datasystemer en måned etter hacking

ØSTRE TOTEN (NRK): PST mener dataangrep er en av de største truslene i 2021. I Østre Toten innrømmer ordføreren at sikkerheten ikke var god nok.

KREVENDE JOBB: Over 1000 PC-er måtte gjenopprettes i Østre Toten etter at noen tok seg inn bak brannmurene til kommunen, sletta alle sikkerhetskopier og krypterte alle data.
FOTO: ANDERS BAKKERUD LARSEN / NRK

Dag Kessel
Journalist

Knut Røsrud
Journalist

Publisert 8. feb. 2021 kl. 17:21
Oppdatert 8. feb. 2021 kl. 17:35

Østre Toten ble 9. januar offer for et stort dataangrep.

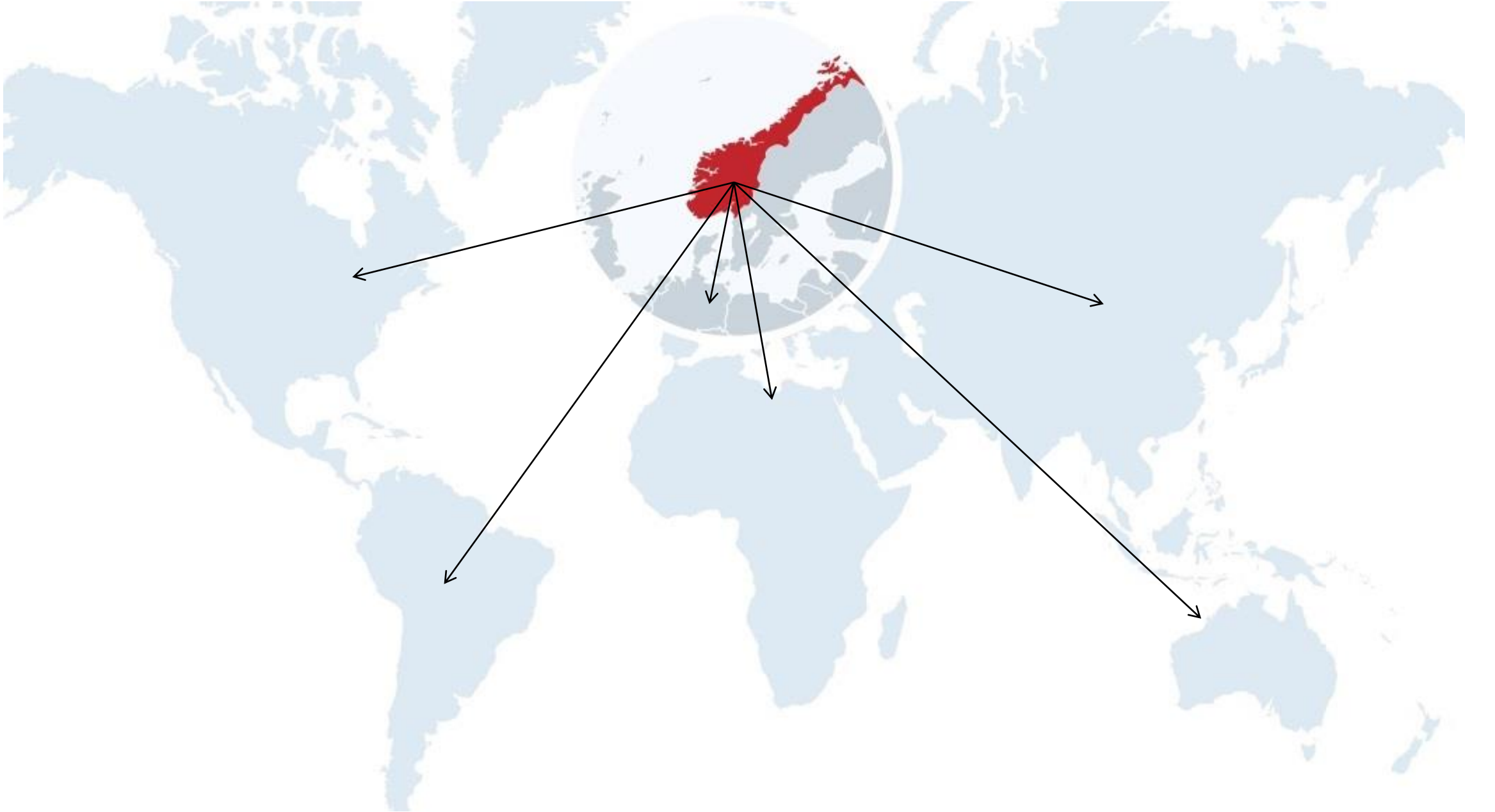
En erfaring fra kommunal sektor

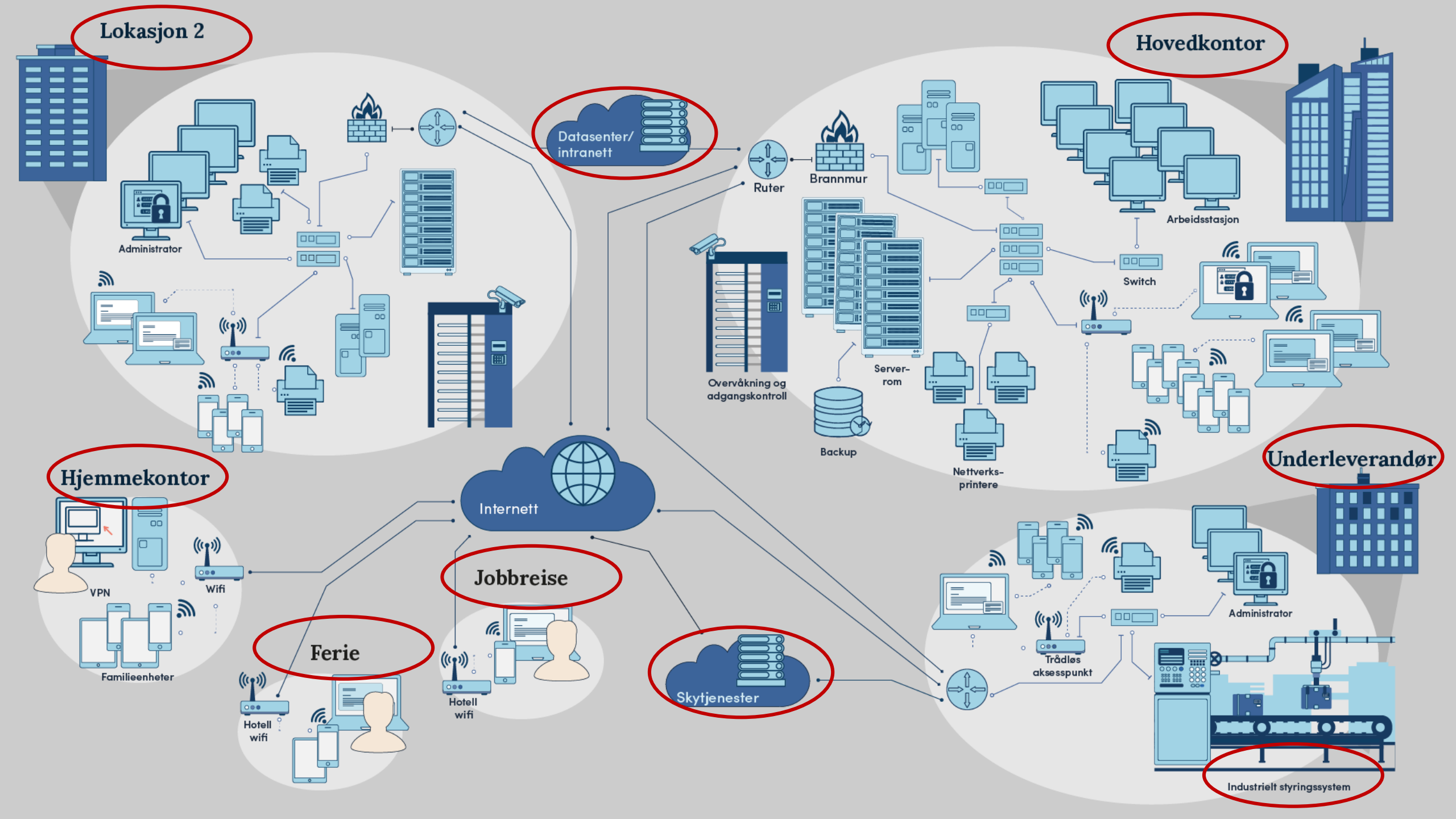
Østre Toten kommune ble i januar utsatt for et krypteringsvirus med krav om løsepenger som satte store deler av kommunens nettverk tilbake til manuell styring i lang tid. Kommunen melder om at enkelte systemer fortsatt er ute av drift et halvt år senere.

Kommune-CSIRT rapporterer[3] om at de lørdag 9. januar ble kontaktet av Østre Toten kommune som var rammet av et løsepengevirus med skadevaren PYSA. Hele den virtuelle serverparken til kommunen ble kryptert og låst ned. Også de internettbaserte sikkerhetskopiene ble kryptert og utilgjengeliggjort. Aktøren hadde også stjålet betydelige mengder data, og dobbel utpressing fremstod som et mulig scenario. Kommunens operative evne ble sterkt redusert da de aller fleste av kommunens digitale tjenester var nede. Situasjonen ble ytterligere forverret den 29. mars, da PYSA publiserte deler av dataene som var stjålet fra kommunen på det mørke nettet. Kommunen måtte håndtere sensitive personopplysninger på avveie, og informere og støtte personer som ble rammet.

På NSMs sikkerhetskonferanse 11. mars fortalte Østre Totens ordfører Bror Helgestad at hendelsen i praksis medførte at de eldres alarm-system på sykehjem ble erstattet med bjeller, låse-systemet på kommunens bygninger ikke fungerte, og at helsestasjonen for barn og unges journaler var utilgjengelige. Kommunen måtte operere manuelt i flere måneder uten fungerende IT-systemer.

Utfordringer for norske virksomheter




Lokasjon 2
Administrator
Datasenter/
intranett
Ruter
Brannmur
Hovedkontor
Arbeidsstasjon
Switch
Overvåkning og
adgangskontroll
Server-
rom
Backup
Nettverks-
printere
Hjemmekontor
VPN
Wifi
Familieenheter
Internett
Jobbreise
Hotell
wifi
Ferie
Hotell
wifi
Skytjenester
Underleverandør
Administrator
Trådløs
aksesspunkt
Industrielt styringssystem

Brukere

som ubevisst gjør feil

som bevisst bryter regler

Tilfeldige hendelser

server som kræsjer

Tilfeldige angrep

kryptovirus

Målrettede angrep

hackere

organiserte grupper eller statlige aktører

Utvikling av grunnprinsippene

NASJONAL
SIKKERHETSMYNDIGHET

Hvorfor lage Grunnprinsipper?

