Asker kommune

Felles anbefalinger for styringsaktiviteter i Asker kommune

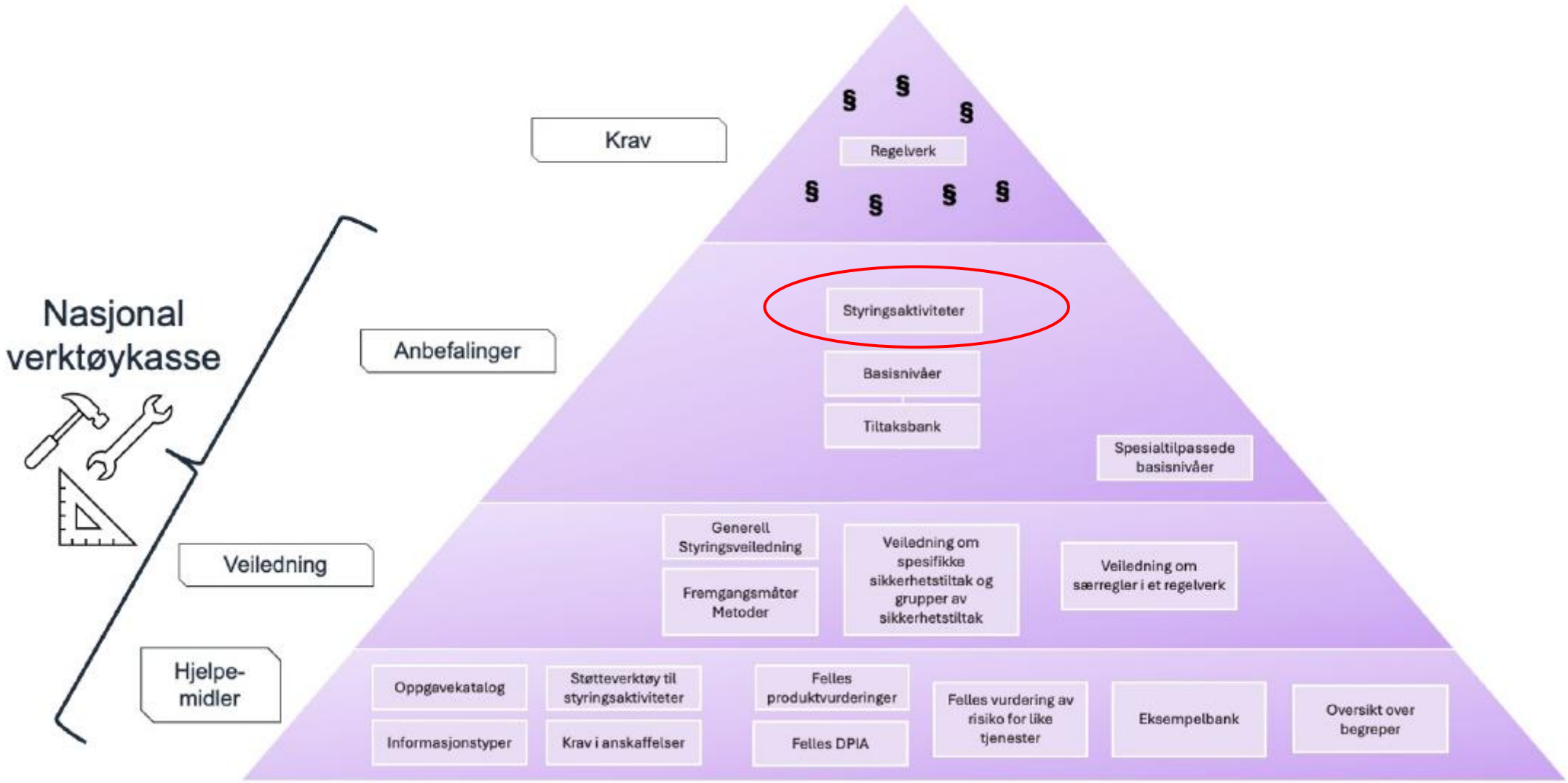
«**Styring av informasjonssikkerhet og personopplysningsvern**»

NIFS / 11-02-2026 / Pål A. Gaure

Tid for praksis – ikke detaljer om styringsverktøy for risikoeiere (selv om det er dit vi skal)

- Superkort repetisjon av SIP
- Kort om virksomhetsstyring i Asker kommune
- SIP erstatter «Policy for informasjonssikkerhet»
- SIP kopieres direkte inn i kvalitetssystemet
- SIP brukes som evalueringsverktøy av eget arbeide
- Datadrevet styring av informasjonssikkerhet og personopplysningsvern
- Spørsmål

Figur 1 – Nasjonal verktøykasse



Figur 1 – Nasjonal verktøykasse – produktmålbildet

Offentlig

Introduksjon

Disse sidene gir anbefalinger til offentlige virksomheter om hvilke styringsaktiviteter de bør ha. Målet er at ledelsen skal kunne ivareta ansvaret sitt.

