INFORMASJONSSIKKERHET I STYRINGSDIALOGEN

Innlegg på NIFS-møte 18.11.2020

Direktoratet for forvaltning og økonomistyring

Fire spørsmål

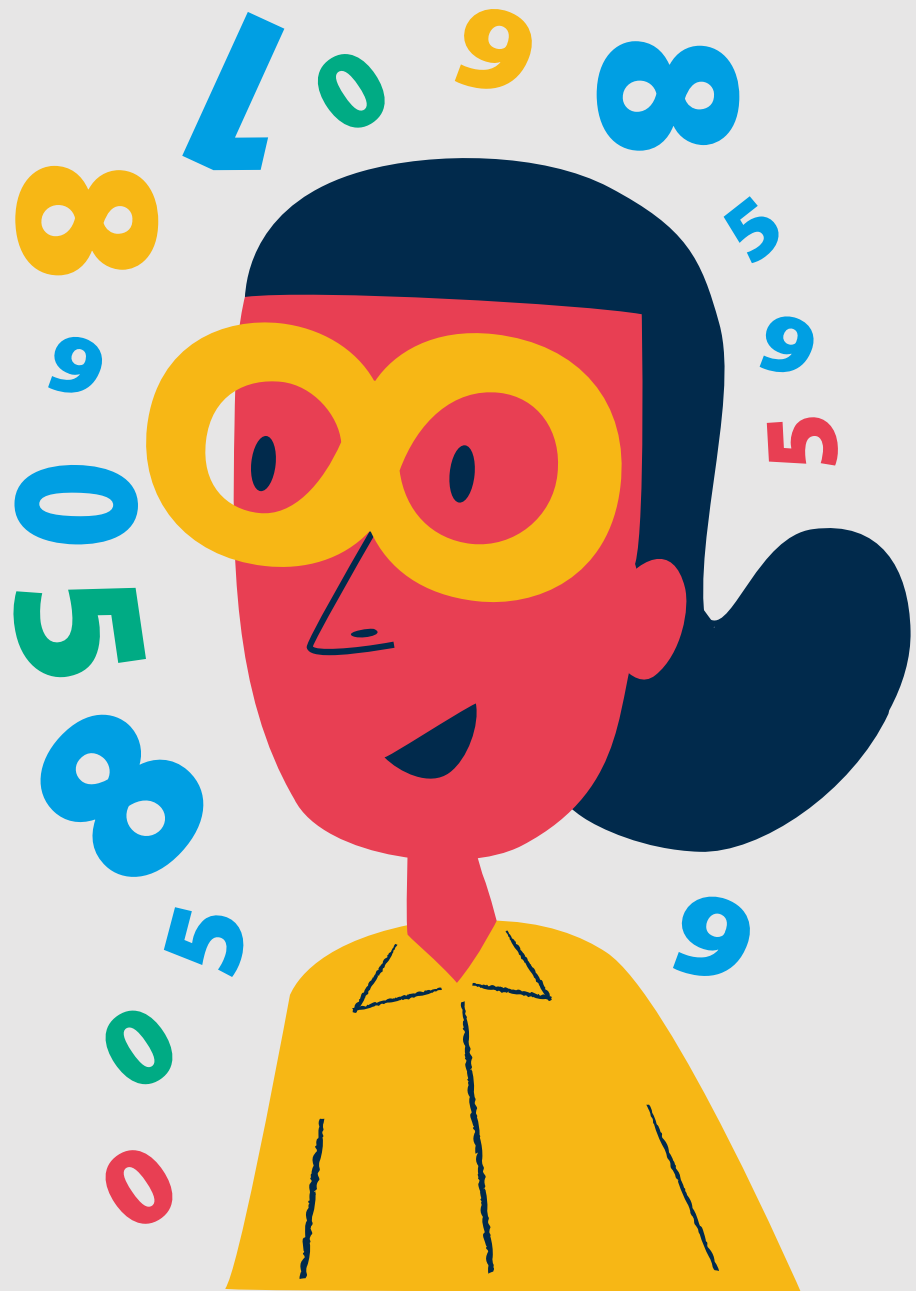
1. ***Hvordan kan departementene følge opp arbeidet med informasjonssikkerhet i virksomhetene de styrer?***

