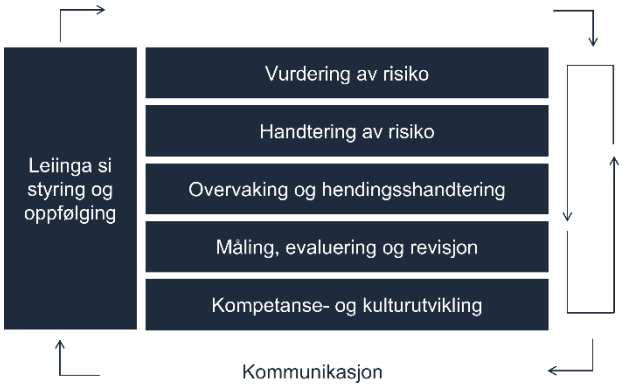
Anbefalte delaktivitetar og dokumentasjon

Støttedokument

Dette er ei oversikt over dei delaktivitetar og den dokumentasjon Digitaliseringsdirektoratet anbefaler for internkontroll på informasjonssikkerheitsområdet. Oversikta er laga for å gi støtte under aktivitetane *Analysere status* og *Planlegge etablering/forbetring.* Strukturen følgjer styringsaktivitetane i Digitaliseringsdirektoratet sin forklaringsmodell (jf. under). Det har inga betyding for analyse og seinare plan om verksemda har valt eller vel ein annan struktur på sitt internkontrollarbeid.



Innhold

Innleiing

Dei sju første aktivitetane er styringsaktivitetane (jf. figuren innleiingsvis). Den siste, etableringsaktivitetar, er aktivitetar som bør gjennomførast når ei verksemd første gong skal etablere styring på informasjonssikkerheitsområdet. Etableringsaktivitetane vil også vere aktuelle ved behov for oppdatering eller vesentlege forbetringar av grunnleggande delar ein allereie har.

I ein analyse av status vil det vere mest føremålstenleg å vurdere status på styringsaktivitetane først. Det gir eit betre grunnlag for å vurdere behova rundt etableringsaktivitetane.

I ein påfølgande plan vil det oftast vere føremålstenleg å plassere gjennomføring av dei mest sentrale etableringsaktivitetane tidleg i planen, medan tiltak for å få i gang eller forbetre styringsaktivitetane kan kome gradvis. Planen bør utformast som ein ordinær prosjektplan. Dette støttedokumentet og tilhøyrande utfylte analyseskjema bør vere sentral støtte i planlegginga.

Kvar hovudaktivitet består av eit sett delaktivitetar. Dei er punktvis beskrivne under.

1 Leiinga si styring og oppfølging

1.1 Verksemdsleiinga sin gjennomgang

- Bør gjennomførast minst årleg av toppleiinga i verksemda.
- Kan med fordel gjennomførast i toppleiargruppa.
- Gjennomgangen bør vere førebudd av fagansvarleg informasjonssikkerheit i samsvar med føringar frå toppleiar og tidlegare gjennomgangar.
- Innhald og fokus vil naturleg variere over tid avhengig av status i verksemda.
- Gjennomgangen må som minimum sikre at ein har gode føringar og hensiktsmessige styrande dokument, og at dei vert etterlevde.
- Ved behov skal toppleiar
    - sørge for at det skjer ei etablering/forbetring av føringane (jf. 8.1)
    - gi eventuelle tilleggsføringar for arbeid med styring av informasjonssikkerheit
    - vurdere om ein skal måle tilstanden på definerte indikatorar over tid, eller få gjennomført evalueringar eller internrevisjon (jf.5.2, 5.3 og 5.4)

Anbefalt dokumentasjon:

- Gode styrande dokument (jf. 8.1) som svarar til Digitaliseringsdirektoratet sine anbefalingar og døme for
    - ein kort overordna policy for informasjonssikkerheit
    - tydelege retningslinjer om
        - rollar og ansvar
        - å forstå, vurdere og handtere risiko
        - korleis ein systematisk skal vurdere behov for risikovurderingar
    - ei eventuell retningslinje eller overordna rettleiing om aktivitetar og ansvar innan styring av informasjonssikkerheit, som utdjupar retningslinja om rollar og ansvar
- Systematiske saksnotat til verksemdsleiinga (jf. 7.5).
- Systematiske avgjerslenotat som viser verksemdsleiinga sine avgjersler etter gjennomgangen.

1.2 Delegere og følgje opp gjennom linjen

- Leiarar på alle nivå bør jamleg vurdere kva som er føremålstenleg oppdeling eller gruppering av underliggande områder, arbeidsoppgåver og IKT-system, og på kva måte det operative ansvaret som risikoeigar, systemeiga og felles tiltaksleverandør eventuelt skal delegerast.

- For å sikre ei kostnadseffektiv gjennomføring bør leiarane jamleg vurdere om nokon styringsaktivitetar skal gjennomførast som fellesaktivitetar på eit høgare organisatorisk nivå enn delegeringa tilseier.
- Det som vert delegert må følgast opp. Dette bør skje som ein del av den ordinære linjestyringa, årsplanlegginga og linjeoppfølginga.

