# Anbefalinger om styring av informasjonssikkerhet og personopplysningsvern

Utarbeidet av Digdir, Datatilsynet, NSM, KS, DFØ og Helsedirektoratet i programmet Felles sikkerhet i forvaltningen.

**Innhold**

# Introduksjon

**Disse sidene gir anbefalinger til offentlige virksomheter om hvilke styringsaktiviteter de bør ha. Målet er at ledelsen skal kunne ivareta ansvaret sitt.**

Offentlige virksomheter og deres ledere har ansvar for å styre risiko for sine oppgaver og tjenester. En del av dette er å styre informasjonssikkerhet og personopplysningsvern. Dette bør være en integrert del av virksomhetsstyringen.

Disse anbefalingene beskriver aktiviteter som bør gjennomføres systematisk for å styre informasjonssikkerhet og personopplysningsvern på en god måte og ivareta plikter i regelverk.

Virksomheten må jobbe effektivt med dette for alle sine oppgaver og tjenester. Ledelsen bruker styringsaktiviteter, sikkerhetstiltak og personverntiltak for å ivareta dette ansvaret.

Svak styring kan føre til brudd på lovkrav, tap av samfunnsverdier og tillit. God styring legger til rette for etterlevelse av blant annet eForvaltningsforskriftens §15, sikkerhetsloven kap. 6, digitalsikkerhetsloven §7, og artikkel 24 i GDPR.

Disse felles anbefalingene om styringsaktiviteter er gitt av

- Nasjonal sikkerhetsmyndighet (NSM)
- Datatilsynet (DT)
- Kommunesektorens organisasjon (KS)
- Digitaliseringsdirektoratet (Digdir)
- Direktoratet for forvaltning og økonomistyring (DFØ)
- Helsedirektoratet (Hdir)

Anbefalingene er utarbeidet i programmet «Felles sikkerhet i forvaltningen».

## Sammenheng med tilgjengelig veiledning

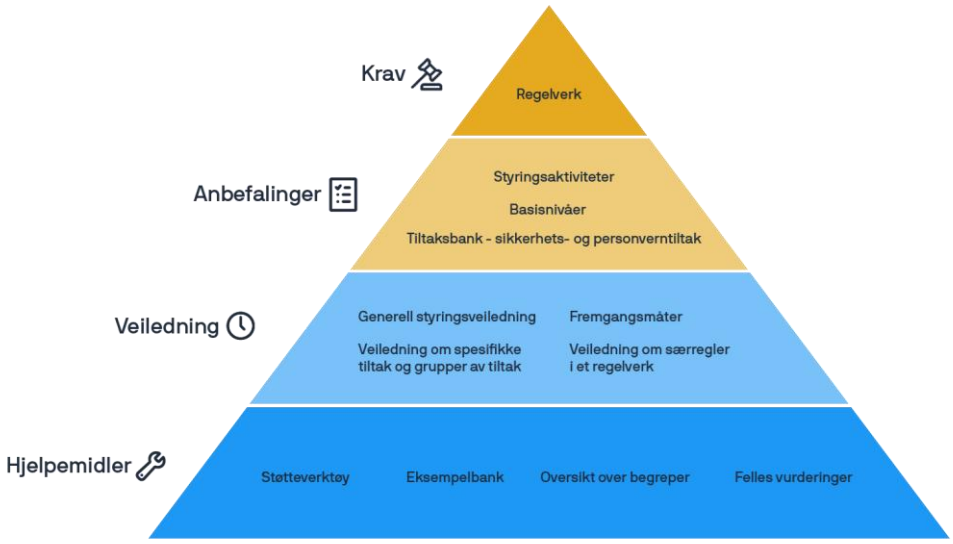
Det finnes mange offentlige aktører som gir veiledning om informasjonssikkerhet og personvern.

Anbefalingene sier **hva** virksomhetene bør gjøre, og **hvorfor**, men mange vil fortsatt trenge hjelp til **hvordan** det skal gjøres, og **hvem** som skal gjøre det. Dette kan for eksempel være i form av metodeveiledning eller praktiske verktøy.

I dag finnes det mye veiledning, men det kan være vanskelig å få oversikt. Et mål i arbeidet med «Felles sikkerhet i forvaltningen» er at det skal finnes felles anbefalinger om hva offentlige virksomheter bør ha på plass for styre informasjonssikkerhet og personopplysningsvern, og ha et forsvarlig sikkerhetsnivå for sine oppgaver og tjenester. Anbefalingene om styringsaktiviteter er første steg i dette arbeidet.

Videre skal det bli lettere å se sammenhengen mellom disse anbefalingene og den veiledningen som finnes. Veiledning skal vise til anbefalingene, og veiledningsaktørene bør forklare hvilke deler av det som er anbefalt de veileder om.

Det gjenstår fortsatt mye arbeid for å rydde og samordne veiledningen på området.




Målbildet kan illustreres som en trekant, med fire nivåer:

1) Krav fra regelverk
2) Anbefalinger, for eksempel om
    a. styringsaktiviteter
    b. basisnivåer av tiltak
    c. felles tiltaksbank med sikkerhets- og personverntiltak
3) Veiledning knyttet til ulike deler av anbefalingene, for eksempel
    a. generell styringsveiledning
    b. veiledning i fremgangsmåter/metoder
    c. veiledning om spesifikke tiltak eller grupper av tiltak
    d. veiledning om særregler i et regelverk
4) Praktiske hjelpemidler, for eksempel
    a. Støtteverktøy
    b. Eksempelbank
    c. Oversikt over begreper
    d. Felles vurderinger

# LS - Ledelsens styring og oppfølging

Virksomhetens leder skal sørge for god styring og kontroll i virksomheten, inkludert ivaretakelse av tilstrekkelig informasjonssikkerhet og personopplysningsvern. Dette skal gjøres ved å lage en plan for styringsaktiviteter som gjennomføres systematisk i hele virksomheten.

Virksomhetens ledelse skal sørge for å

- etablere og følge opp styringsaktivitetene som en del av virksomhetsstyringen
- gi føringer for styringsaktivitetene og det øvrige arbeidet med informasjonssikkerhet og personopplysningsvern
- sørge for tilstrekkelig ressurser til arbeidet med informasjonssikkerhet og personopplysningsvern
- følge opp at styringsaktivitetene fungerer godt og gjøre nødvendige endringer ved behov
- følge opp at virksomhetens oppgaver og tjenester har tilstrekkelig informasjonssikkerhet og personopplysningsvern

## LS-1 Gi føringer

Virksomhetsledelsen skal gi føringer for hvordan styringen av informasjonssikkerhet og personopplysningsvern skal fungere som en del av den helhetlige styringen av virksomheten. Innholdet i føringene bør være basert på virksomhetens interne og eksterne rammebetingelser.