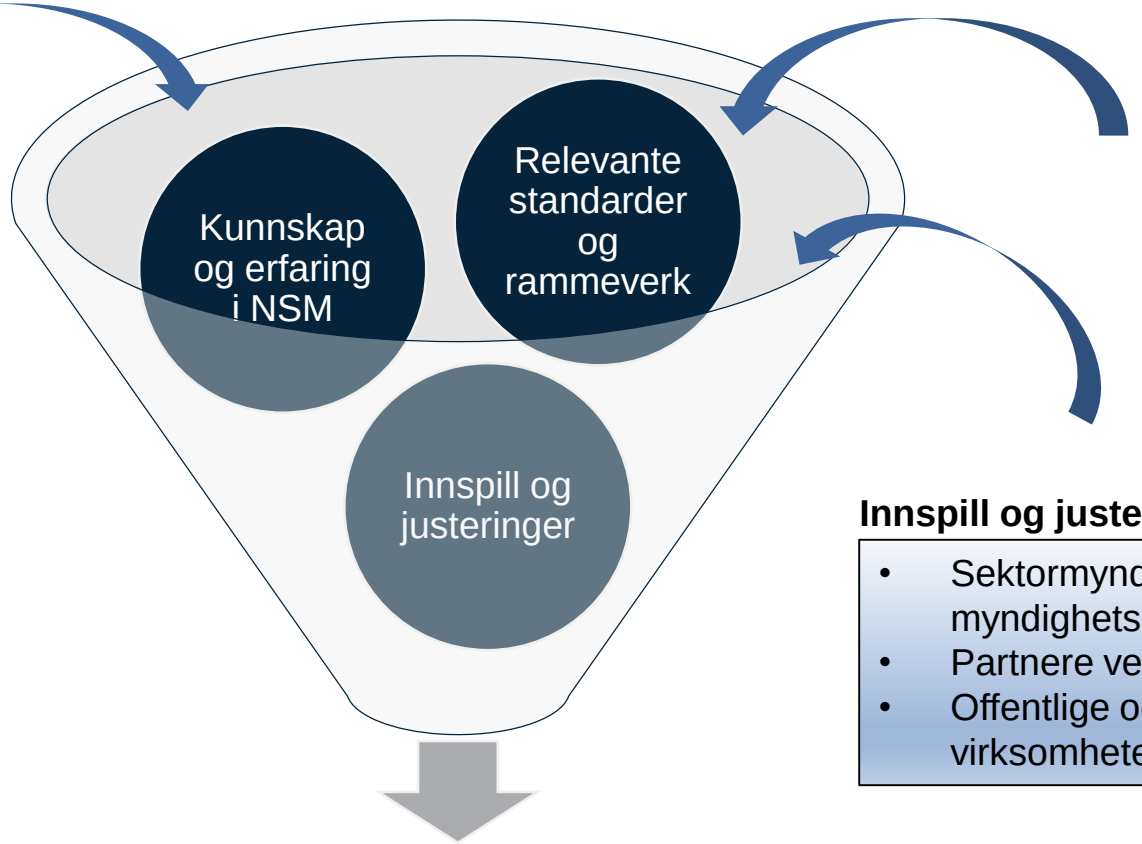
- Masse gode anbefalinger og rammeverk «out there» …
  - Hvorfor finne opp hjulet på nytt?
- Utfordringer med internasjonale rammeverk:
  - Ukjent for mange, noen krever pålogging/betaling, mye å sette seg inn i
  - Ikke alltid optimalt for Norske virksomheter
- Norge:
  - Lite land, små IT-avdelinger
  - Mindre hierarkisk, færre nivåer, mer delegert myndighet
  - Litt raskere til å kjøpe nyere teknologi

ACSC Australian Cyber Security Centre

Hvordan har grunnprinsippene blitt til?

Kunnskap og erfaringer NSM

- Rådgivning
- Hendelser (NCSC)
- Inntrengingstester
- Tilsyn
- Kravutvikling
- Samarbeidspartnere



Relevante standarder og rammeverk

- ISO 27002
- US NIST CSF
- CIS CSC 20
- UK NCSC CAF

Innspill og justeringer

- Sektormyndigheter og myndighetsorganer
- Partnere ved NCSC
- Offentlige og private virksomheter

NSMs Grunnprinsipper for IKT-sikkerhet

Målgruppe – type virksomhet

Målgruppe for Grunnprinsipper-IKT

Alle offentlige og private virksomheter

Kritiske samfunnsfunksjoner

Styringsevne og suverenitet

- Styring og kriseledelse
- Forsvar

Befolkningens sikkerhet

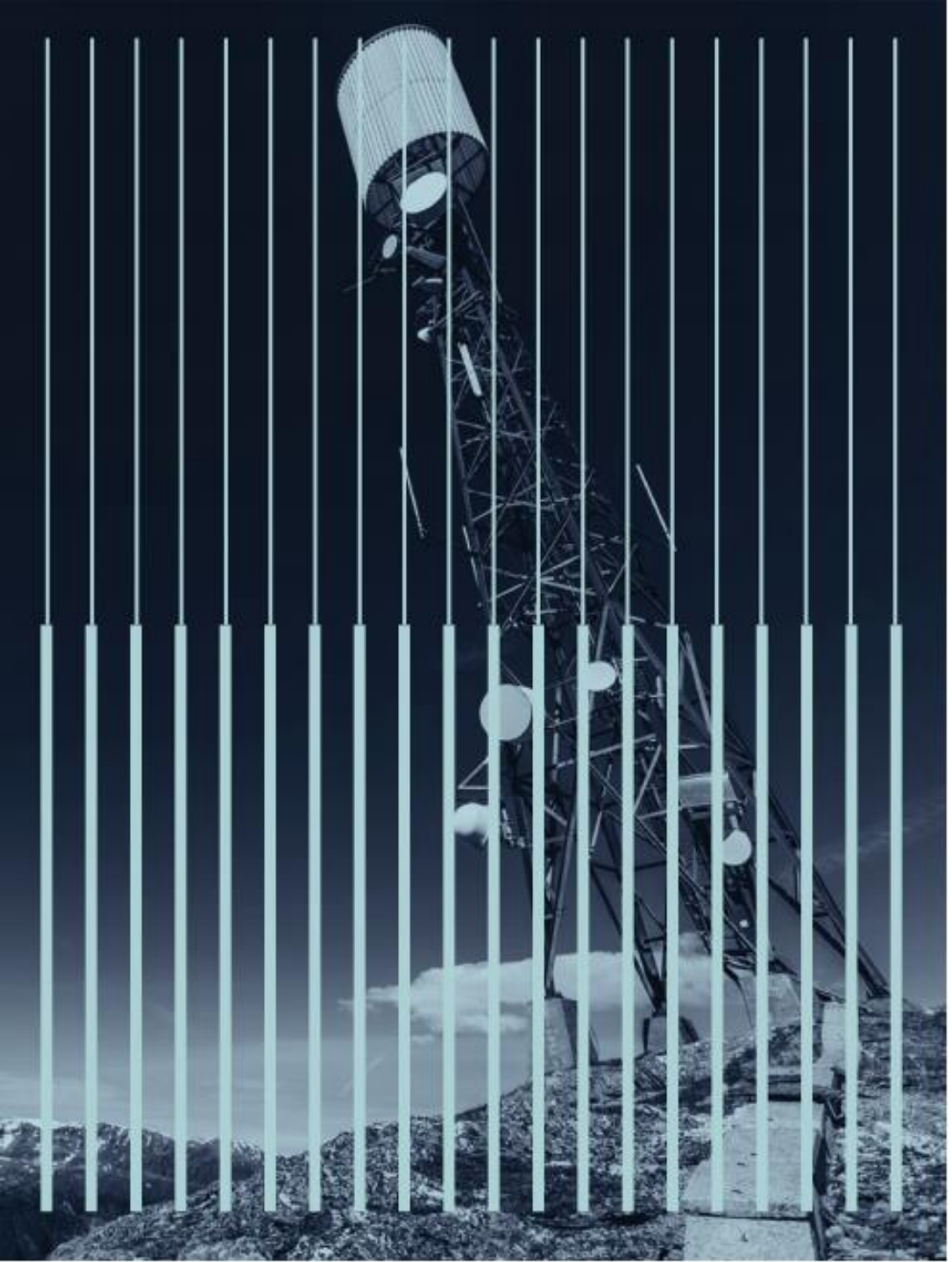
- Lov og orden
- Helse og omsorg
- Redningstjeneste
- IKT-sikkerhet i sivil sektor
- Natur og miljø

Samfunnets funksjonalitet

- Forsyningssikkerhet
- Vann og avløp
- Finansielle tjenester
- Kraftforsyning
- Elektroniske kommunikasjonsnett- og tjenester
- Transport
- Satellittbaserte tjenester

