Digdir

# Delprosjekt - Kompetanse

Zoya Shah
Seniorrådgiver
18.11.2020

digdir.no

# Difi – rapport 2018:4

# Difi-rapport 2018:4

> Samlet sett er vårt inntrykk at virksomhetene arbeider med kompetanseheving på området informasjonssikkerhet, men at arbeidet hos mange er lite målrettet og tilpasset. Det er behov for bedre forståelse for hvilken fagkompetanse som kreves for å løse virksomhetens oppgaver innen fagområdet informasjonssikkerhet.
>
> *Anbefaling 10: Virksomhetene bør vurdere å etablere en plan for kompetanseutvikling på området informasjonssikkerhet.*

Difi rapport 2018:4: https://www.difi.no/rapport/2018/06/arbeidet-med-informasjonssikkerhet-i-statsforvaltningen

# Digital sikkerhetskompetanse

> Digital sikkerhetskompetanse er en viktig forutsetning for at Norge skal lykkes med digitalisering.

# Prosjektleveranser

Difi
Direktoratet for forvaltning og ikt

# Kompetansebeskrivelser

Ansvar, oppgaver og ønsket kompetanse for roller knyttet til styring og kontroll av informasjonssikkerh

Difi
Direktoratet for forvaltning og ikt

## Fagansvarlig informasjonssikkerhet

### Ansvar og oppgaver

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

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.

irksomhetsledelsen
sens styring og

være en
ternkontrollarbeid
t ved å bistå i
g måling,
svaret for å
tgjøringsaktiviteter

KT-teknisk rolle. Den krever imidlertid god forst

Difi
Direktoratet for forvaltning og ikt

## Rådgiver informasjonssikkerhet

### Ansvar og oppgaver

I denne forbindelsen mener vi personer som er støtteressurser i fagansvarlig informasjonssikkerhets arbeide i organisasjonen. Dette trenger ikke være fulltidsressurser.

Hovedansvaret til vedkommende er å støtte fagansvarlig i det arbeidet vedkommende gjør – bistå i tilknytning til ledelsens styring og oppfølging, gi råd og delta som informasjonssikkerhetsressurs i prosjekter og oppgaver i virksomheten, bistå i gjennomføring av risikovurderinger og -håndtering, planlegge og gjennomføre opplæring

Ansvar og
virksomhe

### Ønsket kompetanse

Kompetansebehovet for en støtteressurs i
arbeidsoppgaver vedkommende har.

Ofte vil det være hensiktsmessig at en slik
fagansvarlig, men vedkommende kan ha m

Avhengig av virksomhetens evne og muligh
liten erfaring ha denne rollen. Det er da vik
risikostyring og internkontroll, og at de gje
fagområdene.

I noen virksomheter vil støtteressursene a
hensiktsmessig om de har mer spisskompe
risikovurderinger/-håndtering, revisjon, he

### Tema for intervju/medarbeidersamtale

Når man skal vurdere kompetansen til pers
er det viktig at man tar utgangspunkt i hva
kompetanse som er vesentlig. Noen aspek

Forståelse for at informasjonssikkerhet ha
tilgjengelighet, og at det handler om mye r
sikkerhetsloven.

Forståelse for at risikobildet er i stadig end

Forståelse av de aktivitetene vedkommend
informasjonssikkerhet understøtter virkso

Forståelse for at informasjonssikkerhet er
formidle dette til de ansatte.

Difi
Direktoratet for forvaltning og ikt

## Systemeier

### Ansvar og oppgaver

Med systemeier mener vi i denne forbindelsen ansatte som har et særskilt ansvar for et gitt IKT-system. Dette kan variere fra en virksomhet til en annen.

Systemeiere vil ha ansvaret for risiko knyttet til systemet de er ansvarlige for, og vil derfor også være risikoeiere. De har derfor også ansvar og oppgaver som beskrevet under «Risikoeier». Dersom et system benyttes i kun én arbeidsoppgave/prosess, bør vurdering og håndtering av risiko for arbeidsoppgaven og systemet sees i sammenheng.