→

Ledelsens styring og oppfølging (LS)

Virksomhetens leder skal sørge for god styring og kontroll i virksomheten, inkludert ivaretakelse av tilstrekkelig informasjonssikkerhet og personopplysningsvern.

→

Ha oversikt og prioritere (OP)

Alle risikoeiere i virksomheten skal ha god oversikt over sine ansvarsområder, slik at arbeidet med styring av informasjonssikkerhet og personopplysningsvern gjøres effektivt ...

→

Vurdering av risiko (RV)

Risikoeiere skal sørge for å ha tilstrekkelig oversikt over risiko knyttet til informasjonssikkerhet og personopplysningsvern på sitt ansvarsområde, og vite hvilke risikoer...

→

Håndtering av risiko (RH)

I forlengelse av risikovurderinger, skal virksomheten beslutte hvordan de identifiserte risikoene skal håndteres. Det må avklares om det finnes aktuelle tiltak for å redusere risikoen, eller om den bør...

→

Måling, evaluering og revisjon (ME)

Virksomhetens ledere skal ha innsikt i status på arbeidet med informasjonssikkerhet og personopplysningsvern, og om de har tilstrekkelig oversikt over risiko på sitt...

→

Overvåking og hendelseshåndtering (OH)

Virksomheten skal være i stand til å oppdage og reagere på uønskede hendelser. Feil, avvik og uønskede hendelser skal avdekkes og følges opp, for å redusere konsekvensen og lære av...

→

Kompetanse- og kulturutvikling (KK)

Informasjonssikkerhet og personopplysningsvern involverer mange roller og krever ulike typer kompetanse, fra virksomhetsstyring og risikostyring til regelverkforståelse, tiltak og teknisk...

→

Anskaffelser og leverandørstyring (AL)

Virksomheten skal ivareta krav til informasjonssikkerhet og personopplysningsvern i anskaffelser.

→

Kommunikasjon (KO)

Ledere på alle nivå skal sørge for god og tydelig kommunikasjon, som setter virksomheten i stand til å jobbe helhetlig med informasjonssikkerhet og personopplysningsvern.

→

Sikkerhetsmål må ta utgangspunkt i kommunens «virksomhetsstyring»

«Den røde tråden» - hvor finner vi den...?

Tydelighet fra mål til måling

Mål:
Hvor skal vi?

Hovedmål

Overordnet mål for satsings-området. Verbalt beskrevet.

Delmål

Delmål utledet fra hoved-målet. Verbalt beskrevet.

Handling:
Hvordan kommer vi dit?

Strategi

Fremgangsmåter/veivalg/ endringer for å nå målet

Oppdrag

Oppdragsbrev til virksomhetene

Tiltak

Konkret handling for å nå målene

Resultat:
Hvordan går/gikk det?

Indikatorer og måling

Aktivitet eller resultat som faktisk lar seg måle.

Analyse

Analyse/vurdering av mål-oppnåelsen.

Rapportering

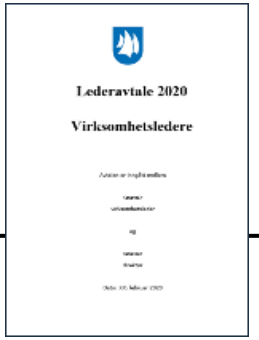
Det må implementeres i organisasjonen

Temaplaner

Oppdragsbrev til virksomhetene

Framsikt

Virksomhetsplan



- 8 hovedmål
- 28 delmål
- 87 strategier

- Utarbeides fra 2020 og utover.

