



Asker
kommune

På vei mot sikkerhetsstyring som er integrert i virksomhetsstyringen

En praktisk tilnærming fra data via styringsinformasjon til
beslutninger tatt av den som eier risikoen

Normkonferansen 2026 – Pål A. Gaure

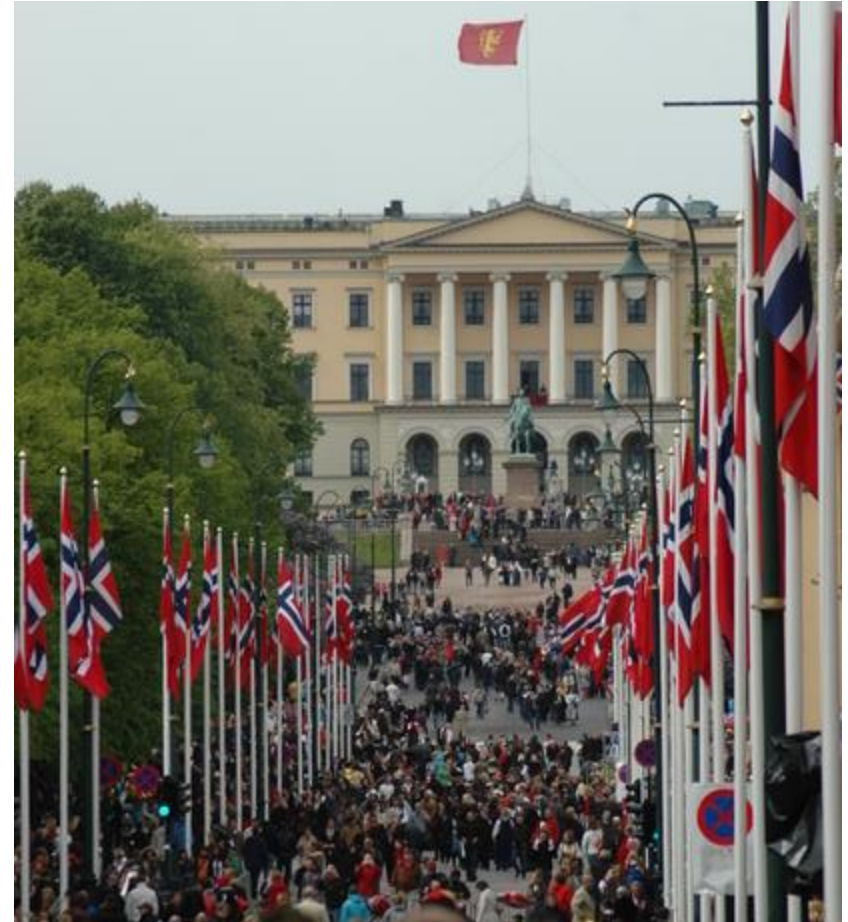


Hva får
dere nå?



Enkelte illustrasjoner i denne presentasjonen kan være KI-generert

Felles retning...?



Bunader og fag – respekt for egenart er viktig!



Valg av styringsmetode - bakgrunn



Løse problemene i FSIF-forarbeidene

- **P2** | Mangler grunnleggende sikkerhetstiltak
- **P4** | Må til en viss grad gjøre de samme vurderingene
- **P5** | Mangelfull forvaltning av sikkerhetstiltak
- **P7** | Arbeidet er ressurskrevende
- **P6** | Arbeidet er kompetansekrevende
- **P12** | Vanskelig å få til helhetlig tilnærming i virksomhetene



Nasjonal digitaliseringsstrategi 2024-2030

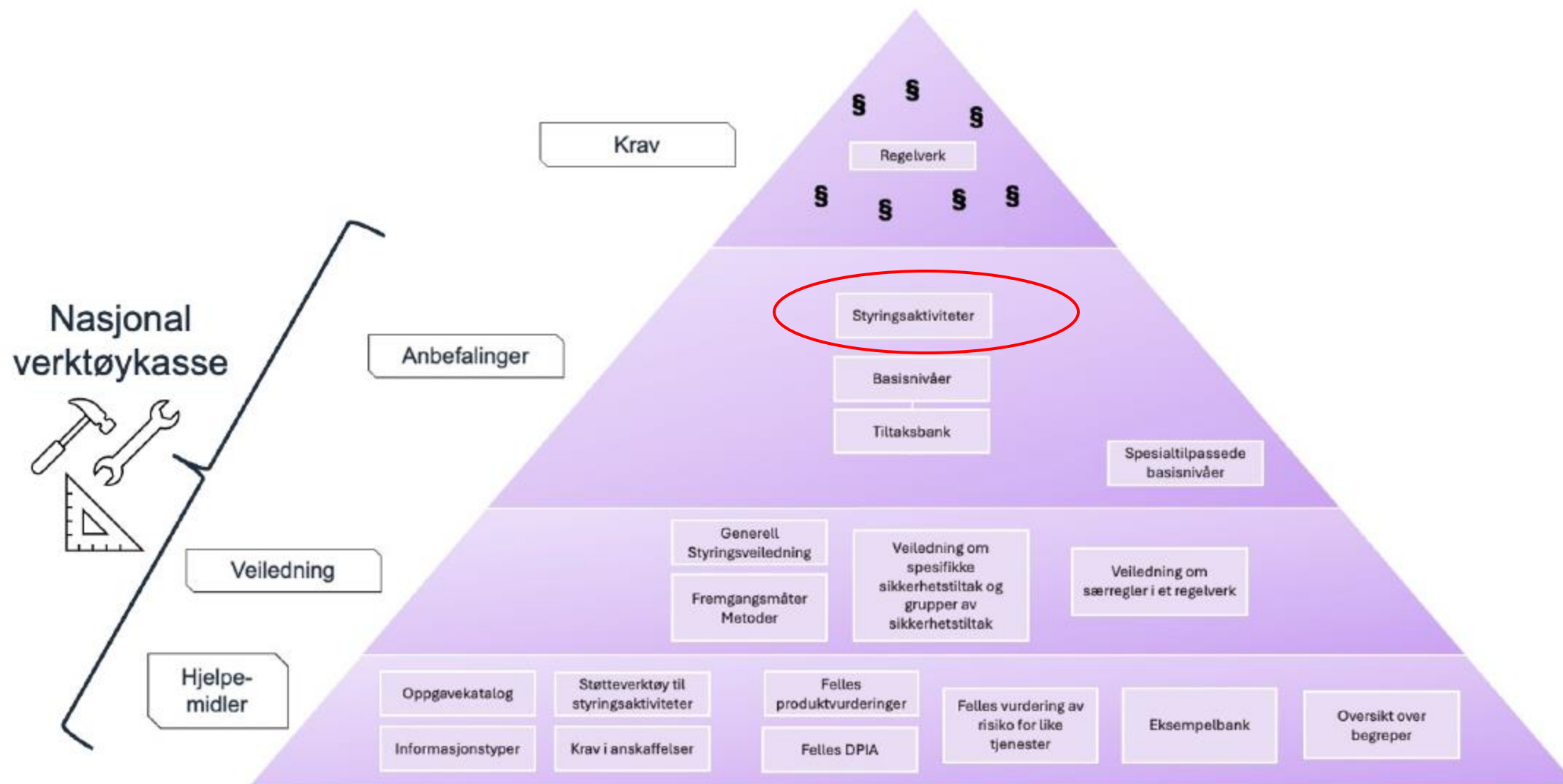
- Det er et mål å samordne og forenkle forvaltningens tilgang til råd og veiledning om digital sikkerhet og nødvendige tiltak for grunnsikring.
- Regjeringen vil samordne råd- og veiledningsressurser innenfor digital sikkerhet bedre.
- Mål 2030: Alle statlige virksomheter har evaluert, forbedret eller fornyet styringssystemet for informasjonssikkerhet.
- Mål 2030: 90 prosent av kommuner har evaluert, forbedret eller fornyet styringssystemet for informasjonssikkerhet.



