



Digitalisering og innovasjon

Informasjonssikkerheit og personvern

Deres ref.

Vår ref.

Dato
17.01.2022

Invitasjon til møte om digital sikkerhet i kommunene

Justis- og beredskapsminister Emilie Mehl og kommunal- og ~~distriktsminister~~ Bjørn Arild Gram inviterer alle landets ordførere til et møte om digital sikkerhet i kommunene mandag 7. februar 12.00 - 14.00.

En stor del av truslene mot Norge skjer i dag i det digitale rom. Offentlige organer og private virksomheter taper stadig større verdier i digitale angrep. Antall alvorlige hendelser registrert hos Nasjonalt cybersikkerhetssenter i Nasjonal sikkerhetsmyndighet er tredoblet siste årene og risikoen er stor for at hendelser ikke blir oppdaget tidlig nok.

Møtet avholdes for å bidra til økt oppmerksomhet om digital sikkerhet, og med et mål om komme i dialog med kommunene om hva staten kan bidra med for å hjelpe kommunene med å forebygge og håndtere digitale hendelser.

På møtet vil statsrådene Mehl og Gram orientere om regjeringens politikk på området, trusler og utfordringer vi står overfor, og viktige nasjonale tiltak. Det blir også innlegg fra Nasjonal sikkerhetsmyndighet, Digitaliseringsdirektoratet og KS Kommunesektorens organisasjon. I tillegg vil ordfører i Østre Toten, Bror Helgestad, orientere om dataangrepet Østre Toten ble utsatt for i fjor.

Politisk ledelse i Justis- og beredskapsdepartementet (JD) og Kommunal- og ~~distriktsdepartementet~~ (KDD) vil i løpet av møtet gjerne ha innspill på hva som er kommunenes utfordringer når det gjelder digital sikkerhet, og hva myndighetene kan bidra med for at det blir enklere for kommunene å følge nasjonale råd og ~~veiledninger~~ om digital sikkerhet.

Antall alvorlige hendelser registrert hos Nasjonalt cybersikkerhetssenter i Nasjonal sikkerhetsmyndighet er tredoblet siste årene

NSM advarer mot cyberoperasjoner i julen



Nasjonalt sikkerhetsmyndighet (NSM) advarer mot alvorlige cyberoperasjoner i julen og ber norske virksomheter ha høy beredskap i fridagene.

Nordland Fylkeskommune utsatt for datainnbrudd. Etter fire dager er nettsidene ennå nede

– Treer ikke sensitive informasjonen er på plass, sier IT-sjefen.



Virksomhet i kommunen som har blitt utsatt for et datainnbrudd som har gjort at nettsidene er nede.

Nordic Choice-angrep: Hackere har lekket informasjon om ansatte

Utdelt i flere dokumenter prøver hackerne å få kontakt med de ansatte i de enkelte restauranter. – Først og fremst vurdert for å sikre at alle ansatte er sikkerhetsinformasjon.



Det er ikke klart om det er en sikkerhetsinformasjon som er lekket.

Politi i samarbeid med Nordtyskland i samarbeid med politiet i Norge.

Nortura utsatt for dataangrep

Nortura har stengt ned sine IT-systemer som følge av et dataangrep. Angrepet fører blant annet til redusert aktivitet ved fabrikkene.



Amedia utsatt for alvorlig dataangrep

Natt til tirsdag 28. desember ble flere av Amedias sentrale datasystemer satt ut av drift. Ingen pasienter ble påvirket av angrepet.



Utsatte pasienter i helsevesen.

Det er ikke klart om det er en sikkerhetsinformasjon som er lekket.

– Saksbehandler i politiet i samarbeid med politiet i Norge.



«Vi er satt tilbake til da jeg starta som sykepleier,
15–20 år tilbake i tid.»

Guri Bråthen, sykepleier



Kommunedirektør Ole Magnus Stensrud fortalte om utfordringene som Østre Toten kommune har hatt etter datainnbruddet tidligere i år.
Foto: Jon Olav Andersen, Totens Blad

Sensitiv pasientinformasjon kan være på avveie etter dataangrep

Datasystemet til Østre Toten kommune er angrepet og gjort utilgjengelig for alle ansatte. – Personnummer og helsedata kan være på avveie, sier ordføreren.