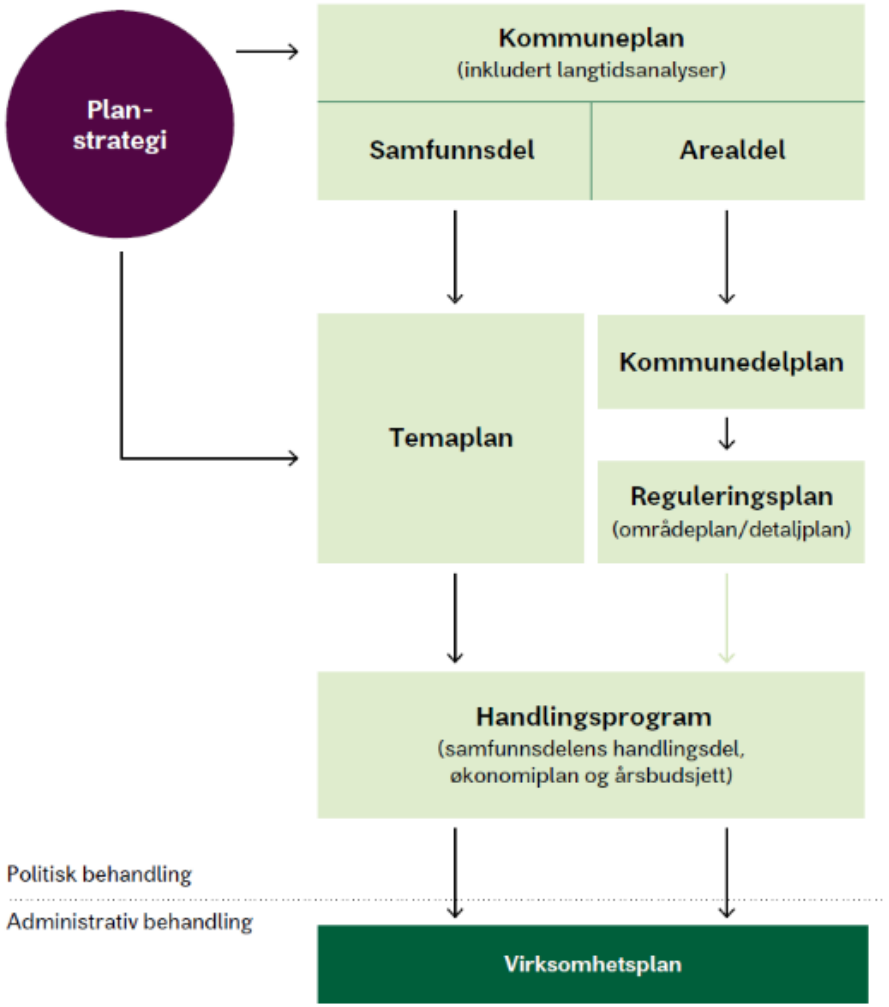
- **Målene fordeles** på tjenesteområdene
- **Prioriteringer** i perioden
- Drifts- og investeringstiltak

- Sendes fra kommunedirektøren til virksomhetene etter budsjett-vedtaket i desember
- Gir virksomhetene **rammer og føringer** for iverksettelsen av handlingsprogrammet
- Inneholder **oppdrag** til virksomheten

- Inneholder virksomhetens mål
- Virksomhetene skal selv definere **konkrete tiltak** ut fra gitte oppdrag

Måling gjennom styringsverktøy

TEORI/MODELL/JUS



SEMANTIKK/LOGIKK

- **Hovedmål**
- **Delmål**
- **Strategier**

- **«Henter» aktuelle mål** fra alle satsingsområder i KP
- **Strategier** for tjenesteutvikling (endringsbehovet for å nå målene og møte utfordringsbildet)

- Fordele delmålene fra KP på tjenesteområdene
- **Prioriteringer i perioden** – for å nå mål og løse utfordringer
- Drifts- og investeringstiltak

