***(Kommentarer og noen råd er skrevet i gult innledningsvis og underveis i dokumentet.***

*Dette eksempelet dekker «alle» internkontrollområder. Det har denne formen for å synlig­gjøre hvordan internkontroll og sikkerhetsarbeid innen informasjonssikkerhet kan integreres med andre områder der det er naturlig. Dette anbefaler vi som primær tilnærming, jf.* [*eForvaltningsforskriften §15*](https://lovdata.no/dokument/SF/forskrift/2004-06-25-988/KAPITTEL_2#KAPITTEL_3)*, om at internkontrollen på informasjonssikkerhetsområdet «bør være en integrert del av virksomhetens helhetlige styringssystem», og sikkerhetsloven § 4-1 om at sikkerhetsarbeidet etter loven skal være en del av virksomhetens styringssystem.*

*Endelig omfang og utforming av dokumentet må sees i sammenheng med de styringsdokumenter virksomheten har fra før på ulike områder. Dersom man ønsker å avgrense dokumentet til kun informasjons­sikkerhet eller for noen færre områder, kan eksempelet enkelt snevres inn ved å ta bort enkelte punkter og spisse andre. Det er kommentert under.* ***De som gjenbruker sentrale deler av eksempelet, er selv ansvarlig for kvalitetssikring av innholdet og tilpasning til egen virksomhet.***

*Dokumentet er av typen retningslinje. Man kan navngi og strukturere både policyer, retningslinjer mv. på flere måter. Alternative måter er bl.a. beskrevet i DFØs «*[*Veiledning - policy for internkontroll*](https://dfo.no/Documents/FOA/publikasjoner/veiledere/internkontroll/Veiledning%20-%20policy%20for%20internkontroll.docx)*» og «*[*Veiledning - dokumentasjon av etablert internkontroll*](https://dfo.no/Documents/FOA/publikasjoner/veiledere/internkontroll/Veiledning%20-%20dokumentasjon%20av%20etablert%20internkontroll_uten%20eksempel%20og%20track%20changes.docx)*», jf.* [*DFØs verktøy for intern­kontroll*](https://dfo.no/fagomrader/internkontroll/verktoy/)*.*

*Dersom man velger alternative dokument­strukturer eller alternative tilnærminger til innholdet, bør man fra et informasjonssikkerhetsperspektiv sikre det detaljeringsnivå og den systematikk som er gjenspeilet i eksempelet under. For de som velger eller har andre godt fungerende strukturer på dokumenter og innhold, kan eksempelet under benyttes som inspirasjon til forbedringer.)*

Innhold

[1. Innledning 2](#_Toc465608870)

[1.1 Målgruppe 2](#_Toc465608871)

[1.2 Formål 2](#_Toc465608872)

[1.3 Relaterte policyer og retningslinjer 2](#_Toc465608873)

[1.4 Detaljeringsnivå og utdypninger 2](#_Toc465608874)

[1.5 Forklaringsmodell internkontroll 2](#_Toc465608875)

[2. Organisering og rapportering 3](#_Toc465608876)

[2.1 Grunnleggende prinsipp 3](#_Toc465608877)

[2.2 Linjen som hovedføring 3](#_Toc465608878)

[2.3 Spesielle funksjoner 3](#_Toc465608879)

[3. Direktørens særskilte ansvar 4](#_Toc465608880)

[4. Ledere på alle nivå 5](#_Toc465608881)

[5. Ledere på operativt nivå (risikoeiere) 6](#_Toc465608882)

[6. Systemeiere fellessystem 7](#_Toc465608883)

[7. Tiltaksleverandører 8](#_Toc465608884)

[8. Alle ansatte 9](#_Toc465608885)

[9. Spesialfunksjoner 9](#_Toc465608886)

[9.1 Fagansvarlig internkontroll 10](#_Toc465608887)

[9.2 Økonomisjef 10](#_Toc465608888)

[9.3 Fagansvarlig informasjonssikkerhet 10](#_Toc465608889)

[9.4 Fagansvarlig personvern 11](#_Toc465608890)

[9.5 Personvernombud 11](#_Toc465608891)

[9.6 Fagansvarlig HMS 11](#_Toc465608892)

[9.7 Kvalitetssjef 12](#_Toc465608893)

[9.8 Lokale sikkerhetskoordinatorer 12](#_Toc465608894)

[9.9 Prosessledere risikovurdering og risikohåndtering 12](#_Toc465608895)

[10. Faste fora med roller i internkontroll- og sikkerhetsarbeidet 12](#_Toc465608896)

[Toppledergruppen 13](#_Toc465608897)

[Avdelingsledergrupper 13](#_Toc465608898)

[Sikkerhetsutvalget 13](#_Toc465608899)

[Forum tiltaksleverandører 13](#_Toc465608900)

[Forvaltergruppe IKT-system 13](#_Toc465608901)

[Ressursgruppe lokale sikkerhetskoordinatorer 13](#_Toc465608902)

[Ressursgruppe prosessledere 13](#_Toc465608903)

# Innledning

## Målgruppe

Dette dokumentet er en del av virksomhetens overordnede styrende dokumenter. Målgruppen er alle ansatte.

