***(Kommentarar og nokre råd er skrivne i gult innleiingsvis og undervegs i dokumentet.***

*Dette dømet dekkjer «alle» internkontrollområde. Det har denne forma for å synleggjere korleis internkontroll og sikkerheitsarbeid innan informasjonssikkerheit kan integrerast med andre område der det er naturleg. Dette tilrår 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 informasjonssikkerheitsområdet «bør vere ein integrert del av verksemda sitt heilskaplege styringssystem», og sikkerhetsloven § 4-1 om at sikkerheitsarbeid etter lova skal vere ein del av verksemda sitt styringssystem.*

*Endeleg omfang og utforming av dokumentet må ein sjå i samanheng med dei styringsdokumenta som verksemda har frå før på ulike område. Om ein ønskjer å avgrense dokumentet til berre informasjonssikkerheit eller for nokre færre område, kan dømet enkelt snevrast inn ved å ta bort enkelte punkt og spisse andre. Det er kommentert under.* ***Dei som gjenbrukar sentrale delar av dømet, er sjølv ansvarlege for kvalitetssikring av innhaldet og tilpassing til eiga verksemd.***

*Dokumentet er av typen retningslinje. Ein kan namngje og strukturere både policyar, retningslinjer mv. på fleire måtar. Alternative måtar er m.a. skildra i DFØ sin «*[*Rettleiing - policy for internkontroll*](https://dfo.no/Documents/FOA/publikasjoner/veiledere/internkontroll/Veiledning%20-%20policy%20for%20internkontroll.docx)*» og «*[*Rettleiing - 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.* [*DFØ sine verktøy for internkontroll*](https://dfo.no/fagomrader/internkontroll/verktoy/)*.*

*Om ein vel alternative dokumentstrukturar eller alternative tilnærmingar til innhaldet, bør ein frå eit informasjonssikkerheitsperspektiv sikre det detaljeringsnivået og den systematikken som er spegla att i dømet under. For dei som vel eller har andre godt fungerande strukturar på dokument og innhald, kan dømet under brukast som inspirasjon til forbetringar.)*

Innhald

[1. Innleiing 2](#_Toc90477871)

[1.1 Målgruppe 2](#_Toc90477872)

[1.2 Føremål 2](#_Toc90477873)

[1.3 Relaterte policyar og retningslinjer 2](#_Toc90477874)

[1.4 Detaljeringsnivå og utdjupingar 2](#_Toc90477875)

[1.5 Forklaringsmodell internkontroll 2](#_Toc90477876)

[2. Organisering og rapportering 3](#_Toc90477877)

[2.1 Grunnleggjande prinsipp 3](#_Toc90477878)

[2.2 Linja som hovudføring 3](#_Toc90477879)

[2.3 Spesielle funksjonar 3](#_Toc90477880)

[3. Direktøren sitt særskilde ansvar 4](#_Toc90477881)

[4. Leiarar på alle nivå 5](#_Toc90477882)

[5. Leiarar på operativt nivå (risikoeigarar) 6](#_Toc90477883)

[6. Systemeigarar fellessystem 7](#_Toc90477884)

[7. Tiltaksleverandørar 8](#_Toc90477885)

[8. Alle tilsette 9](#_Toc90477886)

[9. Spesialfunksjonar 9](#_Toc90477887)

[9.1 Fagansvarleg internkontroll 10](#_Toc90477888)

[9.2 Økonomisjef 10](#_Toc90477889)

[9.3 Fagansvarleg informasjonssikkerheit 10](#_Toc90477890)

[9.4 Fagansvarleg personvern 11](#_Toc90477891)

[9.5 Personvernombod 11](#_Toc90477892)

[9.6 Fagansvarleg HMS 11](#_Toc90477893)

[9.7 Kvalitetssjef 11](#_Toc90477894)

[9.8 Lokale sikkerheitskoordinatorar 12](#_Toc90477895)

[9.9 Prosessleiarar risikovurdering og risikohandtering 12](#_Toc90477896)

[10. Faste fora med roller i internkontroll- og sikkerheitsarbeidet 12](#_Toc90477897)

[Toppleiargruppa 13](#_Toc90477898)

[Avdelingsleiargrupper 13](#_Toc90477899)

[Sikkerheitsutvalet 13](#_Toc90477900)

[Forum tiltaksleverandørar 13](#_Toc90477901)

[Forvaltargruppe IKT-system 13](#_Toc90477902)

[Ressursgruppe lokale sikkerheitskoordinatorar 13](#_Toc90477903)

[Ressursgruppe prosessleiarar 14](#_Toc90477904)

# Innleiing

## Målgruppe

Dette dokumentet er ein del av verksemda sine overordna styrande dokument. Målgruppa er alle tilsette.