Noen systemeiere er imidlertid ansvarlig for systemer som også benyttes av andre risikoeiere – vi kaller dem systemeier fellessystem. I slike tilfeller er det systemeiers ansvar å ivareta interessene til de som benytter systemene i sin oppgaveløsning og tjenesteutføring. Systemeierne må derfor involvere risikoeierne i risikovurderingsarbeid og andre internkontrollaktiviteter som utføres på fellessystemene.

### Ønsket kompetanse

Systemeiere bør ha grunnleggende kunnskap om informasjonssikkerhet, og hvordan sikkerhetshendelser kan påvirke systemet de er ansvarlig for.

Systemeier bør ha grunnleggende kunnskap arbeidsoppgaven(e)/prosessen(e) systemet inngår i.

Systemeier fellessystemer bør ha evnen til å kommunisere og koordinere med ulike risikoeiere, og vurdere deres behov. De bør kunne inkludere dem i gjennomføring av risikovurdering og -håndtering, og hensynta deres vurdering av hvilke konsekvenser som kan oppstå dersom ulike hendelser inntreffer.

### Tema for intervju/medarbeidersamtale

Systemeier må ha forståelse for at man må se sammenhengen mellom system og arbeidsoppgave når man gjennomfører risikovurderinger. Det er ikke tilstrekkelig å gjøre en teknisk risikovurdering av systemet, det må også sees i sammenheng med hvordan arbeidsoppgaven(e) gjennomføres.

Systemeier fellessystem må ha forståelse for at det er de ulike risikoeierne som best kan si hvilke konsekvenser ulike hendelser kan få for virksomhetens måloppnåelse. Disse må derfor involveres i gjennomføringen av risikovurderinger.



Difi
Direktoratet for forvaltning og ikt

## 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

asjonssikkerhetsarbeidet er slik

e skal
iltak etableres, følges opp og

Difi
Direktoratet for forvaltning og ikt

## Toppleder

### Ansvar og oppgaver

Toppleder er ansvarlig for at virksomheten har velfungerende styring og kontroll. Dette innebærer at arbeidet med informasjonssikkerhet gjennom
måte rundt om i hele virksomheten, tilpasset

Toppleder, med sin ledergruppe, må gi føring
informasjonssikkerhetsområdet skal være: h
være ansvarlig, beskrivelse av nivåer for kons
etc. Føringer forankrer ledelsens ansvar.

Topplede
aktivitete
informasj

I det dagl
sette «to
vurdere o
akseptere

Topplede
gjennomg
tilstrekke
virksomhe

### Ønsket kompetanse

Toppleder må forstå at det er ledelsens ansv
virksomheten er hensiktsmessig, og at ledels

Det er nødvendig med tilstrekkelig kunnskap
informasjonssikkerhet i den helhetlige virkso

Toppleder bør ha forståelse for at styring av
fra annen virksomhetsstyring og internkontro
ligger det også å forstå at styringssystem/inte
aktiviteter, ikke en samling dokumenter.

Toppleder eier risikoen for at virksomheten i
arbeidet med styring og kontroll av informas
Effektiv risikostyring er viktig. Noe risiko må
definerte kriterier for å akseptere risiko, mer

Toppleder må også forstå hvordan informasj
informasjonsbehandlingen som gjennomføre
mål. For å forstå dette, må vedkommende og
om å sikre både konfidensialitet, integritet o
mer enn personopplysninger og beskyttelse
Informasjonssikkerhetsbrudd kan få konsekv
kan få konsekvenser for innbyggere, andre vi

I tillegg er det viktig med forståelse for at risi
for eksempel dersom man velger å tjenesteu

Difi
Direktoratet for forvaltning og ikt

## Øvrig ledergruppe

### Ansvar og oppgaver

***Toppledergruppen*** bør ha forståelse for at de må være involvert i føringer for hvordan internkontrollen på informasjonssikkerhetsområdet skal være: hvilke aktiviteter som s gjennomføres, hvem som skal være ansvarlig, beskrivelse av nivåe konsekvens og sannsynlighet, kriterier for å akseptere risiko etc.

