



Oslo

Personvern- og informasjonssikkerhetsforum

14.04.2021
09.00 – 11.00

Kjøreregler

- ▶ Mange deltagere i dag, skru av lyden underveis og rekk opp hånda eller skriv spørsmål eller kommentarer i chatten.
- ▶ Vi vil stoppe noen ganger underveis for å svare på spørsmål. Noen spørsmål kan også bli besvart i chatten.
- ▶ 10 minutter pause ca. kl. 0950



0900-0910	Velkommen og introduksjon til dagens program ved Randi Blystad
0910-0920	Hva skjer på personvernområdet v/Maryke Silalahi Nuth
0920-0930	Hva skjer på informasjonssikkerhetsområdet v/Åsmund Skomedal
0930 - 0950	Personvernombudets observasjoner om personvern i Oslo kommune v/Morten Haug Frøyen
0950-1000	Pause til å fylle kaffekoppen
1000 - 1055	Status og trusselbilde på informasjonssikkerhet og personvern i Oslo kommune v/ Jeanne Hammer Espedalen
1055-1100	Avslutning

Programgruppe til personvern- og informasjonssikkerhetsforum

- ▶ Vi har en programgruppe til forumet som skal være med å gi innspill og sette sammen det faglige innholdet til forumene slik at vi lager et relevant og engasjerende faglig innhold.
- ▶ Gruppa består av:
 - Morten Haug Frøyen (Personvernombudet)
 - Rohan Fininger (UDE)
 - Hans Tore Haagensen (BAL) frem til juni 2021
 - Hana Temsamani (BSN)
 - Iselin Lunde (VEL)
 - Andrea Liebe (MUM)

Kommende datoer for forum

09.juni

1.september

24.november



Oslo





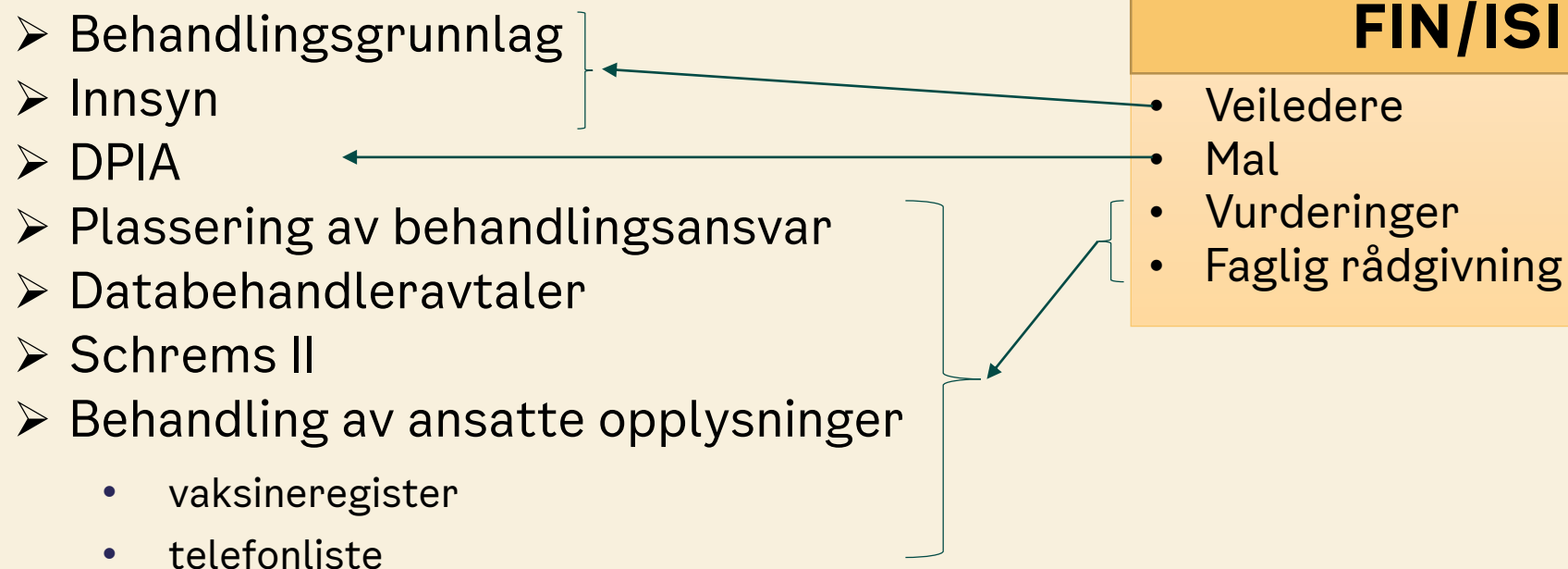
Oslo

Hva skjer på personvernområdet?

Med fokus på konkrete henvendelser

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

Henvendelser i Oslo kommune Q1 2021



Covid-19 vaksineregister over ansatte

Formål med register

- Smittevern hensyn
 - forsvarlighet i pasientbehandling
 - godt og sikkert arbeidsmiljø (HMS)
 - arbeidstakers medvirkningsplikt

Behandlingsgrunnlag

- Rettslig forpliktelse: arbeidsgiver kan bli pålagt til å ha vaksineregister
- Supplerende rettsgrunnlag i arbeidsmiljøloven og helselovgivning (helsepersonelloven og smittevernloven)
- Samtykke kan være utfordrende

Viktige prinsipper

- Lovlighet
- Formålsbegrensning
- Dataminimering
- Lagringsbegrensning



Informasjonssikkerhet

En kort oppdatering

Åsmund Skomedal

Fagsjef informasjonssikkerhet

asmund.skomedal@byr.oslo.kommune.no



Status informasjonssikkerhet

- ▶ **Trusselbildet** – er vesentlig skjerpet (de siste to årene)
 - Bedre organiserte kriminelle og nasjonale aktører (kjøp & salg, auksjoner, opplæring, ...)
 - Mer effektiv utnyttelse av sårbarheter
 - Pandemien og hjemmekontor betyr flere sårbarheter (privat utstyr)
 - Vi må anta at profesjonelle trussel-aktører ser på oss med stor interesse [NSM]
 - Politiske motivert spionasje, desinformasjon, ...
 - Økonomisk vinning; cyber-kriminalitet er en STOR økonomi
- ▶ Oppsummert «**status**» for kommunen basert på LG/VE rapportene
 - Eget punkt senere i programmet
- ▶ Oppdatering av flere rollekort
 - Rolekort for koordinatorene (PVK) og (ISK) oppdatert, presentert i forrige forum
 - Tre reviderte rollekort er til intern kvalitetssikring, øvrige er til vurdering