## Føremål

Føremålet er å klargjere roller og ansvar i direktoratet med tanke på internkontroll og sikkerheitsrelatert arbeid. Dette dekkjer både mål og resultatkrav, økonomistyring, informasjonssikkerheit, HMS, personvern, regelverksetterleving elles, bygningssikkerheit, verdisikkerheit mv. (Område fjernast om ein ønskjer eit avgrensa omfang på dokumentet, t.d. berre til informasjonssikkerheit.)

Dokumentet skal sikre tilstrekkeleg internkontroll (styring og kontroll). Direktoratet sitt sikkerheitsarbeid er ein del av dette. Rollefordelinga synleggjer på den måten direktoratet sin sikkerheitsorganisasjon.

## Relaterte policyar og retningslinjer

Ein må sjå dokumentet i samanheng med følgjande:

* Policy for informasjonssikkerheit
* (Eventuelt tilsvarande policydokument for andre internkontrollområde)
* Retningslinjene
  + Forstå, vurdere og handtere risiko
  + (Eventuelt tilsvarande for risiko på strategisk og taktisk nivå)
  + Vurdere behov for risikovurderingar (eventuelt spesifisert for kva område)

## Detaljeringsnivå og utdjupingar

Dokumentet inneheld ei kort skildring av overordna ansvars- og styresmaktstilhøve. Utdjupingar og presiseringar kan ved behov leggjast i utdjupande retningslinjer, skildringar av tryggingstiltak, stillingsskildringar og rettleiingar. Presiseringar kan også vere nedfelte i lov- og regelverk.

## Forklaringsmodell internkontroll

Arbeidet vårt med internkontroll er basert på forklaringsmodellen under. I dokumentet er det gjennomgåande referert til dei hovudaktivitetane som er nemnde i modellen. (Eller ein annan forklaringsmodell, t.d. frå DFØ, om det blir rekna som meir føremålstenleg. Då må kanskje namn på aktivitetar det refererast til endrast utover i dette dømet for å få tilvisinga konsistent med forklaringsmodellen.)



# Organisering og rapportering

## Grunnleggjande prinsipp

Internkontroll- og sikkerheitsarbeidet i direktoratet skal vere basert på

* ansvarsprinsippet
* likskapsprinsippet
* nærleiksprinsippet
* samvirkeprinsippet

Dette vil seie at den ordinære linja er det berande elementet i internkontroll- og sikkerheitsarbeidet, og at risiko- og sikkerheitsspørsmål i størst mogleg grad skal handterast som linjeaktivitetar elles. Samstundes har alle i direktoratet eit sjølvstendig ansvar for å sikre best mogleg samvirke med andre relevante aktørar, organisatoriske einingar og verksemder.

## Linja som hovudføring

Ansvar, styresmakt og rapportering for internkontroll- og sikkerheitsarbeid skal som hovudregel følgje linja. Det vil seie følgjande hierarki:

* Direktør
* Avdelingsdirektørar
* Seksjonssjefar
* Andre tilsette

Ansvar for prosjekt skal vere kopla til ei organisatorisk eining i linja. Det er denne det skal rapporterast til også i internkontroll- og sikkerheitsspørsmål.

Etablerte system for avviks- og hendingshandtering skal nyttast i rapporteringa for den type avvik og hendingar desse dekkjer.

Handtering av kriser og hendingar med eigne prosedyrar, skal skje i samsvar med dei planar og prosedyrar som er etablerte.

## Spesielle funksjonar

Fellesfunksjonar, støttefunksjonar og samarbeidsgrupper skal ha tydelege roller og ansvar og understøtte linjeleiarane rundt om i verksemda.

Rapportering skal som hovudregel skje gjennom den linja spesialfunksjonane tilhøyrer. Samarbeidsgrupper skal rapportere gjennom den linja gruppeleiar tilhøyrer. Nokre funksjonar kan ha direkte rapportering til direktør på enkelte område. Det skal gå fram av funksjonsskildringa.

# Direktøren sitt særskilde ansvar

Direktør er ansvarleg for at det blir gjennomført tilstrekkelege risikovurderingar på strategisk nivå. Desse må dekkje verksemda si overordna måloppnåing, effektiv organisering, forsvarleg økonomistyring, etterleving av lover og reglar og påliteleg rapportering. Direktør er også ansvarleg for at naudsynte risikoreduserande tiltak blir identifiserte, sette inn og følgde opp i organisering og styring av verksemda. Tiltak skal vere tilpassa risiko og kor vesentlege dei er.

(Avsnittet over gjeld risikostyring på strategisk nivå. Det fell normalt utanfor det internkontrollperspektivet ein har innan informasjonssikkerheit og andre operative område. For å skape ein heilskap i verksemda sitt samla internkontrollarbeid og styringssystem, kan eit avsnitt som dette vere med her, ev. i ein annan variant. Avsnittet over fjernast om dette dokumentet blir avgrensa til informasjonssikkerheit.)

