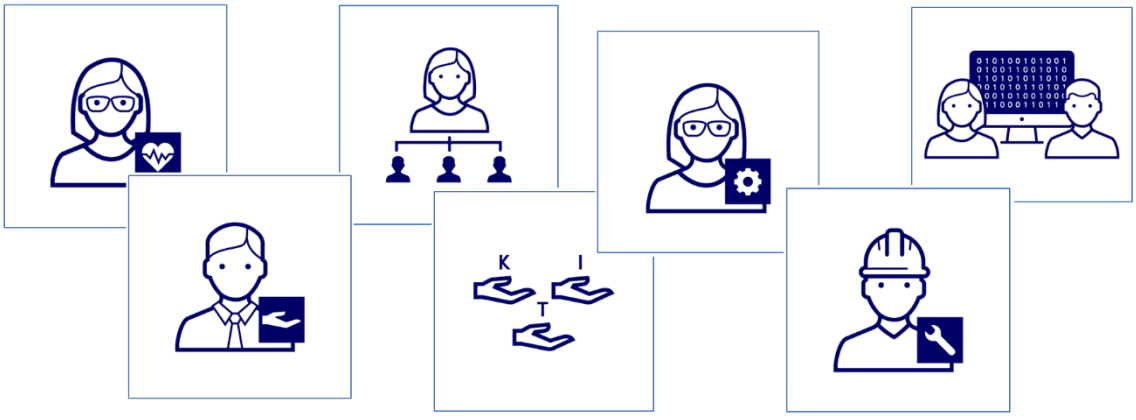
Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

Kompetansebeskrivelser

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



Innhold

Omfang og avgrensninger

Vi avgrenser denne veiledningen til å gjelde roller knyttet til styring og kontroll (internkontroll) på informasjonssikkerhetsområdet, internt i en virksomhet[1].

Tekniske (IKT-nære) roller, for eksempel systemforvalter, utvikler, etc., har vi ikke beskrevet her. Det er imidlertid viktig at virksomheten også har et bilde av hvilken sikkerhetskompetanse disse rollene har behov for, og arbeider for å videreutvikle denne kompetansen.

Vi beskriver heller ikke her hvordan en sikkerhetsorganisasjon bør bygges opp og være organisert. Dette kan løses på mange måter, avhengig av virksomhetens egenart, kultur og størrelse.

> **Merk!** Dette er ingen fasit! Hver virksomhet må til enhver tid kartlegge sine egne kompetansebehov når det skal ansettes nye ressurser, eller når man arbeider med kompetanseutvikling. Beskrivelsene nedenfor kan imidlertid brukes som et utgangspunkt når stillinger skal lyses ut, man skal gjennomføre intervjuer, eller for å kartlegge behov for kompetanseutvikling.

Målgruppe

Kompetansebeskrivelsene skal kunne benyttes av ulike ressurser i virksomheten når nye personer skal ansettes, eller man skal kartlegge om man har tilstrekkelig og ønsket kompetanse i virksomheten. Dette kan være virksomhetsledelsen, fagansvarlig informasjonssikkerhet, ledere i ulike posisjoner etc.

Kompetansebeskrivelsene skal kunne inngå i den veiledning og støtte personalavdelingen i offentlige virksomheter gir ledelse og ansettelsesråd i ansettelsesprosesser.

Om kompetansebeskrivelsene

Her beskriver vi hvilket ansvar, arbeidsoppgaver og kompetansebehov som kan inngå i ulike roller innen styring og kontroll av informasjonssikkerhet. Ansvaret som er lagt til de ulike rollene tar utgangspunkt i beskrivelsen av rollene i eksempelet på «Retningslinje: Roller og ansvar i internkontroll- og sikkerhetsarbeidet»[2] fra Internkontroll i praksis – informasjonssikkerhet[3].

Vær oppmerksom på at det er den enkelte virksomhet som avgjør hvilke oppgaver som er knyttet til de forskjellige rollene, og dette vil medføre at kompetansebehovet til den enkelte rollen vil kunne variere fra virksomhet til virksomhet.

Kompetansebeskrivelsene, med unntak av beskrivelsen for rollen som toppleder, er strukturert på følgende måte:

- **Ansvar og oppgaver:** Denne delen beskriver hvilket ansvar og hvilke arbeidsoppgaver som kan ligge til rollen.
- **Ønsket kompetanse:** Basert på ansvaret beskrevet over, beskrives her hvilken kompetanse vedkommende bør ha for å utføre disse oppgavene.