- **Tiltak** – konkrete handlinger i virksomhetene

TEKNIKK/ SYSTEM

Framsikt

Simpli

Prosjekt-portalen

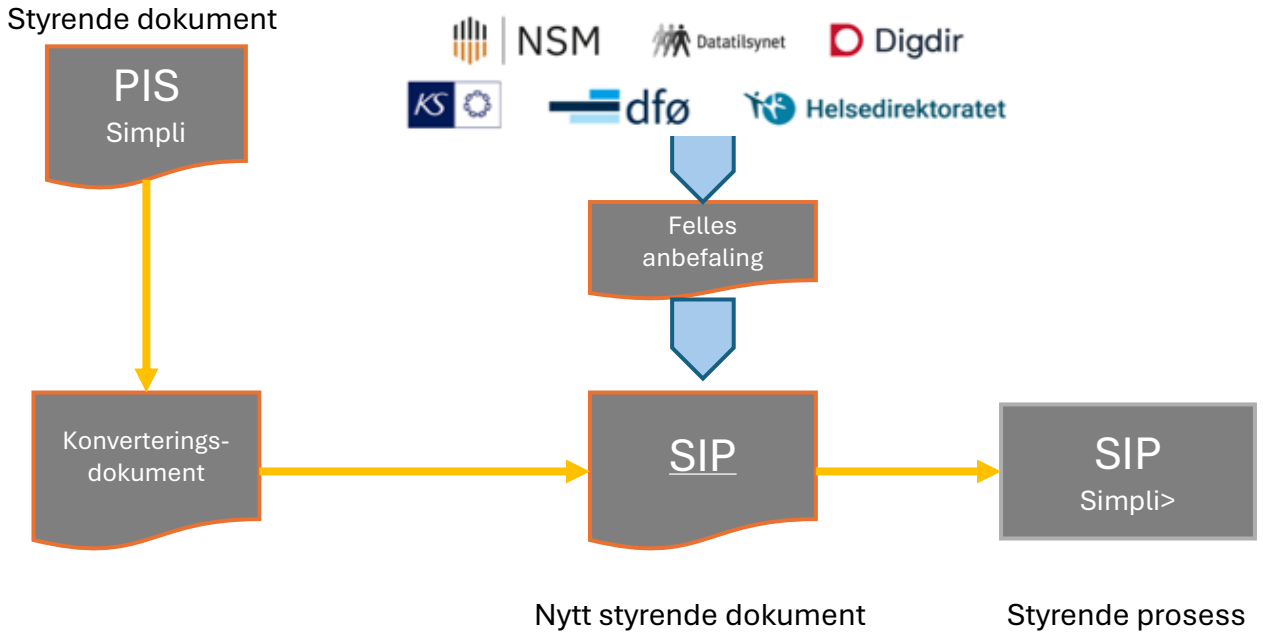
Agresso

BI-løsninger

etc..

Tiltak1 i forvaltningsrevisjonen Asker kommune

(utbedre styringssystem basert på Digdirs veiledning – innhold, ikke internalisering i organisasjonen)



Styringsinformasjon

LS- Ledelsens styring og oppfølging
OP - Ha oversikt og prioritere
RV - Vurdering av risiko
RH - Håndtering av risiko
ME - Måling, evaluering og revisjon
OH - Overvåking og hendelseshåndtering
KK Kompetanse- og kulturutvikling
AL - Anskaffelser og leverandørstyring
KO - Kommunikasjon
10 Etableringsaktiviteter

Neste lysark viser hvordan vi har tatt hele **Felles anbefalinger for styringsaktiviteter** inn i kvalitetssystemet som styringssystem for informasjonssikkerhet.
Slik at dokumentet Policy for informasjonssikkerhet (PIS) **ikke lenger behøves.**

Ha oversikt og prioritere (OP)

Alle risikoeiere i virksomheten skal ha god oversikt over sine ansvarsområder, slik at arbeidet med styring av informasjonssikkerhet og personopplysningsvern gjøres effektivt ...

→

Styring av Informasjonssikkerhet | Ha oversikt og prioritere

Prosess: Identifisere risiko	Prosesseier: Pål Alexander Gaure	Godkjent av: Pål Alexander Gaure	Godkjent dato: 6.11.2025	Publisert versjon: 2

Alle risikoeiere i virksomheten skal ha god oversikt over sine ansvarsområder, slik at arbeidet med styring av informasjonssikkerhet og personopplysningsvern gjøres effektivt og målrettet.

Risikoeiere skal være i stand til å organisere og prioritere arbeidet med informasjonssikkerhet og personopplysningsvern. Dette inkluderer blant annet å beslutte hvor det er behov for å gjennomføre risikovurderinger.

Oversikten vil være nyttig for virksomhetens helhetlige arbeid med beredskap og virksomhetskontinuitet, og bør benyttes til dette.

En helhetlig oversikt for hele virksomheten kan bygges opp gradvis etter hvert som disse aktivitetene gjennomføres. En samlet oversikt gir en felles forståelse av hvilke oppgaver og tjenester som er mest kritiske på tvers av organisasjonen, og danner grunnlag for enhetlig prioritering av tiltak.

Utvid / skjul hele teksten

Aktiviteter

- Oversikt over ansvarsområde
- Kartlegge eksterne krav
- Vurdere behov for risikovurderinger
- Oppdatert oversikt over risikovurderinger

Oversikt over ansvarsområde

Godkjent dato: 16.1.2026 | Versjon: 2

Risikoeiere skal opprette og vedlikeholde en oversikt av eget ansvarsområde. Denne foranalysen skal gi oversikt over hvilken betydning informasjonsbehandlingen har for oppgaver og tjenester, og bør omfatte:

Oversikt over
- oppgaver og tjenester som utføres
- hvilken informasjon som behandles i oppgaver og tjenester, inkludert hvilke personopplysninger som behandles
- formål med behandling av personopplysninger, behandlingsgrunnlag og behandlingsansvar
- overføring av personopplysninger utenfor EØS og overføringsgrunnlag som benyttes
- digitale systemer og digitale tjenester som benyttes, inkludert avhengigheter til eksterne tjenester

