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

*Dette dømet er ei* ***utdjuping og vidare konkretisering*** *av retningslinja «Rollar og ansvar». Dømet gjeld internkontrollområdet informasjonssikkerheit. Dokumentet bør etablerast som ei utdjupande rettleiing viss det vert sett som naudsynt for å sikre god nok forståing og etterleving av internkontrollaktivitetane og ansvaret på informasjonssikkerheits­området.* ***Dei som gjenbruker sentrale delar av dømet, er sjølv ansvarlege for kvalitetssikring av innhaldet og tilpassing til eiga verksemd.****)*

**Innhald**

[1. Innleiing 2](#_Toc90502504)

[1.1 Målgruppe 2](#_Toc90502505)

[1.2 Føremål 2](#_Toc90502506)

[1.3 Relaterte policyar og retningslinjer 2](#_Toc90502507)

[1.4 Forklaringsmodell internkontroll informasjonssikkerheit 2](#_Toc90502508)

[2. Leiinga si styring og oppfølging 2](#_Toc90502509)

[2.1 Verksemdsleiinga sin gjennomgang 2](#_Toc90502510)

[2.2 Delegere og følge opp gjennom linja 3](#_Toc90502511)

[2.3 Sikre finansielle rammer 3](#_Toc90502512)

[2.4 Kommunisere viktigheit 3](#_Toc90502513)

[2.5 Løfte og handtere problemstillingar gjennom linja 4](#_Toc90502514)

[2.6 Beredskap og krisehandtering 4](#_Toc90502515)

[3. Vurdering av risiko 4](#_Toc90502516)

[3.1 Ha oversikt og prioritere 4](#_Toc90502517)

[3.2 Planlegge risikovurdering 5](#_Toc90502518)

[3.3 Gjennomføre risikovurdering 6](#_Toc90502519)

[3.4 Vurdere risiko etter hendingar 6](#_Toc90502520)

[3.5 Vurdere risiko ved anskaffingar og utvikling 6](#_Toc90502521)

[4. Handtering av risiko 6](#_Toc90502522)

[4.1 Føreslå handtering av risikoar 6](#_Toc90502523)

[4.2 Godkjenne forslag til risikohandtering 7](#_Toc90502524)

[4.3 Iverksette godkjende tiltak 7](#_Toc90502525)

[4.4 Utforme og etablere tryggingstiltaka 8](#_Toc90502526)

[4.5 Oppdatere fellessikring og tilleggsikringa 8](#_Toc90502527)

[5. Overvaking og hendingshandtering 9](#_Toc90502528)

[5.1 Overvake i samsvar med avtale 9](#_Toc90502529)

[5.2 Rapportere hendingar, avvik og informasjonssikkerheitsbrot 9](#_Toc90502530)

[5.3 Følge opp hendingar, avvik og informasjonssikkerheitsbrot 9](#_Toc90502531)

[6. Måling, evaluering og revisjon 9](#_Toc90502532)

[6.1 Vurdere status på eige ansvarsområde 9](#_Toc90502533)

[6.2 Måle tilstanden på definerte indikatorar 10](#_Toc90502534)

[6.3 Gjennomføre evalueringar 10](#_Toc90502535)

[6.4 Gjennomføre internrevisjon 11](#_Toc90502536)

[7. Kompetanse- og kulturutvikling 11](#_Toc90502537)

[7.1 Identifisere og følge opp behov for kompetanse- og kulturutvikling 11](#_Toc90502538)

[7.2 Følge opp lokale sikkerheitskoordinatorar 11](#_Toc90502539)

[7.3 Øvingar 11](#_Toc90502540)

[8. Kommunikasjon 12](#_Toc90502541)

[8.1 Formidle nye føringar 12](#_Toc90502542)

[8.2 Dokumentere gjennomførte styringsaktivitetar 12](#_Toc90502543)

[8.3 Dokumentere etterleving av tryggingstiltak 12](#_Toc90502544)

[8.4 Statusrapportar som grunnlag for risikovurderingar 12](#_Toc90502545)

[8.5 Saksnotat til verksemdsleiinga sin gjennomgang 12](#_Toc90502546)

[8.6 Kommunikasjon mellom aktivitetar og aktørar 12](#_Toc90502547)

[8.7 Dialog med styrande organ 12](#_Toc90502548)

[8.8 Ekstern kommunikasjon 13](#_Toc90502549)

# Innleiing

## Målgruppe

Målgruppa for dette dokumentet er leiarar på alle nivå. Dokumentet er ei rettleiing og ein del av dei styrande dokumenta til verksemda.

## Føremål

Føremålet er å sikre god nok internkontroll (styring og kontroll) på informasjonssikkerheits­området. Dokumentet er ei utdjuping på informasjonssikkerheits­området av retningslinja *Rollar og ansvar i internkontroll- og sikkerheitsarbeidet*.

