

Kompetansebeskrivelser

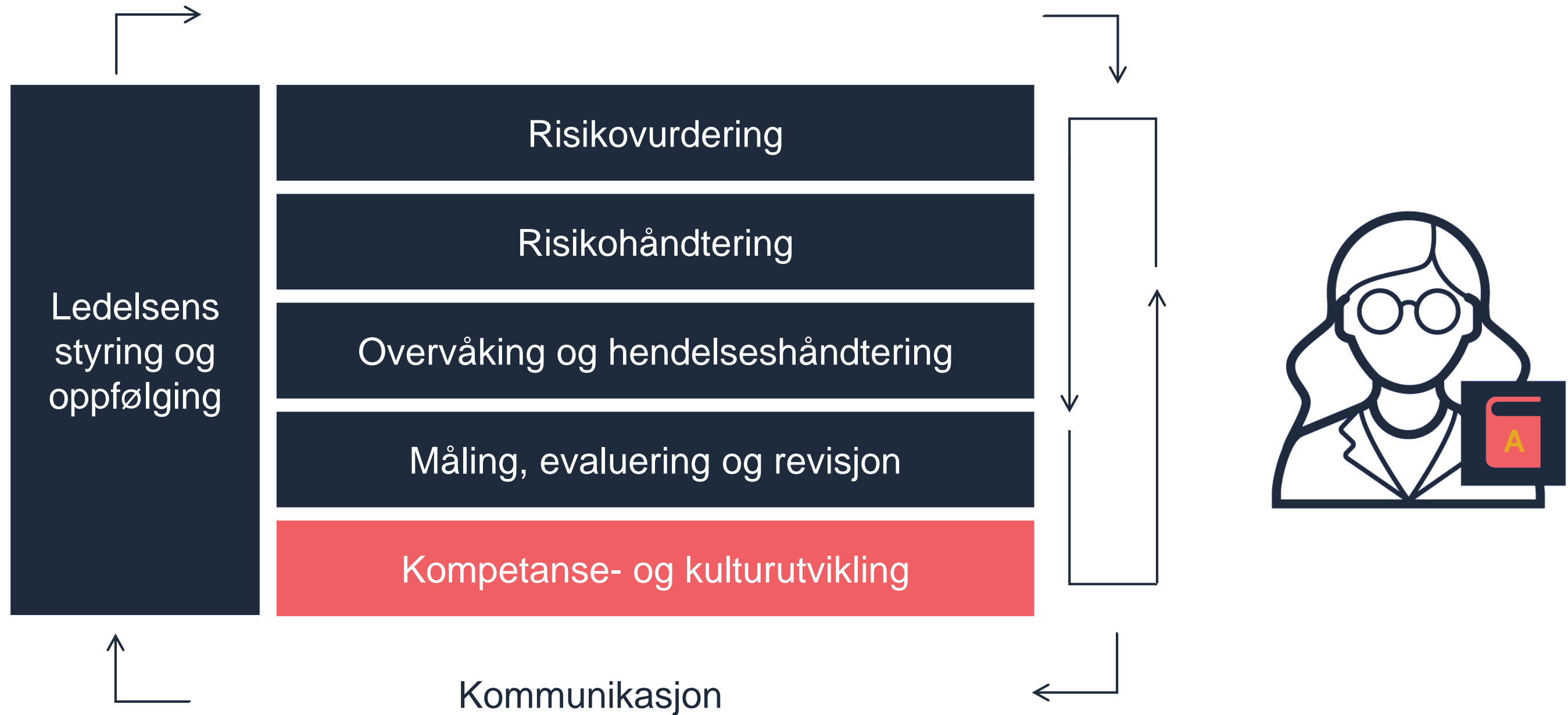
Katrine Aam Svendsen
Seniorrådgiver

Sammen om en sikker digital offentlig sektor – Dag 2
29.10.2020

Internkontroll for informasjonssikkerhet



Kompetanse – en del av internkontrollen



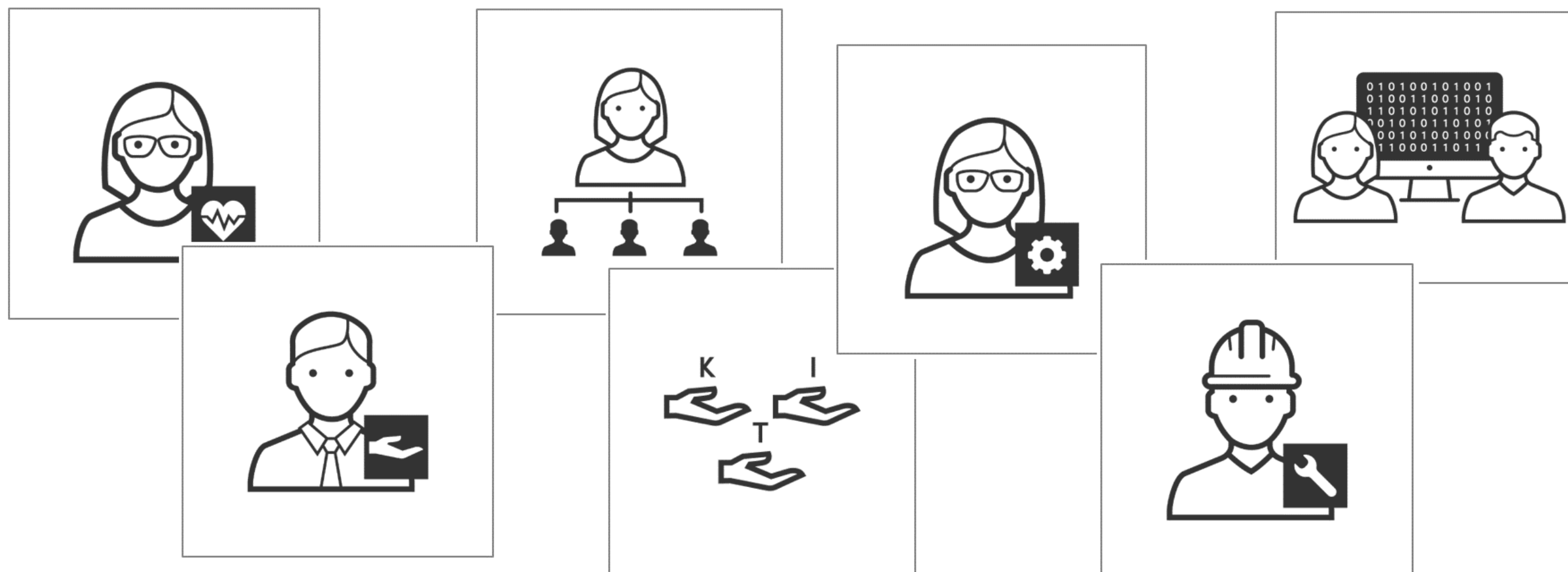
Hva er kompetanse?

”” Kompetanse er de samlede kunnskaper, ferdigheter, evner og holdninger som gjør det mulig å utføre aktuelle oppgaver i tråd med definerte krav og mål

Hva er kompetanse?

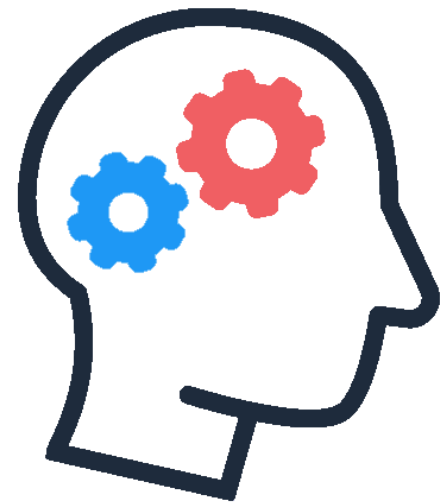
”” Strategisk kompetanseledelse innebærer planlegging, gjennomføring og evaluering av tiltak for å sikre at organisasjonen og den enkelte medarbeider har og bruker nødvendig kompetanse for å nå definerte mål.