2. ***Hvordan kan virksomhetene vite at de har kontroll på arbeidet med informasjonssikkerhet?***

3. ***Hvordan sikre en hensiktsmessig styringsdialog om informasjonssikkerhet?***

4. ***Har styringsrelasjonen mellom departement og virksomhet noen overføringsverdi til kommunene?***

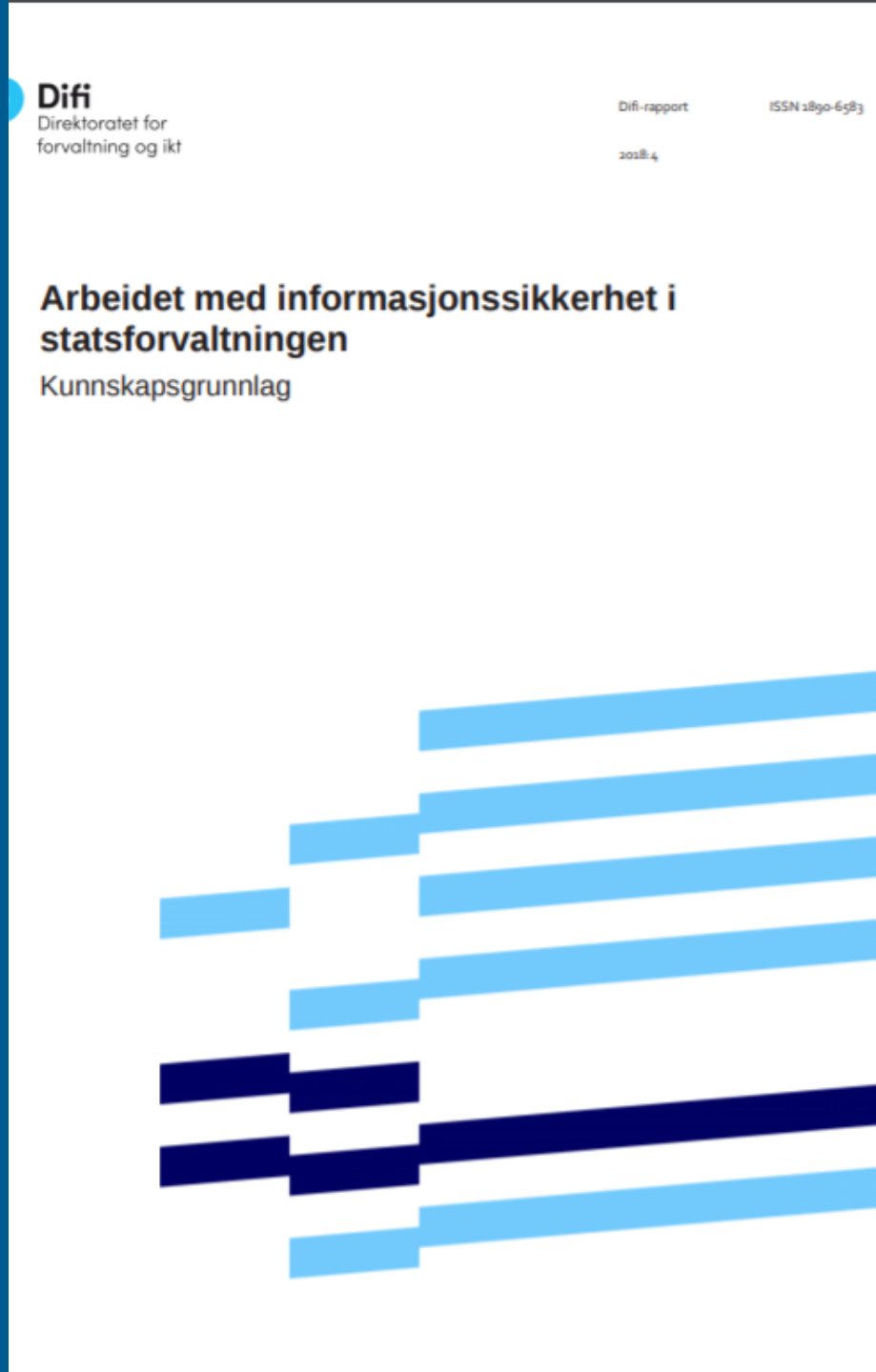
BAKGRUNN



Hovedfunn i Difi-rapport 2018:4

- Intervjuene viser at etatsstyrere i liten grad etterspør status på arbeidet med informasjonssikkerhet hos underliggende virksomheter.

