Oslo

Styring av informasjonssikkerhet i Oslo kommune

Lars Martin Undhjem
Spesialrådgiver informasjonssikkerhet

Susanne Ekeberg Bjørtomt
Fagsjef Informasjonssikkerhet

Foto: Benjamin Pham

Hvordan skal vi møte de utfordringene vi vet kommer?

Endringer og utvikling må til for å redusere gapet

Endringer og utvikling må til for å redusere gapet


Foto: Mark McGregor / Unsplash

- Vi må forstå hvordan risikobildet endrer seg og utvikle oss deretter

1. Standardisering bidrar til at vi jobber mer effektivt og kan måle om vi er på rett vei

2. Helhetlig risikostyring bidrar til at vi iverksetter riktige tiltak

Endring krever ledelse

- Mange ansatte inkluderer **sikkerhet** som en del av sine **daglige oppgaver**
- Men **sikkerhetsstyring** er en lederoppgave
- Verktøyet ledelsen benytter i sikkerhetsstyringen er **styringssystemet**

Foto: TK / Unsplash

Oslo

Styringssystemet er verktøyet for sikkerhetsstyringen

- Vi setter oppgavene i system slik at vi vet at vi
  - Beskytter de riktige tingene
  - Beskytter dem fra de riktige truslene
  - Beskytter dem tilstrekkelig, - ikke for mye og ikke for lite
- Vi styrer/leder for å unngå/motstå uønskede hendelser og håndtere dem når det skjer
- Vi iverksetter systematiske sikkerhetstiltak for å
  - Forebygge
  - Oppdage
  - Håndtere
  - Gjenopprette
- Vi setter opp aktivitetene i et årshjul for å sikre kontinuerlig forbedring

Det handler om å gjøre de riktige tingene, ikke bare om å ha de riktige dokumentene

Styringssystem i Oslo kommune

«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

Krevende krav

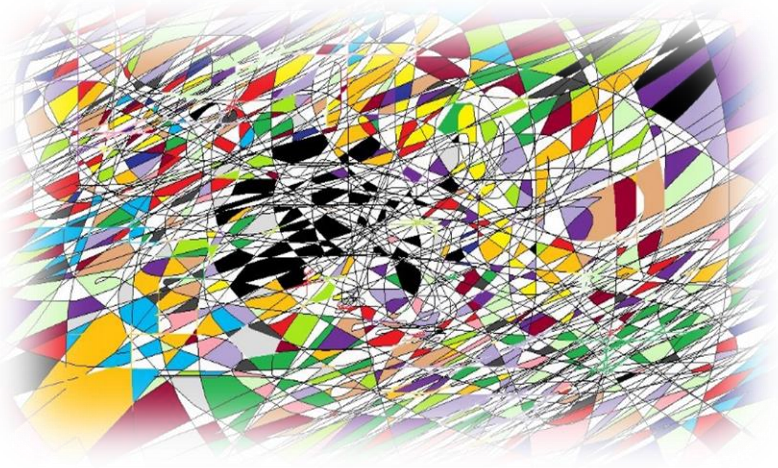
- Virksomheten treffes av en mengde krav innen informasjonssikkerhet
- Det finnes ingen standardisering, så virksomheten står alene i å kartlegge og etterleve kravene
- Det finnes lite støttemateriale fra sentralt hold

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?

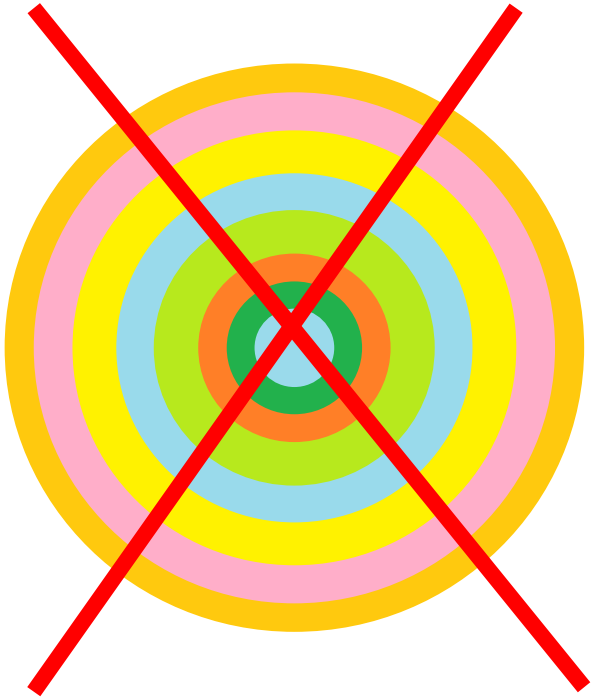
- I dag er styringen for det meste fragmentert



I hvilken grad kan vi standardisere arbeidet med informasjonssikkerhet?

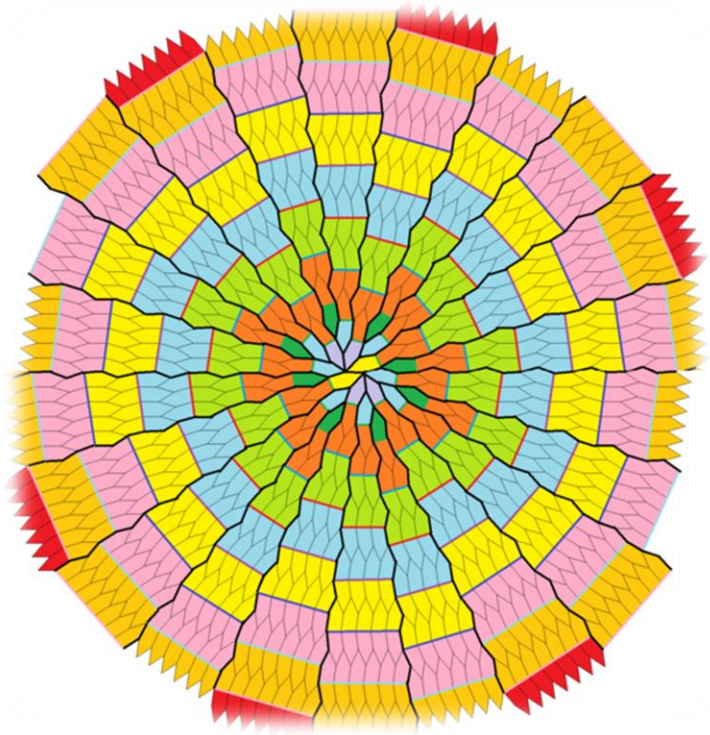
- I dag er styringen for det meste fragmentert