Føringene skal inneholde overordnet beskrivelse av formålet med virksomhetens informasjonsbehandling, og hvilken betydning den har for virksomhetens oppgaver og tjenester.

Virksomhetsledelsen har ansvaret for å gi føringer for

- struktur og innhold i styringsaktivitetene
- roller og myndighet i arbeidet med styring av informasjonssikkerhet og personopplysningsvern
- delegering av oppgaver for å styre informasjonssikkerhet og personopplysningsvern til ledere som er mål- og resultatansvarlige for et område (risikoeiere).
- hvordan risikoeiere skal forstå, vurdere og håndtere risiko, inkludert kriterier for å akseptere risiko
- hvordan risikoeiere skal sørge for innebygd personvern i oppgaver og tjenester som behandler personopplysninger
- hvordan styringsaktivitetene skal gjennomføres

**Gir evne til**

- Helhetlig styring av arbeidet med informasjonssikkerhet og personopplysningsvern.
- Å styre hva som skal gjøres, og hvem som skal gjøre det

## LS-2 Sørge for budsjett til arbeidet

Ledere på alle nivå skal sette av tilstrekkelig med ressurser til arbeidet med informasjonssikkerhet og personopplysningsvern. Det gjelder både styringsaktiviteter, sikkerhetstiltak og personverntiltak.

Øverste ledelse er ansvarlig for at tilstrekkelige midler tilordnes i de ordinære budsjettprosessene. Det må i tillegg settes av ressurser som gir virksomheten handlingsrom til å iverksette nødvendige aktiviteter og tiltak som blir identifisert gjennom budsjettperioden.

**Gir evne til**

- Å ha tilstrekkelig finansiering av det ledelsen har besluttet at skal gjøres innen informasjonssikkerhet og personopplysningsvern.
- Å se ressursbruken på arbeidet med informasjonssikkerhet og personopplysningsvern i sammenheng med virksomhetens andre aktiviteter.

## LS-3 Kommunisere viktighet

Ledere på alle nivå skal benytte sin påvirkningskraft og kommunisere hvor viktig det er å gjennomføre styringsaktiviteter og forvalte sikkerhets- og personverntiltak. De skal også kommunisere hvordan dette arbeidet er prioritert i virksomheten.

Kommunikasjonen bør skje på hensiktsmessig måte, både skriftlig og muntlig.

**Gir evne til**

- Å gjøre ledelsens prioriteringer kjent i virksomheten
- Å påvirke effektiv gjennomføring av styringsaktiviteter i hele virksomheten

## LS-4 Løfte og håndtere problemstillinger gjennom linjen

Når problemstillinger i styringsaktivitetene ikke kan løses på det organisatoriske nivå de oppstår skal det løftes til den som har tilstrekkelig myndighet til å håndtere problemstillingene. Vedkommende må se risikoer, kostnader og negative sideeffekter for flere organisatoriske enheter i sammenheng, og ta nødvendige beslutninger.

Risikoeiere skal løfte problemstillingen når:

- de ikke har budsjett til å finansiere tiltak som anses nødvendige for å redusere risikoer iht. føringene i virksomheten
- de ikke får redusert en risiko til det nivå de har myndighet til å akseptere. Beslutningen tas av person med tilstrekkelig myndighet, slik det er angitt i virksomhetens kriterier for å akseptere risiko.
- det er uenighet om prioriteringer og om hvordan risiko skal håndteres for ressurser som benyttes av flere risikoeiere

**Gir evne til**

- Å ta effektive beslutninger i tråd med virksomhetens myndighetsstruktur, blant annet om aksept av risiko, finansiering av tiltak, og valg av løsninger

## LS-5 Virksomhetsledelsens gjennomgang

Virksomhetsledelsen har ansvaret for å gjennomgå status for styring på informasjonssikkerhets- og personopplysningsvernsområdet minst én gang i året.

Gjennomgangen vil som regel omfatte:

- Vurdering av om styringsaktivitetene fungerer effektivt og gir ønskede resultater
- Status på
    - tjenesteområder, eller tjenester der virksomhetsledelsen har prioritert informasjonssikkerhet og personopplysningsvern
    - risikoer, eller risikoområder virksomhetsledelsen har prioritert
    - endringer og andre beslutninger fra tidligere gjennomganger
    - vesentlige avvik i informasjonssikkerhet og personopplysningsvern
- tilbakemeldinger på arbeidet, slik som avvik, resultater fra måling eller evaluering, resultater fra revisjoner, status på regelverksetterlevelse
- om kulturen i virksomheten understøtter et systematisk arbeid med styring og kontroll
- vesentlige endringer i rammebetingelser
- lokale, nasjonale og internasjonale trender knyttet til trusler, sårbarheter, uønskede hendelser og risikoer

Leder av virksomheten skal på bakgrunn av gjennomgangen gi eventuelle nye, eller oppdaterte føringer for styringsaktivitetene og øvrig arbeid med informasjonssikkerhet, samt sørge for at disse finansieres og iverksettes. Dette kan også innebære å sørge for at det gjennomføres nødvendige evalueringer eller internrevisjon, eller etableres målinger på enkeltområder.

**Gir evne til**

- Å sørge for at virksomheten får utført oppgaver og levert tjenester
- Å ta beslutninger om styringsaktiviteter
- Å ta overordnede beslutninger om risikoaksept i virksomheten
- Å ta overordnede beslutninger om ressursbruk

# OP – Ha oversikt og prioritere

Alle risikoeiere i virksomheten skal ha god oversikt over sine ansvarsområder, slik at arbeidet med styring av informasjonssikkerhet og personopplysningsvern gjøres effektivt og målrettet.

Risikoeiere skal være i stand til å organisere og prioritere arbeidet med informasjonssikkerhet og personopplysningsvern. Dette inkluderer blant annet å beslutte hvor det er behov for å gjennomføre risikovurderinger.

Oversikten vil være nyttig for virksomhetens helhetlige arbeid med beredskap og virksomhetskontinuitet, og bør benyttes til dette.

En helhetlig oversikt for hele virksomheten kan bygges opp gradvis etter hvert som disse aktivitetene gjennomføres. En samlet oversikt gir en felles forståelse av hvilke oppgaver og tjenester som er mest kritiske på tvers av organisasjonen, og danner grunnlag for enhetlig prioritering av tiltak.