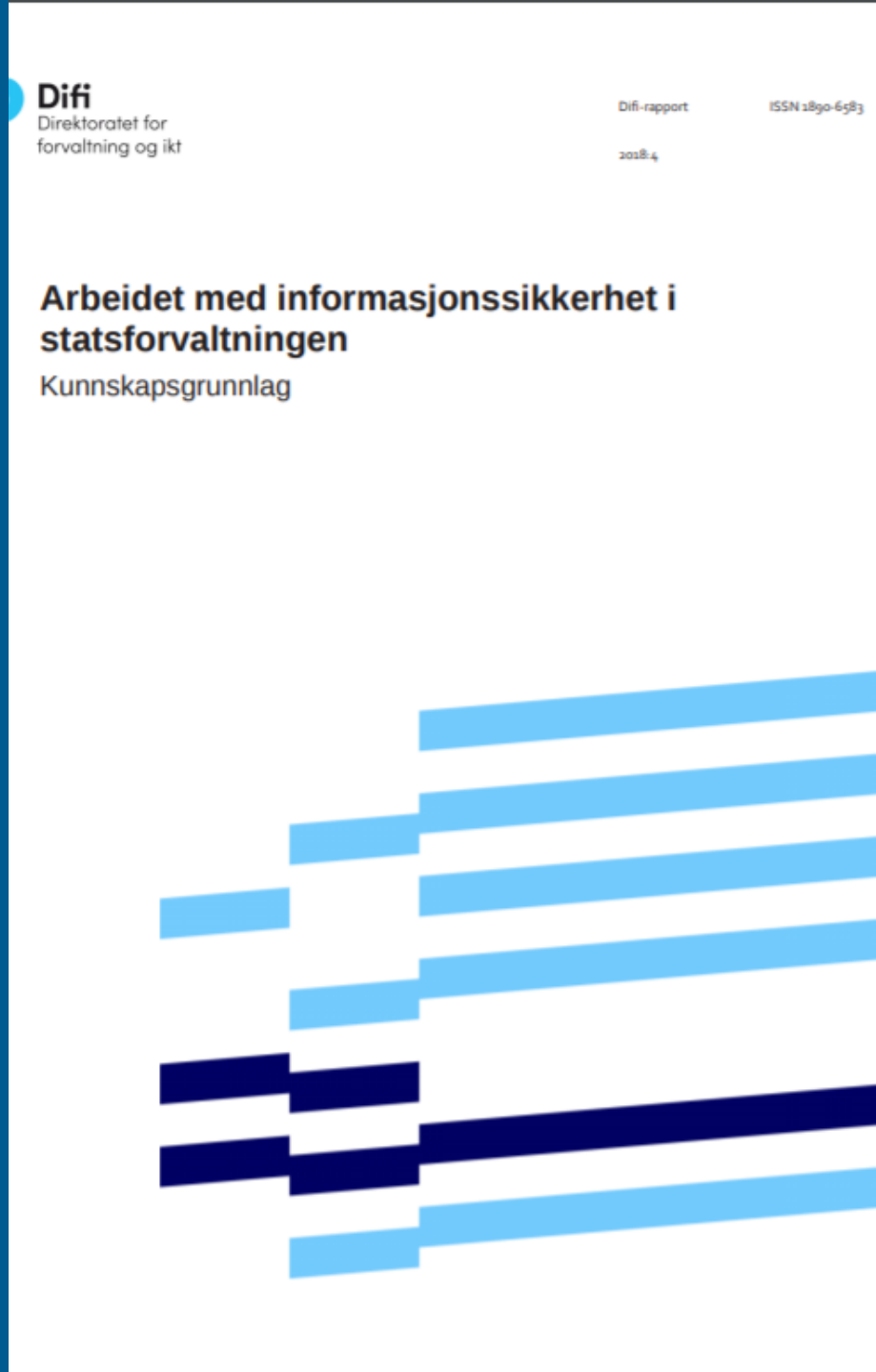
- Kun 64 prosent av virksomhetene svarer at informasjonssikkerhet har vært et tema i etatsstyringsdialogen, og 7 prosent sier at det ikke en gang vil omtales i årsrapporten for 2017.