[1] Med «virksomheter» menes her statlige og kommunale virksomheter, herunder departementer.
[2] https://internkontroll-infosikkerhet.difi.no/sites/sikkerhet/files/06-01-05_eksempel_retningslinje_roller_og_ansvar_i_internkontroll-_og_sikkerhetsarbeidet.docx
[3] «Internkontroll i praksis – Informasjonssikkerhet» beskriver hvordan virksomheter kan etablere og vedlikeholde systematisk internkontroll på informasjonssikkerhetsområdet. Se https://internkontroll-infosikkerhet.difi.no/

- **Tema til intervju/medarbeidersamtale:** Basert på ansvaret og den ønskede kompetansen beskrevet – her formuleres aspekter man kan ha fokus på når man intervjuer nye kandidater, eller vurderer kompetansen til ansatte i virksomheten.

Følgende roller er beskrevet her:

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

Ulike virksomheter kan ha ulike navn på rollene. Fagansvarlig informasjonssikkerhet tilsvarer for eksempel ofte informasjonssikkerhetsansvarlig, informasjonssikkerhetsleder eller CISO. Risikoeier kan være prosesseiere, i tillegg til linjeledere og andre med ansvar for mål og resultater. En stilling kan inneholde mer enn én rolle – informasjonssikkerhetsleder (CISO) vil for eksempel ofte være både fagansvarlig informasjonssikkerhet og en del av ledergruppen.

Formell kompetanse, kurs og sertifiseringer

Vi har i liten grad beskrevet hvilken formell kompetanse de ansatte i de ulike rollene bør ha, da dette kan variere svært mye.

Når man ansetter nye medarbeidere, er det ikke uvanlig å kreve relevant utdanning på bachelor eller masternivå. Det er imidlertid viktig å huske på at lang, relevant erfaring (uformell kompetanse) kan være like mye verdt som formell kompetanse. Det er også viktig å huske på at kompetanse man har oppnådd gjennom et utdanningsløp må vedlikeholdes og oppdateres gjennom praktisk erfaring, kurs eller videreutdanning.

Det finnes en rekke kurs og sertifiseringer man kan ta på informasjonssikkerhetsområdet. Til tross for at slike sertifiseringer ofte er etterspurt, er det varierende i hvor stor grad de kan dokumentere at en person er egnet for en stilling. Å stille krav til sertifiseringer kan i noen tilfeller utelukke aktuelle kandidater.

Det er også viktig at de som ansettes har mulighet til å vedlikeholde sine sertifiseringer – det vil si at de har arbeidsoppgaver som er relevante for sertifiseringen.

I noen virksomheter må man vurdere om medarbeidere har tjenstlig behov for sikkerhetsklarering fordi det for noen oppgaver er en forutsetning at de utføres av sikkerhetsklarert og autorisert person. I en eventuell stillingsutlysning bør det opplyses om sikkerhetsklarering er en forutsetning for å kunne tiltre stillingen[4].

[4] Se statens personalhåndbok, kapittel 2.1.2.3

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.

Fagansvarlig informasjonssikkerhet skal bistå virksomhetsledelsen i utføringen av alle delaktivitetene under ledelsens styring og oppfølging[5].

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

- 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.

[5] https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter/ledelsens-styring-og-oppfolging

Tema for intervju/medarbeidersamtale

Forståelse av at informasjonssikkerhet handler om å sikre både konfidensialitet, integritet og tilgjengelighet, og at det handler om mye mer enn personopplysninger og beskyttelse i henhold til sikkerhetsloven. Informasjonssikkerhetsbrudd kan få konsekvenser for virksomhetens økonomi og tjenestenivå. Det kan få konsekvenser for innbyggere, andre virksomheter og samfunnet. Virksomhetene har behov for å jobbe helhetlig og systematisk med dette for å ivareta alle behov.

Forståelse av hvordan arbeidet med informasjonssikkerhet henger sammen med den øvrige virksomhetsstyringen. Formålet med informasjonssikkerhetsarbeidet er å understøtte virksomhetens primære målsetninger.