## Formål

Formålet er å klargjøre roller og ansvar i direktoratet med hensyn til internkontroll og sikkerhetsrelatert arbeid. Dette dekker både mål og resultatkrav, økonomistyring, informasjonssikkerhet, HMS, personvern, regelverksetterlevelse forøvrig, bygningssikkerhet, verdisikkerhet mv. (Områder fjernes dersom man ønsker et avgrenset omfang på dokumentet, f.eks. kun til informasjonssikkerhet.)

Dokumentet skal sikre tilstrekkelig internkontroll (styring og kontroll). Direktoratets sikkerhetsarbeid er en del av dette. Rollefordelingen synliggjør dermed direktoratets sikkerhetsorganisasjon.

## Relaterte policyer og retningslinjer

Dokumentet må sees i sammenheng med følgende:

* Policy for informasjonssikkerhet
* (Eventuelt tilsvarende policydokument for andre internkontrollområder)
* Retningslinjene
	+ Forstå, vurdere og håndtere risiko
	+ (Eventuelt tilsvarende for risiko på strategisk og taktisk nivå)
	+ Vurdere behov for risikovurderinger (eventuelt spesifisert for hvilke områder)

## Detaljeringsnivå og utdypninger

Dokumentet inneholder en kort beskrivelse av overordnede ansvars- og myndighets­forhold. Utdypninger og presiseringer kan ved behov legges i utdypende retningslinjer, beskrivelser av sikkerhets­tiltak, stillingsbeskrivelser og veiledninger. Presiseringer kan også være nedfelt i lov- og regelverk.

## Forklaringsmodell internkontroll

Vårt arbeidet med internkontroll er basert på forklaringsmodellen under. I dokumentet er det gjennomgående referert til de hovedaktivitetene som er nevnt i modellen. (Eller en alternativ forklaringsmodell, f.eks. fra DFØ, dersom det anses mer formålstjenlig. Da må kanskje navn på aktiviteter det refereres til endres utover i dette eksempelet for å få henvisningen konsistent med forklaringsmodellen.)


# Organisering og rapportering

## Grunnleggende prinsipp

Internkontroll- og sikkerhetsarbeidet i direktoratet skal være basert på

* ansvarsprinsippet
* likhetsprinsippet
* nærhetsprinsippet
* samvirkeprinsippet

Dette innebærer at den ordinære linjen er det bærende element i internkontroll- og sikkerhetsarbeidet, og at risiko- og sikkerhetsspørsmål i størst mulig grad skal håndteres som linjeaktiviteter for øvrig. Samtidig har alle i direktoratet et selvstendig ansvar for å sikre best mulig samvirke med andre relevante aktører, organisatoriske enheter og virksomheter.

## Linjen som hovedføring

Ansvar, myndighet og rapportering for internkontroll- og sikkerhetsarbeid skal som hovedregel følge linjen. Det innebærer følgende hierarki:

* Direktør
* Avdelingsdirektører
* Seksjonssjefer
* Ansatte for øvrig

Ansvar for prosjekter skal være koblet til en organisatorisk enhet i linjen. Det er denne det skal rapporteres til også i internkontroll- og sikkerhetsspørsmål.

Etablerte system for avviks- og hendelseshåndtering skal benyttes i rapporteringen for den type avvik og hendelser disse dekker.

Håndtering av kriser og hendelser med egne prosedyrer, skal skje i samsvar med de planer og prosedyrer som er etablert.

## Spesielle funksjoner

Fellesfunksjoner, støttefunksjoner og samarbeidsgrupper skal ha tydelige roller og ansvar og understøtte linjelederne rundt om i virksomheten.

Rapportering skal som hovedregel skje gjennom den linjen spesialfunksjonene tilhører. Samarbeidsgrupper skal rapportere gjennom den linjen gruppeleder tilhører. Noen funksjoner kan ha direkte rapportering til direktør på enkelte områder. Det skal fremgå av funksjonsbeskrivelsen.

# Direktørens særskilte ansvar

Direktør er ansvarlig for at det blir gjennomført tilstrekkelige risikovurderinger på strategisk nivå. Disse må dekke virksomhetens overordnede måloppnåelse, effektiv organisering, forsvarlig økonomi­styring, etterlevelse av lover og regler og pålitelig rapportering. Direktør er også ansvarlig for at nødvendige risikoreduserende tiltak blir identifisert, iverksatt og fulgt opp i organisering og styring av virksomheten. Tiltak skal være tilpasset risiko og vesentlighet.