ANGREPET: Ordfører i Østre Toten, Bror Helgestad, forteller at de som har satt kommunens system ut av spill har hatt tilgang på alle data i deres systemer.
FOTO: HANS SOLBAKKEN / NRK

Østre Toten kommune: – Dataangrepet har kostet oss mer enn 32 millioner

– Heldigvis finnes det ordninger med krisehjelp fra staten. Jeg har vært i møte med kommunalministeren, og vi håper også å få litt hjelp derfra. Det sa kommunedirektør Ole Magnus Stensrud i Østre Toten kommune under Sikkerhetskonferansen i formiddag.

Komm. Østre



Hans Solbakken
@hanssolbakken
Journalist
Publisert 10. jan. 2021 kl. 20:45
Oppdatert 8. feb. 2021 kl. 12:51



Oslo 2017/11/14. Datatilsynet logo. Foto: Marlam Butt / NTB Marlam Butt

Østre Toten kommune ilagt overtredelsesgebyr på fire millioner etter dataangrep

Datatilsynet legger Østre Toten kommune et overtredelsesgebyr på 4 millioner kroner etter dataangrepet.



Departementene

Strategi

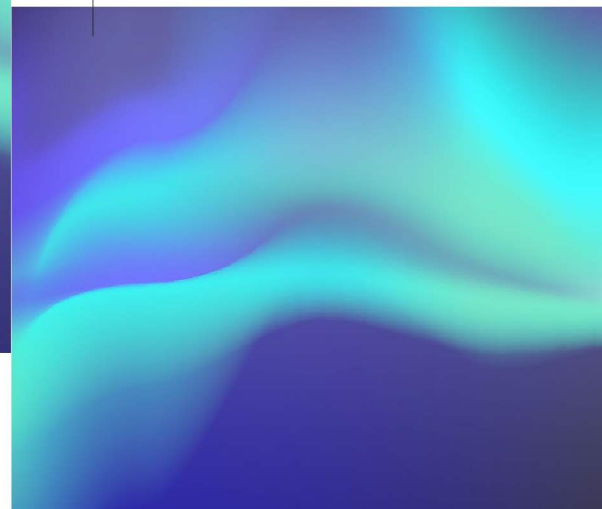
Nasjonal strategi for digital sikkerhet



Departementene

Tiltaksoversikt

Tiltaksoversikt til nasjonal strategi for digital sikkerhet



1



LEDELSE

2



RISIKOSTYRING

3



KARTLEGGE VERDIKJEDER,
INFORMASJONSVERDIER,
UTSTYR OG
BRUKERTILGANGER

4



INKLUDER DIGITAL
SIKKERHET I
VIRKSOMHETSKULTUREN

5



LEVERANDØRKONTROLL

6



SIKKER
KONFIGURASJON

7



KONTROLL PÅ NETTVERK
OG SYSTEMKOMPONENTER

8



EPOST OG
WEBSIKKERHET

9



TILGANGSKONTROLL

10



HENDELSESBEREDSKAP



Prosjekt Informasjonssikkerheit og personvern

Hoved- og delleveranser

Skildring av internkontroll:

Dokument som skildrar policy og prinsipp for korleis kommunane og IKTNH skal ivareta sine lovpålagte krav innan informasjonssikkerheit og personvern.

Synleggjere hovudkrav, organisering, roller og ansvar, ambisjonsnivå og hovudprinsipp og hovudprosessar for sikkerheitsløysinga.

Organisering og bestemmelsar som har innverknad på fellesskapet bør vere like for alle og bli vedtekne hjå den einskilde kommune.

Kommunane kan tilpasse delar som utelukkande er relevant for eigen kommune, typisk intern organisering.

Sikkerheitsløysing organisert og dimensjonert:

Kommunen har avklart eiga rolle og kva IKTNH (og eventuelt andre leverandørar direkte handtert av kommunen) har som ansvar i høve informasjonssikkerheit og personvern

Integrerte prosessar:

Integrerte prosessar er produktet der utføringa av prosessar og aktivitetar i sikkerheitsløysa vert integrert inn i eksisterande prosessar i kommunane og IKTNH.