***Ledere på alle nivåer*** er ansvarlig for å følge opp arbeidet med informasjonssikkerhet på sine ansvarsområder, på samme måte som de følger opp annet arbeid er ansvarlige for.

I tillegg er de ansvarlig for at det blir gjennomført tilstrekkelige risikovurderinger og håndtering a risiko på sine ansvarsområder.

På samme måte som risikoeiere må også ledere på alle nivå minst en gang årlig systematisk vurd status på informasjonssikkerhetsarbeidet innenfor sine ansvarsområder. De har også ansvar for a deres medarbeidere har tilstrekkelig kompetanse innen informasjonssikkerhet til å utføre sine oppgaver på en god måte.

### Ønsket kompetanse

På samme måte som toppleder bør øvrig ledergruppe ha grunnleggende kunnskap om hva informasjonssikkerhet er, hva internkontroll handler om, og hva som er sammenhengen mellom to. De må vite hva som er ledelsens ansvar, kjenne til hvilke aktiviteter som skal gjennomføres, o hvem som har ansvaret for de ulike aktivitetene.

Alle ledere må også forstå hvordan informasjonssikkerhet, gjennom å understøtte den informasjonsbehandlingen som gjennomføres i virksomheten, bidrar til at virksomheten når sine mål. For å forstå dette, må vedkommende også ha forståelse for at informasjonssikkerhet handle om å sikre både konfidensialitet, integritet og tilgjengelighet på informasjonen, og at det gjelder mer enn personopplysninger og beskyttelse i henhold til sikkerhetsloven.
Informasjonssikkerhetsbrudd kan få konsekvenser får virksomhetens økonomi og tjenestenivå. D kan få konsekvenser for innbyggere, andre virksomheter og samfunnet.

Det er nyttig med forståelse for at styring av informasjonssikkerhetsarbeidet ikke skiller seg vese fra annen virksomhetsstyring og internkontroll på andre områder (f.eks. HMS og personvern). I d ligger det også å forstå at styringssystem/internkontroll (generelt) er et sett av systematiske aktiviteter, ikke en samling dokumenter.

Alle ledere må også ha forståelse for at de er ansvarlig for å akseptere risiko på noen nivåer, base på definerte kriterier for å akseptere risiko, mens annen risiko enten må helt opp til toppleder, e kan aksepteres på operativt nivå.

De må også forstå at risikobildet endrer seg når man tar ulike strategiske valg, for eksempel ders man velger å tjenesteutsette oppgaver, eller ta i bruk skytjenester.

### Tema for intervju/medarbeidersamtale

Det vil variere mye hvor naturlig det er å snakke om informasjonssikkerhet i en intervjusituasjon eller en medarbeidersamtale, avhengig av hva slags lederstilling det er snakk om. Det kan imidle være nyttig å snakke med kandidaten om hvilken informasjon som behandles i arbeidsoppgaven vedkommende skal ha ansvar for, hvordan vedkommende ser på informasjonssikkerhet og anne internkontroll, og vedkommendes tanker om punktene under «ønsket kompetanse».



Difi
Direktoratet for forvaltning og ikt

## IT-leder e.l.

### Ansvar og oppgaver

IT-leder har mange oppgaver relatert til informasjonssikkerhet. Vedkommende vil være ansvarlig for flere tekniske sikkerhetstiltak (tiltaksleverandør), og er ansvarlig for å sørge for IT-faglig kompetanse inn i vurdering og håndtering av risiko[9]. I tillegg er det ofte IT-avdelingen som er ansvarlig for overvåking og hendelseshåndtering, og IT-leder vil derfor være ansvarlig for å styre denne aktiviteten.

IT-leder vil også være risikoeier for de arbeidsoppgavene som vedkommende er ansvarlig for.

### Ønsket kompetanse

Avhengig av hva slags IT-miljø virksomheten har, må IT-leder ha god kunnskap om løsningene de benytter, og hvilke trusler og sårbarheter som kan påvirke virksomhetens risikobilde. Vedkommende bør også ha god kunnskap om hvilke tiltak som kan gjennomføres for å redusere risiko, og kunne gi en beskrivelse av et kost/nytte perspektiv.