Anbefalt dokumentasjon:

- Styringsinformasjon bør formidlast i den ordinære linjestyringa med aktuell delegering av styringsaktivitetar på informasjonssikkerheitsområdet.
- Ordinær rapportering gjennom linja om
  - gjennomføring av styringsaktivitetane
  - status på informasjonssikkerheitsarbeidet elles i eiga eining
    - nokre av dei same temaa som er nemnt under saksnotatet til Verksemdsleiinga sin gjennomgang, avhengig av lokale utfordringar

1.3 Sikre finansielle rammar

- Leiarar på alle relevante nivå må sørge for at økonomiske erfaringar og behov rundt styringsaktivitetar og tryggingstiltak er tema når budsjettrammar vert vurderte og diskuterte i verksemda.

Anbefalt dokumentasjon:

- Budsjett og verksemdsplanar inneheld tydeleg nødvendige ressursar til arbeid med styring av informasjonssikkerheit og tryggingstiltak.
- Budsjetta er så fleksible at dei kan dekkje sikkerheitsmessige behov som dukkar opp.

1.4 Kommunisere viktigheit

- Leiarar på alle nivå må systematisk kommunisere viktigheita av både informasjonssikkerheit, dei tryggingstiltaka som er sette i verk og styringsaktivitetane.
- Leiinga si haldning kjem til uttrykk gjennom det leiinga seier og gjer. Kommunikasjonen bør derfor skje både munnleg, skriftleg og gjennom synleg handling.

1.5 Løfte og handtere problemstillinger gjennom linja

- Viss problemstillingar i internkontrollarbeidet ikkje kan løysast på det organisatoriske nivå dei oppstår, skal dei løftast gjennom linja og handterast på eit høgare leiarnivå.
- Dei skal løftast gjennom linja til ein når eit leiarnivå som har økonomisk handlingsrom eller myndigheit til å finne budsjettdekning, akseptere aktuelle risikoar eller ta andre nødvendige avgjersler.
- Årsaka kan m.a. vere manglande finansiering, at kriteria for å akseptere risiko seier at kun leiarar på eit visst nivå kan akseptere store restrisikoar, ueinigheit mellom ulike oppgåveeigarar som nyttar same IKT-system, arbeidslokale e.l., ueinigheit i verksemda om kva tiltak som skal inngå i verksemda si fellessikring og gjelde alle, og kva som bør vere tilleggssikring for dei som har ekstra behov.

Anbefalt dokumentasjon:

- Problemstillingar av vesentleg betyding og tilhøyrande avgjersler vert journalførte og arkiverte.

1.6 Beredskap og krisehandtering

- Leiarar på ulikt nivå vil vere sentrale aktørar i det meste av beredskap og krisehandtering.
- Det er avgjerande at verksemda har gode prosedyrar med klare ansvarslinjer og nødvendig samordning.

- Verksemda må også ha systematiske øvingar for å sikre etterleving på alle leiarnivå.

Anbefalt dokumentasjon:

- Beredskaps- og kriseplanar på verksemdsleiarnivå og for ulike verksemdskritiske arbeidsoppgåver og funksjonar.

2 Vurdering av risiko

- Alle delaktivitetane under Vurdering av risiko bør gjennomførast av eller på oppdrag for risikoeigarar og systemeigarar fellessystem.
- Leiarar som er ansvarlege for å nå mål og få utført tilhøyrande arbeidsoppgåver er normalt verksemda sine risikoeigarar. Dette er oftast alle leiarane på ulike nivå rundt om i verksemda.
- Risikoane er potensielle avvik frå mål risikoeigarane heilt eller delvis er ansvarlege for å nå.
- Risikoeigarane er normalt systemeigarar for eigne IKT-system, og desse er ein del av deira ansvarsområde.
- Systemeigarar fellessystem skal ivareta interessene til alle risikoeigarane som nyttar fellessystema til sine oppgåver. IKT-infrastruktur er eit fellessystem. Det same er typisk e-postsystem og arkivsystem.
- Risikoeigarar som bruker fellessystem er også risikoeigarar for eiga informasjonsbehandling i fellessystema. Dei skal derfor i tilstrekkeleg grad og på føremålstenleg måte involverast i risikovurderingsarbeid mv. som vert utført på fellessystema.
- Leiarar på verksemdsnivå, avdelingsnivå o.l. må passe på å sjølv gjennomføre desse delaktivitetane rundt eigne leiaroppgåver. Dei er normalt sjølv risikoeigarar for desse.