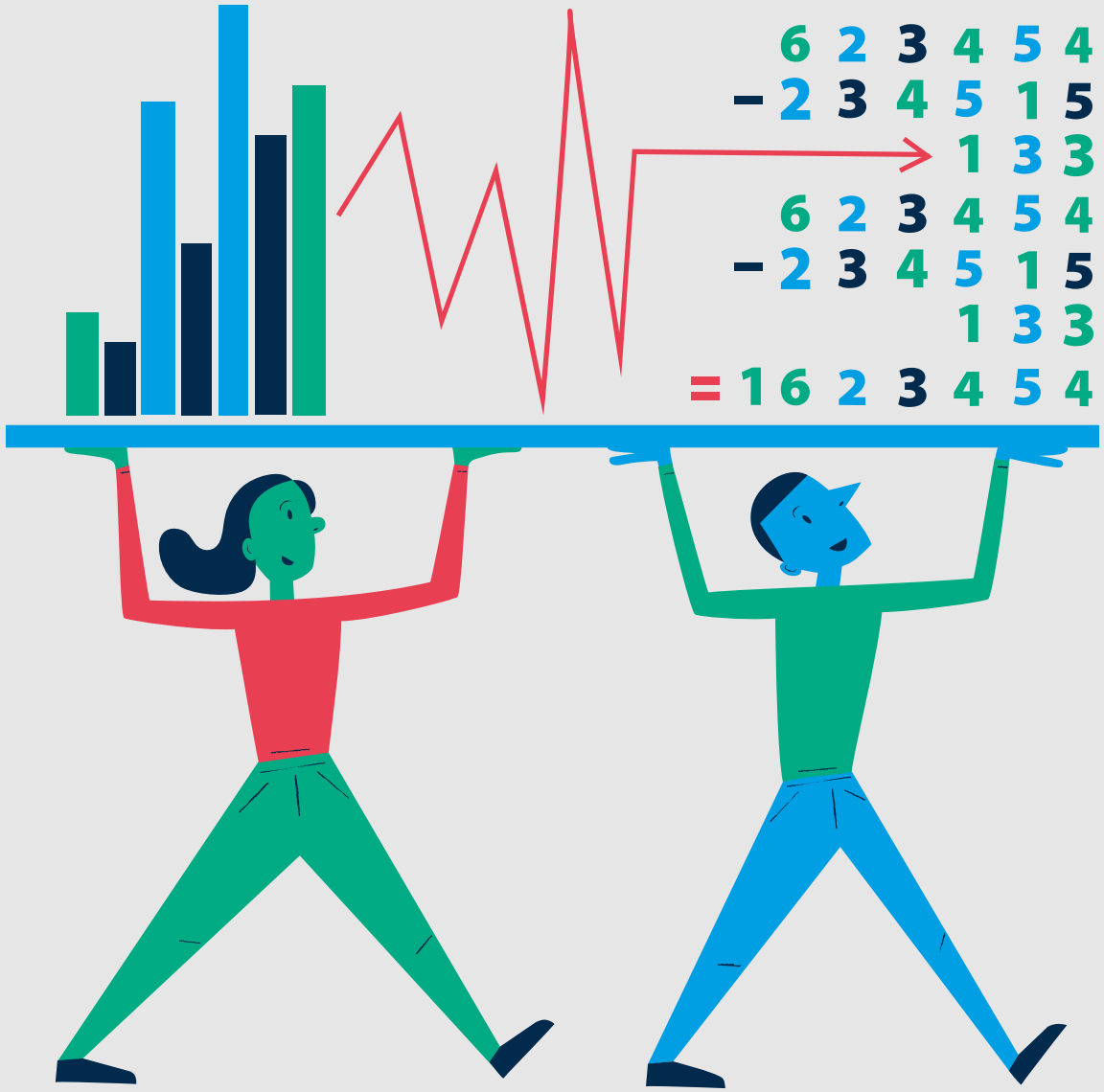
Anbefalinger fra Difi-rapport 2018:4

- Informasjonssikkerhet følges opp i styringsdialogen mellom departement og underliggende virksomhet. Etatsstyrere bør ha tilgang på veiledning om hvordan informasjonssikkerhet bør ivaretas i etatsstyringen. DFØ og Difi bør samarbeide om å gi denne veiledningen.