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



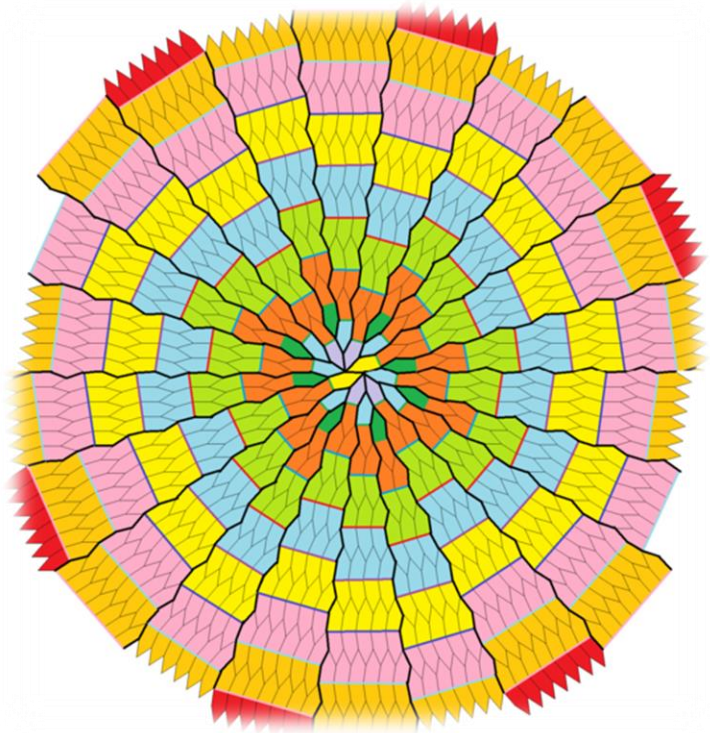
I hvilken grad kan vi standardisere arbeidet med informasjonssikkerhet?

- I dag er styringen for det meste fragmentert
- Vi har sett at vi kan ikke lage et felles, ensartet styringssystem
- Men, det er 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



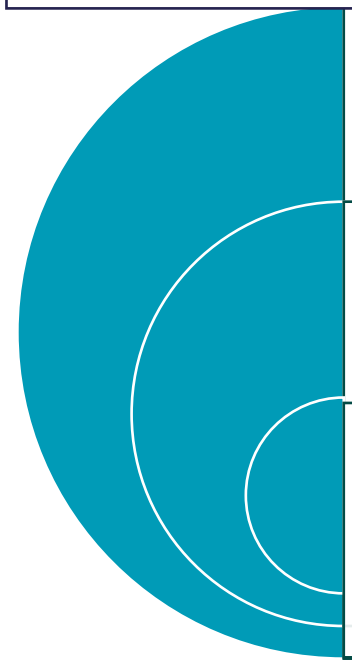
Dette «noe» har arbeidsnavnet **«Overordnet styringssystem for informasjonssikkerhet» (OSIS)**

OSIS beskriver et målbilde, og implementeringen vil ta tid

Bruksområde og gevinster

Hjelpemiddel for

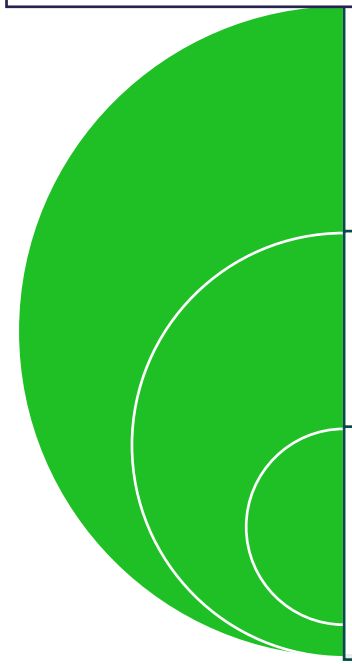
Økt samarbeid på informasjonssikkerhetsområdet



- **virksomhetene** til å videreutvikle deres 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

Hva inneholder OSIS?

Krav

Kravdokumenter

Verktøykasse

Veiledninger

Dokumentmaler

Opplæring

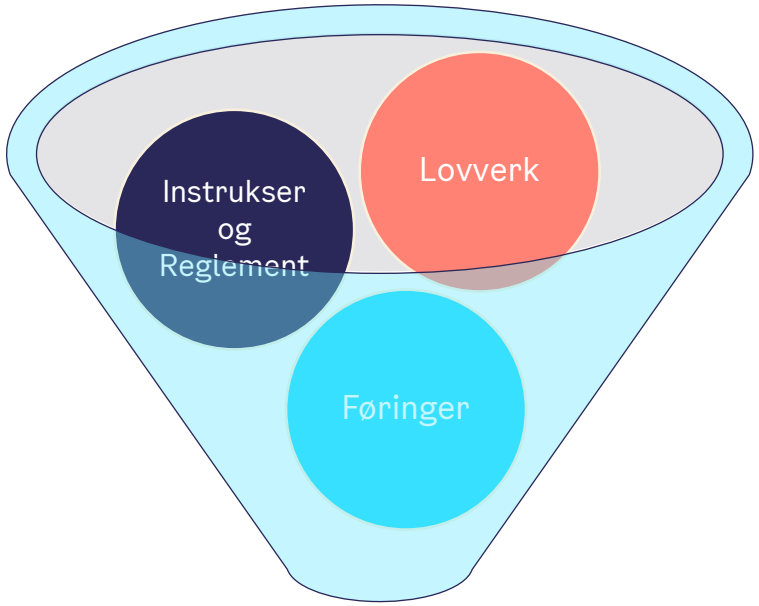
Skjemaer

Verktøy

Nettverk

Hvor kommer kravene fra?