2.1 Ha oversikt og prioritere

- Skal gjennomførast av risikoeigarar rundt om i verksemda og av systemeigarar fellessystem. Det er viktig med ein prosessleiar ved første gongs gjennomføring. Heile eller delar av gjennomføringa kan gjerne gjerast for ei leiargruppe i ei organisatorisk eining samla, og alle oppgåvene dei har ansvaret for.
- Risikoeigarar skal på eit overordna nivå identifisere oppgåver og tenester dei har ansvaret for, sentral informasjon som vert behandla, regelverk som må følgast og kva IKT-system som vert nytta.
- Dei skal deretter anslå potensielt konsekvensnivå ved brot på konfidensialitet, integritet og tilgjenge rundt eigne arbeidsoppgåver, IKT-systema som vert nytta og spesielle hjelpemiddel.
- Systemeigarar fellessystem skal som første trinn anslå potensielt 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 er viktig bakgrunnsinformasjon.
- Alle skal deretter gjere ei overordna vurdering av nivået på relevante truslar, farar og sårbarheiter rundt eige ansvarsområde og merke seg dei som peiker seg spesielt ut.
- Risikoeigarar og systemeigarar fellessystem skal ved behov identifisere og tydeleggjere konkrete krav i regelverk og avtalar som ein må ta omsyn til i arbeidet. Skal gjennomførast for dei regelverk og avtalar som ikkje er tydeleggjort nok på verksemdsnivå (jf. pkt. 8.8).
- For å få fokus på det viktigaste, behandle like ting saman og få målretta tidsbruk på konkrete risikovurderingar, skal alle deretter gruppere det som vert sett som enkelt og oversiktleg og dele opp og skilje ut det som vert sett som kritisk eller som det er knytt spesiell usikkerheit til. Det gjeld både oppgåver og tenester, IKT-system og deler av desse.

- Alle skal så systematisk vurdere behovet for oppdaterte eller nye risikovurderingar for dei ulike delane av eige ansvarsområde. Dei skal også prioritere mellom nødvendige risikovurderingar. Verksemda si retningslinje for dette skal gi føringar.
- 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.
- Resultatet frå det å få oversikt og prioritere skal revurderast og eventuelt oppdaterast minst ei gong årlig. Relevante deler av aktiviteten skal alltid gjennomførast og oppdaterast før nye typar arbeidsoppgåver startar, eller før nye IKT-system vert anskaffa og tekne i bruk.

Anbefalt dokumentasjon:

- Risikoeigarane sine oversikter over oppgåver og tenester, informasjonstypar, regelverk og IKT-system.
- Risikoeigarar og systemeigarar fellessystem sine
    - oversikter over potensielle konsekvensnivå på arbeidsoppgåver, IKT-system m.v.
    - overordna vurderingar av nivået på relevante truslar, farar og sårbarheiter rundt eige ansvarsområde
    - oversikt over konkrete tiltak eller typar tiltak som vert kravde i avtalar eller regelverk for aktuelle arbeidsoppgåver eller IKT-system. Detaljeringsnivå er avhengig av behov.
    - oppdelingar i grupper og delområde og oversikt over kva behov det er for oppdaterte risikovurderingar på dei
    - oversikter over planlagde og gjennomførte risikovurderingar

2.2 Planlegge risikovurdering

- Systematisk planlegging av gjennomføringa av kvar einskild risikovurdering.
- Skal gjennomførast i samarbeid mellom den aktuelle risikoeigar/systemeigar fellessystem og den som vert peika ut som prosessleiar for risikovurderinga.

Anbefalt dokumentasjon:

- Tydeleg mandat for risikovurderinga.

2.3 Gjennomføre risikovurdering

- Systematisk gjennomføring av risikovurderingar det er identifisert behov for.
- Skal gjennomførast under leiing av ein utpeika prosessleiar.
- Følgjer ein systematisk metode, som til dømes den Digitaliseringsdirektoratet foreslår i dette rettleiingsmateriellet.
- Omfang og innretning på arbeid og metodebruk må tilpassast det som vert risikovurdert.

Anbefalt dokumentasjon:

- Risikonotat som kort summerer opp vesentlege delar frå arbeidet.
- Ein vedlagt risikotabell som minimum viser risikobeskriving, konsekvensnivå, tilhøyrande sannsynsnivå og risikonivå for dei identifiserte risikoane.
- Eventuelt andre vedlegg som ved behov utdjupar analysar som er gjennomførte.

2.4 Vurdere risiko etter hendingar

- Systematisk behovsvurdering og eventuell gjennomføring av avgrensa risikovurderingar når informasjonssikkerheitshendingar vert rapporterte til ein oppgåveeigar eller systemeigar.

Anbefalt dokumentasjon:

- Eit kort situasjonstilpassa risikonotat.

2.5 Vurdere risiko ved anskaffingar og utvikling

- Systematisk behovsvurdering og ev. gjennomføring av tilpassa risikovurderingar ved anskaffingar og systemutvikling.

Anbefalt dokumentasjon:

- Behovs- og kravlister til anskaffings- eller utviklingsprosessen. Desse kan utformast i forkant av anskaffinga eller gradvis i anskaffings- eller utviklingsprosessen, avhengig av kva framgangsmåte ein nyttar.

3 Handtering av risiko

3.1 Foreslå handtering av risikoar

- Systematisk oppfølging av føregåande risikovurdering der det er identifisert risikoar som ikkje kan aksepterast utan nærare tiltaksvurdering.
- Vert ofte gjennomført direkte i forlenginga av ei risikovurdering.
- Vert gjennomført under leiing av ein prosessleiar utpeika av aktuell risikoeigar eller systemeigar fellessystem. Det vil ofte vere den same som leia tilhøyrande risikovurdering.
- Følgjer ein systematisk metode, som til dømes den Digitaliseringsdirektoratet foreslår i dette rettleiingsmateriellet.

