Oslo

Forum for informasjonssikkerhet og personvern

Onsdag 19. april

Sendingen starter 09:00

Program

09:00 - 09:05	**Velkommen og introduksjon til dagens program**
09:05 - 09:15	**Hva skjer på personvernområdet?** Maryke Silalahi Nuth
09:15 - 09:20	**Hva skjer på informasjonssikkerhetsområdet?** Åsmund Skomedal
09:20 - 09:35	**Oppsummering av LG/VE 2022**
09:35 - 09:45	**Vil du være med å teste den digitale Virksomhetsleders Egenerklæring (VE)?**
09:45 - 09:55	**Pause til å fylle kaffekoppen**
09:55 – 10:10	**Personvernombudet gjør opp status for personvernet i Oslo kommune i 2022 – Personvernombudets rapport** Morten Haug Frøyen
10:10 - 10:35	Hvordan styres informasjonssikkerhet i Oslo kommune? **Lars Martin Undhjem**
10:35 - 10:55	**Om sikkerhetstesting med CSIRT** Claudia Haubold, Alaa Ghanim, Randi Eskildsen
10:55 - 11:00	**Avslutning**

Oslo

Oslo

Hva skjer på personvernområdet?

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

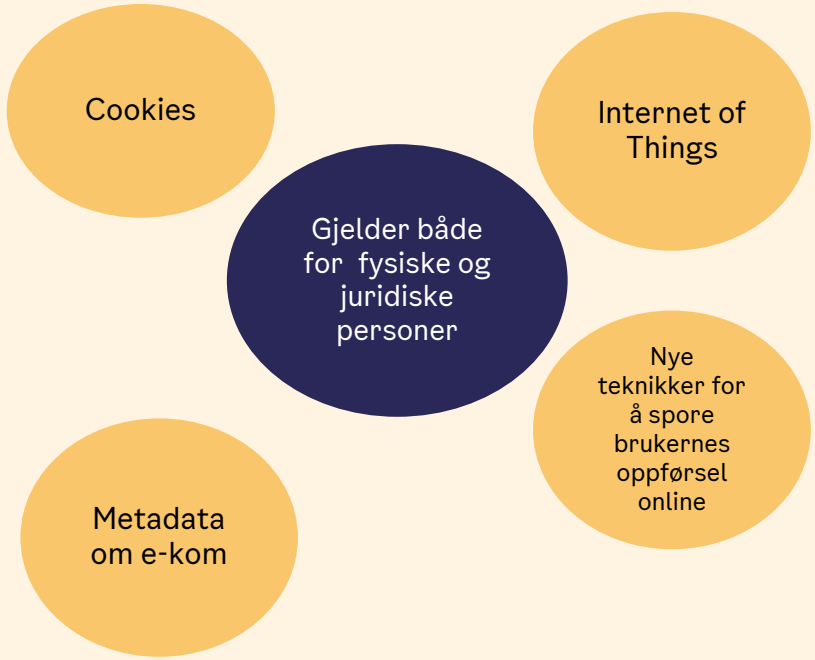
Forum for informasjonssikkerhet og personvern
19. april 2023

Hva skjer i EU?

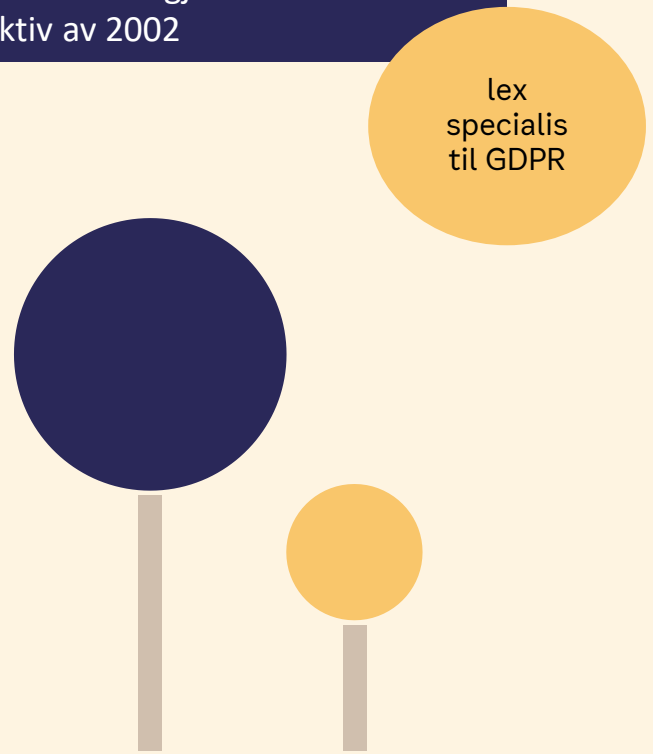
Status på den nye e-Privacy forordningen

Trilogforhandling mellom EU-rådet, Kommisjonen og Parlamentet 31.03.2023

- Forordningen vil kunne bli vedtatt i 2023 med en overgangsperiode på to år



En forordning som skal erstatte gjeldende kommunikasjonsdirektiv av 2002



Oslo

Hva skjer i Norge?

Innhold i brev fra Datatilsynet om tilsyn i kommuner i 2023:

4. Krav om redegjørelse

Vi ber kommunen sende oss følgende:

4.1 Kommunens behandlingsprotokoll, jf. personvernforordningen artikkel 30
4.2 Oversikt over kommunens organisering av ansvarsforhold knyttet til etterlevelse av personvernregelverket, jf. personvernforordningen artikkel 5 nr. 2
4.3 En kort beskrivelse av kommunens overordnede styringssystem (internkontroll) for etterlevelse av personvernregelverket, herunder hvilke verktøy som eventuelt brukes
4.4 Styrende retningslinjer for gjennomføring av risiko- og sårbarhetsanalyser, jf. personvernforordningen artikkel 32.
4.5 Kommunens eventuelle overordnede sikkerhetsstrategi
4.6 Oversikt over eventuelle IKT-samarbeid med andre kommuner
4.7 Styrende retningslinjer for autentiseringsløsninger i kommunen
4.8 Styrende retningslinjer for sikkerhetskopiering og gjenoppretting av systemer, jf. personvernforordningen artikkel 32.1.c)
4.9 Styrende retningslinjer/prosedyrer for sikkerhetsrevisjoner, jf. personvernforordningen artikkel 32.1.d)
4.10 Lenke til kommunens personvernerklæring
4.11 Informasjon om kommunens personvernombud, herunder:
- Navn, telefonnummer og e-postadresse til personvernombudet i kommunen
- Kort beskrivelse av organiseringen av personvernombudsfunksjonen; herunder hvor stor del av full stilling vedkommende skal kunne bruke på utøvelsen av rollen.
- Lenke til kommunens nettside som inneholder informasjon om personvernombudet

Aktuelle nyheter 2023

Tilsyn i kommuner og fylkeskommuner

Vi har satt i gang et større tilsynsarbeid med nærmere hundre norske kommuner og fylkeskommuner sin ivaretakelse av personopplysningssikkerheten.

– Kommunene oppbevarer store menger personopplysninger om innbyggerene sine, og har et stort ansvar for å ivareta dataene på en forsvarlig måte. Vi gjennomfører derfor et samlet *tilsyn* for å undersøke om personopplysningssikkerheten følges godt opp, sier fungerende seksjonssjef i Datatilsynet, Kristine Stenbro.

Tilsyn i to faser

Tilsynsarbeidet vil gjennomføres i to faser. Den første fasen består av en brevkontroll hvor 93 kommuner og fem fylkeskommuner har blitt kontaktet med spørsmål om etterlevelse av konkrete plikter som følger av personvernregelverket. I den andre fasen vil Datatilsynet på bakgrunn av svarene vi mottar i brevkontrollene, gjennomføre et antall stedlige tilsyn.

– Norske kommuner er sammensatte organisasjoner som behandler store mengder opplysninger om den norske befolkningen. Ivaretakelse av personopplysningssikkerheten er viktigere enn noensinne. Gjennom tilsynene håper Datatilsynet å kunne bidra til at kommunene blir enda bedre rustet til å håndtere personvernet og informasjonssikkerheten rundt opplysningene til befolkningen, forteller Stenbro.

Brevene ble sendt ut rett før påske, og svarfristen er 28. april.

Kontaktperson

Kristine Stenbro
fagdirektør
Kontor: +47 22 39 69 55
E-post: kristine.stenbro@datatilsynet.no

Camilla Nervik
seksjonssjef, seksjon for offentlige tjenester
Kontor: (+47) 22 39 69 29
E-post: cgn@datatilsynet.no

Publisert: 14.04.2023

Leveranser på personvernområdet (første halvår 2023)

Under arbeid:

- Veileder
  - retting og sletting
- Maler
  - personvernerklæringer
  - oppdatering og digitalisering av maler for personvernvurderinger
  - kartlegging av bruk av databehandleravtaler og behov for maler

Avvik

- Avviksmelding til Datatilsynet
  - kopi av melding skal sendes til ansvarlig byrådsavdeling personvernombudet og FIN/ISI ved fagsjef for personvern
- FIN/ISI har igangsatt arbeid med å se nærmere på avviksmeldinger fra Oslo kommune til Datatilsynet 2021-2022
  - oversikt over avvik meldt til Datatilsynet på overordnet nivå
    - kategorisering av avvik og tiltak
    - vil gi bilde av hvilke typer avvik som meldes til Datatilsynet
  - resultatet vil tilgjengeliggjøres til nytte for virksomhetene

Kurs

- Bruk av maler for personvernvurderinger
  - Nybegynner: 23. mars
  - Viderekomne: 15. mai
- Grunnleggende personvern
  - Behandlingsgrunnlag: 24. mai

Nettverksmøte

Nettverksmøte for bydeler: 15. juni

Har du spørsmål? Ta kontakt med din sektorkontakt i FIN/ISI Team personvern

	BLK	NOE	KIF	FIN	BYU	MOS	OVK	AIS	HEI	BYD
Sektorkontakt	Siri P. Johansen			Brit Røthe			Linda M. Knutsen	Siril Jonassen		Linda M. Knutsen