Direktør er i tillegg ansvarleg for at verksemda sitt arbeid med internkontroll og sikkerheit blir gjennomført på ein systematisk og tilstrekkeleg omfattande måte rundt om i heile verksemda. Arbeidet skal vere tilpassa risiko og kor vesentleg det er.

Grunnlaget for dette er at direktør har sytt for at

* verksemda har naudsynte føringar for arbeidet og at desse har tilstrekkeleg kvalitet
* andre naudsynte etableringsaktivitetar er gjennomførte

Som del av leiinga si styring og oppfølging er direktør spesielt ansvarleg for gjennomføring av verksemdsleiinga sin gjennomgang på områda

* mål og resultatkrav
* økonomistyring
* informasjonssikkerheit
* kvalitetskrav
* HMS
* etterleving av personvernregelverket
* etterleving av anna relevant regelverk

Omfang og innretning skal vere tilpassa risiko og kor vesentleg det er. Gjennomgangar på to eller fleire område kan slåast saman når det blir rekna som nyttig og forsvarleg for å ha tilstrekkeleg styring og kontroll.

(Område over fjernast om ein ønskjer eit avgrensa omfang på retningslinja, t.d. berre til informasjonssikkerheit.)

Verksemdsleiinga sin gjennomgang skal utførast 1 - 4 gongar årleg avhengig av områda sin eigenart, status, risiko og kor vesentlege dei er. Gjennomgangane skal inngå i den ordinære verksemdsstyringa og synleggjerast i styringshjulet i verksemda. Heile toppleiargruppa skal som hovudregel delta i gjennomgangen til verksemdsleiinga.

Ved behov skal direktør

* syte for at det skjer ei forbetring av overordna styrande dokument
* gje eventuelle tilleggsføringar for verksemda sitt internkontroll- og sikkerheitsarbeid
* stille opp og følgje opp spesifikke krav til enkelte leiarar og einingar
* vurdere om ein skal måle tilstanden på definerte indikatorar over tid, og eventuelt få sett i verk slike målingar
* vurdere om ein skal få gjennomført evalueringar, og eventuelt få sett i verk slike
* vurdere om ein skal få gjennomført internrevisjon, og eventuelt få sett i verk slike

Eventuell gjennomføring av dei tre siste er ein del av verksemda si måling, evaluering og revisjon.

Dokumentasjon av det som er nemnt over skal skje skriftleg i dei arkivløysingane som er etablerte for føremålet. Det skjer normalt gjennom saksnotat og møtereferat med tydelege vedtak frå direktør.

# Leiarar på alle nivå

Leiarar på alle nivå er ansvarlege for at det blir gjennomført tilstrekkelege risikovurderingar av taktisk karakter i og under eige ansvarsområde. Desse må dekkje kva som må gjerast for å nå dei måla og resultatkrava dei er ansvarlege for, samt å ha ei effektiv organisering, forsvarleg økonomistyring, påliteleg rapportering og etterleve lover og reglar. Leiarane er også ansvarlege for å identifisere, setje inn og følgje opp naudsynte risikoreduserande tiltak. Tiltak skal vere tilpassa risiko og kor vesentlege dei er.

(Avsnittet over gjeld risikostyring på taktisk nivå. Det fell normalt utanfor det internkontrollperspektivet ein har innan informasjonssikkerheit og andre operative område. For å skape ein heilskap i verksemda sitt samla internkontrollarbeid og styringssystem, kan eit avsnitt som dette vere med her, ev. i ein annan variant. Avsnittet over fjernast om dette dokumentet blir avgrensa til informasjonssikkerheit.)

Leiarar på alle nivå har også det overordna ansvaret for oppgåveløysing, tenesteutføring, informasjonsbehandling, HMS, regelverksetterleving, eigedelane mv. under eige ansvarsområde. Det operative ansvaret som risikoeigarar for dette, er normalt delegert til lågaste leiarnivå, jf. pkt. 5. (Område fjernast om ein ønskjer eit avgrensa omfang på dokumentet, t.d. berre til informasjonssikkerheit.)

Ved behov for effektivisering og samordning skal overordna leiar ta stilling til kva mål, område, risikovurderingar og risikoar som eventuelt skal vurderast og handterast på eit høgare organisatorisk nivå enn det som følgjer av normal delegering.

For å sikre tilstrekkeleg internkontroll med risikoane i det operative arbeidet, jf. pkt. 5, har leiar på alle nivå viktige oppgåver knytte til aktivitetane

* leiinga si styring og oppfølging
* måling, evaluering og revisjon

Dette må dekkje områda

* informasjonssikkerheit
* kvalitetskrav
* HMS
* etterleving av personvernregelverket
* etterleving av anna relevant regelverk

(Område over fjernast om ein ønskjer eit avgrensa omfang på dokumentet, t.d. berre til informasjonssikkerheit.)