I prosjektimplementeringa identifisere gap mellom eksisterende prosessar og behovet/krava som er skildra innanfor området internkontroll

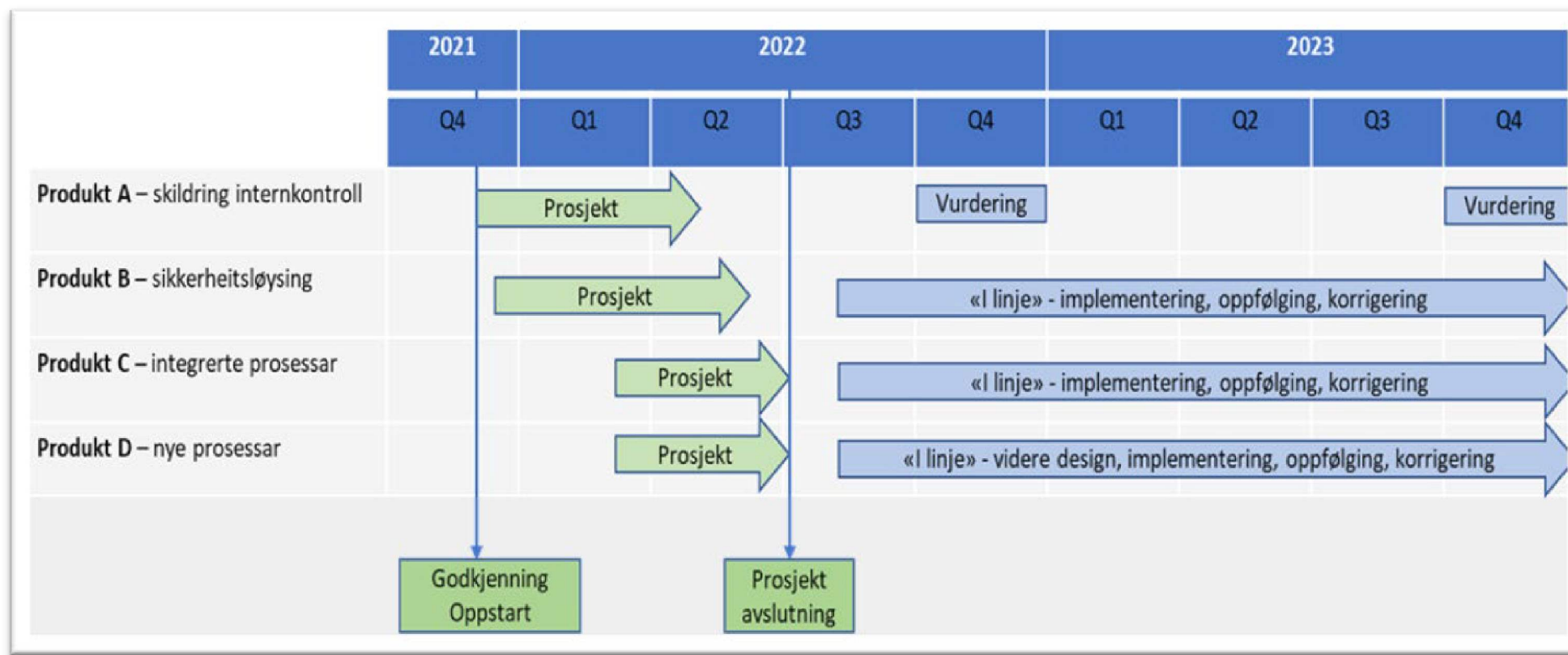
Nye prosessar etablert:

Nye prosessar etablert er produktet der ein i prosjektet har designa og implementert prosessar som det er identifisert behov for, men som ikkje har vore på plass til nå.

Behovet for nye prosessar vert styrt av krav til kommunane, samt behov og krav som skildra innanfor området internkontroll