Anbefalt dokumentasjon:

- Eit eige risikohandteringsnotat eller ei forlenging av risikonotatet frå risikovurderinga, som kort summerer opp vesentlege deler frå arbeidet.
- Eit vedlagt risikohandteringsskjema som viser kva tiltak som vert anbefalt for dei risikoane som bør handterast.
- Ein kopi av den opphavlege risikotabellen med oppdatering av kva tiltak som er foreslått for kvar risiko og kva det betyr for konsekvensnivå, tilhøyrande sannsynsnivå og risikonivå (restrisiko).
- Eventuelt andre vedlegg som ved behov utdjupar analysar, nytte-/kostvurderingar e.l. som er gjennomførte.

3.2 Godkjenne forslag til risikohandtering

- Skal gjennomførast av aktuell risikoeigar eller systemeigar fellessystem.
- Ei systematisk vurdering av forslaget til handtering av risikoar.

Anbefalt dokumentasjon:

- Avgjersle med aksept av risikoane og tiltaka, retur til førre delaktivitet for meir arbeid med tiltaksforslag eller løfting av uavklarte problemstillingar gjennom linja.

3.3 Settje i verk godkjende tiltak

- Skal gjennomførast av ein handteringsansvarleg peika ut av aktuell risikoeigar eller systemeigar fellessystem.
- Utformar konkret handlingsplan for gjennomføringa, inngår avtalar med dei som skal gjennomføre aktivitetane i handlingsplanen, får planen godkjend av oppdragsgivar og følgjer opp gjennomføringa.

Anbefalt dokumentasjon:

- Handlingsplan med tilhøyrande framdriftsrapportering.

3.4 Utforme og etablere tryggingstiltak

- Konkrete tiltak skal utformast, setjast i verk og haldast ved like av tiltaksleverandørar.
- Dette kan vere felles tiltaksleverandørar internt eller eksternt med ansvar som IT-drift, IT-utvikling, eigedom/bygningar, felles personalrutinar o.l.
- Det kan også vere personar hjå aktuell risikoeigar eller systemeigar fellessystem som får ansvar for utvikling av prosedyrar, rutinar, opplæring o.l.
- Testing av tiltaka må gjennomførast som avtalt.

Anbefalt dokumentasjon:

- Dokumentasjon av det einskilde tiltaket avhengig av eigenarta til tiltaket.
- Avtalt rapportering til aktuelle handteringsansvarlege.
- Samla oversikt over alle tiltak i samsvar med overordna føringar.

3.5 Oppdatere fellessikring og tilleggssikring

- Oppdatering av fellessikring skal initierast og gjennomføras viss tiltaksleverandørar meiner nye tiltak best kan etablerast som del av fellessikringa i verksemda, og dermed skal gjelde alle i verksemda.
- Tiltak som ikkje er eigna som fellessikring, men som kan vere aktuelle som tilleggssikring, skal gjerast synlege som tilgjengeleg tilleggssikring.
- Vurderinga skal koordinerast systematisk på verksemdsnivå og gjennomførast som forenkla utgåve av pkt. 8.2.1 *Etablere fellessikring og synleggjere tilleggssikring*.

Anbefalt dokumentasjon:

- Oppdatering av oversikta over fellessikringa i verksemda (jf. pkt. 8.5).

4 Overvaking og hendingshandtering

4.1 Overvake i samsvar med avtale

- Skal gjennomførast systematisk av tiltaksleverandørar for die områda der overvaking er eit avtalt sikkerheitstiltak.

Anbefalt dokumentasjon:

- Eventuelt krav om dokumentasjon av at overvaking vert gjennomført, skal vere ein del av krava til overvakinga.

4.2 Rapportere hendingar, avvik og informasjonssikkerheitsbrot

- Skal gjennomførast systematisk av alle tilsette.
- Systemet etablert for hendings- og avvikshandtering (jf. pkt. 8.4) skal nyttast.

Anbefalt dokumentasjon:

- Nødvendig dokumentasjon skal vere integrert i systemet for hendings- og avvikshandtering.

4.3 Følgje opp hendingar, avvik og informasjonssikkerhetisbrot

- Dei som er ansvarlege for oppfølging av hendingar handterer desse i samsvar med gjeldande rutinar i hendings- og avvikshandteringa.

Anbefalt dokumentasjon:

- Dokumentasjon av oppfølginga skal vere integrert i systemet for hendings- og avvikshandtering.

5 Måling, evaluering og revisjon

5.1 Vurdere status på eige ansvarsområde

- Minst ei gong i året skal følgjande vurdere status for sine ansvarsområde:
  - Leiarar som delegerer og skal følgje opp gjennom linja
  - Risikoeigarar
  - Systemeigarar fellessystem
  - Tiltaksleverandørar
  - Ansvarlege for tenestenivåavtalar eller andre avtalar
  - Ansvarlege for eigne deler av styringsaktivitetane, som til dømes hendingshandteringssystemet og internrevisjon
- Statusvurderinga skal omfatte vurderingar av om ein sjølv, eigne tilsette og leverandørar
  - følgjer gjeldande lov- og regelverk
  - gjennomfører styringsaktivitetane slik ein er pålagt
  - etablerer og følgjer 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 saka vert sett å vere, både for verksemda og eiga eining. Er tilliten høg, er det normalt ingen grunn til ytterlegare undersøkingar. Det føreset 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.