Hvor trengs kompetanse?



 Digdir

Behov for kompetanse hos ledere



- For å gi føringer og følge opp
- For å gjøre jobben sin som risikoeiere



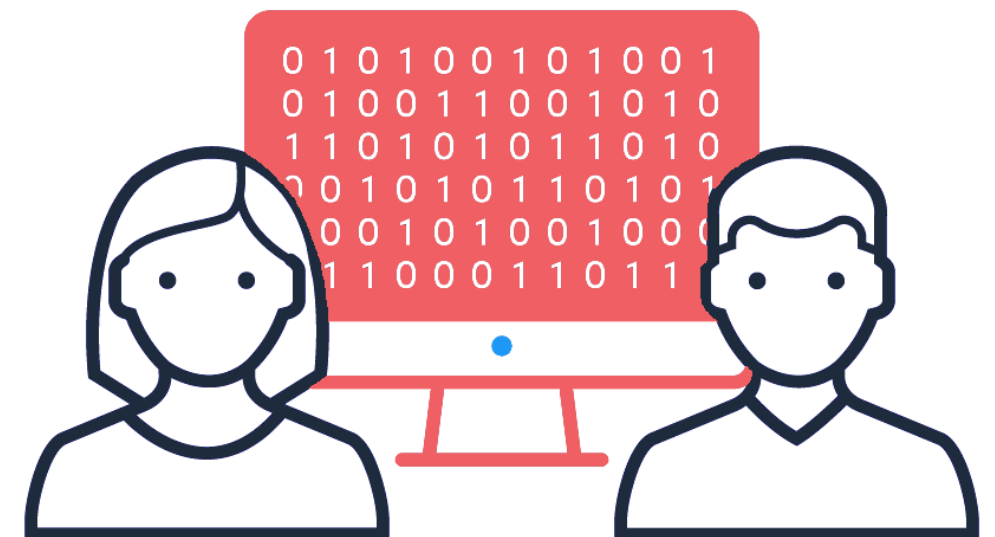
Støtte til ledelsen og virksomheten for øvrig

- Fagansvarlig informasjonssikkerhet
- Rådgiver informasjonssikkerhet
- Informasjonssikkerhet og sammenhengen med virksomhetsstyring
- Kommunikasjon med toppledelse, linjeledelse og IT
- Bistå virksomheten i ulike aktiviteter



Alle ansatte

- Hvilken informasjon behandler jeg?
- Hvilken betydning har informasjonssikkerhet for mine arbeidsoppgaver?
- Hvordan kan jeg gjøre jobben min på en måte som ivaretar behovet for informasjonssikkerhet?



Kompetansebeskrivelser

- Beskriver hvilken kompetanse som er relevant for ulike roller i informasjonssikkerhetsarbeidet

... for å ...

- hjelpe virksomhetene til å få oversikt over hvilken kompetanse de har behov for
- gjøre det lettere å legge en plan for strategisk kompetanseheving i virksomheten

Risikoeier (Linjeleder – operativt ansvarlig)

Ansvar og oppgaver

Alle med mål- og resultatansvar på operativt nivå i virksomheten er ansvarlig for å håndtere den risikoen som er tilstede for de arbeidsoppgavene de er ansvarlige for. Dette innebærer også informasjonssikkerhetsrisiko.

Risikoeiere har ansvar for å ha tilstrekkelig oversikt over sitt ansvarsområde, for å kunne prioritere risikovurderinger slik at arbeidet med risikovurdering og -håndtering gjøres på en effektiv måte. Vedkommende er også ansvarlig for at nødvendige risikovurderinger gjennomføres, at identifiserte risikoer håndteres, blant annet ved at tiltak iverksettes. Beslutninger knyttet til risiko som vedkommende ikke har tilstrekkelig fullmakt til å håndtere, enten fordi risikonivået er for høyt, eller fordi kostnaden av eventuelle tiltak er for høy, må løftes i linjen på samme måte som andre slike avklaringer.