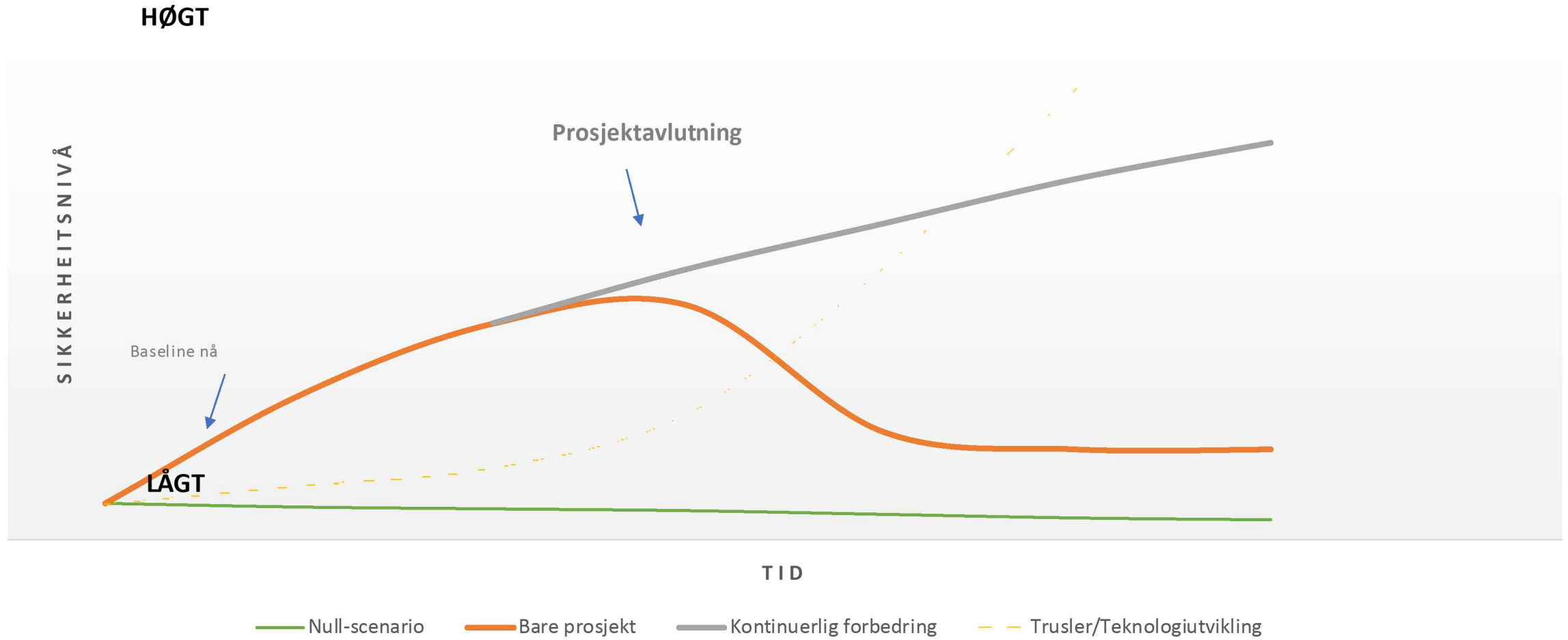
Tentativ tidsplan

Sikkerhetsløsning har ikkje sluttdato. Er satt ein tentativ sluttdato for prosjektorganiseringa