Målbildet «felles plattform for samordnet innsats»

- ❖ Virksomhetene har velfungerende styring av informasjonssikkerhet og personopplysningsvern
- ❖ Virksomhetene har gode rammebetingelser for arbeidet med informasjonssikkerhet og personopplysningsvern, inkludert resultatorienterte anbefalinger og et helhetlig og brukerorientert veiledningstilbud
- ❖ God informasjonssikkerhet og personopplysningsvern på tvers av hele forvaltningen
- ❖ Tydeligere rammer for informasjonssikkerhet og personopplysningsvern i tjenesteutvikling i felles økosystem
- ❖ Legge til rette for effektivt arbeid med informasjonssikkerhet og personopplysningsvern
- ❖ Tilsynsvirksomheter har god oversikt over gjeldende anbefalinger
- Legge til rette for tillit og samarbeid mellom virksomheter og evne til samstyring av risiko for sammenhengende tjenestekjeder og deling av data
- Effektive offentlige anskaffelser der krav til informasjonssikkerhet og personopplysningsvern er av vesentlig betydning

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.



Offentlig

Styring av informasjonssikkerhet og personopplysningsvern

→

 sikkert.no

Ledelsens styring og oppfølging (LS)

Virksomhetens leder skal sørge for god styring og kontroll i virksomheten, inkludert ivaretagelse 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 bær...

→

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 hendeshåndtering (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.

→

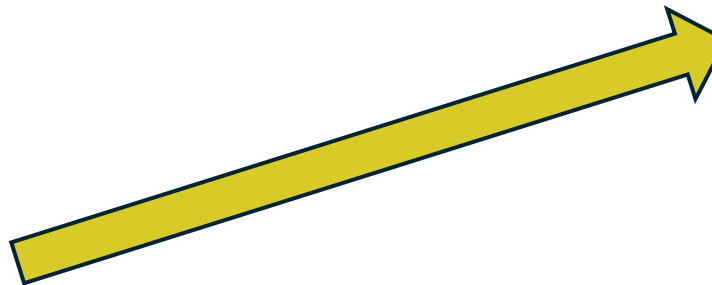


Samlet hele konseptet i et hefte

Hefte lansert i 2019.



Ferdig
oppdatert
med sikkerhet
i
2027?



 sikkert.no

Last ned «Styring av informasjonssikkerhet og personopplysningsvern»

Her kan du laste ned informasjonen i dokumentformat.

 Last ned PDF

Gi meg rss/api

vann over hodet?| hvordan løse gode tanker i praksis

Asker kommune gjør dette i 2026

 Planner

 **Planner**

Bytte systemer

 Legg til oppgave

- ☐ Nytt styringssystem for informasjonssikkerhet **DONE!**
- ☐ Nytt kvalitetssystem **mai 26**
- ☐ Nytt intranett **mai 26**
- ☐ Alt beriket med KI-agenter **mai 26**

Fra system til tjeneste

 Legg til oppgave

- ☐ Behandlingsaktiviteter støttes av
 - ☐ Systemer
 - ☐ Integrasjoner
 - ☐ Andre tekniske og ikke-tekniske løsninger

✓ 0 / 3
- ☐ Behandlingsprotokoller bygges
- ☐ Behandlingsaktiviteter defineres på nytt
- ☐ Fra system til tjeneste mot innbygger
- ☐ Alt med berikelse av KI-agenter

Fra data til styringsinfo

 Legg til oppgave

- ☐ Dette må defineres i ny moodell
 - ☐ Fellessikring
 - ☐ Tilleggssikring

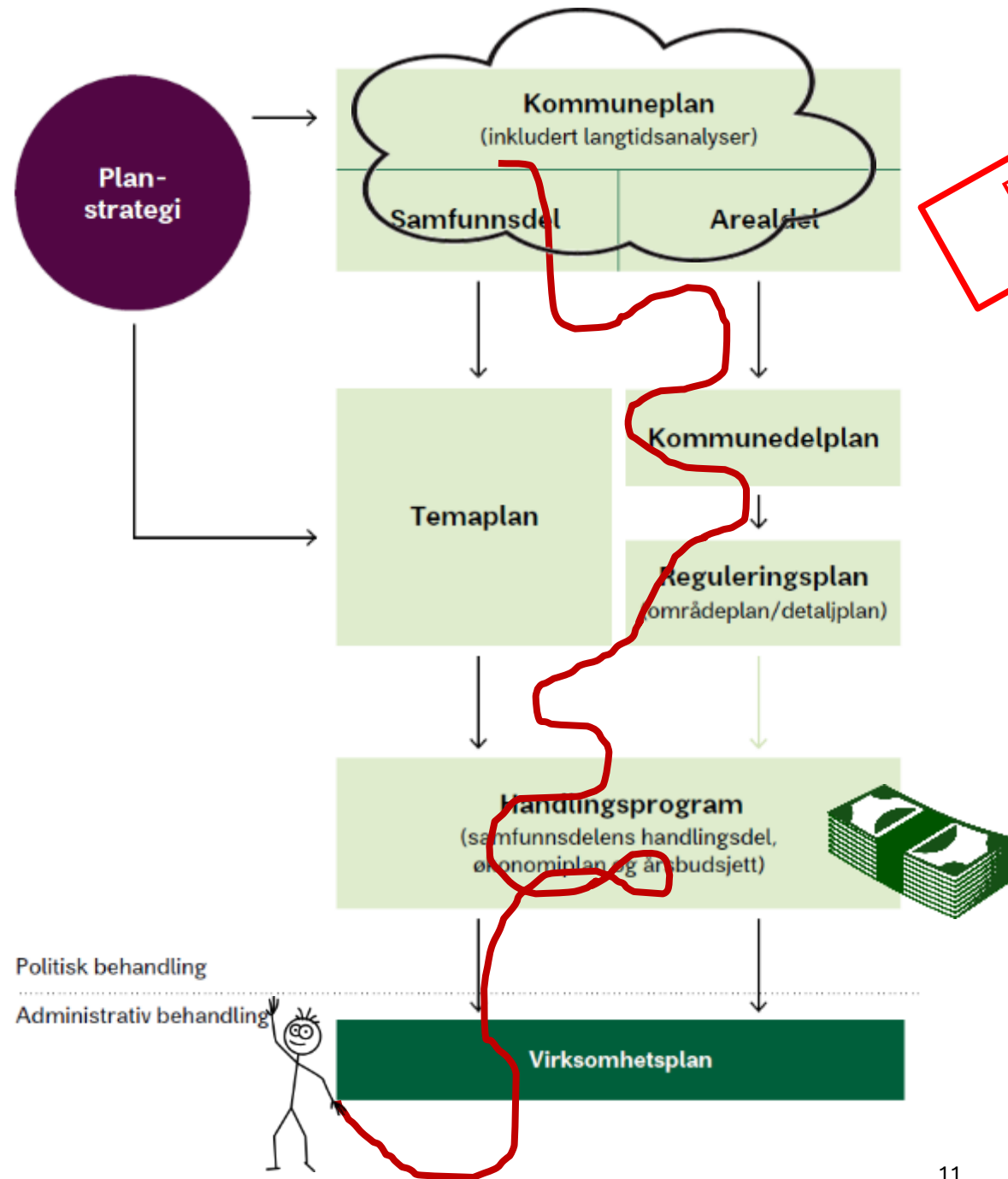
✓ 0 / 2
- ☐ Nye moduler ROS / DPIA
 - ☐ Risiko på riktig nivå
 - ☐ Risiko akkumulert opp til riktig nivå
 - ☐ Risiko må presenteres for beslutningstager p