2 - Oversikt og bruk av grunnprinsippene

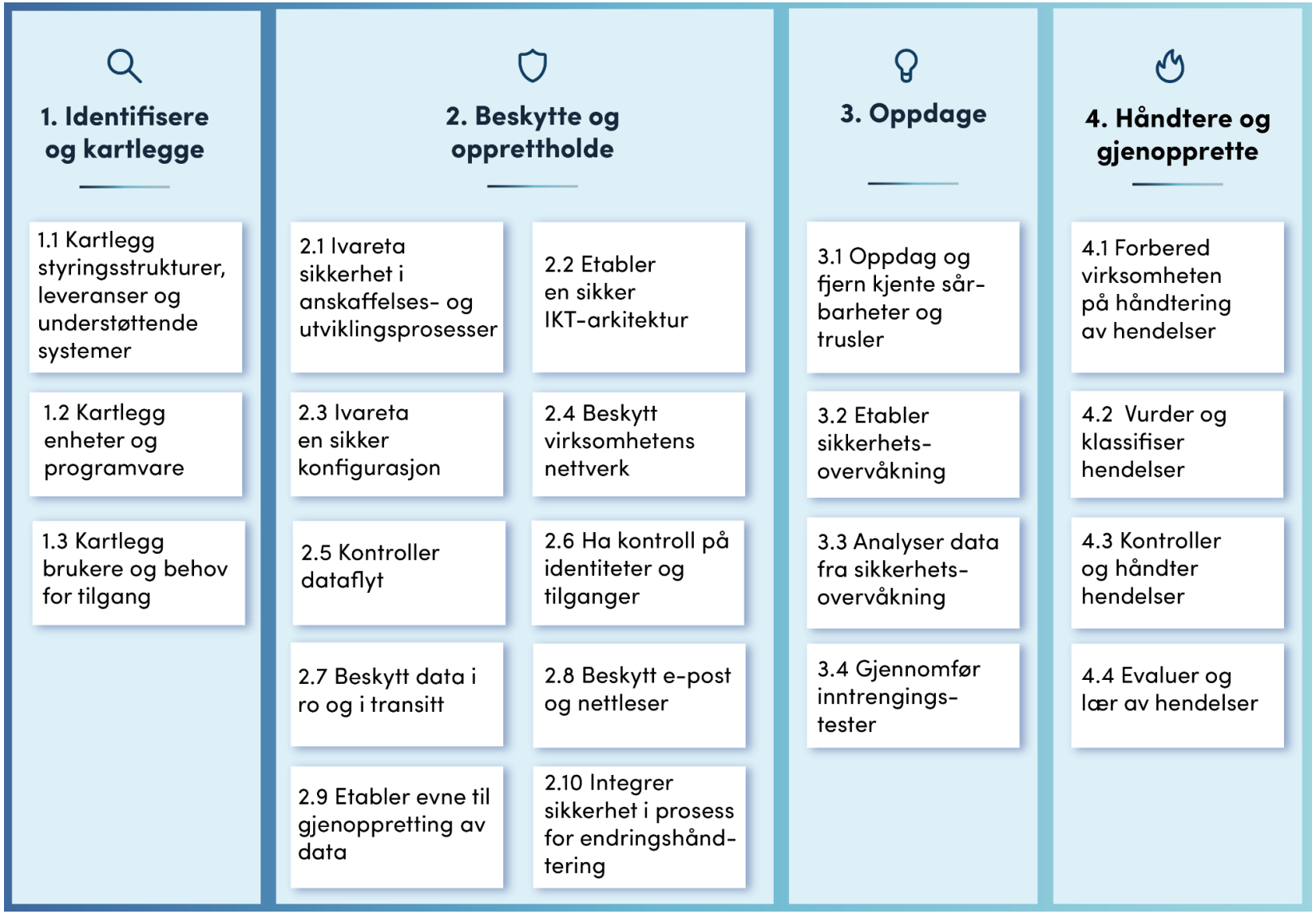
NASJONAL
SIKKERHETSMYNDIGHET



Grunnprinsipper for IKT-sikkerhet

- Identifisere og kartlegge
- Beskytte og opprettholde
- Oppdage
- Håndtere og gjenopprette

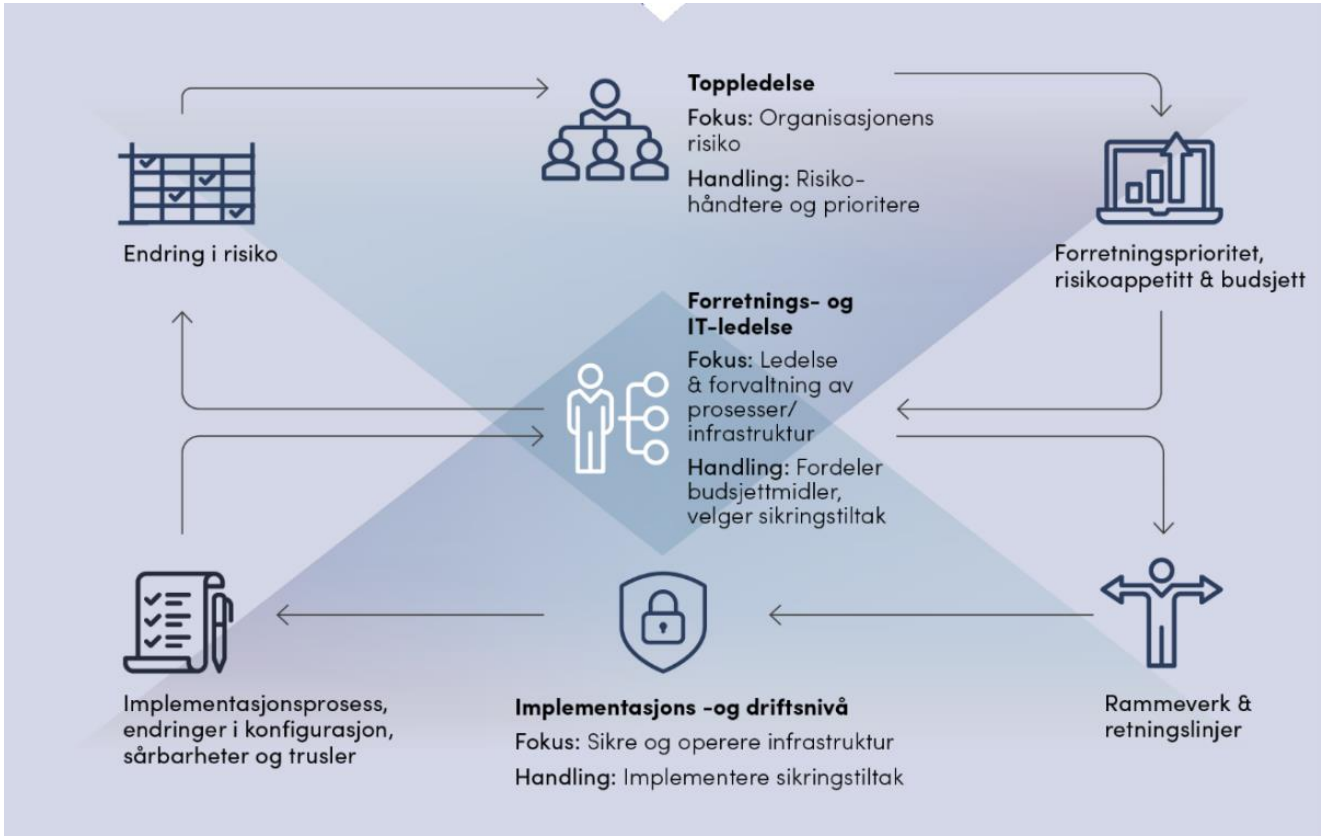
NSMs grunnprinsipper for IKT-sikkerhet (v 2.0)