Generelle henvendelser sendes til fagsjef for personvern Maryke S. Nuth

Oslo

Informasjonssikkerhet - hva skjer

Oslo 19.04.2023

Åsmund Skomedal,
informasjonssikkerhetssjef
asmund.skomedal@byr.oslo.kommune.no

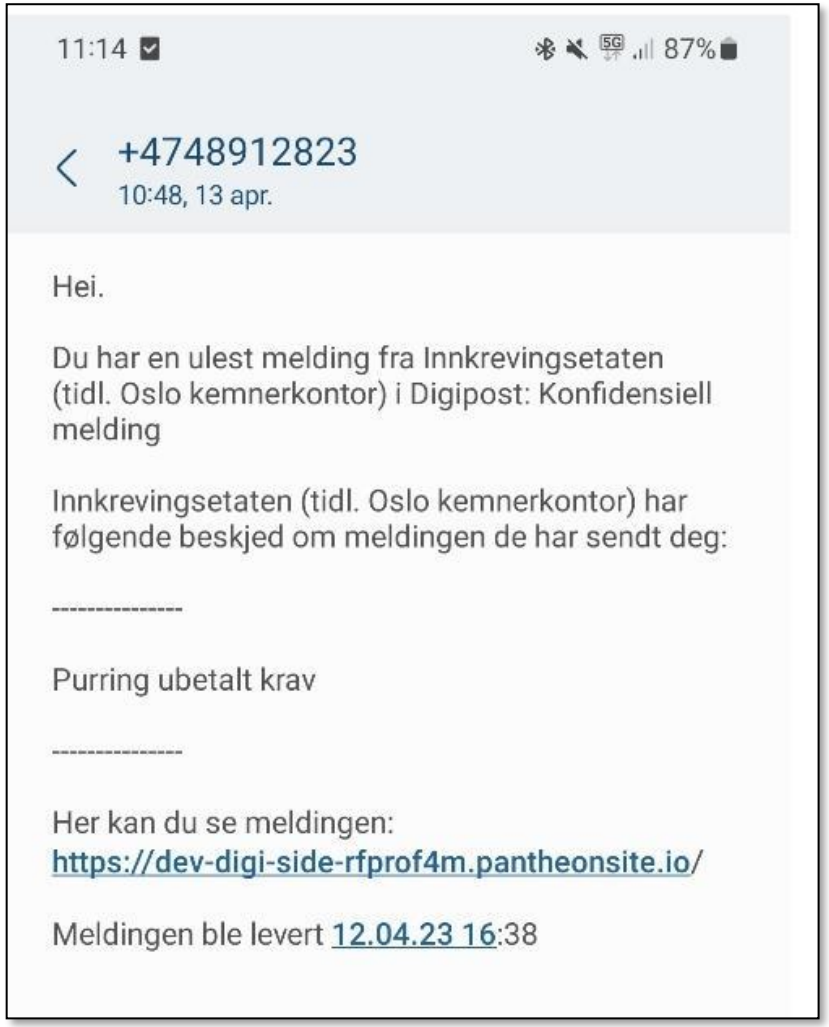
Foto: *Amara Husic*

Oslo

Hendelser og endringer

- **Ny SMS phishing 13. april**
  - Halvbra SMS
  - # er flagget som telefonsalg [hos 1881.no, 150 søk der samme dag]
  - Innkrevingsetaten misbrukt som avsender; purring på ubetalt krav
  - Strakstiltak: informere eksternt på web
  - Omfang: antagelig ikke veldig stort

- **Nye passord regler i Felles IKT-plattform**
  - Lange passord; minimum 16 karakterer
  - Ikke krav til tall og store bokstaver etc
  - Ikke pålagt regelmessig passordbytte
  - Støtte for «single-sign-on» mot flere applikasjoner
  - Verifisering med «to-faktor» ved direkte aksess (uten VPN)



Trusselbildet – Q1 2023

ENISA Foresight Cybersecurity Threats for 2030 [fra mars]

1. SUPPLY CHAIN COMPROMISE OF SOFTWARE DEPENDENCIES
2. ADVANCED DISINFORMATION / INFLUENCE OPERATIONS (IO) CAMPAIGNS
3. RISE OF DIGITAL SURVEILLANCE AUTHORITARIANISM / LOSS OF PRIVACY
4. HUMAN ERROR AND EXPLOITED LEGACY SYSTEMS …
5. TARGETED ATTACKS (E.G. RANSOMWARE) ENHANCED BY SMART DEVICE DATA
6. LACK OF ANALYSIS AND CONTROL OF SPACE-BASED INFRASTRUCTURE AND OBJECTS
7. RISE OF ADVANCED HYBRID THREATS
8. SKILL SHORTAGES
9. CROSS-BORDER ICT SERVICE PROVIDERS AS A SINGLE POINT OF FAILURE
10. ABUSE OF AI

NSM

- **Sikkerhetspulsen = 1**
- **TikTok og Telegram vurderingen**

Anbefaling om TikTok og Telegram

Forankret hos byråden for finans

Fra: kommunaldirektør i FIN
Til: alle byrådsavdelinger og virksomheter

- NSMs faglige vurdering er

  «… at TikTok eller Telegram ikke bør installeres på offentlig ansattes tjenesteenheter som er tilknyttet virksomhetens interne digitale infrastruktur eller tjenester…»
  [«Tiltakene omtalt her bør rettes mot ansatte i offentlig sektor.»]

- Justis- og beredskapsdepartementet

  fraråder å ha TikTok og Telegram på tjenesteenheter. Dette gjelder politisk ledelse og ansatte i departementene og deres underlagte virksomheter.

- Oslo kommune

  fraråder å ha TikTok og Telegram installert på mobile tjenesteenheter i kommunens virksomheter. Byrådsavdelingene bes følge opp anbefalingen overfor virksomhetene i egen sektor.

Overordnet status for informasjonssikkerhet 2022

Prosess for LG/VE rapportering

Drift

Virksomhetsleders egenerklæring

VE

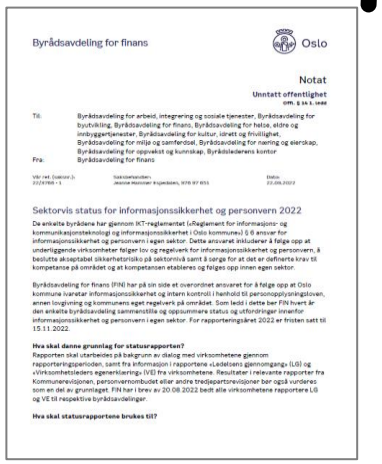
LG

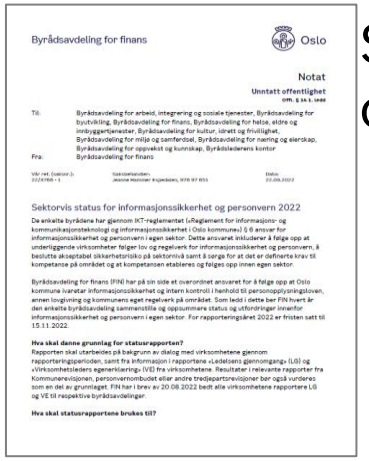
Sektorvis oppsummering

Status Oslo kommune, FIN

Beslutning om overordnede tiltak for kommunen

B-notat


Byrådsavdeling for finans
Oslo
Notat
Unntatt offentlighet
Sektorvis status for informasjonssikkerhet og personvern 2022


Byrådsavdeling for finans
Oslo
Notat
Unntatt offentlighet
Sektorvis status for informasjonssikkerhet og personvern 2022

Sektor-oppsummering

Arbeid og ansvar på **sektor**nivå (2020-2022)

2022	BYR 1	BYR 2	BYR 3	BYR 4	BYR 5	BYR 6	BYR 7	BYR 8	BYR 9
Har byrådsavd. etablert roller og rutiner intern i egen avd. og i styrings-dialogen?									
(2020)									
Er byrådsavd. involvert i alvorlige hendelser og avvik?									
(2020)									
Igangsatt arbeid med akseptabel risiko for sektoren?									
(2020)									

Arbeid og ansvar i sektorenes **virksomheter** (2020)

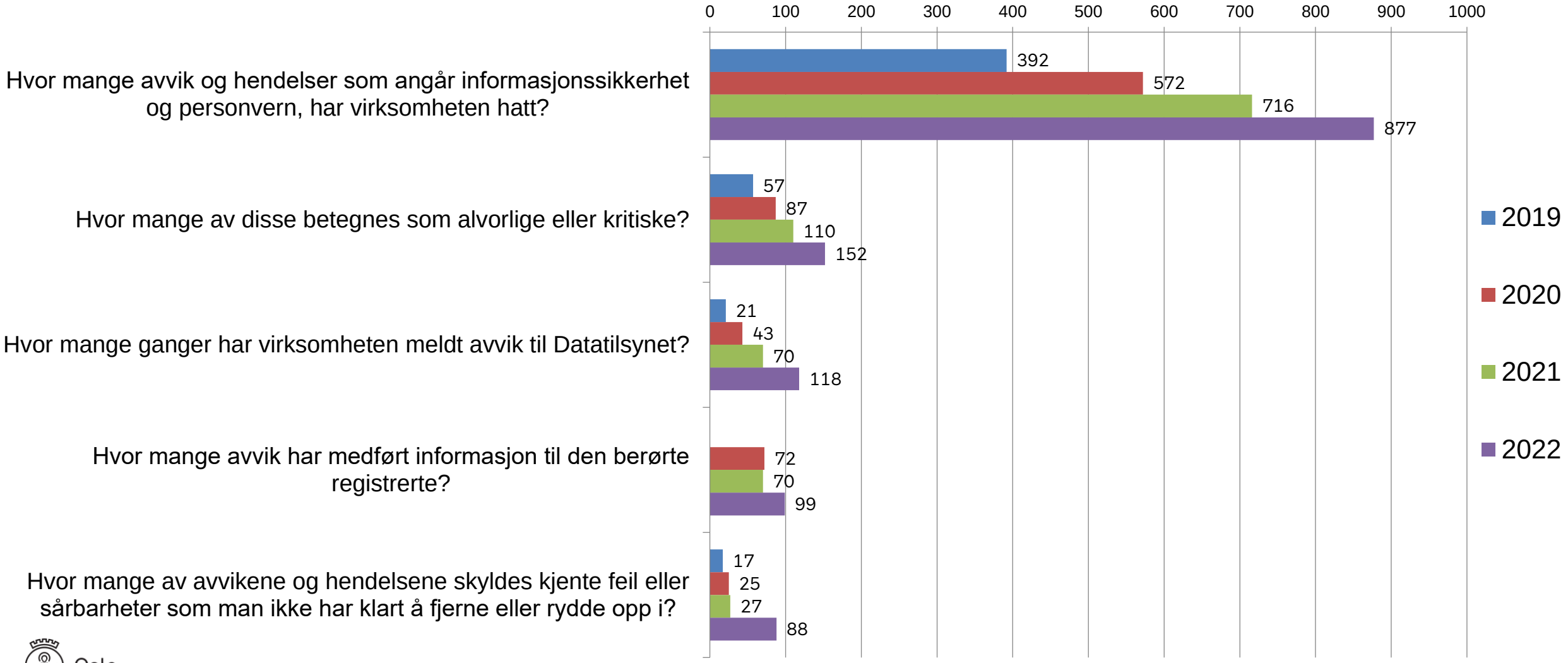
2020	BYR 1	BYR 2	BYR 3	BYR 4	BYR 5	BYR 6	BYR 7	BYR 8	BYR 9
Har virksomhetene etablert internkontroll									
Kartlegging og verdivurdering av informasjonsverdier									
Gjennomføres risikovurderinger – systematisk og på flere nivåer									
Beslutning om akseptabelt risikonivå for virksomhetene									
Etablert systematikk som sikrer tilstrekkelig kompetanse									

Arbeid og ansvar i sektorenes **virksomheter** (**2022**)

2022	BYR 1	BYR 2	BYR 3	BYR 4	BYR 5	BYR 6	BYR 7	BYR 8	BYR 9
Har virksomhetene etablert internkontroll									
Kartlegging og verdivurdering av informasjonsverdier									
Gjennomføres risikovurderinger – systematisk og på flere nivåer									
Beslutning om akseptabelt risikonivå for virksomhetene									
Etablert systematikk som sikrer tilstrekkelig kompetanse									

Avvik og hendelser … ☹ eller ☺ ?