IT-leder må også kjenne organisasjonen, og ha evnen til å formulere IKT-tekniske problemstillinger på en forståelig måte til ledelse og øvrige i organisasjonen, gjerne i samarbeid med fagansvarlig informasjonssikkerhet.

IT-leder må ha kompetanse til å forklare toppleder og øvrig ledergruppe hvordan ulike valg kan påvirke risikobildet. Eksempler kan være dersom man vurderer tjenesteutsetting, eller vurderer å ta i bruk skytjenester.

### Tema for intervju/medarbeidersamtale

Forståelse for forholdet mellom tiltaksleverandør og virksomhetens risikoeiere. En tiltaksleverandør er ansvarlig for visse sikkerhetstiltak risikoeiere har behov for. Dette vil normalt inkludere utforming, iverksetting og vedlikehold av sikkerhetstiltakene.

Difi
Direktoratet for forvaltning og ikt

## Alle ansatte

### Ansvar og oppgaver

Alle ansatte har et ansvar for å bidra til at virksomheten når sine samlede mål på en best mulig måte. De skal ha et bevisst forhold til målene for eget arbeid, hvilken informasjon de behandler, og hvilke krav som stilles til arbeidet deres. Dette gjelder også for fagområdet informasjonssikkerhet.

### Ønsket kompetanse

Alle ansatte bør ha kunnskap om hvilken betydning informasjonssikkerhet har for sine arbeidsoppgaver, og hvordan de kan utføre arbeidet sitt på en måte som ivaretar behovet for informasjonssikkerhet. De bør blant annet ha tilstrekkelig forståelse for trusler og risiko til at de utfører arbeidsoppgavene på en sikker måte.

De må også ha forståelse for hvordan uønskede hendelser kan hindre dem i å få gjort jobben sin slik de skal, eller få konsekvenser for andre parter.

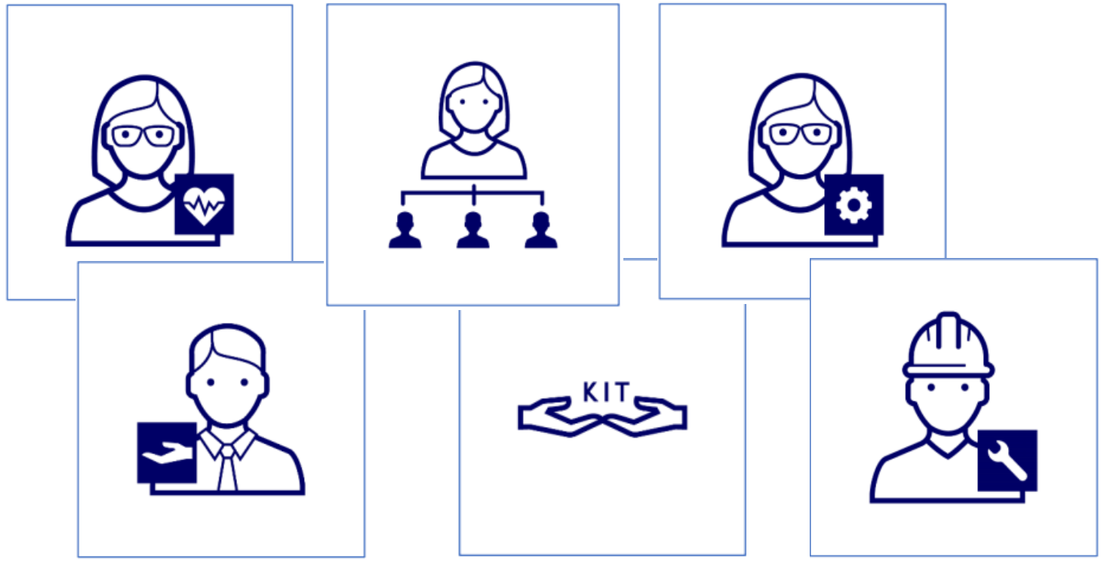
Alle ansatte må også kjenne til virksomhetens interne rutiner for varsling av informasjonssikkerhetshendelser.