## OP-1 Oversikt over ansvarsområde

Risikoeiere skal opprette og vedlikeholde en oversikt av eget ansvarsområde. Denne foranalysen skal gi oversikt over hvilken betydning informasjonsbehandlingen har for oppgaver og tjenester, og bør omfatte:

- Oversikt over
    - oppgaver og tjenester som utføres
    - hvilken informasjon som behandles i oppgaver og tjenester, inkludert hvilke personopplysninger som behandles
    - formål med behandling av personopplysninger, behandlingsgrunnlag og behandlingsansvar
    - overføring av personopplysninger utenfor EØS og overføringsgrunnlag som benyttes
    - digitale systemer og digitale tjenester som benyttes, inkludert avhengigheter til eksterne tjenester
- En vurdering av hvor store konsekvensene ved brudd på informasjonssikkerhet eller personopplysningsvern kan bli, for virksomheten og for eksterne parter
- Vedlikehold av protokoll over behandlingsaktiviteter, med informasjon om behandling av personopplysninger
- En gjennomgang av vesentlige trusler, farer og sårbarheter

**Merk:**

Begrepet «verdivurdering» brukes ikke her, men en tilsvarende vurdering er en del av denne aktiviteten.

«Verdivurdering» i denne sammenhengen handler om å synliggjøre hvor store konsekvensene kan bli, dersom det blir brudd på informasjonssikkerheten eller personopplysningsvernet.

**Gir evne til**

- å ha oversikt over hvor viktig ulike oppgaver og tjenester er for virksomheten
- å vurdere behov for risikovurderinger, og prioritere ressursbruken på arbeidet med informasjonssikkerhet og personopplysningsvern
- å ha oversikt over all behandling av personopplysninger

## OP-2 Kartlegge eksterne krav

Risikoeiere skal ha oversikt over de regler og avtaler som gjelder for sitt ansvarsområde. De må kartlegge eksterne krav for å identifisere spesifikke sikkerhetstiltak og personverntiltak som må etableres for at kravene skal etterleves. Eksterne krav kan for eksempel komme fra regelverk, avtaler eller bransjekrav/-normer.

Virksomheten bør gjøre en felles kartlegging, hvor man analyserer kravene i regelverk og avtaler som gjelder flere områder i virksomheten. Risikoeiere bør bruke den felles kartleggingen i sitt arbeid.

**Gir evne til**

- å etablere sikkerhets- og personverntiltak slik at regelverk og avtaler etterleves

## OP-3 Vurdere behov for risikovurderinger

Risikoeiere skal regelmessig vurdere behovet for oppdaterte eller nye risikovurderinger innen sitt ansvarsområde. Foranalysen er grunnlaget for behovsvurderingen. Vurderingen skal avdekke om det er behov for ytterligere risikovurdering og -håndtering på ansvarsområdet.

Risikoeier skal også vurdere behovet for risikovurdering eller personvernkonsekvensvurdering dersom det skjer endringer som i vesentlig grad kan påvirke informasjonssikkerhet og personopplysningsvern i oppgaver og tjenester.

Vurderingen skal dokumenteres.

**Gir evne til**

- å prioritere ressursbruken ved at risikovurderinger gjennomføres på de områdene der konsekvensene kan bli størst.
- å arbeide effektivt med informasjonssikkerhet og personopplysningsvern

## OP-4 Oppdatert oversikt over risikovurderinger

Risikoeiere skal etablere og vedlikeholde en oversikt over gjennomførte risikovurderinger på sitt ansvarsområde, og hvilke risikovurderinger som er planlagt. Oversikten skal benyttes når risikoeier vurderer behov for nye risikovurderinger, samt for å sikre at risikovurderinger følges opp og oppdateres når det er nødvendig.

Oversikten bør inneholde informasjon om

- Når risikovurderingen har vært gjennomført, og tidspunkt for planlagt ny vurdering
- Hvor man kan finne dokumentasjon fra risikovurderingen
- Høyeste risikonivå identifisert i risikovurderingen
- Kunnskapsstyrken for risikovurderingen

**Gir evne til**

- å prioritere arbeidet med vurdering og håndtering av risiko

# RV - Vurdering av risiko

Risikoeiere skal sørge for å ha tilstrekkelig oversikt over risiko knyttet til informasjonssikkerhet og personopplysningsvern på sitt ansvarsområde, og vite hvilke risikoer som må håndteres.

Risikoeiere planlegger og gjennomfører risikovurderinger på sitt ansvarsområde, for å styre risiko på oppgaver og tjenester.

Avhengig av hvor stort og komplekst ansvarsområdet er, bør risikoeier benytte resultatet av foranalysen til å dele opp området i hensiktsmessige deler, eller gruppere deler som kan vurderes sammen.

Vurdering av risiko gjennomføres systematisk og planlagt (ref. **OP-3Vurdere behov for risikovurderinger (OP-3)**), men også når det oppstår særskilt behov – for eksempel etter hendelser eller i forbindelse med endringer i oppgaver og tjenester, inkludert anskaffelser og utvikling av digitale systemer.

**Merk:**

Begrepet ROS (Risiko og sårbarhetsanalyse) brukes ikke her, men aktivitetene som beskrives i kapittelet RV – Vurdering av risiko tilsvarer det som gjennomføres i en ROS-analyse.

## RV-1 Planlegge risikovurdering

Risikoeier skal sørge for at det legges en plan før en risikovurdering gjennomføres.

Planleggingen bør som minimum inneholde:

- Beskrivelse av omfang og avgrensninger
- Hvilken kompetanse det er behov for, og hvem som skal delta
- Valg av framgangsmåte, inkludert hensiktsmessige metoder og støttemetoder
- Estimat av ressursbruk
- Hvordan arbeidet skal dokumenteres

**Tips:** Det finnes en rekke regelverk som stiller spesifikke krav til hvordan en risikovurdering skal gjennomføres, og elementer som skal tas med (ref. **Kartlegge eksterne krav (OP-2)**). Dette må tas hensyn til i planleggingen.

### Gir evne til

- effektiv gjennomføring av risikovurderinger, som gir et godt beslutningsgrunnlag

## RV-2 Vurdere personvernkonsekvensvurdering (DPIA)

All behandling av personopplysninger krever et formål, et behandlingsgrunnlag, en vurdering av nødvendighet og proporsjonalitet og skal i hovedsak dokumenteres i en protokoll over behandlingsaktiviteter. En slik behandlingsprotokoll kan publiseres offentlig som en del av personvernerklæringen.

Dersom det er sannsynlig at en type behandling av personopplysninger kan medføre høy risiko for fysiske personer skal risikoeier i tillegg sørge for å gjennomføre en personvernkonsekvensvurdering (DPIA) for å finne de ekstra tiltakene som må til for å redusere en høy risiko. Slike vurderinger skal omfatte alle forhold og plikter knyttet til personvern, inkludert personopplysningssikkerhet. En vurdering av personvernkonsekvenser skal minimum inneholde:

- En systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen
- En vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene
- En vurdering av risikoene for de registrertes rettigheter og friheter
- De planlagte tiltakene for å håndtere risikoene og for å påvise at forordningen overholdes

Funn og tiltak fra denne prosessen skal valideres (sjekke at de er gode nok for formålet, og oppfyller kravene) og godkjennes av ledelsen.