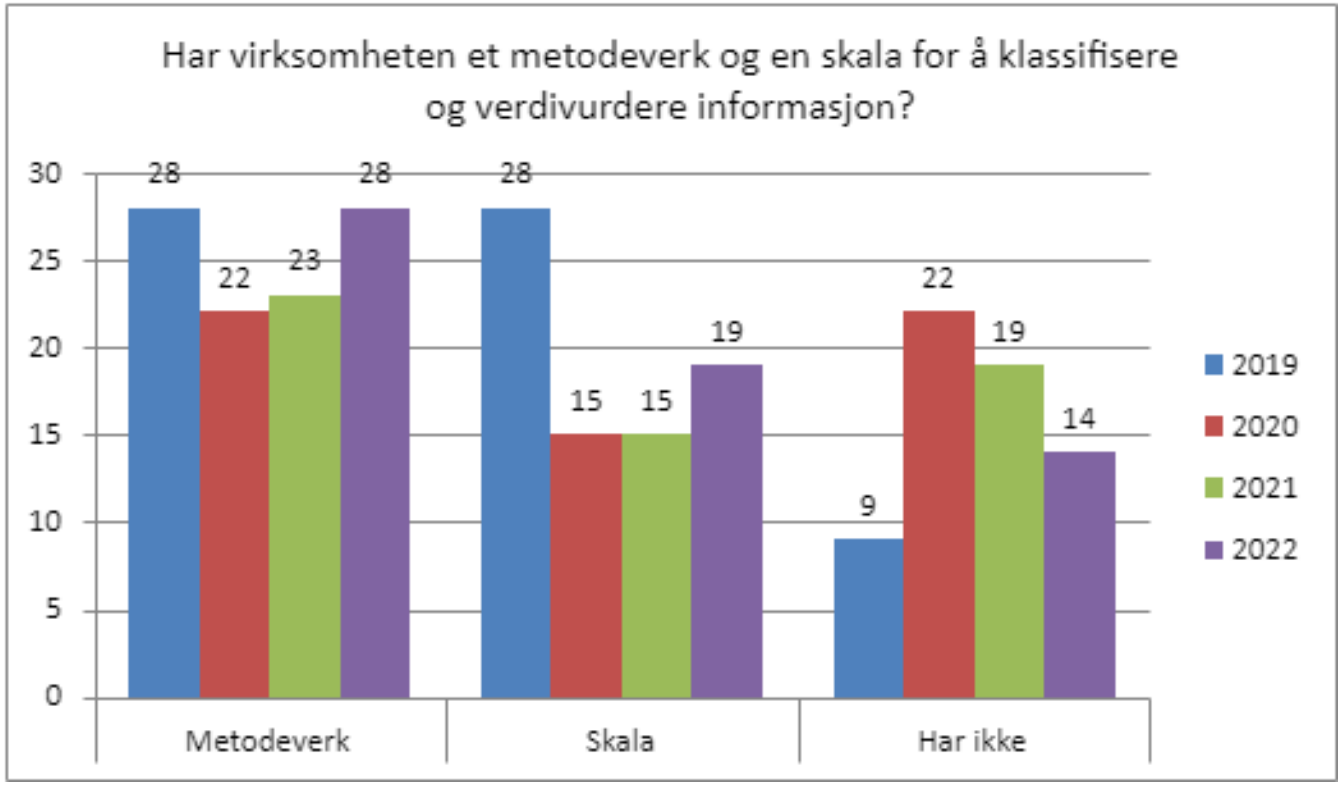
Tall for 2022



Oslo

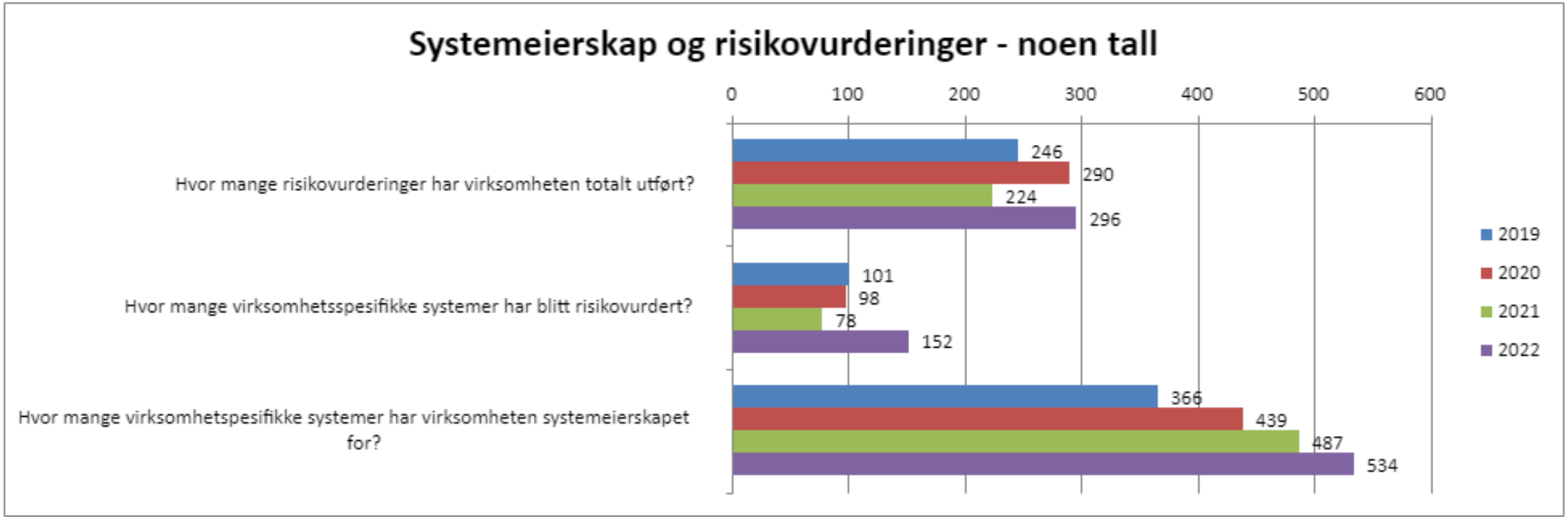
#2 Kjenner virksomhetene informasjonsverdiene?

2022	BYR 1	BYR 2	BYR 3	BYR 4	BYR 5	BYR 6	BYR 7	BYR 8	BYR 9
Kartlegging og verdivurdering av informasjonsverdier									
(2020)									



#3 Risikovurderinger – noen tall (2019-2022)

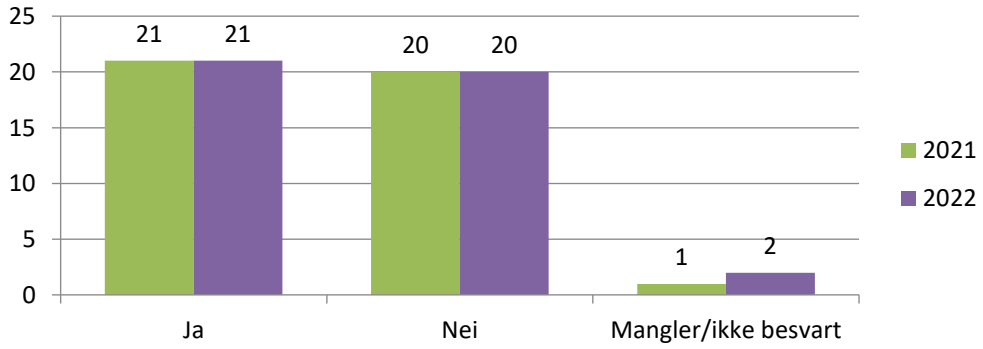
2022	BYR 1	BYR 2	BYR 3	BYR 4	BYR 5	BYR 6	BYR 7	BYR 8	BYR 9
Gjennomføres risikovurderinger – systematisk og på flere nivåer?									
(2020)									



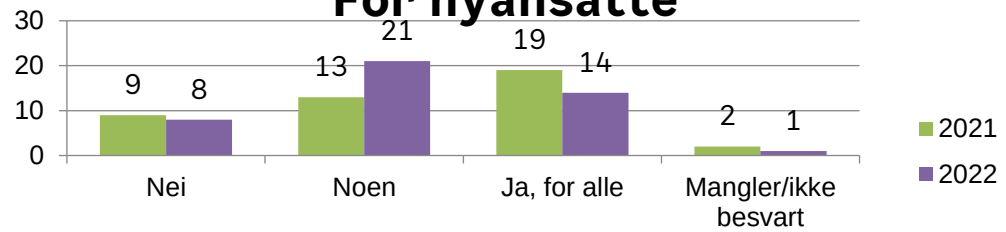
#5 Ressurser og kompetanse – noen tall (2021-2022)

2022	BYR 1	BYR 2	BYR 3	BYR 4	BYR 5	BYR 6	BYR 7	BYR 8	BYR 9
Etablert systematikk som sikrer tilstrekkelig kompetanse									
(2020)									

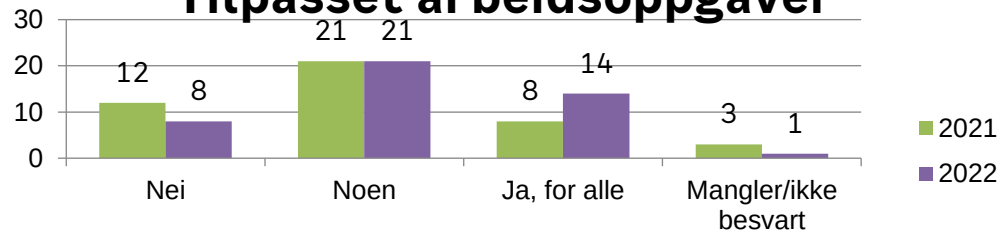
Har virksomhetene systematikk for å planlegge og gjennomføre kompetanseaktiviteter innenfor informasjonssikkerhet og personvern?