Dokumentet er strukturert etter styringsaktivitetar og beskriv kva delaktivitetar som skal gjennomførast, kven som har ansvaret for dei ulike oppgåvene og krav til gjennomføringa.

## Relaterte policyar og retningslinjer

Dokumentet må sjåast i samanheng med

* Policy for informasjonssikkerheit
* Retningslinjene
	+ Rollar og ansvar
	+ Forstå, vurdere og handtere risiko
	+ Vurdere behov for risikovurderingar

## Forklaringsmodell internkontroll informasjonssikkerheit

Internkontrollarbeidet er basert på forklaringsmodellen under. Dette dokumentet er strukturert etter hovudaktivitetane i forklaringsmodellen.



# Leiinga si styring og oppfølging

## Verksemdsleiinga sin gjennomgang

Verksemdleiinga skal minimum årleg gå gjennom status for internkontroll (styring og kontroll) på informasjonssikkerheits­området. Heile toppleiargruppa skal i størst mogleg grad delta. Omfang og innretting skal vere tilpassa risiko og vesentlegheit. Gjennomgangen skal vere førebudd av fagansvarleg informasjonssikkerheit i samsvar med føringar frå Direktør og tidlegare gjennomgangar.

Direktør skal på bakgrunn av gjennomgangen gje eventuelle tilleggsføringar for internkontrollarbeidet i verksemda innan informasjonssikkerheit.

Ved behov skal Direktør sørge for etablering eller endring i føringane. Fagansvarleg informasjonssikkerheit skal normalt vere saksbehandlar og resten av organisasjonen skal involverast på føremålstenleg måte.

Ved behov for meir informasjon om status, kan Direktør avgjere at verksemda skal måle tilstanden på definerte indikatorar over tid, eller få gjennomført evalueringar eller internrevisjon, jf. pkt. 6.2, 6.3 og 6.4.

## Delegere og følge opp gjennom linja

Leiarar på alle nivå skal jamleg vurdere kva som er føremålstenleg oppdeling og gruppering av underliggande område, arbeidsoppgåver og IKT-system, og på kva måte det operative ansvaret som risikoeigar, systemeigar og felles tiltaksleverandør eventuelt skal delegerast. Tiltak skal vere tilpassa risiko og vesentlegheit.

Leiarar som er mål- og resultatansvarlege for eit område, vil ofte automatisk få delegert rolla som risikoeigarar for området. Avvik frå dette bør dokumenterast spesielt.

Systemeigarar fellessystem og felles tiltaksleverandørar, kan heilt eller delvis få tildelt eller delegert sitt ansvar gjennom retningslinjer eller tilhøve som ligg utanfor informasjons­sikkerheit. Oppfølging av at ansvaret vert etterlevd, skal uansett skje gjennom linja.

Leiarar på alle nivå skal jamleg vurdere om nokre styringsaktivitetar bør gjennomførast som fellesaktivitetar på eit høgare organisatorisk nivå enn delegeringa tilseier. Målet er å sikre ei kostnadseffektiv gjennomføring av internkontrollarbeidet.

All oppfølging av ansvar og oppgåver skal skje som ein del av den ordinære linjestyringa, årsplanlegginga og årsoppfølginga.

Det skal gå fram av dokumentasjonen i linjestyringa at delegering og oppfølging også har omfatta aktivitetane innan internkontroll på informasjonssikkerheitsområdet.

## Sikre finansielle rammer

Leiarar på alle nivå skal sørge for at økonomiske erfaringar og behov rundt styringsaktivitetar og tryggingstiltak er tema når budsjettrammer vert vurderte og diskuterte i verksemda.

Å sikre naudsynte finansielle rammer skal primært skje i dei ordinære budsjettprosessane. Budsjetta må samtidig settast opp slik at verksemda har handlingsrom til å sette i verk naudsynte tiltak som vert identifiserte gjennom året.

## Kommunisere viktigheit

Leiarar på alle nivå skal kommunisere viktigheita av både informasjonssikkerheit, dei tryggingstiltaka som er sette i verk og dei systematiske aktivitetane i internkontrollarbeidet.

Haldninga til leiinga kjem til uttrykk gjennom det leiinga seier og gjer. Kommunikasjonen skal derfor skje både munnleg, skriftleg og gjennom synleg handling.

## Løfte og handtere problemstillingar gjennom linja

Viss problemstillingar i internkontrollarbeidet ikkje kan løysast på det organisatoriske nivået dei oppstår, skal dei løftast gjennom linja og handterast på eit høgare leiarnivå.

Dei skal løftast gjennom linja til eit leiarnivå vert nådd som har økonomisk handlingsrom eller myndigheit til å finne budsjettdekning, akseptere aktuelle risikoar eller ta andre naudsynte avgjersler.