✓ 0 / 3
- ☐ Alt beriket med KI-genter
 - ☐ For beslutningsstøtte og

✓ 0 / 1

Planlegging

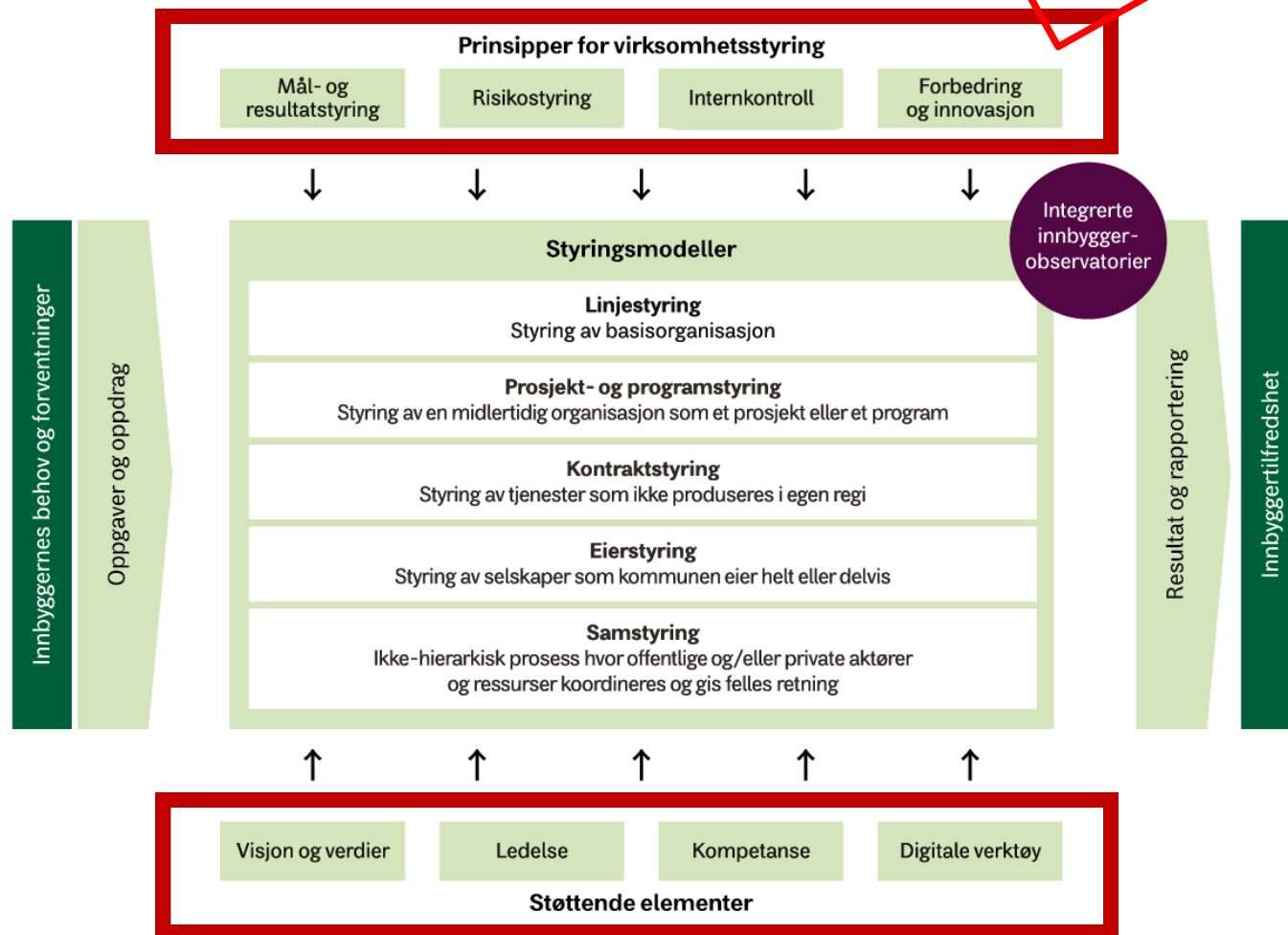
Grunnlaget for
helhetlig styring og
oppfølging, viser
veien fra visjoner til
aktiviteter og tiltak



Repetisjon fra
foredrag 1

Styring

Å styre innebærer
å *organisere* og
koordinere aktiviteter for
å *følge opp* politiske
vedtak, mål og
prioriteringer.



Plan og styring

Repetisjon fra foredrag 1

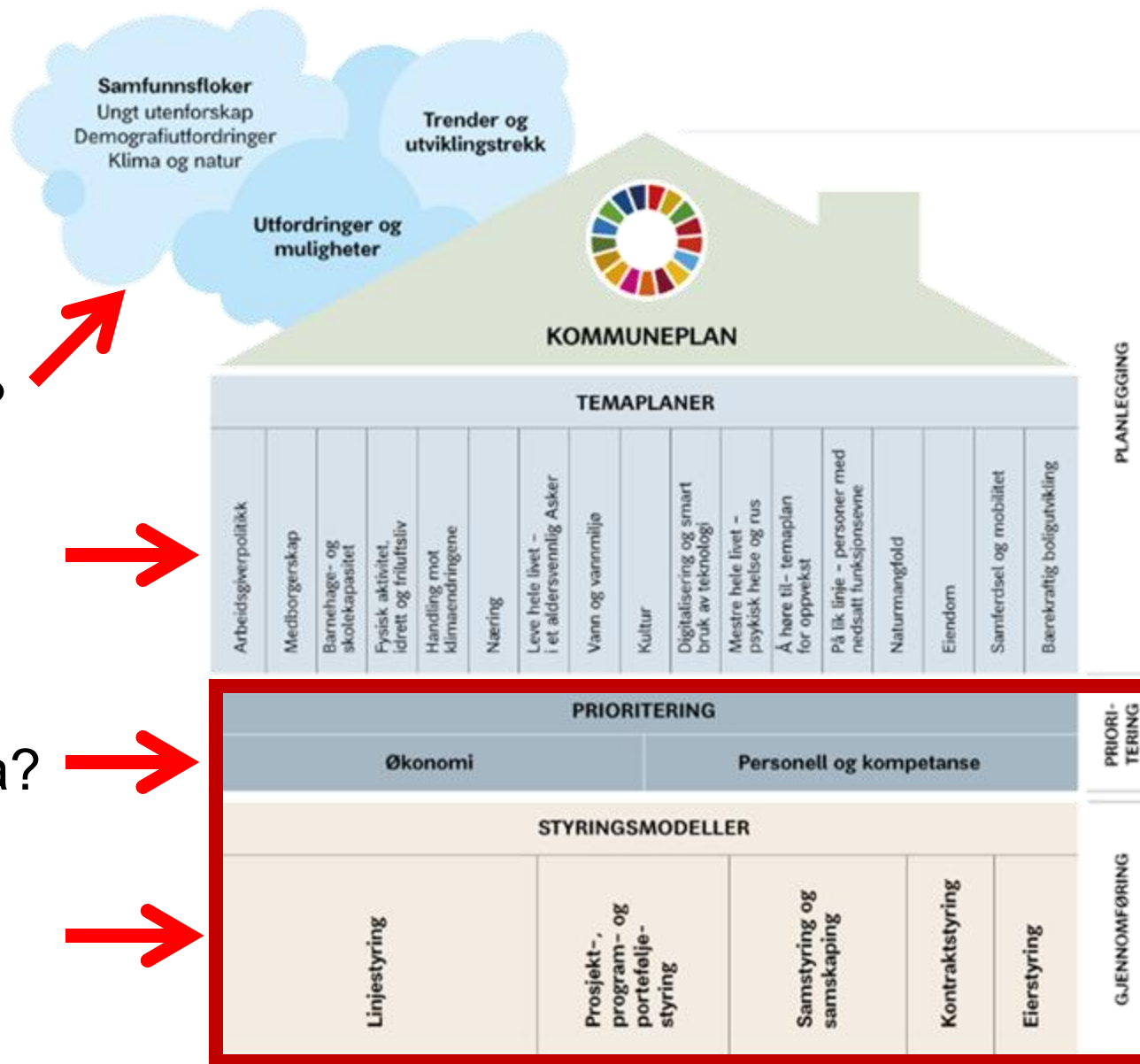
• **Hvorfor** må vi gjøre noe?