Som del av leiinga si styring og oppfølging skal leiarar på alle nivå systematisk

* delegere og følgje opp internkontroll- og sikkerheitsarbeidet gjennom linja
* sikre finansielle rammer for internkontroll- og sikkerheitsarbeidet
* kommunisere at det er viktig med internkontroll- og sikkerheitsarbeidet
* handtere problemstillingar løfta gjennom linja
* ha planar for og å trening i relevant beredskap og krisehandtering

Som del av måling, evaluering og revisjon skal leiarar på alle nivå minst ein gong årleg systematisk vurdere status på eige ansvarsområde. Det omfattar ei reell vurdering av

* om tryggingsstiltak dei har ansvaret for fungerer som føresett
* om dei sjølv og dei personar dei har ansvaret for
  + følgjer gjeldande lov- og regelverk
  + gjennomfører pålagde oppgåver i internkontroll- og sikkerheitssarbeidet på ein tilfredsstillande måte,
  + etablerer og følgjer opp vedtekne eller avtalte tryggingsstiltak
  + etterlever innførte tryggingsstiltak

Ved vesentleg uvisse på punkta over skal leiarane gjennomføre nærmare undersøkingar av status. Dette kan vere enkle undersøkingar eller meir omfattande evalueringar avhengig av eigenarten til området. Ved vesentlege avvik og manglar skal tiltak setjast inn for å rette opp tilhøva.

Ansvaret til leiinga under måling, evaluering og revisjon omfattar også ansvaret for å sikre gjennomføring av lovpålagde eller avtalte systemgjennomgangar, systemrevisjonar o.l. Dette kan i prinsippet gjennomførast som evalueringar tilpassa aktuelle pålegg og avtalar.

Arbeidet over skal så langt som det er føremålstenleg integrerast i den ordinære linjestyringa.

Der det ikkje er klart ueigna, skal dokumentasjon skje skriftleg i dei arkivløysingane som er etablerte for føremålet. Med unntak for beredskap og krisehandtering, samt spesielle evalueringar og standardisert rapportering, vil eit kort notat ofte vere nok.

# Leiarar på operativt nivå (risikoeigarar)

I samsvar med dei grunnleggjande prinsippa, jf. pkt. 2.1, vil ansvaret som risikoeigar på operativt nivå normalt vere delegert til lågaste leiarnivå. Det overordna ansvaret blir alltid liggjande igjen i linja, jf. pkt. 4.

Operative risikoar omfattar uønskte hendingar og konsekvensar i den operative utføringa av oppgåver og tenester.

Ansvaret til risikoeigarane omfattar oppgåveløysing, tenesteutføring, informasjonsbehandling, HMS, regelverksetterleving, eigedelane mv. under eige ansvarsområde. (Område fjernast om ein ønskjer eit avgrensa omfang på dokumentet, t.d. berre til informasjonssikkerheit.)

Gjennom aktiviteten vurdering av risiko skal risikoeigarar syte for at dei systematisk får

* etablert og vedlikehalde tilstrekkeleg oversikt over eige ansvarsområde, og gruppert og prioritert naudsynte risikovurderingar
* tilstrekkeleg kjennskap til relevante lover, reglar og avtalar, og identifisert konkrete krav som må følgjast opp
* planlagd og gjennomført naudsynte risikovurderingar
* vurdert risiko ved behov i oppfølging av hendingshandteringa
* vurdert risiko ved anskaffingar og utvikling

Oversikt og vurderingar skal kvar for seg, eller i føremålstenlege kombinasjonar, dekkje risikoar som omfattar brot på

* informasjonssikkerheit (konfidensialitet, integritet, tilgjenge)
* kvalitetskrav
* HMS
* etterleving av personvernregelverket
* etterleving av anna relevant regelverk,

samt dei konsekvensar slike brot kan få.

(Område over fjernast om ein ønskjer eit avgrensa omfang på dokumentet, t.d. berre til informasjonssikkerheit.)

Som del av aktiviteten handtering av risiko skal risikoeigarar syte for at dei får

* framlegg om handtering av risikoar frå risikovurderingar
* godkjent framlegg til risikohandtering
* iverksett godkjende tiltak

Arbeidet skal skje i tilstrekkeleg omfang og detaljeringsnivå innanfor gjeldande retningslinjer og krav.

Val av risikoreduserande tiltak skal vere basert på risiko, kor vesentleg det er, nytte-kost-vurderingar og leiinga sine føringar for risikohandtering og eit effektivt sikkerheitsarbeid.

