Digdir

digdir.no

Etatsstyring

OBS

- Litt drodling og mange forenklinger

  - Den virkelige verden er (som alltid) mye mer nyansert og kompleks
  - Detaljert veiledning om etatsstyring finner dere hos Direktoratet for forvaltning og økonomistyring (DFØ)

Styringsmodeller

- Du kan lese om ansvar, oppgavefordeling og styringsutfordringer i Riksrevisjonens rapport.
  - HOD - Regionale helseforetak (RHF) - Helseforetak (HF)
  - Styre + Daglig ledelse (Adm.dir.)
  - Felleseide/styrte leverandører

- Her vil det stort sett handle om:
  - Styrende organ ←→ Underliggende virksomhet

Helse- og omsorgsdepartementet har vært for passive i sin oppfølging av informasjonssikkerhetsarbeidet i helseregionene

[..] departementet har i foretaksmøtene stilt krav om informasjonssikkerhet.

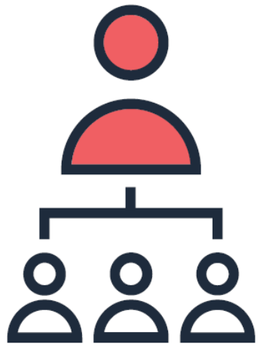
[..] helseforetakene har i all hovedsak ikke rapportert konkret tilbake…

…og departementet har heller ikke etterspurt denne informasjonen.

God dialog?

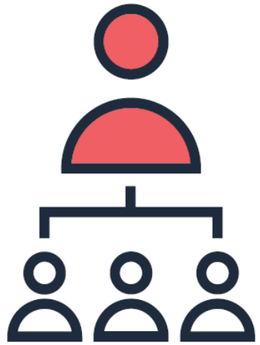
Hva mener vi med «følge opp informasjonssikkerhet»?

Oppgaver
Tjenester



Selvstendig ansvar for styring og kontroll i virksomheten

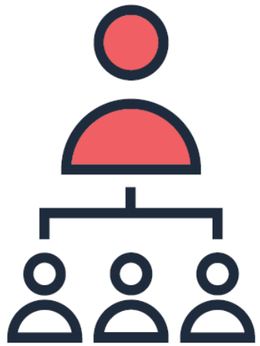
Påse at underliggende virksomhet har tilstrekkelig styring og kontroll



Selvstendig ansvar for styring og kontroll

- Påse at det er etablert hensiktsmessige systemer og strukturer for styring og kontroll
- I stedet for å stille konkrete krav til tiltak og aktiviteter
- Basere seg på virksomhetens egen vurdering

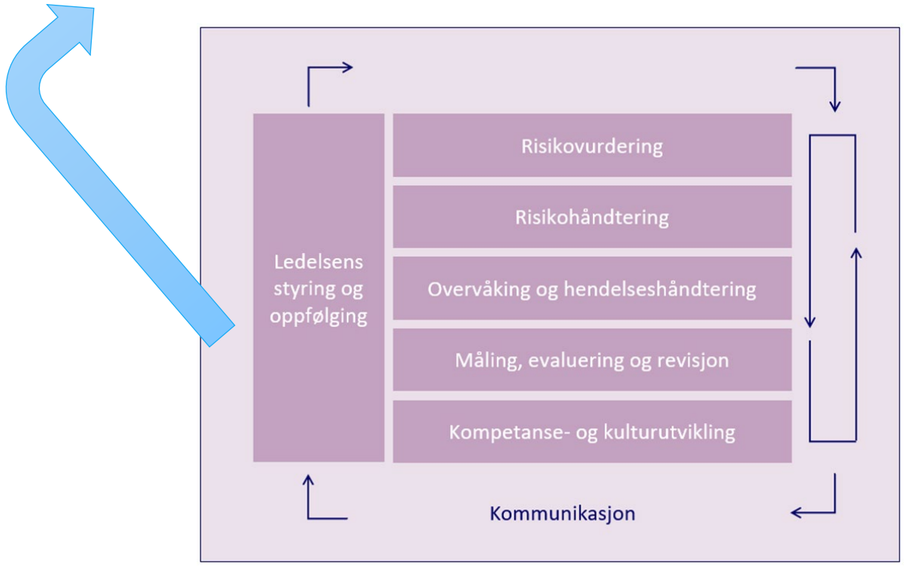
Påse at underliggende virksomhet har tilstrekkelig styring og kontroll