• **Hva** velger vi å gjøre?

(Hvilke «utviklingsretninger» setter vi?)

• **Hvor mye** kan vi gjøre nå?

• **Hvordan** gjør vi dette og sammen med **hvem**?



Kommuneplan
med overordnede mål og strategier for samfunns- og tjenesteutvikling, basert på FN's bærekraftsmål

17 temaplaner
med innsatsområder og strategier

Prioritering
av hva som skal gjennomføres når og med hvilke ressurser

Gjennomføring
av prioriterte oppdrag og aktiviteter med en styringsform som passer til oppdraget som skal løses

Porteføljer – samfunnsflokke:

- Ungt utenforskap
- Inkluderende og aldersvennlig steds- og boligutvikling
- Klima og natur

vårt valg av styringsmetode | **vevet inn i kvalitetssystemet**

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 ...



Ha oversikt og prioritere (OP)

OP-1 Oversikt over ansvarsområde

OP-2 Kartlegge eksterne krav

OP-3 Vurdere behov for risikovurderinger

OP-4 Oppdatert oversikt over risikovurderinger



Skjermdump fra kvalitetssystemet

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 ...

→

Ha oversikt og prioritere (OP)

- OP-1 Oversikt over ansvarsområde
- OP-2 Kartlegge eksterne krav
- OP-3 Vurdere behov for risikovurderinger
- OP-4 Oppdatert oversikt over risikovurderinger

Styring av Informasjonssikkerhet X Ha oversikt og prioritere X

Prosess: Identifisere risiko	Prosesseier: Pål Alexander Gaure	Godkjent av: Pål Alexander Gaure	Godkjent dato: 6.11.2025	Publisert versjon: 2	Icons: Edit, Info, Share, Print
------------------------------	----------------------------------	----------------------------------	--------------------------	----------------------	---------------------------------

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

- o oppgaver og tjenester som utføres
- o hvilken informasjon som behandles i oppgaver og tjenester, inkludert hvilke personopplysninger som behandles
- o formål med behandling av personopplysninger, behandlingsgrunnlag og behandlingsansvar
- o overføring av personopplysninger utenfor EØS og overføringsgrunnlag som benyttes
- o 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...

Skjermdump fra
kvalitetssystemet

Fra yppersteprest CISO med rammeverk og regneark til datadrevet beslutnings- støtte (med KI)

knisk K
Antal
kritikalitets
r med teknis
Kritiske syste
stemer med tk
e kritiske systeme
stemer med tk ros
e kritiske systemer
stemer med tk ros
rikling PV over tid
t pers opplysninger
fende DPIA gj ført
m antall systemer
ehandler registrert
lleravtale registrert
i/d

LS- Ledelsens
OP - Ha oversikt
RV - Vurdering
RH - Håndt
ME - Måling
OH - Ov
KK - K
AL - A
KO - Komm
10 Etableringsak



Egenevaluering

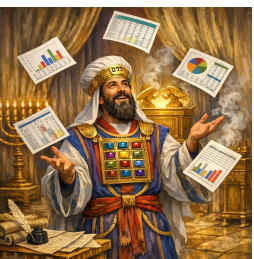
basert på **internkontroll i praksis** siden 2022
konvertert til «styring av informasjonssikkerhet og personopplysningsvern»
i januar 2026

Ledelsens styring og oppfølging (LS) Ledelsen styrer og oppfølger virksomheten gjennom strategiske planer, mål og kriterier for god styring og kontroll. Ledelsen har ansvar for informasjonssikkerhet og personopplysningsvern.	Ha oversikt og prioritere (OP) Ledelsen har oversikt over virksomhetens aktiviteter og prioriterer oppgavene. Ledelsen har ansvar for informasjonssikkerhet og personopplysningsvern.	Vurdering av risiko (RV) Ledelsen vurderer risikoen for informasjonssikkerhet og personopplysningsvern. Ledelsen har ansvar for informasjonssikkerhet og personopplysningsvern.
Håndtering av risiko (RH) Ledelsen håndterer risikoen for informasjonssikkerhet og personopplysningsvern. Ledelsen har ansvar for informasjonssikkerhet og personopplysningsvern.	Måling, evaluering og revisjon (ME) Ledelsen måler, evaluerer og revisjon virksomhetens aktiviteter og prioriterer oppgavene. Ledelsen har ansvar for informasjonssikkerhet og personopplysningsvern.	Overvåking og hendelseshåndtering (OH) Ledelsen overvåker hendelser og håndterer dem. Ledelsen har ansvar for informasjonssikkerhet og personopplysningsvern.
Kompetanse- og kulturutvikling (KK) Ledelsen utvikler kompetanse og kultur i virksomheten. Ledelsen har ansvar for informasjonssikkerhet og personopplysningsvern.	Anskaffelser og leverandørstyring (AL) Ledelsen anskaffer og leverandørstyre virksomhetens aktiviteter og prioriterer oppgavene. Ledelsen har ansvar for informasjonssikkerhet og personopplysningsvern.	Kommunikasjon (KO) Ledelsen kommuniserer med virksomheten og leverandørene. Ledelsen har ansvar for informasjonssikkerhet og personopplysningsvern.

Ikke reelle data

<u>måling ved utgangen av 2025</u>	Oppstart 2022	2022	2023	2024	2025
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

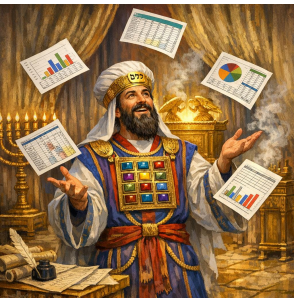
Skjermdump fra regneark for styring indikatorer



OP - Ha oversikt og prioritere

							A
OP-1 Oversikt over ansvarsområde				3		3	
o oppgaver og tjenester som utføres							
o hvilken informasjon som behandles i oppgaver og tjenester, inkludert hvilke personopplysninger som behandles							
o formål med behandling av personopplysninger, behandlingsgrunnlag og behandlingsansvar							
o overføring av personopplysninger utenfor EØS og overføringsgrunnlag som benyttes							
o 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.							