Forståelse av at arbeidet med internkontroll/styringssystem er et sett med aktiviteter som skal gjennomføres, ikke et sett med dokumenter. Hvordan aktivitetene skal gjennomføres i virksomheten, og hvem som er ansvarlig, bør være dokumentert og forankret i ledelsen, men for å ha styring og kontroll på informasjonssikkerheten må aktivitetene gjennomføres slik de skal i hele organisasjonen.

Kandidaten bør kunne snakke om hvordan han/hun ønsker å støtte ledelsen og risikoeiere i arbeidet med informasjonssikkerhet. Hvilke virkemidler kan tas i bruk, og hvilke områder er det naturlig å tilby støtte på?

Forståelse for at risikobildet er i stadig endring.

Forståelse av hvordan kriterier for å akseptere risiko er førende for hvordan beslutninger skal tas i virksomheten.

Forståelse for skillet mellom de systematiske aktivitetene for styring og kontroll (styringsaktiviteter)[6], og spesifikke sikkerhetstiltak[7], og evne til å formidle dette både til ledelse og til ansatte i ulike roller i virksomheten.

Forståelse for at informasjonssikkerhet er en del av alle ansattes daglige arbeid, og evne til å formidle dette til de ansatte.

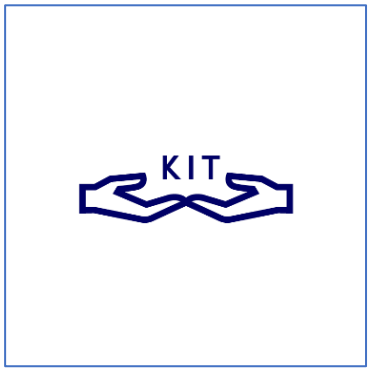
[6] «Styringsaktiviteter» er de sentrale aktivitetene som normalt inngår i styring og kontroll på informasjonssikkerhetsområdet. Jf. ISO/IEC 27001 (kapittel 4 til 10) og de systematiske aktivitetene som er beskrevet i Difi veileder «Internkontroll i praksis – informasjonssikkerhet».

[7] «Sikkerhetstiltak» er de varige tiltakene som en virksomhet etablerer for å redusere risikoen for brudd på KIT i informasjonsbehandlingen knyttet til oppgavene de utfører. Dette er tiltak som ved en risikobasert tilnærming velges og etableres ved bruk av styringsaktivitetene «risikovurdering» og «risikohåndtering».

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 og bevisstgjøring, og ellers bidra til virksomhetens arbeid med informasjonssikkerhet.

Ansvar og oppgaver vil i stor grad variere fra virksomhet til virksomhet.

Ønsket kompetanse

Kompetansebehovet for en støtteressurs innen informasjonssikkerhet vil variere basert på hvilke arbeidsoppgaver vedkommende har.

Ofte vil det være hensiktsmessig at en slik ressurs har mye av den samme kompetansen som fagansvarlig, men vedkommende kan ha mindre erfaring.

Avhengig av virksomhetens evne og mulighet til å lære opp en person, kan personer med relativt liten erfaring ha denne rollen. Det er da viktig at de har interesse for informasjonssikkerhet, risikostyring og internkontroll, og at de gjerne har grunnleggende kunnskap om og forståelse av fagområdene.

I noen virksomheter vil støtteressursene arbeide med mer konkrete oppgaver, og det kan da være hensiktsmessig om de har mer spisskompetanse – for eksempel innen gjennomføring av risikovurderinger/-håndtering, revisjon, hendelseshåndtering etc.

Tema for intervju/medarbeidersamtaler

Når man skal vurdere kompetansen til personer i denne rollen (eksisterende eller ved nyansettelser), er det viktig at man tar utgangspunkt i hva virksomheten har behov for. Det vil variere hvilken kompetanse som er vesentlig. Noen aspekter kan man imidlertid trekke frem som generelle:

Forståelse for at informasjonssikkerhet handler om å sikre både konfidensialitet, integritet og tilgjengelighet, og at det handler om mye mer enn personopplysninger og beskyttelse i henhold til sikkerhetsloven.

Forståelse for at risikobildet er i stadig endring.

Forståelse av de aktivitetene vedkommende skal bistå i, og for hvordan arbeidet med informasjonssikkerhet understøtter virksomhetens måloppnåelse.

Forståelse for at informasjonssikkerhet er en del av alle ansattes daglige arbeid, og evne til å formidle dette til de ansatte.