Aktiviteter innen informasjonssikkerhet

- ▶ **Veileder** for sikkerhet og personvern i skytjenester (for IaaS og PaaS)
 - Formålet er å unngå uakseptabel risiko
 - Organisatorisk/administrativ nivå; leveranse- og tjenestemodeller, leverandørvurderinger
 - Personvern - kompliseres (noe) av Schrems II dommen
 - Forventer en runde med innspill fra flere virksomheter i Q2
- ▶ **Behandlingsregler** for dokumenter i Office 365, første utkast foreligger
 - Basert på «**Klassifisering av informasjon v1.0**» (jf. forrige forum)
 - Fire konfidensialitetsklasser; «Åpen» – «Intern» – «Beskyttet» – «Strengt beskyttet»
 - Vil først prøves ut i O365 piloter – og revideres før innføring i virksomhetene



Årsrapport 2020

Personvernombudet
i
Oslo kommune



«Personvernombudets observasjoner om personvern i Oslo kommune» - Årsrapport 2020

- ▶ Personvernombudet i Oslo kommune – ordning, historikk, regelverk, mandat og oppgaver
- ▶ Samarbeid med Datatilsynet
 - Brudd på personopplysningssikkerheten – avviksmeldinger til Datatilsynet
- ▶ Nettverk og samarbeid
 - Internt
 - Personvern i prosjekter
 - Eksternt
- ▶ Henvendelser fra innbyggere i Oslo kommune
- ▶ Særlige saker



Anbefalinger og videre arbeid

1. Avvikskultur
 - Økning fra 2019 til 2020
 - Store forskjeller mellom virksomhetene
2. Delingskultur
 - Erfaringsutveksling, «Beste praksis»
3. Ressursbruk
4. Ansvarsfordeling
5. Lederkultur
6. Ikke glemme å bygge videre på alt det positive som skjer!



Status for arbeid med informasjonssikkerhet og personvern 2020

Jeanne H. Espedalen

Forum for personvern og
informasjonssikkerhet
14.04.2021



Hva skal jeg presentere?

- ▶ Et skjerpet digitalt trusselbilde
- ▶ Status for arbeid med informasjonssikkerhet og personvern i Oslo kommune – et overordnet bilde
- ▶ Hvilke utfordringer har vi i kommunen og hva er det viktig å fokusere på i arbeidet fremover?

Skjerpet trusselbilde nasjonalt og internasjonalt

- ▶ Trussel-aktørenes "økosystem" utvikles stadig; bedre organisert og bedre økonomi
- ▶ Status fra Norske organisasjoner
 - NSM: «Et skjerpet digitalt trusselbilde»
 - Stadig mer profesjonelle aktører tilpasser seg raskt mulighetsrommet som oppstår når samfunnet endres
 - Med den digitale utviklingen oppstår nye sårbarheter og gamle/kjente sårbarheter kan utnyttes i stort omfang og på nye måter.
 - Aktørene kan ha økonomiske eller politiske motiver, og de har store ressurser
 - Politiet: «Det vurderes som meget sannsynlig at norske virksomheter vil bli utsatt for datainnbrudd med løsepengevirus»
 - PST: «Den digitale trusselen fra statlige aktører er alvorlig, og ingenting tyder på at den blir redusert»
 - Kommune-CSIRT: «Trusselbildet er skjerpet og at alle kommuner og andre virksomheter kan bli utsatt for alvorlige cyberangrep»
- ▶ Noen sikkerhetshendelser (i 2021)
 - Østre Toten, Skien kommune, Stortinget, Oslo bystyre, Drammen kommune, Akva group, Tietoevry, Acer...
- ▶ Personvern (i 2021)
 - Gebyr til Ålesund kommune for bruk av Strava, varsel til Grindr, gebyr til Asker kommune, gebyr for automatisk videresending av e-post

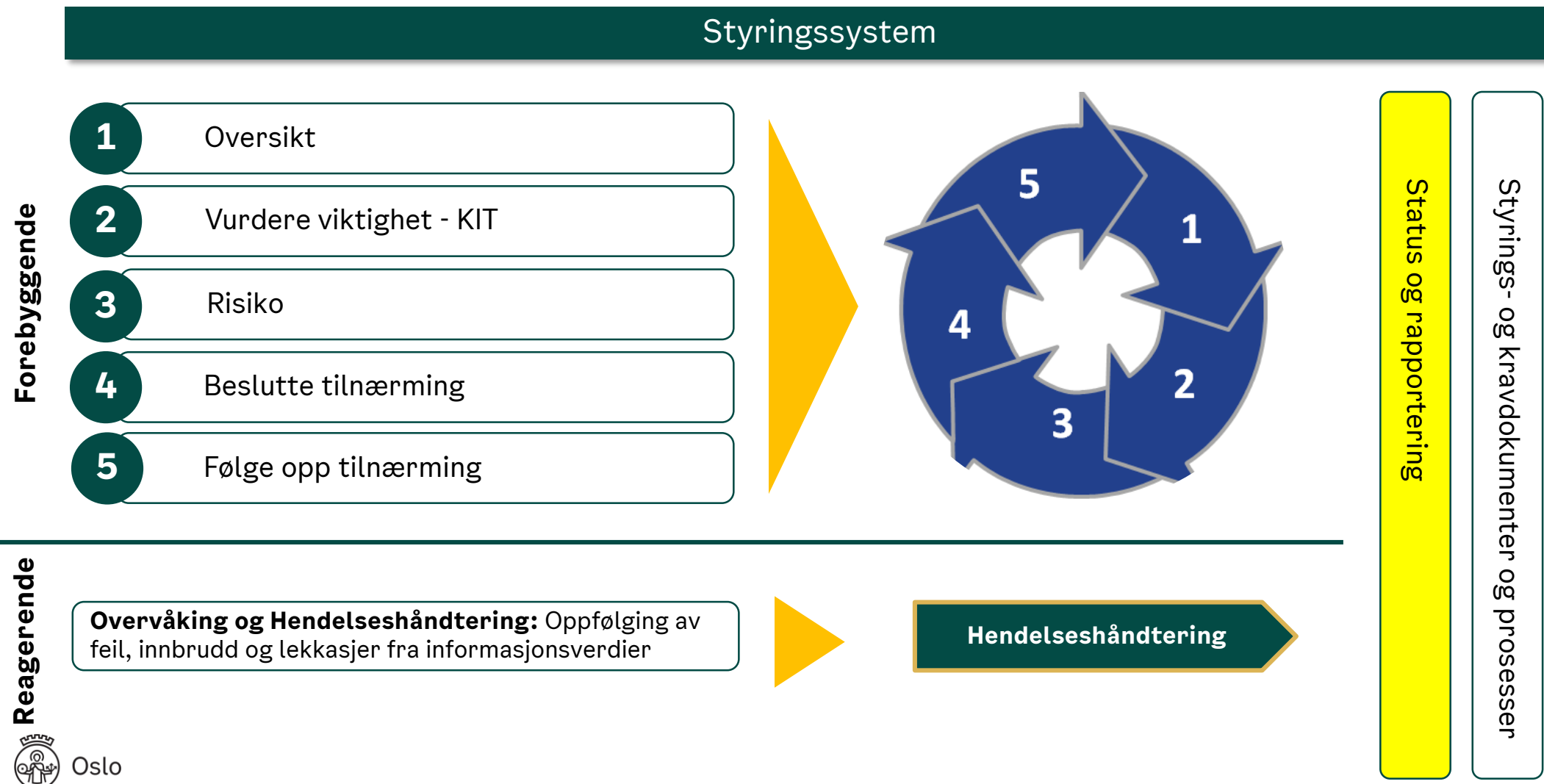
Fremover – ny teknologi, nye sårbarheter, nye trusler..