Selvstendig ansvar for styring og kontroll

Rapportering på styring og kontroll

Virksomhetsledelsens gjennomgang

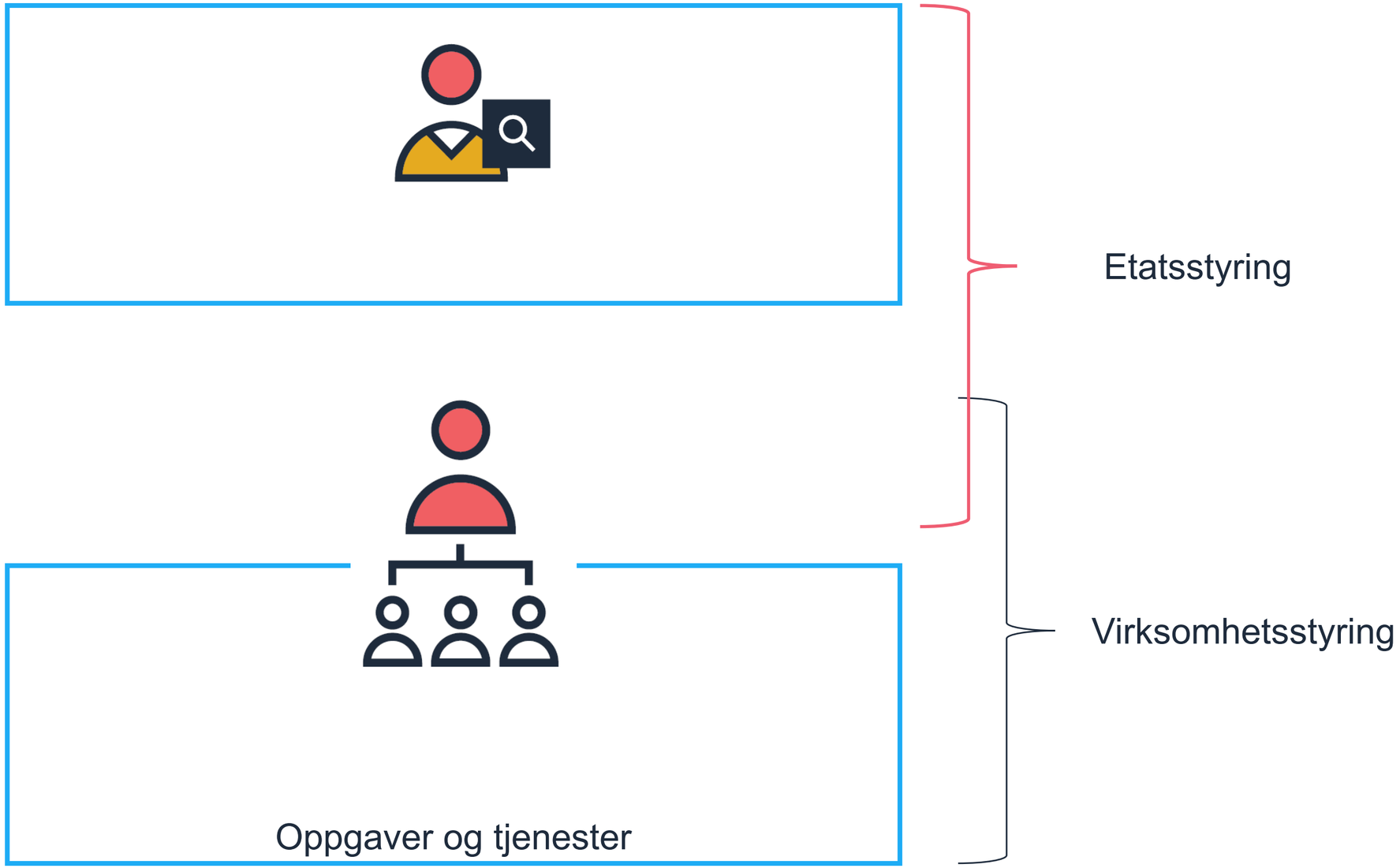


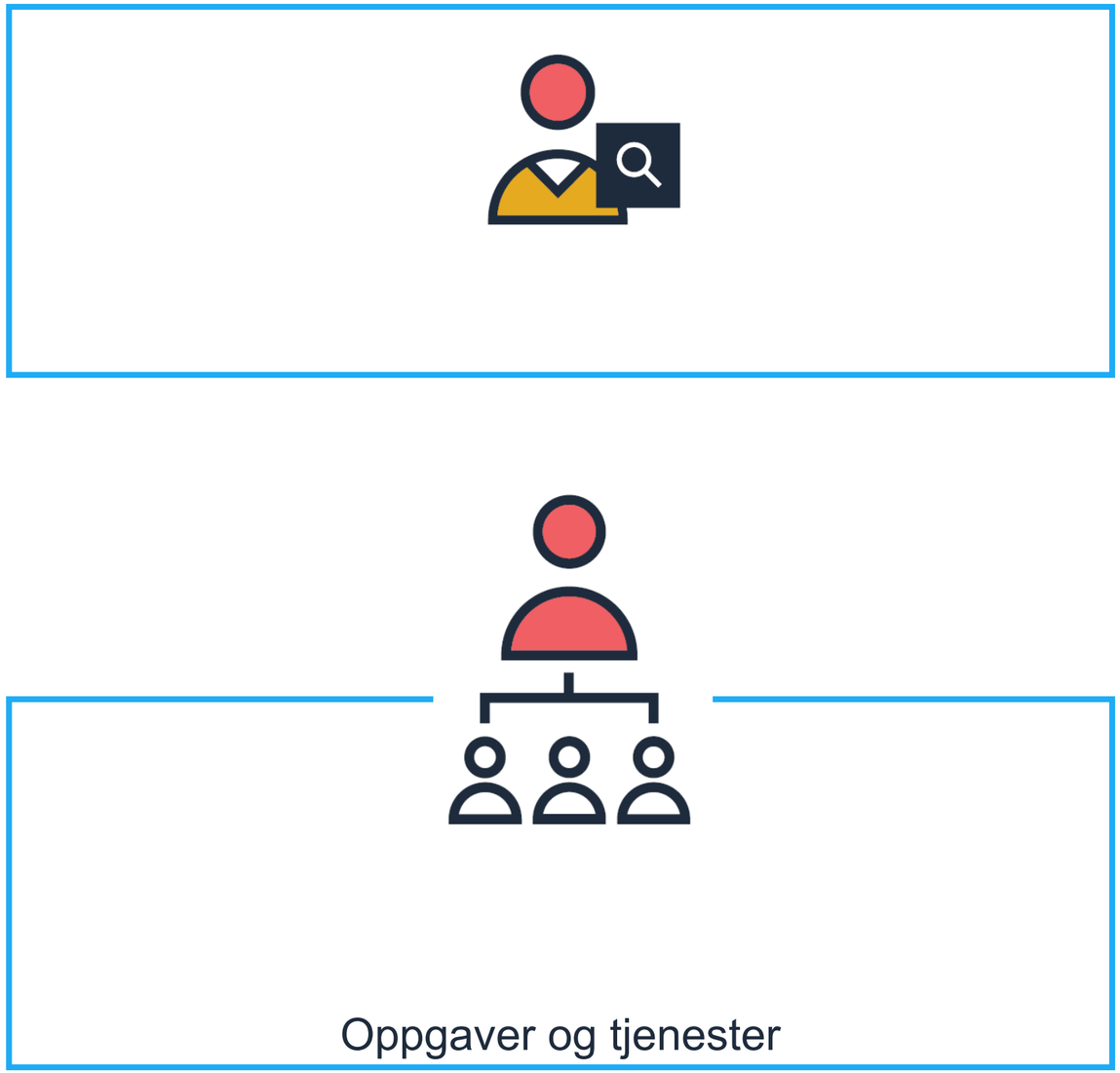