Skjermdump fra regneark for styring indikatorer



Vurderingskoder

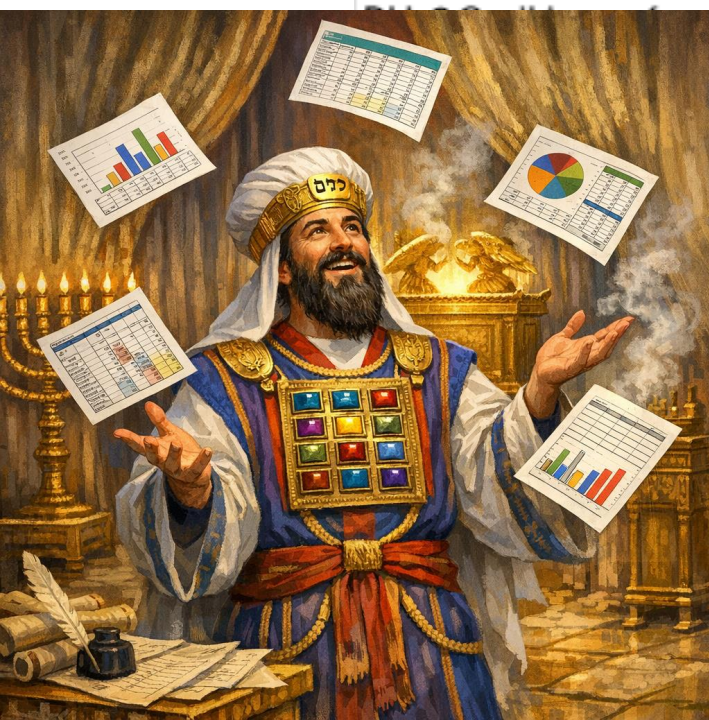
Kodene benyttes i analyseskjemaet under.

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.

Med utgangspunkt i måling 6.1 januar 2026					
Prioritet 1 er å flytte alle 0 og enere til minimum verdien 2					
	Flytte 1 med verdien NULL til verdien 2	innen utgangen av februar 2026			
	Flytte 10 med verdien EN til verdien 2	innen utgangen av februar 2026			
Med utgangspunkt i oppdatert måling ved utgangen av februar 2026:					
Prioritet 1 er å flytte alle 0 og enere til minimum verdien 2					
Prioritet 2 besluttes ut fra måling februar 2026 inkludert måloppnølse fra februar 26.					

Oppgaver som skal fra null eller en til to	status 2025	løpende 2026
LS-1 Gi føringer	1,0	1,0
RV-1 Planlegge risikovurdering	1,0	1,0
RH-1 Foreslå håndtering av risikoer	1,0	1,0
Planlegge tiltak for håndtering av risiko	1,0	1,0
Implementering av håndtering av risiko	1,0	1,0
Vurdering av sikkerhets- og personverntiltak	1,0	1,0
	1,0	1,0
Utvikling av sikkerhets- og personverntiltak	0,0	1,0
Utvikling av sikkerhets- og personverntiltak	0,0	1,0
	0,0	0,0
Utvikling av sikkerhets- og personverntiltak	1,0	1,0
	0,0	0,0



Styring av informasjonssikkerhet og personopplysningsvern (SiP) i Asker kommune

Skjermdump fra regneark for styring

	Fremdrift oppfølging av SiP på en skala fra 0 til og med 4						
	Mål 1 HÅ26	2026 løpende	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	2,2		
OP - Ha oversikt og prioritere	3,30	2,75	-0,55	3,0	2,0		
RV - Vurdering av risiko	3,30	2,50	-0,80	2,5	2,5		
RH - Håndtering av risiko	2,00	1,25	-0,75	1,3	1,3		
ME - Måling, evaluering og revisjon	2,50	2,00	-0,50	2,0	2,0		
OH - Overvåking og hendelseshåndtering	3,75	3,75	0,00	3,8	3,8		
KK - Kompetanse- og kulturutvikling	2,33	2,00	-0,33	1,7	2,0		
AL - Anskaffelser og leverandørstyring	2,60	1,20	-1,40	1,2	1,2		
KO - Kommunikasjon	2,50	2,25	-0,25	2,3	2,3		
Styringsaktiviteter	3,13	3,13	0,00	3,0	3,1		

Ikke reelle data



Overvåkning av SIP i Asker kommune

Mål første halvår 2026, vist mot faktisk skår gjennom 2026

Skjermdump fra regneark for styring

Ikke reelle data

Overvåkning av SIP i Asker kommune, basert på anbefalinger fra norske offentlige veiledningsaktører



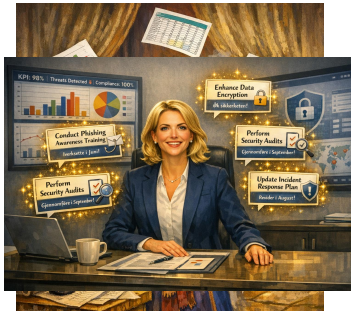
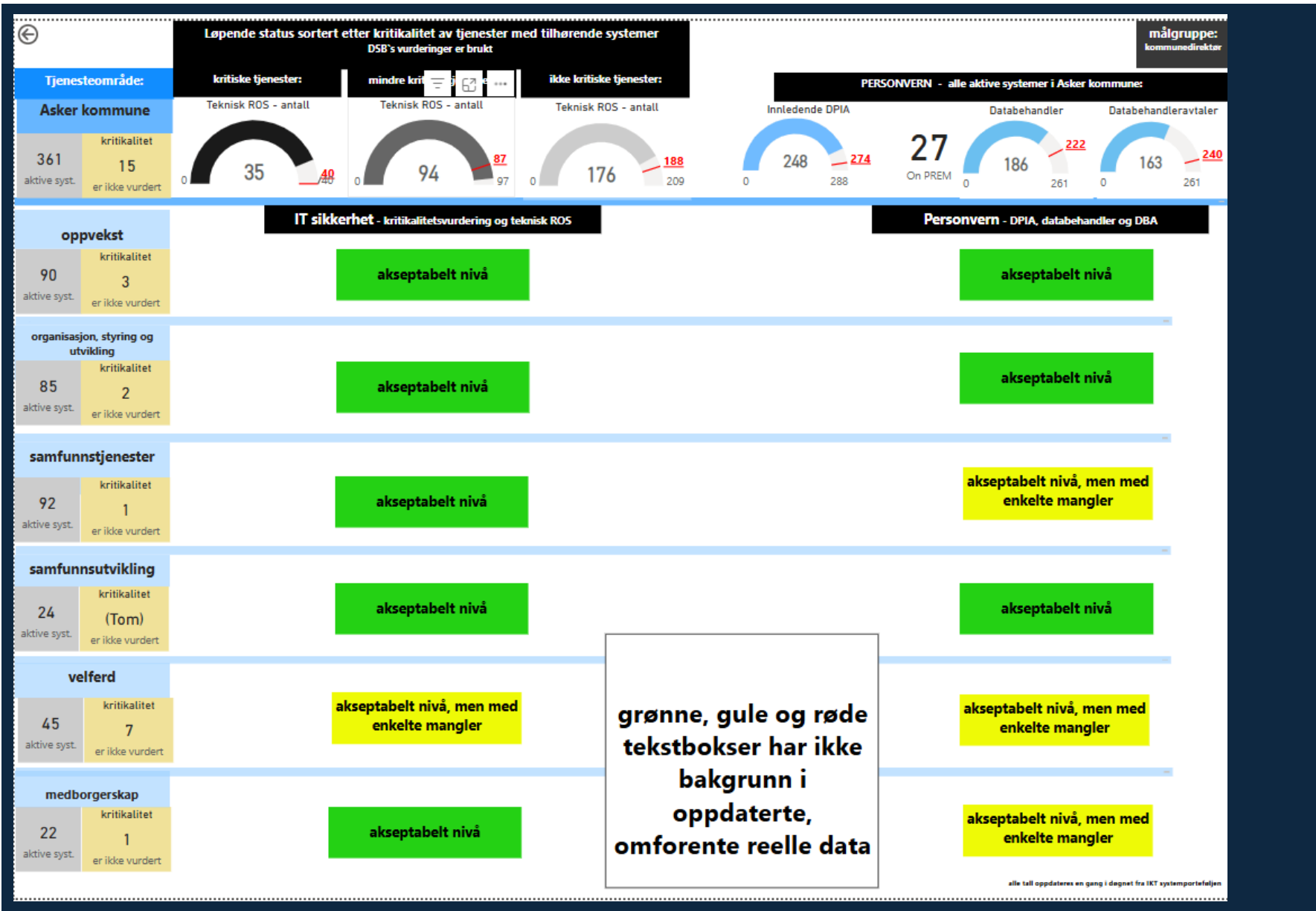
Hva er operasjonalisert (digitalisert og automatisert) av disse styringsaktivitetene?