Anbefalt dokumentasjon:

- Resultatet av statusvurderinga saman med kva undersøkingar og oppfølgingstiltak som er gjennomførte, bør dokumenterast i eit kort notat.

5.2 Måle tilstanden på definerte indikatorar

- Verksemdsleiinga kan vedta at dei vil følgje tilstanden over tid på einskilde områder, jf. pkt.1.1.
- Dei skal då peike ut nokre ansvarlege som skal utarbeide forslag til systematiske målingar, inkludert område, indikatorar, metodar, frekvens, ansvarlege og rapportering. Vedtak skal gjerast av verksemdsleiinga.
- Målingane skal gjennomførast av dei som vert peika ut til det gjennom linjeavgjersler.
- Resultata skal stillast saman av fagansvarleg informasjonssikkerheit og presenterast for verksemdsleiinga, normalt som del av verksemdsleiinga sin gjennomgang.

Anbefalt dokumentasjon:

- Samanstilte resultatet av målingane samanlikna over tid.

5.3 Gjennomføre evalueringar

- Verksemdsleiinga kan avgjere at det skal gjennomførast evalueringar, jf. pkt.1.1. Evalueringar kan omfatte heile eller deler av arbeidet med styring av 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, til dømes krav om «sikkerheitsrevisjonar» e.l.. Slike krav vil normalt dekkjast av målretta evalueringar.

- Oppdragsgivar skal peike ut dei som skal vere ansvarlege 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 oppdragsgivar. Eventuelle avvik skal følgjast opp.

Anbefalt dokumentasjon:

- Evalueringsrapportar

5.4 Gjennomføre internrevisjon

- Føremålet med ein internrevisjon er å få ei formell vurdering av om verksemda følgjer bestemte krav, og om krava er implementerte og haldne ved like på en føremåls- og kostnadseffektiv måte.
- Verksemdsleiinga kan vedta at det skal gjennomførast internrevisjon, jf. pkt. 1.1. Ein internrevisjon kan omfatte heile eller deler av arbeidet med styring av informasjonssikkerheit i verksemda.
- Internrevisjonen 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.

Anbefalt dokumentasjon:

- Revisjonsrapportar

6 Kompetanse- og kulturutvikling

6.1 Identifisere behov løpande

- Identifisering av behov for kompetanse- og kulturutvikling skal gjerast løpande som ein del av arbeidet med styring av informasjonssikkerheit 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

Anbefalt dokumentasjon:

- Identifiserte behov for kompetanse- og kulturutvikling.

6.2 Følgje opp behova systematisk

- Når det er identifisert eit behov skal det gjennomførast føremålstenlege tiltak. Tiltaka skal
    - vere tilpassa riktig målgruppe
    - ta i bruk føremålstenleg(e) verkemiddel
    - sjåast i samanheng med andre opplæringstiltak i verksemda
    - vere tilrettelagt slik at ein kan måle effekten av tiltaket.

Anbefalt dokumentasjon:

- Planar for kompetanse- og kulturutvikling.

6.3 Følgje opp lokale sikkerhetskoordinatorer

- Fagansvarleg informasjonssikkerheit og verksemda sine lokale sikkerheitskoordinatorar 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

Anbefalt dokumentasjon:

- Oppsummeringsnotat frå møta med sikkerheitskoordinatorane.

6.4 Øvingar

- Øvingar på området informasjonssikkerheit skal gjennomførast minst årleg for å
  - auke kompetansen og kunnskapen til dei tilsette
  - avdekke om det er behov for å hente inn fleire ressursar
  - gi dei tilsette trening i å arbeide i lag
  - avdekke behov for kompetanse- og kulturutvikling

Anbefalt dokumentasjon:

- Plan for øvingar
- Materiale frå gjennomføring
- Evalueringsrapportar etter gjennomføring, med punkt for læring og oppfølging

7 Kommunikasjon

7.1 Formidle nye føringar

- Nye eller oppdaterte føringar skal formidlast raskt og effektivt til dei som har eller kan få bruk for dei. Ansvaret ligg hjå dei som godkjenner føringane.

Anbefalt dokumentasjon:

- Dokumentasjon og formidlingskanal skal vere i samsvar med verksemda sine felles krav til dokumentasjon av internkontroll.

7.2 Dokumentere gjennomførte styringsaktivitetar

- Gjennomføring av styringsaktivitetar skal som hovudregel dokumenterast skriftleg.

Anbefalt dokumentasjon:

- Eit kort notat vil ofte vere nok. Arkivering og journalføring bør skje i samsvar med verksemda sine felles krav til dokumentasjon av internkontroll.

7.3 Dokumentere etterleving av tryggingstiltak

- Viss tryggingstiltak, prosedyrar eller rutinar stiller krav om det, skal etterlevinga av dei dokumenterast skriftleg. Slike krav skal vere basert på risiko og behov.
- Dokumentasjonskrav skal leggjast opp på ein måte som gjer at dei ikkje vert opplevde som unødvendige eller vesentleg hemmande for anna viktig arbeid.