- 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
- Fellesføringer på informasjonssikkerhets-området

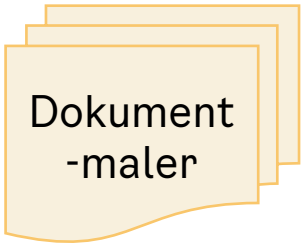


Alle felles krav, tolket og tydeliggjort

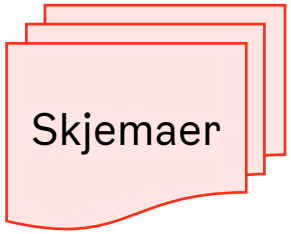
Verktøykasse er under utvikling

- Verktøykassa skal hjelpe til med å oppfylle kravene
  - For eksempel: Der det for stilles krav til at man skal ha et dokument bør det finnes en mal for dette dokumentet i verktøykassa.
- Alle kan bidra med verktøy
- Eksisterende (og eventuelt nye) nettverk for informasjons-sikkerhet benyttes til å dele og videreutvikle verktøy

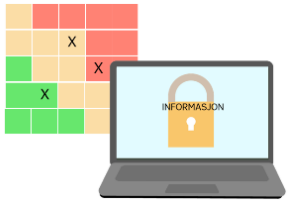
Eksempler på innhold i verktøykassa



Mal for informasjonssikkerhetspolicy



Skjema for kravoversikt

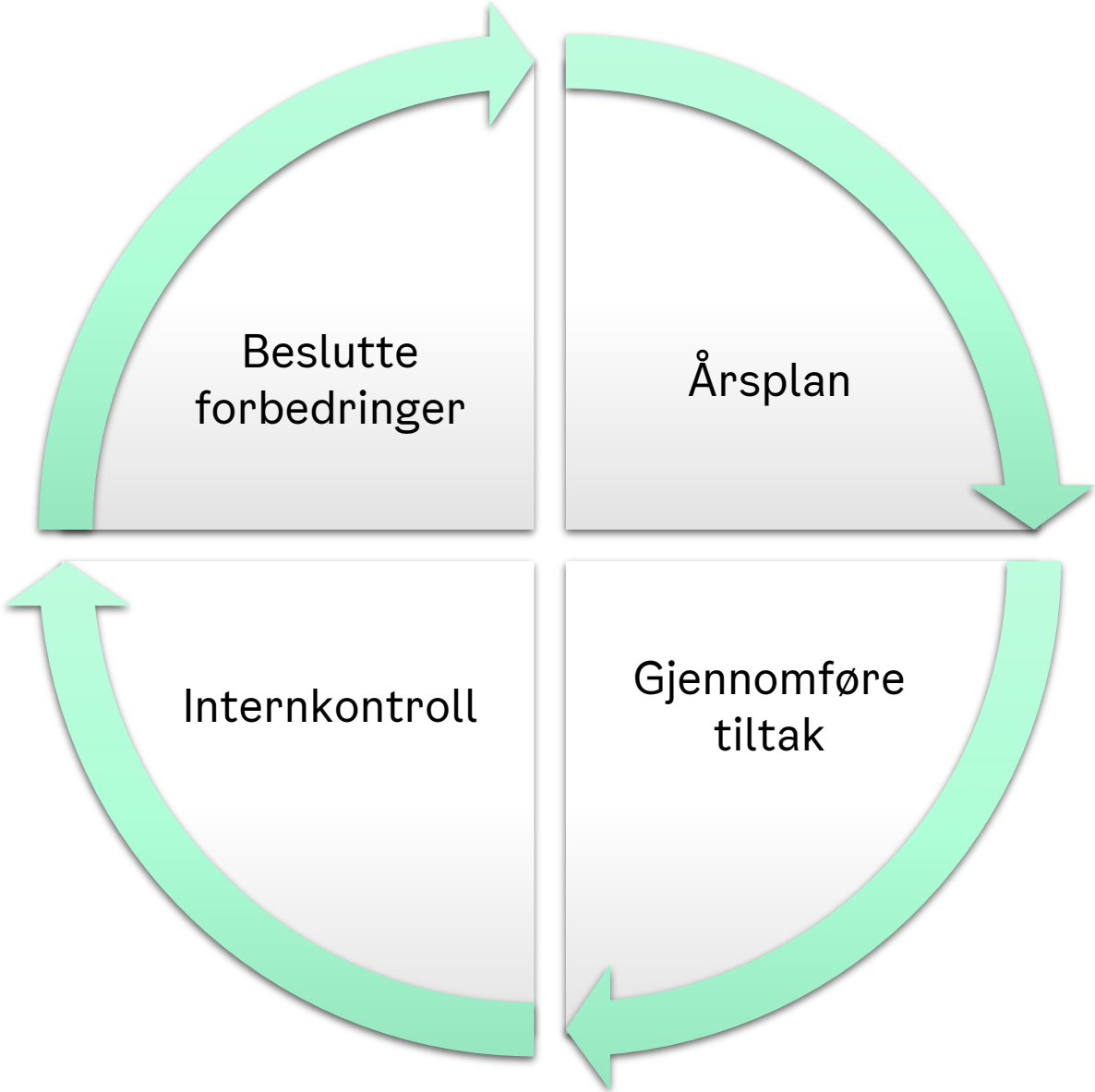


Oppdatert risikovurderingsverktøy

Modernisert verktøy for VE-rapportering

Anbefalte prosesser, for eksempel årshjul i virksomhet

Ledelsens gjennomgang
Hva er risikoen nå?
Hvilke forbedringer bør vi gjennomføre?