Dersom en vurdering av personvernkonsekvenser tilsier at behandlingen tross tiltak fremdeles vil medføre en høy risiko, skal den behandlingsansvarlige rådføre seg med Datatilsynet (gjennom den formelle prosessen Forhåndsdrøftelse) før behandlingen av personopplysninger igangsettes.

### Gir evne til

- å ivareta de registrertes rettigheter før behandling av personopplysninger starter
- å effektivt behandle, dele og motta personopplysninger knyttet til oppgaver, tjenester og produkter
- å dokumentere at personopplysninger behandles lovlig og ansvarlig
- å oppfylle informasjonsplikten til de registrerte, samarbeidspartnere og myndigheter
- å skape tillit fra ansatte, kunder/brukere, samarbeidspartnere og samfunnet generelt

En vurdering av personvernkonsekvenser er særlig nødvendig i følgende tilfeller (listen er ikke uttømmende):

- bruk av ny teknologi, nye måter å behandle personopplysninger på eller nye bruksområder for personopplysninger
- en systematisk og omfattende vurdering av personopplysninger basert på automatisert behandling som i betydelig grad påvirker den fysiske personen
- behandling i stor skala av særlige kategorier av personopplysninger
- en systematisk overvåking i stor skala

## RV-3 Gjennomføre risikovurdering

Risikoeiere skal sørge for at nødvendige risikovurderinger og personvernkonsekvensvurderinger blir gjennomført. Omfang og praktisk gjennomføring må tilpasses det som skal vurderes. Risikoeier skal sørge for at metodene som benyttes er egnet til det som skal vurderes, og ivaretar relevante regelverkskrav.

Risikoeiere skal benytte resultatet fra foranalysen i **Oversikt over ansvarsområde (OP-1)** når de vurderer risiko.

Når vurderinger oppdateres kan det være tilstrekkelig å vurdere om det har skjedd endringer som påvirker eksisterende vurderinger. For eksempel ny kunnskap om sårbarheter, hvilke hendelser som kan inntreffe, eller hvilke konsekvenser som kan oppstå.

Risikovurderingen skal dokumenteres, og danner et beslutningsgrunnlag for risikoeier for håndtering av risiko.

Ved gjennomføring av en risikovurdering vil normalt være behov for å ta hensyn til

- hvilke konsekvenser informasjonssikkerhets- og personvernbrudd kan få for virksomhetens oppgaver og tjenester, virksomhetens økonomi, individer, andre virksomheter, miljø, samfunnsfunksjoner eller nasjonale sikkerhetsinteresser
- allerede etablerte sikkerhets- og personverntiltak for å forebygge, oppdage og reagere på hendelser som kan føre til informasjonssikkerhets- eller personvernbrudd
- hvor sannsynlig det er at konsekvensene inntreffer

### Gir evne til

- å få oversikt over risiko på et område (oppgave, tjeneste, digitalt system eller annen avgrensing)
- å ta beslutninger om risiko, inkludert bruk av virksomhetens ressurser på håndtering av risiko

## RV-4 Vurdere risiko etter hendelser

Når risikoeiere blir kjent med informasjonssikkerhetshendelser eller hendelser som har påvirket personopplysningsvernet, skal de gjøre ny behovsvurdering, og gjennomføre risikovurderinger hvis det er behov for det.

**Husk:** Det kan her være snakk om både hendelser som har inntruffet i egen virksomhet, og relevante hendelser man hører om fra andre virksomheter.

**Gir evne til**

- å ha oppdatert oversikt over risiko når hendelser har tilført ny informasjon til bruk i vurderingene

# RH – Håndtering av risiko

I forlengelse av risikovurderinger, skal virksomheten beslutte hvordan de identifiserte risikoene skal håndteres. Det må avklares om det finnes aktuelle tiltak for å redusere risikoen, eller om den bør håndteres ved å unngå eller dele den, eller akseptere den.

Risikoeier skal sørge for at

- det utarbeides forslag til håndtering av risikoer
- forslagene godkjennes
- tiltak etableres
- en oversikt over fellessikring og tilleggssikring vedlikeholdes

**Fellessikring** er et sett med sikkerhets- og personverntiltak som gir et grunnleggende sikkerhetsnivå i hele virksomheten. Fellessikringen bidrar til å håndtere risiko for alle, eller de fleste, av virksomhetens oppgaver og tjenester. **Tilleggssikring** er sikkerhetstiltak for oppgaver og tjenester med behov utover fellessikringen.

Et felles sett med sikkerhets- og personverntiltak bidrar til en felles forståelse av hvilke grunnleggende tiltak som er etablert i virksomheten. Slik kan risikoeiere i større grad konsentrere seg om risiko som er spesifikk for sine oppgaver, tjenester og informasjonssystemer, og behov utover det som allerede er etablert i fellessikringen.

## RH-1 Foreslå håndtering av risikoer

Risikoeier skal sørge for at det utarbeides forslag til hvordan risikoer skal håndteres.

For hver risiko skal det vurderes om det finnes aktuelle tiltak for å redusere risikoen, eller om den bør håndteres ved å unngå eller dele den, eller akseptere den. Virksomhetens kriterier for å akseptere risiko skal være førende for hvordan risiko håndteres.

Når risiko skal reduseres ved å iverksette tiltak, skal kost/nytte av de aktuelle tiltakene vurderes ut fra faktorene

- risikoreduserende effekt
- direkte økonomisk kostnad (etablering og drift)
- negative sideeffekter

Arbeidet skal også inkludere forslag til spesifikke sikkerhetstiltak som følger av krav i regelverk eller avtaler (ref. **Kartlegge eksterne krav (OP-2)**).

Der det er behov, bør man vurdere midlertidige tiltak inntil endelig løsning er på plass.

Forslaget skal begrunnes og dokumenteres.

**Husk:** Det finnes regelverk som stiller spesifikke krav til hvordan risiko skal håndteres (ref. **Kartlegge eksterne krav (OP-2)**).

Virksomhet kan for eksempel ikke akseptere høy risiko for de registrerte når de behandlinger personopplysninger.

**Gir evne til**

- å vurdere ulike tiltak opp mot hverandre for å håndtere risiko på en kostnadseffektiv måte, med minst mulig negative sideeffekter.

## RH-2 Godkjenne forslag til risikohåndtering

Risikoeier skal vurdere og godkjenne forslagene til håndtering av risiko. Vurderingen og beslutningen skal dokumenteres på hensiktsmessig måte.