Styringsaktiviteter
- Status
- Modenhet
- Formålseffektivitet
- Kostnadseffektivitet

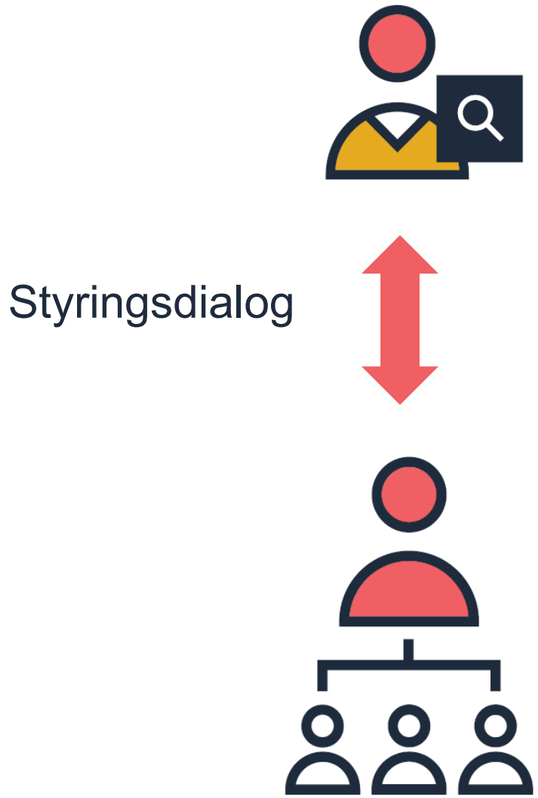
Sikkerhetstiltak
- Status
- Ressursbehov

Problemer?
Områder med høy risiko?
Endringer?

