



Arbeid med informasjonssikkerhet i Oslo kommune

DigDir – NIFS møte
November 2021

Åsmund Skomedal
Fagsjef informasjonssikkerhet

asmund.skomedal@byr.oslo.kommune.no



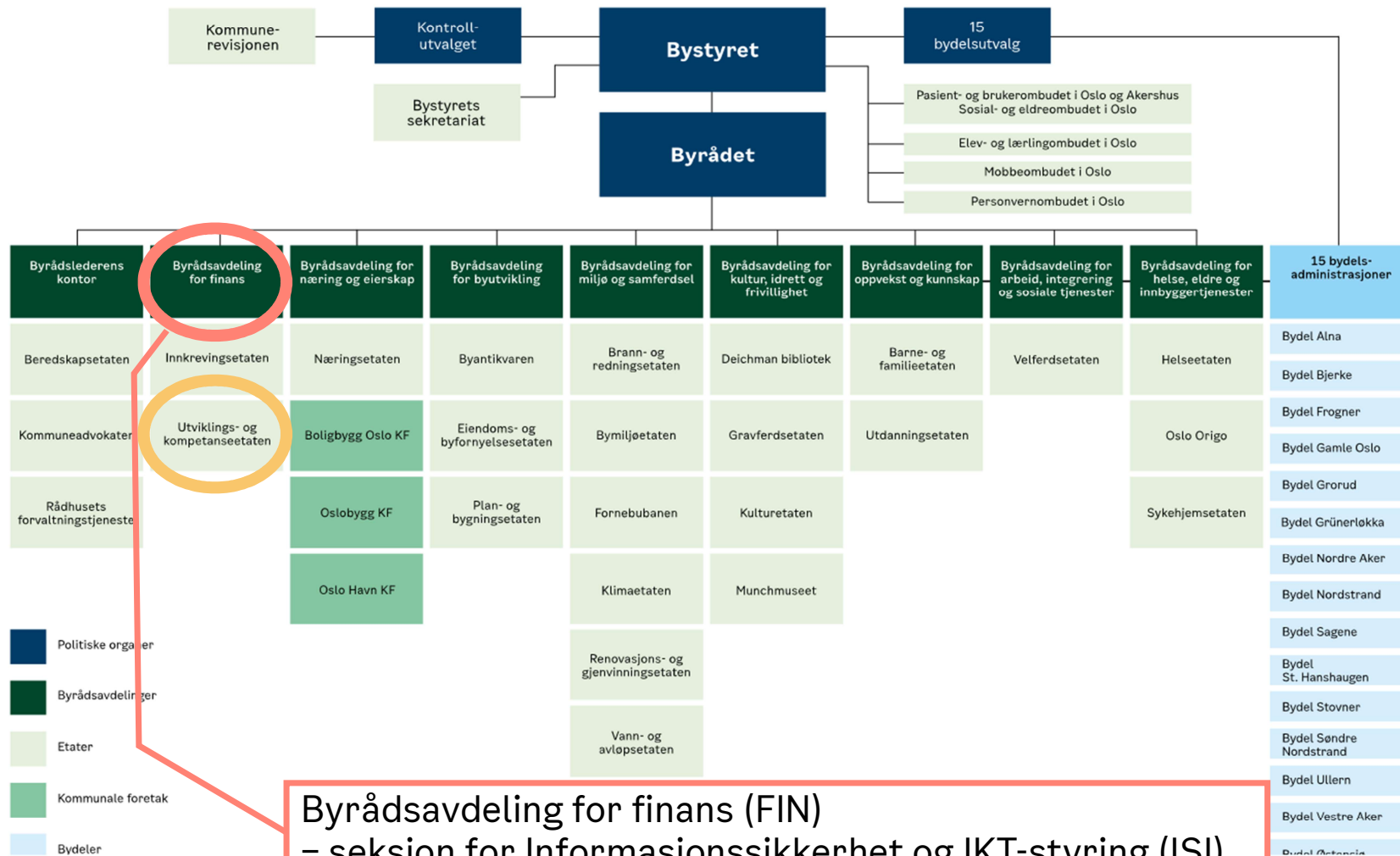


Tema

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

Organisasjon

Organisasjonskart Oslo kommune



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



ISI – aktiviteter

- ▶ Strategisk arbeid
 - Digitaliseringsstrategi
 - Som inkluderer 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