Oslo kommune

- ▶ Leverer viktige tjenester til mange mennesker, og håndterer store mengder personopplysninger som befolkningen forventer at skal bli ivare tatt på en god måte og i henhold til regelverk.
- ▶ Stadig mer avhengig av å ha på plass tilstrekkelige **tekniske**, **organisatoriske** og **operasjonelle** tiltak for å sikre trygg håndtering av informasjonen.
- ▶ Vi må ha en teknisk, operasjonell og organisatorisk evne til å **forebygge** og **oppdage** hendelser og uønsket aktivitet, og også en teknisk, operasjonell og organisatorisk evne til å **håndtere** hendelser og sikre kontinuitet i tjenesteleveranser.

Rapportering er en del av arbeidet med styring og kontroll

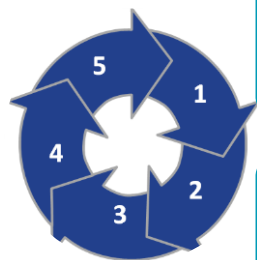


Instruks for informasjonssikkerhet



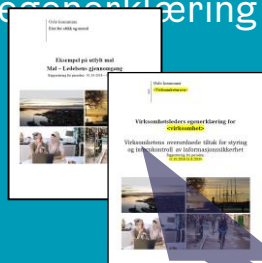
- ▶ Forankring av «Ledelsens gjennomgang» og «Virksomhetsleders egenerklæring»
- ▶ Krav til sikkerhetsarbeidet
 - Roller og ansvar
 - Dokumentasjon og rapportering
 - Oppfølging kontroll og revisjon
- ▶ Krav til kartlegging og oversikt
 - Forpliktelser og rettslige krav
 - Informasjonsverdier
- ▶ Krav til sikring av informasjon
 - Den enkeltes ansvar
 - Fysisk sikring
 - Tilgangskontroll
 - Anskaffelser, utvikling og vedlikehold av systemer
 - Drift av systemer og IKT-infrastruktur
 - Hendelseshåndtering og kontinuitetsplanlegging

Proessen som ligger bak statusoppsummeringen



Virksomhetene

- Arbeid med PV og IS
- Ledelsens gjennomgang
- Virksomhetsleders egenrapportering



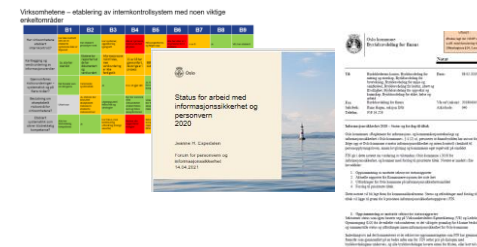
Byrådsavdelingene

- Følger opp virksomhetene
- Sammenstiller status
- Rapporterer til byrådsavdeling for finans



Byrådsavdeling for finans

- Sammenstiller
- Oppsummerer status for Oslo kommune
- Presenterer resultatet til ulike grupper
- Prioriterer tiltak
- Utarbeider nye maler



Oslo

Hva dekker oppsummeringen?

- Oppsummering er i stor grad basert på egenrapportering fra virksomheter og byrådsavdelinger (dette er ikke en revisjon..)
 - I stor grad egevaluering
 - Mange synes det er vanskelig å svare godt på spørsmålene
 - Vesentlig usikkerhet i svarene
 - Vi ser utvikling i svarene år for år, mer kritiske vurderinger betyr det gjerne økt (selv-) innsikt
- Spørsmålene i malene vi bruker er overordnede og dekker ikke alt
 - Har for eksempel ikke spurt om virksomheten har beredskaps-/kontinuitetsplaner og har øvd disse
 - Spør ikke noe rundt tekniske tiltak og fysisk sikkerhet



Ikke et totalbilde av situasjonen i Oslo kommune

Hvordan ser det ut i kommunen?