Anbefalt dokumentasjon:

- Eventuelle dokumentasjonskrav på etterleving skal vere ein del av beskrivinga av tiltaket.

7.4 Utarbeide statusrapporter som grunnlag for risikovurderingar

- Fagansvarleg informasjonssikkerheit skal ein gong i året 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 gjennomføre risikovurderingar rundt om i verksemda. Rapporten må vere tilpassa det føremålet.

Anbefalt dokumentasjon:

- Statusrapport som grunnlag for risikovurderingar.

7.5 Utarbeide saksnotat til verksemdsleiinga sin gjennomgang

- Fagansvarleg informasjonssikkerheit skal i god tid før verksemdsleiinga sin gjennomgang produsere eit saksnotat til gjennomgangen. Det skal også utarbeidast og leggjast 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.

Anbefalt dokumentasjon:

- Systematiske saksnotat til verksemdsleiinga (jf. 1.1) med tema som til dømes
  - status på vedtekne tiltak etter tidlegare gjennomgangar
  - bakgrunnskunnskap om trendar og utfordringar lokalt og nasjonalt
  - status på arbeidet med styring av informasjonssikkerheit
  - tilbakemeldingar på informasjonssikkerheitsnivået
  - status på risikoar eller risikoområde leiinga er spesielt opptekne av
  - moglegheiter for forbetring

7.6 Kommunikasjon mellom aktivitetar og aktørar

- Alle styringsaktivitetar føreset ein rask og effektiv kommunikasjon med andre delaktivitetar 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.

Anbefalt dokumentasjon:

- Dokumentasjon skal vere i samsvar med krav i dei einskilde delaktivitetane.

7.7 Dialog med styrande organ

- Kommunikasjon om informasjonssikkerheit til eit overordna eller styrande organ.
- Vil normalt inngå som ein del av dialog om verksemda sin risiko og styring og kontroll i verksemda.
- Styringsdialogen mellom departement og underliggande statleg verksemd er eit døme på slik kommunikasjon.

Anbefalt dokumentasjon:

- Dokument og dokumentasjon i samsvar med behov og krav for slik dialog. Til dømes i tråd med føringar for, og rettleiing om, styringsdialogen mellom departement og underliggande statleg verksemd.

7.8 Ekstern kommunikasjon

- Eventuell kommunikasjon med personar utanfor verksemda om risikoar, tiltak, internkontroll, informasjonssikkerheit, mv., skal skje i samsvar med verksemda sin policy og

retningslinjer for ekstern kommunikasjon. Det gjeld både innhald og kven som uttaler seg om kva.

8 Etableringsaktivitetar

Etableringsaktivitetar er eit sett av spesielle aktivitetar. Dei vert gjennomførte ut frå behov ved første gongs etablering av styring på informasjonssikkerheitsområdet, eller ved behov for oppdatering eller vesentleg forbetring av grunnleggande delar ein allereie har.

I rettleiingsmateriellet frå Digitaliseringsdirektoratet er dei to første etableringsaktivitetane *Analysere status* og *Planlegge etablering/forbetring*. Dei er ikkje tekne med i oversikta her på grunn av deira eigenart og fokus.

Analysere status er det som vert gjort ved hjelp av dette støttedokumentet og tilhøyrande analyseskjema. *Planlegge etablering/forbetring* er det som skal gjerast viss analysen viser vesentlege avvik frå Digitaliseringsdirektoratet sine anbefalingar, og verksemdsleiinga bestemmer at verksemda skal gjennomføre eit systematisk arbeid for å rette på forholda.

Under følger andre anbefalte etableringsaktivitetar ein bør ta stilling til status på og behovet for.

8.1 Utforme føringar

- Er ein føresetnad for og den viktigaste delen i eit systematisk internkontrollarbeid på informasjonssikkerheitsområdet.
- Etablering/forbetring skal ideelt sett initierast av verksemdsleiinga, jf. pkt. 1.1, som må eige dokumenta.
- Må utformast med god involvering og forankring både hjå verksemdsleiinga og ut i organisasjonen elles.
- Delar av arbeidet og dokumenta kan med fordel integrerast som fellesarbeid for fleire internkontrollområde og utformast i eit samarbeid med fagansvarlege på desse områda.
- I ein analyse av eigen status er det særs viktig med kvalitative vurderingar av innhaldet i det ein har, opp mot Digitaliseringsdirektoratet sine døme og anbefalingar på overordna styrande dokument.

Anbefalt dokumentasjon:

- Gode styrande dokument (jf. pkt. 1.1) som svarar til Digitaliseringsdirektoratet sine anbefalingar og døme for:
  - Policy for informasjonssikkerheit
  - Retningslinjene
    - Rollar og ansvar
    - Forstå, vurdere og handtere risiko
    - Vurdere behov for risikovurderingar
  - Ei retningslinje eller overordna rettleiing om aktivitetar og ansvar innan internkontroll informasjonssikkerheit, som utdjupar retningslinja om rollar og ansvar

8.2 Få på plass nøkkelpersonar

- Ut frå av status i verksemda, utfordringar og eigenart, samt føringar for roller og ansvar, må ein
  - setje av ressursar til å dekke rollane når det er behov for at de vert aktiverte
  - peike ut eller tilsette fagansvarleg informasjonssikkerheit eller tilsvarande – viss ein ikkje har dekt rolla allereie eller ikkje har nok kompetanse/ressursar p.t.

