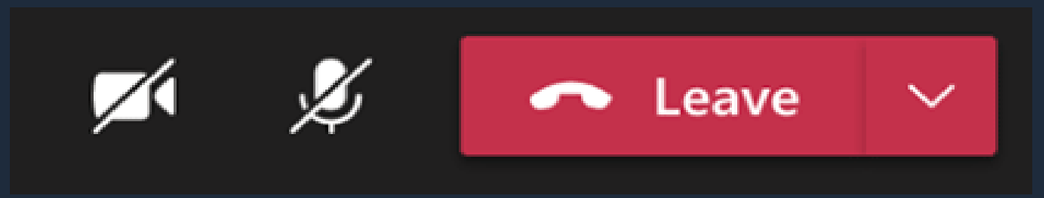
Digdir

digdir.no

# Orienteringsmøte
# Felles sikkerhet i forvaltningen

08.02.2022



# Agenda

| TID | TEMA |
|---|---|
| 10:00 | Innledning |
| 10:05 | Et nasjonalt løft for informasjonssikkerhet. Vi går gjennom kontekst, utfordringsbildet og mulig retning. |
| 10:30 | Oppgave «En ting som dere synes er vanskelig i arbeidet med informasjonssikkerhet» |
| 10:45 | Diskusjon i plenum |
| 10:55 | Avslutning |

Digdir

# Felles sikkerhet i forvaltningen

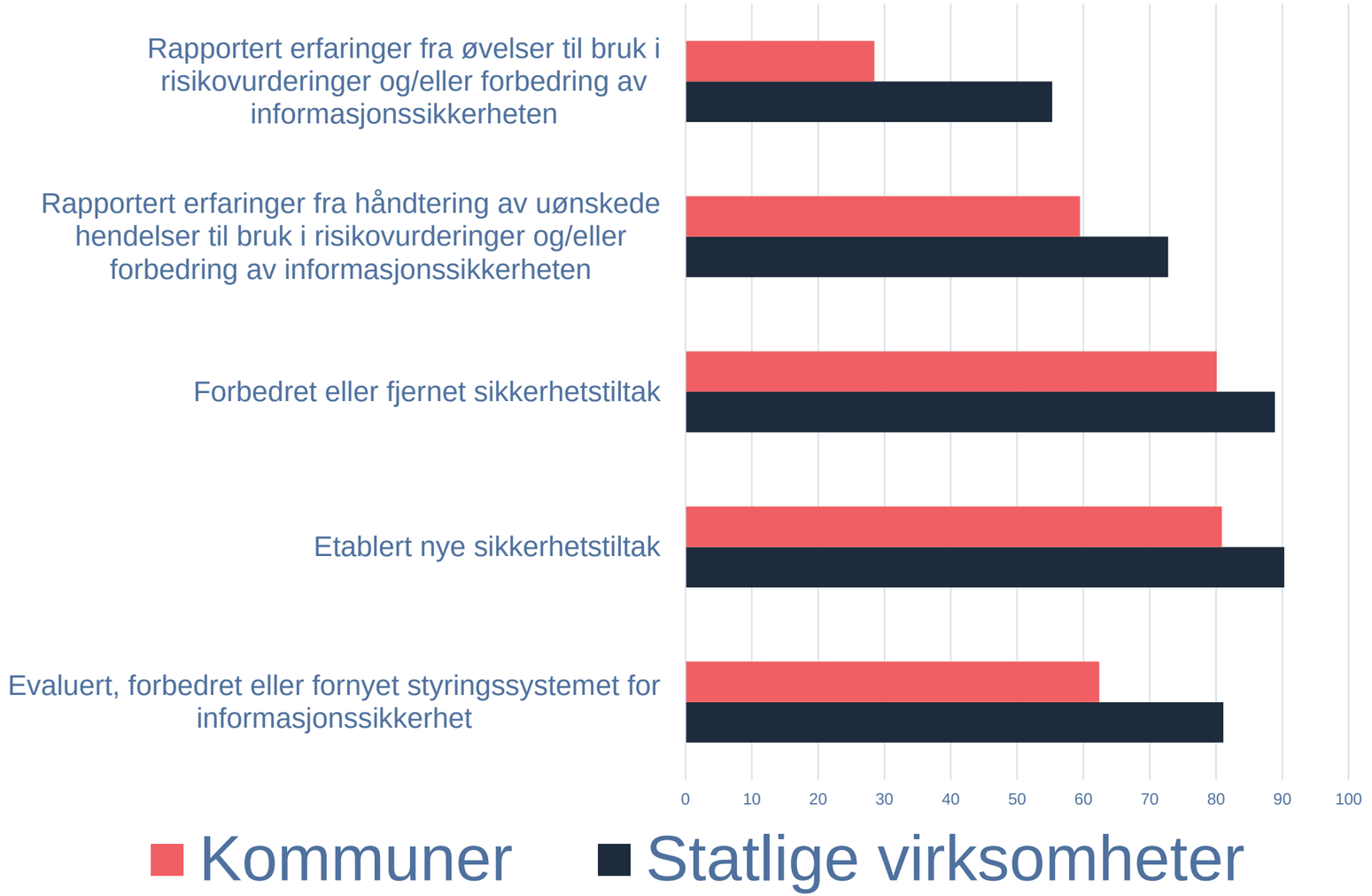
- Behov for taktskifte i forvaltningen
- Et nasjonalt løft for informasjonssikkerhet
- Spesielt digital sikkerhet