Dette er gjennomført i 2025 – IT-teknisk



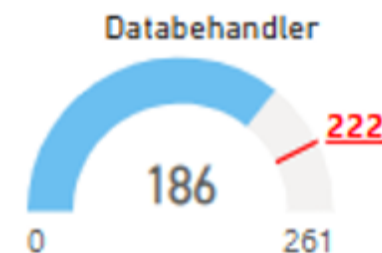
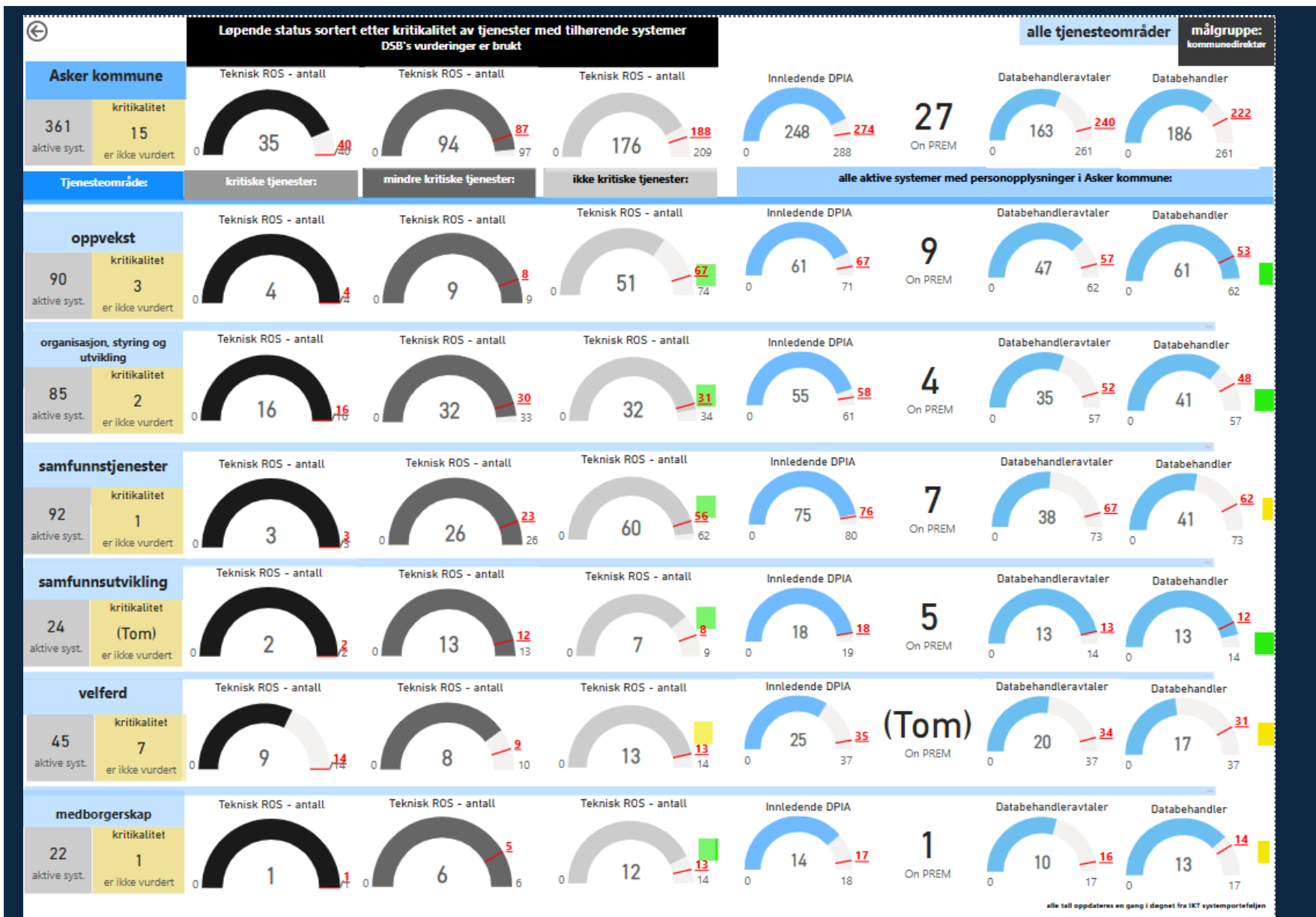
IT-teknisk (T)