## Beredskap og krisehandtering

Leiarar på alle nivå skal ha oversikt over behovet for beredskaps- og kriseplanar for sitt ansvarsområde, og sørge for etablering av slike der det er naudsynt. Dei skal kjenne beredskaps- og kriseplanar der dei har ei rolle, systematisk øve på relevante situasjonar og vere i stand til å ta si rolle i beredskaps- og krisesituasjonar.

# Vurdering av risiko

Vurdering av risiko skal organiserast og gjennomførast av risikoeigarar for eit ansvarsområde og av systemeigarar for fellessystem. Risikoeigarane er systemeigarar for eigne IKT-system, og desse er ein del av ansvarsområdet deira.

Det må presiserast at risikoeigarar som bruker fellessystem, også er risikoeigarar for eiga informasjonsbehandling i fellessystema. Dei skal derfor i tilstrekkeleg grad og på føremålstenleg måte involverast i risikovurderingsarbeid og andre internkontrollaktivitetar som vert utført på fellessystema. Både systemeigarar fellessystem og risikoeigarane sjølv har ansvaret for å sikre dette.

## Ha oversikt og prioritere

Foranalyse

Risikoeigarar skal på eit overordna nivå identifisere oppgåver og tenester dei har ansvar for, informasjonsbehandlinga i desse, regelverk som må følgast og kva IKT-system dei nyttar. Dei bør og avklare tilgrensande behov knytt til personvern, og følge opp dette i samsvar med eigne rutinar.

Risikoeigarar skal deretter anslå høgaste konsekvensnivå[[1]](#footnote-2) ved brot på konfidensialitet, integritet og tilgjenge rundt eigne arbeidsoppgåver, nytta IKT-system og spesielle hjelpemiddel. Referanseramma skal vere oppgåvene risikoeigarane utfører, informasjonen som vert behandla og konsekvensnivåa i retningslinja *Forstå, vurdere og handtere risiko*.

Systemeigarar fellessystem skal som første trinn i sine foranalysar anslå høgaste konsekvens­nivå ved brot på konfidensialitet, integritet og tilgjenge rundt fellessystema dei har ansvar for. Dei kartleggingar og vurderingar som er gjort av risikoeigarar som nyttar fellessystema, jf. framfor, er viktig bakgrunnsinformasjon. Referanseramma er den same.

Både risikoeigarar og systemeigarar fellessystem skal deretter gjere ei overordna vurdering av nivået på relevante truslar, farar og sårbarheiter og merke seg dei som peiker seg spesielt ut.

Til slutt kan foranalysane med fordel oppsummerast med nokre stikkord om eventuelle område eller forhold ein må vere spesielt merksam på i det vidare risikoarbeidet.

**Analysere eksterne krav**

Risikoeigarar og systemeigarar fellessystem skal ha oversikt over kva regelverk og avtalar som gjeld for arbeidsoppgåvene og IKT-systema dei har ansvar for og kva krava i desse medfører i praksis. Oversikta skal nyttast i risikovurderingar og risikohandtering.

Viss relevante krav ikkje er identifisert og konkretisert på verksemdsnivå, skal risiko- og systemeigarane sjølv sørge for at krava vert identifiserte, analyserte og i tilstrekkeleg grad konkretiserte.

**Gruppere og dele opp**

For å få fokus på det viktigaste, behandle like ting saman og få målretta tidsbruk på konkrete risikovurderingar, skal både risikoeigarar og systemeigarar fellessystem gruppere det som vert vurdert som enkelt og oversiktleg og dele opp og skilje ut det som vert vurdert som kritisk eller som det er knytt spesiell usikkerheit til. Det gjeld både arbeidsoppgåver, IKT-system og deler av desse. Resultatet frå foranalysane skal vere bakgrunn og støtte.

Vurdere behov for risikovurderingar

Både risikoeigarar og systemeigarar fellessystem skal deretter systematisk vurdere behovet for oppdaterte eller nye risikovurderingar for dei ulike delane av eige ansvarsområde. Dei skal også prioritere mellom naudsynte risikovurderingar. Vurdering og prioritering skal følge retningslinja *Vurdere behov for risikovurderingar*.

Oversikt over risikovurderingar

Risikoeigarar og systemeigarar fellessystem skal ut frå det som er nemnt over og dei risikovurderingar som faktisk vert gjennomførte, halde ved like ei oversikt over planlagde og gjennomførte risikovurderingar innan eige ansvarsområde.

Oppdateringar

Resultatet frå det å få oversikt og prioritere skal revurderast og eventuelt oppdaterast minst ei gong årleg. Relevante deler av aktiviteten skal alltid gjennomførast og oppdaterast før nye oppgåver eller tenester starter, eller før nye IKT-system vert anskaffa og tekne i bruk.

