Oslo

# Arbeid med informasjonssikkerhet i Oslo kommune

DigDir – NIFS møte
November 2021

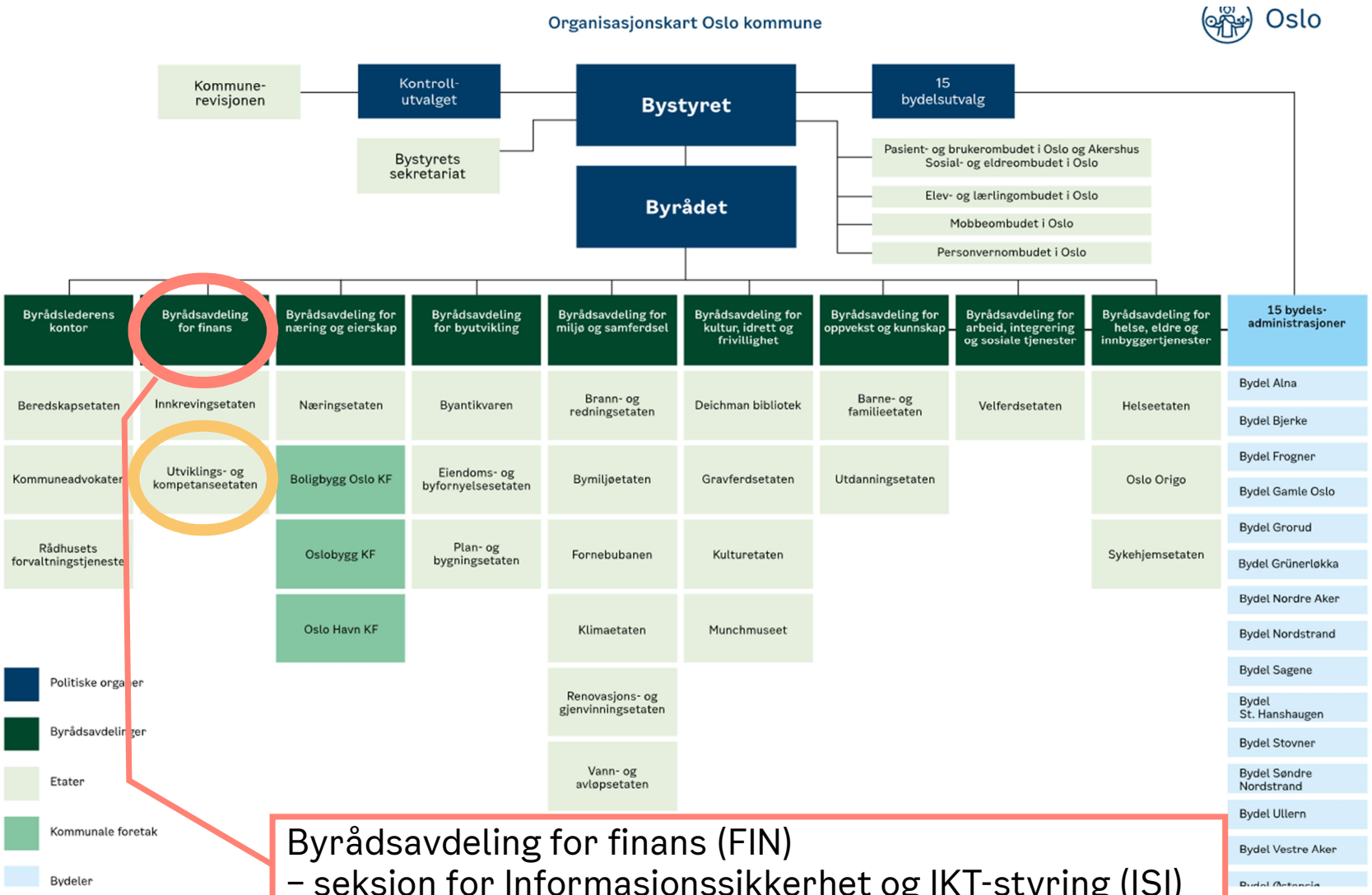
Åsmund Skomedal
Fagsjef informasjonssikkerhet

asmund.skomedal@byr.oslo.kommune.no

# Tema

- Organisering og målsetninger
- (Overordnet) styringssystem og rapportering
- Roller og koordinatorer
- Kurs og veiledere
- Nettverk og møteplasser