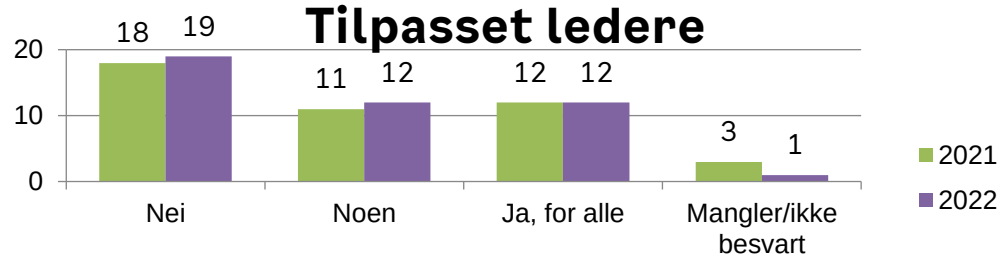
For nyansatte



Tilpasset arbeidsoppgaver



Tilpasset ledere



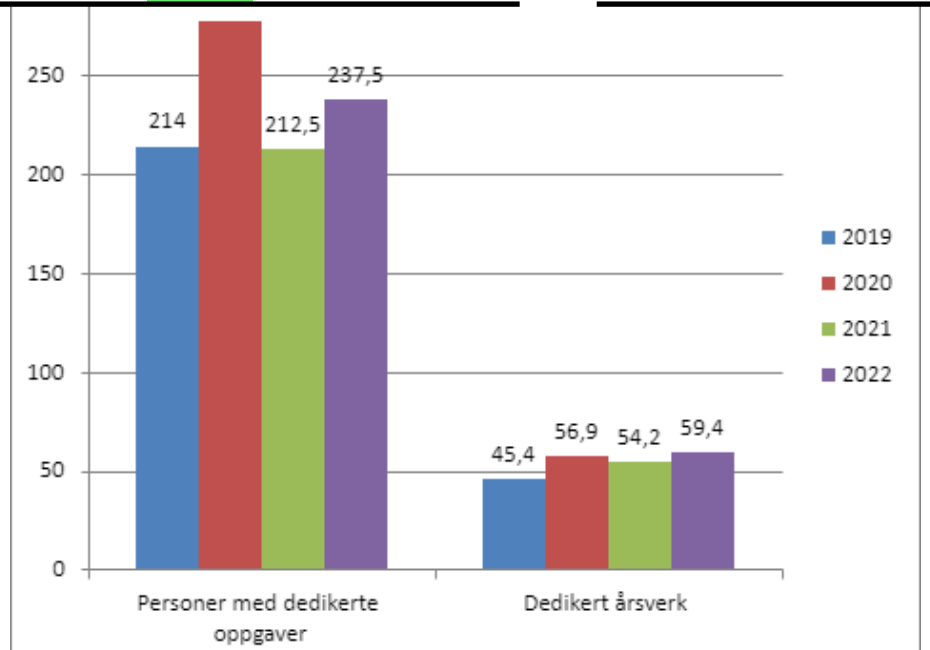
Med flere datakilder blir bildet mer nyansert …

Virksomhetsleders Egenerklæring (VE) 2022

VE rapportering 2022	Ja	delv.	nei
Har styringssystem	19	18	5
Systematiske risikovurderinger	21	23	0
Har kontinuitetsplaner	21	18	9
Har gjennomført øvelse	3		

Revisjon av kontinuitetsplaner for bortfall av IKT

Internrevisjon 2022	ja	delv.
Oppdatert risikovurdering	9	22
Har kontinuitetsplaner	10	28
Jevnlig øvelse på kontinuitetsplan	4 av	de 10



Oslo

Byrådsavdelingenes vurdering av status (2020-2022)

2022	BYR 1	BYR 2	BYR 3	BYR 4	BYR 5	BYR 6	BYR 7	BYR 8	BYR 9
Informasjons-sikkerhet	**4**	**3-4**	**3-4**	**3-4**	**4**	**3-4**	**4**	**3,5**	**2-4**
(2020)	4	3	3-4	3-4	4	4-	4+	3,4	3
Personvern	**4**	**4-**	**3-4**	**4**	**4**	**3+**	**4**	**3,5**	**2+**
(2020)	3	3	3-4	3	4	3	4+	3,4	2

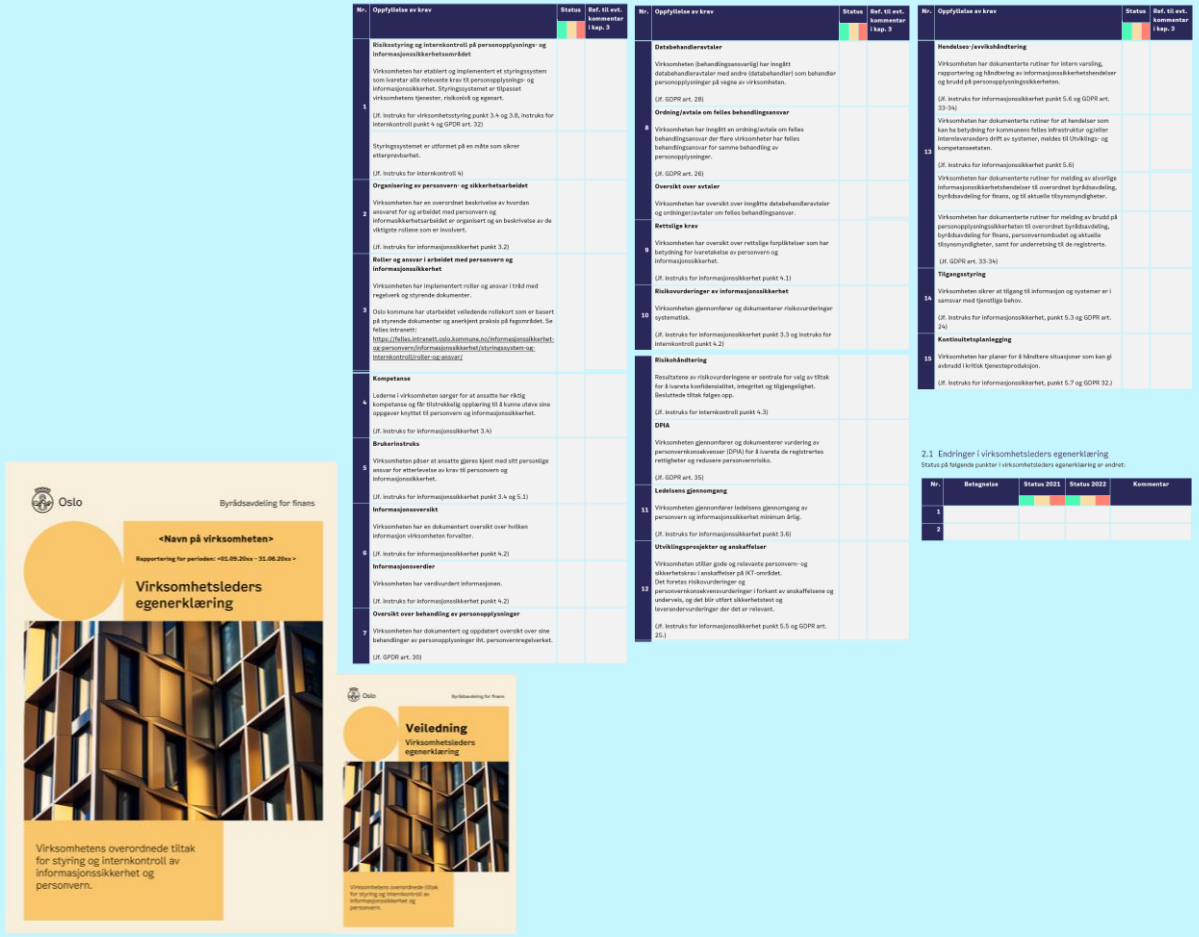
1 2 3 4 5

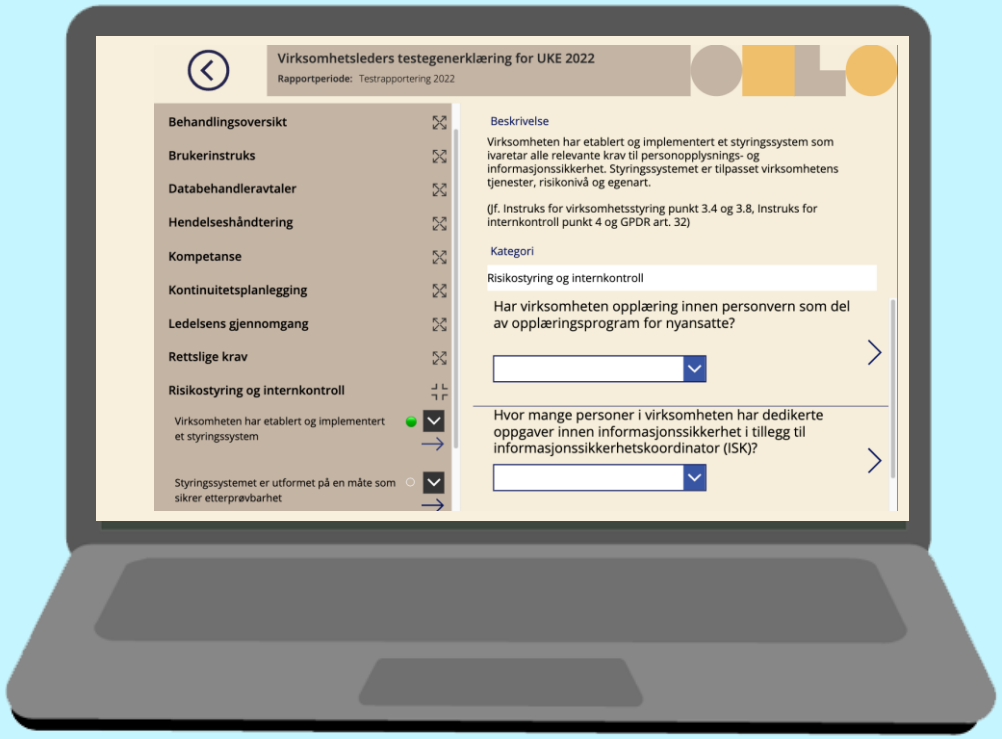
1 = veldig dårlig (store mangler)

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

Foto: irpp.org, Creativ

Rapporteringsprosessen – fra papir til digital løsning, vil du være med?