Aktivitet	Styring				Etterlevelse	Felles løsninger	
	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 egen-erklæring
- ROS - Risiko og sårbarhet
- DPIA - Data Privacy Impact Assessment

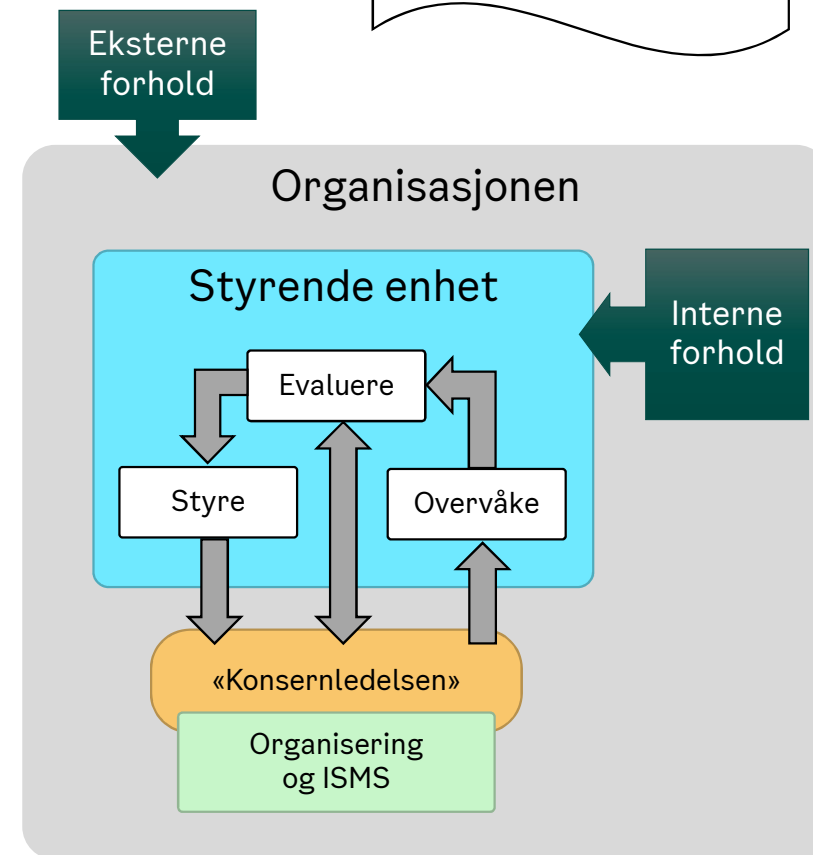
Aktivitet	Styring				Etterlevelse		Felles løsninger	
	ISO 9000	ISO 14000	ISO 45001	ISO 27001	ISO 27001	ISO 27001	ISO 27001	ISO 27001
Standardisere	Plagb	LG/VE	De facto mal	Koordinatorer	De facto mal	Plagging & brukertilgng	O365, arkiv, HR ++	
Veilede	Planlagt	Maler	Maler	Rollekort	Om malen	Intranett	Intranett	
Holde kurs	Eksterne	-	3-4 årlig	-	Flere årlig	-	O365 ++	
Nettverk / Forum	-	Forum Q2	Forum orientering	Forum orientering	Nettverk og koordinering	Arkitektur forum	- forum	

Overordnet styringssystem (planlagt)