# Organisasjon




Byrådsavdeling for finans (FIN)
– seksjon for Informasjonssikkerhet og IKT-styring (ISI)

# ISI – aktiviteter

- Strategisk arbeid
  - Digitaliseringsstrategi
  - Som inkluder en informasjonssikkerhetsstrategi
- Overordnet styring – «konsernperspektivet»
  - Organisering og risikostyring
  - Styringsmodell for hver enkelt virksomhet (ISMS)
- Operativ styring - Utviklings- og kompetanse etaten (UKE)
  - Felles IKT-plattform
  - Felles fagsystemer
- Standardisering
- Veiledere og maler
- Kompetanseheving

# Arbeid med harmonisering

| | Styring | | | | Etter-levelse | Felles løsninger | |
|---|---|---|---|---|---|---|---|
| **Aktivitet** | **ISMS** | **Årlig rapp.** | **ROS** | **Roller** | **DPIA** | **Plattform** | **Fagsystem** |
| Standardisere | Pågår | VE; egen-erklæring | De facto mal | Koordinatorer | De facto mal | Pålogging & brukertilgang | O365, arkiv, HR ++ |
| Veilede | Planlagt | Maler | Maler | Rollekort | Om malen | Intranett | Intranett |
| Holde kurs | Eksterne | - | 3-4 årlig | - | Flere årlig | - | O365 ++ |
| Nettverk / Forum | - | Forum Q2 | Forum orientering | Forum orientering | Nettverk og koordinering | Arkitektur forum | * forum |

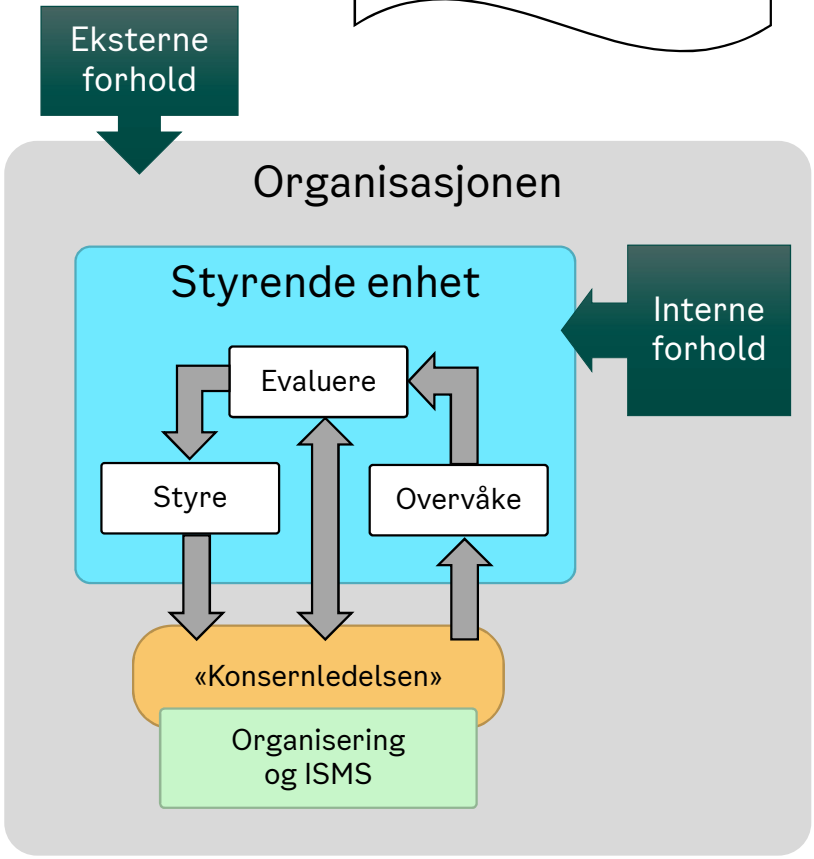
- ISMS - Styringsrammeverk for informasjonssikkerhet
- VE - Virksomhetsleders egenerklæring
- ROS – Risiko og sårbarhet
- DPIA - Data Privacy Impact Assessment