Støtte

Viss ikkje særskilte grunnar tilseier noko anna, skal dei rettleiingar, malar og verktøy som verksemda stiller til disposisjon nyttast i arbeidet med å få oversikt og prioritere.

Risikoeigarar og systemeigarar fellessystem er ansvarlege for gjennomføring og resultat, men dei skal få støtte frå dei felles prosessleiarane i verksemda minimum første gong arbeidet vert gjennomført.

## Planlegge risikovurdering

Før ei risikovurdering startar skal den planleggast. Omfanget av planlegginga skal tilpassast behovet. Planlegging skal skje i samarbeid mellom risikoeigar/systemeigar fellessystem og den de peiker ut som prosessleiar for arbeidet. Dette kan vere ei av dei felles prosessleiarane i verksemda eller andre, avhengig av kompleksiteten i risikovurderinga og tilgjengelege ressursar.

Viss ikkje særskilte grunnar tilseier noko anna, skal dei rettleiingar verksemda stiller til disposisjon nyttast.

Mandatet for risikovurderinga kan utformast slik at arbeidet skal omfatte både aktiviteten *Gjennomføre risikovurdering,* jf. pkt. 3.4, og oppfølgingsaktiviteten *Foreslå handtering av risikoar*, jf. pkt. 4.1

## Gjennomføre risikovurdering

Risikoeigarar og systemeigarar fellessystem skal sørge for at naudsynte risikovurderingar innan eige ansvarsområde vert gjennomført. Eit viktig grunnlag er oversikta som vart utarbeidd under delaktiviteten *Ha oversikt og prioritere*.

Gjennomføring av risikovurderingar skal skje i samsvar med retningslinja *Forstå, vurdere og handtere risiko*. Viss ikkje særskilte grunnar tilseier noko anna, skal i tillegg dei rettleiingar og støtteverktøy verksemda stiller til disposisjon nyttast.

Utpeikt prosessleiar skal sørge for at risikovurderingane vert gjennomførte på ein måte som er tilpassa objektet for risikovurderinga og dei planar som er lagde, jf. pkt. 3.3.

Risikoar som ikkje kan aksepterast ut frå retningslinja *Forstå, vurdere og handtere risiko* skal gjennomgå aktiviteten *Føreslå handtering av risikoar*, jf. pkt. 4.1.

## Vurdere risiko etter hendingar

Risikoeigar og systemeigar fellessystem kan under hendingshandtering oppdage alvorlege uønskte hendinga rein ikkje har vore tilstrekkeleg merksam på i tidlegare risikovurderingar.

Dei skal då sørge for at det vert gjennomført ei avgrensa behovsvurdering og eventuelt påfølgande risikovurdering og risikohandtering for denne og relevante tilgrensande hendingar.

Risiko- og systemeigarane er ansvarlege for at dette vert gjennomført effektivt og i tide, t.d. ved eigne prosedyrar i eiga organisatorisk eining.

## Vurdere risiko ved anskaffingar og utvikling

Ved anskaffing eller utvikling av IKT-system, skal aktuell systemeigar sørge for at behova og krava vert beskrivne i behovs- og/eller kravlister. Desse kan utformast i forkant av anskaffinga eller gradvis i anskaffinga- eller utviklingsprosessen, avhengig av kva framgangsmåte ein nyttar.

Nokre overordna sikkerheitsmessige behov, som at systemet skal ha tilgangsstyring og pålogging, kan identifiserast med same analytiske tilnærming som ved identifiseringa av funksjonelle behov. Nokre krav kan også verte avdekte gjennom aktiviteten *Analysere eksterne krav*, jf. pkt . 3.1.

For å få ei tilstrekkeleg identifisering av sikkerheitsbehova, skal systemeigarane også vurdere behovet for, og eventuelt gjennomføre, ein eller ein serie risikovurderingar, avhengig av om krava skal utformast i forkant eller undervegs i anskaffings- eller utviklingsprosessen.

Risikoar som i utgangspunktet ikkje kan aksepterast som dei er, kan ofte presenterast som behov som leverandøren må finne løysing på. Løysingsforslaga vil då vere forslag til risikoreduserande tiltak som må vurderast av systemeigar. Ved semje vil desse tiltaka representere krav til IKT-systemet.

# Handtering av risiko

## Føreslå handtering av risikoar

For risikoar som ikkje kan aksepterast i risikovurderinga, jf. pkt.3.4, skal risikoeigar / systemeigar fellessystem sørge for at eventuelle tiltak som kan redusere risikoane vert identifiserte og vurderte. Arbeidet skal skje i samsvar med retningslinja *Forstå, vurdere og handtere risiko*. Arbeidet kan vere ein del av eit større heilskapleg oppdrag gitt i mandatet til risikovurderinga.