Arbeid og ansvar på byrådsavdeling-/sektornivå

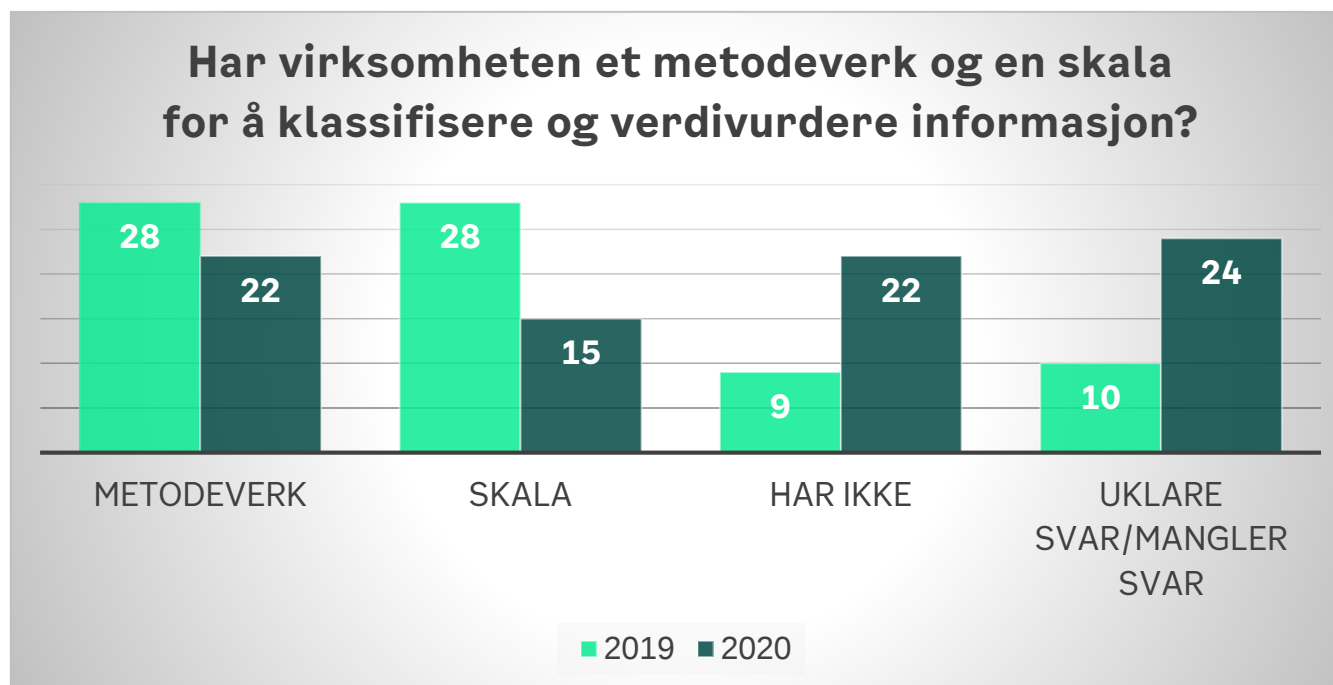
	B1	B2	B3	B4	B5	B6	B7	B8	B9
Har byrådsavd. etablert roller og rutiner intern i egen avd. og i styringsdialogen?	Ikke etablert rutiner for oppfølging	Ivaretas som del av ordinær aktivitet	PKO ig ISK, egen seksjon fra 2021	Fordelt roller basert på vedtak i KLM	Egen stilling som PISK	Ja, etatsansvarlige, saksbehandlere har intern rolle	Integrert del av virksomhetsstyring	PISK og roller i styringsdialog	Delvis
Er byrådsavd. involvert i alvorlige hendelser og avvik?	Har ikke vært noen	Litt varierende	I varierende grad. Virksomheter skal oppdatere rutiner	Virksomhetene skal varsle	Har ikke vært noen siste periode	Blir informert i den grad det har vært	Etatene har ikke rapportert (men 5 rapportert i VE)	Har rutiner og blir involvert	Har ikke vært i virksomhet, men involvert når det gjelder sektor-systemer
Igangsatt arbeid med akseptabel risiko for sektoren?	Må jobbe videre med	Etablert i forbindelse med utarb. av sektor-strategi	I varierende grad. Virksomheter skal oppdatere rutiner	Etablert med involvering fra virksomhetene	Etablert basert på virksomhetenes aksept-kriterier	Nei, er forsinket, vil ha behov for bistand fra FIN	Foreløpig ikke gjort, planlegges igrangsatt 2020	Vil se på mulighet for å etablere akseptabelt nivå for sektor	Nei, må støtte oss på arbeid gjort i EHA

Virksomhetene – etablering av internkontrollsystem med noen viktige enkeltområder

	B1	B2	B3	B4	B5	B6	B7	B8	B9
Har virksomhetene etablert internkontroll?	Har ikke mottatt info om at etablerte systemene ikke er tilpasset	Har etablert prosedyre-verk	Har systemer, oppdatering igangsatt	Alle er i prosess, men kun en har på plass	Må kompletteres og følges opp	Alle har eller er i en prosess for å etablere	4 av 6	Ja	Har etablert
Kartlegging og verdivurdering av informasjonsverdier	Ja, alle har oversikt	Etatene har rapportert at de har dokumentert og verdivurdert	Informasjonsoversikt finnes, men verdivurdering er ikke ferdigstilt	11 av 18 har gjennomført, de øvrige er i prosess	1 virksomhet har ikke sluttført	Virksomhetene enten har, eller er i gang med dette.	2 av 6 har kartlagt og verdivurdert, for de øvrige gjenstår arbeid	Ja	Har kartlagt og verdivurdert
Gjennomføres risikovurderinger – systematisk og på flere nivåer?	Det fremstår som om det gjøres	Varierende systematikk	Ja	8 av 18 gjør det	Ja, 1 virksomhet har behov for mer kompetanse	I ulik grad	Gjenstår arbeid i 2 etater	Ja, i stor grad	Ja
Beslutning om akseptabelt risikonivå for virksomhetene?	Uklart svar	Ja, etatene har besluttet akseptabelt risikonivå i etablerte risikomatriser	utgangspunkt i felles mål og strategier	Byr har sammen med virksomheter utviklet felles nivå og felles akseptkriterier	Virksomhetene har fastsatt akseptabelt risikonivå	Svarer litt uklart	Kun 1 av 6	Bekreftet i fjorårets rapportering	Oppgir at de har fastsatt akseptabelt risikonivå
Etablert systematikk som sikrer tilstrekkelig kompetanse?	Alle har tilstrekkelig kompetanse	Ja	Har fokus, men kontinuerlig utfordring (mange ansatte)	Nesten alle rapporterer mangler	Behov for økt komp. på risikovurd. og DPIA	Ulikt for virksomhetene	Kun en etat er grønn	Bør tilstrebe at alle ansatte får tilpasset opplæring	Behov for infosisikk-bevisstgjøring

Kjenner virksomhetene informasjonsverdiene?

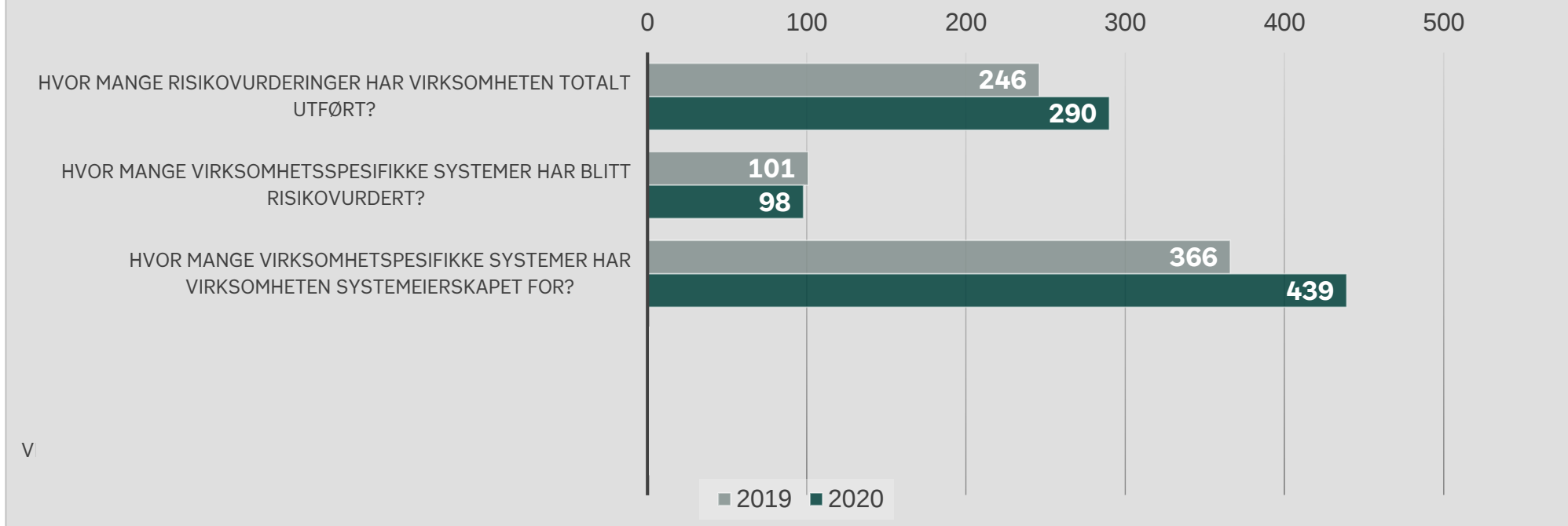
Kartlegging og verdivurdering av informasjonsverdier	Ja, alle har oversikt	Etatene har rapportert at de har dokumentert og verdivurdert	Informasjonsoversikt finnes, men verdivurdering er ikke ferdigstilt	11 av 18 har gjennomført, de øvrige er i prosess	1 virksomhet har ikke sluttført	Virksomhetene enten har, eller er i gang med dette.	2 av 6 har kartlagt og verdivurdert, for de øvrige gjenstår arbeid	Ja	Virksomhet har kartlagt og verdivurdert
--	-----------------------	--	---	--	---------------------------------	---	--	----	---