(Avsnittet over gjelder risikostyring på strategisk nivå. Det faller normalt utenfor det internkontrollperspektivet man har innen informasjonssikkerhet og andre operative områder. For å skape en helhet i virksomhetens samlede internkontrollarbeid og styringssystem, kan et avsnitt som dette være med her, ev. i en annen variant. Avsnittet over fjernes dersom dette dokumentet avgrenses til informasjonssikkerhet.)

Direktør er i tillegg ansvarlig for at virksomhetens arbeid med internkontroll og sikkerhet gjennomføres på en systematisk og tilstrekkelig omfattende måte rundt om i hele virksomheten. Arbeidet skal være tilpasset risiko og vesentlighet.

Grunnlaget for dette er at direktør har sørget for at

* virksomheten har nødvendige føringer for arbeidet og at disse har tilstrekkelig kvalitet
* andre nødvendige etableringsaktiviteter er gjennomført

Som del av ledelsens styring og oppfølging er direktør spesielt ansvarlig for gjennomføring av virksomhets­ledelsens gjennomgang på områdene

* mål og resultatkrav
* økonomistyring
* informasjonssikkerhet
* kvalitetskrav
* HMS
* etterlevelse av personvernregelverket
* etterlevelse av annet relevant regelverk

Omfang og innretning skal være tilpasset risiko og vesentlighet. Gjennomganger på to eller flere områder kan slås sammen når det anses nyttig og forsvarlig for å ha tilstrekkelig styring og kontroll.

(Områder over fjernes dersom man ønsker et avgrenset omfang på retningslinjen, f.eks. kun til informasjonssikkerhet.)

Virksomhetsledelsens gjennomgang skal utføres 1 - 4 ganger årlig avhengig av områdenes egenart, status, risiko og vesentlighet. Gjennomgangene skal inngå i den ordinære virksomhetsstyringen og synliggjøres i virksomhetens styringshjul. Hele toppledergruppen skal som hovedregel delta i virksomhetsledelsen gjennomgang.

Ved behov skal direktør

* sørge for at det skjer en forbedring av overordnede styrende dokumenter
* gi eventuelle tilleggsføringer for virksomhetens internkontroll- og sikkerhetsarbeid
* stille og følge opp spesifikke krav til enkelte ledere og enheter
* vurdere om man skal måle tilstanden på definerte indikatorer over tid, og eventuelt få iverksatt slike målinger
* vurdere om man skal få gjennomført evalueringer, og eventuelt få iverksatt slike
* vurdere om man skal få gjennomført internrevisjon, og eventuelt få iverksatt slike

Eventuell gjennomføring av de tre siste er en del av virksomhetens måling, evaluering og revisjon.

Dokumentasjon av ovennevnte skal skje skriftlig i de arkivløsninger som er etablert for formålet. Det skjer normalt gjennom saksnotat og møtereferat med tydelige beslutninger fra direktør.

# Ledere på alle nivå

Ledere på alle nivå er ansvarlig for at det blir gjennomført tilstrekkelige risikovurderinger av taktisk karakter i og under eget ansvarsområde. Disse må dekke hva som må gjøres for å nå de mål og resultatkrav de er ansvarlige for, samt å ha en effektiv organisering, forsvarlig økonomistyring, pålitelig rapportering og etterleve lover og regler. Lederne er også ansvarlig for å identifisere, iverksette og følge opp nødvendige risikoreduserende tiltak. Tiltak skal være tilpasset risiko og vesentlighet.

(Avsnittet over gjelder risikostyring på taktisk nivå. Det faller normalt utenfor det internkontrollperspektivet man har innen informasjonssikkerhet og andre operative områder. For å skape en helhet i virksomhetens samlede internkontrollarbeid og styringssystem, kan et avsnitt som dette være med her, ev. i en annen variant. Avsnittet over fjernes dersom dette dokumentet avgrenses til informasjonssikkerhet.)

Ledere på alle nivå har også det overordnede ansvaret for oppgaveløsning, tjenesteutføring, informasjons­behandling, HMS, regelverksetterlevelse, eiendelene mv. under eget ansvarsområde. Det operative ansvaret som risikoeiere for dette, er normalt delegert til laveste ledernivå, jf. pkt. 5. (Områder fjernes dersom man ønsker et avgrenset omfang på dokumentet, f.eks. kun til informasjonssikkerhet.)

Ved behov for effektivisering og samordning skal overordnet leder ta stilling til hvilke mål, områder, risikovurderinger og risikoer som eventuelt skal vurderes og håndteres på et høyere organisatorisk nivå enn det som følger av normal delegering.