Fritt etter ISO 27014

Overbygging på tvers av alle sektorene

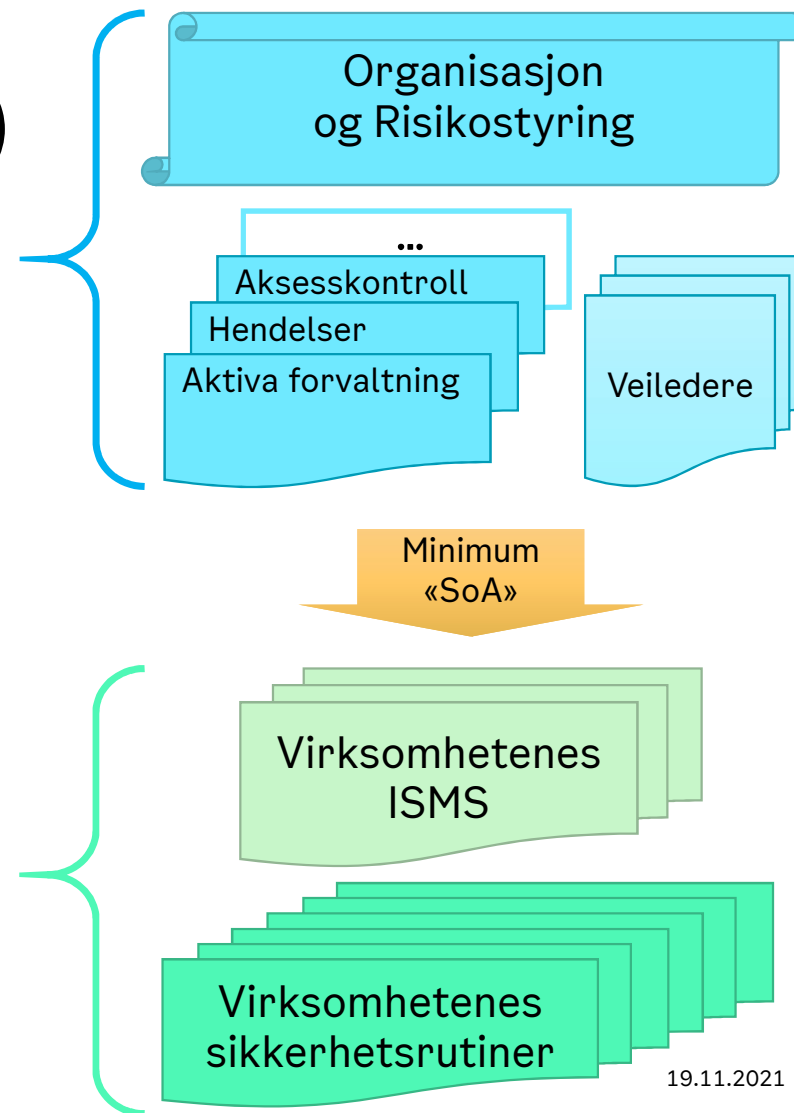
- ▶ Organisering; basert på ISO 27014 og rollene til
 - Byrådsavdeling for finans (FIN)
 - Øvrige Byrådsavdelinger
 - Virksomhetene
- ▶ Risikostyring
- ▶ Balansere flere hensyn
 - Risikobildet må være helhetlig og forstått
 - Dynamikk i styring og prioritering på tvers
 - Virksomhetene (etater, bydeler,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



Aktivitet	Styring				Etterlevelse		Felles løsninger	
	ISO/IEC	ISO 9001	ISO 27001	ISO 27002	ISO 27001	ISO 27002	ISO 27001	ISO 27002
Standardisere	Plaggr	LG/VE	De facto mal	Koordinatorer	De facto mal	Plattformer & brukertilgjeng	O365, arkiv, HR ++	
Veilede	Planlagt	Maier	Maier	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	

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



Aktivitet	Stilling				Etterlevelse		Felles løsninger	
	1944	Arbeids-	ROS	Rolle	SP/A	Plattformer	Eggsystem	
Standardisere	Pligter	LG/VE	De facto mal	Koordinatorer	De facto mal	Pligging & brukertilgang	O365, arkiv, HR ++	
Veilede	Planlagt	Maler	Maler	Rollekort	Om malen	Intranett	Intranett	
Holde kurs	Dokument	-	3-4 årlig	-	Flere årlig	-	O365 ++	
Nettverk / Forum	-	Forum Q2	Forum orientering	Forum orientering	Nettverk og koordinering	Arkitektur forum	forum	

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?