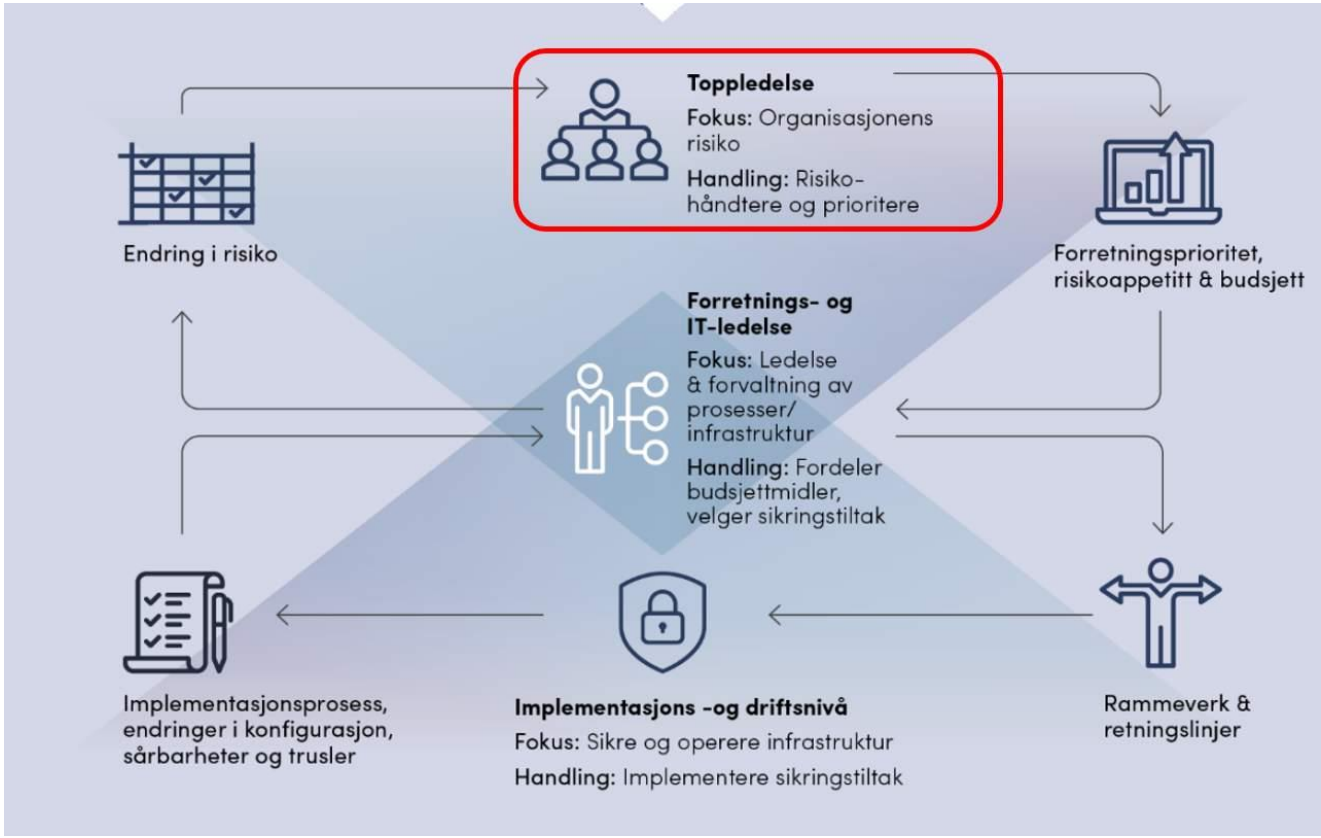
Målgruppe - roller i virksomheten

NASJONAL SIKKERHETSMYNDIGHET

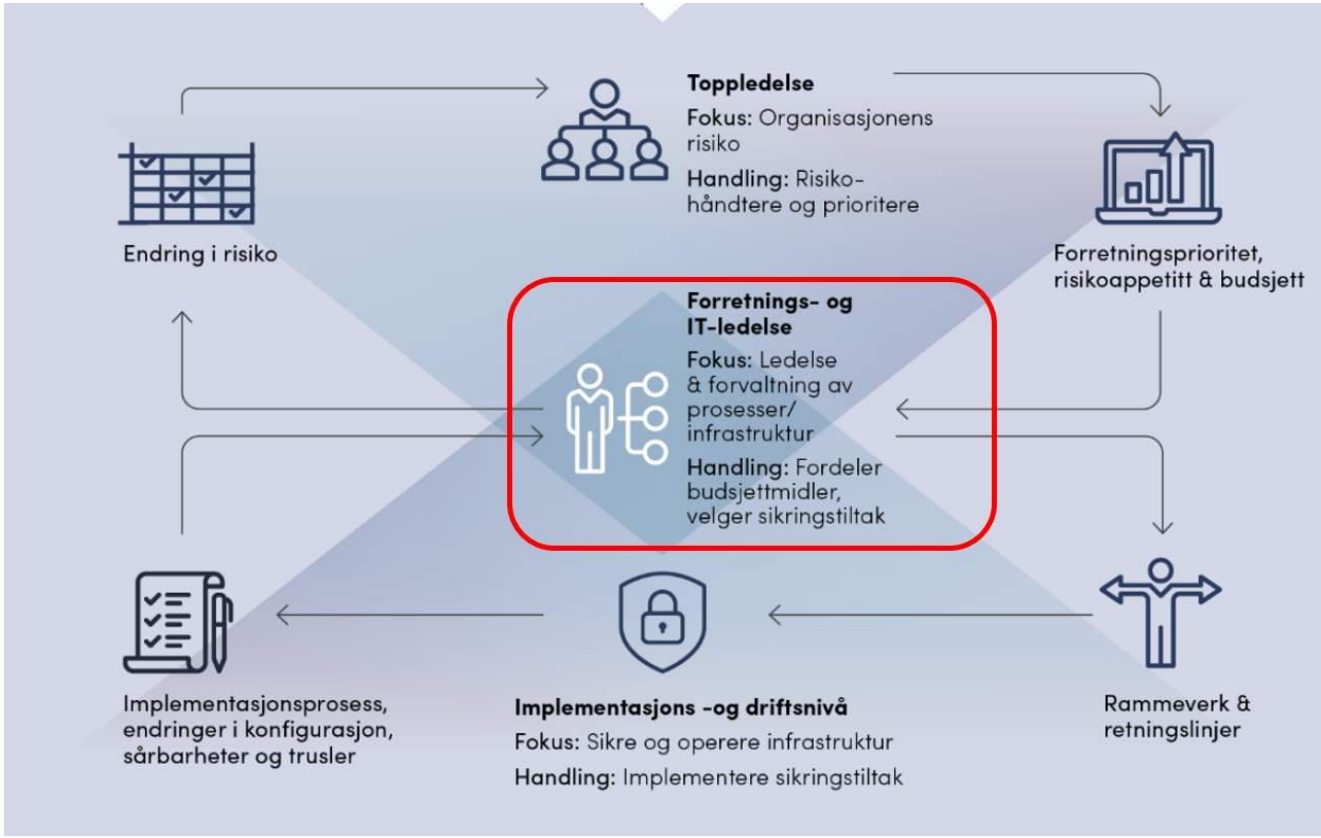
Hvordan kan de ulike rollene i virksomheten benytte grunnprinsippene?