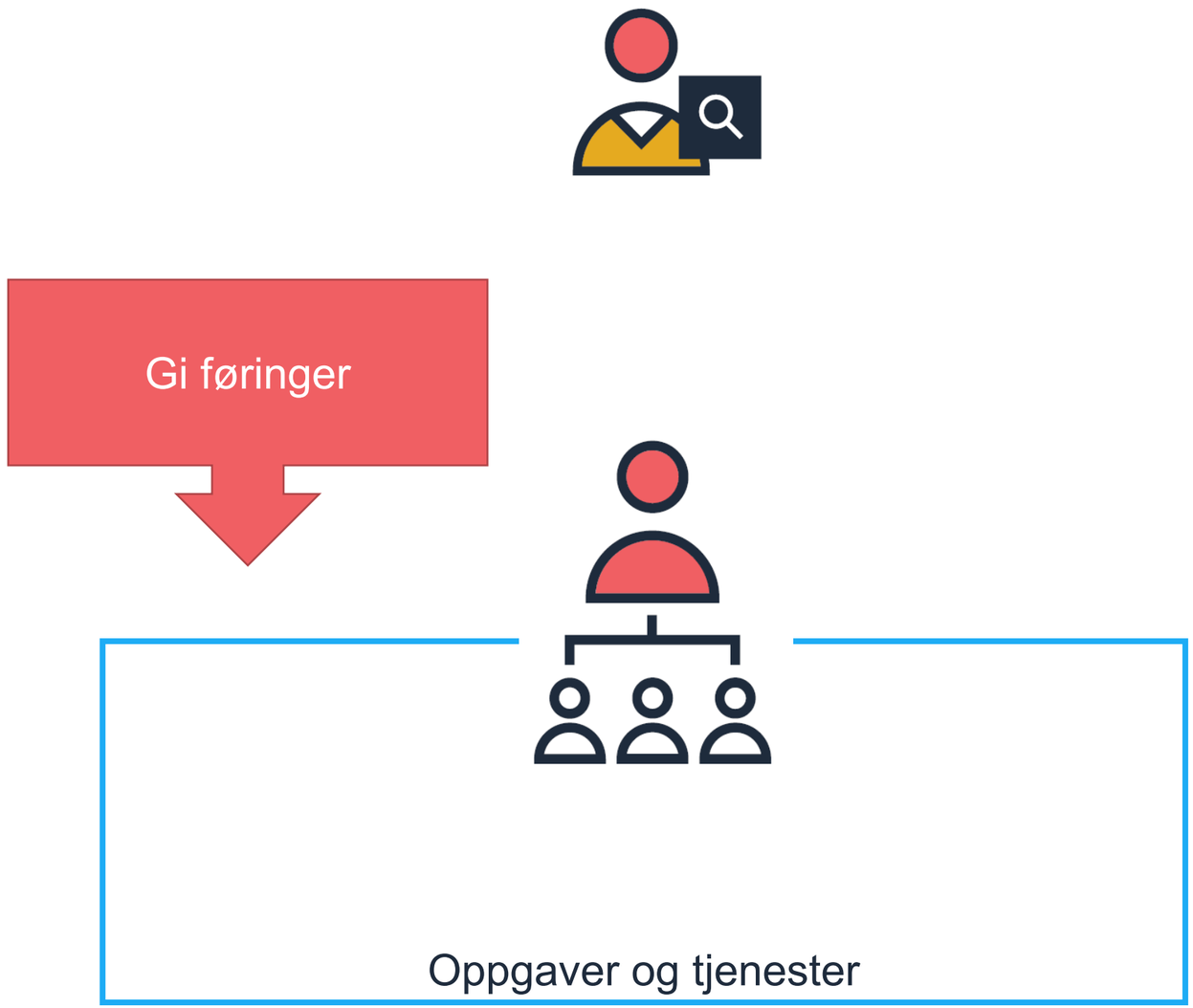

Oppgaver og tjenester
Virksomhetsstyring

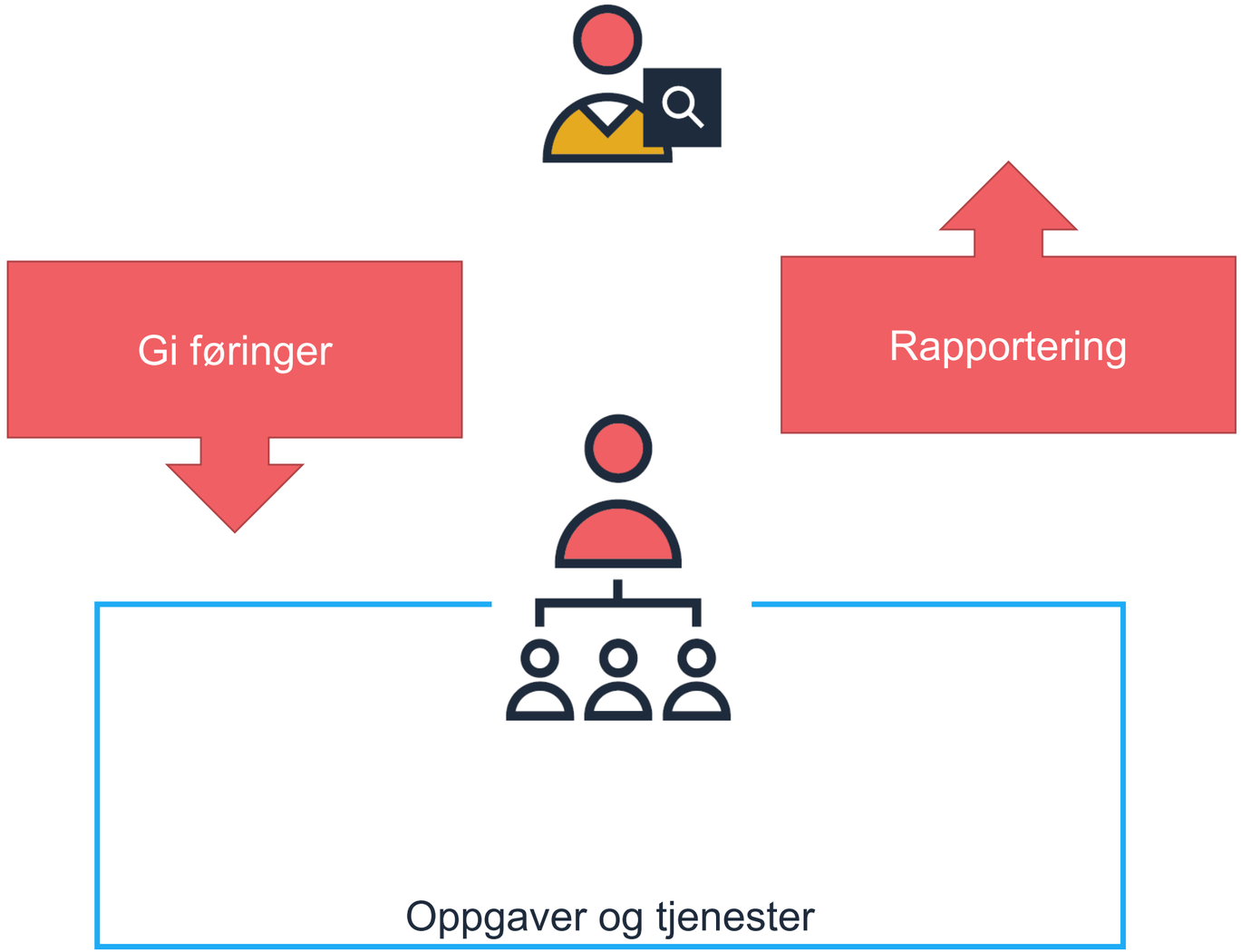

Etatsstyring
Virksomhetsstyring
Oppgaver og tjenester