Risikovurderinger – noen tall

Gjennomføres risikovurderinger – systematisk og på flere nivåer?	Det fremstår som om det gjøres	Varierende systematikk	Ja	8 av 18 gjør det	Ja, 1 virksomhet har behov for mer kompetanse	I ulik grad	Gjenstår arbeid i 2 etater	Ja, i stor grad	Ja
--	--------------------------------	------------------------	----	------------------	---	-------------	----------------------------	-----------------	----

Systemeierskap og risikovurderinger - noen tall



Sikkerhet i anskaffelser

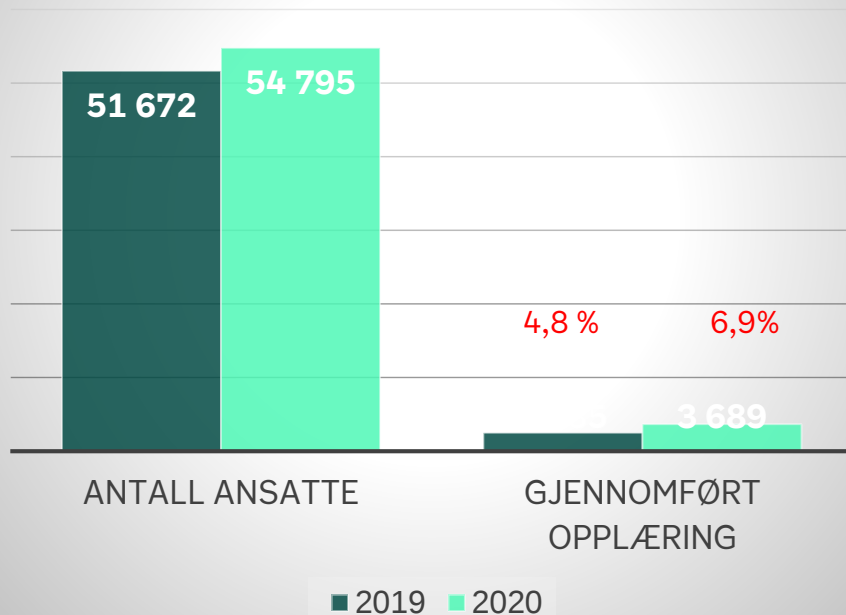


Funn i Kommunerevisjonens rapport fra 2019

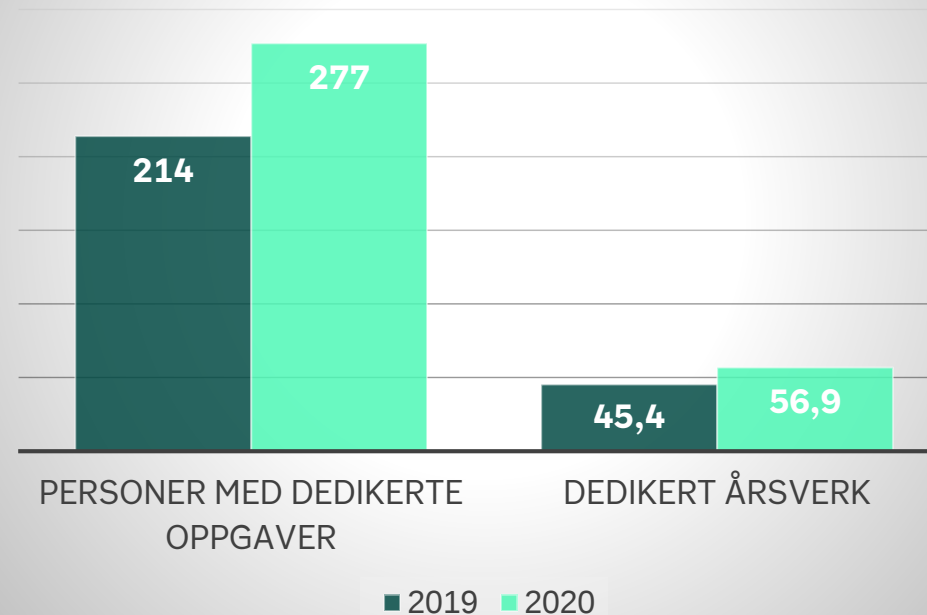
Ressurser og kompetanse

Etablert systematikk som sikrer tilstrekkelig kompetanse?	Alle har tilstrekkelig kompetanse	Ja	Har fokus, men kontinuerlig utfordring (mange ansatte)	Nesten alle rapporterer mangler	Behov for økt komp. på risikovurd. og DPIA	Ulikt for virksomhetene	Kun en etat er grønn	Bør tilstrebe at alle ansatte får tilpasset opplæring	Behov for infosikk-bevisstgjøring
---	-----------------------------------	----	--	---------------------------------	--	-------------------------	----------------------	---	-----------------------------------