Rapportering og oppsummering av status PV og IS

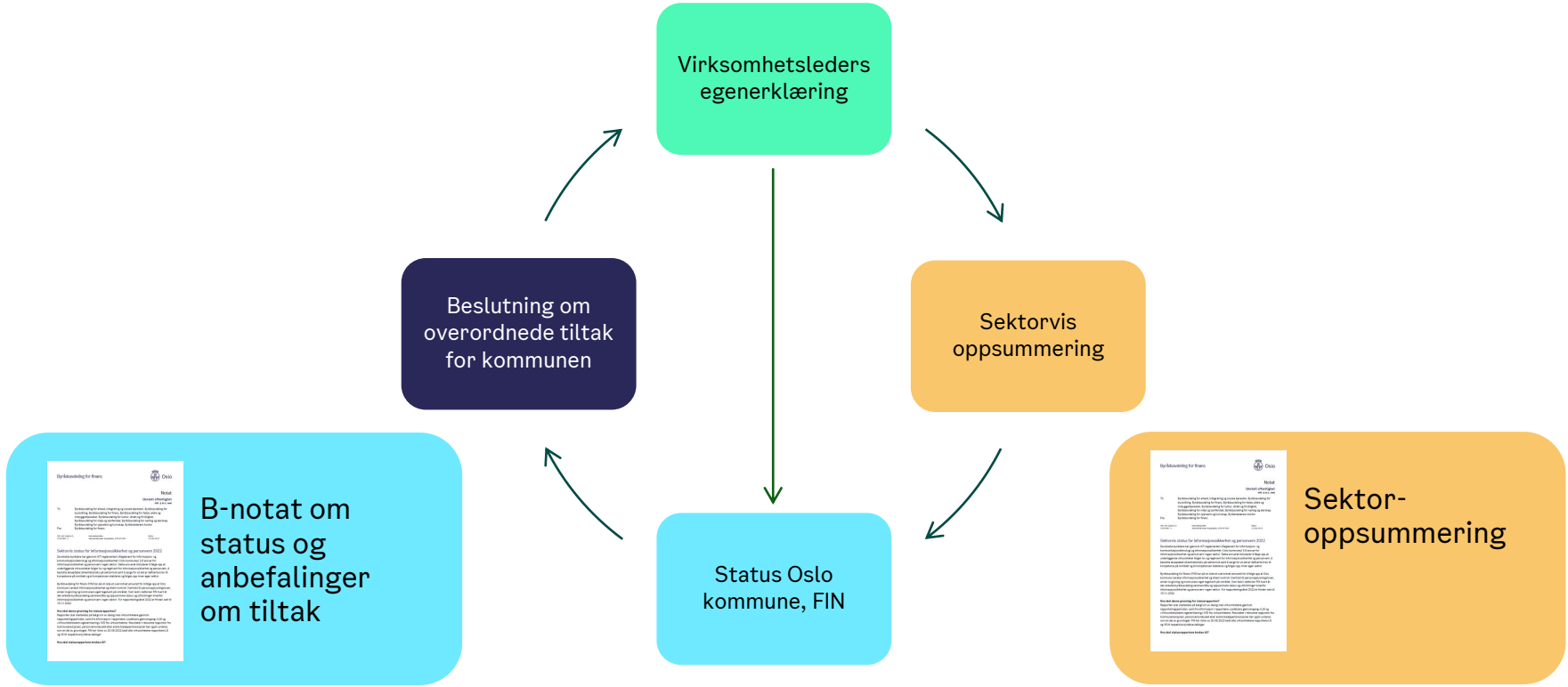
LG – Ledelsens gjennomgang

Intern aktivitet i virksomhet/etat/bydel for å følge opp, forbedre og effektivisere styringen av PV- og IS-arbeidet

VE – Virksomhetsleders egenerklæring

Samsvarsvurdering på 15 områder i 2022 med oppfølgingsspørsmål for noen av områdene.

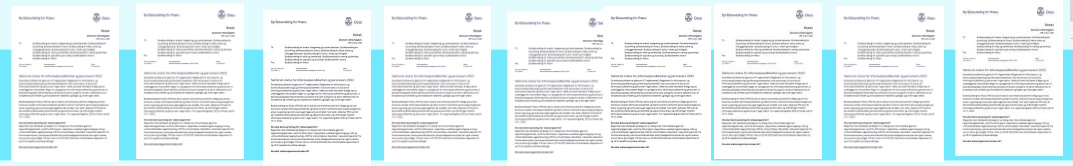
Grønt
Gult
Rødt



Byrådet **beslutter tiltak**

B-notat om status og anbefalinger om tiltak

Byrådsavdeling for finans

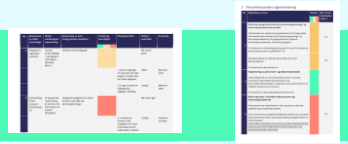


Sammen-stiller 9 sektorer

Byrådsavdeling

Sektor-oppsummering

Virksomhet



Leverer LG og VE

SPARER TID

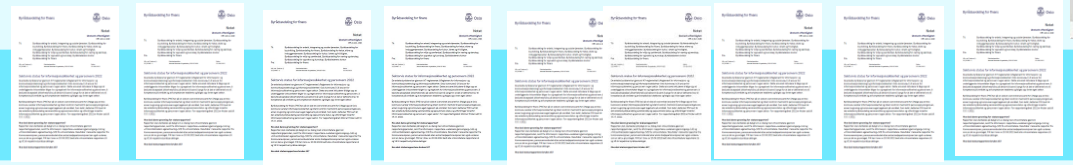
BEDRE DATAGRUNLAG

SER UTVIKLING OVER TID

Byrådet **beslutter tiltak**

B-notat om status og anbefalinger om tiltak

Byrådsavdeling for finans



Sammen-stiller 9 sektorer

Byrådsavdeling

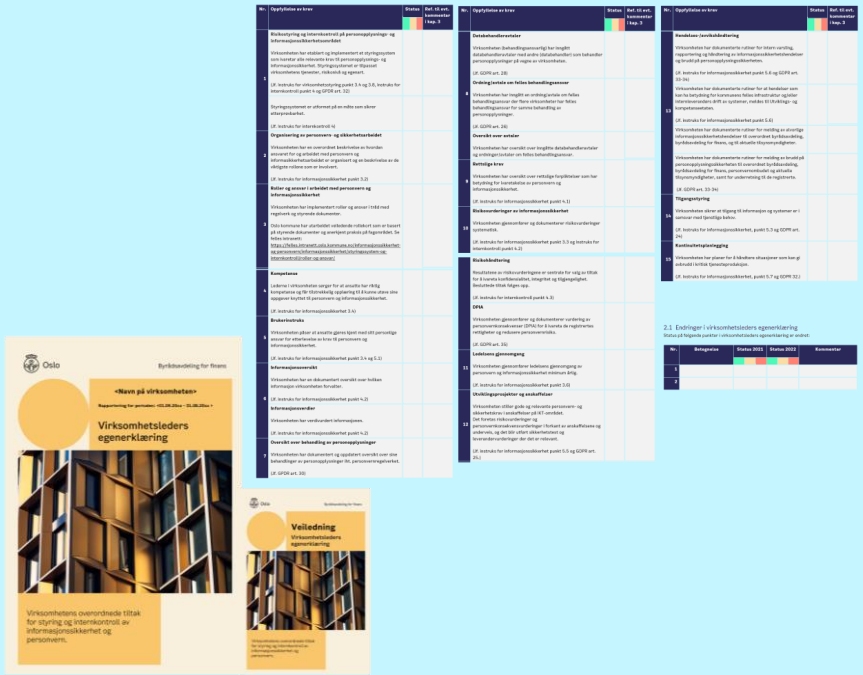
Sektor-oppsummering

Virksomhet

Leverer LG og VE

Vil du være med?

Hybrid i år – valgfritt om rapportering gjøres på papir i eller i ny løsning



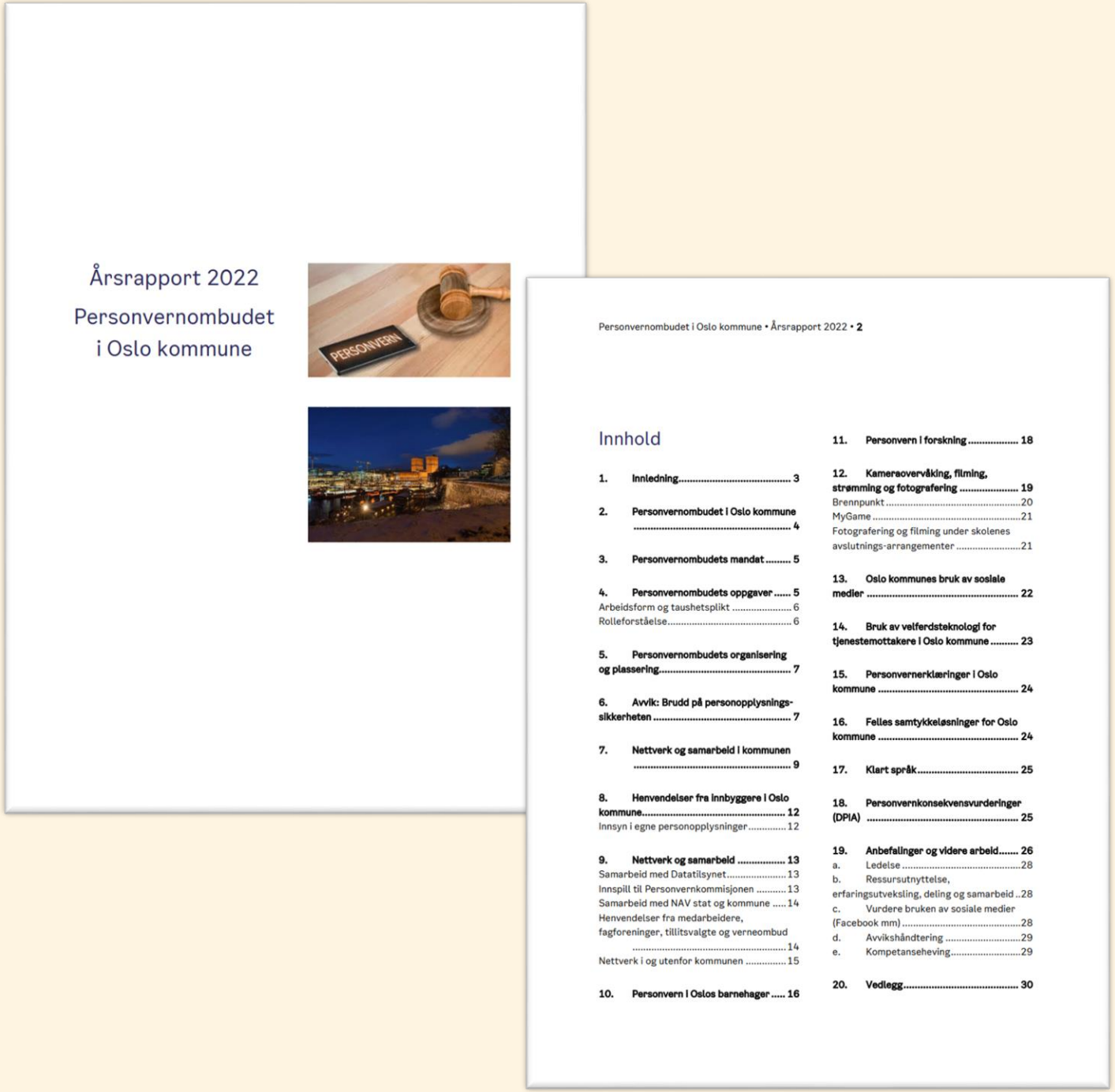
Oslo

Årsrapport 2022

Personvernombudet
i
Oslo kommune

Årsrapport 2022 - innhold

1. Innledning
2. Ombudet; mandat og oppgaver, organisering og plassering
3. Avvik
4. Samarbeid
5. Noen utvalgte saker
6. Anbefalinger og videre arbeid