- Departementene stiller krav om at virksomhetene rapporterer på sikkerhetstilstanden for egen virksomhet, og status på arbeidet med styring og kontroll av informasjonssikkerhet i årsrapporten. Rapporteringen bør være lik og sammenlignbar for alle statlige virksomheter. DFØ bør i samarbeid med Difi gi veiledning om dette.



VEILEDNINGS-MATERIALET



- Helge Spildrejorde (DFØ)

- Anniken Grønli Foss (Difi/DFØ)

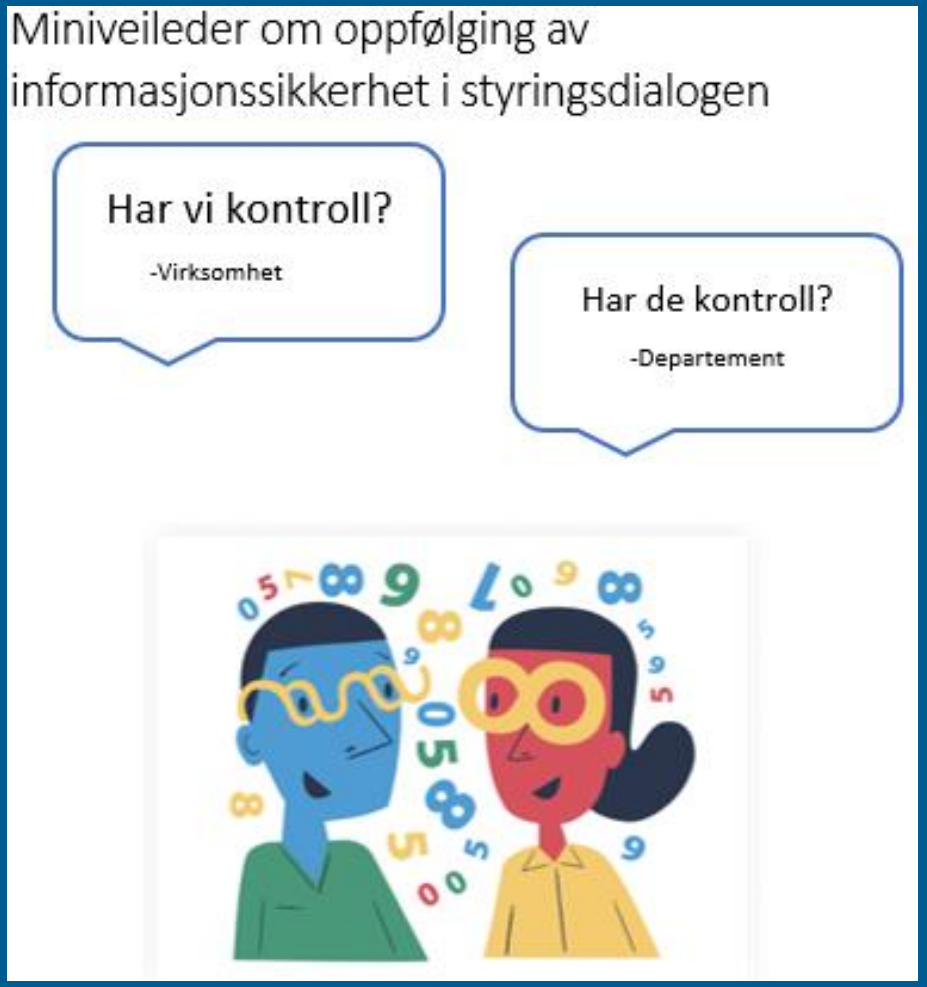
- Remi Longva (Difi/Digdir)

- Are Søndenaa (NSM)