Risikoeier skal:

- ta stilling til kvaliteten på grunnarbeidet
- vurdere om restrisiko på forslagene er akseptabel
- vurdere kost/nytte på foreslåtte tiltak, inkludert mulige negative sideeffekter
- sikre at regelverkskrav er ivaretatt
- sikre finansieringen av det som godkjennes
- løfte godkjenning i linjen dersom det er nødvendig

**Gir evne til**

- å iverksette formåls- og kostnadseffektive tiltak

## RH-3 Iverksette godkjent håndtering av risiko

Risikoeiere skal sørge for at godkjent håndtering av risiko blir gjennomført og fulgt opp. Det kan inkludere

- å etablere sikkerhets- og personverntiltak for å redusere risiko
- å formalisere og dokumentere aksept av risiko
- å endre på hvilke oppgaver som utføres, eller hvordan oppgaver og tjenester utføres, for å unngå risiko
- å dele risiko med andre

Nye eller endrede sikkerhets- og personverntiltak må etableres, inkludert ansvaret for å forvalte dem. De må testes under utforming, etablering og forvaltning for å sikre at de fungerer etter hensikten.

Virksomhetens oversikt over sikkerhets- og personverntiltak skal vedlikeholdes, slik at alle planlagte og etablerte tiltak er tilstrekkelig dokumentert.

**Gir evne til**

- å utføre oppgaver og levere tjenester med risiko som ledelsen har styring og kontroll med
- å ha oversikt over sikkerhets- og personverntiltak, og hvem som har ansvar for at de er etablert og virker etter hensikten

## RH-4 Forvalte fellessikring og tilleggssikring

Virksomhetens leder skal sørge for at fellessikring og tilleggssikring forvaltes.

Når nye sikkerhets- og personverntiltak etableres, skal risikoeiere vurdere om de kan inngå i virksomhetens fellessikring, eller om det er tilleggssikring som risikoeiere kan velge ut fra behov. Kostnadseffektiv forvaltning av tiltakene, og negative sideeffekter for andre oppgaver, tjenester eller informasjonssystemer, skal være med i vurderingen.

**Gir evne til**

- å ha effektiv og helhetlig forvaltning av virksomhetens samlede sett av sikkerhets- og personverntiltak
- å forenkle og effektivisere aktivitetene for vurdering og håndtering av risiko.

# ME – Måling, evaluering og revisjon

Virksomhetens ledere skal ha innsikt i status på arbeidet med informasjonssikkerhet og personopplysningsvern, og om de har tilstrekkelig oversikt over risiko på sitt ansvarsområde.

Ledere skal ha forståelse av tilstanden på sine tjenester og sitt ansvarsområde. Risikoeiere skal systematisk vurdere om styringsaktivitetene blir etterlevd og fungerer effektivt, om sikkerhets- og personverntiltak fungerer, er kostnadseffektive, og om regelverk blir etterlevd. Ledelsen skal sørge for:

- at risikoeiere vurderer status av deres ansvarsområder minst én gang i året
- at det etableres målinger for å følge tilstanden over tid der det er behov for det
- at styringen av informasjonssikkerhet og personopplysningsvern blir evaluert
- at effektiviteten av sikkerhets- og personverntiltak vurderes regelmessig

## ME-1 Vurdere status på eget ansvarsområde

Risikoeiere skal vurdere status på sitt ansvarsområde minst én gang i året, og iverksette forbedringer etter behov.

Statusvurderingen skal omfatte vurderinger av om man selv, egne ansatte og leverandører:

- gjennomfører styringsaktivitetene
- etablerer og følger opp vedtatte eller avtalte sikkerhets- og personverntiltak
- etterlever gjeldende sikkerhets- og personverntiltak
- følger regelverk

De som har ansvar for tiltak, skal vurdere om tiltakene fungerer som forutsatt (Ref. **Vurdere effektivitet av sikkerhets- og personverntiltak (ME-4)**).

Dersom vurderingen avdekker avvik, må disse utbedres, og oppfølgingen skal dokumenteres.

**Gir evne til**

- å ha kunnskap om tilstand på ansvarsområder
- å vite om styringsaktivitetene blir gjennomført som forutsatt, om etablerte sikkerhets- og personverntiltak er effektive, og om regelverk blir etterlevd
- bedre beslutningsgrunnlag i virksomhetsledelsens gjennomgang

## ME-2 Måle tilstanden på områder over tid

På områder der virksomhetsledelsen eller risikoeier har behov for å følge tilstanden over tid, må de sørge for å etablere systematisk måling og rapportering. Målingene kan være på både organisatorisk, menneskelig og teknisk nivå.

Det vil både variere fra virksomhet til virksomhet, og i en enkelt virksomhet over tid, hva man har behov for å måle. Det må derfor jevnlig vurderes om de målingene som er etablert er hensiktsmessig innrettet, og om det er de riktige områdene det gjennomføres målinger på.

Resultatene skal sammenstilles og følges opp over tid, og presenteres for virksomhetsledelsen etter behov.

**Gir evne til**

- å enklere følge tilstanden i virksomheten over tid
- å sette konkrete resultatmål for hele eller deler av virksomheten

## ME-3Gjennomføre evalueringer/internrevisjon

Virksomhetsledelsen skal sørge for at det gjennomføres evalueringer av hele eller deler av arbeidet med styring av informasjonssikkerhet og personopplysningsvern i virksomheten. Dette kan være internrevisjoner som følge av lovkrav eller andre forpliktelser, eller andre evalueringer basert på behov.

Ved gjennomføring av evalueringer skal det alltid gjøres en vurdering av behovet for uavhengighet. Ved særskilt behov for uavhengighet eller kompetanse, kan man hente inn eksterne til å gjennomføre evalueringen.

En evaluering kan være på oppdrag fra virksomhetsledelsen, eller fra en risikoeier for et avgrenset område. Det skal utarbeides en rapport eller oppsummering, og resultatet skal presenteres for oppdragsgiver. Eventuelle avvik skal følges opp.

Gjennomfør ved behov en **analyse av status** på arbeidet med informasjonssikkerhet og personopplysningsvern. Vurder innhold og kvalitet på det dere allerede har og gjør, både innen informasjonssikkerhet og personopplysningsvern, og på andre internkontrollområder. Avstanden mellom nåsituasjonen og ønsket situasjon viser hvor det er behov for vesentlig forbedring. Prioriter disse behovene, og si noe om forventet bruk av ressurser.

**Gir evne til å**

- vurdere om arbeidet med styring av informasjonssikkerhet og personopplysningsvern i virksomheten fungerer som tiltenkt
- avdekke om virksomheten følger bestemte krav, og om nødvendige tiltak er etablert og vedlikeholdt på en formåls- og kostnadseffektiv måte.