Prioritering, planlegging og ressurstildeling

Status
Etterlevelse
Læring av hendelser

Risikovurderinger, risikostyring, implementering av tiltak

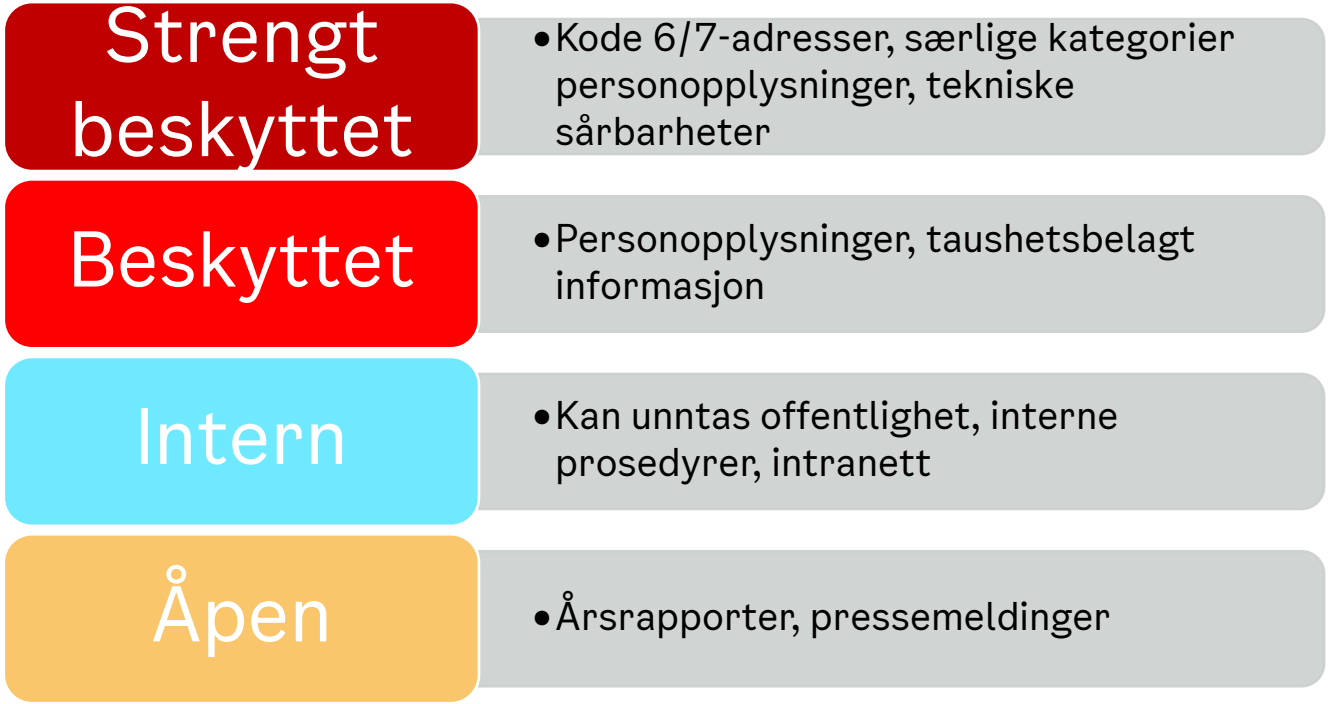
Konkret eksempel på standardiseringsbehov: Klassifisering av informasjon

Klassifisering av informasjon

For å kommunisere hvordan vi skal beskytte ulike typer av informasjon benyttes **konfidensialitetsklasser**

Eksempel på konfidensialitetsklasser:

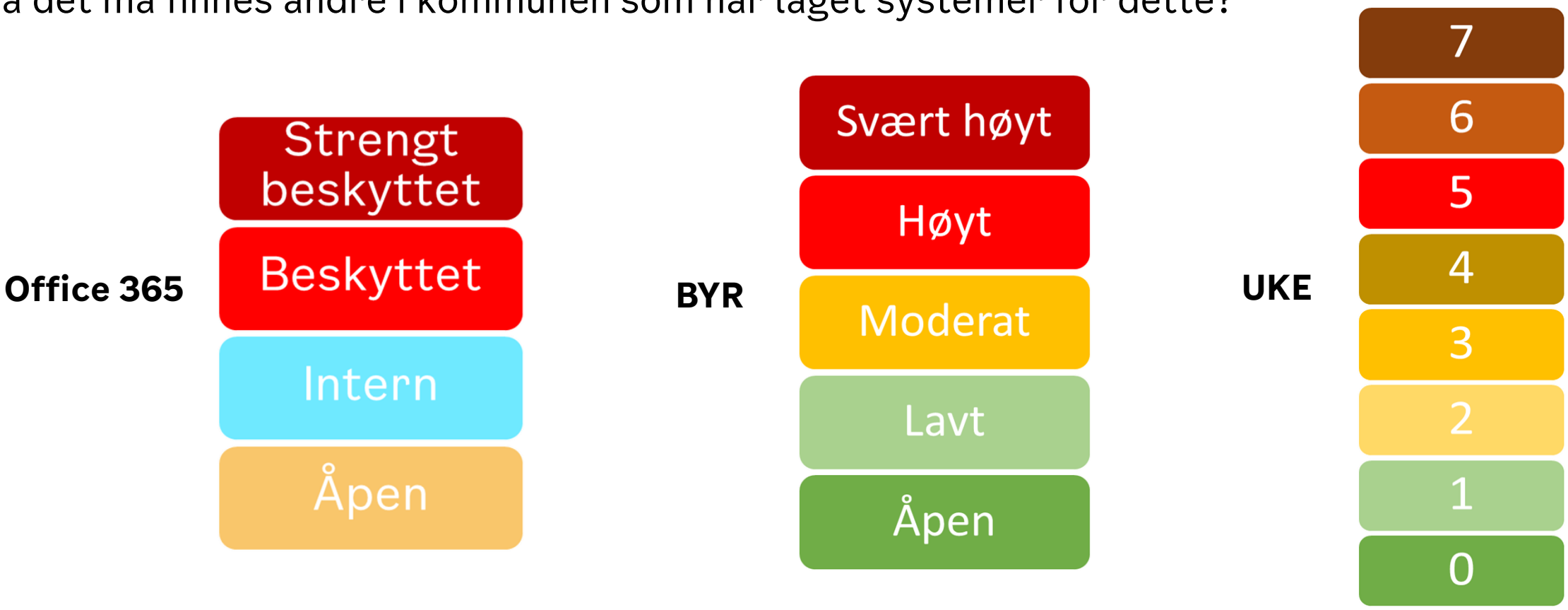
(fra Office 365)



Klassifisering av informasjon

Hvorfor måtte innføringsprosjektet for Office365 lage sine egne konfidensialitetsklasser?

Alle virksomheter er lovpålagt å skille på ulike typer informasjon,
så det må finnes andre i kommunen som har laget systemer for dette?