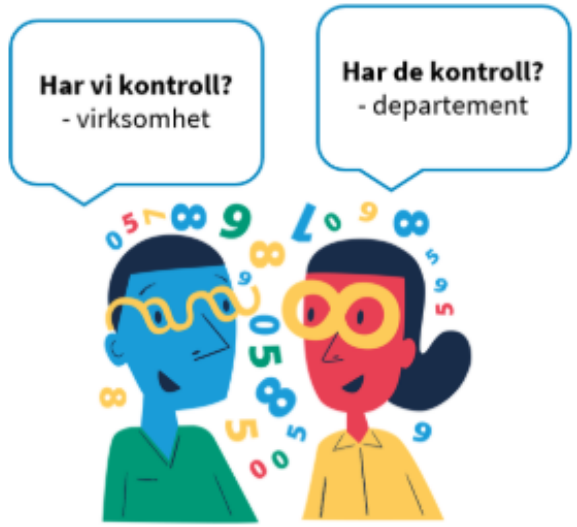
- Trine Wold Møller (DFØ)

Prosjektets leveranser

- **Miniveileder**
- **Dialogverktøy**
- **Justert veiledning i årsrapport**



Om veilederen



Oppdatert 10. feb. 2020

Denne veilederen gir en innføring i informasjonssikkerhet i underliggende virksomheter og viser hvordan departementet kan følge opp informasjonssikkerheten i styringsdialogen. Den kan derfor være nyttig både for deg som er etatsstyrer, og for deg som er ansvarlig for informasjonssikkerheten i en virksomhet.

Hvem bør lese denne veilederen?

Du bør lese denne miniveilederen hvis du

- er etatsstyrer som skal ivareta departementets overordnede ansvar for oppfølgingen av informasjonssikkerhet i en underliggende etat, for eksempel forberede et etatsstyringsmøte
- lurer på hvordan informasjonssikkerhet bør følges opp, og hvordan temaet bør behandles som en integrert del av virksomhetsstyringen i en underliggende virksomhet

Miniveileder om oppfølging av informasjonssikkerhet i styringsdialogen

- Gir innføring i informasjonssikkerhet i underliggende virksomheter og viser hvordan departementer kan følge opp informasjonssikkerhet
- Være til nytte for underliggende virksomhet i forståelsen av hvordan/ på hvilket nivå informasjonssikkerhet bør omtales i styringsdialogen
- Gir oversikt over temaer som alle involverte i styringsdialogen bør ta stilling til for å få mest mulig hensiktsmessig oppfølging
- Orienterer om krav i økonomiregelverket, og i andre aktuelle regelverk

Hva sier økonomireglementet?