Viss ikkje særskilte grunnar tilseier noko anna, skal dei rettleiingar og støtteverktøy verksemda stiller til disposisjon nyttast.

## Godkjenne forslag til risikohandtering

Dokumentasjonen av risikovurderingar og forslag til handtering av risikoar er eit avgjerdsgrunnlag.

Oppdragsgjevar, dvs. aktuelle risikoeigarar eller systemeigar fellessystem, skal alltid gjere ei sjølvstendig vurdering av dette avgjerdsgrunnlaget. Vurderinga skal skje i samsvar med retningslinja *Forstå, vurdere og handtere risiko*. Viss ikkje særskilte grunnar tilseier noko anna, skal elles dei rettleiingar verksemda stiller til disposisjon nyttast.

En systemeigar fellessystem må avstemme si vurdering med risikoeigarar som nytter systemet. Ved usemje må aktuelle problemstillingar løftast til eit høgare avgjerdsnivå.

Viss oppdragsgjevar ser behov for at det vert gjort nye vurderingar for at han skal kunne ta ei avgjersle, må han sørge for at dette vert gjort.

Oppdragsgjevar har ansvaret for å få finansiert godkjende forslag. Viss oppdragsgjevar ikkje disponerer tilstrekkelege budsjettmidlar, må problemstillinga løftast gjennom linja, jf. pkt. 2.5.

Viss oppdragsgjevar ikkje har myndigheit til å akseptere restrisikoar for oppgåver han har ansvaret for og som han meiner må utførast, må problemstillinga rundt desse risikoane løftast gjennom linja.

## Iverksette godkjende tiltak

Når forslag til risikohandtering er godkjend og finansiert, skal oppdragsgjevar peike ut ein handteringsansvarleg som skal planlegge og følge opp den samla gjennomføringa eller etableringa av godkjende tiltak.

Oppdragsgjevar kan sjølv vere handteringsansvarleg der det vert sett som føremålstenleg. Viss det er ein annan person, skal denne systematisk følgast opp av oppdragsgjevar.

Handteringsansvarleg skal utforme ein handlingsplan for gjennomføring eller etablering av dei godkjende tiltaka. Planen bør utformast i dialog med dei som skal gjennomføre aktivitetane. Planlegginga skal følge god praksis for prosjekt- og aktivitetsplanlegging generelt, og ha fokus på tid, kost og forventa effekt av tiltaka.

Planen skal innehalde fristar og kva som skal gjerast av kven. Formalisme og detaljeringsnivå skal tilpassast

* kor viktige tiltaka er
* omfang og kompleksitet på det som skal gjerast
* kven som skal vere ansvarleg
* korleis verksemda har organisert seg internt

Handlingsplanen skal godkjennast av oppdragsgjevar før den vert sett i verk.

Handteringsansvarleg skal systematisk følge opp framdrifta. Naudsynt rapportering skal skje til oppdragsgjevar i samsvar med dei føringar som er gjevne.

## Utforme og etablere tryggingstiltaka

Konkrete tiltak skal utformast, settast i verk og haldast ved like av tiltaksleverandørar.

Kven som er felles tiltaksleverandør for ulike fellesområde i verksemda, går fram av retningslinja *Rollar og ansvar*.

Risikoeigar og systemeigar fellessystem kan i tillegg sjølv vere tiltaksleverandør for einskilde tiltak knytt til eigne arbeidsoppgåver eller IKT-system. Dette vil ofte vere krav, prosedyrar, rutinar, kompetanse- og kulturutvikling o.l.

Tiltaksleverandørar skal utforme og implementere tiltak i samsvar med avtalar gjort med ulike handteringsansvarlege, jf. pkt. 4.3. Dokumentasjon av tiltaka skal skje i samsvar med anerkjend god praksis og dei krav som er stilte frå risikoeigar og systemeigar fellessystem.

Tiltaka må testast slik det er avtalt. Det bør i den grad det er naudsynt skje under både utforming, implementering, gjennomføring og i kontinuerleg bruk. Viss testar under etablering eller seinare drift viser at tiltaka ikkje fungerer som avtalt, må dei justerast. Dette bør inngå i avtalt vedlikehald.

Risikoeigar og systemeigar fellessystem er ansvarleg for at naudsynt testing, undersøkingar og vedlikehald vert avtalt med både interne og eksterne tiltaksleverandørar.

Felles tiltaksleverandørar skal systematisk oppdatere ei oversikt over etablerte tryggingstiltak og tiltaksstyrken deira. Det skal skje i det system som er etablert for føremålet.

## Oppdatere fellessikring og tilleggsikringa

Dei tiltak som skal gjennomførast eller implementerast, kan i utgangspunktet etablerast som del av fellessikringa[[2]](#footnote-3) i verksemda, eller som tilleggssikring som risikoeigarar og systemeigarar kan velje ut frå behov.