Dette er bare de første vi fant. Det finnes også en rekke slike skalaer i lovverket, blant annet sikkerhetsloven

Behandlingsregler

- Basert på informasjonens beskyttelsesbehov stilles ulike krav til hvordan den skal
  - Merkes
  - Lagres
  - Sendes
  - Behandles
  - Slettes

Strengt beskyttet	Ikke tillatt i Office 365
Beskyttet	• Personopplysninger, taushetsbelagt informasjon
Intern	• Kan unntas offentlighet, interne prosedyrer, intranett
Åpen	• Årsrapporter, pressemeldinger

Eksempel på behandlingsregel

Uten felles konfidensialitetsklasser og behandlingsregler er det vanskelig å samhandle mellom virksomheter

Felles forvaltning av informasjonsaktiva

- Inneholder felles konfidensialitetsklasser og behandlingsregler
- Minste felles multiplum basert på lovverk som gjelder for alle virksomheter
- Veiledningsmateriale følger med
  - Eksempler på informasjon i de ulike klassene
  - Flytskjema for klassifisering
  - Juridisk bakgrunn

Utkast til felles konfidensialitetsklassifisering

	Konsekvenser ved konfidensialitetsbrudd	Beskrivelse
Sikkerhets-gradert	***Varierer etter gradering***	Informasjon gradert etter sikkerhetsloven
Strengt beskyttet	**Meget høy**	Informasjon som kan gi **svært alvorlige konsekvenser*** om den havner hos uvedkommende
Beskyttet	**Høy**	Informasjon som kan gi **alvorlige konsekvenser*** om den havner hos uvedkommende
Avgrenset intern	**Middels**	Informasjon som kan gi **moderate konsekvenser*** om den havner hos uvedkommende
Intern	**Lav**	Informasjon med lavt beskyttelsesbehov, ofte knyttet til kommunens interne drift
Åpen	**Ubetydelig**	Informasjon som kan offentliggjøres

Helhetlig risikostyring for å iverksette riktige tiltak

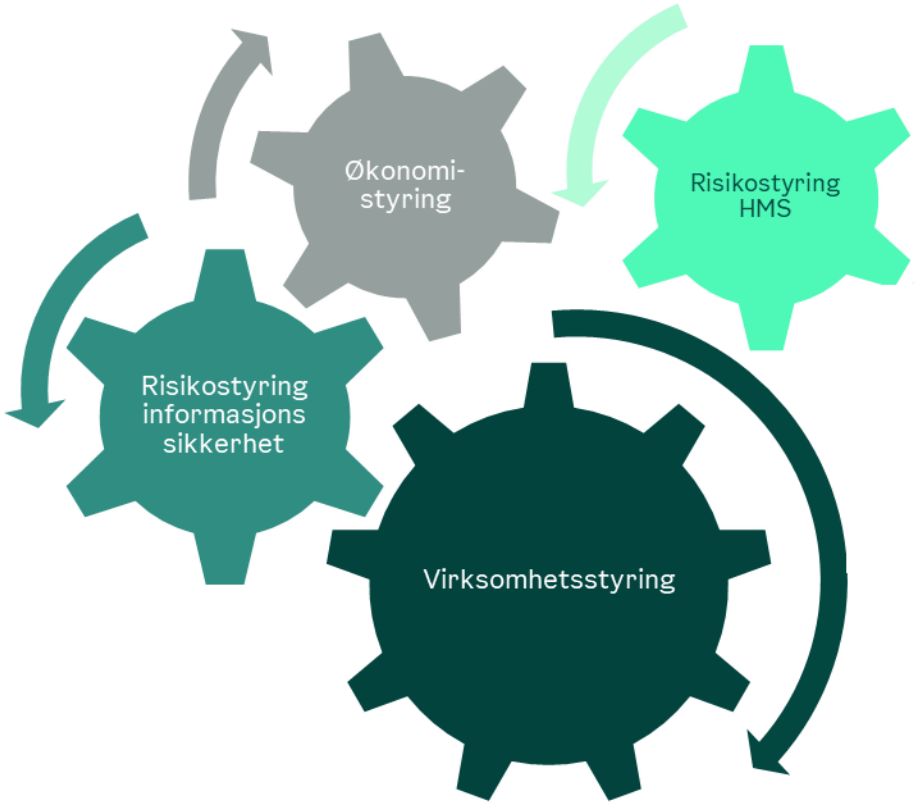
Helhetlig risikostyring og organisering av arbeidet

- Hvem har ansvaret for å beskytte informasjonsverdiene?
- Hvordan fordeler ansvaret seg i kommunens interne verdikjede?
- Hvilke roller har vi og hvilke roller trenger vi?
- Hvordan bruker vi risikovurderinger i beskyttelsen?
- Hvordan får vi til risikostyring på tvers i Oslo kommune?

Styring av informasjonssikkerhet er integrert i virksomhetsstyringen

- Følger etablert måte å styre på i kommunen
- Informasjonssikkerhet er et annet fag, men også dette handler om risikostyring for at virksomheten skal nå sine mål

Det er viktig at det ikke er en sideaktivitet, men en iboende del av eksisterende styringssystem