# Felles sikkerhet i forvaltningen

- Et initiativ fra Digitaliseringsdirektoratet
- Konkret veiledning - brukerorientert
- Gjøre like ting likt
- Samarbeid mellom veiledningsaktørene
- Notat – utgangspunkt for videre arbeid
- Forståelse for utfordringsbildet

# Utfordringsbildet





← Til dfo.no

Miniveileder om oppfølging av informasjonssikkerhet i styringsdialogen

Skriv ut | Innhold | Søk

1. Om veilederen | 2. Hva og hvorfor er det viktig? | 3. Oppfølging av informasjonssikkerhet | 4. Dialogverktøy | 5. Begrepsforståelse | 6. Krav i regelverk

# 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.

Innholdsfortegnelse

→ Hvem bør lese denne veilederen?

Hva kan du bruke veilederen til?

## 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
- er leder eller ansvarlig for arbeidet med informasjonssikkerhet i en virksomhet og skal ha dialog med departementet om dette

## Hva kan du bruke veilederen til?

Miniveilederen er en hjelp for å
informasjonssikkerhet. Vi har l
tar hensyn til at behovene vari

- Behovet for å følge opp in
departement til departen

ovelse.no

Om ovelse.no | Logg inn | Registrer deg

# Velkommen til øvelser for bedre digital sikkerhet

Velkommen til myndighetenes øvingsportal som skal bidra til at alle virksomheter i Norge får et øvingstilbud innen digital sikkerhet. Bruk av øvelser er sentralt element i Nasjonal strategi for digital sikkerhet.

Portalen er laget som et ledd i den nasjonale øvelsen Digital 2020, og her tilbys diskusjonsøvelser basert på ulike scenarier som kan ramme din virksomhet.

Hensikten med øvelsene er at din virksomhet skal få mulighet til å diskutere seg frem til hvordan det er naturlig å håndtere ulike type hendelser. Samtidig får virksomheten din litt støtte på veien i form av diskusjonsspørsmål og råd om hva du bør tenke på for å forberede deg på denne type scenarioer.

Lykke til!

Logg inn | Registrer deg

Hva er en diskusjonsøvelse?

Kom i gang

Forskning og diskusjonsø

enfor info

Digdir

Søk | Meny

Hjem > Informasjonssikkerhet > Kompetanse- og kulturutvikling

# Kompetanse- og kulturutvikling innen informasjonssikkerhet

Her finner du veiledning som kan hjelpe deg når du skal arbeide med kompetanse og kultur innen informasjonssikkerhet i din virksomhet.

### Kartlegging av digital sikkerhetskultur

Få veiledning om hvordan du kan kartlegge den digitale sikkerhetskulturen i din virksomhet.

### Kompetanse- og kulturutvikling innen digital sikkerhet

Få veiledning om hvordan du kan arbeide med utvikling av kompetanse og kultur knyttet til digital sikkerhet.

## Virkemidler

Meny

# 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.

Oppdatert 14. des. 2021

Innholdsfortegnelse

→ Dialogverktøyet er delt i to: en hoveddel og en fordypningsdel

Gå videre til de ulike delene

Last ned dialogverktøyet som PDF

Bruk dialogverktøyet sammen med miniveileder

Forarbeid

Hvordan verktøyet kan benyttes

## Dialogverktøyet er delt i to: en hoveddel og en fordypningsdel

Dialogverktøyet beskriver hvilke temaer som kan være relevant å ta opp i styringsdialogen. Om temaene skal tas opp, hvordan de skal tas opp og behandles, eller hvilke spørsmål som skal stilles, må – i likhet med all annen etatsstyring – tilpasses egenart, samt risiko og vesentlighet. Verktøyet er ikke uttømmende for alle tenkelige behov, for oppfølgingen av alle statlige virksomheter.

Innholdet er basert på krav og anbefalinger i lov, forskrift og veiledninger. Det er likevel ikke ment å fungere som en fasit, men som et hjelpemiddel til dialog mellom departement og underliggende virksomhet.

Alt i dialogverktøyet handler om arbeidet med informasjonssikkerhet i en virksomhet. For eksempel, der «styring og kontroll» er brukt, så menes det «styring og kontroll på informasjonssikkerhetsområdet».

### Gå videre til de ulike delene

Hoveddel – styringsdialog om informasjonssikkerhet →

Fordypning i temaer knyttet til informasjonssikkerhet →

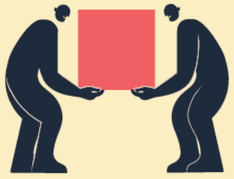
Digdir

Søk | Meny

Hjem > Informasjonssikkerhet > Styring av informasjonssikkerhet > Helhetlig styring og kontroll

# Helhetlig styring og kontroll av informasjonssikkerhet

For å sikre god styring og kontroll av informasjonssikkerhet må man jobbe helhetlig, og se informasjonssikkerhet som en del av virksomhetsstyringen. Her kan du lese om sammenhengen mellom virksomhetsstyring, informasjonssikkerhet, personvern og sikkerhetsstyring etter sikkerhetsloven.