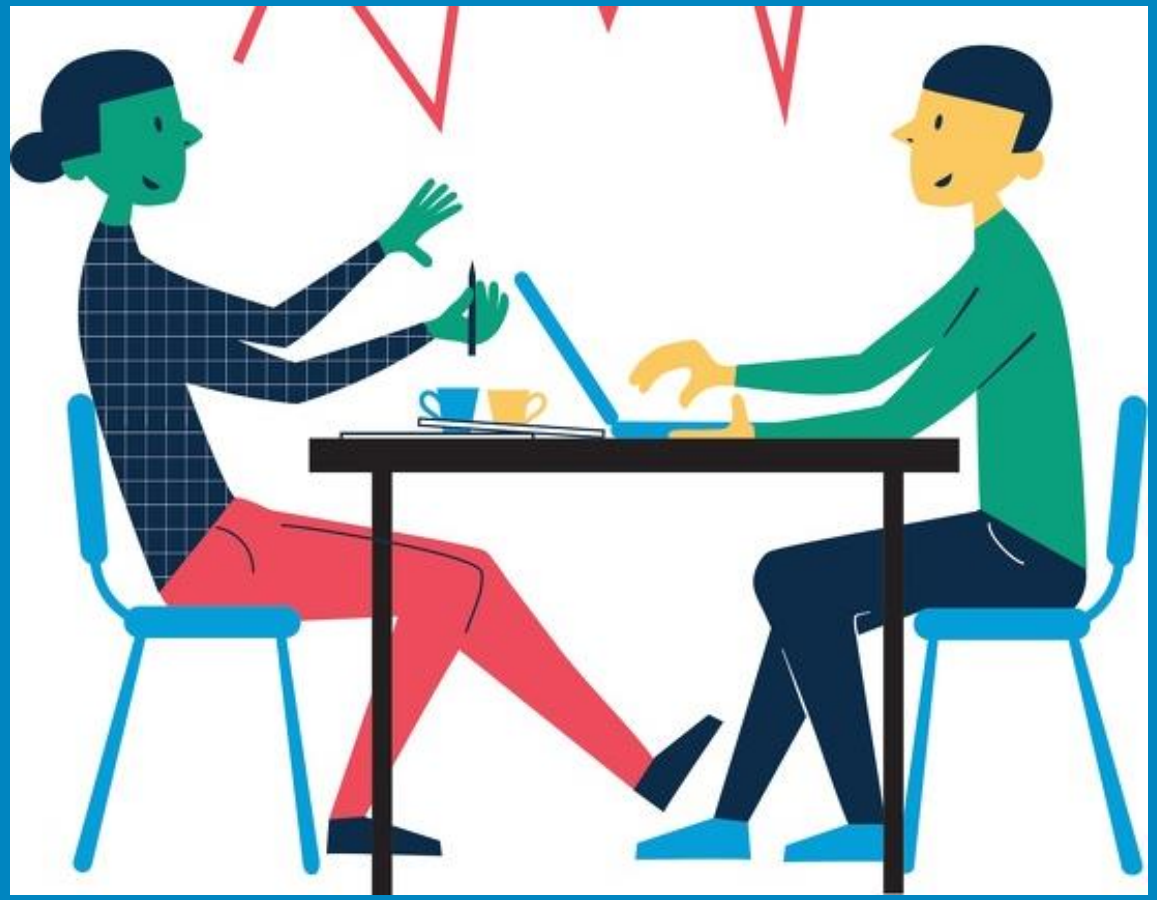
ØR §4 Grunnleggende styringsprinsipper

- Styring, oppfølging, kontroll og forvaltning må tilpasses virksomhetens **egenart** samt **risiko** og **vesentlighet**

ØR §14 Internkontroll

Styringen skal være tilpasset egenart, samt risiko og vesentlighet

- **Hva betyr egentlig det for oppfølgingen av informasjonssikkerhet?**



Hvor skal dialogen om informasjonssikkerhet inngå?

- **årsrapport:** omtale informasjonssikkerhet som en del av statusrapporten for styring og kontroll i del IV,
- **tildelingsbrev:** fastsette føringer for informasjonssikkerhet eller spesifikke rapporteringskrav
- **etatsstyringsmøter:** utdype krav og rapporteringspunkter
- **instruks:** sette generelle krav til styring og kontroll og sette eventuelle utdypende krav til informasjonssikkerhet

Om dialogverktøyet

Et hjelpemiddel i styringsdialogen, men også nyttig for virksomheten

Hvordan kan dette være relevant for kommunene?

Dialogverktøy – støtte til styringsdialogen om informasjonssikkerhet

Dette dialogverktøyet er et hjelpemiddel til styringsdialogen om informasjonssikkerhet mellom departement og virksomhet. Målgruppen er primært etatsstyrere i departementene, men verktøyet kan også være et nyttig for virksomheter. Dialogverktøyet kan benyttes både som forberedelse til, og i selve styringsdialogen.

Oppbyggingen av dialogverktøyet

Hoveddel

- Overordnede vurderinger av risiko, status og utfordringer i tillegg til virksomhetens styringssystem
- Departementet påser at det er etablert god nok internkontroll i virksomheten framfor å undersøke konkrete tiltak og aktiviteter

Fordypningsdel

- Når det er behov for å gå mer grundig inn i enkelte deler
- Systematiske aktiviteter for styring og kontroll
- Sikkerhetstiltak
- Etterlevelse av regelverk
- Spesielle temaer