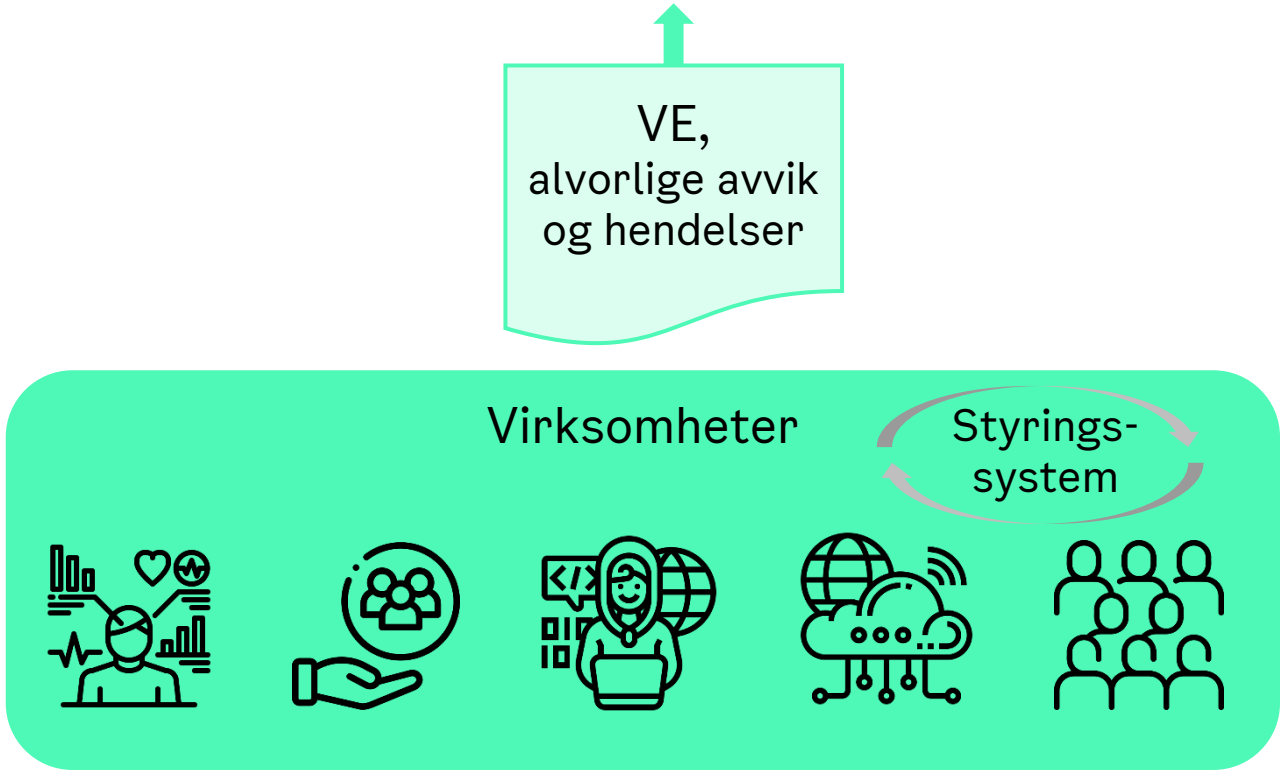


Det er i virksomhetene mesteparten skjer

Virksomhetene har ansvaret for å legge til rette for, og produsere tjenester kommunen har ansvar for

Samtidig som informasjonssikkerhet blir ivaretatt

- Bruker styringssystem som et verktøy for risikostyring og internkontroll
- Gjennomfører ledelsens gjennomgang for å få status og beslutte forbedringer
- Gjennomfører øvelser og lærer av dem
- Rapporterer tilstand, informerer om alvorlige avvik og hendelser



Virksomhetsleder har ansvar for å ivareta informasjonssikkerheten i sin virksomhet

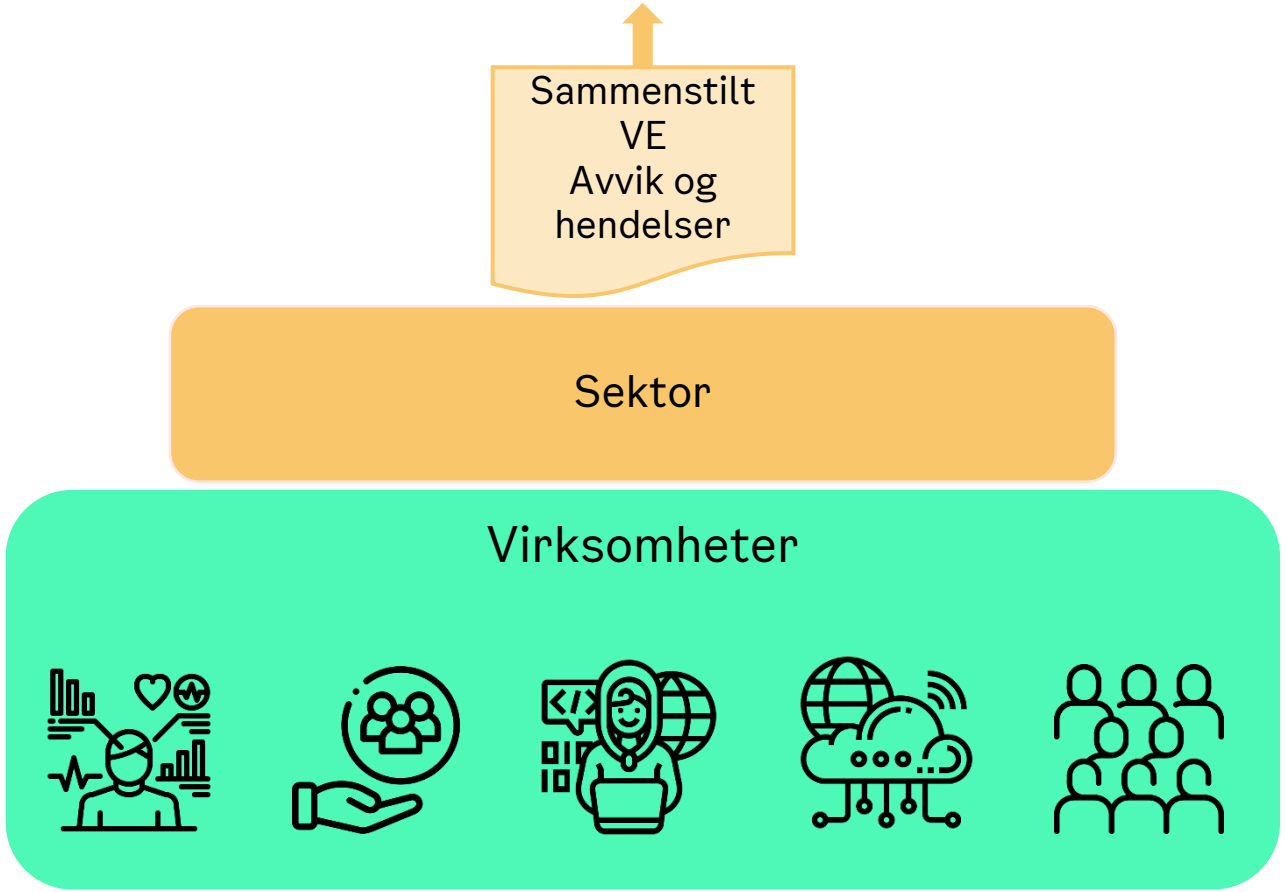
Hvem hjelper virksomhetsleder med å ivareta sitt ansvar?