# Overordnet styringssystem (planlagt)

Fritt etter ISO 27014

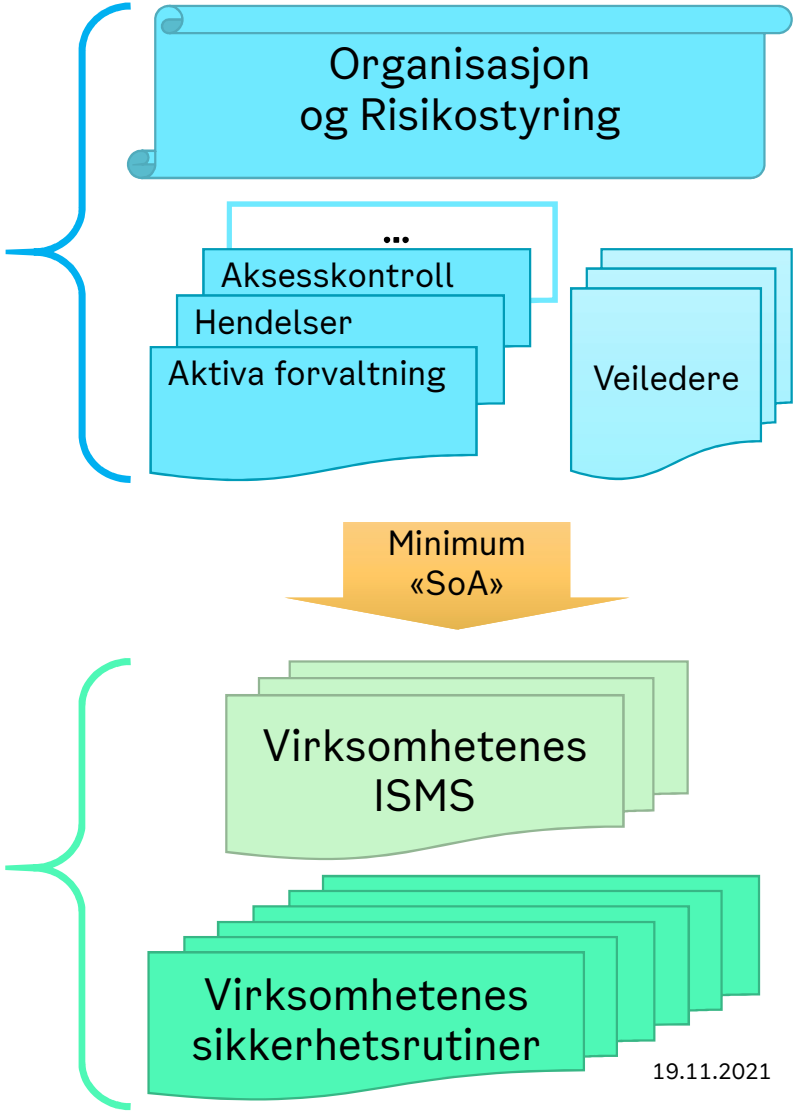
Overbygging på tvers av alle sektorene

- Organisering; basert på ISO 27014 og rollene til
  - Byrådsavdeling for finans (FIN)
  - Øvrige Byrådsavdelinger
  - Virksomhetene
- Risikostyring
- Balansere flere hensyn
  - Risikobildet må være helhetlig og forstått
  - Dynamikk i styring og prioritering på tvers
  - Virksomhetene (etater, bydeler, … ) skal i en parlamentarisk styringsmodell har betydelig frihet




# Overordnet styringssystem (2)

- Overbygging på tvers av alle byrådsavdelingene
- Serie med standarder for ulike ISO-27k «domener» Minimumskrav til virksomhetenes «SoA»
  - Forvaltning av aktiva
  - Hendelseshåndtering
  - Aksesskontroll, …
- Veiledere til de enkelte standardene
- Virksomhetene er selv ansvarlige for å etablere og å etterleve egne
  - Styringssystemer
  - Sikkerhetsrutiner og prosedyrer




# Årlig rapportering

- Virksomhetsleders Egenerklæring (VE)
  - Virksomhetsledere -> Byrådsavdelingene