Tiltaksleverandørane skal vurdere kva verksemda samla er best tent med. Det skal skje allereie i dialogen med handteringsansvarleg. Tiltaksleverandørane skal i første omgang vurdere om innplasseringa som fellessikring eller tilleggssikring gjev vesentlege forskjellar mot. kostnadseffektiv drift av sikkerheitsarbeidet. Dei bør også gjere ei enkel vurdering av negative sideeffektar for andre oppgåve- og systemeigarar viss tiltaket vert ein del av fellessikringa.

Viss sideeffektane vert sett som små, eller kostnadsvurderinga klart taler for ei endring i fellessikringa, skal spørsmålet om ei slik endring sendast til fagansvarleg informasjonssikkerheit.

Viss fagansvarleg informasjonssikkerheit er einig, skal han initiere og leie ein grundigare vurderingsprosess. Det skal då gjennomførast ei identifisering av negative sideeffektar for andre arbeidsoppgåver og IKT-system, samt estimering av kostnader. I tillegg skal dei som sideeffektane får følgjer for få uttale seg.

Endeleg avgjersle om utviding av fellessikringa skal takast av Direktør eller den han utpeiker.

# Overvaking og hendingshandtering

## Overvake i samsvar med avtale

Overvaking er eit tryggingstiltak som vert valt og utforma i risikohandteringa på linje med andre tiltak, jf. pkt.4. Slike tiltak skal innehalde informasjon om kva som skal overvakast, kven som er ansvarleg for overvakinga og korleis resultatet av overvakinga skal rapporterast.

For eksterne tiltaks- eller tenesteleverandørar skal krava om overvaking vere nedfelt i ein tenestenivåavtale (SLA).

Det skal ikkje etablerast overvakingstiltak av tilsette eller andre personar, viss tiltaka ikkje er utvikla og innførte i samsvar med regelverk, avtalar og tilstrekkeleg involvering av dei det gjeld eller deira representantar.

## Rapportere hendingar, avvik og informasjonssikkerheitsbrot

Alle tilsette og innleigde med tilgang til system og informasjon er ansvarlege for å rapportere hendingar, avvik og informasjonssikkerheitsbrot dei oppdagar eller mistenker.

Rapporteringa skal skje etter krava i vårt system for hendings- og avvikshandtering, utan unødig opphald etter at hendinga er oppdaga.

## Følge opp hendingar, avvik og informasjonssikkerheitsbrot

Systemet for hendings- og avvikshandtering er eit tryggingstiltak som skal ha klare ansvarsforhold og prosedyrar om både handtering og kommunikasjon.

Det skal til ei kvar tid vere minst ein person som er ansvarleg for å følge opp innrapporterte hendingar og rute dei vidare til rette vedkomande. Det skal vere planlagt for ferieavvikling og anna fråvere. Det skal følgast opp at innrapporterte hendingar av ulik type vert handterte innan gjevne fristar.

Alle rapporterte hendingar, avvik eller informasjonssikkerheitsbrot skal følgast opp av rette vedkomande utan unødig opphald. Ved behov skal beredskapsplanar eller andre konsekvensreduserande tiltak setjast i verk utan ugrunna opphald.

Det skal alltid vurderast om vi kan lære av erfaringane frå ei hending. Særleg skal det vurderast om hendingane og avvika tilseier justering av risikovurderingar og tilhøyrande tiltak. Kunnskapen må brukast i det vidare risikovurderingsarbeidet.

# Måling, evaluering og revisjon

## Vurdere status på eige ansvarsområde

Minst ei gang i året skal følgande vurdere status for sine ansvarsområde:

* leiarar som delegerer og skal følge opp gjennom linja
* risikoeigarar
* systemeigarar fellessystem
* tiltaksleverandørar
* ansvarlege for tenestenivåavtalar eller andre avtalar
* ansvarlege for eigne deler av internkontrollaktivitetane, som t.d. hendingshandteringssystemet og internrevisjon

Statusvurderinga skal omfatte vurderingar av om ein sjølv, eigne tilsette og leverandørar

* følger gjeldande lov- og regelverk
* gjennomfører internkontrollaktivitetane slik ein er pålagt
* etablerer og følger opp vedtekne eller avtalte tryggingstiltak
* etterlever gjeldande tryggingstiltak

I tillegg skal dei som har ansvar for tiltak vurdere om tiltaka fungerer som føresett.

Alle skal i første omgang vurdere kor stor tillit dei har til at status er slik den skal vere. Viss tilliten er låg, skal nærare undersøkingar gjennomførast. Viss tilliten er moderat, skal behovet for nærare undersøkingar vurderast ut frå kor viktig saken vert vurdert å vere, både for verksemda og eiga eining. Er tilliten høg, er det normalt ingen grunn til ytterlegare undersøkingar. Det føreset likevel at tillitsnivået bygger på kritisk refleksjon om eigen kunnskap.