Aktivitet	Styring			Roller	Etterlevelse	Felles løsninger		
	IRHS	Årsrap.	ROS			SIHA	Plattform	Fagsystem
Standardisere	Plagr	LG/VE	De facto mat	beredninger	De facto mat	Plagging & brukertilgang	O365, arkiv, HR ++	
Veilede	Planlagt	Maier	Maier	Rollekort	Om malen	Intranett	Intranett	
Holde kurs	Dikterne	-	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



[Hovedside](#) | [Informasjonssikkerhet og personvern](#) | [Styrende dokumenter og styringssystem](#) | [Styringssystem og internkontroll](#) | [Roller og ansvar](#)



Virksomhetsleder

skal sørge for at følgende oppgaver løses:

PLANLEGGJE

- 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 verddivurdere all informasjon som virksomheten behandler.
- Utfylle og vedlikeholde behandlingsoversikt for personopplysninger.
- Inngå og vedlikeholde databehandlingsavtaler med leverandører.
- Gjennomføre personvernkonsekvensvurdering ved behandling av personopplysninger.
- Jevnlige gjennomføre risikovurderinger av informasjonsbehandlingsprosesser og av egne systemer i virksomheten.
- Gjennomføre risikovurderinger ved bruk av leverandører, både vurdering av deres løsninger tilnærming til risikostyring og iverksette nødvendige tiltak under hele kontraktsperioden.
- 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.
- Jevnlige 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 ansettelse, fratredelse 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.

9

Aktivitet	Styring			Rolle	Etterlevelse	Felles løsninger		
	ISHS	Arbeidsplan	ROS			ISHS	Plattform	Eggsystem
Standardisere	Plag	LG/VE	De facta mat	ordførere	De facta mat	Plagging & brukertilgang	O365, arkiv, HR ++	
Veilede	Planlagt	Maier	Maier	Rollekort	Om malen	Intranett	Intranett	
Holde kurs	Dikterne	-	3-4 årlig	-	Flere årlig	-	O365 ++	
Nettverk / Forum	-	Forum Q2	Forum orientering	Forum orientering	Nettverk og koordinering	Arkitektur forum	forum	

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	Stilling		Etterlevelse	Felles løsninger			
	IRHS	Ansvar		ROK	RAA	Plattformer	Fagsystem
Standardisere	Planlgt	LG/VE	De facto mal	Verktøystøtter	De facto mal	Planlegg & brukertilgang	O365, arkiv, HR ++
Veilede	Planlagt	Maier	Maier	Rolekort	Om maier	Intranett	Intranett
Holde kurs	Dikterne	-	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

Risikobivå	Beskrivelse	Kriterier for å akseptere risiko
Lav	Tilbak ikke nødvendig	Risiko kan aksepteres uten å lete etter eller vurdere nytten av flere tiltak. Tiltak kan allikevel vurderes dersom de er kostnadseffektive. 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 risikobehandling er mindre effektiv, gir høyere risiko på andre områder, eller er dyrt. Risikoen kan aksepteres av systemer eller virksomhetsledere.
Høy	Tiltak skal iverksettes raskest.	Det er gjennomført et systematisk og grundig arbeid for å identifisere risikobehandlede tiltak. Alternativ risikobehandling er svært uhensiktsmessig, gir høyere risiko på dette eller andre områder, eller er svært kostbar. Risikoen kan kun aksepteres av virksomhetsledere og skal rapporteres til overordnet byrådsavdeling.