Ansvaret omfattar også IKT-system og anna teknisk utstyr som berre understør risikoeigarane sine oppgåver og tenester og som dei sjølv er systemeigarar for. For fellessystem, sjå pkt.6.

Støtte kan gjevast av relevante spesialfunksjonar, jf. pkt. 9.

Iverksetjing av tiltak i risikohandteringa, skal ved behov avtalast med verksemda sin felles tiltaksleverandør, jf. pkt. 7. Enkelte tiltak kan også etablerast og vedlikehaldast av risikoeigarane sjølve, jf. pkt. 7.

Ansvaret til risikoeigarar omfattar også å sikre tilstrekkeleg overvaking og hendingshandtering, kompetanse- og kulturutvikling og kommunikasjon rundt risikoar i eige ansvarsområde. Der det er pålagt eller føremålstenleg skal dette skje innanfor felles systematikk og felles støttesystem i direktoratet.

Dokumentasjon skal som hovudregel skje skriftleg i dei malar, støtteverktøy og arkivløysingar som er etablerte for føremålet.

Risikoeigarar skal til ei kvar tid vedlikehalde ei oppdatert oversikt over kva system dei er systemeigarar for, føremålet med systemet, brukskrav og kven som er kontaktpersonar. Dei skal systematisk registrere oversikta i arkivsystemet vårt og publisere henne på felles stad for føremålet på intranettet vårt.

# Systemeigarar fellessystem

Alle IKT-system og anna teknisk utstyr som brukast av fleire risikoeigarar kallast fellessystem. Dei skal ha ein utpeikt systemeigar. Systemeigarar fellessystem blir peikte ut av øvste leiarnivå for dei som brukar systemet. Styring, samordning og rapportering skal følgje den linja som systemeigar fellessystem tilhøyrer.

Systemeigarar for fellessystem skal ta hand om interessene til dei som nyttar systema i oppgåveløysinga og tenesteutføringa si. Det presiserast at risikoeigarar som brukar fellessystem, også er risikoeigarar for eigen bruk av fellessystema. Dei skal difor i tilstrekkeleg grad og på føremålstenleg måte involverast i risikovurderingsarbeid og andre internkontrollaktivitetar som utførast på fellessystema. Både systemeigarar fellessystem og risikoeigarane sjølv har ansvaret for å sikre dette.

Systemeigarar fellessystem har ansvar for dei same oppgåvene for sine fellessystem som risikoeigarane har for sine ansvarsområde. Sjå pkt. 5 for konkret oversikt over ansvar, oppgåver og dokumentasjonskrav. Støtte kan gjevast av relevante spesialfunksjonar, jf. pkt. 9.

# Tiltaksleverandørar

Verksemda har følgjande felles tiltaksleverandørar med ansvar for etablering, gjennomføring og systematisk kontroll med tryggingsstiltaka innan ansvarsområdet sitt.

| Område | Ansvarleg |
| --- | --- |
| Overordna føringar | Seksjon for styring og kontroll i Direktørens stab |
| Personal | Seksjon for personalforvaltning i Administrasjonsavdelinga |
| Bygg | Seksjon for bygningsforvaltning i Administrasjonsavdelinga |
| 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-anskaffingar | Seksjon for anskaffingar i Avdeling for IKT utvikling og drift |

I samsvar med dei grunnleggjande prinsippa, jf. pkt. 2, vil det operative ansvaret som sams tiltaksleverandør normalt vere delegert til leiar for dei nemnde einingane. Det overordna ansvaret blir alltid liggjande igjen i den linja dei høyrer til.

I tillegg til det nemnt over kan følgjande vere tiltaksleverandørar for eigne ansvarsområde og system

* Risikoeigarar
* Systemeigarar fellessystem

Tryggingstiltaka dei to siste har ansvar for vil ofte vere organiserte av det operative arbeidet, samt krav, prosedyrar, rutinar, kompetanse- og kulturutvikling o.l. knytte til eigne arbeidsoppgåver, tenester og system.

Som del av aktiviteten handtering av risiko skal relevante tiltaksleverandørar

* utforme og implementere avtalte og pålagde tiltak
* oppdatere verksemda si fellessikring i dialog med Fagansvarleg informasjonssikkerheit, jf. pkt. 9.3.

Fellessikring er eit sett av tryggingsstiltak som er etablerte for å gje eit felles grunnleggjande sikkerheitsnivå for sentrale område av verksemda. Andre tiltak tilpassa enkelte organisatoriske einingar eller system kallast tilleggssikring.