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[8] 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 intervjusituasjon 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.

[8] 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.

Toppleder

Ansvar og oppgaver

Toppleder er ansvarlig for at virksomheten har velfungerende styring og kontroll. Dette innebærer at arbeidet med informasjonssikkerhet gjennomføres på en systematisk og tilstrekkelig omfattende måte rundt om i hele virksomheten, tilpasset egenart, risiko og vesentlighet.

Toppleder, med sin ledergruppe, må gi føringer for hvordan internkontrollen på informasjonssikkerhetsområdet skal være: hvilke aktiviteter som skal gjennomføres, hvem som skal være ansvarlig, beskrivelse av nivåer for konsekvens og sannsynlighet, kriterier for å akseptere risiko etc. Føringer forankrer ledelsens ansvar.

Toppleder er også ansvarlig for at eventuelle nødvendige aktiviteter for å etablere og/eller forbedre internkontrollen på informasjonssikkerhetsområdet gjennomføres.

I det daglige er toppleder ansvarlig for å kommunisere viktighet – sette «tonen på toppen». I tillegg er det topplederes ansvar å vurdere og akseptere risikoer som er så store at de ikke kan aksepteres i linjen.

Toppleder er spesielt ansvarlig for at virksomhetsledelsens gjennomgang gjennomføres minst årlig. Vedkommende må ha tilstrekkelig oversikt til å rapportere status til etatsstyrer og/eller virksomhetens styre.

Ønsket kompetanse

Toppleder må forstå at det er ledelsens ansvar at arbeidet med informasjonssikkerhet i virksomheten er hensiktsmessig, og at ledelsen er ansvarlig for å legge føringene for dette arbeidet.

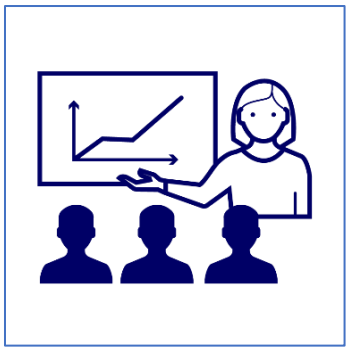
Det er nødvendig med tilstrekkelig kunnskap om informasjonssikkerhet til å kunne innarbeide informasjonssikkerhet i den helhetlige virksomhetsstyringen.

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

Toppleder eier risikoen for at virksomheten ikke når sine mål, og det er viktig med forståelse for at arbeidet med styring og kontroll av informasjonssikkerhet er vesentlig for å møte denne risikoen. Effektiv risikostyring er viktig. Noe risiko må opp til toppleder for å eventuelt aksepteres, basert på definerte kriterier for å akseptere risiko, mens annen risiko kan aksepteres på operativt nivå.

Toppleder 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 handler om å sikre både konfidensialitet, integritet og tilgjengelighet på informasjonen, og at det gjelder mye mer enn personopplysninger og beskyttelse i henhold til sikkerhetsloven. Informasjonssikkerhetsbrudd kan få konsekvenser for virksomhetens økonomi og tjenestenivå. Det kan få konsekvenser for innbyggere, andre virksomheter og samfunnet.

I tillegg er det viktig med forståelse for at risikobildet endrer seg når man tar ulike strategiske valg, for eksempel dersom man velger å tjenesteutsette oppgaver, eller ta i bruk skytjenester.



Øvrig ledergruppe

Ansvar og oppgaver

Toppledergruppen bør ha forståelse for at de må være involvert i å gi føringer for hvordan internkontrollen på informasjonssikkerhetsområdet skal være: hvilke aktiviteter som skal gjennomføres, hvem som skal være ansvarlig, beskrivelse av nivåer for 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 de er ansvarlige for.

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

På samme måte som risikoeiere må også ledere på alle nivå minst en gang årlig systematisk vurdere status på informasjonssikkerhetsarbeidet innenfor sine ansvarsområder. De har også ansvar for at 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 de to. De må vite hva som er ledelsens ansvar, kjenne til hvilke aktiviteter som skal gjennomføres, og 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 handler om å sikre både konfidensialitet, integritet og tilgjengelighet på informasjonen, og at det gjelder mye mer enn personopplysninger og beskyttelse i henhold til sikkerhetsloven. Informasjonssikkerhetsbrudd kan få konsekvenser får virksomhetens økonomi og tjenestenivå. Det kan få konsekvenser for innbyggere, andre virksomheter og samfunnet.