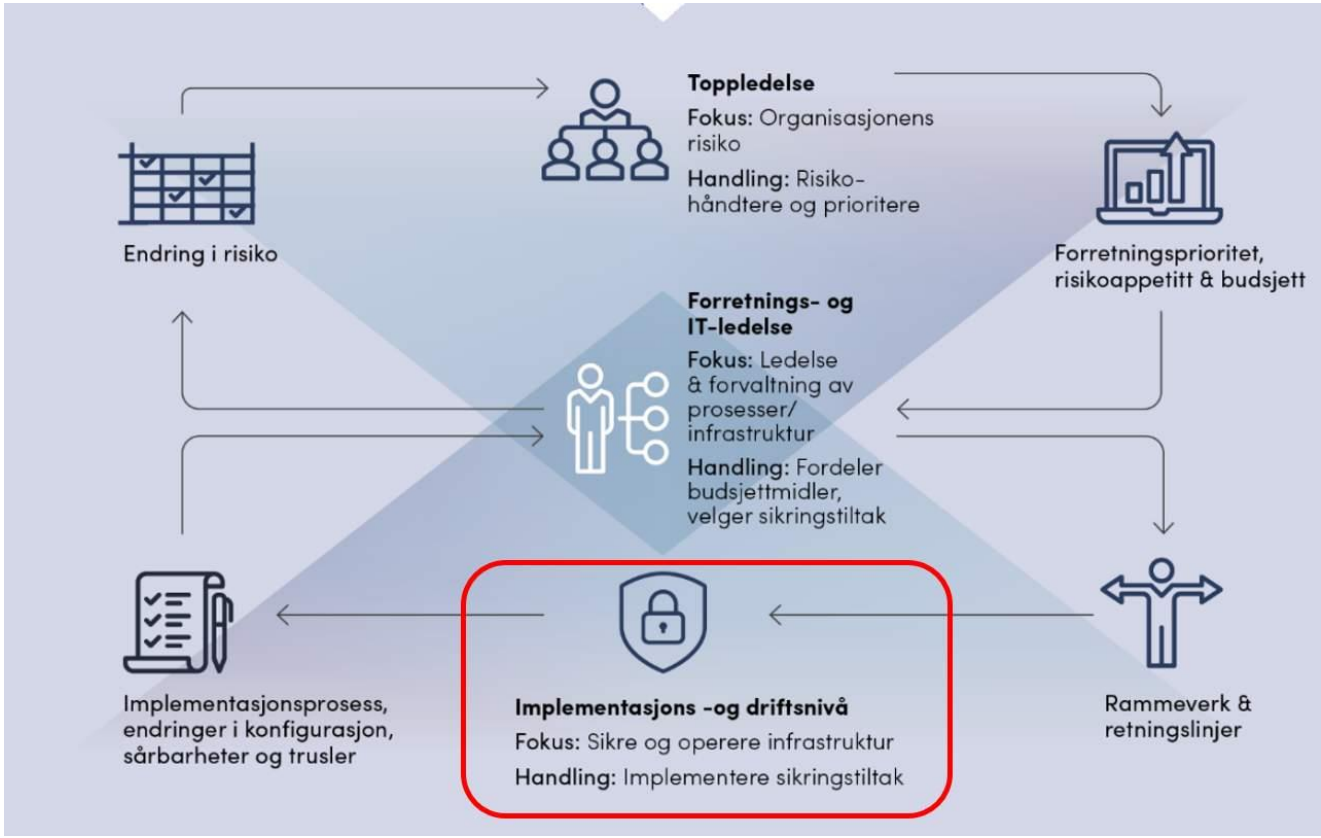
Toppledelse



Forretnings- og IT-ledelse



Implementasjons- og driftsnivå

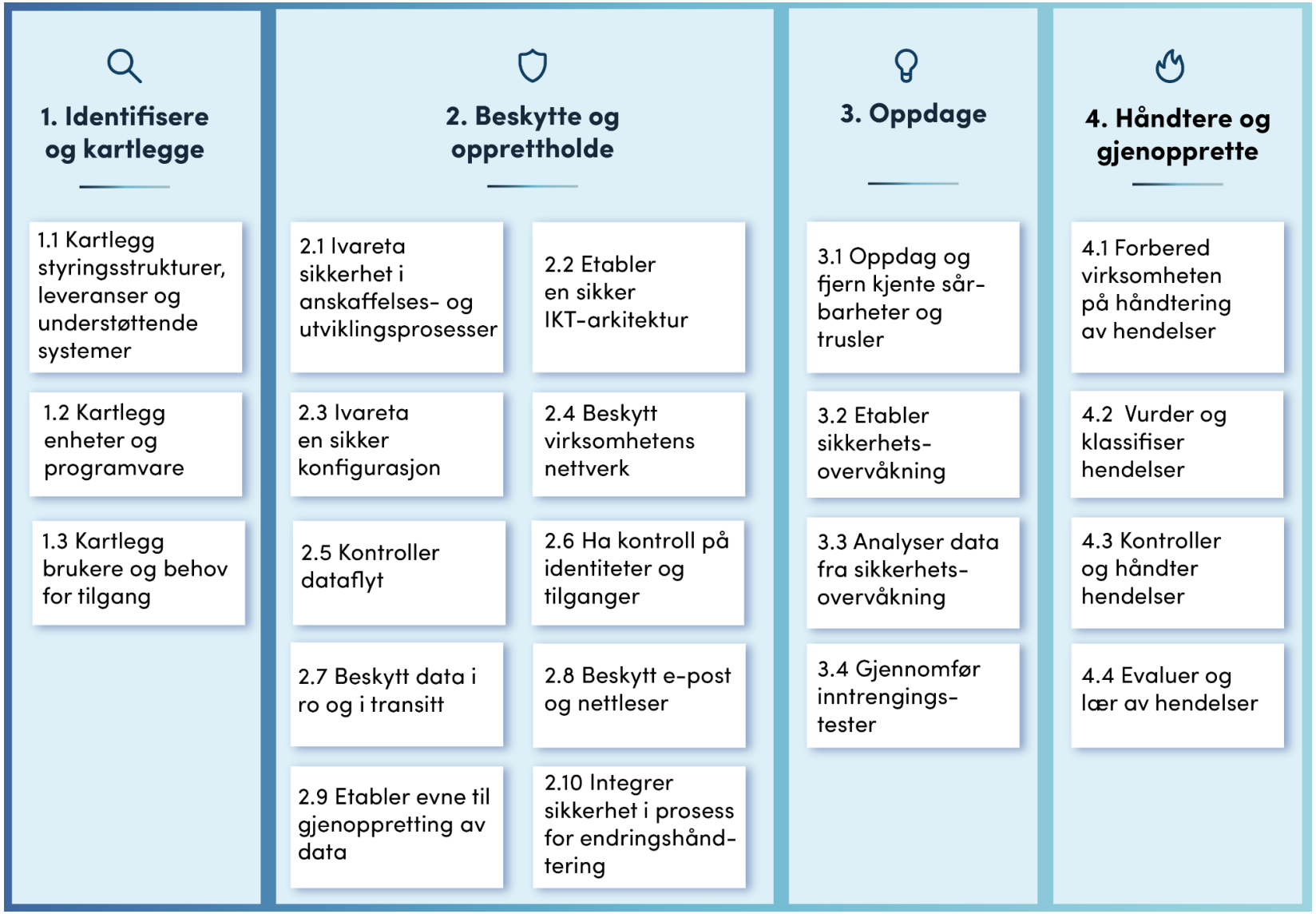


Oppsummering

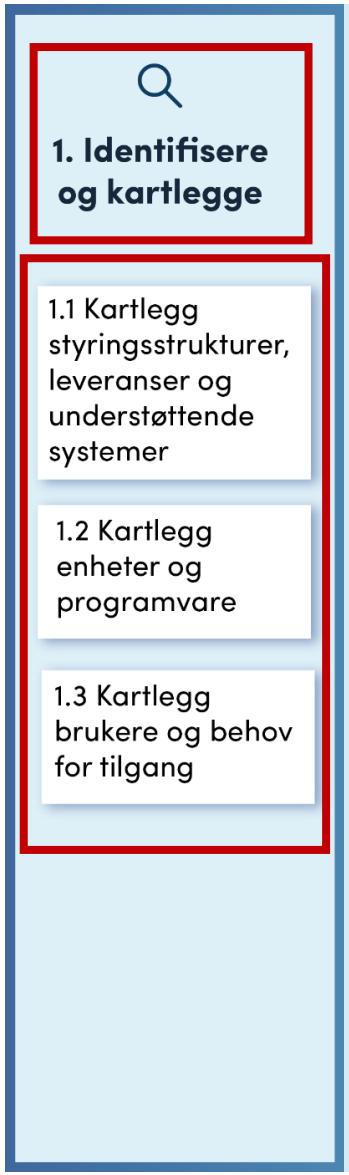
Roller	Relevante deler av grunnprinsippene
Toppledere	Lese de 3 første sidene i innledningen. («Introduksjon», «Hvem er målgruppen» og «Hva er NSMs grunnprinsipper for IKT-sikkerhet»
Avdelingsledere (ansvarlige for prosess- eller forretningsområder)	Innledningen og i tillegg bidra med kompetanse og innspill inn i kategori 1 når denne gjennomføres.
IT-ledere	Innledningen, alle prinsippene med fokus på «Målet med prinsippet» og «Hvorfor dette er viktig?»
IT- og sikkerhetseksperter og IT-drift	Hele NSMs grunnprinsipper for IKT-sikkerhet

Oversikt over grunnprinsippene

NSMs grunnprinsipper for IKT-sikkerhet (v 2.0)



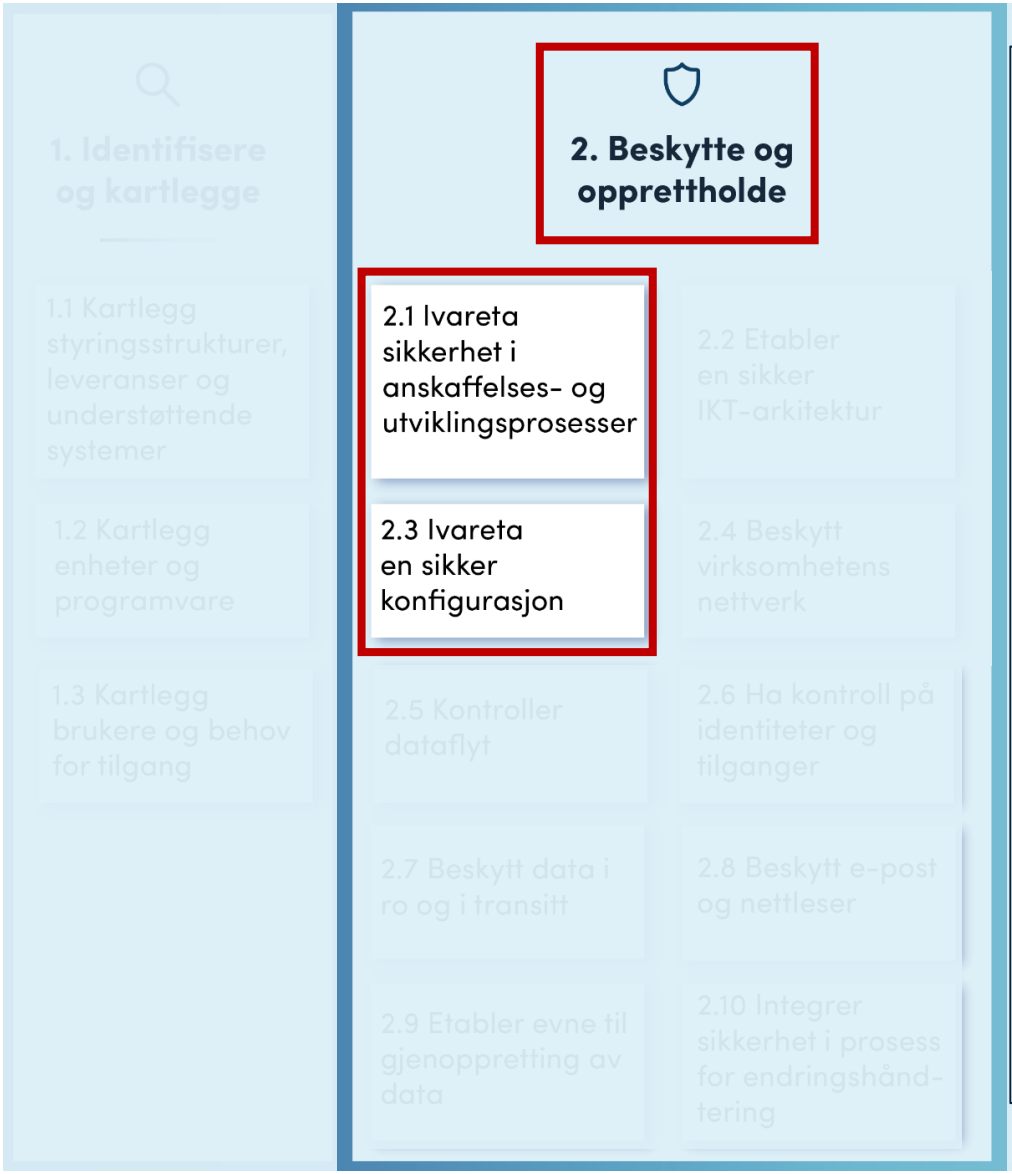
Kategori 1 – Identifisere og kartlegge



Vanskelig å sikre noe uten at man vet:

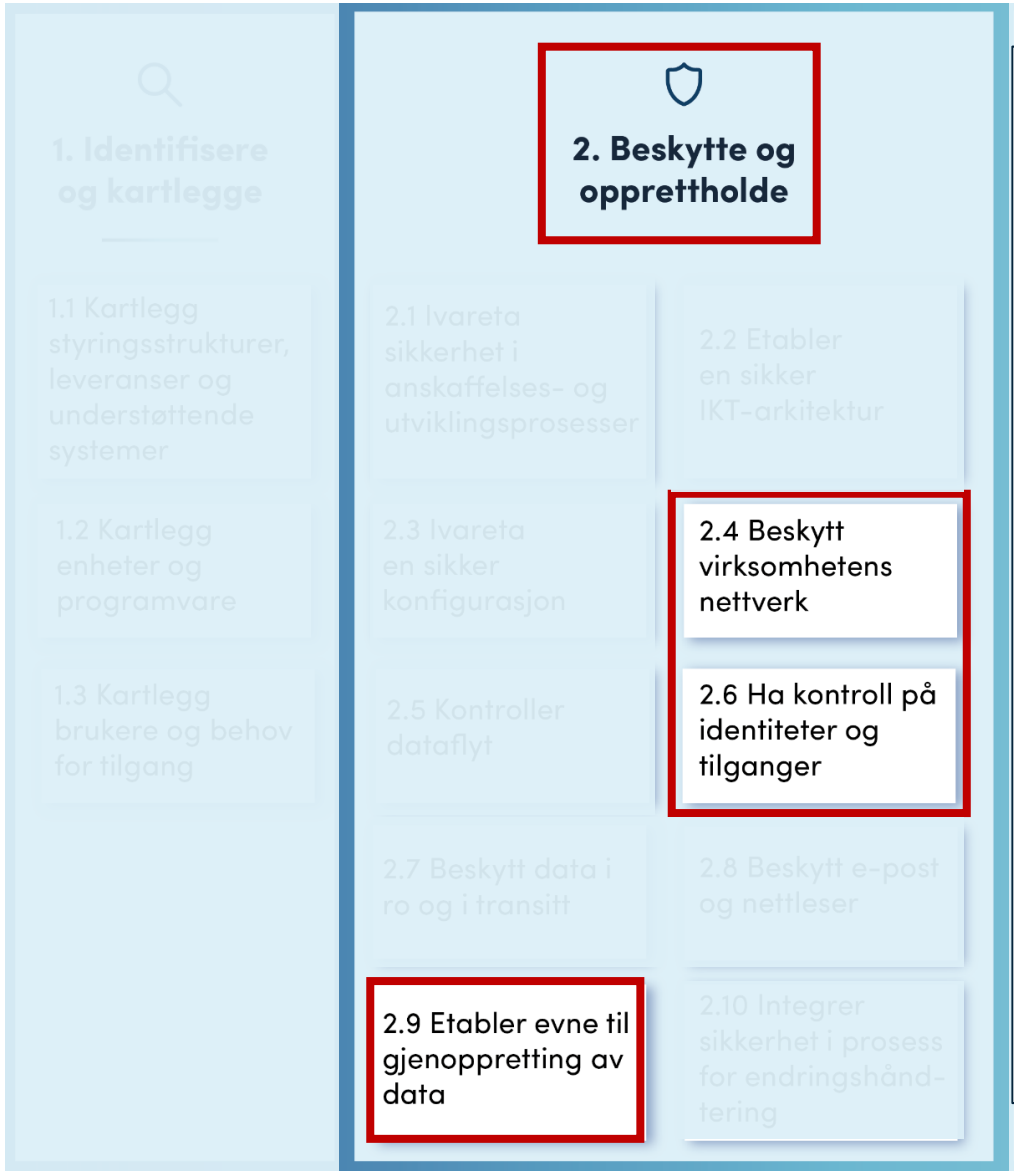
- Hva er det man skal sikre, hvorfor er det viktig for virksomheten
- Hva benyttes av programvare og enheter
- Hvem brukerne er og deres behov

Kategori 2 – Beskytte og opprettholde



- Sikkert kjøp
  - Sikkerhet angår ikke bare sikkerhetsprodukter!
  - Fas ut eldre IKT-produkter
  - Virtualisering og “sky”
- Sikkerhetskonfigurasjon
  - sentralt styrt regime for sikkerhetsoppdatering
  - klienter slik at kun kjent programvare kjører på dem