### Hva vil det si?

Å jobbe helhetlig betyr at man skal se sammenhengen mellom viktige områder og aktiviteter i virksomheten.

### Hva er felles?

De samme grunnreglene gjelder uavhengig av hvilket fagområde man skal drive styring og kontroll på. Les mer om fellestrekkene her.

### Hva er ulikt?

Helheten er ikke den samme for alle, og ulike perspektiver gir ulikt fokus. Les mer om noe av det som må tas hensyn til dersom man skal lykkes med å jobbe helhetlig.

## Hvor får du hjelp?

### Aktører som veileder innen styring og kontroll

DFØ, Digitaliseringsdirektoratet, KS, NSM og Datatilsynet har alle veiledning som er relevant når man jobber med ulike deler av informasjonssikkerhet.

→

### Om denne veiledningen

Denne veiledningen er resultatet av et samarbeid mellom NSM, DFØ og Digitaliseringsdirektoratet. Datatilsynet og KS har også bidratt i arbeidet.

→

Kompetansebeskrivelser

- Rolle: Fagansvarlig informasjonssikkerhet
- Rolle: Rådgiver informasjonssikkerhet
- Rolle: Risikoeier
- Rolle: Topplеder
- Rolle: Øvrig ledergruppe
- Rolle: IT-leder
- Rolle: Systemeier
- Rolle: Alle ansatte

# Rolle: Fagansvarlig informasjonssikkerhet

Fagansvarlig informasjonssikkerhet har som hovedansvar å være pådriver og støtte til ledelsen og organisasjonen for øvrig i informasjonssikkerhetsarbeidet.

## Ansvar og oppgaver

Hvilken stilling den fagansvarlige har i virksomheten, vil variere avhengig av virksomhetens organisering og behov. Dersom fagansvarlig har en stilling som leder i virksomheten, vil oppgavene og ansvaret komme i tillegg til oppgaver og ansvar vedkommende har som følger stillingsbeskrivelsen.

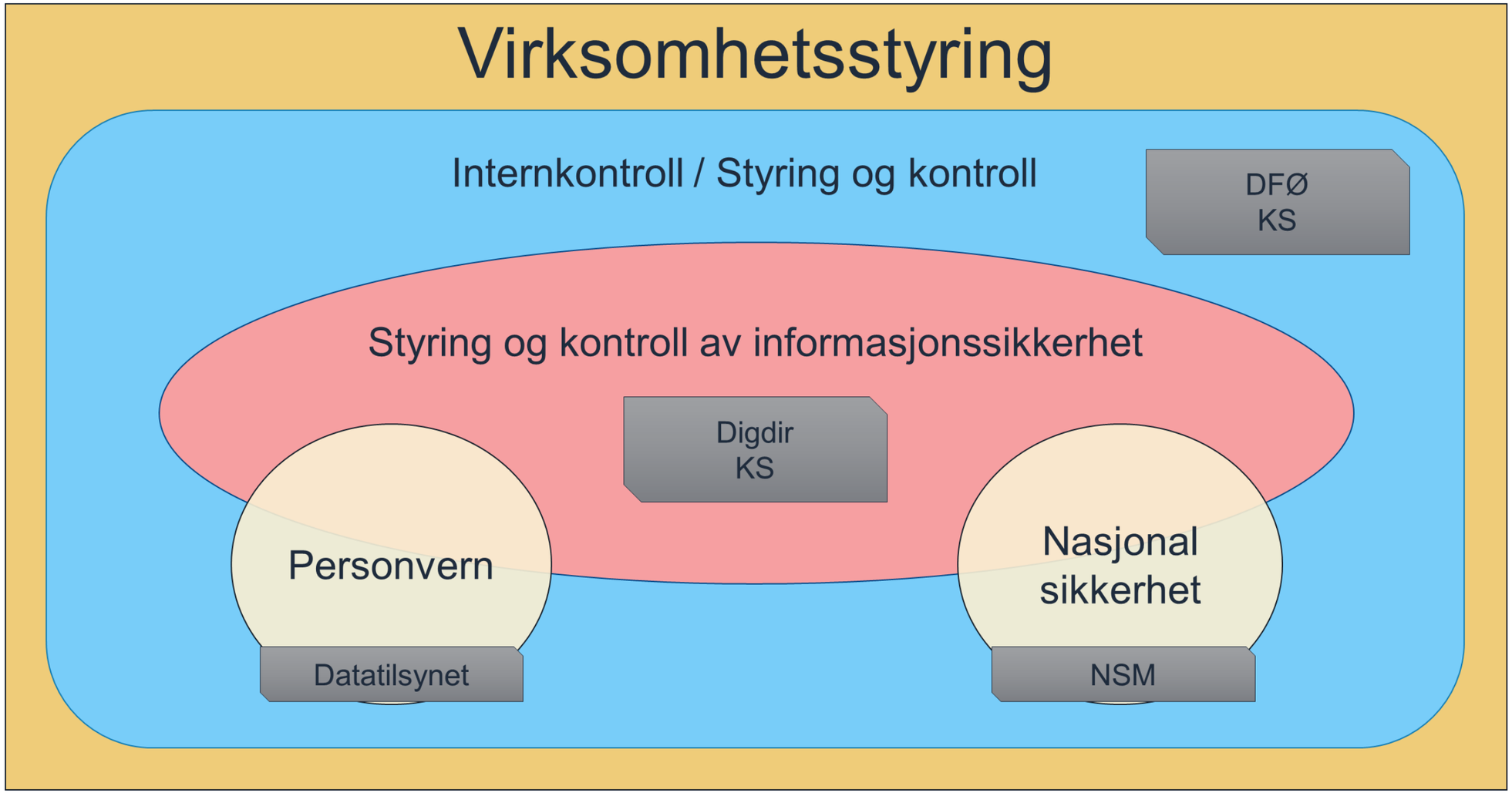
Fagansvarlig informasjonssikkerhet skal bistå virksomhetsledelsen i utføringen av alle delaktivitetene under ledelsens styring og oppfølging.