Fordelinga mellom kva som skal vere respektive fellessikring og tilleggssikring, skal styrast av kva som gjev best nytte-kost for verksemda samla. Ein skal då ta omsyn til

* kor mange som har vesentleg nytte av tryggingstiltaket
* omfanget av negative sideeffektar av tiltaket for risikoeigarar med låg nytteverdi
* behovet for kostnadseffektiv drift av det samla sikkerheitsarbeidet

Alle tiltaksleverandørar skal ut frå dette systematisk vurdere kva tiltak som bør etablerast som respektive fellessikring og tilleggssikring. Meiner dei auka fellessikring er riktig, skal dei kontakte fagansvarleg informasjonssikkerheit. Ho skal leie og koordinere arbeidet med å avgjere omfanget av fellessikringa. Avgjerd takast av den som direktør peikar ut.

Dokumentasjon av tiltaksleverandøren si risikohandtering skal som hovudregel skje skriftleg i dei malar, støtteverktøy og arkivløysingar som er etablerte for føremålet.

Som del av overvaking og hendingshandtering skal tiltakleverandørane

* overvake i samsvar til avtale
* rapportere relevante hendingar, avvik og informasjonssikkerheitsbrot i samsvar med gjeldande rutinar og forventingar
* følgje opp det nemnt over her, der dei har oppfølgingsansvaret

Der det er pålagt eller føremålstenleg skal dette skje innanfor felles systematikk og felles støttesystem i direktoratet.

Ansvaret til tiltaksleverandørane omfattar også å sikre tilstrekkeleg kompetanse- og kulturutvikling i eiga eining.

# Alle tilsette

Alle tilsette har eit overordna ansvar for å bidra til at direktoratet når dei samla måla våre på ein best mogleg måte.

Alle tilsette skal ha eit medvite tilhøve til måla for eige arbeid, kva slags informasjon og kva verdiar dei behandlar og kva krav som blir stilte til oppgåvegjennomføring, tenesteutføring, informasjonsbehandling og bruk av IKT og anna utstyr.

Alle tilsette skal etterleve dei lover, reglar, retningslinjer, krav, rutinar mv. som gjeld for dei og det arbeidet dei gjer.

Uønskte hendingar og avvik skal meldast systematisk og utan ugrunna opphald på den måten som er gjeven opp i systemet vårt for hendings- og avvikshandtering. Rapportering elles skal skje gjennom linja på ordinær måte.

# Spesialfunksjonar

Underståande spesialfunksjonar er etablerte for å understøtte internkontroll- og sikkerheitsarbeidet. Nærmaste leiar for spesialfunksjonane skal til ei kvar tid vedlikehalde ei oppdatert oversikt med namn på kven som dekkjer funksjonane. Dei skal systematisk registrere oversikta i arkivsystemet vårt og publisere henne på felles stad for føremålet på intranettet vårt.

Éin fysisk person kan dekkje fleire av funksjonane under, og også ha nokre av rollene over. Den som peikar ut personar til spesialfunksjonar skal forsikre seg om at dette ikkje går på kostnad av krav og behov for at funksjonar og roller er uavhengige av kvarandre.

(Første setning i avsnittet over er eit svært viktig punkt for å få ei effektiv organisering av det samla internkontroll- og sikkerheitsarbeidet, spesielt i små og mellomstore verksemder. I tillegg til å sikre at dei er uavhengige, vil storleiken på verksemda, eigenarten og tilgjengeleg kompetanse ha noko å seie for om ein person bør og kan dekkje fleire av funksjonane under.

Dømet under skisserer ei mogleg heilskapleg tilnærming til sentrale funksjonar, både ut frå ev. behov og ut frå [eForvaltningsforskriften § 15](https://lovdata.no/dokument/SF/forskrift/2004-06-25-988/KAPITTEL_2#KAPITTEL_3), som seier at internkontrollen på informasjonssikkerheitsområdet «*bør være en integrert del av virksomhetens helhetlige styringssystem*».

Det blir presisert at ansvaret til funksjonane nemnde under er døme. Somme spesialfunksjonar under kan fjernast om dei ikkje blir rekna som relevante, t.d. kvalitetssjef.

Fleire av spesialfunksjonane under bør fjernast om dette dokumentet avgrensast til informasjonssikkerheit.)

## Fagansvarleg internkontroll

* Funksjon i Seksjon for styring og kontroll i Direktørens stab
* Ansvar for å
  + støtte verksemdsleiinga i internkontrollspørsmål generelt
  + koordinere internkontroll- og kvalitetsarbeidet for alle område og sikre eit heilskapleg internkontroll- og styringssystem i verksemda
  + etablere føremålstenlege hjelpemiddel for vurdering av risiko på strategisk, taktisk og operativt nivå
  + vere ein ressursperson, pådrivar og tilretteleggjar for ei god etablering og risikobasert gjennomføring av verksemda sitt internkontrollarbeid innan mål og resultatkrav, påliteleg rapportering og regelverksetterleving som ikkje er dekt av spesialfunksjonane under
  + utarbeide saksnotat til verksemdsleiinga sin gjennomgang innan mål og resultatkrav, samt regelverksetterleving som ikkje er dekt av spesialfunksjonane under