Det er nyttig med forståelse for at styring av informasjonssikkerhetsarbeidet ikke skiller seg vesentlig fra annen virksomhetsstyring og internkontroll på andre områder (f.eks. HMS og personvern). I dette 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, basert på definerte kriterier for å akseptere risiko, mens annen risiko enten må helt opp til toppleder, eller kan aksepteres på operativt nivå.

De må også forstå at risikobildet endrer seg når man tar ulike strategiske valg, for eksempel dersom 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 imidlertid være nyttig å snakke med kandidaten om hvilken informasjon som behandles i arbeidsoppgavene vedkommende skal ha ansvar for, hvordan vedkommende ser på informasjonssikkerhet og annen internkontroll, og vedkommendes tanker om punktene under «ønsket kompetanse».

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 topplеder 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.

Forståelse for skillet mellom de systematiske aktivitetene for styring og kontroll (styringsaktiviteter)[10], og spesifikke sikkerhetstiltak[11].

Forståelse for hvordan IT-avdelingen kan bistå risikoeiere i vurdering av risiko, ved å beskrive potensielle scenarioer, og i håndtering av risikoer, ved å foreslå og etablere (etter beslutning fra risikoeier) sikkerhetstiltak.

Forståelse for at det er nødvendig å ha gode kommunikasjonsevner. En IT-leder må kommunisere med mange ulike nivåer i virksomheten – alt fra ledelse, via fagansvarlig informasjonssikkerhet, til teknisk IKT-personell og øvrige ansatte.

---

[9] Tiltaksleverandørene har som regel en viktig rolle i å bistå med vurdering av risiko (de vet hva som kan skje) og håndtering av risiko (de vet hvilke tiltak som er aktuelle og kostnadene forbundet med disse). Ansvaret for å styre risiko og ressursbruk, og ta beslutningene, ligger likevel hos risikoeierne.

[10] «Styringsaktiviteter» er de sentrale aktivitetene som normalt inngår i styring og kontroll på informasjonssikkerhetsområdet. Jf. ISO/IEC 27001 (kapittel 4 til 10) og de systematiske aktivitetene som er beskrevet i Difi veileder «Internkontroll i praksis – informasjonssikkerhet».

[11] «Sikkerhetstiltak» er de varige tiltakene som en virksomhet etablerer for å redusere risikoen for brudd på KIT i informasjonsbehandlingen knyttet til oppgavene de utfører. Dette er tiltak som ved en risikobasert tilnærming velges og etableres ved bruk av styringsaktivitetene «risikovurdering» og «risikohåndtering».

Systemeier

Ansvar og oppgaver

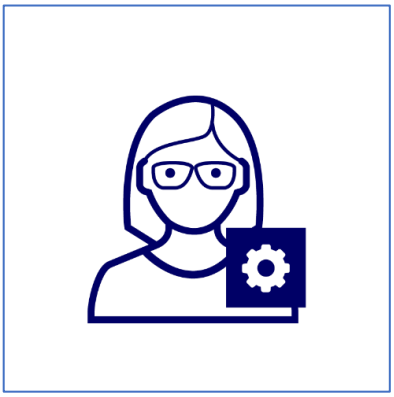
Med systemeier mener vi i denne forbindelsen ansatte som har et særskilt ansvar for et gitt IKT-system. Dette kan variere fra en virksomhet til en annen.

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.

Alle ansatte

Ansvar og oppgaver

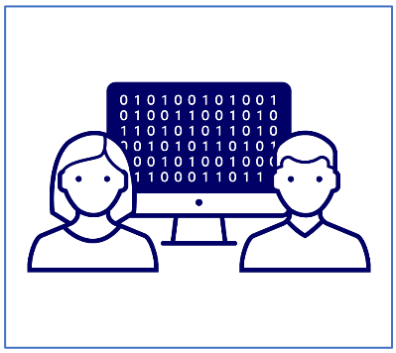
Alle ansatte har et ansvar for å bidra til at virksomheten når sine samlede mål på en best mulig måte. De skal ha et bevisst forhold til målene for eget arbeid, hvilken informasjon de behandler, og hvilke krav som stilles til arbeidet deres. Dette gjelder også for fagområdet informasjonssikkerhet.

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.