For å sikre tilstrekkelig internkontroll med risikoene i det operative arbeidet, jf. pkt. 5, har leder på alle nivå viktige oppgaver knyttet til aktivitetene

* ledelsens styring og oppfølging
* måling, evaluering og revisjon

Dette må dekke områdene

* informasjonssikkerhet
* kvalitetskrav
* HMS
* etterlevelse av personvernregelverket
* etterlevelse av annet relevant regelverk

(Områder over fjernes dersom man ønsker et avgrenset omfang på dokumentet, f.eks. kun til informasjonssikkerhet.)

Som del av ledelsens styring og oppfølging skal ledere på alle nivå systematisk

* delegere og følge opp internkontroll- og sikkerhetsarbeidet gjennom linjen
* sikre finansielle rammer for internkontroll- og sikkerhetsarbeidet
* kommunisere viktigheten av internkontroll- og sikkerhetsarbeidet
* håndtere problemstillinger løftet gjennom linjen
* ha planer for og trening i relevant beredskap og krisehåndtering

Som del av måling, evaluering og revisjon skal ledere på alle nivå minst en gang årlig systematisk vurdere status på eget ansvarsområde. Det omfatter en reell vurdering av

* om sikkerhetstiltak de har ansvaret for fungerer som forutsatt
* om de selv og de personer de har ansvaret for
	+ følger gjeldende lov- og regelverk
	+ gjennomfører pålagte oppgaver i internkontroll- og sikkerhetsarbeidet på en tilfredsstillende måte,
	+ etablerer og følger opp vedtatte eller avtalte sikkerhetstiltak
	+ etterlever innførte sikkerhetstiltak

Ved vesentlig usikkerhet på punktene over skal lederne gjennomføre nærmere undersøkelser av status. Dette kan være enkle undersøkelser eller mer omfattende evalueringer avhengig av områdets egenart. Ved vesentlige avvik og mangler skal tiltak iverksettes for å rette opp forholdene.

Ledernes ansvar under måling, evaluering og revisjon omfatter også ansvaret for å sikre gjennomføring av lovpålagte eller avtalte systemgjennomganger, systemrevisjoner o.l. Disse kan i prinsippet gjennomføres som evalueringer tilpasset aktuelle pålegg og avtaler.

Arbeidet over skal så langt det er hensiktsmessig integreres i den ordinære linjestyringen.

Der det ikke er klart uhensiktsmessig, skal dokumentasjon skje skriftlig i de arkivløsninger som er etablert for formålet. Med unntak for beredskap og krisehåndtering, samt spesielle evalueringer og standardisert rapportering, vil et kort notat ofte være nok.

# Ledere på operativt nivå (risikoeiere)

I samsvar med de grunnleggende prinsippene, jf. pkt. 2.1, vil ansvaret som risikoeier på operativt nivå normalt være delegert til laveste ledernivå. Det overordnede ansvaret blir alltid liggende igjen i linjen, jf. pkt. 4.

Operative risikoer omfatter uønskede hendelser og konsekvenser i den operative utføringen av oppgaver og tjenester.

Ansvaret til risikoeierne omfatter oppgaveløsning, tjenesteutføring, informasjons­behandling, HMS, regelverksetterlevelse, eiendelene, mv. under eget ansvarsområde. (Områder fjernes dersom man ønsker et avgrenset omfang på dokumentet, f.eks. kun til informasjonssikkerhet.)

Gjennom aktiviteten risikovurdering skal risikoeiere sørge for at de systematisk får

* etablert og vedlikeholdt tilstrekkelig oversikt over eget ansvarsområde, og gruppert og prioritert nødvendige risikovurderinger
* tilstrekkelig kjennskap til relevante lover, regler og avtaler, og identifisert konkrete krav som må følges opp
* planlagt og gjennomført nødvendige risikovurderinger
* risikovurdert ved behov i oppfølging av hendelseshåndteringen
* risikovurdert ved anskaffelser og utvikling

Oversikt og vurderinger skal hver for seg, eller i hensiktsmessige kombinasjoner, dekke risikoer som omfatter brudd på

* informasjonssikkerhet (konfidensialitet, integritet, tilgjengelighet)
* kvalitetskrav
* HMS
* etterlevelse av personvernregelverket
* etterlevelse av annet relevant regelverk,

samt de konsekvenser slike brudd kan få.

(Områder over fjernes dersom man ønsker et avgrenset omfang på dokumentet, f.eks. kun til informasjonssikkerhet.)

Som del av aktiviteten risikohåndtering skal risikoeiere sørge for at de får

* foreslått håndtering av risikoer fra risikovurderinger
* godkjent forslag til risikohåndtering
* iverksatt godkjente tiltak

Arbeidet skal skje i tilstrekkelig omfang og detaljeringsnivå innenfor gjeldende retningslinjer og krav.