Den ansvarlege må sørge for at nærare undersøkingar vert gjort i tilstrekkeleg omfang og med tilstrekkeleg kvalitet. Viss undersøkingar avdekker avvik, må desse utbetrast slik at ting fungerer og tilliten vert auka til eit tilfredsstillande nivå.

Resultatet av statusvurderinga, saman med kva undersøkingar og oppfølgingstiltak som eventuelt er gjennomført, skal dokumenterast i eit kort notat. Rapportering skal skje gjennom linja. I tillegg skal risikoeigarar, som kan ha vorte påverka av identifiserte svakheiter, informerast spesielt om det som er relevant for dei.

## Måle tilstanden på definerte indikatorar

Verksemdleiinga kan avgjere at dei vil følge tilstanden over tid på einskilde område, jf. pkt. 2.1.

Dei skal då peike ut nokre ansvarlege som skal utarbeide forslag til systematiske målingar, inkludert område, indikatorar, metodar, frekvens, ansvarlege og rapportering. Avgjersle skal takast av verksemdsleiinga.

Målingane skal gjennomførast av dei som vert peikte ut til det gjennom linjeavgjersler.

Resultata skal samanstillast av fagansvarleg informasjonssikkerheit og presenterast for verksemdsleiinga, normalt som del av verksemdsleiinga sin gjennomgang.

## Gjennomføre evalueringar

Verksemdsleiinga kan avgjere at det skal gjennomførast evalueringar, jf. pkt. 2.1. Evalueringar kan omfatte heile eller deler av arbeidet med internkontroll og informasjonssikkerheit i verksemda.

Leiarar på ulikt nivå kan i tillegg avgjere at dei skal få gjennomført evalueringar på deler av sine ansvarsområde. Noko av dette kan vere lovpålagt, t.d. krav om «sikkerheitsrevisjonar» e.l.. Slike krav vil normalt dekkast av målretta evalueringar.

Oppdragsgjevar skal peike ut dei som skal vere ansvarleg for ei evaluering. Det skal alltid gjerast ei vurdering av behovet for uavhengigheit. Ved særskilt behov for uavhengigheit eller kompetanse, kan ein hente inn eksterne til å gjennomføre evalueringa.

Evalueringsoppdrag skal vere spesifisert og avgrensa og gjennomførast på ein profesjonell måte. Resultatet skal presenterast for oppdragsgjevar. Eventuelle avvik skal følgast opp.

## Gjennomføre internrevisjon

Verksemdsleiinga kan avgjere at det skal gjennomførast internrevisjon, jf. pkt. 2.1. Ein internrevisjon kan omfatte heile eller deler av arbeidet med internkontroll og informasjonssikkerheit i verksemda.

Føremålet med internrevisjon er å få ei formell uavhengig vurdering av om vi følger eksterne og interne krav til arbeidet med internkontroll og informasjonssikkerheit, og om krava er implementerte og haldne ved like på ein føremåls- og kostnadseffektiv måte.

Arbeidet skal gjennomførast etter anerkjende revisjonsstandardar. Arbeidet kan utførast av interne eller eksterne, men reell uavhengigheit skal sikrast.

Resultatet av ein internrevisjon skal presenterast for verksemdsleiinga. Avvik skal følgast opp på ein systematisk måte.

# Kompetanse- og kulturutvikling

## Identifisere og følge opp behov for kompetanse- og kulturutvikling

Identifisering av behov for kompetanse- og kulturutvikling skal gjerast løpande som ein del av internkontrollarbeidet i verksemda. Dette skal gjerast av leiarar på alle nivå og for alle ansvarsområde.

Behova kan identifiserast gjennom ulike delaktivitetar, til dømes

* medarbeidarsamtalar
* risikovurderingar
* oppfølging av hendingar, avvik og informasjonssikkerheitsbrot
* vurdering av status på eige ansvarsområde
* revisjonar og evalueringar
* verksemdsleiinga sin gjennomgang

Når det er identifisert eit behov skal det gjennomførast føremålstenlege tiltak. Tiltaka skal

* vere tilpassa riktig målgruppe
* ta i bruk føremålstenlege verkemiddel
* sjåast i samanheng med andre opplæringstiltak i verksemda
* vere tilrettelagt slik at ein kan måle effekten av tiltaket.

## Følge opp lokale sikkerheitskoordinatorar

Fagansvarleg informasjonssikkerheit og dei lokale sikkerheitskoordinatorane i verksemda skal møtast jamleg for å utveksle erfaringar og lære av kvarandre.