I tillegg skal fagansvarlig informasjonssikkerhet være en nøkkelressurs i virksomhetens kontinuerlige internkontrollarbeid på informasjonssikkerhetsområdet, blant annet ved å bistå i arbeidet med risikovurdering og -håndtering, og måling, evaluering og revisjon. Fagansvarlig har ofte ansvaret for å planlegge og gjennomføre opplæring og bevisstgjøringsaktiviteter innen informasjonssikkerhet i virksomheten.

## Ønsket kompetanse

Fagansvarlig informasjonssikkerhet er ikke en IKT-teknisk rolle. Den krever imidlertid god forståelse for IKT-relaterte risikoer, og andre typer informasjonssikkerhetsrisikoer. I tillegg må fagansvarlig informasjonssikkerhet ha god forståelse for

# Aktørkart


Virksomhetsstyring
Internkontroll / Styring og kontroll
DFØ
KS
Styring og kontroll av informasjonssikkerhet
Digdir
KS
Personvern
Datatilsynet
Nasjonal
sikkerhet
NSM

# Flere utfordringer

digdir.no

- Kompetansekrevende
- Ressurskrevende
- Virksomheter gjør delvis de samme vurderingene
- Utilstrekkelig oversikt over informasjonsbehandlingen
- Mangelfull forvaltning av sikkerhetstiltak
- Mangler grunnleggende sikkerhetstiltak
- Krevende å undersøke om omfang av sikkerhetstiltak er tilstrekkelig
- Bruk av tjenesteleverandører
- Manglende tillit mellom virksomheter hinder for digitalisering
- Vanskelig å få en helhetlig tilnærming i virksomheter
- Mangelfull og fragmentert regulering
- Vanskelig å måle/evaluere på tvers av virksomheter

# IKT-sikkerhetsutvalget - dagens regelverk er krevende å etterleve

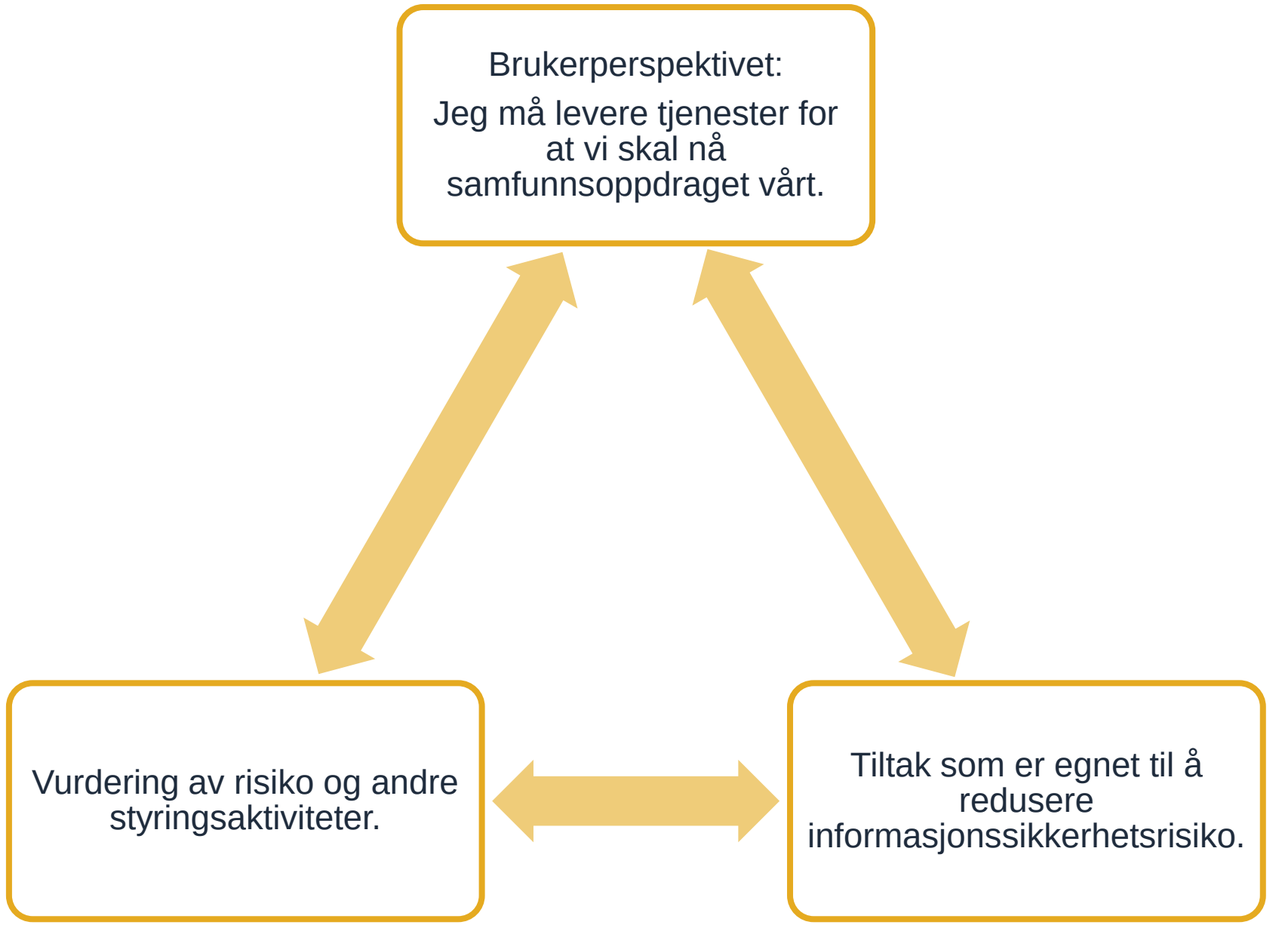
01 **Mange har ikke tilstrekkelig kompetanse** til å etterleve funksjonsbaserte regelverk, og kravene er ofte overordnede og vage. For vage krav kan medføre dårligere etterlevelse på grunn av **usikkerhet rundt hva som kreves for å oppfylle kravet**.