- Informasjonssikkerhetskoordinator
- Beredskapskoordinator
- Systemeiere/Systemforvaltere
- Vi anbefaler å vurdere behovet for Informasjonssikkerhetsleder
- Vi anbefaler også å vurdere behovet for roller for å ivareta digital sikkerhet

Virksomheter

Men byrådsavdelingene har også et ansvar i sin styring

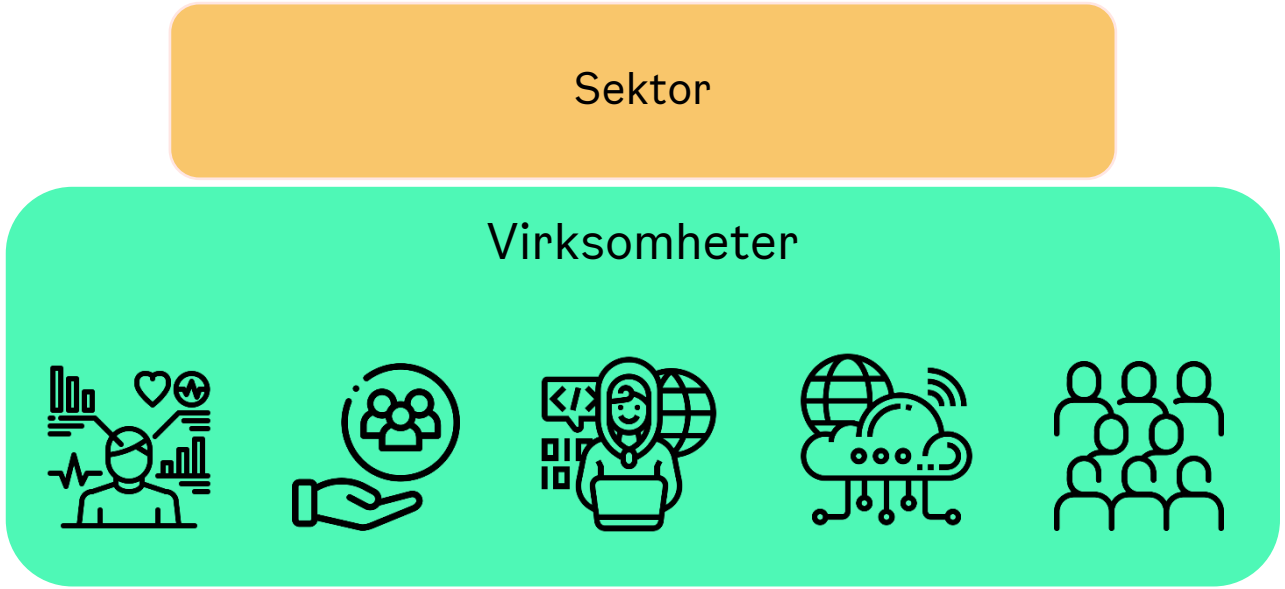
- Dette ivaretas på forskjellige måter:
  - Systemeierskap for felles- eller sektorsystemer
  - Etatsstyring av sine virksomheter
- Holde oversikt over sektorspesifikke krav og formidle disse til virksomhetene
- Støtte håndtering av rapporterte avvik og hendelser i virksomhetene ved behov
- Sammenstille og oppsummere status i sin sektor, og rapportere dette til FIN



Kommunaldirektøren har ansvar for å ivareta informasjonssikkerhet i sin sektor

Hvem hjelper kommunaldirektøren med å ivareta sitt ansvar?

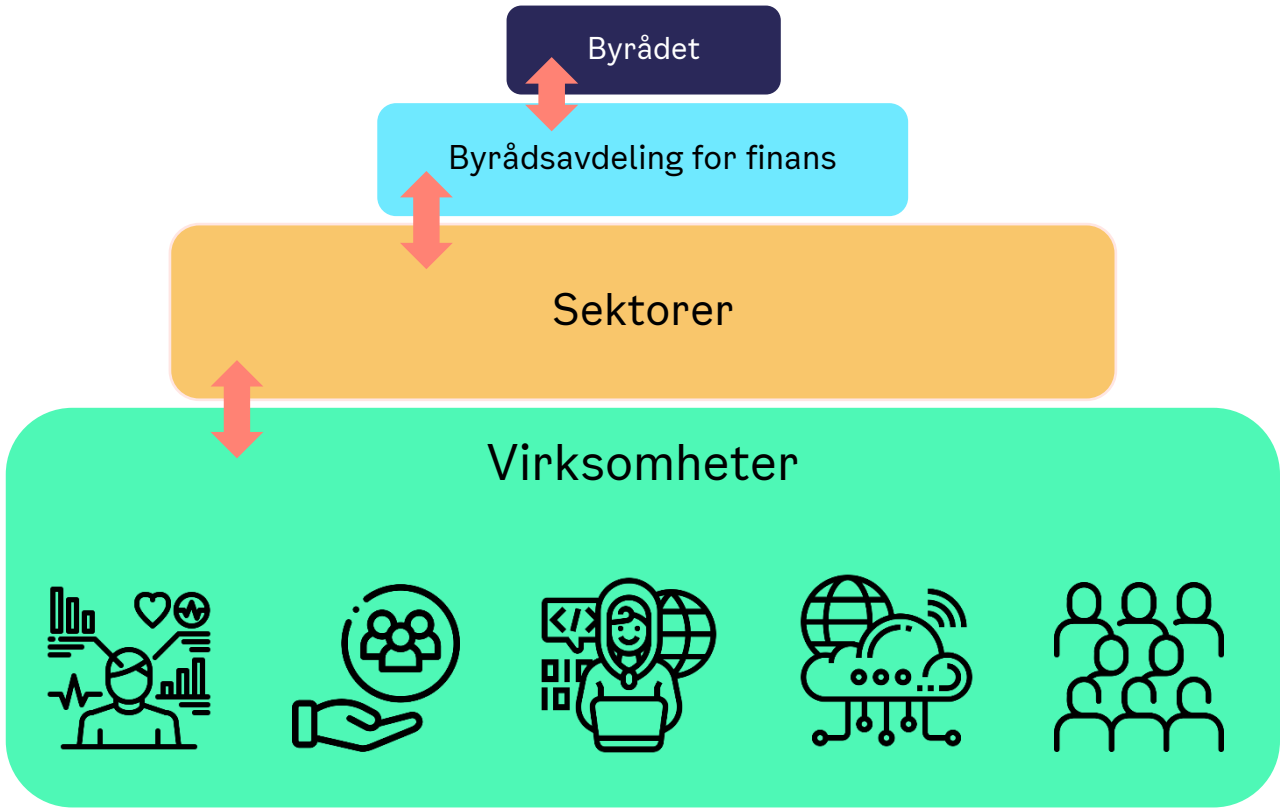
- Systemeiere
- Etatsstyrere
- Vi anbefaler å vurdere behovet for en koordinerende rolle for å sammenstille status på tvers av etatsstyringen og IKT-styringen i sektoren