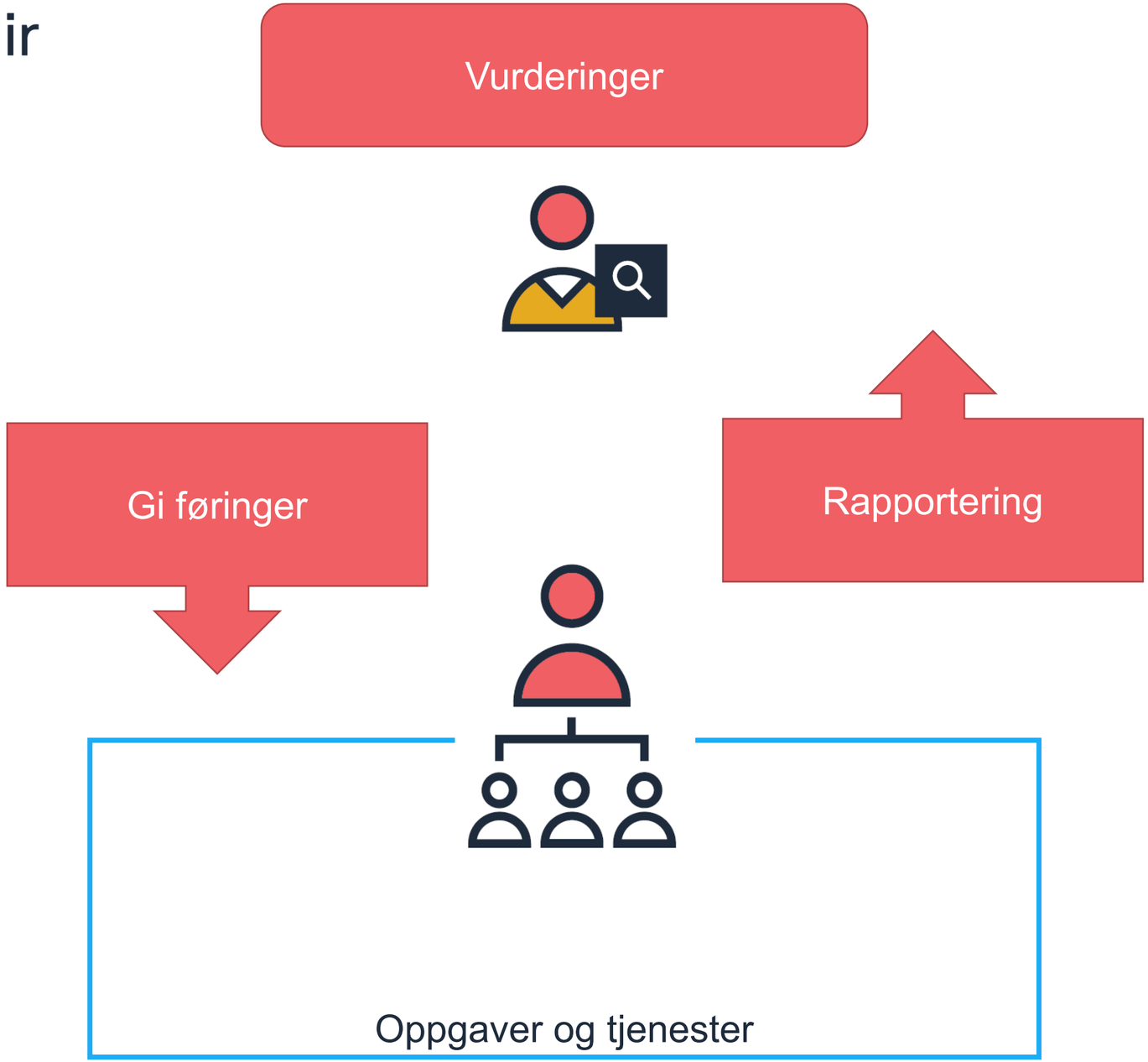

Governance
ISO/IEC 27014
Management
ISO/IEC 27001
Oppgaver og tjenester



Governance


Gi føringer
Oppgaver og tjenester


Gi føringer
Rapportering
Oppgaver og tjenester


Vurderinger
Gi føringer
Rapportering
Oppgaver og tjenester

Digdir

EVALUATE

Vurderinger

Risiko
Vesentlighet
Egenart

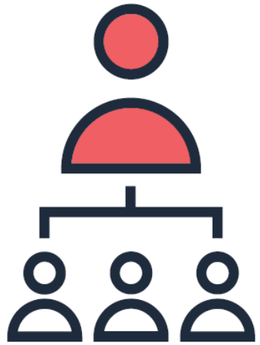
Får de det til?
Hva skal vi dytte på?