Dette er gjennomført i 2025 - IT-teknisk / personvern



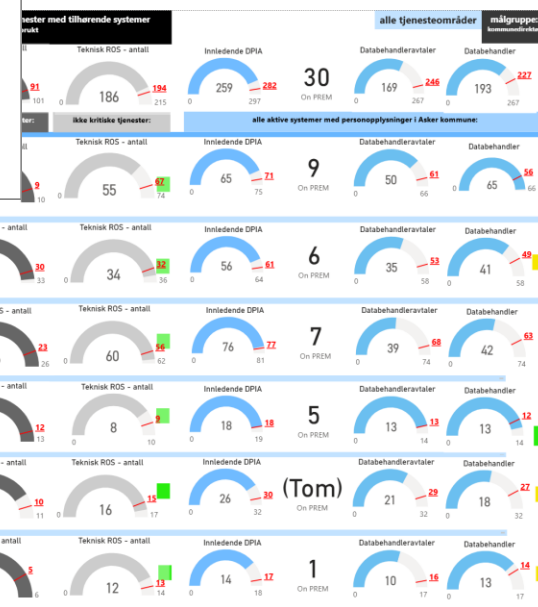
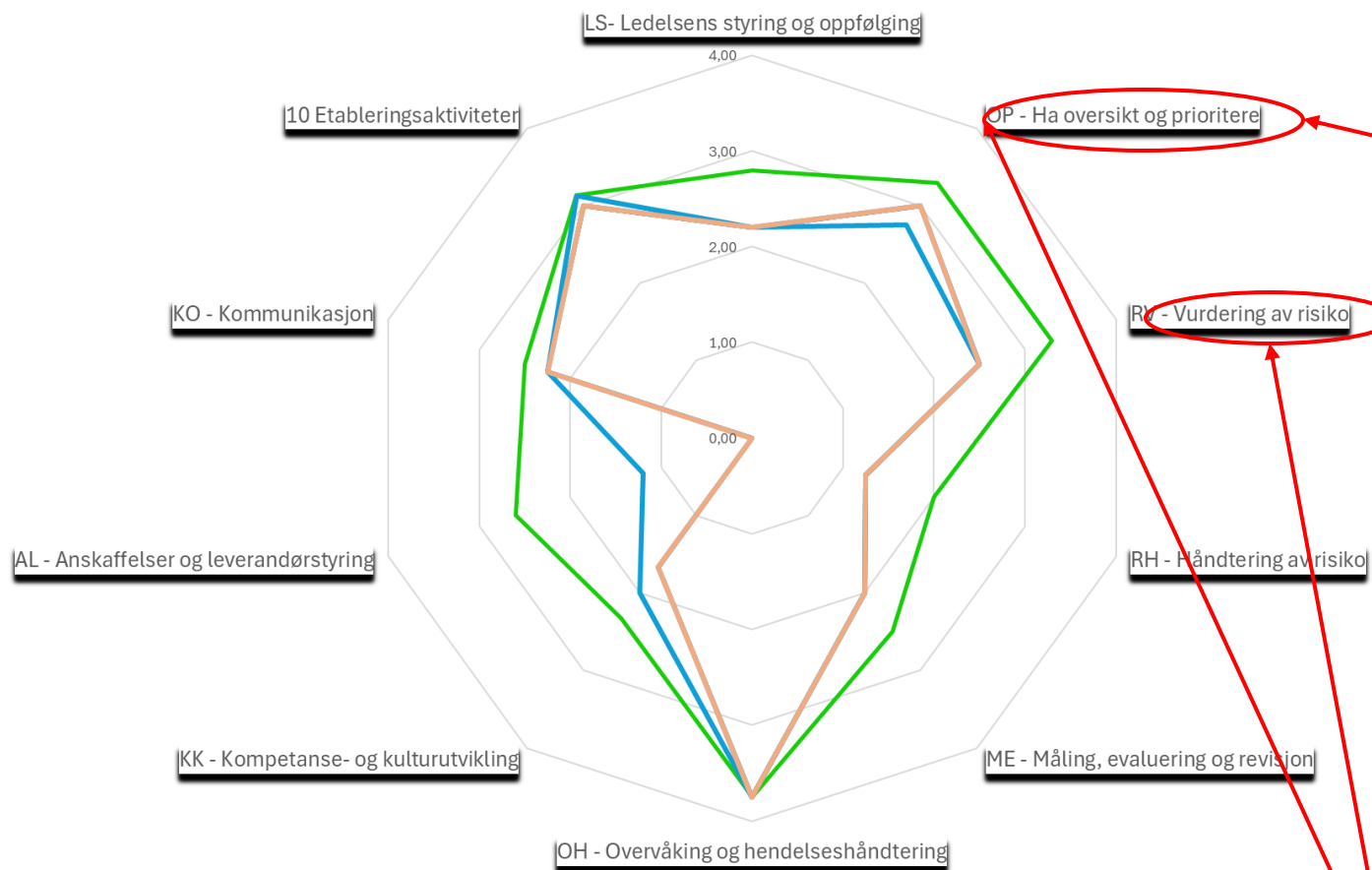
IT-teknisk (T)



nederst til høyre er antallet vi forventer i midten vises antallet som er registrert
Tall i rødt viser KRAVET (som kan være mindre enn forventet)



Overvåking av SIP i Asker kommune, basert på anbefalinger fra norske offentlige veiledningsaktører



Bruke data fra behandlingsprotokoll og «systemlister» for «automatisk» skår av OP, RV, RH, ME og OH

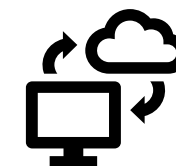
Dette er gjennomført i 2025 – IT-teknisk (T)



Oppdateres hvert kvartal: 31.12.2025						Utvikling i tekniske ROS og personvern på overordnet nivå.							
						Prosent 23 - 24 - 25					Mangler vist i absolutte tall		
		2023	2024	2025		2023	2024	2025			2023	2024	2025
Utvikling i teknisk ROS over tid													
Antall systemer		334	356	378						Antall systemer	334	356	378
Systemer kritikalitetsvurdert		222	328	366		66 %	92 %	97 %		Ikke kritikalitetsvurdert	112	28	12
Summert ant systemer med teknisk ROS		211	266	335		63 %	75 %	89 %		mangler teknisk ROS	123	90	43
Kritiske systemer		23	38	41									
Kritiske systemer med tk ros		22	33	40		96 %	87 %	98 %		Kritiske systemer uten tek ros	1	5	1
Mindre kritiske systemer		56	86	102									
Mindre kritiske systemer med tk ros		49	79	100		88 %	92 %	98 %		Mindre kritiske systemer uten tek ros	7	7	2
Ikke kritiske systemer		132	204	223									
Ikke kritiske systemer med tk ros		77	154	195		58 %	75 %	87 %		Ikke kritiske systemer uten tek ros	55	50	28
Utvikling PV over tid													
Antall systemer med pers opplysninger		235	291	303		70 %	82 %	85 %		Antall systemer med pers opplysninger	235	291	303
Innledende DPIA gj ført		145	222	265		62 %	76 %	87 %		Mangler innledende DPIA	90	69	38
OnPrem antall systemer				30									30
Databehandler registrert		98	163	199		42 %	56 %	73 %		Databehandler ikke registrert	137	128	74
Databehandleravtale registrert		i/d	121	178		i/d	42 %	65 %		Databehandleravtale ikke registrert	i/d	170	95



Yppersteprest CISO`s dashboard



IT-teknisk (T)

Åpne status sortert etter KD`s initielle kritikalitetsvurdering
DSB`s vurderinger av kritikalitet er brukt

systemer som understøtter:

kritiske tjenester:

datert teknisk ROS	ant. systemer
2022	1
2024	3
2025	13
2026	23
Totalt	41

ant systemer	innl DPIA datert
4	
2	2020
1	2021
3	2022
4	2023
30	

mindre kritiske tjenester:

datert teknisk ROS	ant. systemer
2021	2
2022	1
2023	6
2024	13
2025	39
2026	37
Totalt	99

ant. systemer	innl DPIA datert
8	
2	2020
5	2021
5	2022
10	2023
83	

ikke kritiske tjenester:

datert teknisk ROS	ant. systemer
2021	23
2022	3
2023	16
2024	31
2025	77
2026	68
Totalt	224

ant. systemer	innl DPIA datert
20	
3	2020
14	2021
13	2022
26	2023
180	

ikke vurdert:

datert teknisk ROS	ant. systemer
2022	11
2025	1
Totalt	13

ant. systemer	innl DPIA datert
9	
9	

verdikjede (verdinettverk):

ikke reg. databehandler	ikke reg. databeh. avtale
4	4
72	11
ant. integrasjoner	SSO-koblinger
risiko >= 16	
17	

Systemnavn
VM-3000 Talevarlingsanlegg

ikke reg. databehandler	ikke reg. databeh. avtale
31	20
140	39
ant. integrasjoner	SSO-koblinger
risiko >= 16	
14	