Akseptkriterier

Konsekvenskriterier for informasjonssikkerhet – v1.0					
	Liv eller helse	Økonomi	Tiln	Etterlevelse av lov, forskrift og andre	Måloppfyllelse
Svært alvorlig	Drøtt eller flere personer dømt av alvorlig sykdom, funksjonsnedsettelse eller skade.	Tap/ubest på over 1 mill. kroner for virksomheten.	Langevare og svært negativ oppslag i medier/brukertryk.	Kan medføre alvorlig tap av informasjon på liv, helse, forsikring eller annet regelverk.	Manglende oppfyllelse av kritiske mål i dokumentasjon.
Alvorlig	Alvorlig personskade eller alvorlig sykdom.	Tap/ubest mellom 1 og 1 mill. kroner for virksomheten.	Negativ oppslag i medier/brukertryk.	Kan medføre alvorlig tap av informasjon på liv, helse, forsikring eller annet regelverk.	Manglende oppfyllelse av viktige mål i dokumentasjon.
Moderat	Mindre alvorlig personskade.	Tap/ubest mellom 250.000 til 1 mill. kroner for virksomheten.	Moderat og kortvarig oppslag i medier/brukertryk.	Kan medføre alvorlig tap av informasjon på liv, helse, forsikring eller annet regelverk.	Moderat innbrudd i oppfyllelse av viktige mål i dokumentasjon.
Lav	Utskuddet.	Tap/ubest mellom 50.000 og 250.000 kroner for virksomheten.	Hverken alvorlig eller negativ oppslag i medier/brukertryk.	Kan medføre alvorlig tap av informasjon på liv, helse, forsikring eller annet regelverk.	Uten innbrudd i oppfyllelse av viktige mål i dokumentasjon.
Ubetydelig	Ingen skade.	Tap/ubest på mindre enn 50.000 kroner for virksomheten.	Ubeskyddet på kortvarig oppslag i medier/brukertryk.	Flukter ikke etter regelverk.	Utslipp av informasjon til virksomhetsinterne mål.

Sannsynlighetskriterier for informasjonssikkerhet – v1.0					
	Forekomst	Estimert sannsynlighet	Sikkerhet	Kapasitet og øvne	Integritet
Svært alvorlig	Utenfor 3 års sikt, svært alvorlig.	Mer enn 100 ganger per år.	Ikke sikkerhet.	Ikke kapasitet og øvne.	Ikke integritet.
Alvorlig	Utenfor 3 års sikt, alvorlig.	Mer enn 10 ganger per år.	Ikke sikkerhet.	Ikke kapasitet og øvne.	Ikke integritet.
Moderat	Utenfor 3 års sikt, moderat.	Mer enn 10 ganger per år.	Ikke sikkerhet.	Ikke kapasitet og øvne.	Ikke integritet.
Lav	Utenfor 3 års sikt, lav.	Mer enn 10 ganger per år.	Ikke sikkerhet.	Ikke kapasitet og øvne.	Ikke integritet.
Høyt	Utenfor 3 års sikt, høyt.	Mer enn 10 ganger per år.	Ikke sikkerhet.	Ikke kapasitet og øvne.	Ikke integritet.

Konsekvens- og sannsynlighetskriterier

Regneark for risikovurdering



Mal for sluttrapport

	Styring				Etterlevelse	Felles løsninger		
Aktivitet	IRHS	Ansvar	ROS	Rolle	DPIA	Plattformer	Eggsystem	
Standardisere	Pilgr	LG/VE	De facto mal	Koordinatorer	De facto mal	Pilgring & brukertilgang	O365, arkiv, HR ++	
Veilede	Planlagt	Maier	Maier	Rollekort	Om malen	Intranett	Intranett	
Holde kurs	Dikterne	-	3-4 årlig	-	Flere årlig	-	O365 ++	
Nettverk / Forum	-	Forum Q2	Forum orientering	Forum orientering	Nettverk og koordinere	Arkitektur forum	- forum	

Personvern vurdering 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 Personvernkonsekvensvurdering ved lav/middels risiko (PLM)

➔ A ELLER B

B Personvernkonsekvensvurdering 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

a. Samtykke

b. Avtale

c. Rettslig forpliktelse

[Dette behandlingsgrunnlaget vil kreve supplerende rettsgrunnlag.]

d. Vitale interesser til den registrerte eller en annen fysisk person

e. Allmenhetens interesse eller utøvelse av offentlig myndighet som den behandlingsansvarlige er pålagt.