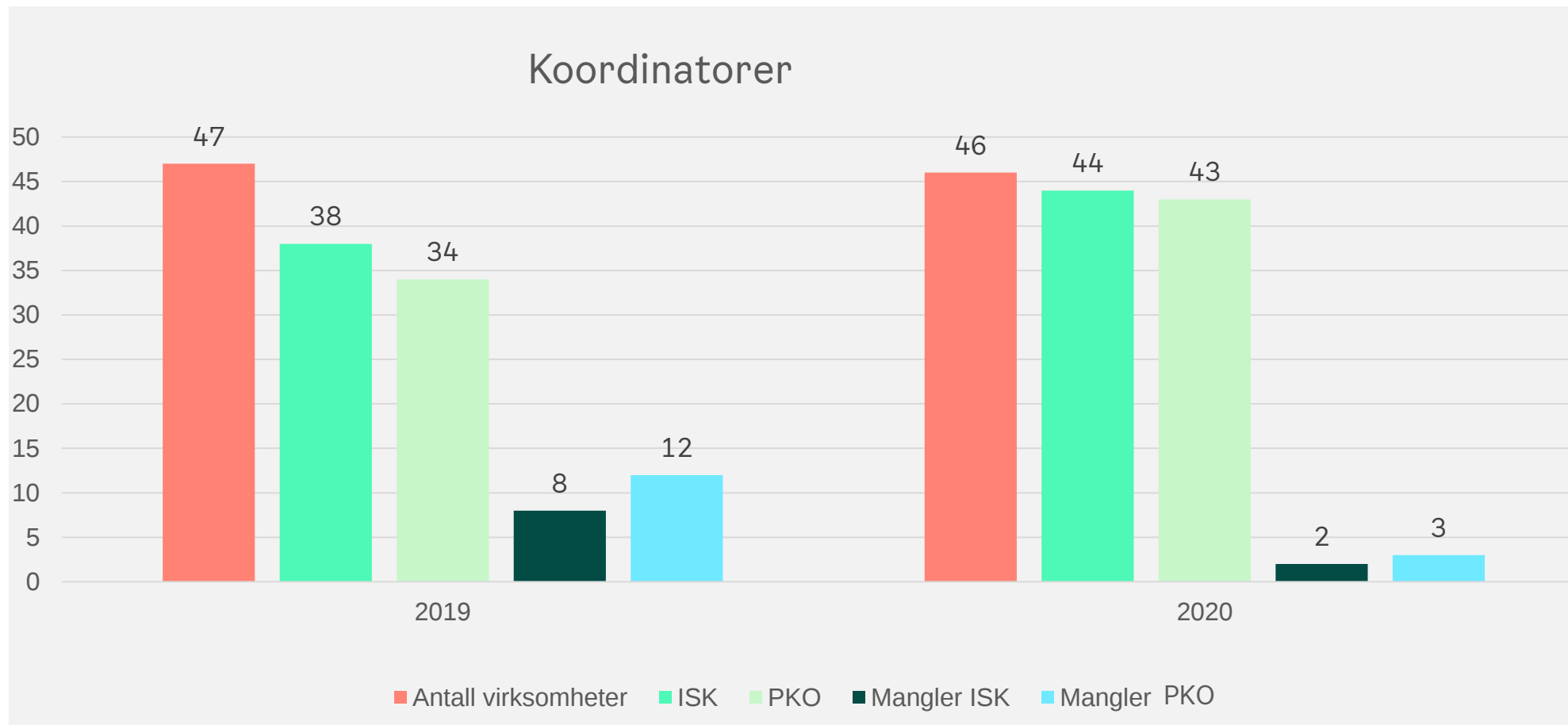
Gjennomført opplæring 1/2 dag



Dedikerte ressurser utenom PKO og ISK



Koordinatorer, PKO og ISK – fellesføring/krav 2020



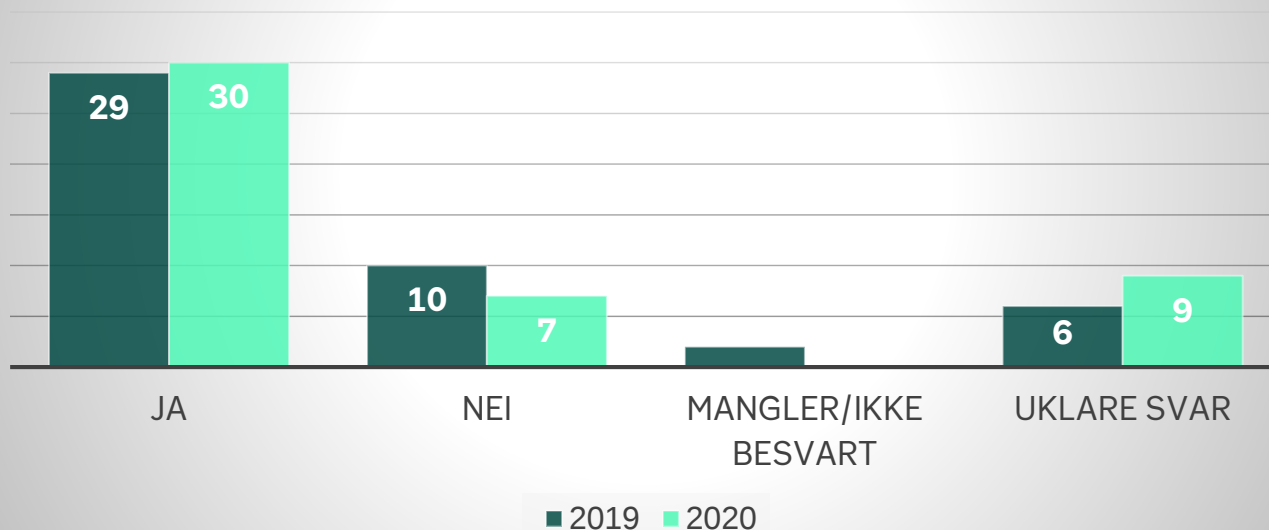
Personverntema

	B1	B2	B3	B4	B5	B6	B7	B8	B9
Oppdaterte behandlings-oversikter	Fremstår tilfreds-stillende	Ja	Halvparten har oppdatert	Halvparten har, resten i prosess	Gjenstår noe arbeid i 1 virksomhet	1 etat har behov for å oppdatere rutiner	Gjenstår noe arbeid i 3 av 6	Ok	Ok
Tilstrekkelig antall DPIA	Vurderer at det er gjort der det er pålagt	Varierende, (en virksomhet melder at de har behandlings-oversikt..)	Nei, og dette må prioriteres	Så nær som alle må forbedre arbeidet	3 har gjort 1 hver	OK for 3, 1 mangler	4 av 6 har vurdert DPIA, gjenstår noe arbeid	Mangler for en rekke behandlinger	Utført der det er pålagt
Er antall meldte avvik til DT rimelig?	Byrådsavd er ikke kjent med at det er meldt inn avvik	Det meldes avvik, uklar vurdering fra byrådsavd om det er riktig nivå	Vanskelig å vurdere – ikke entydige rutiner	Krevende å vite selv om antallet meldinger øker	Kun BYR har hatt brudd, meldt 2 til DT	Byrådsavd mener det er riktig nivå for 3 etater 1 har ikke god nok rutine	Vurderes at antallet er riktig	Vanskelig å fastslå, antar at det kan være under-rapportering	Ikke mottatt mld. om avvik, men usannsynlig at det ikke har forekommet

Behandlingsoversikter

Oppdaterte behandlingsoversikter	Fremstår tilfreds- stillende	Ja	Halvparten har oppdatert	Halvparten har, resten i prosess	Gjenstår noe arbeid i 1 virksomhet	1 etat har behov for å oppdatere rutiner	Gjenstår noe arbeid i 3 av 6	Ok	Ok
-------------------------------------	------------------------------------	----	-----------------------------	--	--	---	---------------------------------	----	----

Har virksomheten revidert sine behandlingsoversikter?