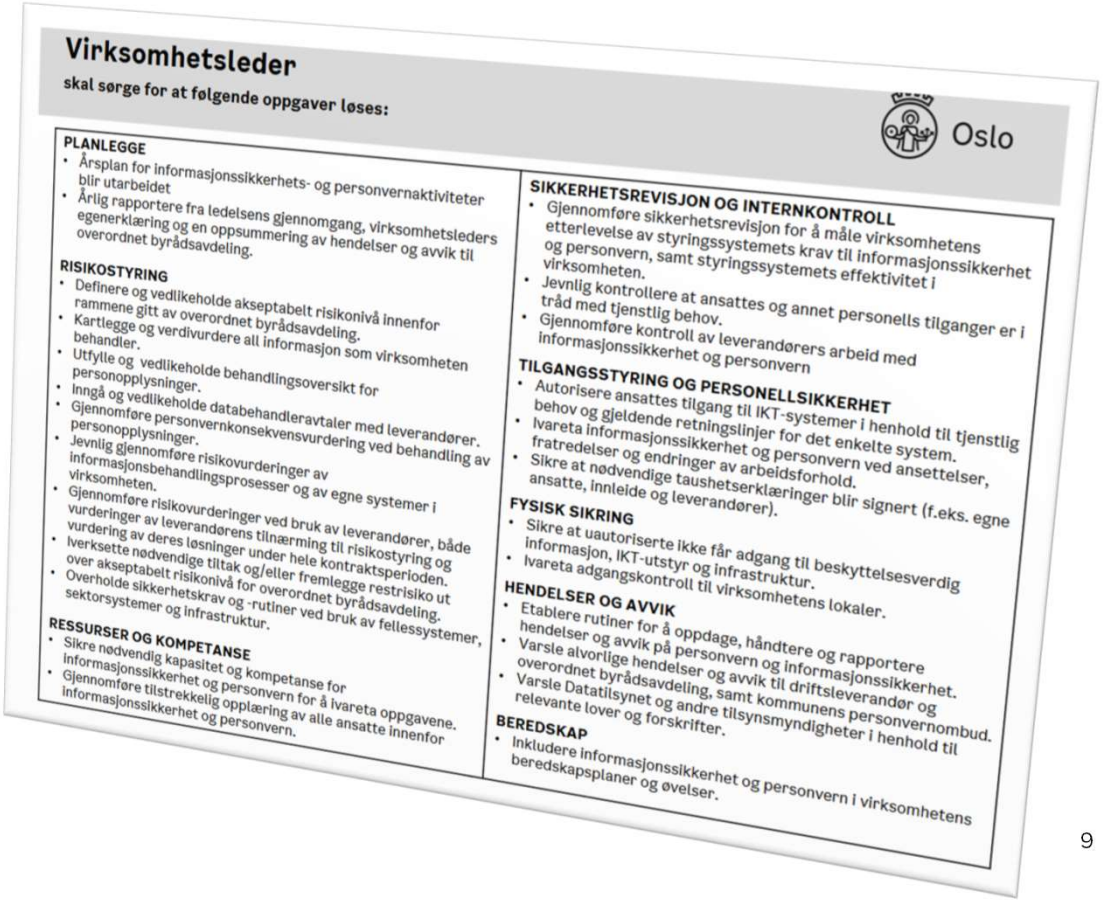
  Aggregert for hver sektor
  - Byrådsavdelingene -> Byrådsavdeling for Finans (FIN)
  - Byrådsavdeling for Finans -> Byrådet (vanligvis)

    Rapporterer status og vesentlige endringer fra tidligere år
- Noen «målepunkter»
  - Er akseptabel risiko definert i sektor/virksomhet?
  - Er det etablert system for internkontroll?
  - Er informasjonsverdier kartlagt og verdivurdert?
  - Hvor mange sytemeierskap og hvor mange ROS-vurderinger?
  - Hvor mange avvik er meldt til datatilsynet?

| | Styring | | | | Etter-levelse | Felles løsninger | |
|---|---|---|---|---|---|---|---|
| Aktivitet | ISMS | Årlig rapp. | ROS | Roller | DPIA | Plattform | Fagsystem |
| Standardisere | Pågår | LG/VE | De facto mal | oordinatorer | De facto mal | Pålogging & brukertilgang | O365, arkiv, HR ++ |
| Veilede | Planlagt | Maler | Maler | Rollekort | Om malen | Intranett | Intranett |
| Holde kurs | Eksterne | - | 3-4 årlig | - | Flere årlig | - | O365 ++ |
| Nettverk / Forum | - | Forum Q2 | Forum orientering | Forum orientering | Nettverk og koordinering | Arkitektur forum | * forum |

# Rollekort ~linjeorganisasjon for sikkerhet

- Fra 2019; noen nye og noen revidert i år
  - Kommunaldirektør
  - Virksomhetsleder
  - Informasjonssikkerhetskoordinator (ny)
  - Personvernkoordinator (ny)
  - Systemeier
  - Systemforvalter



**Virksomhetsleder**

**skal sørge for at følgende oppgaver løses:**

Oslo

**PLANLEGGE**
- Årsplan for informasjonssikkerhets- og personvernaktiviteter blir utarbeidet
- Årlig rapportere fra ledelsens gjennomgang, virksomhetsleders egenerklæring og en oppsummering av hendelser og avvik til overordnet byrådsavdeling.