Årsrapport 2022

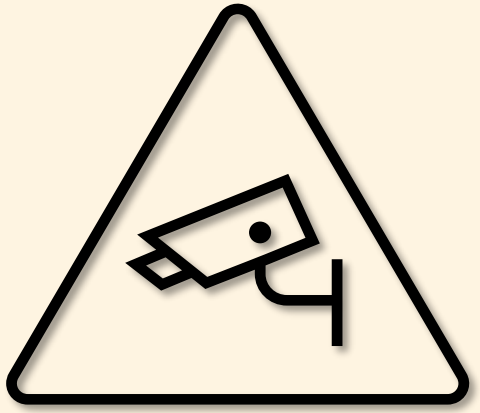
Personvernombudet i Oslo kommune

Innhold

Oslo

Noen utvalgte saker

- Personvern i barnehager
- Personvern i forskning
- Kameraovervåking
- Oslo kommunes bruk av sosiale medier
- DPIA
- Klart språk



Anbefalinger og videre arbeid

- ✓ Ledelse
- ✓ Rolleavklaringer
- ✓ Ressurser

- ✓Vurdere bruken av sosiale medier
- ✓Avvikshåndtering
- ✓Kompetanseheving

Hvordan styres informasjonssikkerhet i Oslo kommune?

Lars Martin Undhjem, FIN/ISI

Forum 19.april 2023

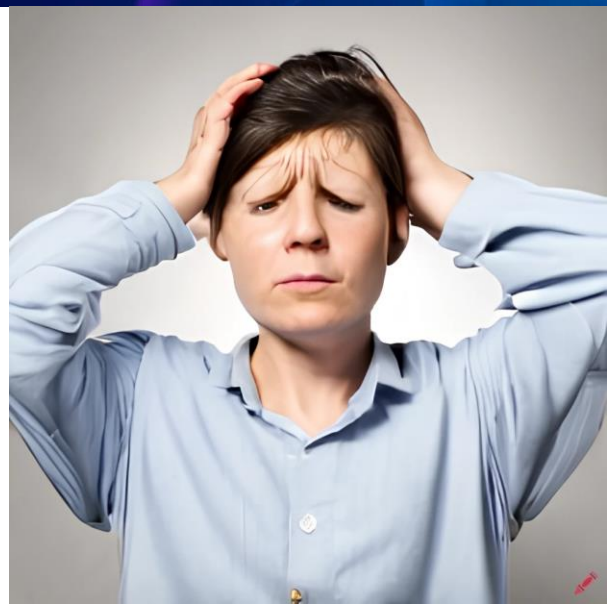
Oslo

Hvem har egentlig ansvaret for informasjonssikkerhet?

- Hvem bestemmer hvilken informasjon som er verdifull?
- Hvem har ansvaret for å beskytte informasjonsverdiene?
- Hvem har ansvaret for at systemene våre er trygge?
- Hvem setter retningslinjer for bruk av PCer og mobile enheter?
- Hvem bestemmer hvilke apper vi kan installere?

Spørreundersøkelse

Hvem kan vi spørre tro?



LA snakker du norsk?

Ja, jeg kan snakke norsk. Hvordan kan jeg hjelpe deg i dag?

LA Jeg lurer på hvem som har ansvar for informasjonssikkerheten i Oslo kommune

I Oslo kommune er det kommunens ledelse og administrasjon som har det overordnede ansvaret for informasjonssikkerheten. Dette ansvaret er delegert til et eget sikkerhetsstyre, som har ansvar for å etablere og opprettholde en helhetlig og koordinert sikkerhetsstyring i kommunen.

I tillegg har Oslo kommune et eget informasjonssikkerhetsprogram som skal sikre at kommunen håndterer personopplysninger og annen sensitiv informasjon på en trygg og forsvarlig måte. Programmet er utarbeidet av kommunens IT-avdeling og inneholder blant annet retningslinjer og rutiner for håndtering av informasjonssikkerhet.

Det er også etablert en egen informasjonssikkerhetsgruppe i Oslo kommune som har ansvar for å koordinere og samordne arbeidet med informasjonssikkerhet på tvers av kommunens virksomheter.

Nei, vi får vel lete internt i kommunen i stedet..

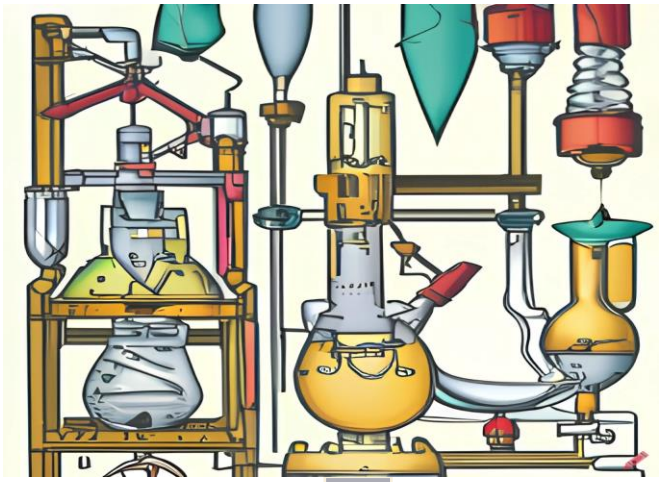
Reglement for informasjons- og kommunikasjonsteknologi og informasjonssikkerhet

Instruks for informasjonssikkerhet

Instruks for virksomhetsstyring

Instruks for internkontroll

Reglement for Oslo kommunes arbeid med samfunnssikkerhet, beredskap og sikkerhet

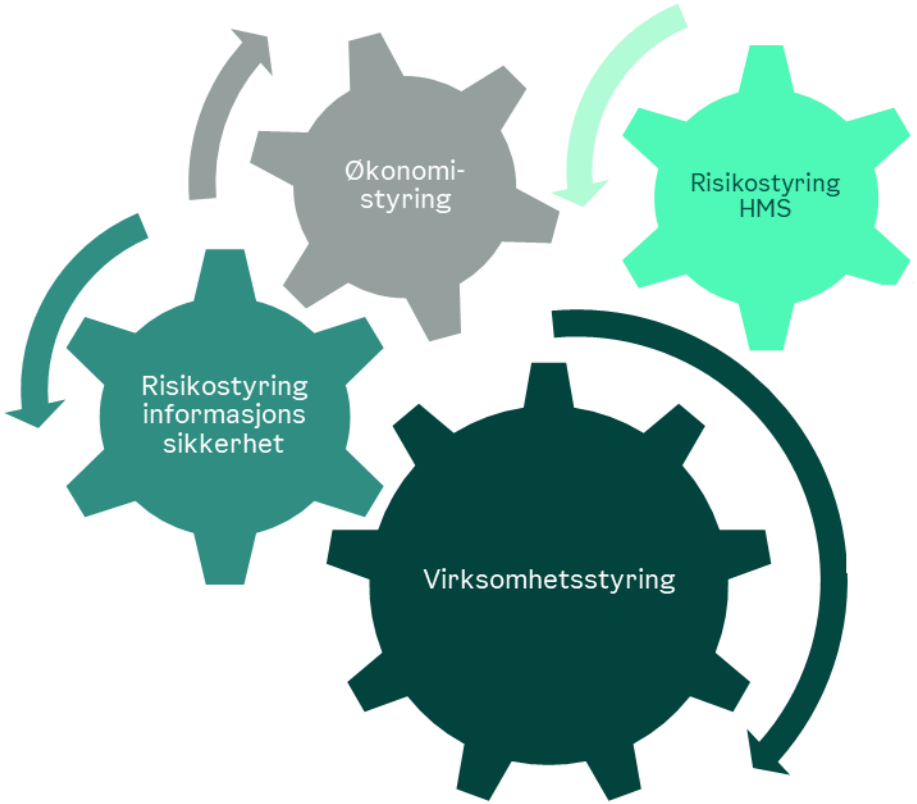


Svaret!?

Grunnprinsipp: Styring av informasjonssikkerhet er integrert i øvrig virksomhetsstyring

- Informasjonssikkerhet er et eget fagområde, men følger etablert måte å styre på i kommunen i likhet med alle andre områder (økonomi, HMS, måloppnåelse osv.)
- Alle disse områdene handler om det samme: Risikostyring for at virksomheten skal nå sine mål

Det er viktig at informasjonssikkerhet ikke er en sideaktivitet, men en iboende del av eksisterende styring



Det er i virksomhetene det skjer

Det er virksomheten selv som har ansvaret, også for sikkerheten

...men...