Valg av risikoreduserende tiltak skal være basert på risiko, vesentlighet, nytte-kost vurderinger og ledelsens føringer for risikohåndtering og et effektivt sikkerhetsarbeid.

Ansvaret omfatter også IKT-system og annet teknisk utstyr som kun understøtter risikoeiernes oppgaver og tjenester og som de selv er systemeiere for. For fellessystem se pkt. 6.

Støtte kan gis av relevante spesialfunksjoner, jf. pkt. 9.

Iverksetting av tiltak i risikohåndteringen, skal ved behov avtales med virksomhetens felles tiltaksleverandører, jf. pkt.7. Enkelte tiltak kan også etableres og vedlikeholdes av risikoeierne selv, jf. pkt.7.

Ansvaret til risikoeiere omfatter også å sikre tilstrekkelig overvåking og hendelseshåndtering, kompetanse- og kulturutvikling og kommunikasjon rundt risikoer i eget ansvarsområde. Der det er pålagt eller hensiktsmessig skal dette skje innenfor felles systematikk og felles støttesystem i direktoratet.

Dokumentasjon skal som hovedregel skje skriftlig i de maler, støtteverktøy og arkivløsninger som er etablert for formålet.

Risikoeiere skal til enhver tid vedlikeholde en oppdatert oversikt over hvilke system de er systemeiere for, systemets formål, brukskrav og hvem som er kontaktpersoner. De skal systematisk registrere oversikten i vårt arkivsystem og publisert den på felles sted for formålet på vårt intranett.

# Systemeiere fellessystem

Alle IKT-system og annet teknisk utstyr som benyttes av flere risikoeiere kalles fellessystem. De skal ha en utpekt systemeier. Systemeiere fellessystem pekes ut av øverste ledernivå for de som benytter systemet. Styring, samordning og rapportering skal følge den linjen som systemeier fellessystem tilhører.

Systemeiere for fellessystem skal ivareta interessene til de som benytter systemene i sin oppgave­løsning og tjenesteutføring. Det presiseres at risikoeiere som bruker fellessystem, også er risikoeiere for egen bruk av fellessystemene. De skal derfor i tilstrekkelig grad og på hensiktsmessig måte involveres i risikovurderingsarbeid og andre internkontrollaktiviteter som utføres på fellessystemene. Både systemeiere fellessystem og risikoeierne selv har ansvaret for å sikre dette.

Systemeiere fellessystem har ansvar for de samme oppgavene for sine fellessystem som risikoeierne har for sine ansvarsområder. Se pkt. 5 for konkret oversikt over ansvar, oppgaver og dokumentasjonskrav. Støtte kan gis av relevante spesialfunksjoner, jf. pkt. 9.

# Tiltaksleverandører

Virksomheten har følgende felles tiltaksleverandører med ansvar for etablering, gjennomføring og systematisk kontroll med sikkerhetstiltakene innen sitt ansvarsområde.

| Område | Ansvarlig |
| --- | --- |
| Overordnede føringer | Seksjon for styring og kontroll i Direktørens stab |
| Personal | Seksjon for personalforvaltning i Administrasjonsavdelingen |
| Bygg | Seksjon for bygningsforvaltning i Administrasjonsavdelingen |
| IKT-drift | Seksjon for IKT-drift i Avdeling for IKT utvikling og drift |
| IKT-utvikling | Seksjon for IKT-utvikling i Avdeling for IKT utvikling og drift |
| IKT-anskaffelser | Seksjon for anskaffelser i Avdeling for IKT utvikling og drift |

I samsvar med de grunnleggende prinsippene, jf. pkt. 2, vil det operative ansvaret som felles tiltaksleverandør normalt være delegert til leder for de nevnte enhetene. Det overordnede ansvaret blir alltid liggende igjen i den linjen de tilhører.

I tillegg til ovennevnte kan følgende være tiltaksleverandører for egne ansvarsområder og systemer

* Risikoeiere
* Systemeiere fellessystem

Sikkerhetstiltakene de to siste har ansvar for vil ofte være organisering av det operative arbeidet, samt krav, prosedyrer, rutiner, kompetanse- og kulturutvikling o.l. knyttet til egne arbeidsoppgaver, tjenester og system.

Som del av aktiviteten risikohåndtering skal relevante tiltaksleverandører

* utforme og implementere avtalte og pålagte tiltak
* oppdatere virksomhetens fellessikring i dialog med Fagansvarlig informasjonssikkerhet, jf. pkt. 9.3.

Fellessikring er et sett av sikkerhetstiltak som er etablert for å gi et felles grunnleggende sikkerhetsnivå for sentrale områder av virksomheten. Øvrige tiltak tilpasset enkelte organisatoriske enheter eller systemer kalles tilleggssikring.