02 Funksjonsbaserte regelverk setter også **større krav til at virksomhetene har tilstrekkelig kompetanse** og evne til å vurdere hva som ligger innenfor regelverkets krav.

03 Blir regelverket for generelt eller vagt, kan det gi store **variasjoner i etterlevelsen og håndhevingen**.

[1] IKT-sikkerhet i alle ledd - Organisering og regulering av nasjonal IKT-sikkerhet (NOU 2018:14)

# Virksomhetsperspektivet



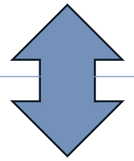
# *«Felles sikkerhet i forvaltningen»*

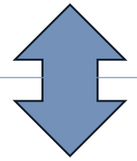
**Viktige spørsmål virksomhetene må stille seg selv.**

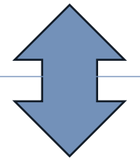
Hvilke oppgaver leverer vi, og hvilken informasjon behandles?

Hvor store konsekvenser kan informasjons-sikkerhetshendelser få?

Hvilke sikkerhetstiltak bør vi etablere?







Katalog over oppgaver, og informasjonsbehandling

Vurdering av konsekvensnivå per oppgave


Anbefalte minimumstiltak

**Svar fra veiledningsaktørene, på ett sted, felles for alle.**

# Leveransen kan ha flere konkrete gevinster

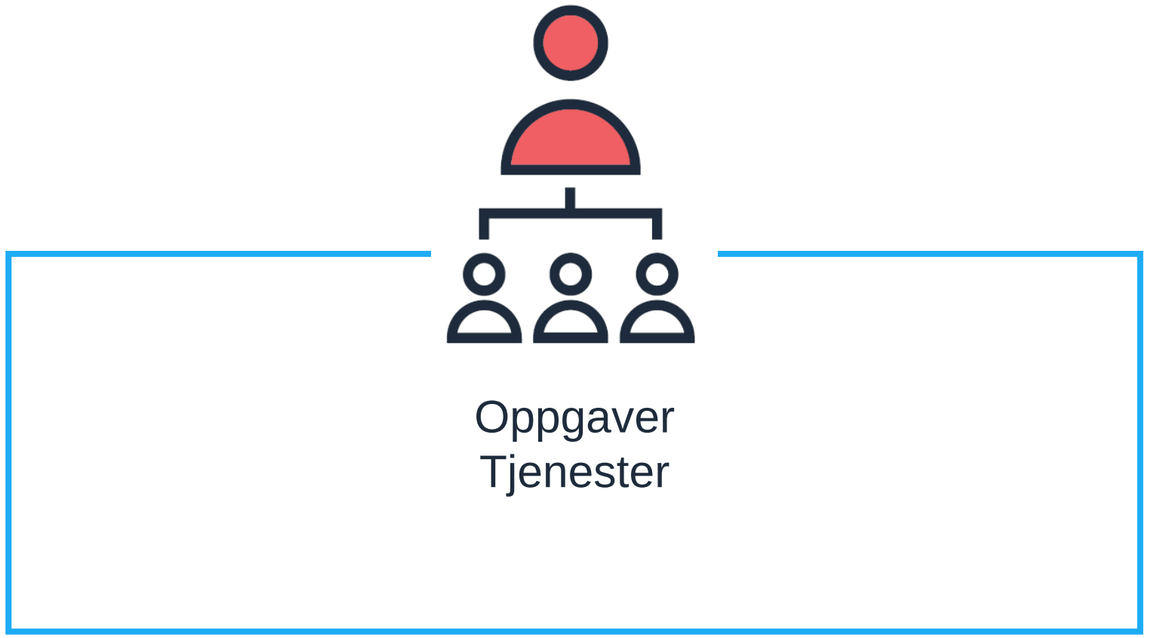
- Sentraliserte faglige vurdering, som **effektiviserer** arbeidet i hver enkelt virksomhet og gir **bedre sikkerhet**
- En styrket grunnmur på tvers av virksomheter som gir **tillitt,** enklere utvikling av **sammenhengende tjenester** og **deling av data**
- Mulighet til å **måle** virksomheter og **sammenlikne** tilstand mellom virksomheter
- Kan gi et forenklet mer **effektivt grensesnitt mot leverandørmarkedet** gjennom markedsplassen for skytjenester