Byrådsavdelingene har også et ansvar

- Særlig to viktige ansvarsområder:
  - Etatsstyring av sine virksomheter
  - Systemeierskap for felles- eller sektorsystemer
- I tillegg:
  - Holde oversikt over sektorspesifikke krav og formidle disse til virksomhetene
  - Støtte håndtering av rapporterte avvik og hendelser i virksomhetene ved behov
  - Sammenstille og oppsummere status i sin sektor, og rapportere videre til FIN

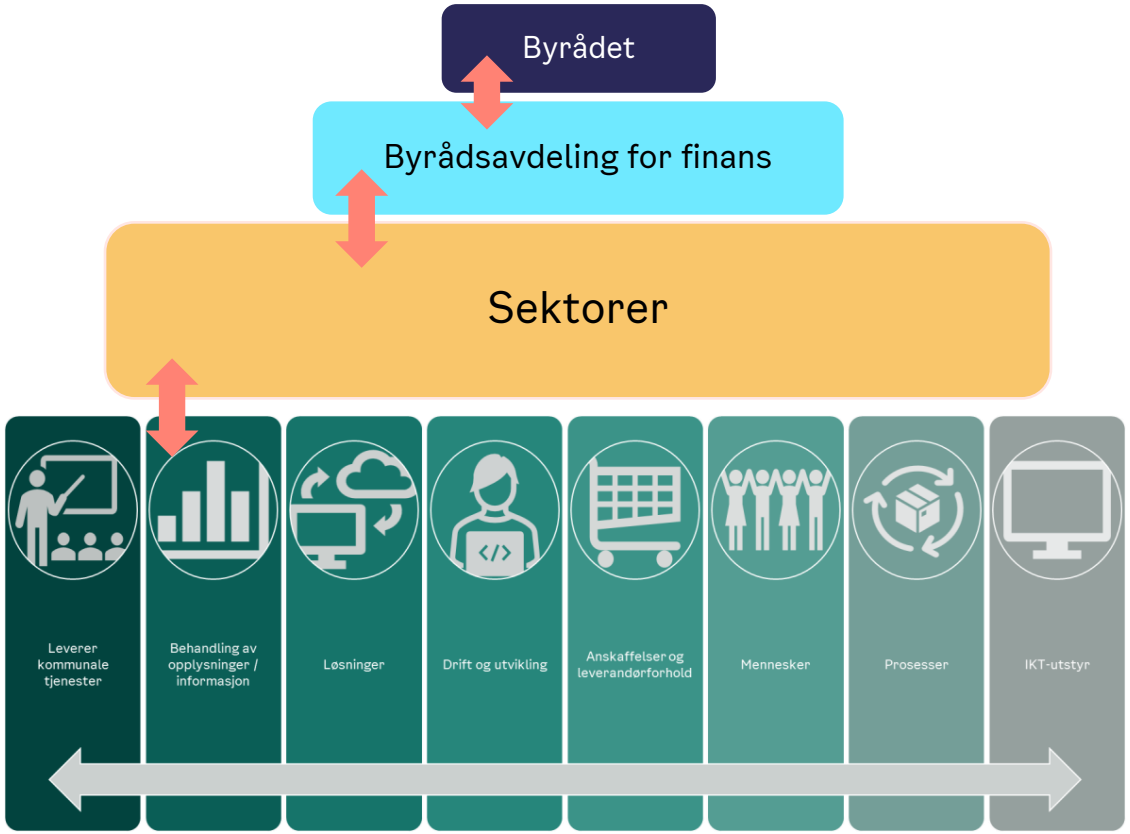
FIN har et overordnet ansvar

Reglement for informasjons- og kommunikasjonsteknologi og informasjonssikkerhet §4

Men hva betyr det overordnede ansvaret egentlig?

Delvis uklart, men vi kan nok trygt si dette:

- Holde oversikt over felles krav
- Utvikle metodeverk (verktøy, maler, kurs)
- Rapportering fra sektorene gjennom VE-prosess
- Oppsummerer og informerer om status til byrådet



Systemeier har ansvar for informasjonssikkerheten til systemet

- Lovkrav og interne føringer etterleves
- Risikovurderinger brukes for å identifisere nødvendige og riktige tiltak
- Følge opp akseptabel risiko
- Sikkerhet reguleres i avtaler
  - Forvalteravtaler med systemforvalter
  - Leverandøravtaler med eksterne leverandører
- Gir bestemmelser for bruk av systemet
- Internkontroll
  - Etterlevelse av lovkrav og interne føringer
  - Etterlevelse av avtaler
  - Etterlevelse av tiltaksplan

Hva utgjør et system? Ikke alltid enkelt å avgrense til et «program».

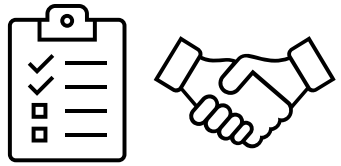
Vi tenker for eksempel på felles IKT-plattform som et system, med FIN som systemeier.

Ansvaret for et system kan likevel være komplisert

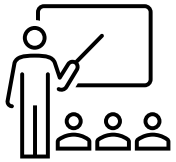
IKT-reglementet gir ikke alle svar på disse utfordringene

– bl.a. nevnes knapt eksterne leverandører

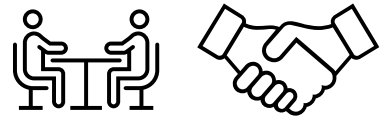
Virksomhet er systemeier



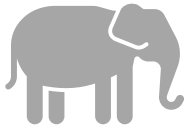
Byrådsavdeling er systemeier – virksomhet systemforvalter



Bydel og/eller annen virksomhet bruker systemet i sine tjenester



Systemet er en del av et større økosystem med eksterne leverandører og skytjenester



Jo mer komplisert leveransekjede, jo viktigere er det at

- beslutningsansvar, styrings- og rapporteringslinjer er klart definerte, dokumenterte og tydelige for alle parter
- gode avtaler utarbeides og følges opp
- det finnes tydelige retningslinjer som gjelder for bruk av systemet (basert på risikovurdering)

Hvem har egentlig ansvaret for informasjonssikkerhet?

- Hvem bestemmer hvilken informasjon som er verdifull?
- Hvem har ansvaret for å beskytte informasjonsverdiene våre?
- Hvem har ansvaret for at systemene våre er trygge?
- Hvem setter retningslinjer for bruk av PCer og mobile enheter?
- Hvem bestemmer hvilke apper vi kan installere?

Virksomheten

Plattformeier

Virksomheten

Leverandører

FIN: Metode og verktøy innen informasjonssikkerhet, eierskap til felles IKT-plattform

UKE: Sikkerhetsmekanismer i felles infrastruktur, systemforvalter for plattform++

ORIGO: Sikkerhet og sikker kode i egenutviklede løsninger, eierskap til egen plattform (AWS)

Styring og kontroll

- Styringssystem for informasjonssikkerhet er virksomhetens verktøy for sikkerhetsstyringen
- Styringssystemet skal bidra til at vi
  - Beskytter de riktige tingene
  - Beskytter dem fra de riktige truslene
  - Beskytter dem tilstrekkelig - ikke for mye og ikke for lite
- Styringssystemet skal sørge for at det iverksettes systematiske sikkerhetstiltak
  - Organisasjon
  - Mennesker
  - Teknologi
- Ønskede effekter av styringssystemet er
  - Å unngå/motstå uønskede hendelser og håndtere dem når det skjer
  - Kostnadseffektivitet i sikkerhetstiltakene som innføres

Spørreundersøkelse

Hver enkelt virksomhet må ha et styringssystem for informasjonssikkerhet

..men vent litt

«Kan ikke noen i kommunen sentralt bare lage et styringssystem for oss?»

- Virksomheter har ulike oppgaver, ulik størrelse, ulik kompleksitet og ulik IKT-portefølje
- Alle er ikke engang på samme IKT-plattform
- Oslo kommune er ikke et konsern og kan ikke bruke den vanlige konserntilnærmingen med en sentral funksjon som tar hånd om fagområdet

Oslo kommune er for stor, for variert og for kompleks til at vi kan ha ett styringssystem som dekker hele kommunen

Krav

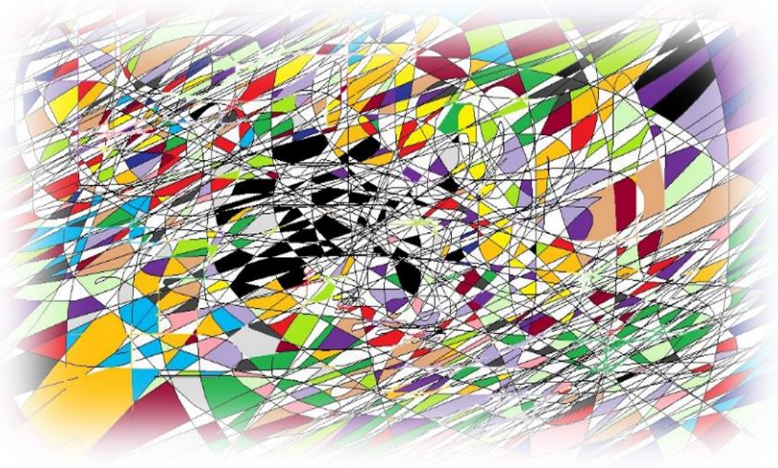
- Virksomheten treffes av en mengde krav innen informasjonssikkerhet
- Det finnes ingen standardisering, så virksomheten står alene i å kartlegge og etterleve kravene
- Det finnes lite støttemateriale fra sentralt hold
- Det er ikke så mye samarbeid mellom virksomhetene på området

Kan vi gjøre noe for å forbedre situasjonen?

Det ser ut som en stor del av kravene er felles?

I hvilken grad kan vi standardisere arbeidet med informasjonssikkerhet?

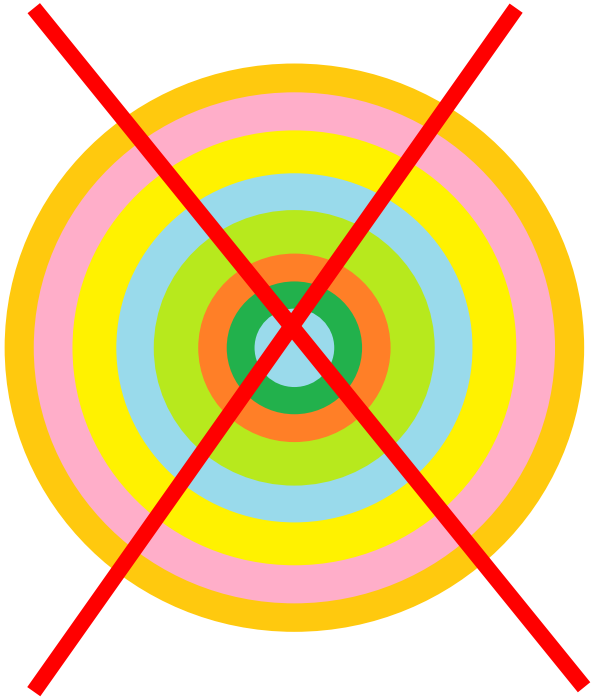
- I dag er styringen for det meste fragmentert



I hvilken grad kan vi standardisere arbeidet med informasjonssikkerhet?