## ME-4Vurdere effektivitet av sikkerhets- og personverntiltak

Virksomhetsledelsen har ansvar for at det regelmessig vurderes om sikkerhets- og personverntiltakene er effektive. Hensikten er å undersøke om tiltakene er etablert, at de virker som tiltenkt, og at de har ønsket effekt på virksomhetens informasjonssikkerhet og personopplysningsvern.

**Gir evne til**

- å kjenne status på sikkerhets- og personverntiltak
- å ha formåls- og kostnadseffektive sikkerhets- og personverntiltak
- å vurdere om styringsaktivitetene for å vurdere og håndtere risiko fungerer godt

# OH – Overvåking og hendelseshåndtering

Virksomheten skal være i stand til å oppdage og reagere på uønskede hendelser. Feil, avvik og uønskede hendelser skal avdekkes og følges opp, for å redusere konsekvensen og lære av det som har skjedd.

Ledere skal sørge for:

- overvåking etter behov
- forsvarlig rapportering, registrering og oppfølging av uønskede hendelser og avvik
- varsling til myndigheter og responsmiljøer i henhold til regelverk og avtaler
- å ha prosedyrer for beredskap og krisehåndtering som trer inn ved en hendelse

Virksomhetens rutiner for hendelses- og avvikshåndtering bør ha føringer for

- hva som skal rapporteres
- hvem som skal rapportere og når det skal rapporteres
- hvordan rapporteringen skal skje
- hvem som skal håndtere hva
- hvem som skal informeres om hva, inkludert varsling til myndigheter og responsmiljøer

**Husk:** Hendelser kan ha ulike årsaker. Det kan for eksempel være snakk om:

- Tilsiktede handlinger
- Uaktsomhet
- Uhell og ulykker
- Naturhendelser

## OH-1 Overvåking etter behov

Sikkerhetsovervåking er ett virkemiddel for å oppdage avvik og uønskede hendelser. Risikoeiere skal vurdere behov for overvåking av systemer og tjenester innenfor sitt ansvarsområde, og sørge for at nødvendig overvåking iverksettes. Vurderingen skal være basert på foranalysen av ansvarsområdet og vurdering av risiko.

Omfanget av slik overvåkning må være lovlig, strengt nødvendig og forholdsmessig. I tillegg må det tas hensyn til kostnadene ved overvåkingen, risikoen for hendelser og avvik, samt i hvilken grad overvåkingen er egnet til å redusere denne risikoen.

Hva som skal overvåkes, hvordan overvåkingen skal gjennomføres og hvor lenge opplysningene skal lagres, må dokumenteres. Det finnes anbefalinger til hva som bør overvåkes i relevante ramme- og regelverk.

**Gir evne til**

- å oppdage uønskede hendelser, håndtere de og redusere konsekvensene ved slike hendelser

## OH-2 Følge opp hendelser og avvik

Risikoeier skal sørge for at meldinger om hendelser og avvik på sitt ansvarsområde blir håndtert. Varsel om hendelser kan komme fra interne og eksterne kilder.

Ledere på alle nivåer skal sørge for at hendelser og identifiserte avvik brukes som grunnlag for læring.

**Gir evne til**

- å unngå eller redusere negative konsekvenser for virksomhetens oppgaver og tjenester
- å lære av hendelser
- å forbedre styringsaktiviteter, sikkerhets- og personverntiltak
- å varsle myndigheter og responsmiljøer

## OH-3 Varsling ved hendelser

Virksomheten skal varsle ved brudd på informasjonssikkerhet eller personopplysningssikkerhet der regelverk stiller krav til dette. Det kan inkludere varsling til

- Datatilsynet uten ugrunnet opphold og senest innen 72 timer, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter
- de registrerte uten ugrunnet opphold, dersom det er sannsynlig at bruddet vil medføre en høy risiko for fysiske personers rettigheter og friheter
- sikkerhetsmyndigheten og andre ved brudd eller mulighet for brudd i henhold til Sikkerhetsloven
- myndigheter i henhold til Digitalsikkerhetsloven, første varsel innen 24 timer
- relevante sektormyndigheter og responsmiljøer
- andre relevante berørte aktører
- politiet (anmeldelse eller tips) der det er relevant

**Gir evne til**

- å etterleve varslingsplikter i regelverk
- å etablere dialog med relevante myndigheter, responsmiljøer og andre berørte
- å understøtte myndigheters overordnede situasjonsforståelse og underlag til å reagere i en større sammenheng

## OH-4 Beredskap og krisehåndtering

Ledere på alle nivå skal sørge for beredskap for å være i stand til å redusere konsekvensene av hendelser. Virksomhetsledelsen må sørge for at det er klare føringer for når en hendelse defineres som en krise, og hvilke prosedyrer som da iverksettes. Prosedyrene må beskrive klare ansvarslinjer og nødvendig samordning, og være tilgjengelig i en krisesituasjon, slik at alle kjenner sitt ansvar og kan utføre sine oppgaver.

Beredskapsarbeid og krisehåndtering baseres på

- ansvarsprinsippet
- likhetsprinsippet
- nærhetsprinsippet
- samvirkeprinsippet

Det bør etableres beredskaps- og kriseplaner for ulike virksomhetskritiske arbeidsoppgaver og funksjoner.

**Følg Direktoratet for samfunnssikkerhet og beredskap (DSB) sine råd om egenberedeskap for virksomheter:**

1) Kartlegg kritiske områder
2) Vurder konsekvensene av forstyrrelser eller stans
3) Skaff oversikt over avhengigheter
4) Gjennomfør tiltak for å sikre drift
5) Ha en plan for gjenoppretting og normalisering

https://www.dsb.no/ros-og-beredskap/beredskap-og-krisehandtering/rad-om-egenberedskap-for-virksomheter/

### Gir evne til

- å reagere raskt ved hendelser med betydelige konsekvenser
- å opprettholde viktige oppgaver og tjenester
- å redusere konsekvens av hendelser

# KK – Kompetanse- og kulturutvikling

Informasjonssikkerhet og personopplysningsvern involverer mange roller og krever ulike typer kompetanse, fra virksomhetsstyring og risikostyring til regelverkforståelse, tiltak og teknisk innsikt.

Virksomhetens leder har ansvaret for at medarbeidere har riktig kompetanse, og at virksomheten har en kultur preget av forståelse for hva som skal oppnås innen informasjonssikkerhet og personopplysningsvern.

Ledere på alle nivå skal

- sørge for at risikoeiere får hensiktsmessig grunnopplæring
- identifisere og følge opp behov for kompetanseheving og kulturutvikling
- bidra til at øvelser gjennomføres i tilstrekkelig omfang

## KK-1 Gi grunnopplæring til risikoeiere

Risikoeiere må ha tilstrekkelig kunnskap for å kunne styre informasjonssikkerhet og personopplysningsvern på sitt ansvarsområde.