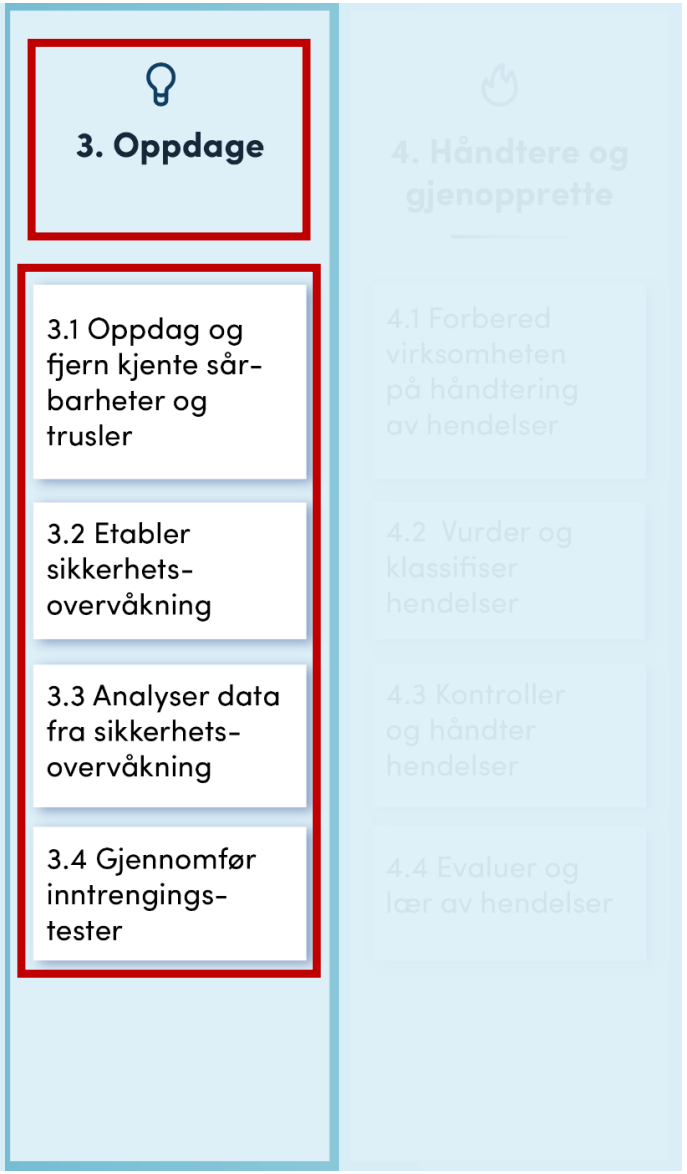
Kategori 2 – Beskytte og opprettholde (forts.)



- Nettverk
  - Etabler tilgangskontroll på flest mulige nettverksporter
  - Krypter alle trådløse og kablede forbindelse
- Identiteter og tilganger
  - Gi ansatte kun de rettighetene de trenger
  - Driftskontoer: ikke alle egg i en kurv …
- Backup
  - Lag en plan
  - Test plan og sikkerhetskopi

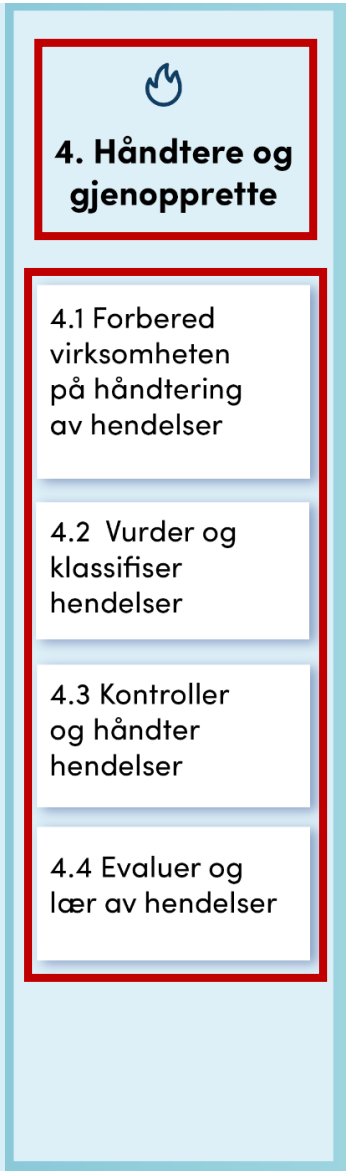
Kategori 3 – Oppdage

- Oppdage trusler og sårbarheter
  - Jevnlig sårbarhetskartlegging, helst automatiserte verktøy
- Etabler sikkerhetsovervåkning
  - Beslutt hvilke data som er sikkerhetsrelevant
  - Verifiser at innsamling fungerer
  - Analyser data fra sikkerhetsovervåkning
- Inntrengningstester



Kategori 4 - Håndtere og gjenopprette

- Forbered virksomheten på håndtering av hendelser
  - Plan!
  - Øve!
- Håndter hendelser når de inntreffer
- Lær av hendelsen



Oppbygning av hvert prinsipp

Grunnprinsippet (overskriften)
- et anbefalt prinsipp som virksomheter bør følge

2.3. Ivareta en sikker konfigurasjon

Målet med prinsippet: Virksomheten konfigurerer og tilpasser maskin- og programvare slik at det tilfredsstiller virksomhetens behov for sikkerhet. Det er etablert rutiner for sporing, rapportering og korrigering av sikkerhetskonfigurasjon på enheter, programvare og tjenester for å hindre angripere i å utnytte disse.

Hvorfor er dette viktig?

De fleste IKT-produkter leveres med en standardkonfigurasjon utviklet av produsent eller forhandler. Disse konfigurasjonene er vanligvis utviklet for å forenkle installasjon eller bruk, ikke for å tilby god sikkerhet. *Åpne tjenester og porter, standardkontoer og passord, eldre (og ofte sårbare) protokoller og forhåndsinstallert programvare kan gi en angriper en rekke muligheter til å oppnå uautorisert tilgang. Systemer som ikke er eksplisitt konfigurert har mest sannsynlig sårbarheter som en angriper kan utnytte.* Virksomheter må derfor herde IKT-produktene, eksempelvis ved å ta bort funksjonalitet det ikke er tjenstlig behov for samt fjerne standard-innstillinger og passord.

Anbefalte tiltak: Ivareta en sikker konfigurasjon

2.3.1	**Etabler et sentralt styrt regime for sikkerhetsoppdatering.** Installer sikkerhetsoppdateringer så fort som mulig. **a)** Etabler en prioriteringsliste for oppdateringer. Operativsystem og applikasjoner på de ansattes klienter bør prioriteres. Videre bør man oppdatere servere som inneholder standard applikasjoner og operativsystem, programvaren i skrivere, samt enheter som styrer virksomhetens nettverk (svitsjer, rutere). **b)** Etabler en rutine med klare ansvarsforhold for *i)* hvor ofte oppdateringer skal utføres (mye bør kunne automatiseres) og *ii)* ansvarlig rolle for oppfølging hvis en oppdatering ikke kan gjennomføres eller må utsettes. **c)** Isoler servere og annet som oppleves som vanskelig å holde oppdatert, se 2.5.4. **d)** Virksomheter bør automatisere og forenkle prosessen for å implementere nye sikkerhetsoppdateringer.

Utdypende informasjon

Herding er en viktig del av den totale informasjonssikkerheten. Manglende herding av systemkomponenter er ofte en årsak til at angripere får fotfeste i virksomheten. *Operativsystemer på*

Lenker

[1] NSM - Sikring av Network Time Protocol (NTP): https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/U-09_Sikring_av_NTP.pdf

Målet med prinsippet

- beskriver hva man skal oppnå ved å innføre grunnprinsippet

2.3. Ivareta en sikker konfigurasjon

Målet med prinsippet: Virksomheten konfigurerer og tilpasser maskin- og programvare slik at det tilfredsstiller virksomhetens behov for sikkerhet. Det er etablert rutiner for sporing, rapportering og korrigering av sikkerhetskonfigurasjon på enheter, programvare og tjenester for å hindre angripere i å utnytte disse.

Hvorfor er dette viktig?

De fleste IKT-produkter leveres med en standardkonfigurasjon utviklet av produsent eller forhandler. Disse konfigurasjonene er vanligvis utviklet for å forenkle installasjon eller bruk, ikke for å tilby god sikkerhet. *Åpne tjenester og porter, standardkontoer og passord, eldre (og ofte sårbare) protokoller og forhåndsinstallert programvare kan gi en angriper en rekke muligheter til å oppnå uautorisert tilgang. Systemer som ikke er eksplisitt konfigurert har mest sannsynlig sårbarheter som en angriper kan utnytte.* Virksomheter må derfor herde IKT-produktene, eksempelvis ved å ta bort funksjonalitet det ikke er tjenstlig behov for samt fjerne standard-innstillinger og passord.

Anbefalte tiltak: Ivareta en sikker konfigurasjon

2.3.1	**Etabler et sentralt styrt regime for sikkerhetsoppdatering.** Installer sikkerhetsoppdateringer så fort som mulig. **a)** Etabler en prioriteringsliste for oppdateringer. Operativsystem og applikasjoner på de ansattes klienter bør prioriteres. Videre bør man oppdatere servere som inneholder standard applikasjoner og operativsystem, programvaren i skrivere, samt enheter som styrer virksomhetens nettverk (svitsjer, rutere). **b)** Etabler en rutine med klare ansvarsforhold for *i)* hvor ofte oppdateringer skal utføres (mye bør kunne automatiseres) og *ii)* ansvarlig rolle for oppfølging hvis en oppdatering ikke kan gjennomføres eller må utsettes. **c)** Isoler servere og annet som oppleves som vanskelig å holde oppdatert, se 2.5.4. **d)** Virksomheter bør automatisere og forenkle prosessen for å implementere nye sikkerhetsoppdateringer.

Utdypende informasjon

Herding er en viktig del av den totale informasjonssikkerheten. Manglende herding av systemkomponenter er ofte en årsak til at angripere får fotfeste i virksomheten. *Operativsystemer på*

Lenker

[1] NSM - Sikring av Network Time Protocol (NTP): https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk_sikkerhet/U-09_Sikring_av_NTP.pdf

Hvorfor er dette viktig?