Årlig skal risikoeiere vurdere om de har tilstrekkelig tillit til at informasjonssikkerhetsarbeidet er slik det bør være. De bør vurdere om:

- internkontrolloppgavene^a gjennomføres slik de skal
- de sikkerhetstiltakene de har ansvaret for fungerer slik de skal
 - Det vil si ha tilstrekkelig måling av at sikkerhetstiltak etableres, følges opp og etterleves
- de som jobber for dem følger de lover og regler de skal

Dette kaller vi å vurdere status på sitt ansvarsområde.

Merk: Det er i liten grad hensiktsmessig å stille detaljerte krav til ønsket kompetanse for risikoeier i en stillingsannonse, men det er allikevel viktig å tenke på når man spesifiserer kompetansekravene. Nedenfor beskrives den kompetansen en risikoeier ideelt sett har, men det er viktig å huske at mye av denne kompetansen også kan oppnås ved opplæring etter ansettelse. Her er det like viktig at man i en intervusituasjon sikrer at kandidaten har den rette forståelsen av risiko og sammenhengen mellom informasjonssikkerhet og måloppnåelse.

Ønsket kompetanse

Alle med mål- og resultatansvar på operativt nivå i virksomheten bør ha grunnleggende kunnskap om informasjonssikkerhet, og hvordan risiko på informasjonssikkerhetsområdet kan påvirke deres måloppnåelse.

Risikoeiere må ha tilstrekkelig kompetanse til å holde oversikt over sitt ansvarsområde – hvilke arbeidsoppgaver utføres, hvilke informasjonstyper behandles, hvilke systemer benyttes, hva er potensielle konsekvenser dersom noe inntreffer etc. Dette gjelder både på informasjonssikkerhetsområdet og andre områder.

^a <https://internkontroll-infosikkerhet.difi.no/>

Basert på en slik oversikt må risikoeier kunne prioritere hvor det er viktigst å gjennomføre grundige risikovurderinger, og vedkommende må kunne drive prosessen med å foreslå håndtering av risikoer, godkjenne forslag av disse (eller løfte dette i linjen), og iverksette de nødvendige tiltakene.

Risikoeiere må kjenne til den metoden som virksomheten har valgt for gjennomføring av risikovurderinger.

Dersom risikoeier ikke selv har spisskompetanse på fagområdet informasjonssikkerhet, må vedkommende imidlertid ha tilstrekkelig kompetanse til å få bistand på området. Fagansvarlig informasjonssikkerhet - eventuelt rådgiver informasjonssikkerhet – kan bistå i risikovurderinger og håndtering av risiko.

Tema for intervju/medarbeidersamtale

Merk: Det vil variere hvor viktig god forståelse av og evne til å lede arbeid med informasjonssikkerhet er, alt etter hva en person skal ha ansvaret for. Det er viktig å gjøre en vurdering av dette i forkant av en samtale. I tilfeller der det er viktig med fokus på å sikre informasjonen i arbeidsoppgavene vedkommende skal være ansvarlig for, kan man legge vekt på noen av aspektene nedenfor. Dette må tilpasses den gitte situasjonen.

Forståelse for at arbeidet med informasjonssikkerhet understøtter virksomhetens måloppnåelse.

Forståelse for viktigheten av å innarbeide informasjonssikkerhet i virksomhetens helhetlige risikostyring.

Forståelse for at vedkommende har ansvar for at sine medarbeidere har tilstrekkelig forståelse for og kunnskap om informasjonssikkerhet til å gjøre sine arbeidsoppgaver på en god måte.

- Har dere beskrivelser av ansvar og/eller behov for kompetanse på informasjonssikkerhet på ulike nivåer eller roller i virksomheten?
 - Ja
 - I noen grad
 - Nei
 - Vet ikke

[Digdir.no/infosikkerhet](https://digdir.no/infosikkerhet)

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