Ledelsen skal sørge for at risikoeiere har tilstrekkelig forståelse av

- hvordan informasjonssikkerhet og personopplysningsvern skal styres
- hvordan innebygd personvern skal ivaretas
- hvilke oppgaver de har ansvaret for

Risikoeierne må få hensiktsmessig opplæring i de oppgavene de har ansvaret for gjennomføringen av. De bør få informasjon om hvor de kan få hjelp og støtte i arbeidet.

**Gir evne til**

- Å ha godt informerte risikoeiere som kan arbeide effektivt med risikostyring
- Å tilpasse seg endringer i eksterne og interne rammebetingelser

## KK-2 Identifisere og følge opp behov

Ledere på alle nivå skal systematisk identifisere og følge opp behov for kompetanse- og kulturutvikling innen informasjonssikkerhet og personopplysningsvern. Både individuelle og organisatoriske behov skal følges opp.

Behovene bør identifiseres gjennom ulike aktiviteter, inkludert

- risikovurderinger
- revisjoner, evalueringer og kartlegginger
- virksomhetsledelsens gjennomgang
- erfaring fra øvinger eller hendelseshåndtering
- plikter pålagt i lov eller avtale

Tiltak som skal dekke identifiserte behov, skal være tilpasset målgruppen.

**Gir evne til**

- at ledere og medarbeidere har forståelse for hva som skal oppnås, og har vilje og evne til å få det til
- forståelse for den enkeltes rolle i styring av informasjonssikkerhet og personopplysningsvern
- effektiv bruk av ressurser til kompetanse- og kulturutvikling, ved at tiltak iverksettes der det er størst behov

## KK-3 Øvelser

Ledere på alle nivå skal sørge for at øvelser blir prioritert og gjennomført.

Øvelser skal gjennomføres i tilstrekkelig omfang minst årlig for å

- øke kompetansen og kunnskapen til de ansatte, og gi dem trening i å samarbeide både i virksomheten og med andre relevante aktører
- avdekke behov for kompetanse- og kulturutvikling
- avdekke eventuelle ressursbehov

Omfang og innretning av øvelsene skal være tilpasset virksomheten og området det øves innenfor. Øvelser skal evalueres og følges opp i etterkant, for å sørge for god læring og å identifisere behov for forbedring.

**Gir evne til**

- god beredskap som sikrer effektiv håndtering av hendelser
- å ha ansatte som er forberedt på å håndtere reelle hendelser
- å samarbeide om håndtering av hendelser internt og med eksterne aktører
- å forbedre arbeidet gjennom praktisk erfaring, og ha en kultur preget av kontinuerlig læring

# AL – Anskaffelser og leverandørstyring

Virksomheten skal ivareta krav til informasjonssikkerhet og personopplysningsvern i anskaffelser. Dette innebærer å vurdere hvilke krav som skal gjelde for leverandørene innenfor leveransens omfang, om leverandørene tilfredsstiller kravene, og sørge for at disse kravene følges opp og helhetlig og aktivt forvaltes gjennom hele leveransens levetid. Gjennom tydelige kontraktskrav, risikovurderinger, revisjoner og tett samarbeid med leverandørene, skal virksomheten oppnå en robust og effektiv styring av risiko knyttet til anskaffelser.

Virksomheten skal bygge på eksisterende sikkerhetstiltak og fellessikring, supplert med spesifikke krav tilpasset den enkelte anskaffelse. Slik sikres en helhetlig tilnærming som både dekker virksomhetens behov, og legger til rette for kontinuerlig forbedring.

Virksomheten skal sørge for at anskaffelses - og leverandørstyringsprosesser er i samsvar med regelverk og avtaler.

## AL-1 Identifisere behov

Risikoeier skal vurdere hvordan risiko for oppgaver og tjenester endrer seg ved anskaffelse av en tjeneste som leveres av en tredjepart. Dette innebærer også å evaluere risiko knyttet til leverandører, og deres underleverandører, og deres evne til å oppfylle krav til informasjonssikkerhet og personopplysningsvern.

Basert på føringene fra virksomhetsledelsen, skal risikoeier definere og tilpasse krav til informasjonssikkerhet og personopplysningsvern.

For den enkelte anskaffelse, vil en vurdering av risiko knyttet til oppgaven tjenesten skal inn i, og tjenesten i seg selv, benyttes for å definere spesifikke krav til den aktuelle leveransen. I tillegg bør behov for kompetansebyggende tiltak i virksomheten identifiseres – både med tanke på oppfølging av leveransen, og for å ta i bruk det som anskaffes.

Følgende bør dokumenteres:

- risikovurderinger knyttet til anskaffelser som kan brukes som beslutningsgrunnlag for håndtering av risiko
- behov for kompetansebyggende tiltak i virksomheten

***Tips:*** Ta utgangspunkt i virksomhetens fellessikring, og behovet for samhandling i styringsaktivitetene når krav defineres - for eksempel vurdering og håndtering av risiko, og overvåking og hendelseshåndtering.

Vurder hvilke tiltak i fellessikringen leverandøren vil ha ansvaret for, hvilke dere selv må ivareta, og hvilke det vil være delt ansvar for.

For anskaffelser som gjøres ofte vil denne vurderingen kunne gjøres én gang, og gjenbrukes.

**Gir evne til**

- å vurdere risiko ved anskaffelse av en leverandørtjeneste.
- å stille krav til leverandører og tjenester, og ha dialog med leverandører i hele leveransens levetid
- kompetansestyring – hva gjør leverandøren, og hva må virksomheten selv ha av kompetanse
- å evaluere leverandørens evne til å opprettholde informasjonssikkerhet og personopplysningsvern i samsvar med virksomhetens krav.
- å ta velinformerte beslutninger om samarbeid med leverandører.

## AL-2 Håndtere risiko og stille krav

Risikoeier skal sørge for at risiko håndteres i forbindelse med anskaffelser av tjenester med betydning for informasjonsbehandlingen i virksomheten.

På samme måte som i **Håndtering av risiko (RH),** så skal risikoeiere sørge for at det utarbeides forslag til hvordan risiko skal håndteres, og ta beslutninger om hvilke forslag som skal følges. Sikkerhets- og personverntiltak som leverandøren skal ha helt eller delvis ansvar for, må inkluderes i kontrakter med leverandører. Leverandørens forpliktelser både i normalsituasjon og under kriser bør beskrives.

Virksomheten må sørge for at etterlevelse av kravene kan kontrolleres.

Aktiviteten gir en liste med sikkerhetskrav som kan pålegges leverandører gjennom kontrakter, og danner beslutningsgrunnlag for valg av leverandører.