- beskriver hvorfor grunnprinsippet er viktig og mulige konsekvenser dersom grunnprinsippet ikke blir implementert

2.3. Ivareta en sikker konfigurasjon

Målet med prinsippet: Virksomheten konfigurerer og tilpasser maskin- og programvare slik at det tilfredsstiller virksomhetens behov for sikkerhet. Det er etablert rutiner for sporing, rapportering og korrigering av sikkerhetskonfigurasjon på enheter, programvare og tjenester for å hindre angripere i å utnytte disse.

Hvorfor er dette viktig?

De fleste IKT-produkter leveres med en standardkonfigurasjon utviklet av produsent eller forhandler. Disse konfigurasjonene er vanligvis utviklet for å forenkle installasjon eller bruk, ikke for å tilby god sikkerhet. *Åpne tjenester og porter, standardkontoer og passord, eldre (og ofte sårbare) protokoller og forhåndsinstallert programvare kan gi en angriper en rekke muligheter til å oppnå uautorisert tilgang. Systemer som ikke er eksplisitt konfigurert har mest sannsynlig sårbarheter som en angriper kan utnytte.* Virksomheter må derfor herde IKT-produktene, eksempelvis ved å ta bort funksjonalitet det ikke er tjenstlig behov for samt fjerne standard-innstillinger og passord.

Anbefalte tiltak: Ivareta en sikker konfigurasjon

2.3.1	**Etabler et sentralt styrt regime for sikkerhetsoppdatering.** Installer sikkerhetsoppdateringer så fort som mulig. **a)** Etabler en prioriteringsliste for oppdateringer. Operativsystem og applikasjoner på de ansattes klienter bør prioriteres. Videre bør man oppdatere servere som inneholder standard applikasjoner og operativsystem, programvaren i skrivere, samt enheter som styrer virksomhetens nettverk (svitsjer, rutere). **b)** Etabler en rutine med klare ansvarsforhold for *i)* hvor ofte oppdateringer skal utføres (mye bør kunne automatiseres) og *ii)* ansvarlig rolle for oppfølging hvis en oppdatering ikke kan gjennomføres eller må utsettes. **c)** Isoler servere og annet som oppleves som vanskelig å holde oppdatert, se 2.5.4. **d)** Virksomheter bør automatisere og forenkle prosessen for å implementere nye sikkerhetsoppdateringer.

Utdypende informasjon

Herding er en viktig del av den totale informasjonssikkerheten. Manglende herding av systemkomponenter er ofte en årsak til at angripere får fotfeste i virksomheten. *Operativsystemer på*

Lenker

[1] NSM - Sikring av Network Time Protocol (NTP): https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk_sikkerhet/U-09_Sikring_av_NTP.pdf

Anbefalte tiltak

- beskriver sikkerhetstiltak en virksomhet bør gjøre for å følge grunnprinsippet

2.3. Ivareta en sikker konfigurasjon

Målet med prinsippet: Virksomheten konfigurerer og tilpasser maskin- og programvare slik at det tilfredsstiller virksomhetens behov for sikkerhet. Det er etablert rutiner for sporing, rapportering og korrigering av sikkerhetskonfigurasjon på enheter, programvare og tjenester for å hindre angripere i å utnytte disse.

Hvorfor er dette viktig?

De fleste IKT-produkter leveres med en standardkonfigurasjon utviklet av produsent eller forhandler. Disse konfigurasjonene er vanligvis utviklet for å forenkle installasjon eller bruk, ikke for å tilby god sikkerhet. *Åpne tjenester og porter, standardkontoer og passord, eldre (og ofte sårbare) protokoller og forhåndsinstallert programvare kan gi en angriper en rekke muligheter til å oppnå uautorisert tilgang. Systemer som ikke er eksplisitt konfigurert har mest sannsynlig sårbarheter som en angriper kan utnytte.* Virksomheter må derfor herde IKT-produktene, eksempelvis ved å ta bort funksjonalitet det ikke er tjenstlig behov for samt fjerne standard-innstillinger og passord.

Anbefalte tiltak: Ivareta en sikker konfigurasjon

2.3.1	**Etabler et sentralt styrt regime for sikkerhetsoppdatering.** Installer sikkerhetsoppdateringer så fort som mulig. **a)** Etabler en prioriteringsliste for oppdateringer. Operativsystem og applikasjoner på de ansattes klienter bør prioriteres. Videre bør man oppdatere servere som inneholder standard applikasjoner og operativsystem, programvaren i skrivere, samt enheter som styrer virksomhetens nettverk (svitsjer, rutere). **b)** Etabler en rutine med klare ansvarsforhold for *i)* hvor ofte oppdateringer skal utføres (mye bør kunne automatiseres) og *ii)* ansvarlig rolle for oppfølging hvis en oppdatering ikke kan gjennomføres eller må utsettes. **c)** Isoler servere og annet som oppleves som vanskelig å holde oppdatert, se 2.5.4. **d)** Virksomheter bør automatisere og forenkle prosessen for å implementere nye sikkerhetsoppdateringer.

Utdypende informasjon

Herding er en viktig del av den totale informasjonssikkerheten. Manglende herding av systemkomponenter er ofte en årsak til at angripere får fotfeste i virksomheten. *Operativsystemer på*

Lenker

[1] NSM - Sikring av Network Time Protocol (NTP): https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/U-09_Sikring_av_NTP.pdf

2.3. Ivareta en sikker konfigurasjon

Målet med prinsippet: Virksomheten konfigurerer og tilpasser maskin- og programvare slik at det tilfredsstiller virksomhetens behov for sikkerhet. Det er etablert rutiner for sporing, rapportering og korrigering av sikkerhetskonfigurasjon på enheter, programvare og tjenester for å hindre angripere i å utnytte disse.

Hvorfor er dette viktig?

De fleste IKT-produkter leveres med en standardkonfigurasjon utviklet av produsent eller forhandler. Disse konfigurasjonene er vanligvis utviklet for å forenkle installasjon eller bruk, ikke for å tilby god sikkerhet. *Åpne tjenester og porter, standardkontoer og passord, eldre (og ofte sårbare) protokoller og forhåndsinstallert programvare kan gi en angriper en rekke muligheter til å oppnå uautorisert tilgang. Systemer som ikke er eksplisitt konfigurert har mest sannsynlig sårbarheter som en angriper kan utnytte.* Virksomheter må derfor herde IKT-produktene, eksempelvis ved å ta bort funksjonalitet det ikke er tjenstlig behov for samt fjerne standard-innstillinger og passord.

Anbefalte tiltak: Ivareta en sikker konfigurasjon

2.3.1	**Etabler et sentralt styrt regime for sikkerhetsoppdatering.** Installer sikkerhetsoppdateringer så fort som mulig. **a)** Etabler en prioriteringsliste for oppdateringer. Operativsystem og applikasjoner på de ansattes klienter bør prioriteres. Videre bør man oppdatere servere som inneholder standard applikasjoner og operativsystem, programvaren i skrivere, samt enheter som styrer virksomhetens nettverk (svitsjer, rutere). **b)** Etabler en rutine med klare ansvarsforhold for *i)* hvor ofte oppdateringer skal utføres (mye bør kunne automatiseres) og *ii)* ansvarlig rolle for oppfølging hvis en oppdatering ikke kan gjennomføres eller må utsettes. **c)** Isoler servere og annet som oppleves som vanskelig å holde oppdatert, se 2.5.4. **d)** Virksomheter bør automatisere og forenkle prosessen for å implementere nye sikkerhetsoppdateringer.

Utdypende informasjon

- beskriver «kjekt-å-vite-informasjon» om prinsippet og lenker hvor man kan finne utdypende informasjon

Utdypende informasjon

Herding er en viktig del av den totale informasjonssikkerheten. Manglende herding av systemkomponenter er ofte en årsak til at angripere får fotfeste i virksomheten. *Operativsystemer på*

Lenker

[1] NSM - Sikring av Network Time Protocol (NTP): https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/U-09_Sikring_av_NTP.pdf

3 - Oppsummering og veien videre

NASJONAL
SIKKERHETSMYNDIGHET

Overordnet oppsummering – grunnprinsipper-IKT

- Få *oversikt* over maskiner og programvare *i bruk*
- Fjern de vanligste *sårbarhetene*:
  - Klientkonfigurasjon (+ serverkonfigurasjon)
  - Nettverkskonfigurasjon
  - Sikkerhetsoppdatering
- Sørg for god *tilgangsstyring*
  - Bedre og mer finmasket styring av rettigheter
    - sluttbrukere og drift
  - Avslutt bruk av enkle passord
  - Avslutt bruk av enkle påloggingsmekanismer (→MFA)
- Ha tilstrekkelig *beredskap*
  - Backup, systemovervåkning og logging
  - Plan ved hendelser (og øve)

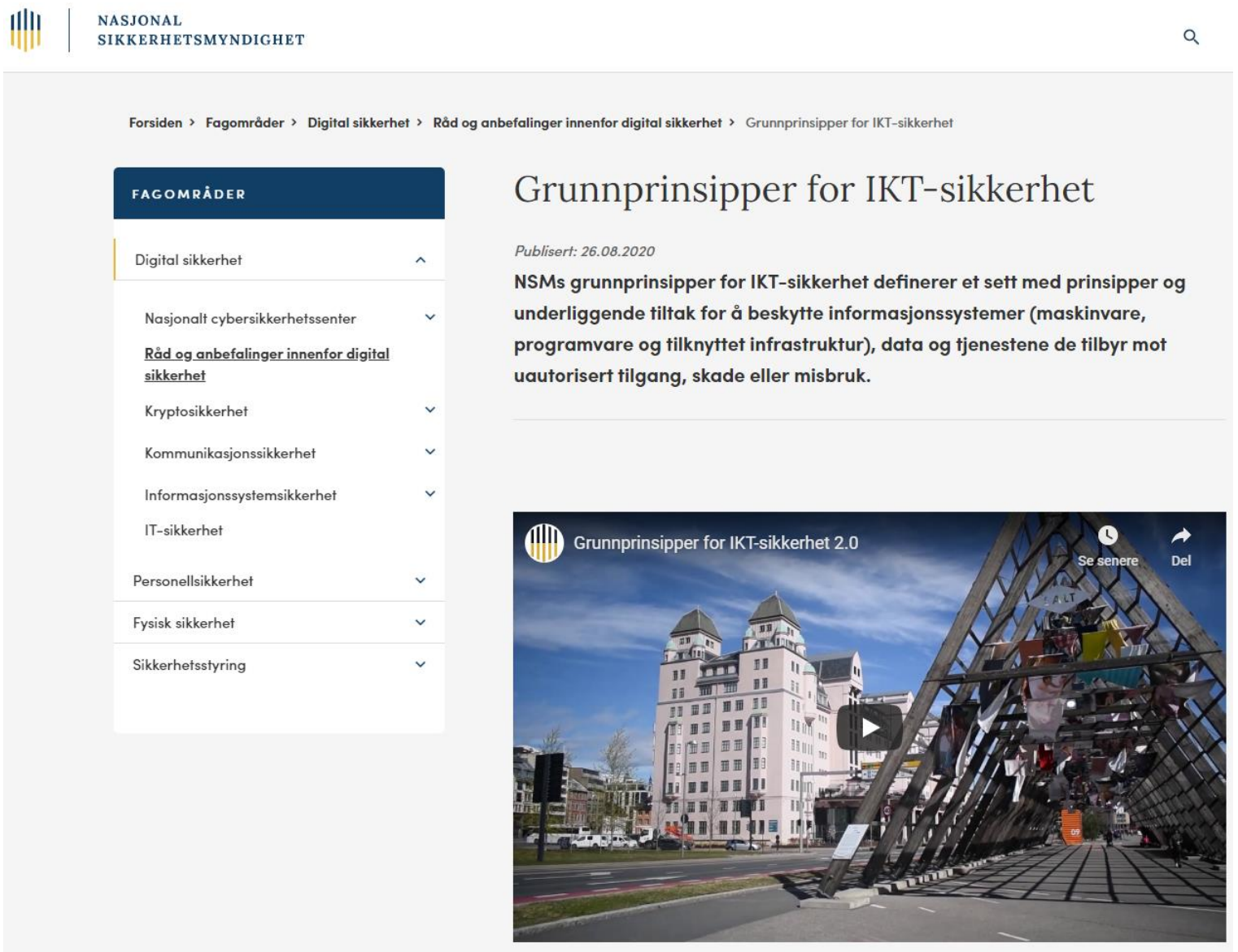
Merknader:

- **Gjennomgående:** mest mulig *sentralisert, automatisert og standardisert drift* av klienter, servere og nettverk.
- **Sky:** Tiltakene er like relevant for både virtualisert og fysisk infrastruktur, og både for «on-prem» og ved kjøp av f.eks. IaaS-tjenester.
- **I sum:** *Forebygg, forebygg, forebygg*, men vær også forberedt på at noe kan gå galt.

Støtteprodukter

- Regneark med sikkerhetstiltak
  - 15 tiltak – Prioritetsgruppe 1
  - 20 tiltak – prioriteringsgruppe 2
  - 83 tiltak – prioriteringsgruppe 3
  - Kobling mot ISO 27002
- Verktøy for risikovurdering
- Scenariobasert tilnærming – skadevare løsepengevirus
- Ofte stilte spørsmål
- E-læringskurs

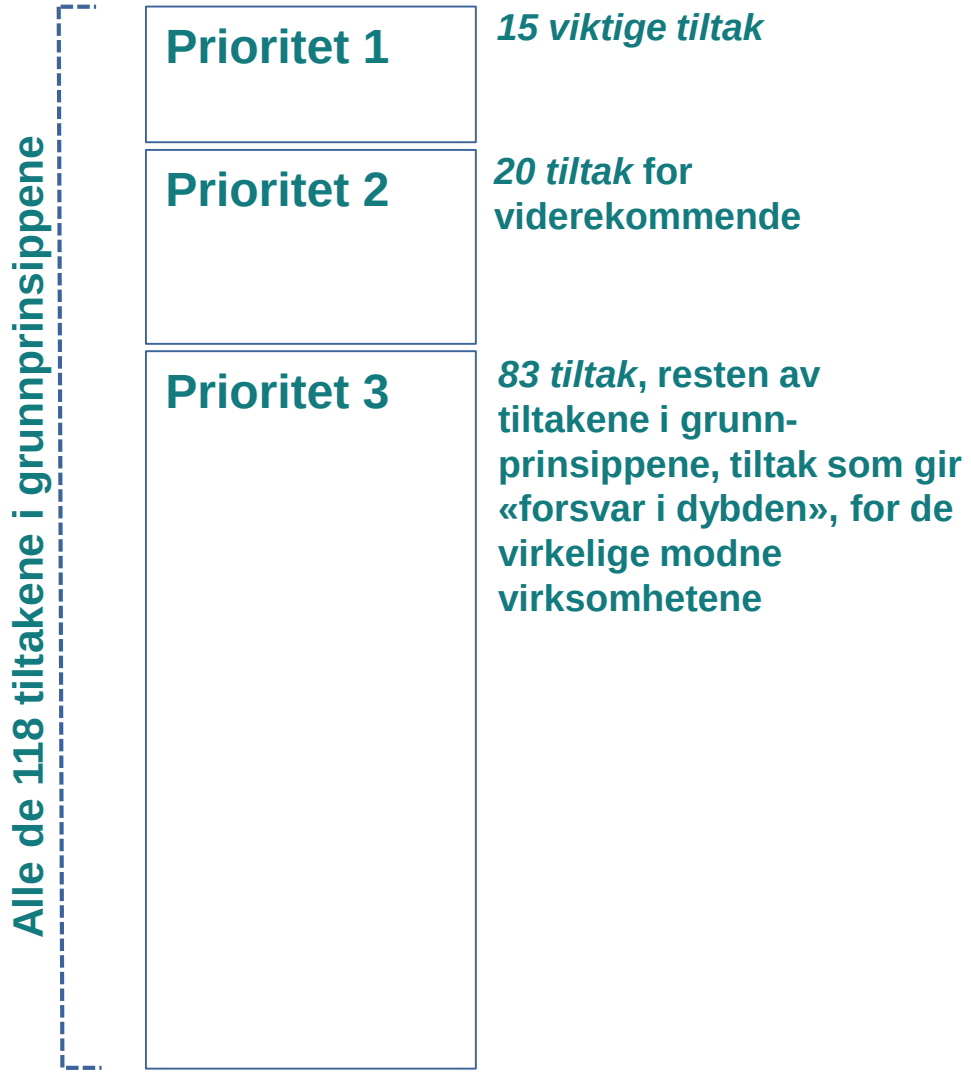
- nsm.no/grunnprinsipper-ikt



Steg i sikkerhetsarbeidet

Anbefalt rekkefølge ved implementering av tiltakene i grunnprinsippene:

1. Prioritetsgruppe 1 (15 tiltak)
2. Prioritetsgruppe 2 (20 tiltak)
3. Prioritetsgruppe 3 (83 tiltak)



15 prioriterte tiltak

1. Kartlegg enheter i bruk i virksomheten
2. Kartlegg programvare i bruk i virksomheten
3. Kjøp moderne og oppdatert maskin- og programvare
4. Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting
5. Del opp virksomhetens nettverk etter virksomhetens risikoprofil
6. Etabler et sentralt styrt regime for sikkerhets-oppdatering
7. Konfigurer klienter slik at kun kjent programvare kjører på dem
8. Deaktiver unødvendig funksjonalitet
9. Endre standardpassord på IKT-produktene før produksjonssetting
10. Minimer rettigheter til sluttbrukere og spesialbrukere
11. Minimer rettigheter på driftskontoer
12. Legg en plan for regelmessig sikkerhets-kopiering av alle virksomhetsdata
13. Avgjør hvilke deler av IKT-systemet som skal overvåkes
14. Beslutt hvilke data som er sikkerhetsrelevant og bør samles inn
15. Etabler et planverk for hendelseshåndtering

Tiltakene i prioritetsgruppe 1

15 viktige tiltak:

1. 1.2.3 Kartlegg enheter i bruk i virksomheten.
2. 1.2.4 Kartlegg programvare i bruk i virksomheten.
3. 2.1.2 Kjøp moderne og oppdatert maskin- og programvare.
4. 2.1.9 Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting.
5. 2.2.3 Del opp virksomhetens nettverk etter virksomhetens risikoprofil.
6. 2.3.1 Etabler et sentralt styrt regime for sikkerhetsoppdatering.
7. 2.3.2 Konfigurer klienter slik at kun kjent programvare kjører på dem.
8. 2.3.3 Deaktiver unødvendig funksjonalitet.
9. 2.3.7 Endre alle standardpassord på IKT-produktene før produksjonssetting.
10. 2.6.4 Minimer rettigheter til sluttbrukere og spesialbrukere.
11. 2.6.5 Minimer rettigheter på drifts-kontoer.
12. 2.9.1 Legg en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata.
13. 3.2.3 Avgjør hvilke deler av IKT-systemet som skal overvåkes.
14. 3.2.4 Beslutt hvilke data som er sikkerhetsrelevant og bør samles inn.
15. 4.1.1 Etabler et planverk for hendelseshåndtering.

Merknader: alt henger sammen med alt …

- Merknad til 1.2.3: Se tiltaket i sammenheng med 1.2.1 og 1.2.2.
- Merknad til 1.2.4: Se tiltaket i sammenheng med 1.2.1 og 1.2.2.
- Merknad til 2.1.2: Fokuser i første omgang på klientene.
- Merknad til 2.2.3: Bør sees i sammenheng med 2.5.1.
- Merknad til 2.3.2: Dette må tilpasses klient-operativsystem og applikasjoner.
- Merknad til 2.3.3: Fokuser i første omgang på klientene.
- Merknad til 2.3.7: Og vurder generelt passordkvaliteten i virksomheten, se 2.6.3.e.
- Merknad til 2.3.7: Og vurder å ta i bruk multi-faktor autentisering, se 2.6.7.
- Merknad til 2.9.1: Test sikkerhetskopier regelmessig ref. 2.9.3.
- Merknad til 3.2.3: Se tiltaket i sammenheng med bl.a. 3.2.4, 3.3.1 og 3.3.3.
- Merknad til 3.2.4: Se tiltaket i sammenheng med bl.a. 3.2.3, 3.3.1 og 3.3.3.
- Merknad til 4.1.1: Som minimum planlegg roller og ansvar ref 4.1.3. Og øv på dette, ref. 4.1.6.

nsm.no/grunnprinsipper-ikt

Nyttige lenker NSM

- NSMs elæringskurs
  - https://nsm.muniolms.com/sv/shop/nsm/category/40
- NSM.no
  - nsm.no/grunnprinsipper-ikt
  - nsm.no/ncsc
  - nsm.no/sky
  - nsm.no/skadevare
  - nsm.no/digitalutpressing (går til samme sted som skadevare)
  - nsm.no/regelverk-og-hjelp/rapporter/
  - nsm.no/aktuelt/nasjonalt-digitalt-risikobilde-2021