  - peike ut andre sentrale rollar som felles tiltaksleverandørar for ulike område, prosessleiarar for risikovurderingar o.l., lokale sikkerheitskoordinatorar mv.
  - peike ut klare systemeigarar for IKT-system – viss det ikkje er gjort tidlegare (både fellessystem og system for den einskilde risikoeigar)
  - etablere eventuelle nye forum
  - etablere dei arbeidsgrupper ein har behov for i etableringsfasen av arbeidet med styring av informasjonssikkerheit
- Det meste av det som er nemnt over bør kome på plass gradvis og bør leggast inn i planen for å etablere/forbetre styringa av informasjonssikkerheit.
- Fagansvarleg informasjonssikkerheit er den viktigaste rolla å få på plass tidleg. Vedkommande har ei sentral rolle som leiarstøtte og pådrivar for det samla arbeidet med styring av informasjonssikkerheit, og vil normalt vere ansvarleg for nemnte plan.

8.3 Grunnopplæring

- Bør gjennomførast viss verksemda manglar viktig kompetanse i etableringsfasen av styring på informasjonssikkerheitsområdet
- Ut frå behov bør ein anskaffe eller utvikle
  - grunnleggande informasjonsmateriell eller kurs for leiarar om informasjonssikkerheit
  - grunnopplæring for leiarar i sentrale styringsaktivitetar informasjonssikkerheit
  - grunnopplæring prosessleiarar i *Ha oversikt og prioritere* (jf. pkt. 2.1), *Gjennomføre risikovurdering* (jf. pkt. 2.3) og *Foreslå handtering av risikoar* (jf. pkt. 3.1).
  - grunnopplæring for handteringsansvarlege som har ei sentral rolle i aktiviteten *Settje i verk godkjende tiltak* (jf. 3.3)
  - grunnleggande kurs/opplæring i informasjonssikkerheit for tilsette
- Alle kursa bør vere tilpassa styringsaktivitetane og sikkerheitskrava i verksemda
- Opplæringa bør leggast inn i planen for etablering/forbetring slik at tidspunkt for gjennomføring vert tilpassa aktivitetane der

Anbefalt dokumentasjon:

- Informasjons- og opplæringsaktivitetar integrert i planen for å etablere/forbetre styringa av informasjonssikkerheit.

8.4 Etablere system for hendelses- og avvikshåndtering

- Bør gjennomførast viss verksemda manglar eit godt og velfungerande system for hendings- og avvikshandtering som også dekker informasjonssikkerheit.
- Eit slikt system kan med fordel integrerast og nyttast som fellessystem på tvers av fleire internkontrollområde
- Systemet er ikkje berre eit IT-system, men like mykje klargjering av ansvar, prosedyrar og rutinar.
- Systemet bør omfatte krav om kva som skal rapporterast, kven som skal rapportere, korleis rapporteringa skal skje og kven som skal handtere kva.
- Informasjonsflyt for ulike typar hendingar bør vere klart definert.
- Det må sikrast at innrapporterte hendingar av ulike typar vert handterte av rette vedkomande innan gitte fristar.
- Ved behov må beredskapsplanar eller andre konsekvensreduserande tiltak settast i verk utan ugrunna opphald.
- Det bør alltid vurderast om ein kan lære av erfaringane frå ei hending. Særleg bør det vurderast om hendingane og avvika tilseier justering av risikovurderingar og tilhøyrande tiltak. Kunnskapen må brukast i det vidare risikovurderingsarbeidet.

Anbefalt dokumentasjon:

- Systemet bør innehalde den dokumentasjon som er nødvendig ut frå det som er nemnt over.