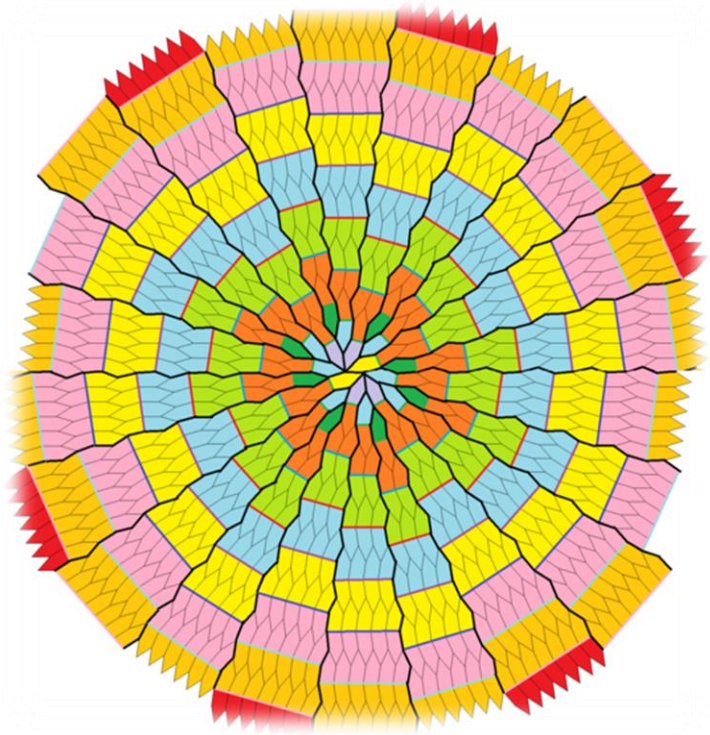
- I dag er styringen for det meste fragmentert

- Vi har sett at vi kan ikke lage et felles, ensartet styringssystem



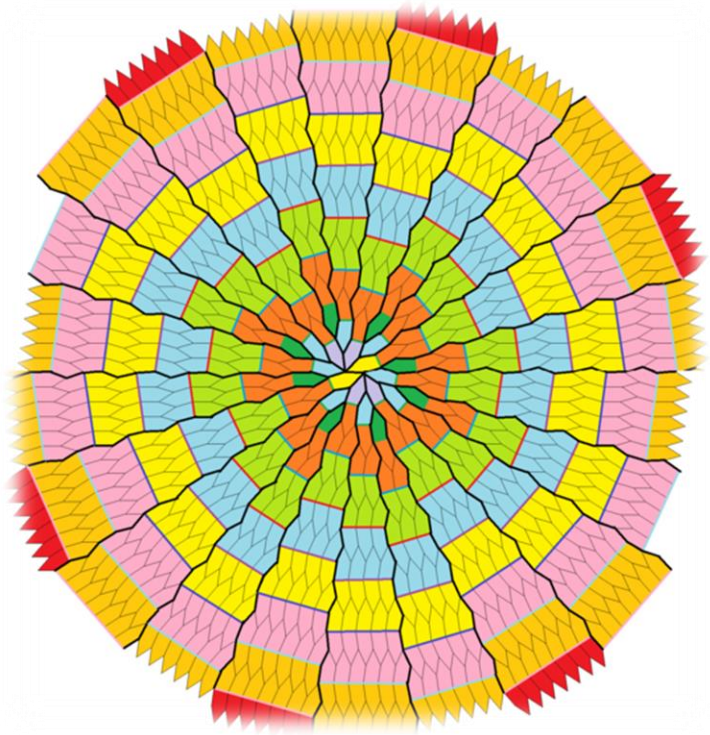
I hvilken grad kan vi standardisere arbeidet med informasjonssikkerhet?

- I dag er styringen for det meste fragmentert
- Vi har sett at vi kan ikke lage et felles, ensartet styringssystem
- Men, det er kanskje mulig å lage et felles grunnlag som alle kan bygge videre på og som bidrar til at vi
  - snakker samme språk
  - har noenlunde de samme komponentene i styringssystemet
  - gjør ting likt der vi samhandler, særlig i grensesnittene mellom styringsnivåer



I hvilken grad kan vi standardisere arbeidet med informasjonssikkerhet?

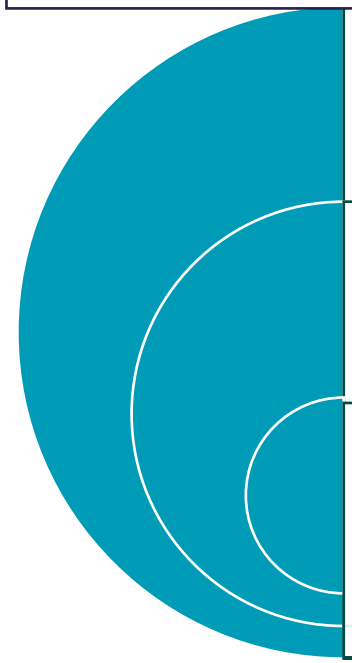
- Det kan se ut som at FIN bør utarbeide noe som
  - samler alle felles krav i ett kravsett
  - tydeliggjør definisjoner, ansvar, roller og oppgaver
  - Inneholder støttemateriale som underbygger kravene



Bruksområde og gevinster

Hjelpemiddel for

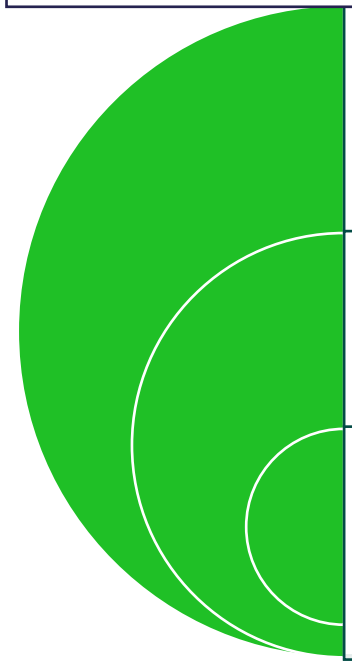
Økt samarbeid på informasjonssikkerhetsområdet



- **virksomhetene** til å videreutvikle sitt styringssystem
- **byrådsavdelingene** til å ivareta informasjonssikkerheten i egen sektor
- **kommunen** til å holde oversikt over risikobildet i stort

Gevinster

Redusert risiko for uønskede hendelser



- Forenkle arbeidet med informasjonssikkerhet i kommunen
- Spare ressurser ved at ikke alle må finne opp hjulet selv
- Enklere å sammenstille status på tvers av virksomheter og utøve helhetlig risikostyring

Mulig struktur

Krav

Kravdokumenter

01 Risikostyring og organisering

02 Forvaltning av informasjonsaktiva

Verktøykasse

Veiledninger

Dokumentmaler

Opplæring

Skjemaer

Verktøy

Nettverk

Vi startet med to viktige kravdokumenter

De to dokumentene var på høring i byrådsavdelingene før påske

Vi har fått mange innspill, summen av disse medfører at dokumentene må endre form

FIN vil fortsatt komme med et rammeverk, men vi må gå en runde til før publisering

Oslo

Oslo kommune CSIRT

Foto: Benjamin Pham

Sikkerhetstestingsteamet

Alaa Ghanim

Christian Hagby

Claudia Haubold

Randi Eskildsen

Oslo

Sikkerhetstest

- Tenke som en angriper for å finne svakheter i systemet
- Bryte informasjonssikkerhetsprinsippene konfidensialitet, integritet, tilgjengelighet
- Skaffe uautorisert tilgang til informasjon
- Vi finner sikkerhetshullene før angriperne

Oslo

Sikkerhetstesting som tjeneste

- Tilbud fra 1. Mars i år
- I førsteomgang kun til virksomheter på OsloFelles plattformen
- Tjenesten er foreløpig gratis. Markedspris varierer, men ligger på 50 – 500 000 NOK
- Vi tilbyr 3 typer test: **webapplikasjonstest**, **infrastrukturtest**, og **phishing-øvelser**
- Testens varighet varierer men gjennomsnittlig 2 uker. Rapport leveres siste dag

Oslo

Fra A til Å

- Forespørsel fra virksomhet
- Oppstartsmøte
- Start av test
- Varsling ved behov
- Rapportering
- Presentasjon hvis ønskelig

Oslo

Infrastruktur

- Evaluere sikkerheten til et nettverk, maskinvare, programvare, databaser, servere med mer.
- Utnytter feilkonfigureringer og sårbarheter som befinner seg i infrastrukturen.
- Avhengig av omfanget, vil en infrastruktur test vare i 2 uker eller mer.

Oslo

Webapplikasjon

- Webapplikasjoner er dynamiske nettsider
- Testes for de 10 mest kjente sårbarhetene (OWASP Top 10)
- Eksempler: Feilkonfigurasjoner, Tilgangsstyring
- Kan gjøres autentisert og/eller uautentisert

Oslo

Phishing

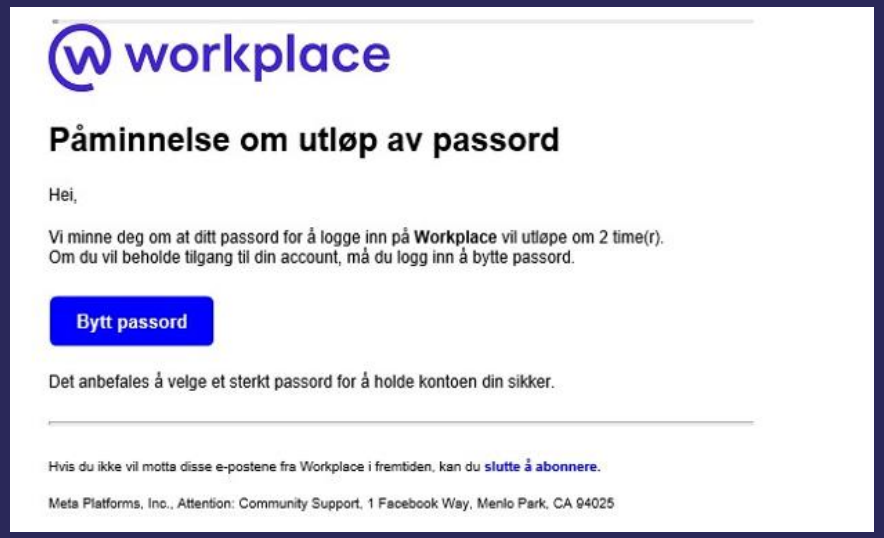
82% av alle dataangrep i fjor involverte en menneskelig faktor

Må ha fokus på opplæring og bevisstgjøring

Phishingøvelser er en effektiv opplæringsmetode

Oslo

Prosess - phishing



- Samarbeid med virksomheten om utforming av test (design, system, varighet, etc)
- Testperiode (ca 3 dager)
- Innsamling av statistikk, rapportskriving
- Presentasjon

Oslo

Kontakt oss

Ønsker du en uforpliktende samtale, eller å bestille en sikkerhetstest?

Forespørsler og spørsmål kan rettes til:

csirt@oslo.kommune.no

Avslutning

- Det er fortsatt ledige plasser på risikovurderingskurs 3.mai.
  - https://forms.office.com/pages/responsepage.aspx?id=gVB55pFjLkSatF6e908Y6lt8HePUeAZDgdbLk2KJMUhUNEQ1WVNLOFRXUjFWNUZVWUdVT1oxM0w3SS4u
- Flere kurs framover:
  - 15. mai: Risikovurdering av personvern
  - 24. mai: Behandlingsgrunnlag i praksis
- 15. juni - Nettverksdag for koordinatorer i bydelene
- Årets forum – du kan melde deg på!
  - Se her: https://felles.intranett.oslo.kommune.no/informasjonssikkerhet-og-personvern/kompetanse/forum-for-informasjonssikkerhet-og-personvern/

Forum 2023

~~01. mars~~
~~19. april~~
14. juni – OBS! Ny dato
6. september
29. november