Behandlingsgrunnlag for særlige kategorier personopplysninger etter GDPR art. 9

a. Samtykke

b. Forpliktelser og rettigheter for den behandlingsansvarlige eller den registrerte på området arbeidsrett, trygderett og sosialrett.

[Dette behandlingsgrunnlaget vil kreve supplerende rettsgrunnlag.]

c. Vitale interesser til den registrerte eller en annen fysisk person, dersom samtykke ikke kan gis

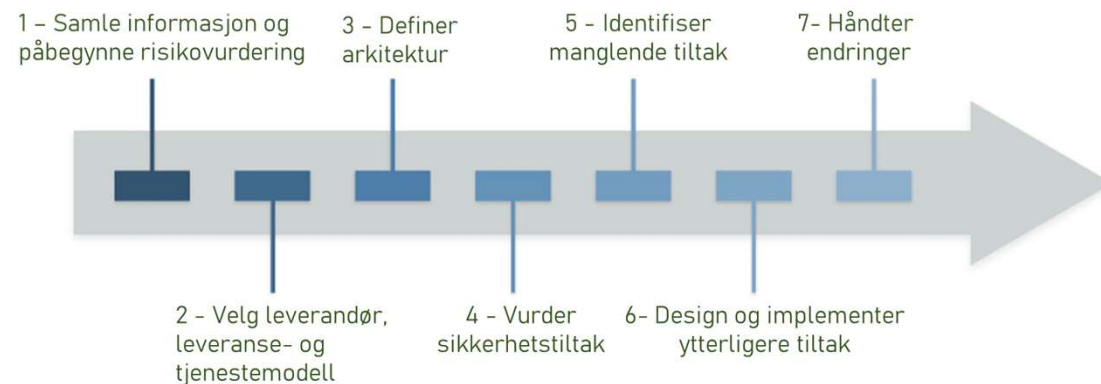
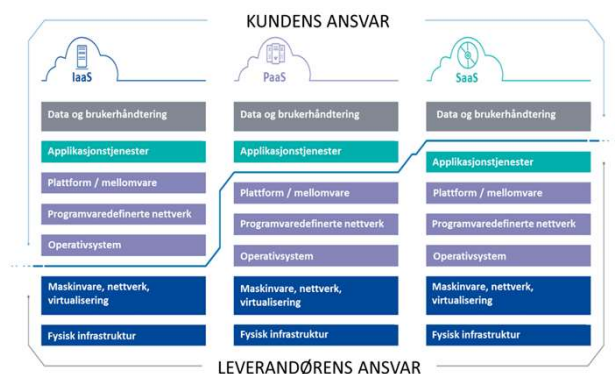
d. Behandlingen utføres av en stiftelse, sammenslutning eller et annet ideelt organ hvis mål er av politisk, religiøs eller fagforeningsmessig art

e. Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte har offentliggjort

Aktivitet	Styring				Etter- levetide	Felles løsninger	
	ISHS	Arbeids- møte	ROS	Rolleskema	SI/A	Plattform	Flagsystem
Standardisere	Plaggr	LG/VE	De facto mal	Koordinatorer	De facto mal	Pilgging & brukertilgen	O365, arkiv, HR ++
Veilede	Planlagt	Maler	Maler	Rollekort	Om malen	Intranett	Intranett
Holde kurs	Dikterne	-	3-4 Årlig	-	Flere Årlig	-	O365 ++
Nettverk / Forum	-	Forum Q2	Forum orientering	Forum orientering	Nettverk og koordinering	Arkitektur forum	forum