Digdir

digdir.no

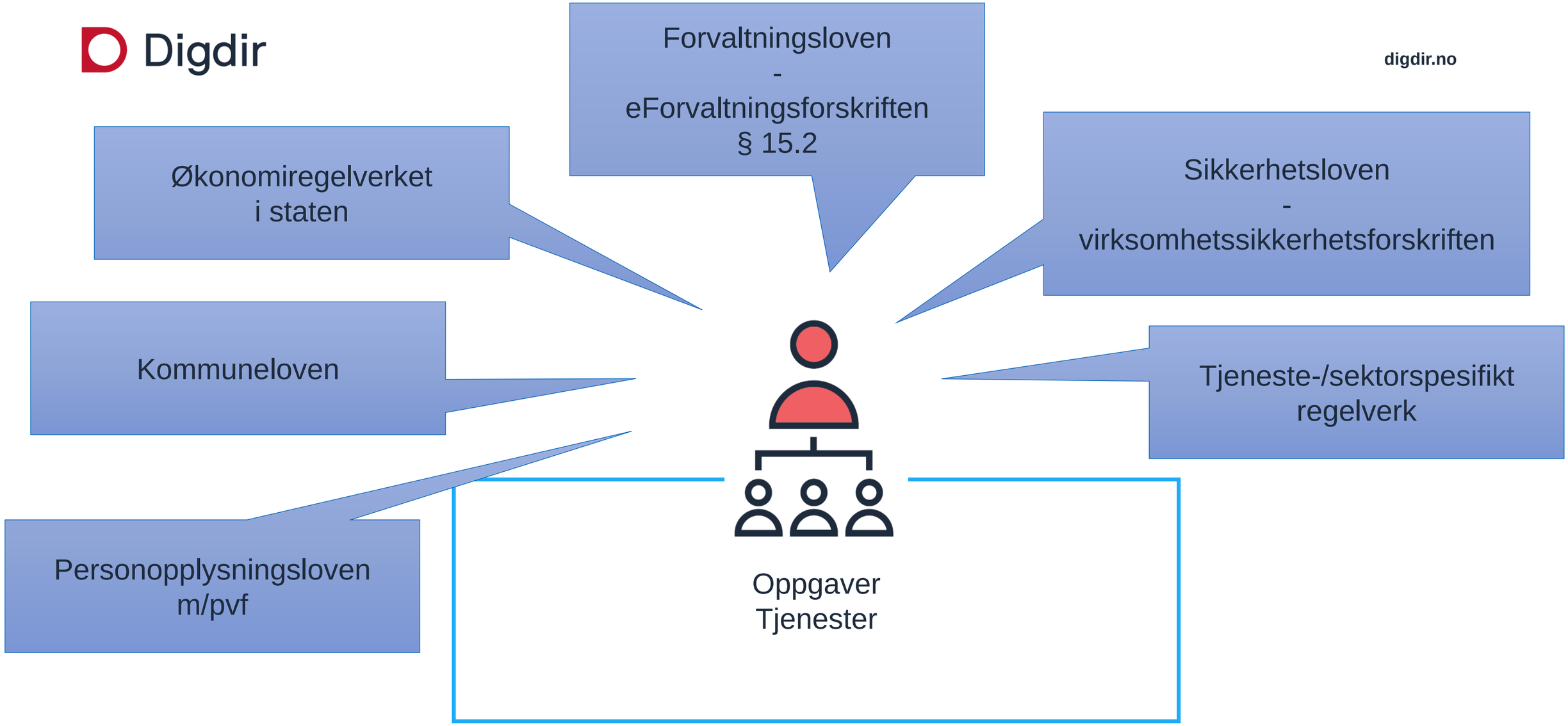
# Utfordringsbildet –vårt perspektiv

# Selvstendig ansvar for styring og kontroll

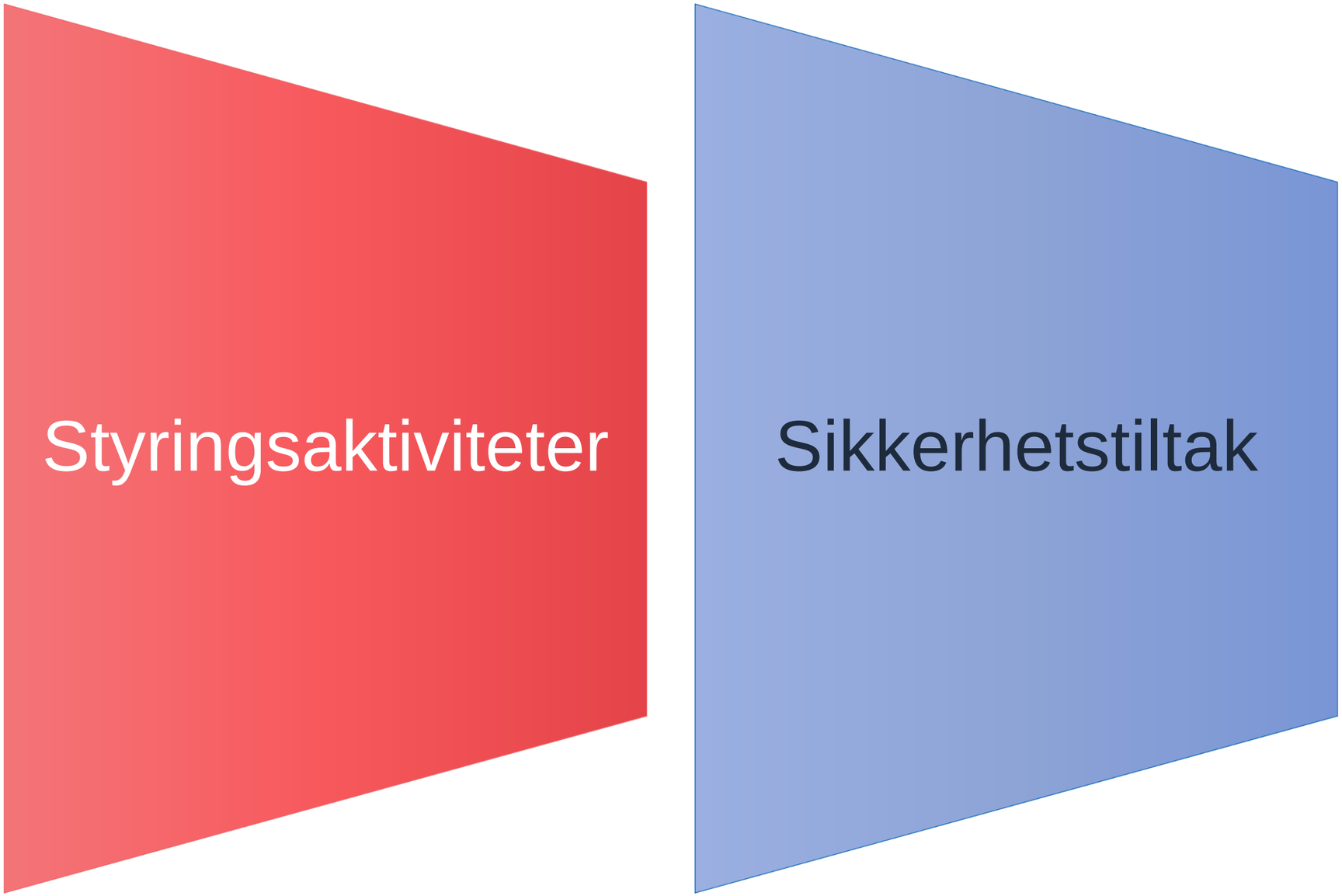


Digdir

digdir.no




# Selvstendig ansvar for styring og kontroll


Styringsaktiviteter
Sikkerhetstiltak

# Svake eller manglende styringsaktiviteter

- Ledelse som ikke er i stand til å ivareta ansvaret sitt
- Svak vurdering og håndtering av risiko på området
  - kan være delvis frikoblet fra oppgaver og tjenester
  - kan være delvis frikoblet fra ledelsens prioritering av ressursbruk
- Viktig for oppgaveløsningen – kan ikke bare være forankret i ledelsen – ledelsen må styre aktivt

# Mangler grunnleggende sikkerhetstiltak

- Når hendelser inntreffer eller tilsynsmyndigheter gjør grundige undersøkelser
- Helt grunnleggende sikkerhetstiltak er ikke etablert
- Eller de fungerer ikke etter hensikten

# Utilstrekkelig oversikt

- Mangler god oversikt over
  - oppgaver og tjenester
  - informasjonstyper som behandles i disse
  - informasjonssystemene (inkl. digitale systemer) de benytter
  - hva konsekvensene kan bli ved informasjonssikkerhetsbrudd
- Gjør det vanskelig å
  - Prioritere ressursinnsatsen
  - Ha oversikt over risiko
  - Dekke behovet for sikkerhetstiltak

# Mangelfull forvaltning av sikkerhetstiltak

- Systematisk godkjenning og etablering av sikkerhetstiltak
- Kostnadseffektiv forvaltning av sikkerhetstiltak på tvers av oppgaver og tjenester
- Tydelig ansvar for sikkerhetstiltak
  - Inkludert de hos tjenesteleverandører
- Evaluering og oppfølging av etablerte sikkerhetstiltak

Rapport om Østre Toten kommune:
Basert på at implementering av sikkerhetstiltak fremstår som noe tilfeldig, samtidig som enkelte mangler er blitt identifisert, men ikke gjort noe med, vurderer KPMG sikkerhetsstyringen i kommunen som svak eller mangelfull.