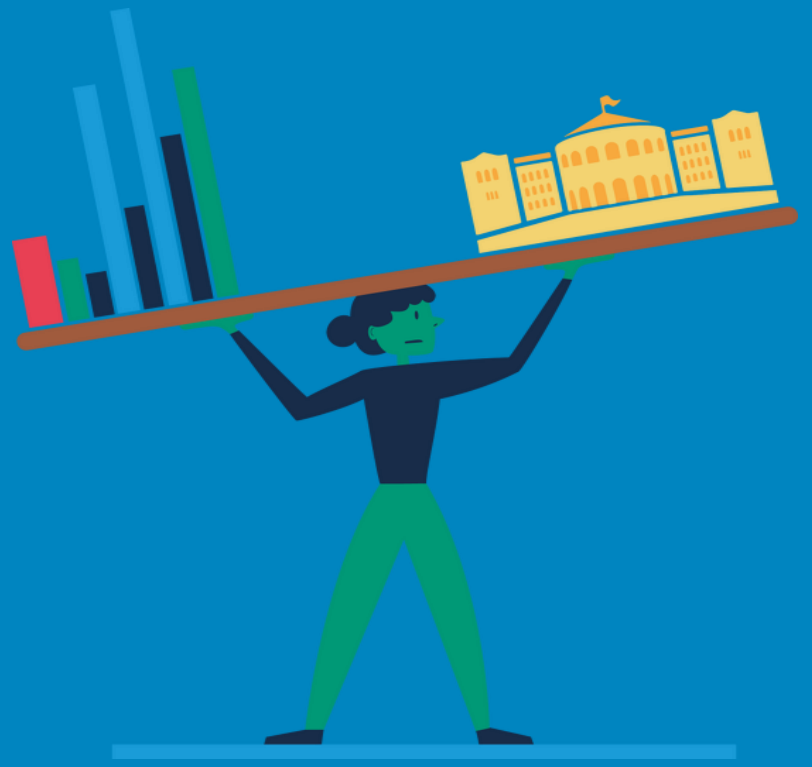
Indikerer god styring og kontroll
Ledelsen har oversikt over de systematiske aktivitetene for styring og kontroll med informasjonssikkerhet og kan redegjøre for disse.
Styring og kontroll av informasjonssikkerhet er en integrert del av styring og kontroll i virksomheten.
Internkontrollens struktur og innhold er lagt opp i tråd med gjeldende krav og anbefalinger. Eksempler er • eForvaltningsforskriften § 15 andre ledd, med krav om helhetlig styring som ivaretar krav i ulike regelverk • Digitaliseringsdirektoratets veiledning • sikkerhetsloven, med krav om sikkerhetsstyring som en del av virksomhetsstyringen
Virksomheten har systematiske aktiviteter som dekker det som er anbefalt: • ledelsens styring og oppfølging • risikovurdering • risikohåndtering • overvåking og hendelseshåndtering • måling, evaluering og revisjon • kompetanse- og kulturutvikling • kommunikasjon

Kan indikere manglende styring og kontroll
Ledelsen ser ikke på styringssystemet som sitt redskap for å ha styring og kontroll på området.
Informasjonssikkerhet styres for seg selv – uten knytning til virksomhets- og risikostyringen ellers.
Virksomheten har en rekke dokumenter, policy og retningslinjer, men kan ikke redegjøre for hvordan arbeidet blir gjennomført i praksis.

Ledelsen beskriver ikke styringsaktiviteter, inkludert aktiviteter for å foreta gode beslutninger om ressursbruk, prioritering og risiko tilknyttet de oppgavene og tjenestene de har ansvaret for.
Ledelsen beskriver hovedsakelig forskjellige sikkerhetstiltak uten å vektlegge de ledelsesstyrte systematiske aktivitetene for å styre informasjonssikkerhetsområdet. (Styringsaktivitetene inkluderer aktiviteter for å vurdere risiko og håndtere risiko – bl.a. for å velge sikkerhetstiltak.)

Relevant for kommunene?

- Generelle prinsipper for virksomhetsstyring
- Generelle prinsipper for risikostyring og internkontroll
- Hovedbudskap gjennom veiledningsmaterialet: Arbeidet med informasjonssikkerhet skal være en integrert del av virksomhetsstyringen



Direktoratet
for forvaltning og
økonomistyring

Takk for meg!

trinewold.moller@dfo.no