En vurdering av hvor store konsekvensene ved brudd på informasjonssikkerhet eller personopplysningsvern kan bli, for virksomheten og for eksterne parter
Vedlikehold av protokoll over behandlingsaktiviteter, med informasjon om behandling av personopplysninger
En gjennomgang av vesentlige trusler, farer og sårbarheter

Gir evne til
- å ha oversikt over hvor viktig ulike oppgaver og tjenester er for virksomheten
- å vurdere behov for risikovurderinger, og prioritere ressursbruken på arbeidet med informasjonssikkerhet og personopplysningsvern
- å ha oversikt over all behandling av personopplysninger

Hvem
Risikoeiere på alle nivåer ned til virksomhetsledere

Hvordan og når
Virksomhetsledere løpende ved å følge med på indikatorer, som er beskrevet i...

Styring av Informasjonssikkerhet | Vurdering av risiko

Prosess: Vurdering av risiko	Prosesseier: Pål Alexander Gaure	Godkjent av: Pål Alexander Gaure	Godkjent dato: 29.1.2026	Publisert versjon: 1

Risikoeiere planlegger og gjennomfører risikovurderinger på sitt ansvarsområde, for å styre risiko på oppgaver og tjenester.

Avhengig av hvor stort og komplekst ansvarsområdet er, bør risikoeier benytte resultatet av foranalysen til å dele opp området i hensiktsmessige deler, eller gruppere deler som kan vurderes sammen.

Vurdering av risiko gjennomføres systematisk og planlagt (ref. Vurdere behov for risikovurderinger (OP-3)), men også når det oppstår særskilt behov – for eksempel etter hendelser eller i forbindelse med endringer i oppgaver og tjenester, inkludert anskaffelser og utvikling av digitale systemer.

Aktiviteter

- Planlegge risikovurdering
- Vurdere personvernkonsekvensvurdering (DPIA
- Gjennomføre risikovurdering
- Vurdere risiko etter hendelser

Relevante dokumenter | Kravområde

Vurdere personvernkonsekvensvurdering (DPIA)

Gjennomføre risikovurdering

Godkjent dato: 10.2.2026 | Versjon: 1

Risikoeiere skal sørge for at nødvendige risikovurderinger og personvernkonsekvensvurderinger blir gjennomført. Omfang og praktisk gjennomføring må tilpasses det som skal vurderes. Risikoeier skal sørge for at metodene som benyttes er egnet til det som skal vurderes, og ivaretar relevante regelverkskrav.

Risikoeiere skal benytte resultatet fra foranalysen i Oversikt over ansvarsområde (OP-1) når de vurderer risiko.

Når vurderinger oppdateres kan det være tilstrekkelig å vurdere om det har skjedd endringer som påvirker eksisterende vurderinger. For eksempel ny kunnskap om sårbarheter, hvilke hendelser som kan inntreffe, eller hvilke konsekvenser som kan oppstå.

Risikovurderingen skal dokumenteres, og danner et beslutningsgrunnlag for risikoeier for håndtering av risiko.

Gir evne til

- å få oversikt over risiko på et område (oppgave, tjeneste, digitalt system eller annen avgrensing)
- å ta beslutninger om risiko, inkludert bruk av virksomhetens ressurser på håndtering av risiko

Hvem

Hvordan og når

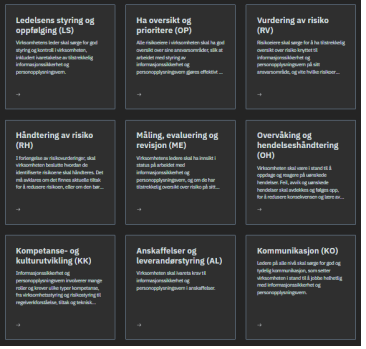
SIP beskriver:
«hvorfor» og «hva»

Asker kommune legger til:
«hvem»
«hvordan»
«når».

Utfordring:

Vi har ikke en god metode for å hente ut «hva», «hvem», «hvordan» og «når».

Det må vi løse slik at en leder eller ansatt kan hente ut sin egen gjøremålsliste direkte fra kvalitetssystemet.