## Økonomisjef

* Leiar av Seksjon for økonomistyring i Administrasjonsavdelinga
* Ansvar for å
  + støtte verksemdsleiinga innan økonomistyring
  + koordinere eige arbeid med Fagansvarleg internkontroll
  + vere ein ressursperson, pådrivar og tilretteleggjar for ei god etablering og risikobasert gjennomføring av den samla økonomistyringa i verksemda
  + utarbeide saksnotat til verksemdsleiinga sin gjennomgang innan økonomistyring

## Fagansvarleg informasjonssikkerheit

* Funksjon i Seksjon for styring og kontroll i Direktørens stab
* Ansvar for å
  + støtte verksemdsleiinga i internkontrollspørsmål innan informasjonssikkerheit
  + koordinere eige arbeid med Fagansvarleg internkontroll
  + koordinere eige arbeid med Fagansvarleg personvern
  + vere ein ressursperson, pådrivar og tilretteleggjar for ei god etablering og risikobasert gjennomføring av verksemda sitt samla internkontrollarbeid innan informasjonssikkerheit
  + leie og koordinere arbeidet med å avgjere omfanget av verksemda si fellessikring
  + utarbeide saksnotat til verksemdsleiinga sin gjennomgang innan informasjonssikkerheit
  + utarbeide minimum årlege statusrapportar som grunnlag for linjeleiarar si vurdering av risiko innan informasjonssikkerheit

## Fagansvarleg personvern

* Funksjon i Seksjon for styring og kontroll i Direktørens stab
* Ansvar for å
  + støtte verksemdsleiinga i internkontrollspørsmål innan personvern
  + koordinere eige arbeid med Fagansvarleg internkontroll
  + koordinere eige arbeid med Fagansvarleg informasjonssikkerheit
  + eige, etablere og systematisk evaluere naudsynte rutinar for at verksemda skal etterleve føresegnene i personvernregelverket utover informasjonssikkerheit
  + vere ein ressursperson, pådrivar og tilretteleggjar for ei god etablering og risikobasert gjennomføring av internkontrollarbeidet til verksemda for etterleving av personvernregelverket
  + koordinere handteringa av krav om innsyn mv. etter personvernregelverket
  + sikre, i samarbeid med fagansvarleg informasjonssikkerheit, at verksemda har naudsynt sentral oversikt over arbeidsoppgåver og tenester som behandlar personopplysningar
  + sikre, i samarbeid med IKT-sjef, at verksemda har naudsynt sentral oversikt over databehandlarar og databehandlaravtalar
  + koordinere meldingar og konsesjonssøknader til Datatilsynet
  + utarbeide saksnotat til verksemdsleiinga sin gjennomgang innan etterleving av personvernregelverket

## Personvernombod

* Ta hand om krava til eit personvernombod i samsvar med personvernregelverket

(Om verksemda ønskjer å inkludere personvern utover informasjonssikkerheit i dette dokumentet, bør dei sjølv vurdere om dei har behov for både funksjonen personvernombod og fagansvarleg personvern e.l., slik dette dømet skisserer. Dei bør også ev. vurdere om same fysiske person eventuelt kan dekkje begge funksjonane. Det avgjerande vil truleg vere dei styringsbehova verksemdsleiinga må ha på ein fagansvarleg personvern, for å få ein tilstrekkeleg internkontroll på personvernområdet. Dette må vurderast opp mot at personvernombodet skal vere uavhengig. [Datatilsynet](https://www.datatilsynet.no/) har rettleiingsansvaret for personvernregelverket, og vi viser til dei for eventuelle råd.)

## Fagansvarleg HMS

* Funksjon i Seksjon for personforvaltning i Administrasjonsavdelinga
* Ansvar for å
  + støtte verksemdsleiinga i internkontrollspørsmål innan HMS
  + koordinere eige arbeid med Fagansvarleg internkontroll
  + vere ein ressursperson, pådrivar og tilretteleggjar for ei god etablering og risikobasert gjennomføring av det samla HMS-arbeidet til verksemda
  + utarbeide saksnotat til verksemdsleiinga sin gjennomgang innan HMS
  + utarbeide minimum årlege statusrapportar som grunnlag for linjeleiarane si vurdering av risiko innan HMS

## Kvalitetssjef

* Funksjon i Seksjon for styring og kontroll i Direktørens stab
* Ansvar for å
  + støtte verksemdsleiinga i kvalitetsspørsmål
  + koordinere eige arbeid med Fagansvarleg internkontroll
  + vere ein ressursperson, pådrivar og tilretteleggjar for ei god etablering og risikobasert gjennomføring av det samla kvalitetsarbeidet til verksemda

(Sikkerhetsloven: om verksemda behandlar skjermingsverdig informasjon (§ 5-1), tryggingsgradert informasjon (§ 5-3), eller har ansvaret for skjemingsverdige informasjonssystem (§ 6-1) eller objekt og infrastruktur som er peikte ut som skjermingsverdige (§ 7-1), bør i tillegg naudsynte roller med tanke på verksemdsikkerheitsforskrifta § 6 og forskrift om kryptosikkerhet §§ 6 til 10 leggjast inn her under spesialfunksjonar, i den grad dei er relevante.