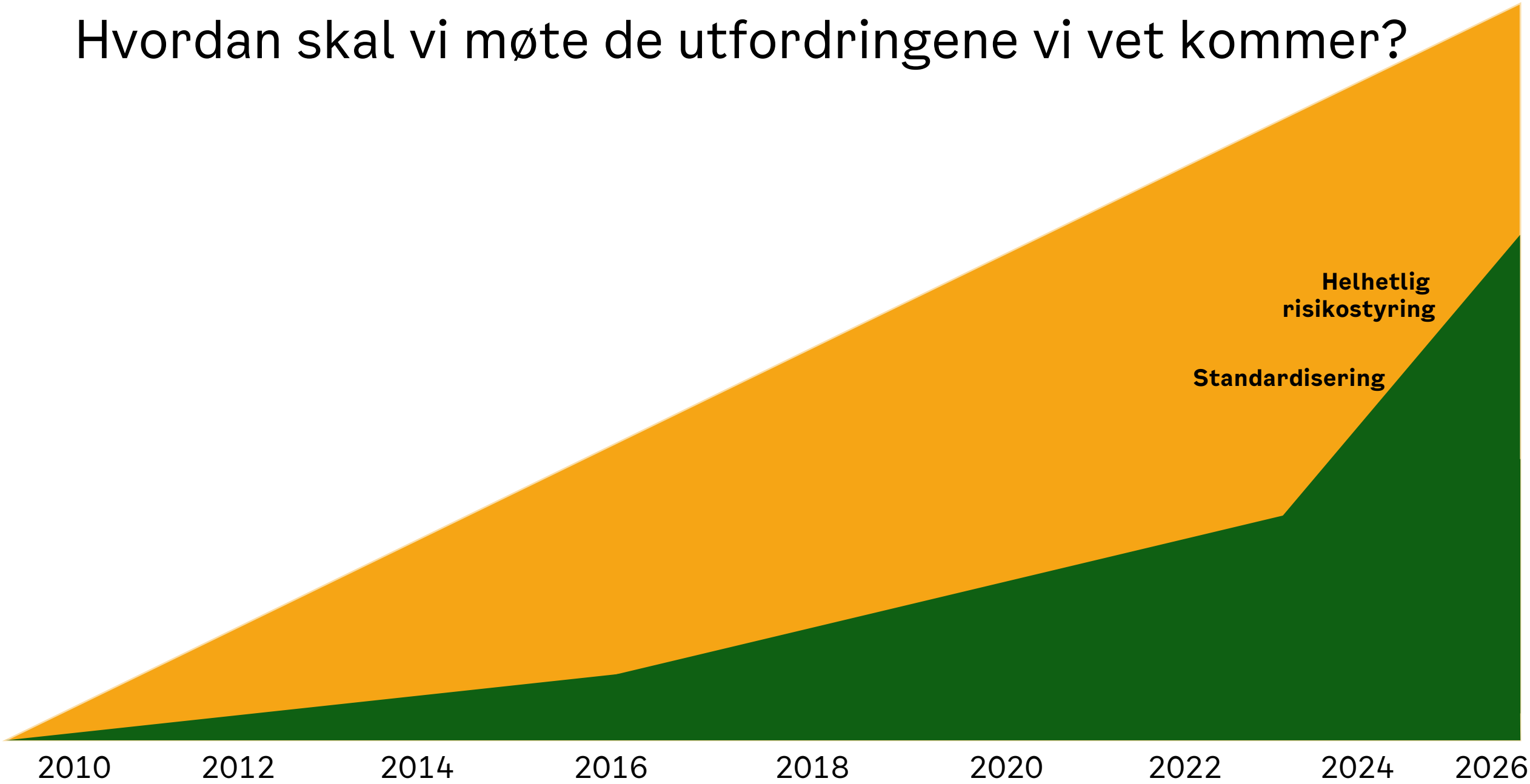
FIN har et overordnet ansvar

Risikostyring på tvers er avhengig av samarbeid, informasjonsutveksling og dialog – integrert i eksisterende styringsmodell

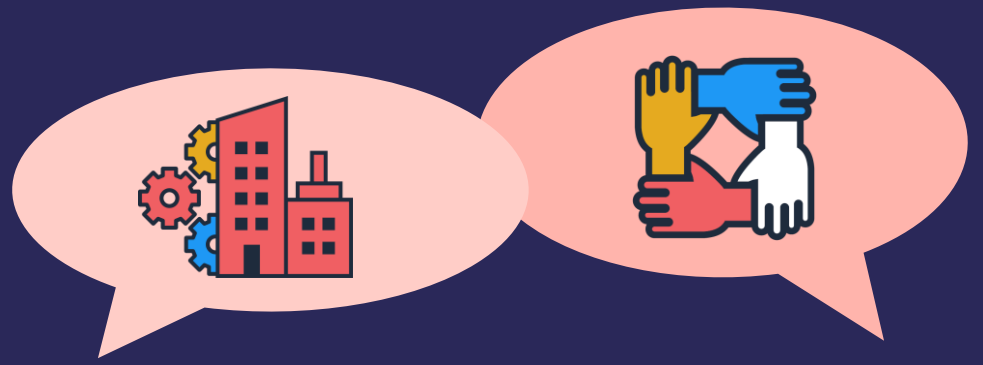
- Tydeliggjør informasjonssikkerhetsoppgaver
  - Utvikler hjelpemidler for virksomhetene og byrådsavdelingene
- Får informasjon om risiko fra byrådsavdelingene
- Oppsummerer og informerer om risiko til byrådet



Hvordan skal vi møte de utfordringene vi vet kommer?



Styringssystem



- Hvordan er informasjonssikkerhet et tema i ledergruppa og i etatsstyringen?
- Hvordan kan min virksomhet ha nytte av standardisering i styringen av informasjonssikkerhet?
- Har dere noen refleksjoner etter i dag på om hvordan vi kan jobbe annerledes i Oslo kommune med sikkerhet?

Take aways – hva nå?

- Har dere kontinuitetsplaner?
- Slå av en prat
  med koordinator(ene) hos deg
- Hvor ofte har du sikkerhet på agendaen og i hvilke anledninger er temaet oppe i ledergruppa?