# Ressurs- og kompetansekrevende

- Risikobasert / fleksibelt / tilstrekkelig / balansert
- Det krever likevel betydelig kompetanse og ressurser å arbeide iht. gjeldende regelverk

# Tillit og samarbeid mellom virksomheter

- Virksomheter i forvaltningen skal dele og bruke data og bygge sammenhengende tjenester på tvers av virksomhetsansvaret
- Behov for tillit til at andre virksomheter har tilstrekkelig informasjonssikkerhet
- Et svakt ledd i en tjenestekjede kan få konsekvenser for tjenester hos alle virksomhetene som er involvert

# Bruk av tjenesteleverandører

- Mange har utfordringer med bruk av tjenesteleverandører i informasjonsbehandlingen
- Det er ikke helhetlig og ensartet kravstilling fra offentlig forvaltning til leverandørmarkedet

# Delvis de samme vurderingene

- Virksomheter må ofte gjøre tilsvarende vurderinger
- Kan være stor variasjon i vurderingene
  - uten at de er begrunnet i ulike og unike behov
- Virksomheter har delvis like oppgaver og tjenester
  - En del av oppgaver / tjenester i kommuner og fylkeskommuner
  - Støtteoppgaver som eksempel personalforvaltning eller anskaffelsesprosess

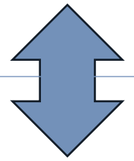
# *«Felles sikkerhet i forvaltningen»*

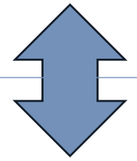
**Viktige spørsmål virksomhetene må stille seg selv.**

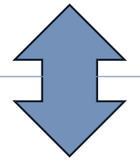
Hvilke oppgaver leverer vi, og hvilken informasjon behandles?

Hvor store konsekvenser kan informasjons-sikkerhetshendelser få?

Hvilke sikkerhetstiltak bør vi etablere?







Katalog over oppgaver, og informasjonsbehandling

Vurdering av konsekvensnivå per oppgave


Anbefalte minimumstiltak

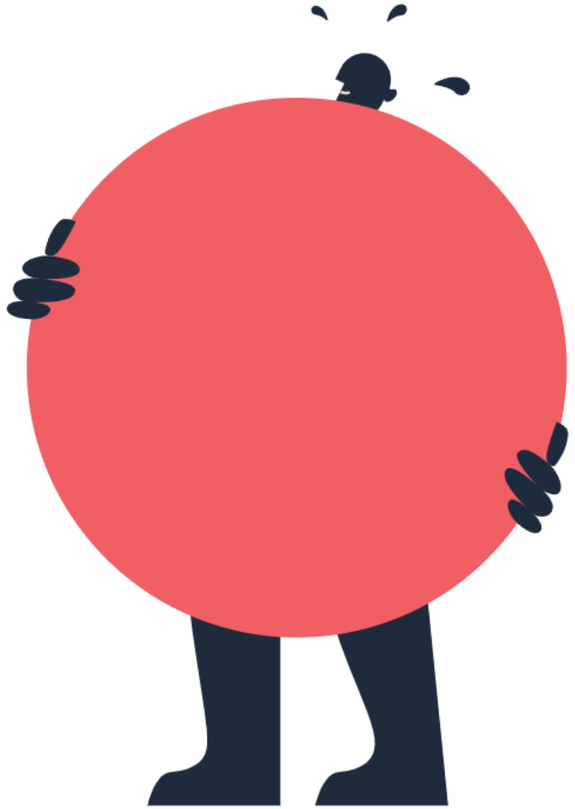
**Svar fra veiledningsaktørene, på ett sted, felles for alle.**

Digdir

digdir.no

# Oppgave

En ting som dere synes er vanskelig i arbeidet med informasjonssikkerhet.



Digdir

digdir.no

# Vi vil høre dine vurderinger

# Tilbakemeldinger - Questback

- Sendes ut etter møtet
- Ranger utfordringene knyttet til hvordan du opplever de i din arbeidshverdag
- Opplever du flere utfordringer enn vi har listet opp?
- Vil du høre mer om dette arbeidet og være en bidragsyter videre.
- Vi ønsker svar i løpet av 15.02.2022

Spørsmål?

infosikkerhet@digdir.no

**digdir.no**

**Digitaliseringsdirektoratet**
postmottak@digdir.no
22 45 10 00
Postboks 1382 Vika, 0114 Oslo

**Besøksadresser:**
**Industriveien 1, 8900 Brønnøysund**
**Skrivarevegen 2, 6863 Leikanger**
**Grev Wedels Plass 9, 0151 Oslo**