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



Aktivitet	Styring				Etter-levetide	Felles løsninger	
	ISHS	Ansvar	ROS	Roller		DPIA	Plattformer
Standardisere	Pilgr	LG/VE	De facto mal	Koordinatorer	De facto mal	Pilgging & brukertilgng	O365, arkiv, HR **
Hold 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
- ▶ Sikkerhetsmåned
- ▶ E-læringer og anti-phishing program



Aktivitet	Styring				Etterlevelse	Felles løsninger	
	ISO/IEC	Arbeidsplan	ROS	Roller		SI/SA	Plattform
Standardisere	Pilgr	LG/VE	De factum	Koordinatorer	De factum	Pilgring & brukertilgang	O365, arkiv, HR ++
Hold 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

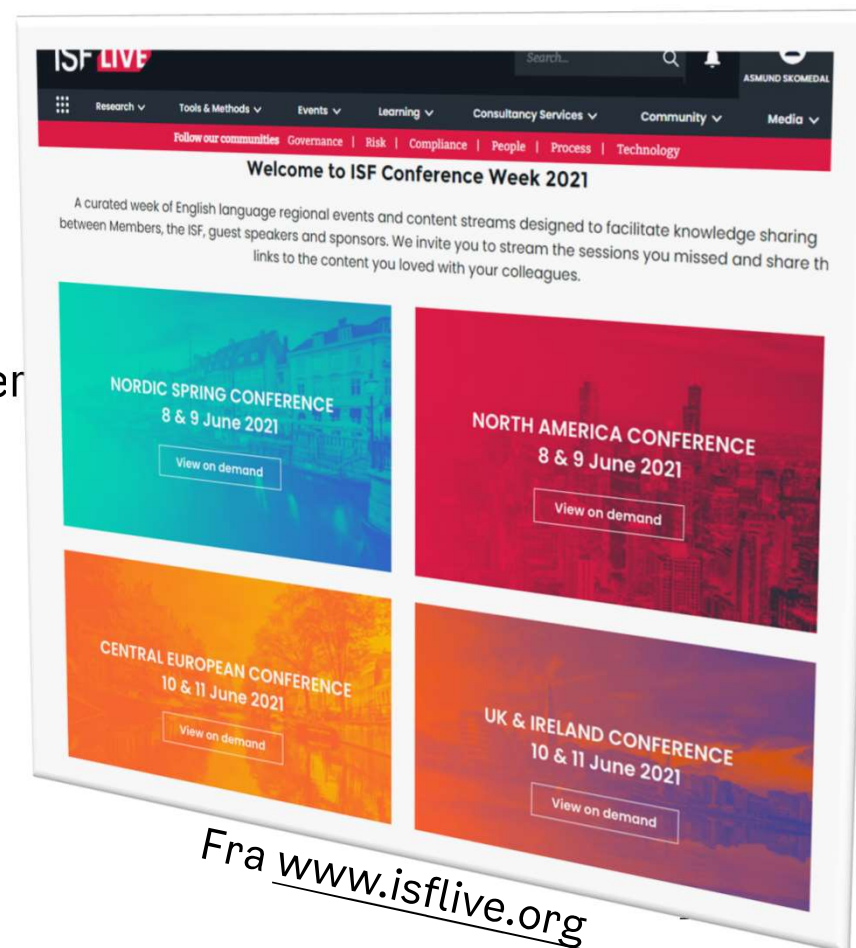
➤ Inkludert i medlemskapet:

- All dokumentasjon på metoder og verktøy
- Konferanser, seminarer og opplæringsmateriale

➤ Noen kurs og konsulenttjenester må betales for



Oslo



The image features a futuristic, blue-toned digital interface. On the right side, there is a large, glowing padlock icon, symbolizing security or a locked state. The background is filled with various digital elements, including data streams, grid patterns, and abstract shapes, creating a sense of a complex, high-tech environment. The overall aesthetic is clean and modern, with a strong emphasis on the color blue.

Let's be careful out there!

Foto: irpp.org, Creativ