DIRECT

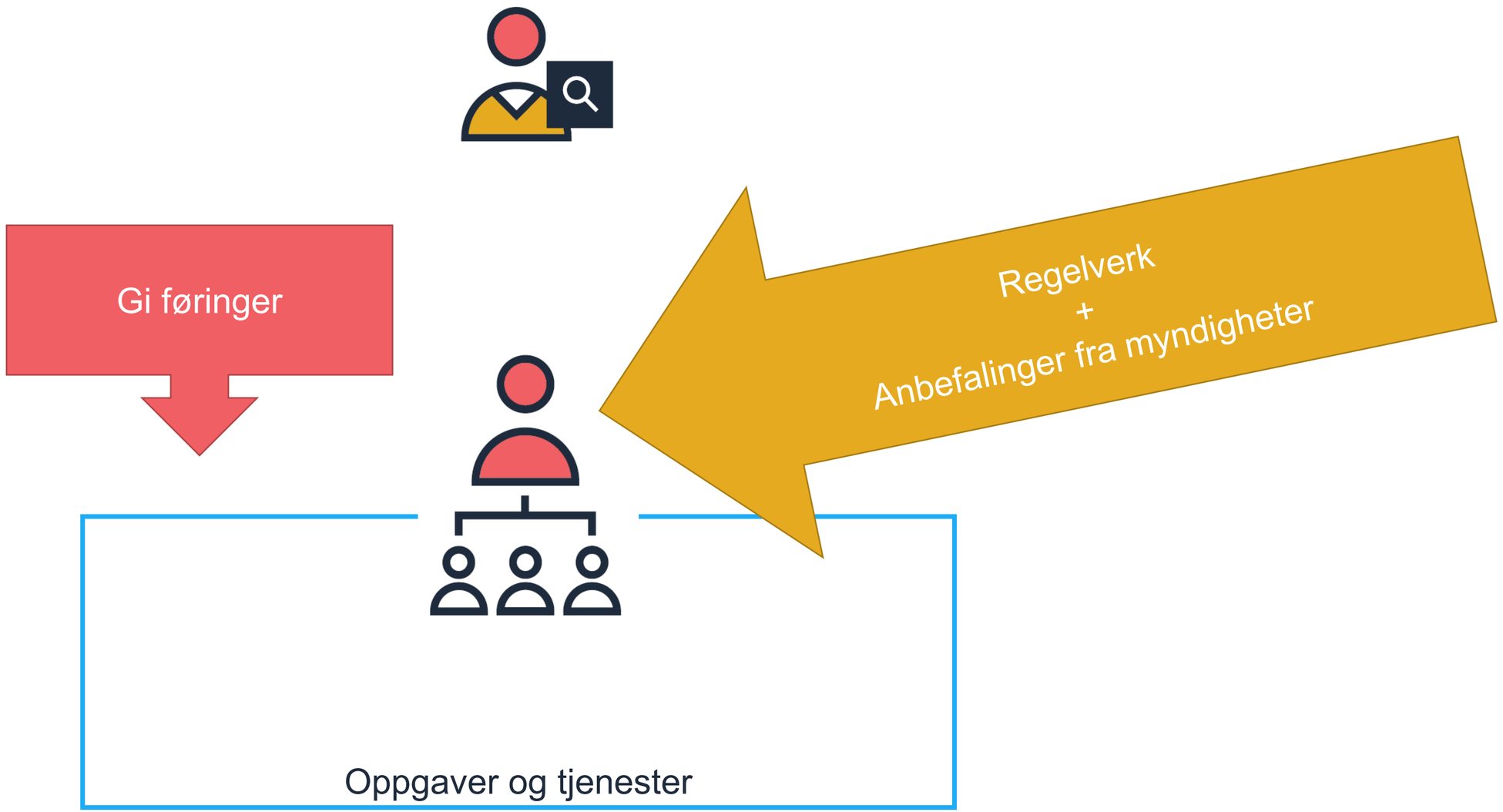
Instruks
Tildelingsbrev

MONITOR

Etatsstyringsmøter
Årsrapport



Oppgaver og tjenester


Gi føringer
Regelverk
+
Anbefalinger fra myndigheter
Oppgaver og tjenester

Digdir

digdir.no

Grunnleggende spørsmål

Risiko
Vesentlighet
Egenart

- Hvilken betydning har oppgavene og tjenestene virksomheten har ansvaret for?
- Hvilken betydning har informasjonsbehandling for disse oppgavene og tjenestene?
  - «Informasjonsbehandling» inkluderer også all bruk av digitale systemer i alle varianter (inkludert styring av vannverk i Østre Toten)
- Hva kan konsekvensene bli ved informasjonssikkerhetsbrudd i oppgaver og tjenester?

- Konsekvenser for virksomheten?
  - Tjenestenivå
  - Økonomi
  - Ansatte
- Konsekvenser for andre?
  - Innbyggere
  - Andre virksomheter
  - Samfunnsfunksjoner
  - Nasjonale sikkerhetsinteresser

Øk-regelverket
Kommuneloven

Arbeidsmiljøloven

Personopplysningsloven m/pvf

Sikkerhetsloven

- Behov for utvikling og innovasjon?
  - Hvilken betydning vil informasjonssikkerhet ha?
- Er rammevilkårene i endring?
  - Strategiske valg
  - Oppgaveportefølje
  - Regelverk
  - Teknologisk utvikling
- Hvilken betydning har digitale tjenester for oppgaveløsningen?
  - Bruk av informasjonsteknologi generelt?

Østre Toten kommune

Beskriver konsekvenser for

- Barnehagene
- Grunnskolen
- Barnevernstjenesten
- Helse- og omsorgstjenester
- Nav-tjenester
- Plan og næring
- Vann og avløp

Det er dette informasjonssikkerhet hovedsakelig handler om for kommuneledelsen

Arbeidet med IKT-sikkerhet er en forutsetning for å sikre forsvarlig pasientbehandling og for å lykkes med økt digitalisering av helsektoren.

Digdir

digdir.no

Hvor detaljert oppfølging?

Hvor dypt inn?

- Departementet bør utøve kontroll på systemnivå. Det betyr for internkontrollen å **påse at det er etablert hensiktsmessig systemer og strukturer for internkontroll** i virksomheten, heller enn å stille konkrete krav til tiltak og kontrollaktiviteter.
- Dere trenger normalt sett ikke kjenne til innholdet i internkontrollsystemet i detalj eller gjøre egne vurderinger av om innholdet er «godt nok». Dere bør heller **basere dere på virksomheten sin egen vurdering** [..]