Egenevaluering

basert på **internkontroll i praksis** siden 2022

sikkert.no

Ikke reelle data

måling ved utgangen av 2025	Oppstart 2022	2022	2023	2024	2025 22.8
Gjennomsnitt:	1,88	2,44	2,40	2,77	2,79
LS- Ledelsens styring og oppfølging		2,7	2,7	2,7	2,5
OP - Ha oversikt og prioritere	1,7	2,0	2,0	3,3	3,3
RV - Vurdering av risiko	2,0	2,0	2,0	2,3	2,7
RH - Håndtering av risiko	1,8	2,4	2,4	2,2	2,2
ME - Måling, evaluering og revisjon	2,3	2,3	2,0	2,8	3,3
OH - Overvåking og hendelseshåndtering	2,3	3,0	2,7	3,0	3,7
KK Kompetanse- og kulturutvikling	2,0	2,0	3,0	3,0	2,3
AL - Anskaffelser og leverandørstyring	i/a	i/a	i/a	i/a	i/a
KO - Kommunikasjon	2,0	2,4	2,4	2,5	2,1
10 Etableringsaktiviteter	2,4	2,8	2,6	3,3	3,5

OP - Ha oversikt og prioritere

							A
OP-1 Oversikt over ansvarsområde				**3**		3	
○ oppgaver og tjenester som utføres							
○ hvilken informasjon som behandles i oppgaver og tjenester, inkludert hvilke personopplysninger som behandles							
○ formål med behandling av personopplysninger, behandlingsgrunnlag og behandlingsansvar							
○ overføring av personopplysninger utenfor EØS og overføringsgrunnlag som benyttes							
○ digitale systemer og digitale tjenester som benyttes, inkludert avhengigheter til eksterne tjenester							
• En vurdering av hvor store konsekvensene ved brudd på informasjonssikkerhet eller personopplysningsvern kan bli, for virksomheten og for eksterne parter							
• Vedlikehold av protokoll over behandlingsaktiviteter, med informasjon om behandling av personopplysninger							
En gjennomgang av vesentlige trusler, farer og sårbarheter							
OP-2 Kartlegge eksterne krav					**4**	4	
Risikoeiere skal ha oversikt over de regler og avtaler som gjelder for sitt ansvarsområde							
OP-3 Vurdere behov for risikovurderinger			**2**			2	
Risikoeiere skal regelmessig vurdere behovet for oppdaterte eller nye risikovurderinger innen sitt ansvarsområde.							
OP-4 Oppdatert oversikt over risikovurderinger				**3**		3	
risikovurderinger på sitt ansvarsområde, og hvilke risikovurderinger som er planlagt.							

Vurderingskoder

Kodene benyttes i analyseskjemaet under.

I hvilken grad gjennomfører vi de systematiske aktivitetene og lager anbefalte dokumenter? (eller)
I hvilken grad har vi gjennomført etableringsaktivitetene og laget anbefalte dokumenter?

0	Ikke i det hele tatt, eller i liten grad
1	Noe samsvar i praksis eller i formaliserte krav, men behov for store forbedringer
2	En god del samsvar i praksis eller i formaliserte krav, men behov for en del justeringer og forbedringer
3	Tilstrekkelig samsvar i praksis, men mangler noe i formalisering/dokumentasjon
4	Tilstrekkelig samsvar i praksis og god formalisering/dokumentasjon. Ingen forbedring er nødvendig.

Styring av informasjonssikkerhet og personopplysningsvern (SIP) i Asker kommune

	Fremdrift oppfølging av SiP						
	Mål 1 HÅ26	**2026**	Diff 1 HÅ 26	06.01.2026	28.02.2026	30.04.2026	30.06.2026
LS- Ledelsens styring og oppfølging	2,80	2,20	-0,60	**2,2**			
OP - Ha oversikt og prioritere	3,30	3,00	-0,30	**3,0**			
RV - Vurdering av risiko	3,30	2,50	-0,80	**2,5**			
RH - Håndtering av risiko	2,00	1,25	-0,75	**1,3**			
ME - Måling, evaluering og revisjon	2,50	2,00	-0,50	**2,0**			
OH - Overvåking og hendelseshåndtering	3,75	3,75	0,00	**3,8**			
KK - Kompetanse- og kulturutvikling	2,33	1,67	-0,66	**1,7**			
AL - Anskaffelser og leverandørstyring	2,60	1,20	-1,40	**1,2**			
KO - Kommunikasjon	2,50	2,25	-0,25	**2,3**			
10 Etableringsaktiviteter	3,13	3,00	-0,13	**3,0**			