**RISIKOSTYRING**
- Definere og vedlikeholde akseptabelt risikonivå innenfor rammene gitt av overordnet byrådsavdeling.
- Kartlegge og verdivurdere all informasjon som virksomheten behandler.
- Utfylle og vedlikeholde behandlingsoversikt for personopplysninger.
- Inngå og vedlikeholde databehandleravtaler med leverandører.
- Gjennomføre personvernkonsekvensvurdering ved behandling av personopplysninger.
- Jevnlig gjennomføre risikovurderinger av informasjonsbehandlingsprosesser og av egne systemer i virksomheten.
- Gjennomføre risikovurderinger ved bruk av leverandører, både vurderinger av leverandørens tilnærming til risikostyring og vurdering av deres løsninger under hele kontraktsperioden.
- Iverksette nødvendige tiltak og/eller fremlegge restrisiko ut over akseptabelt risikonivå for overordnet byrådsavdeling.
- Overholde sikkerhetskrav og -rutiner ved bruk av fellessystemer, sektorsystemer og infrastruktur.

**RESSURSER OG KOMPETANSE**
- Sikre nødvendig kapasitet og kompetanse for informasjonssikkerhet og personvern for å ivareta oppgavene.
- Gjennomføre tilstrekkelig opplæring av alle ansatte innenfor informasjonssikkerhet og personvern.

**SIKKERHETSREVISJON OG INTERNKONTROLL**
- Gjennomføre sikkerhetsrevisjon for å måle virksomhetens etterlevelse av styringssystemets krav til informasjonssikkerhet og personvern, samt styringssystemets effektivitet i virksomheten.
- Jevnlig kontrollere at ansattes og annet personells tilganger er i tråd med tjenstlig behov.
- Gjennomføre kontroll av leverandørers arbeid med informasjonssikkerhet og personvern

**TILGANGSSTYRING OG PERSONELLSIKKERHET**
- Autorisere ansattes tilgang til IKT-systemer i henhold til tjenstlig behov og gjeldende retningslinjer for det enkelte system.
- Ivareta informasjonssikkerhet og personvern ved ansettelser, fratredelser og endringer av arbeidsforhold.
- Sikre at nødvendige taushetserklæringer blir signert (f.eks. egne ansatte, innleide og leverandører).

**FYSISK SIKRING**
- Sikre at uautoriserte ikke får adgang til beskyttelsesverdig informasjon, IKT-utstyr og infrastruktur.
- Ivareta adgangskontroll til virksomhetens lokaler.

**HENDELSER OG AVVIK**
- Etablere rutiner for å oppdage, håndtere og rapportere hendelser og avvik på personvern og informasjonssikkerhet.
- Varsle alvorlige hendelser og avvik til driftsleverandør og overordnet byrådsavdeling, samt kommunens personvernombud.
- Varsle Datatilsynet og andre tilsynsmyndigheter i henhold til relevante lover og forskrifter.

**BEREDSKAP**
- Inkludere informasjonssikkerhet og personvern i virksomhetens beredskapsplaner og øvelser.

Oslo | Felles intranett for Oslo kommune

Hovedside | Informasjonssikkerhet og personvern | Styrende dokumenter og styringssystem | Styringssystem og internkontroll | Roller og ansvar


# Om rollekortene

Rollekortene er utarbeidet for å gjøre det enklere for deg som ansatt i Oslo kommune å sette deg inn i ansvar og oppgaver innenfor informasjonssikkerhet og personvern, knyttet til rollene dine.