Fordelingen mellom hva som skal være henholdsvis fellessikring og tilleggssikring, skal styres av hva som gir best nytte-kost for virksomheten samlet. Man skal da ta hensyn til

* hvor mange som har vesentlig nytte av sikkerhetstiltaket
* omfanget av negative sideeffekter av tiltaket for risikoeiere med lav nytteverdi
* behovet for kostnadseffektiv drift av det samlede sikkerhetsarbeidet

Alle tiltaksleverandører skal ut fra dette systematisk vurdere hvilke tiltak som bør etableres som henholdsvis fellessikring og tilleggssikring. Mener de økt fellessikring er riktig, skal de kontakte fagansvarlig informasjonssikkerhet. Hun skal lede og koordinere arbeidet med å avgjøre omfanget av fellessikringen. Beslutning tas av den direktør utpeker.

Dokumentasjon av tiltaksleverandørenes risikohåndtering skal som hovedregel skje skriftlig i de maler, støtteverktøy og arkivløsninger som er etablert for formålet.

Som del av overvåking og hendelseshåndtering skal tiltakleverandørene

* overvåke i henhold til avtale
* rapportere relevante hendelser, avvik og informasjonssikkerhetsbrudd i henhold til gjeldende rutiner og forventninger
* følge opp ovennevnte der de har oppfølgingsansvaret

Der det er pålagt eller hensiktsmessig skal dette skje innenfor felles systematikk og felles støttesystem i direktoratet.

Ansvaret til tiltaksleverandørene omfatter også å sikre tilstrekkelig kompetanse- og kulturutvikling i egen enhet.

# Alle ansatte

Alle ansatte har et overordnet ansvar for å bidra til at direktoratet når våre samlede mål på en best mulig måte.

Alle ansatte skal ha et bevisst forhold til målene for eget arbeid, hvilken informasjon og hvilke verdier de behandler og hvilke krav som stilles til oppgavegjennomføring, tjenesteutføring, informasjons­behandling og bruk av IKT og annet utstyr.

Alle ansatte skal etterleve de lover, regler, retningslinjer, krav, rutiner mv. som gjelder for dem og det arbeid de utfører.

Uønskede hendelser og avvik skal meldes systematisk og uten ugrunnet opphold på den måten som er angitt i vårt system for hendelses- og avvikshåndtering. For øvrig skal rapportering skje gjennom linjen på ordinær måte.

# Spesialfunksjoner

Understående spesialfunksjoner er etablert for å understøtte internkontroll- og sikkerhets­arbeidet. Nærmeste leder for spesialfunksjonene skal til enhver tid vedlikeholde en oppdatert oversikt med navn på hvem som dekker funksjonene. De skal systematisk registrere oversikten i vårt arkivsystem og publisert den på felles sted for formålet på vårt intranett.

Én fysisk person kan dekke flere av funksjonene under, og også inneha noen av rollene over. Den som utpeker personer til spesialfunksjoner skal forsikre seg om at dette ikke går på bekostning av krav og behov for uavhengighet mellom funksjoner og roller.

(Første setning i avsnittet over er et svært viktig punkt for å få en effektiv organisering av det samlede internkontroll- og sikkerhetsarbeidet, spesielt i små og mellomstore virksomheter. I tillegg til å sikre nødvendig uavhengighet, vil virksomhetens størrelse, egenart og tilgjengelig kompetanse ha betydning for om en person bør og kan dekke flere av funksjonene under.

Eksempelet under skisserer en mulig helhetlig tilnærming til sentrale funksjoner, både ut fra ev. behov og ut fra [eForvaltningsforskriften § 15](https://lovdata.no/dokument/SF/forskrift/2004-06-25-988/KAPITTEL_2#KAPITTEL_3), som sier at internkontrollen på informasjonssikkerhetsområdet «*bør være en integrert del av virksomhetens helhetlige styringssystem*».

Det presiseres at ansvaret til funksjonene nevnt under er eksempler. Enkelte spesialfunksjoner under kan fjernes dersom de ikke anses relevante, f.eks. kvalitetssjef.

Flere av spesialfunksjonene under bør fjernes dersom dette dokumentet avgrenses til informasjonssikkerhet.)

## Fagansvarlig internkontroll

* Funksjon i Seksjon for styring og kontroll i Direktørens stab
* Ansvar for å
	+ støtte virksomhetsledelsen i internkontrollspørsmål generelt
	+ koordinere internkontroll- og kvalitetsarbeidet for alle områder og sikre et helhetlige internkontroll- og styringssystem i virksomheten
	+ etablere hensiktsmessige hjelpemidler for risikovurderinger på strategisk, taktisk og operativt nivå
	+ være en ressursperson, pådriver og tilrettelegger for en god etablering og risikobasert gjennomføring av virksomhetens internkontrollarbeid innen mål og resultatkrav, pålitelig rapportering og regelverksetterlevelse som ikke er dekket av spesialfunksjonene under
	+ utarbeide saksnotat til virksomhetsledelsens gjennomgang innen mål og resultatkrav, samt regelverksetterlevelse som ikke er dekket av spesialfunksjonene under