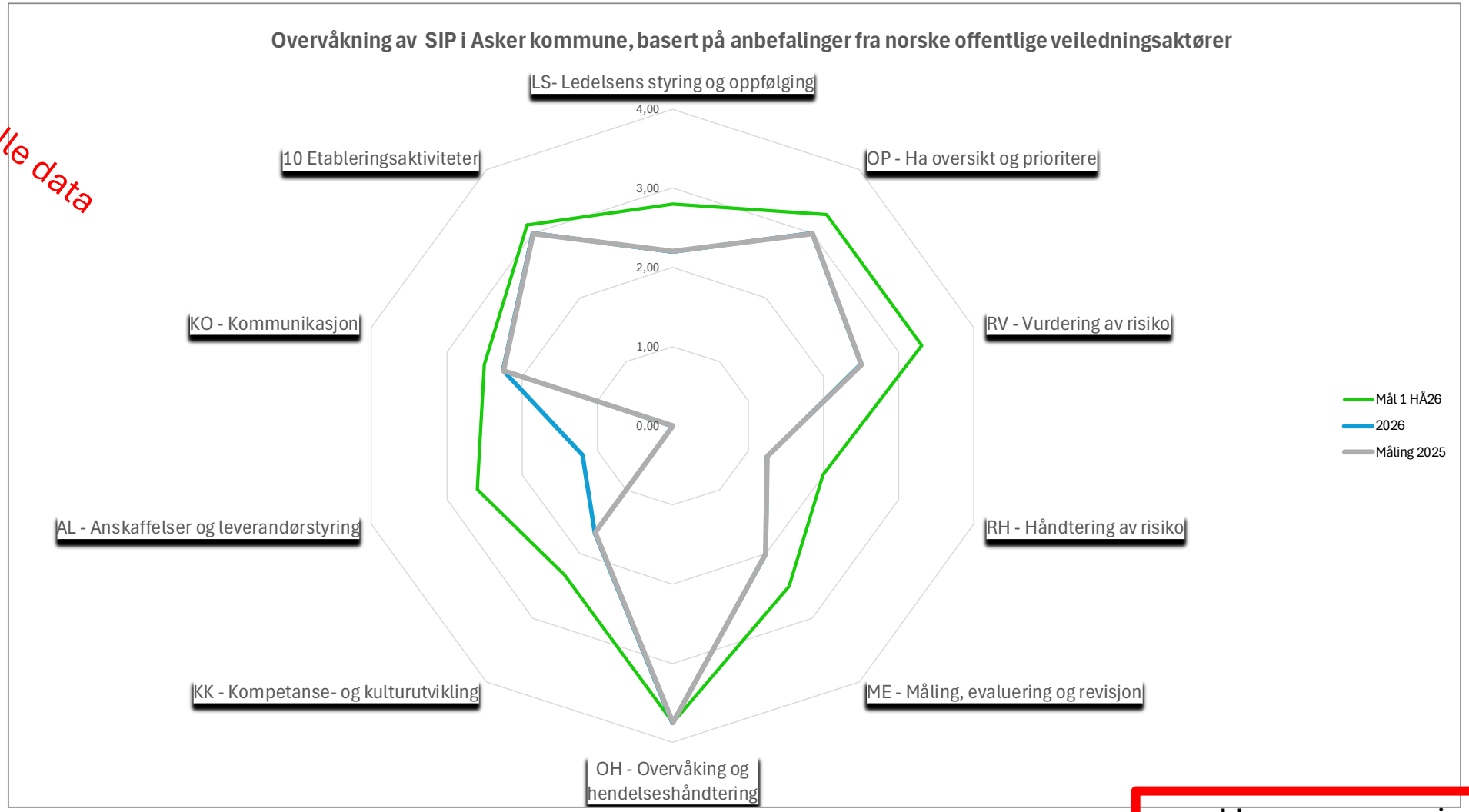
Ikke reelle data

https://nsm-xp7test.enonic.cloud/offentlig

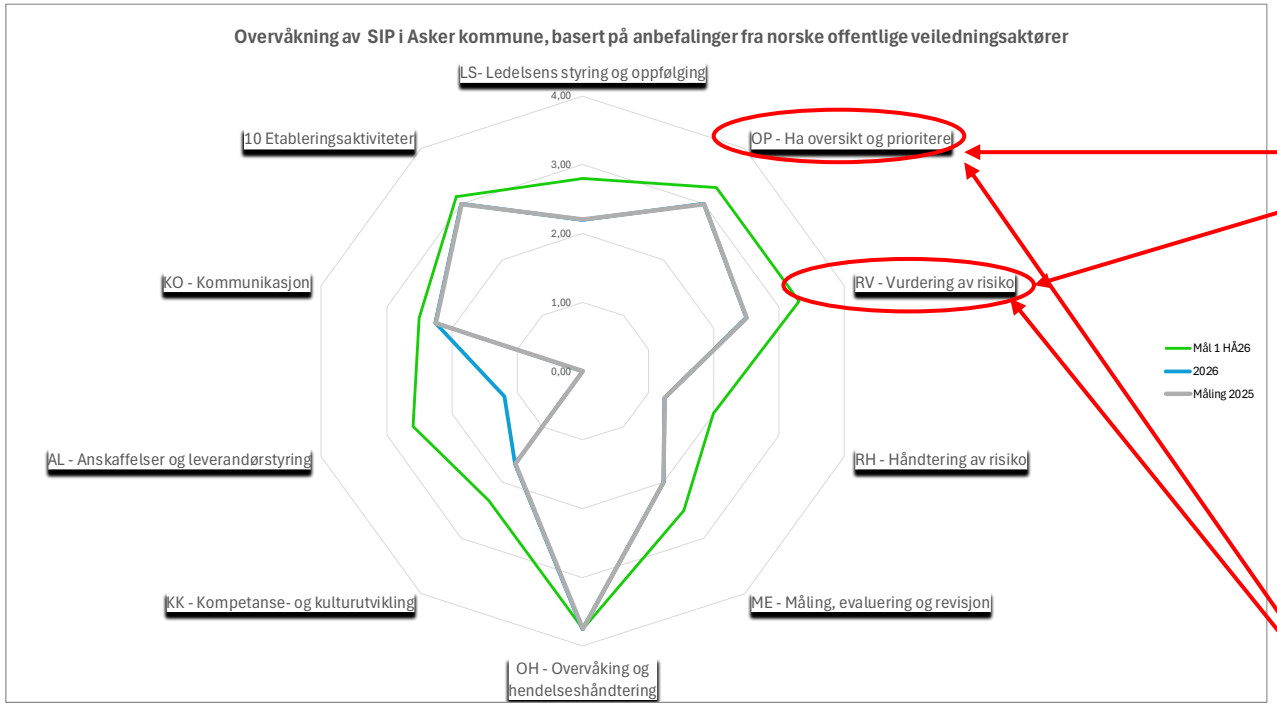
Overvåkning av SIP I Asker kommune

Mål første halvår 2026, vist mot faktisk skår gjennom 2026

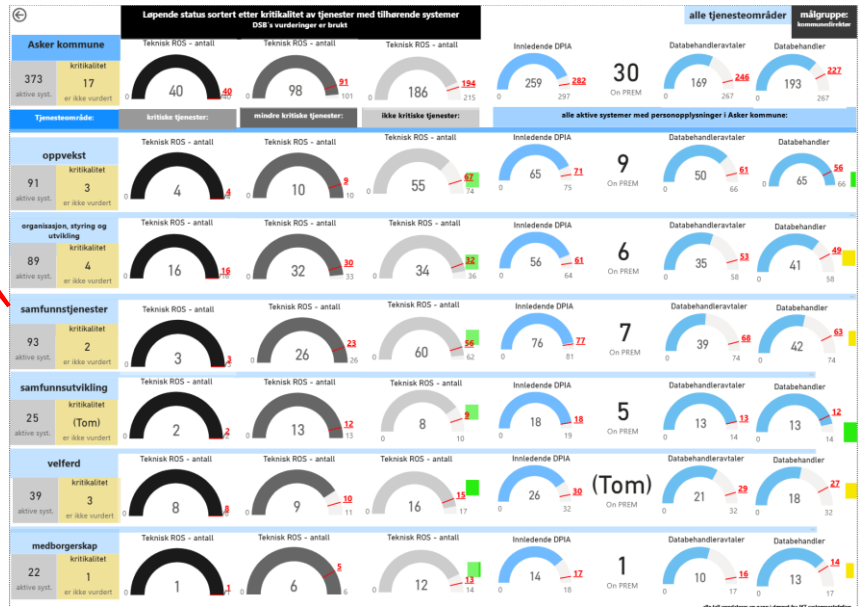
Ikke reelle data



Hva er operasjonalisert (digitalisert og automatisert) av disse styringsaktivitetene?



Ikke reelle data



Bruke data fra behandlingsprotokoll og «systemlister» for automatisk skår av OP og RV

Asker kommune

Litt tid til spørsmål?

Asker kommune

Takk for meg

Asker / 11-02-2026 / Pål A. Gaure

Neste NIFS-møte

- Tema: Øvelser
- Dato: 27. mai 2026

infosikkerhet@digdir.no

Neste NIFS-møte:
Dato 27. mai 2026
Øvelser

Spørsmål?
infosikkerhet@digdir.no

digdir.no

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

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