- Rollekortene er **veiledninger**, basert på styrende dokumenter i Oslo kommune og anerkjent praksis på fagområdene. 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 personvern som tilligger ulike roller. Oppgavene kan tilpasses den enkelte virksomhet, med mindre annet er bestemt.
- Informasjonssikkerhet- og personvern**koordinator er obligatoriske** roller

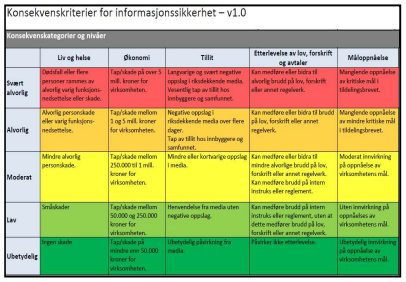
| Aktivitet | ISMS | Årlig rapp. | ROS | Roller | DPIA | Plattform | Fagsystem |
|---|---|---|---|---|---|---|---|
| | Styring | | | | Etter-levelse | Felles løsninger | |
| Standardisere | Pågår | LG/VE | De facto mal | oordinatorer | De facto mal | Pålogging & brukertilgang | O365, arkiv, HR ++ |
| Veilede | Planlagt | Maler | Maler | Rollekort | Om malen | Intranett | Intranett |
| Holde kurs | Eksterne | - | 3-4 årlig | - | Flere årlig | - | O365 ++ |
| Nettverk / Forum | - | Forum Q2 | Forum orientering | Forum orientering | Nettverk og koordinering | Arkitektur forum | * forum |

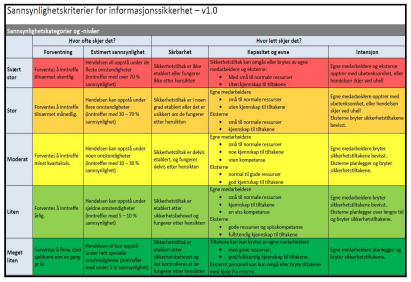
# Risikovurderinger – felles ressurser


Veileder for risikovurdering av informasjonssikkerhet

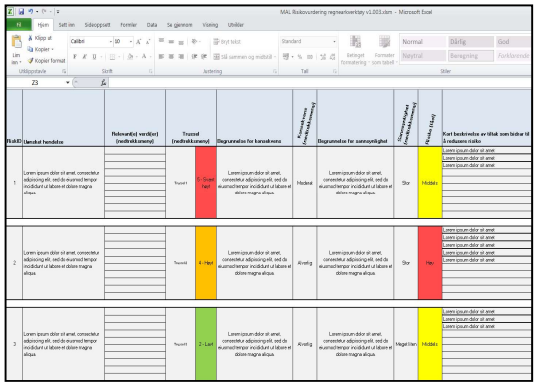
| Risikonivå | Beskrivelse | Kriterier for å akseptere risiko |
|---|---|---|
| Lav | Tiltak er ikke nødvendig | Risiko kan aksepteres uten å lete etter eller vurdere nytten av flere tiltak. Tiltak kan allikevel vurderes dersom de er kostnadseffektive.<br><br>**Risikoen kan aksepteres av ledere på alle beslutningsnivå.** |
| Middels | Tiltak skal vurderes. Risiko må følges opp. | Det er gjennomført et systematisk arbeid for å identifisere tiltak. Alternativ risikohåndtering er mindre effektiv, gir høyere risiko på andre områder, og/eller er dyrere.<br><br>**Risikoen kan aksepteres av systemeier eller virksomhetsleder.** |
| Høy | Tiltak skal iverksettes snarest. | Det er gjennomført et systematisk og grundig arbeid for å identifisere risikoreduserende tiltak. Alternativ risikohåndtering er svært uhensiktsmessig, gir høyere risiko på dette eller andre områder, eller er svært kostbar.<br><br>**Risikoen kan kun aksepteres av virksomhetsleder og skal rapporteres til overordnet byrådsavdeling.** |

Akseptkriterier




Konsekvens- og sannsynlighetskriterier



Regneark for risikovurdering


Mal for sluttrapport


# Personvernvurdering og DPIA

## - mal og veileder

1 Start med innledende vurdering av personvernet til den registrerte


Vurdering av om risikoen for den registrerte er **lav/middels** eller **høy**

A Personvernkonsekvens-vurdering ved lav/middels risiko (PLM)

A ELLER B

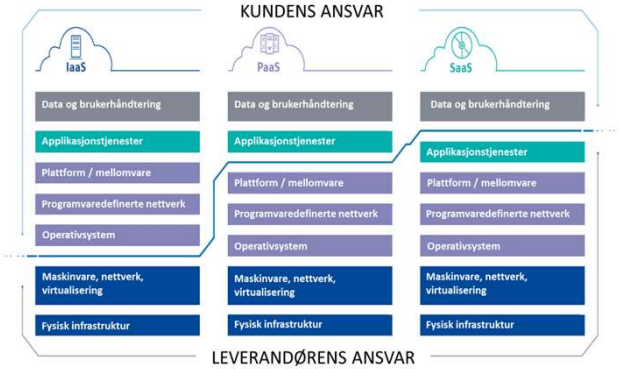
B Personvernkonsekvens-vurdering ved høy risiko