## Økonomisjef

* Leder av Seksjon for økonomistyring i Administrasjonsavdelingen
* Ansvar for å
	+ støtte virksomhetsledelsen innen økonomistyring
	+ koordinere eget arbeid med Fagansvarlig internkontroll
	+ være en ressursperson, pådriver og tilrettelegger for en god etablering og risikobasert gjennomføring av virksomhetens samlede økonomistyring
	+ utarbeide saksnotat til virksomhetsledelsens gjennomgang innen økonomistyring

## Fagansvarlig informasjonssikkerhet

* Funksjon i Seksjon for styring og kontroll i Direktørens stab
* Ansvar for å
	+ støtte virksomhetsledelsen i internkontrollspørsmål innen informasjonssikkerhet
	+ koordinere eget arbeid med Fagansvarlig internkontroll
	+ koordinere eget arbeid med Fagansvarlig personvern
	+ være en ressursperson, pådriver og tilrettelegger for en god etablering og risikobasert gjennomføring av virksomhetens samlede internkontrollarbeid innen informasjonssikkerhet
	+ lede og koordinere arbeidet med å avgjøre omfanget av virksomhetens fellessikring
	+ utarbeide saksnotat til virksomhetsledelsens gjennomgang innen informasjonssikkerhet
	+ utarbeide minimum årlige statusrapporter som grunnlag for linjeledernes risikovurderinger innen informasjonssikkerhet

## Fagansvarlig personvern

* Funksjon i Seksjon for styring og kontroll i Direktørens stab
* Ansvar for å
	+ støtte virksomhetsledelsen i internkontrollspørsmål innen personvern
	+ koordinere eget arbeid med Fagansvarlig internkontroll
	+ koordinere eget arbeid med Fagansvarlig informasjonssikkerhet
	+ eie, etablere og systematisk evaluere nødvendige rutiner for at virksomheten skal etterleve personvernregelverkets bestemmelser utover informasjonssikkerhet
	+ være en ressursperson, pådriver og tilrettelegger for en god etablering og risikobasert gjennomføring av virksomhetens internkontrollarbeid for etterlevelse av personvernregelverket
	+ koordinere håndteringen av krav om innsyn mv. etter personvernregelverket
	+ sikre, i samarbeid med fagansvarlig informasjonssikkerhet, at virksomheten har nødvendig sentral oversikt over arbeidsoppgaver og tjenester som behandler personopplysninger
	+ sikre, i samarbeid med IKT-sjef, at virksomheten har nødvendig sentral oversikt over databehandlere og databehandleravtaler
	+ koordinere meldinger og konsesjonssøknader til Datatilsynet
	+ utarbeide saksnotat til virksomhetsledelsens gjennomgang innen etterlevelse av personvernregelverket

## Personvernombud

* Ivareta kravene til et personvernombud i henhold til personvernregelverket

(Dersom virksomheten ønsker å inkludere personvern utover informasjonssikkerhet i dette dokumentet, bør de selv vurdere om de har behov for både funksjonen personvernombud og fagansvarlig personvern e.l., slik dette eksempelet skisserer. De bør også ev. vurdere om samme fysiske person eventuelt kan dekke begge funksjonene. Det avgjørende vil trolig være de styringsbehov virksomhetsledelsen må ha på en fagansvarlig personvern, for å få en tilstrekkelig internkontroll på personvernområdet. Dette må vurderes opp mot den uav­hengighet et personvernombud skal ha. [Datatilsynet](https://www.datatilsynet.no/) har veiledningsansvaret for person­vern­regleverket, og vi viser til dem for eventuelle råd.)

## Fagansvarlig HMS

* Funksjon i Seksjon for personalforvaltning i Administrasjonsavdelingen
* Ansvar for å
	+ støtte virksomhetsledelsen i internkontrollspørsmål innen HMS
	+ koordinere eget arbeid med Fagansvarlig internkontroll
	+ være en ressursperson, pådriver og tilrettelegger for en god etablering og risikobasert gjennomføring av virksomhetens samlede HMS-arbeid
	+ utarbeide saksnotat til virksomhetsledelsens gjennomgang innen HMS
	+ utarbeide minimum årlige statusrapporter som grunnlag for linjeledernes risikovurderinger innen HMS

## Kvalitetssjef

* Funksjon i Seksjon for styring og kontroll i Direktørens stab
* Ansvar for å
	+ støtte virksomhetsledelsen i kvalitetsspørsmål
	+ koordinere eget arbeid med Fagansvarlig internkontroll
	+ være en ressursperson, pådriver og tilrettelegger for en god etablering og risikobasert gjennomføring av virksomhetens samlede kvalitetsarbeidet

(Sikkerhetsloven: dersom virksomheten behandler skjermingsverdig informasjon (§ 5-1), sikkerhetsgradert informasjon (§ 5-3), eller har ansvaret for skjermingsverdige informasjonssystemer (§6-1) eller objekter og infrastruktur som er utpekt som skjermingsverdig (§ 7-1), bør i tillegg nødvendige roller iht. virksomhetsikkerhetsforskriften §6 og forskrift om kryptosikkerhet §§ 6 til 10 legges inn her under spesialfunksjoner, i den grad de er relevante.