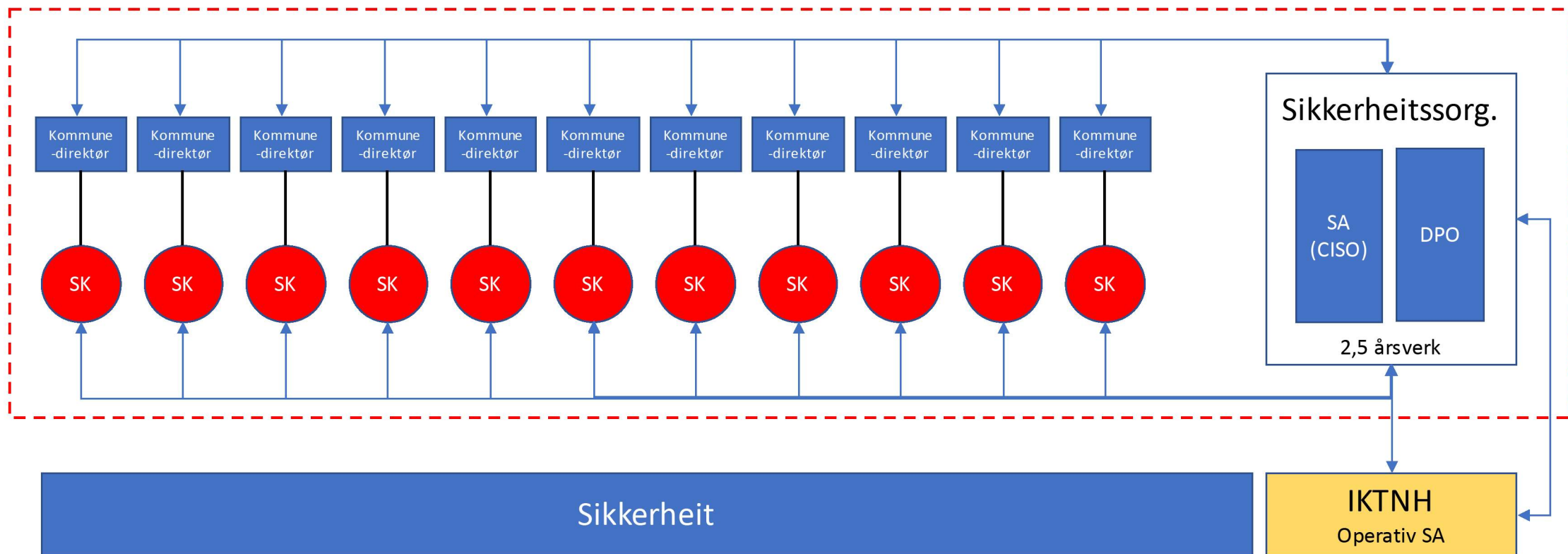
Sikkerhedsorganisering

Sikkerhetsnivå over tid



Kommunane må:

- Sikre god implementering av internkontroll informasjonssikkerheit
- Sørge for
 - Å få innsikt i risikosituasjonen mhp cyber/informasjonssikkerheit
 - Å sikre at bestemmelsar og rutinar er etablert i kommunen og vert fulgt
 - Gjennomføring av risikovurderingar
 - Interne sikkerhetsrevisjonar og ledergjennomgangar
 - Oppbygging og vedlikehald av sikkerheitskultur i kommunen
 - Planlegging, gjennomføring og evaluering av sikkerhetsøvingar / beredskapsøvingar (cybersikkerheit)
 - Prioritering av prosjekt innan informasjonssikkerheit
 - Krav til og oppfølging av leverandørar (herunder IKTNH)



Tiltak:

- Etablere ny rolle
 - Sikkerhetsansvarleg (SA)
 - Sikkerheitskoordinator (SK)
- Etablere ny eining, Sikkerheitsorganisasjon (SO)

SA

Sikkerheitsansvarleg - ivareta kommunedirektørane sitt ansvar

- Utøve ansvaret for internkontroll informasjonssikkerhet på rådmannens vegne
- Bistå kommunen(e) med
 - Å få innsikt i risikosituasjonen mhp cyber/informasjonssikkerhet
 - Å sikre at bestemmelser og rutiner er etablert i kommunen og blir fulgt
 - Gjennomføring av risikovurderinger
 - Interne sikkerhetsrevisjoner og ledergjennomganger
 - Oppbygging og vedlikehold av sikkerhetskultur i kommunen
 - Planlegging, gjennomføring og evaluering av sikkerhetsøvelser / beredskapsøvelser (cybersikkerhet)
 - Prioritering av prosjekter innen informasjonssikkerhet
 - Krav til og oppfølging av leverandører (herunder IKTNH)

SK

Oppgaver for sikkerheitskoordinator - med støtte frå SA

- Tilrettelegging og sikre at bestemmelsar og rutinar er etablert i kommunen og vert fulgt
- Støtte i gjennomføring av risikovurderingar
- Tilrettelegging og sikre at sikkerheitsrevisjonar og leiar gjennomgang vert gjennomført
- Tilrettelegging, sikre og kontrollere oppbygging og vedlikehald av sikkerheitskultur i kommunen
- Tilrettelegging og sikre planlegging, gjennomføring og evaluering av sikkerheitsøvingar / beredskapsøvingar (cybersikkerheit)

OSA (IKTNH)

Typiske funksjonsområder for operativ sikkerhetsansvarlig

- Skal utøve den prosessuelle og teknologiske sikkerhetsfunksjonen
- Ansvarsområder og oppgaver
 - Planlegging, utvikling/etablering og oppfølging av tekniske og organisatoriske sikkerhetstiltak, herunder hendelseshåndtering og endringshåndtering
 - Etablere grunnlag for å kommunisere trussel- og sårbarhetsbildet til sikkerhetsansvarlig
 - Beslutte sikkerhetsrammeverk IKTNH, implementere og følge opp (eks ISO27000)
 - Bistå i anskaffelsesprosesser med tekniske sikkerhetskrav
 - Bistå i risikovurderinger og sårbarhetsavdekking
 - Håndtering av sikkerhetsavvik

DPO - Personvernombud

- Personvernombud skal **bidra** til at kommunen behandler personopplysninger i tråd med gjeldende personvernregler og at de som er registrert får nødvendig hjelp til å ivareta sine rettigheter
- Personvernombudet har en rådgivende og kontrollerende funksjon og **skal normalt ikke ha ansvar** for informasjonssikkerhet



Takk for oppmerksomheten