Håndtering av risiko i anskaffelser kan inkludere å:

- opprettholde fellessikringen, ved at leverandør har ansvar for relevante deler av denne i tjenesteleveransen
- sette krav til nye sikkerhets- og personverntiltak som leverandører skal ha ansvaret for
- inngå databehandleravtaler med leverandører
- etablere nye sikkerhets- og personverntiltak i egen virksomhet
- akseptere ny risiko

**Gir evne til å**

- redusere virksomhetens risiko og sårbarheter i leverandørkjeden

## AL-3 Vurdering av leverandører

Risikoeier skal vurdere leverandørenes evne til å oppfylle virksomhetens krav til informasjonssikkerhet og personopplysningsvern. Vurderingen skal gi beslutningsgrunnlag for valg av leverandører, og brukes i den videre leverandørstyringen. Virksomheten bør også vurdere

leverandørens arbeid med informasjonssikkerhet og personopplysningsvern. Ved behov skal også eierskapsforhold og fysisk beliggenhet være en del av vurderingen.

Vurderingene skal sikre at valgte leverandører kan ivareta virksomhetens informasjonssikkerhet og arbeid med personopplysningsvern, overholde regelverk og bidra til en trygg leverandørkjede.

Vurderingene skal dokumenteres.

**Gir evne til å**

- velge leverandører som kan levere tjenester iht. behovet for informasjonssikkerhet og personopplysningsvern

## AL-4 Oppfølging av leverandører

Virksomheten skal regelmessig følge opp tjenesteleverandørens evne til å følge kontraktfestede krav. I tilfeller hvor man oppdager tjenesteavvik, brudd på kontrakt og lignende, skal virksomheten håndtere disse avvikene.

Virksomheten bør etablere og opprettholde et kommunikasjons-/kontaktpunkt hos sine leverandører, for å enklere følge opp status, problemstillinger og utfordringer.

Ved avvik eller mangler hos leverandører skal det utarbeides og gjennomføres handlingsplaner for å utbedre det.

**Gir evne til å**

- overvåke og bekrefte leverandørens overholdelse av avtalte krav
- bygge tillit mellom virksomheten og leverandørene gjennom transparens og samarbeid

## AL-5 Holde helhetlig oversikt over leverandører

Virksomheten skal sørge for å holde oversikt over alle leverandører virksomheten benytter.

Virksomheten skal dokumentere en helhetlig og systematisk vurdering av informasjonssikkerhet, personopplysningsvern og avhengigheter til tjenesteleveranser, tjenesteleverandører og leverandørkjeder. Basert på denne vurderingen skal virksomheten jobbe for å redusere risiko i leverandørkjeden og avhengighet til tredjeparter, og bygge robusthet i tilfelle leverandører opplever en uønsket hendelse.

> ***Tips:*** En helhetlig oversikt kan brukes til å sortere leverandører i grupper eller kategorier, basert på kritikalitet og omfang. Kategoriseringen av leverandører kan brukes til å prioritere ressursbruk på leverandøroppfølging.

**Gir evne til å**

- vurdere og håndtere risiko knyttet til leverandørkjeder
- gjøre prioriteringer i arbeid med oppfølging av leverandører

- få oversikt over hvordan virksomhetens oppgaver og tjenester er avhengig av eksterne leverandører og underleverandører

# KO – Kommunikasjon

Ledere på alle nivå skal sørge for god og tydelig kommunikasjon, som setter virksomheten i stand til å jobbe helhetlig med informasjonssikkerhet og personopplysningsvern.

Dokumentasjon er en viktig del av dette. Det skal være lett å utforme og vedlikeholde dokumentasjon, og mulig å kontrollere etterlevelse når det er behov for det. Informasjon skal være lett tilgjengelig for de som har behov for den.

Ledere på alle nivå skal sørge for at

- føringer formidles til de som har behov for dem
- gjennomførte styringsaktiviteter dokumenteres
- det utarbeides hensiktsmessig underlagsdokumentasjon til styringsaktivitetene
- dialog med styrende organ ivaretas på en god måte

## KO-1 Formidle føringer

Virksomhetsledelsen og ledere på alle nivå skal formidle føringer innen sitt ansvarsområde raskt og effektivt.

Ledere på alle nivå skal vurdere behovet for veiledning og andre kompetansetiltak for å formidle og sørge for at føringene er forstått og etterleves.

**Gir evne til**

- å gi alle ansatte på alle nivå tilstrekkelig kunnskap, forståelse og evne til å følge føringene.

## KO-2 Dokumentere gjennomførte styringsaktiviteter

Ledere på alle nivå, og andre som gjennomfører styringsaktiviteter, skal sørge for tilstrekkelig dokumentasjon av gjennomføring og resultater.

Risikoeier skal dokumentere gjennomføring av styringsaktiviteter, inkludert:

- Foranalyse av eget ansvarsområde
- Vurdering av behov for risikovurderinger
- Resultater av risikovurderinger
- Beslutninger om håndtering av risiko, inkludert finansiering
- Vurdering av status på eget ansvarsområde
- Vurdering av effektivitet av sikkerhets- og personverntiltak
- Resultater fra evalueringer og revisjoner
- Gjennomført kompetanseheving
- Gjennomførte øvelser
- Gjennomførte anskaffelser
- Oppfølging av leverandører

**Gir evne til**

- å kunne revurdere, evaluere eller etterprøve beslutninger

- å dokumentere etterlevelse av interne og eksterne krav
- å lære av hva andre har gjort før deg
- å dokumentere gjennomførte styringsaktiviteter til tilsyn, myndigheter og andre

## KO-3 Utarbeide underlagsdokumentasjon

Virksomhetsledelsen skal sørge for at det utarbeides underlagsdokumentasjon til bruk i ulike styringsaktiviteter, blant annet virksomhetsledelsens gjennomgang, foranalyse av ansvarsområder, og vurdering av risiko. Underlagsdokumentasjonen skal gi støtte til virksomhetsledelsen og risikoeierne i gjennomføring av aktivitetene.

**Gir evne til**

- faktabasert arbeid med styringsaktiviteter
- å ta gode beslutninger

## KO-4 Dialog med styrende organ

Virksomhetsledelsen skal sørge for at informasjonssikkerhet og personopplysningsvern er en del av dialogen med virksomhetens styrende organ.

Styringsinformasjon til styrende organ bør basere seg på informasjonen som utarbeides til og benyttes i virksomhetsledelsens gjennomgang: Kunnskap om risiko knyttet til oppgaver og tjenester, og status og modenhet på arbeidet med informasjonssikkerhet og personopplysningsvern.

**Gir evne til**

- å gi styrende organ nødvendig innsikt i status, risiko og ressursbruk på områdene informasjonssikkerhet og personopplysningsvern, og dens betydning for virksomhetens evne til å levere oppgaver og tjenester
- å styrke tillit og dialog mellom virksomheten og styrende organ
- å etterleve krav til rapportering om styring og kontroll