8.5 Etablere fellessikring og synleggjere tilleggssikring

- Fellessikring er eit sett av tryggingstiltak som vert etablerte for å gi eit felles grunnleggande sikkerheitsnivå for sentrale område av verksemda. Dei gjeld alle i verksemda.
- Tilleggssikring er sikkerheitstiltak som kan etablerast for bestemte oppgåver eller system som har spesielle behov.
- Føremålet med denne aktiviteten er kombinasjonen av å etablere ei fellessikring som er behovsorientert, forenkle vurderingar og handtering av risiko rundt om i verksemda, og ta omsyn til effektiviseringsbehovet for tiltaksleverandørane.
- Aktiviteten bør gjennomførast viss verksemda manglar ei systematisk etablering og synleggjering av fellessikring og tilleggssikring.
- Aktiviteten bør gjennomførast i eit fellesprosjekt med fagansvarleg informasjonssikkerheit som koordinator, verksemda sine interne tiltaksleverandørar som nøkkelpersonar og nokre utvalde fagområde og risikoeigarar som pilotar.
- **Fase 1** handlar om å få på plass eit utkast til minimumsnivå på fellessikringa
- Tiltaksleverandørane bør gå gjennom eigen praksis og utvalde tiltaksbankar for å identifisere aktuelle tiltak for verksemda.
- Tiltak som klart har vesentleg tyding for dei fleste i verksemda bør leggast inn som forslag til fellessikring. Tiltak som truleg er nyttige for nokon, men som kan ha vesentlege negative sideeffektar for andre, bør leggast inn som mogleg tilleggssikring. Dette bør gjerast uavhengig av om tiltaka i dag gjeld for store delar av verksemda eller berre for nokre få.
- **Fase 2** handlar om å gjennomføre risikovurderingar og utarbeide tilhøyrande forslag til risikohandtering for 2-4 pilotområde i verksemda.
- Valde pilotområde bør vere representative for breidda i verksemda si informasjonsbehandling, både med omsyn til kritikalitet og ressursbruk. I tillegg bør ein vurdere å ta med fellessystem som er mykje brukte.
- Relevante risikoeigarar, systemeigarar fellessystem og sentrale tiltaksleverandørar må vere representerte i arbeidet.
- Risikovurderingane bør gjennomførast med berre førsteutkast til fellessikring i botn (jf. fase 1). Lista med potensiell tilleggssikring bør nyttast som hovudkjelde til forslag til tryggingstiltak i handteringa. Andre tiltak kan takast med ved behov.
- **Fase 3** handlar om å utarbeide eit forslag til fellessikring. Deltakarar er tiltaksleverandørane og representantar for risikoeigarar og systemeigarar fellessystem på pilotområda. Ein bør også vurdere å inkludere ei breiare referansegruppe.
- I vurderinga av kva tiltak frå fase 2 som skal vere verksemda si fellessikring og kva som skal være tilleggssikring må ein balansere fleire forhold. Dette gjeld kostnadseffektiv drift for tiltaksleverandørane opp mot behov, ulemper og kostnadar for dei ulike risikoeigarane.
- **Fase 4** er ei intern høyring i verksemda over forslaget til fellessikring, spesielt med tanke på å identifisere vesentlege ulemper for fagområde som ikkje har vore involverte som pilotar.
- **Fase 5** er eit vedtak frå verksemdsleiinga eller den ho peiker ut basert på høyringa.
- **Fase 6** er iverksetting av vedtaket**.**

Anbefalt dokumentasjon:

- Oversikt over kva tiltaksområde og tilhøyrande tryggingstiltak som inngår i verksemda si fellessikring.
- Oversikt over standardisert tilleggssikring på ulike område som risikoeigarar og systemeigarar fellessystem kan velje ut frå behov.

8.6 Etablere dokumentasjonsrammeverk

- Bør gjennomførast viss verksemda manglar ein tydeleg definert struktur og føringar på dokumentasjon og attfinning av dokument, malar mv.
- Bør i størst mogleg grad etablerast som felles på tvers av alle internkontrollområde i verksemda.
- Bør ta utgangspunkt i det rammeverket eller dei føringane verksemda allereie har.
- Arbeidet bør inkludere fagansvarlege på alle internkontrollområde i verksemda, samt arkivpersonell og kommunikasjonseininga i verksemda.

Anbefalt dokumentasjon:

- Eit dokument som klargjer dokumenthierarki, malar, lagrings- og publiseringsstad mv.

8.7 Identifisere typiske oppgåve- og informasjonstypar

- Bør gjennomførast viss ei oversikt over typiske oppgåve- og informasjonstypar manglar i verksemda eller er særs mangelfull.
- Føremålet med oversikta er å støtte arbeidet i delaktiviteten *Ha oversikt og prioritere* (jf. pkt. 2.1) under hovudaktiviteten *Vurdering av risiko*.
- Digitaliseringsdirektoratet si dømeoversikt vil kunne danne eit første grunnlag for dei fleste. Denne kan då byggast ut og tilpassast eigenarten til verksemda.

Anbefalt dokumentasjon:

- Felles oversikt over typiske oppgåver/tenester som vert utførte i verksemda og kva informasjon som normalt vert behandla i desse
    - Både oppgåver/tenester og informasjonstypar må vere på eit overordna abstraksjonsnivå

8.8 Felles analyse av eksterne krav

- Bør gjennomførast på fellesnivå i verksemda viss viktig regelverk og avtalar gjeld for fleire område i verksemda og fleire har behov for ei konkretisering av krava.
- Identifisere og tydeleggjere konkrete krav i regelverk og avtalar ein må ta omsyn til i arbeidet.
- Fellesarbeidet skal redusere behovet for tilsvarande arbeid rundt om i verksemda i delaktiviteten *Analysere eksterne krav* i *Ha oversikt og prioritere* (jf. pkt. 2.1) under hovudaktiviteten *Vurdering av risiko*.

Anbefalt dokumentasjon:

- Felles oversikt over konkrete tiltak eller typar tiltak som vert kravde i avtalar eller regelverk som gjeld for oppgåver/tenester som vert utførte av fleire i verksemda. Detaljeringsnivå er avhengig av behov.