Aktuelle tema for samlingane vil vere

* Sikkerheitskoordinatorane si eiga kompetanseheving innan informasjonssikkerheit og internkontroll
* kompetanse- og kulturutfordringar rundt om i verksemda og innspel og råd til sentralstyrte tiltak på området
* innspel og råd til verksemdsleiinga sin gjennomgang
* innspel og råd rundt fellessikring i verksemda

## Øvingar

Verksemdsleiinga er ansvarleg for at det minst en gang i året gjennomførast ei øving på informasjonssikkerheitsområdet. Fagansvarleg informasjonssikkerheit skal være sentral i gjennomføringa. Øvingane skal evaluerast, slik at man fangar opp behov for kompetanseheving eller andre behov for forbetringar.

# Kommunikasjon

## Formidle nye føringar

Nye eller oppdaterte føringar skal formidlast raskt og effektivt til dei som har eller kan få bruk for dei. Ansvaret ligg hos dei som godkjenner føringane. Dokumentasjon og formidlingskanal skal vere i samsvar med våre felles krav til dokumentasjon av internkontroll.

Dei ansvarlege skal alltid vurdere om det i tillegg er behov for eigne informasjonsmøte, opplæringstiltak o.l. Føremålet er å forsikre seg om at informasjonen er tilgjengeleg for mottakarane når dei har behov for den, at den er forstått, samt at mottakaren har haldningar og tilstrekkeleg kompetanse til å etterleve føringane. Ved behov skal den ansvarlege sørge for at føremålstenlege tiltak vert gjennomførte.

## Dokumentere gjennomførte styringsaktivitetar

Gjennomføring av styringsaktivitetar beskrivne i dette dokumentet skal som hovudregel dokumenterast skriftleg. Eit kort notat vil ofte vere nok. Arkivering og journalføring skal skje i samsvar med våre felles krav til dokumentasjon av internkontroll.

## Dokumentere etterleving av tryggingstiltak

Viss tryggingstiltak, prosedyrar eller rutinar stiller krav om det, skal etterlevinga av dei dokumenterast skriftleg. Slike krav skal vere baserte på risiko og behov. Eventuelle dokumentasjonskrav på etterleving skal vere ein del av beskrivinga av tiltaket.

Dokumentasjonskrav skal leggast opp på ein måte som gjer at dei ikkje vert opplevde som unødvendige eller vesentleg hemmande for anna viktig arbeid.

## Statusrapportar som grunnlag for risikovurderingar

Fagansvarleg informasjonssikkerheit skal i januar kvart år lage ein rapport over status og trendar på informasjonssikkerheitsområdet både internt i verksemda og i samanliknbare verksemder eksternt. Rapporten skal vere bakgrunnskunnskap for dei som skal vurdere risiko rundt om i verksemda. Rapporten må vere tilpassa det føremålet.

## Saksnotat til verksemdsleiinga sin gjennomgang

Fagansvarleg informasjonssikkerheit skal seinast to veker før verksemdsleiinga sin gjennomgang produsere eit saksnotat til gjennomgangen. Det skal også utarbeidast og leggast ved ein tilpassa rapport om status på relevante område innan informasjonssikkerheit. Notatet og rapporten skal vere tilpassa dei føringar verksemdsleiinga har gitt frå tidlegare gjennomgangar.

## Kommunikasjon mellom aktivitetar og aktørar

Alle aktivitetar i dette dokumentet føreset ein rask og effektiv kommunikasjon med andre aktivitetar og mellom ulike aktørar. Det er eit ansvar for alle tilsette å bidra til at riktig informasjon kjem fram til riktig person til riktig tid. Ivaretaking av lovpålagt teieplikt ligg i omgrepet *riktig informasjon til riktig person.*

## Dialog med styrande organ

Status på arbeidet med styring av informasjonssikkerheit skal rapporterast til styrande departement i etterkant av verksemdsleiinga sin gjennomgang, i årsrapporten og i den løpande styringsdialogen etter behov.

## Ekstern kommunikasjon

Eventuell kommunikasjon med personar utanfor vår verksemd om risikoar, tiltak, internkontroll, informasjonssikkerheit, mv., skal skje i samsvar med vår policy og retningslinjer for ekstern kommunikasjon. Det gjeld både innhald og kven som uttaler seg om kva.

Lovpålagt teieplikt og offentleglovas reglar om unntatt offentlegheit og meiroffentlegheit skal ligge til grunn for all kommunikasjon.

1. «Høgaste konsekvensnivå» er det høgaste nivået på konsekvensar på området som ein med ei viss grad av sannsyn må rekne med kan inntreffe. Urealistiske utfall vert derfor haldne utanfor. [↑](#footnote-ref-2)
2. Fellessikring er eit sett av sikkerheitstiltak som er etablert for å gje eit felles grunnleggande sikkerheitsnivå for sentrale område av verksemda [↑](#footnote-ref-3)