DPIA- personvernkonsekvensvurdering - spørsmål i VE

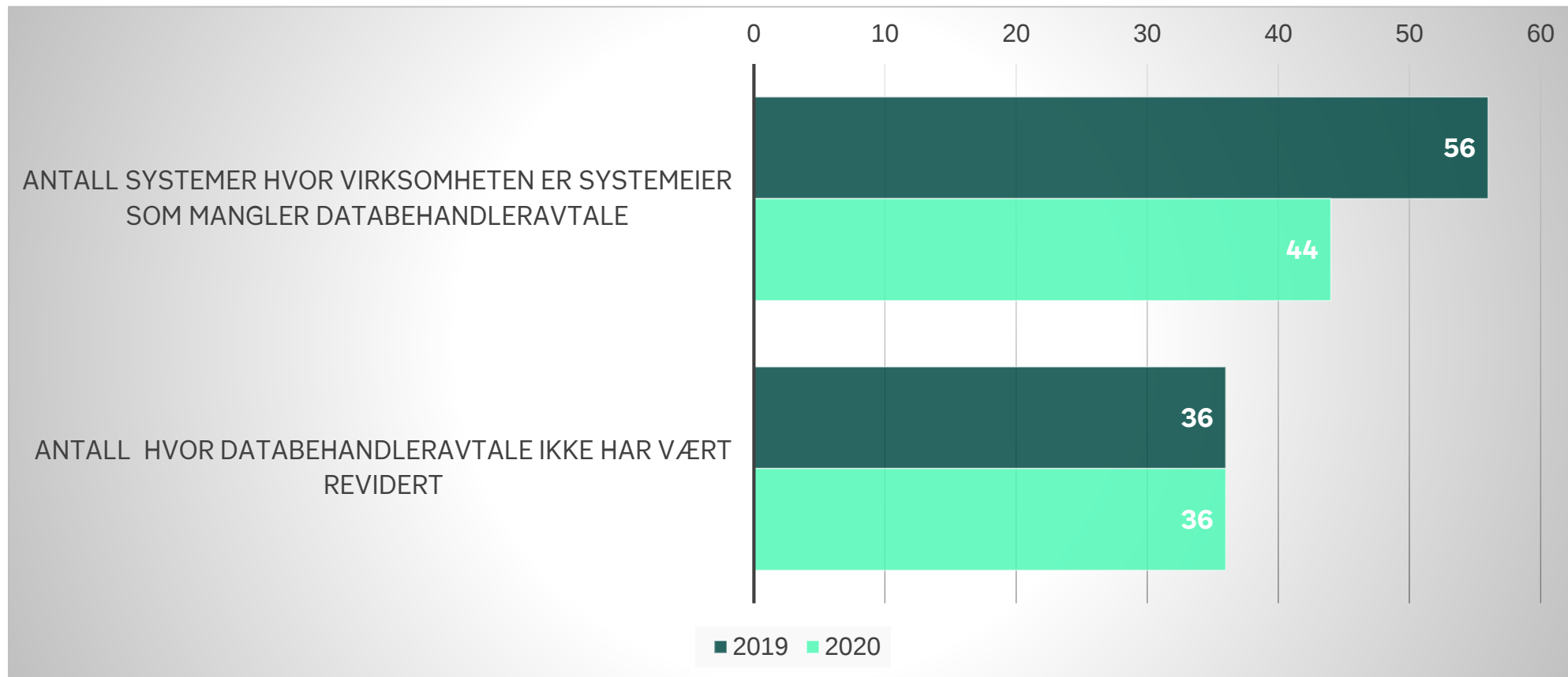
Tilstrekkelig antall DPIA	Vurderer at det er gjort der det er pålagt	Varierende, (en virksomhet melder at de har behandlingsoversikt..)	Nei, og dette må prioriteres	Så nær som alle må forbedre arbeidet	3 har gjort 1 hver	OK for 3, 1 mangler	4 av 6 har vurdert DPIA, gjenstår noe arbeid	Mangler for en rekke behandlinger	Utført der det er pålagt
---------------------------	--	--	------------------------------	--------------------------------------	--------------------	---------------------	--	-----------------------------------	--------------------------

	Totalt antall DPIA	Antall virksomheter som har besvart (av 46)	Antall virksomheter med svar=0
Hvor mange er utført?	263	46	23
Hvor mange er oversendt Datatilsynet for forhåndsdrøftelse?	0	42	41

2019: Totalt antall DPIA 220, herav 200 utført i en bydel, 27 virksomheter svarte «0»

	Antall virksomheter som har besvart	Ja	Nei	Uklare svar
Har virksomheten etablert rutiner for gjennomføring av DPIA?	41	20	14	7