Merk samstundes det som står innleiingsvis under pkt. 9 *Spesialfunksjonar* i dette dømet, om at éin fysisk person kan dekkje fleire funksjonar og roller om det ikkje går på kostnad av naudsynt uavhengigheit. [NSM](https://nsm.stat.no/) har rettleiingsansvaret for sikkerhetsloven, og dei har omfattande rettleiing om forståing og bruk av dette regelverket.)

## Lokale sikkerheitskoordinatorar

* 2-4 i kvar avdeling avhengig av storleik
* Peikast ut av avdelingsdirektør
* Ansvar for å støtte dei lokale avdelingane i sikkerheitsspørsmål og vere eit bindeledd opp mot verksemda sin fagansvarleg informasjonssikkerheit

## Prosessleiarar risikovurdering og risikohandtering

* Minimum 4
* Peikast ut av Direktør
* Ansvar for å støtte risikoeigarar rundt om i verksemda ved å vere prosessleiar i arbeid med risikovurdering og gjere framlegg om handtering

# Faste fora med roller i internkontroll- og sikkerheitsarbeidet

Det er etablert fleire fora med roller i internkontroll- og sikkerheitsarbeidet. Ei oversikt ligg i tabellen under.

Den ansvarlege for dei ulike foruma kallar inn til møta og er ansvarleg for gjennomføringa, eit kort referat og naudsynt rapportering til relevante aktørar. Den ansvarlege skal alltid ha ei oppdatert oversikt over dei faktiske deltakarane. Deltakaroversikt og møtereferat skal systematisk registrerast i arkivsystemet vårt og publiserast på felles stad for føremålet på intranettet vårt.

(Verksemdene må kritisk vurdere kva forum dei faktisk treng. Samstundes er det viktig å formalisere rolla inn mot internkontroll- og sikkerheitsarbeid til dei foruma som allereie eksisterer for å ta hand om ordinær linjestyring, til dømes toppleiargruppa og avdelingsleiargrupper. Det blir presisert at underståande forum berre er døme.)

**Oversikt over faste forum med roller i internkontroll- og sikkerheitsarbeidet**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Forum | Føremål | Deltakarar | Møtefrekvens | Ansvarleg |
| Toppleiargruppa | Årlege gjennomgangar på ulike internkontrollområder. Behandling av enkeltsaker ved behov. | Direktør og avdelingsdirektørar. | Internkontrollspørsmål minst ein gong årleg for kvart internkontrollområde. Elles ved behov | Direktør |
| Avdelingsleiargrupper | Årlege gjennomgangar på ulike internkontrollområder. Behandling av enkeltsaker ved behov | Avdelingsdirektørar og seksjonssjefar | Internkontrollspørsmål minst ein gong årleg for kvart internkontrollområde. Elles ved behov | Avdelingsdirektørar |
| Sikkerheitsutvalet | Rådgjevande organ i internkontroll- og sikkerheitsspørsmål | Assisterande direktør. Ein leiarrepresentant frå kvar avdeling. Fagansvarleg for internkontrollområde | Ein gong kvart halvår og elles ved spesielle behov | Assisterande direktør |
| Forum tiltaksleverandørar | Koordinering av tryggingstiltak på tvers av tiltaksleverandørar | Assisterande direktør. Fagansvarleg informasjonssikkerheit. Ein kontaktperson frå kvar av direktoratet sine felles tiltaksleverandørar. | Ein gong kvart halvår og elles ved spesielle behov | Assisterande direktør |
| Forvaltargruppe IKT-system | Koordinering av forvaltninga av IKT-system | Faste personar frå seksjon IKT-utvikling. Fagansvarleg informasjonssikkerheit. Systemeigarar IKT-system. | Ein gong kvart halvår og elles ved spesielle behov | Seksjonssjef IKT-utvikling |
| Ressursgruppe lokale sikkerheitskoordinatorar | Kompetanseheving og erfaringsdeling | Lokale sikkerheitskoordinatorar, Fagansvarleg informasjonssikkerheit. | Ein gong per kvartal | Fagansvarleg info.sikkerheit |
| Ressursgruppe prosessleiarar | Kompetanseheving og erfaringsdeling | Prosessleiarar for aktivitetar under vurdering og handtering av risiko | Ein gong per kvartal | Fagansvarleg internkontroll |