### Tema for intervju/medarbeidersamtale

Det vil variere mye hvor naturlig det er å snakke om informasjonssikkerhet i en intervjusituasjon eller en medarbeidersamtale, avhengig av hva slags stilling det er snakk om. Det kan imidlertid være nyttig å snakke med kandidaten om hva arbeidsoppgaven innebærer, og hvordan vedkommende reflekterer med tanke på hvilken informasjon som behandles, og hvordan dette kan påvirke enhetens måloppnåelse.

# Roller

- Fagansvarlig informasjonssikkerhet
- Rådgiver informasjonssikkerhet
- Risikoeier (operativt ansvarlig)
- Toppleder
- Øvrig ledergruppe
- IT-leder
- Systemeier
- Alle ansatte




https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet/veiledere/kompetansebeskrivelser-styring-og-kontroll-av-informasjonssikkerhet

# Formål med kompetansebeskrivelsene

- Beskrive 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

# Kompetansebeskrivelser - innhold

- Ansvar og oppgaver
- Ønsket kompetanse
- Tema til intervju/medarbeidersamtale

# Hvorfor det er viktig med riktig kompetanse

# Deks - Direktoratet for eksempler

Medarbeider - Siri

Leder - Ulla

HR – Kari

# Toppleder

Leder - Ulla

## Agenda – Ledermøte

1. Godkjenne forrige møtereferat
2. Risikovurdering
3. Kommunikasjonsplan
4. Ansettelse – Fagansvarlig informasjonssikkerhet

# Ansette – fagansvarlig informasjonssikkerhet

HR – Kari

## 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

- innholdet i og oppfølging av internkontrollsystem/styringssystem
- risikovurderinger og kommunikasjon av risiko
- sammenheng med andre internkontrollområder, slik som virksomhetsstyring generelt, HMS og sikkerhetsstyring etter sikkerhetsloven
- virksomhetens mål, organisering og arbeidsmåter
- virksomhetens leverandørkjeder og avhengigheter til andre aktører
- digital sikkerhet/informasjonssikkerhet/samfunnssikkerhet

Fagansvarlig informasjonssikkerhet skal bistå slik at kommunikasjonen mellom toppledelsen, øvrig linjeledelse, og teknisk personell (f.eks. IT) fungerer på en effektiv måte. Dette innebærer å ha evnen til å «oversette» informasjonen fra teknisk personell slik at ledelsen kan forstå den, og omvendt.

Fagansvarlig bør ha kompetanse til å bistå hele linjen i risikovurderinger, og støtte dem ved håndtering av risiko. Det er ønskelig med kompetanse i å formidle kunnskap videre, slik at den enkelte risikoeier på sikt blir mer og mer selvgående i sine oppgaver.

# Kompetanseheving av alle ansatte

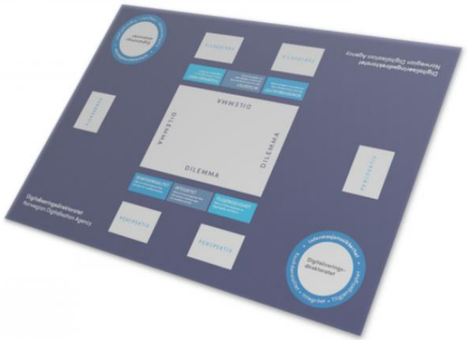
Medarbeider - Siri

Alle ansatte har et ansvar for å bidra til at virksomheten når sine samlede mål på best mulig måte.

De skal ha et bevisst forhold til målene for eget arbeid, hvilken informasjons de behandler og hvilke krav som stilles til arbeidet deres.

Dette gjelder også for fagområdet informasjonssikkerhet.

Dilemmatrening - informasjonssikkerhet



Digdir

digdir.no

# Lykke til med kompetanseheving i din virksomhet