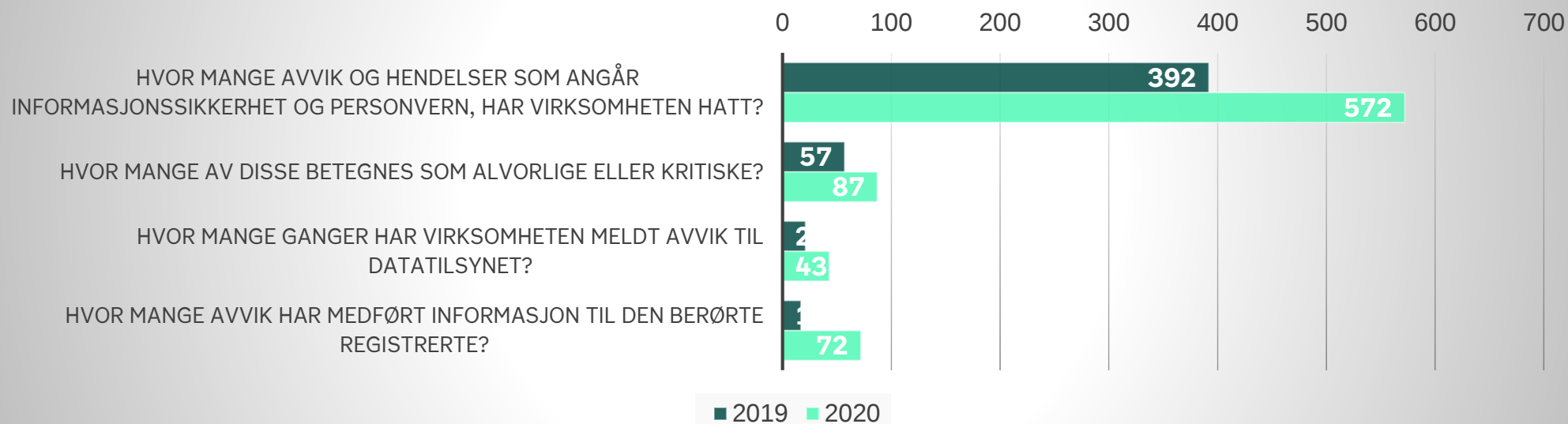
Manglende databehandleravtaler



Hendelseshåndtering

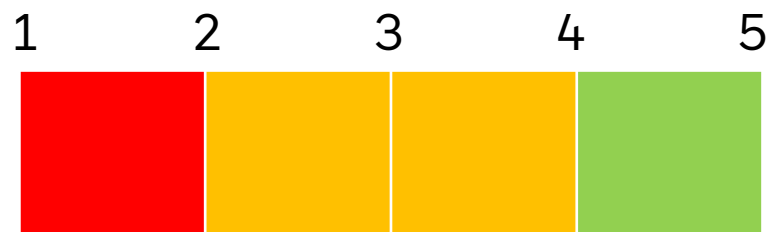
Er byrådsavd. involvert i alvorlige hendelser og avvik?	Har ikke vært noen	Litt varierende	I varierende grad. Virksomheter skal oppdatere rutiner	Virksomhetene skal varsle	Har ikke vært noen siste periode	Blir inform-ert i den grad det har vært	Etatene har ikke rapportert (men 5 rapportert i VE)	Har rutiner og blir involvert	Har ikke vært i virksomhet, men involvert når det gjelder sektor-systemer
Er antall meldte avvik til DT rimelig?	Byr er ikke kjent med at det er meldt inn avvik	Det meldes avvik, uklar vurdering om det er riktig nivå	Vanskelig å vurdere – ikke entydige rutiner	Krevende å vite selv om antallet meldinger øker	Kun BYR har hatt brudd, meldt 2 til DT	Mener det er riktig nivå for 3 etater 1 har ikke god nok rutine	Vurderes at antallet er riktig	Vanskelig å fastslå, antar at det kan være under-rapportering	Ikke mottatt mld. om avvik, men usannsynlig at det ikke har fore-kommet

Avvik og hendelser - noen tall



Byrådsavdelingenes vurdering av status

	B1	B2	B3	B4	B5	B6	B7	B8	B9
Personvern	4	3-4	3	3-4	3	3	3	2	4+
Informasjons-sikkerhet	4	3-4	4-	3-4	4	3	3	3	4+



1 = veldig dårlig
(store mangler)

5 = veldig god
(alt er på plass og god kontroll)



Oppsummering

Utviklingen i kommunen går sakte i riktig retning:

- ▶ Stadig økt bevissthet og fokus generelt i kommunen
 - Stor etterspørsel etter kompetanse og bistand, spesielt på personvernområdet
 - Henvendelsene blir også mer krevende
 - Godt oppmøte på forum, møter og kurs
 - Sikkerhetsmåned 2020 – digital og med god oppslutning og gode tilbakemeldinger
- ▶ Nesten alle virksomheter har etablert roller som informasjonssikkerhetskoordinator og personvernkoordinatorer
 - 44 ISK, 43 PKO (2 hhv 3 virksomheter som mangler)
- ▶ Mange jobber godt med informasjonssikkerhet og personvern (men det er store forskjeller!)

Utfordringer - overordnet

- ▶ Kompetanse/opplæring
 - Mangelfull kompetanse og manglende bevissthet på alle nivåer
- ▶ Mangelfull modenhet på ledelsesnivå gir mangelfull styring og kontroll
- ▶ Svak prioritering og mangel på ressurser
- ▶ Teknisk kompleksitet og vedlikeholdsetterslep på IKT-området

Høye forventninger til digitale tjenester - stor endringstakt - stor og kompleks organisasjon - trusselbilde i stadig endring.

Utfordringer på informasjonssikkerhetsområdet

- ▶ Risikostyring og risikovurderinger – generelt stort ressurs- og kompetansebehov
 - Styringsprosesser; tydelige kriterier for akseptabelt risikonivå
 - Kartlegging av informasjonsverdier og verdivurdering av disse
 - Innarbeides i forebyggende aktiviteter; anskaffelser, utvikling
- ▶ Hendelser og avvik – identifisering, varsling, håndtering og rapportering og eskalering
- ▶ Kontinuitetsplanlegging og beredskap
 - Behov for å ha oppdaterte planer som er øvd er aktualisert med hendelser og skjerpet trusselbildet

Utfordringer på personvernområdet

- ▶ Ikke oppdaterte behandlingsoversikter
- ▶ Manglende databehandleravtaler
- ▶ Personvernkonsekvensvurderinger (DPIA)
 - Manglende gjennomføring når DPIA er påkrevd, dette gjelder også gamle systemer
 - Manglende rutiner og kompetanse for å gjennomføre nødvendige vurderinger
- ▶ Manglende eskalering/involvering ved avvik

Hvordan jobber vi videre med dette? (Byrådsavd. for finans)

- ▶ Løfte blikket og ha fokus på ønsket utvikling/mangel på nødvendig utvikling
- ▶ Hvordan vil vi legge til rette for nødvendige utvikling fremover
 - Oppfølging og veiledning i sektorer/virksomheter
 - Lage maler/veiledere
 - Strategisk kompetanseutvikling
 - Overordnet styringssystem
 - Krav i fellesføringer
- ▶ Innsikt gir grunnlag for videre prioriteringer og tiltak
 - Jobber mot politisk ledelse og beslutningstagere
- ▶ Nye rapporteringsmaler før sommeren
- ▶ Er det viktige områder eller temaer vi ikke «ser» i rapporteringene? (Dere kan komme med innspill i evalueringen)

Avslutning



Dette skjer fremover

- Kurs i risikovurdering av informasjonssikkerhet 02.juni
 - Klokken 09-1430
- Innsiktsarbeid knyttet til læringstilbud til koordinatorene
 - Spørreundersøkelse til alle koordinatorene
 - Vi kommer også til å ta kontakt med noen virksomheter for dybdeintervjuer.
- Neste forum 09.juni
- Det blir sendt ut en evaluering etter dette forumet som vi håper dere vil besvare