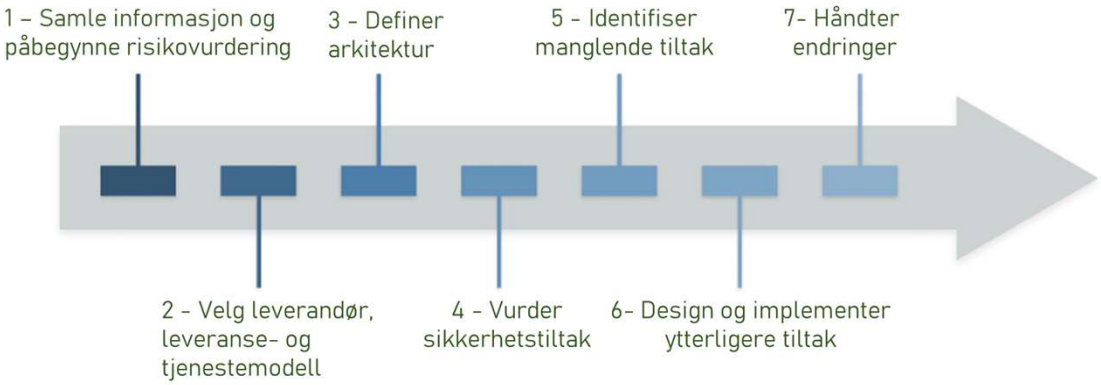
(DPIA – Data Protection Impact Assessment)

| Har behandlingen av personopplysninger behandlingsgrunnlag i GDPR? *[For å finne riktig behandlingsgrunnlag, se Veileder om behandlingsgrunnlag]* | |
|---|---|
| **Behandlingsgrunnlag for alminnelige personopplysninger etter GDPR art. 6** | **Behandlingsgrunnlag for særlige kategorier personopplysninger etter GDPR art. 9** |
| ☐ a. Samtykke | ☐ a. Samtykke |
| ☐ b. Avtale | ☐ b. Forpliktelser og rettigheter for den behandlingsansvarlige eller den registrerte på området arbeidsrett, trygderett og sosialrett. *[Dette behandlingsgrunnlaget vil kreve supplerende rettsgrunnlag.]* |
| ☐ c. Rettslig forpliktelse *[Dette behandlingsgrunnlaget vil kreve supplerende rettsgrunnlag.]* | ☐ c. Vitale interesser til den registrerte eller en annen fysisk person, dersom samtykke ikke kan gis |
| ☐ d. Vitale interesser til den registrerte eller en annen fysisk person | ☐ d. Behandlingen utføres av en stiftelse, sammenslutning eller et annet ideelt organ hvis mål er av politisk, religiøs eller fagforeningsmessig art |
| ☐ e. Allmenhetens interesse eller utøvelse av offentlig myndighet som den behandlingsansvarlige er pålagt. | ☐ e. Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte har offentliggjort |


# Skytjenester – en veileder for IaaS & PaaS

- Formålet 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
- Veilederen fokuserer på disse særskilte vurderingene som må gjøres for skytjenester
- Primært om oppgaver som bør eller må utføres i **vurderingsprosessen** rundt etablering av infrastruktur og plattform i sky




*Information Security Forums rapport «Using Cloud Services Securely»)*

| | Styring | | | | Etter-levelse | Felles løsninger | |
|---|---|---|---|---|---|---|---|
| Aktivitet | ISMS | Årlig rapp. | ROS | Roller | DPIA | Plattform | Fagsystem |
| Standardisere | Pågår | LG/VE | De facto mal | Koordinatorer | De facto mal | Pålogging & brukertilgang | O365, arkiv, HR ++ |
| Holde kurs | Eksterne | - | 3-4 årlig | - | Flere årlig | - | O365 ++ |
| Nettverk / Forum | - | Forum Q2 | Forum orientering | Forum orientering | Nettverk og koordinering | Arkitektur forum | * forum |