Systemnavn
AddView

ikke reg. databehandler	ikke reg. databeh. avtale
63	36
49	90
ant. integrasjoner	SSO-koblinger
risiko >= 16	
11	

Systemnavn
11. Pickatale for School

ikke reg. databehandler	ikke reg. DBA
7	8
(Tom)	1
ant. integrasjoner	SSO-koblin...
risiko >= 16	

System ikke vurdert etter kritikalitet
Sosialarkiv - NAV

alle tjenesteområder

velg tjeneste og virksomhet

Tjeneste

- ☐ Medborgerskap
- ☐ Medborgerskap, Medborgerskap
- ☐ Oppvekst
- ☐ Oppvekst, Oppvekst
- ☐ Organisasjon, styring og utvikling
- ☐ Organisasjon, styring og utvikling, Org..
- ☐ Samfunnstjenester
- ☐ Samfunnstjenester, Samfunnstjenester
- ☐ Samfunnsutvikling
- ☐ Samfunnsutvikling, Samfunnsutvikling

Virksomhet

- Anskaffelser
- Anskaffelser - Anskaffelser
- Asker Drift
- Asker Drift, Samfunnstjenester - Eiendom, Samfunnstjenester - Miljø og samferdsel
- Avlastning og omsorgstjenester til barn og unge
- Barne- og familietjenesten, Oppvekst - Inkludering og mangfold
- Barnevernstjenesten
- Bibliotekene
- Byggesak
- Byggesak, Samfunnsutvikling - Byggesak - Byggesak
- Eiendom
- FOU
- FOU, Velferd
- Heldannelse

Systemansvarlig
Ann-Kristin Bjørnstad

systemeier

målgruppe: sikkerhetsteam

377

aktive systemer

13

er ikke vurdert

37

ROS ikke datert

42

risiko >= 16

inne

in

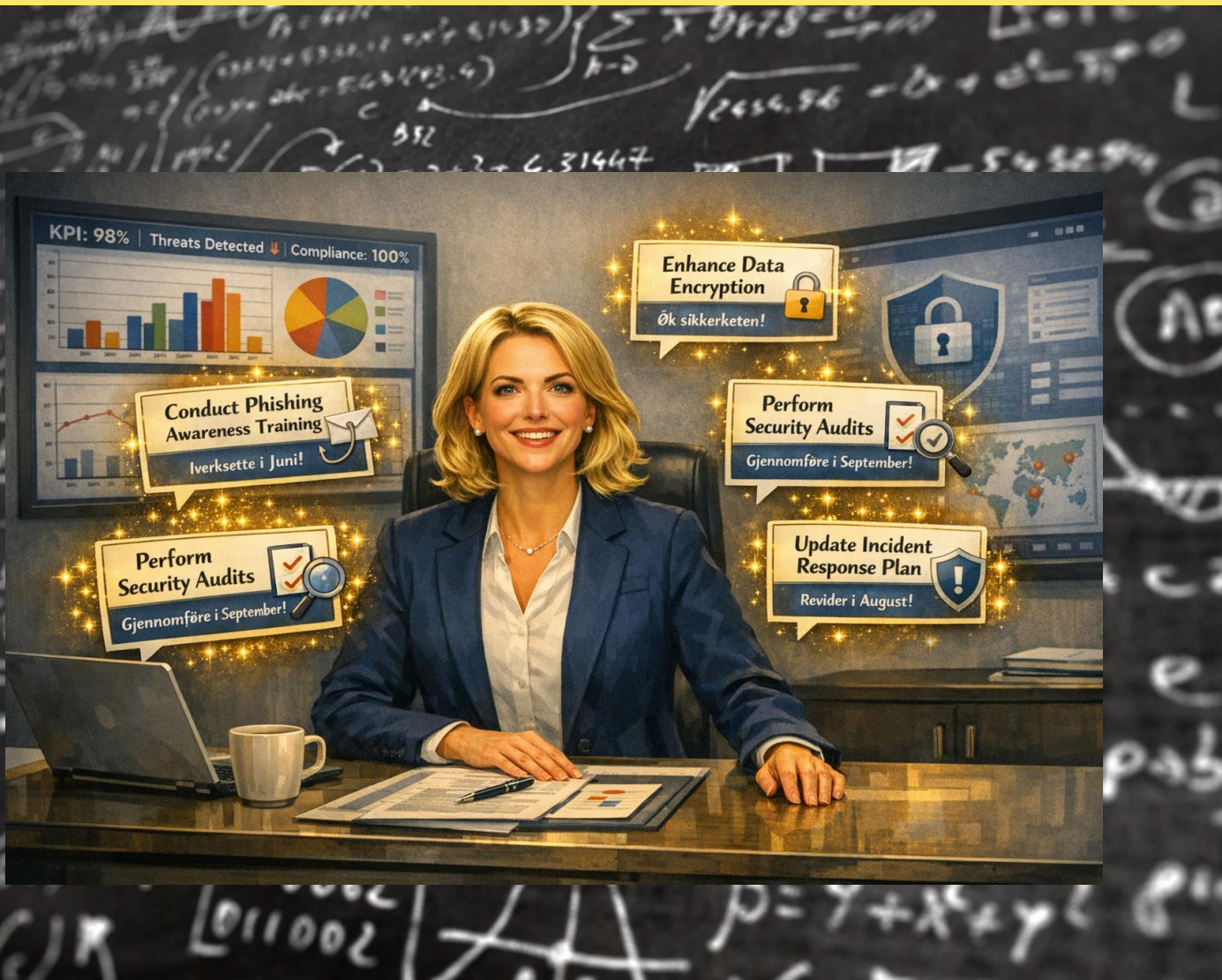
mar





Asker
kommune

Data hentet fra mange
kilder, forslag til
beslutningstekst generert
via en KI-agent



Fra: Din kjære direktør
Til: Ledere av alle virksomheter

- **Innen utgangen av juni 2027:**
Prioriter ROS på systemer og integrasjoner som understøtter kritiske tjenester iht. DSB`s krav og vår tolkning dokumentert i kvalitetssystemet.
- Sørge for at identifiserte tiltak er gjennomført eller planlagte tiltak gjennomføres innen **november 2027**.
- Bruk IKKE ressurser på mindre kritiske og ikke kritiske tjenester, vi vurderer det på nytt i **juni 27**
- Oppdatér (innledende) DPIA for tjenester (behandlingsaktiviteter) som berører mer enn 25% av befolkningen.
I tillegg oppdater DPIA for alle tjenester som berører særskilte kategorier.
- Bruk IKKE ressurser på aktiviteter som i liten grad berører samfunnet slik definert i kvalitetssystemet.
- **Velferd:** Iverksett sikkerhetsnøkkel for alle ansatte
- **Samfunnstjenester:** Gjennomføre øvelse "bortfall av ekom i 48t" for Vann og vannmiljø
- **Oppvekst:** Grunnopplæring for alle skoleledere



Klarer vi å
forene
ørne-
perspektivet
og
dykker-
perspektivet?

følg med...

Hvordan setter vi risikoeier i stand til å styre digital sikkerhet?

Pål Alexander Gaure, informasjonssikkerhetsrådgiver i Asker kommune

Innlegget viser hvordan ledere kan få et tydelig styringsgrunnlag for informasjonssikkerhet ved å bruke data fra tjenesteoversikter, behandlingsaktiviteter, systemlister, ROS og DPIA til å gi tjenesteeiere reell innsikt og evne til å ta informerte beslutninger.