Klippet fra veiledning om etatsstyring

Dialogverktøy

Når det er behov for å gå mer grundig inn i enkelte deler

HOVEDDEL

- Overordnet om risiko, status og utfordringer
- Styringssystem

Departementet påser at det er etablert god nok internkontroll i virksomheten framfor å undersøke konkrete tiltak og aktiviteter

FORDYPNINGSDEL

- Styringsaktivitetene
- Sikkerhetstiltak
- Etterlevelse av regelverk
- Spesielle temaer


Styringsaktiviteter
• Ledelsens styring og oppfølging
• Risikovurdering
• Risikohåndtering
• Overvåking og hendelseshåndtering
• Måling, evaluering og revisjon
• Kompetanse- og kulturutvikling
• Kommunikasjon
Sikkerhetstiltak
Formål
• Forebygge
• Oppdage
• Håndtere og gjenopprette
Typer
• Organisatoriske
• Menneskelige
• Fysiske
• Teknologiske

Behov for å undersøke sikkerhetstiltak?

- Det er få (som regel ingen) krav til spesifikke sikkerhetstiltak i regelverk
  - på sikkerhetslovens område er det en god del minimumskrav
- Virksomhetene står fritt til å hente tiltak fra ulike tiltaksbanker, eller utforme dem på egenhånd

Sikkerhetstiltak - Tiltaksbanker

NIST

SP 800-53

ISO/IEC

27002

NSM
IKT-sikkerhet

NSM
Fysisk sikkerhet

NSM
Personellsikkerhet

NIST

Cyber Security
Framework

ISF

SoGP

CIS Controls

Dersom et departement går for langt i å gjøre helt egne vurderinger av, og gi føringer for, hvordan risiko burde håndteres, inkludert hvilke tiltak som burde etableres …

… så vil de kunne ende opp med å «overta risikostyringen» i underliggende virksomhet.

Digdir

digdir.no

Veiledning

Veileder

Dialogverktøy

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.

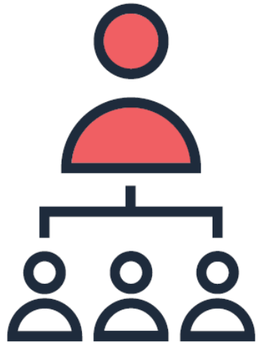
En del av etatsstyringsveiledningen på dfo.no. Dialogverktøy også tilgjengelig som PDF-dokument.

Kan benyttes av alle som har tilsvarende eller liknende forhold

Inspirasjon

Opplæring til personer med styringsansvar

Påse at underliggende virksomhet har tilstrekkelig styring og kontroll



Selvstendig ansvar for styring og kontroll

Digdir

Er det noe du lurer på?

infosikkerhet@digdir.no

Les også blogg-artikkel ☺

Digitaliseringsbloggen

Tonen på toppen – etatsstyring og informasjonssikkerhet

Remi Longva
Seniorrådgiver, Digitaliseringsdirektoratet

Alle er enige om at informasjonssikkerhet er viktig. Like fullt får man ofte inntrykk av at det er vanskelig og vrient å lykkes med. Hva informasjonssikkerhet handler om, kommer litt an på hvem du er, og hvilken rolle du har. Vi skal se litt nærmere på hva styring av informasjonssikkerhet handler om i staten.

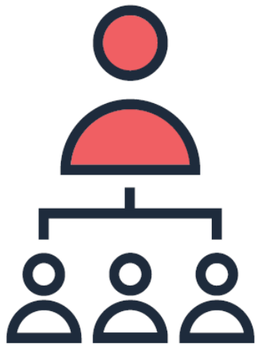
digdir.no

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

Toppleder i virksomheten

- Vet jeg hvilken betydning informasjonssikkerhet har for våre oppgaver og tjenester? For vår måloppnåelse?
- Kan jeg redegjøre for modenhet og effektivitet i styringsaktivitetene?
- Er vi i stand til å forebygge, oppdage og reagere på hendelser?
- Hva er det vi ikke lykkes med, og hva kan jeg gjøre med det?
- Har jeg og mine ledere tilstrekkelig faglig støtte? Og får vi den styringsinformasjonen vi har behov for?
- Er ressursene til arbeidet med informasjonssikkerhet tilstrekkelig?
- Fungerer styring av informasjonssikkerhet godt i sammenheng med den øvrige risikostyringen i virksomheten?



Området er i stor grad regulert av lover og forskrifter som foretakene må forholde seg til i sitt arbeid.

Ut over juridiske virkemidler har departementet valgt å bruke foretaksmøtene [..] til å stille krav om informasjonssikkerheten [..] når dette vurderes å være aktuelt.

Eksempler på eksterne vurderinger

Styringsaktiviteter

- Sertifiseringsrevisjon 27001
  - ISO 19011
  - ISO/IEC 27007

Sikkerhetsstiltak

- Attestasjon av internkontroll hos en tjenesteleverandør
  - ISAE 3402
  - SOC 2 rapport
- Baserer seg på virksomhetens beskrivelse av internkontrollsystem og (sikkerhets)tiltak
- Involverer testing av sikkerhetstiltak