# Kompetanseheving og nettverk

- ROS kurs - 3-4 heldagskurs i året med 30-40 deltagere
  - teori – trussel-scenarier, sårbarheter, sannsynlighet, verdivurdering, tiltak
  - og praksis – case-studie med bruk av felles ROS ressurser Verktøy, veileder, maler
- DPIA kurs - under planlegging
- «Forum» (kvartalsvis)
  - Informasjonssikkerhet og personvern: primært rettet mot koordinatorene
  - Arkitekturforum: primært rettet mot systemeiere og plattformer
- Sikkerhetsmåneden
- E-læringer og anti-phishing program

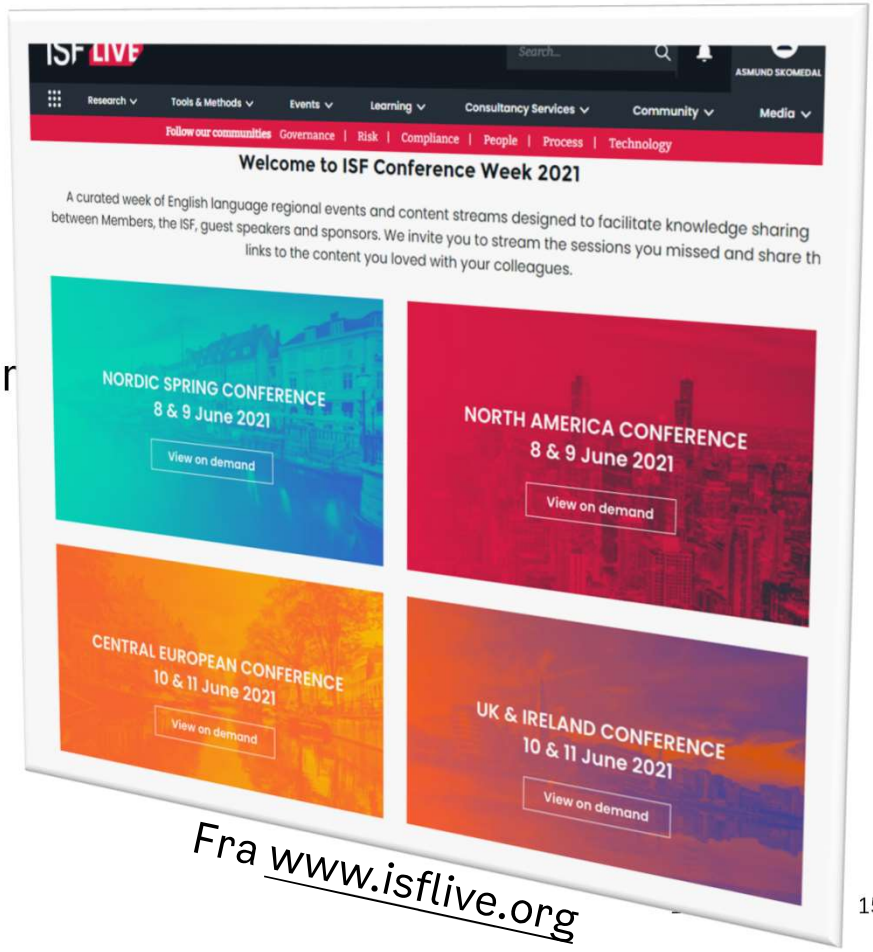
| | Styring | | | | Etter-levelse | Felles løsninger | |
|---|---|---|---|---|---|---|---|
| Aktivitet | ISMS | Årlig rapp. | ROS | Roller | DPIA | Plattform | Fagsystem |
| Standardisere | Pågår | LG/VE | De facto mal | Koordinatorer | De facto mal | Pålogging & brukertilgang | O365, arkiv, HR ++ |
| Holde kurs | Eksterne | - | 3-4 årlig | - | Flere årlig | - | O365 ++ |
| Nettverk / Forum | - | Forum Q2 | Forum orientering | Forum orientering | Nettverk og koordinering | Arkitektur forum | * forum |

# ISF International medlemskap (i)

- Aktuelle brukere:
  - Koordinatorer
  - Systemeiere / Systemforvaltere / Superbrukere
  - Utviklingsmiljø
- Relevant for alle som jobber med sensitive oppgaver
  - Saksbehandling internt eller innbyggere

Ressurser innen en rekke områder

- Inkludert i medlemskapet:
  - All dokumentasjon på metoder og verktøy
  - Konferanser, seminarer og opplæringsmateriale
- Noen kurs og konsulenttjenester må betales for




Fra www.isflive.org


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