Merk samtidig det som står innledningsvis under pkt. 9 *Spesialfunksjoner* i dette eksempelet, om at én fysisk person kan dekke flere funksjoner og roller dersom det ikke går på bekostning av nødvendig uavhengighet. [NSM](https://nsm.stat.no/) har veiledningsansvaret for sikkerhetsloven, og de har omfattende veiledning om forståelse og bruk av dette regelverket.)

## Lokale sikkerhetskoordinatorer

* 2-4 i hver avdeling avhengig av størrelse
* Utpekes av avdelingsdirektør
* Ansvar for å støtte de lokale avdelingene i sikkerhetsspørsmål og være et bindeledd opp mot virksomhetens fagansvarlig informasjonssikkerhet

## Prosessledere risikovurdering og risikohåndtering

* Minimum 4
* Utpekes av Direktør
* Ansvar for å støtte risikoeiere rundt om i virksomhetene ved å være prosessleder i arbeid med risikovurdering og foreslå håndtering

# Faste fora med roller i internkontroll- og sikkerhetsarbeidet

Det er etablert flere faste fora med roller i internkontroll- og sikkerhetsarbeidet. En oversikt ligger i tabellen under.

Den ansvarlige for de ulike foraene kaller inn til møtene og er ansvarlig for gjennomføringen, et kort referat og nødvendig rapportering til relevante aktører. Den ansvarlige skal alltid ha en oppdatert oversikt over de faktiske deltakerne. Deltakeroversikt og møtereferat skal systematisk registreres i vårt arkivsystem og publiseres på felles sted for formålet på vårt intranett.

(Virksomhetene må kritisk vurdere hvilke fora de faktisk trenger. Samtidig er det viktig å formalisere rollen inn mot internkontroll og sikkerhetsarbeid til de fora som allerede eksisterer for å ivareta ordinær linjestyring, eksempelvis toppledergruppen og avdelingsledergrupper. Det presiseres at understående fora bare er eksempler)

**Oversikt over faste fora med roller i internkontroll- og sikkerhtsarbeidet**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Forum | Formål  | Deltakere | Møtefrekvens | Ansvarlig |
| Toppledergruppen | Årlige gjennomganger på ulike internkontroll­områder. Behandling av enkeltsaker ved behov. | Direktør og avdelingsdirektører. | Internkontroll­spørsmål minst en gang årlig for hvert internkontroll­område. Ellers ved behov | Direktør |
| Avdelingsledergrupper | Årlige gjennomganger på ulike internkontroll­områder. Behandling av enkeltsaker ved behov | Avdelings­direktører og seksjonssjefer. | Internkontroll­spørsmål minst en gang årlig for hvert internkontroll­område. Ellers ved behov | Avdelings­direktører |
| Sikkerhetsutvalget | Rådgivende organ i internkontroll- og sikkerhetsspørsmål | Assisterende direktør. En leder­representant fra hver avdeling. Fag­ansvarlige for internkontrollområder | En gang hvert halvår og ellers ved spesielle behov | Assisterende direktør |
| Forum tiltaksleverandører | Koordinering av sikkerhetstiltak på tvers av tiltaksleverandører | Assisterende direktør. Fagansvarlig informasjonssikkerhet. En kontaktperson fra hver av direktoratets felles tiltaksleverandører. | En gang hvert halvår og ellers ved spesielle behov  | Assisterende direktør |
| Forvaltergruppe IKT-system | Koordinering av forvaltningen av IKT-system | Faste personer fra seksjon IKT-utvikling. Fagansvarlig informasjonssikkerhet. Systemeiere IKT-­system. | En gang hvert halvår og ellers ved spesielle behov | Seksjonssjef IKT-utvikling |
| Ressursgruppe lokale sikkerhetskoordinatorer | Kompetanseheving og erfaringsdeling | Lokale sikkerhets­koordinatorer, Fagansvarlig informasjonssikkerhet. | En gang pr kvartal | Fagansvarlig info.­sikkerhet |
| Ressursgruppe prosessledere | Kompetanseheving og erfaringsdeling | Prosessledere for aktiviteter under risikovurdering og risikohåndtering | En gang pr kvartal | Fagansvarlig internkontroll |