Anbefalte delaktiviteter og dokumentasjon

Støttedokument

Dette er en samlet oversikt over de delaktiviteter og den dokumentasjon Difi anbefaler for internkontroll på informasjonssikkerhetsområdet. Oversikten er en punktvis versjon laget for å gi støtte under aktivitetene *Analysere status* og *Planlegge etablering/forbedring.* Strukturen følger hovedaktivitetene i Difis forklaringsmodell (jf. under). Det har ingen betydning for analyse og senere plan om virksomheten har valgt eller velger en annen struktur på sitt internkontrollarbeid.

Innhold

Innledning

De syv første hovedaktivitetene er de systematiske aktivitetene i internkontrollarbeidet (jf. figuren innledningsvis). Den siste, etableringsaktiviteter, er aktiviteter som bør gjennomføres når en virksomhet første gang skal etablere internkontroll på informasjonssikkerhetsområdet.

Etableringsaktivitetene vil også være aktuelle ved behov for oppdatering eller vesentlige forbedringer av grunnleggende deler man allerede har.

I en analyse av status vil det være mest hensiktsmessig å vurdere status på de systematiske aktivitetene først. Det gir et bedre grunnlag for å vurdere behovene rundt etableringsaktivitetene.

I en eventuell påfølgende plan vil det oftest være hensiktsmessig å plassere gjennomføring av de mest sentrale etableringsaktivitetene tidlig i planen, mens tiltak for å få i gang eller forbedre de systematiske aktivitetene kan komme gradvis. Planen utformes som en ordinær prosjektplan. Dette støttedokumentet og tilhørende utfylte analyseskjema bør være sentral støtte i planleggingen.

Hver hovedaktivitet består av et sett delaktiviteter. De er punktvis konkretisert under.

1 Ledelsens styring og oppfølging

1.1 Virksomhetsledelsens gjennomgang

- Bør gjennomføres minst årlig av toppledelsen i virksomheten.
- Kan med fordel gjennomføres i toppledergruppen.
- Gjennomgangen bør være forberedt av fagansvarlig informasjonssikkerhet i samsvar med føringer fra toppleder og tidligere gjennomganger.
- Innhold og fokus vil naturlig variere over tid avhengig av status i virksomheten.
- Gjennomgangen må som minimum sikre at man har gode overordnede styrende dokumenter og at de etterleves.
- Ved behov skal toppleder
    - sørge for at det skjer en etablering/forbedring av de overordnede styrende dokumentene (jf. 8.1 Utforme overordnede styrende dokumenter)
    - gi eventuelle tilleggsføringer for virksomhetens internkontrollarbeid innen informasjonssikkerhet
    - vurdere om man skal måle tilstanden på definerte indikatorer over tid, eller få gjennomført evalueringer eller internrevisjon (jf. 5.2, 5.3 og 5.4)

Anbefalt dokumentasjon:

- Gode overordnede styrende dokumenter (jf. 8.1) som tilsvarer Difis anbefalinger og eksempler for
    - en kort overordnet policy for informasjonssikkerhet
    - tydelige retningslinjer om
        - roller og ansvar i internkontroll- og sikkerhetsarbeidet
        - å forstå, vurdere og håndtere operativ risiko
        - hvordan man systematisk skal vurdere behov for risikovurderinger
    - en eventuell retningslinje eller overordnet veiledning om aktiviteter og ansvar innen internkontroll informasjonssikkerhet, som utdyper retningslinjen om roller og ansvar
- Systematiske saksnotat til virksomhetsledelsen (jf. 7.5).
- Systematiske beslutningsnotat som viser virksomhetsledelsens beslutninger etter gjennomgangen.

1.2 Delegere og følge opp gjennom linjen

- Ledere på alle nivå bør jevnlig vurdere hva som er hensiktsmessig oppdeling og gruppering av underliggende områder, arbeidsoppgaver og IKT-system, og på hvilken måte det operative. ansvaret som risikoeier, systemeier og felles tiltaksleverandør eventuelt skal delegeres.

- For å sikre en kostnadseffektiv gjennomføring bør lederne jevnlig vurdere om noen internkontrollaktiviteter skal gjennomføres som fellesaktiviteter på et høyere organisatorisk nivå enn delegeringen tilsier.
- Det som delegeres må følges opp. Dette bør skje som en del av den ordinære linjestyringen, årsplanleggingen og linjeoppfølgingen.

Anbefalt dokumentasjon:

- Styringsinformasjon formidles i den ordinære linjestyringen med aktuell delegering av internkontrollaktiviteter på informasjonssikkerhetsområdet.
- Ordinær rapportering gjennom linjen om
  - gjennomføring av de systematiske aktivitetene i internkontrollarbeidet
  - status på informasjonssikkerhetsarbeidet for øvrig i egen enhet
    - noen av de samme temaene som er nevnt under saksnotatet til Virksomhets-ledelsens gjennomgang, avhengig av lokale utfordringer

1.3 Sikre finansielle rammer for internkontroll- og sikkerhetsarbeidet

- Ledere på alle relevante nivå må sørge for at økonomiske erfaringer og behov rundt internkontrollaktiviteter og sikkerhetstiltak systematisk er tema når budsjettrammer vurderes og diskuteres i virksomheten.

Anbefalt dokumentasjon:

- Budsjetter og virksomhetsplaner inneholder tydelig nødvendige ressurser til internkontrollarbeid og sikkerhetstiltak.
- Budsjettene er så fleksible at de kan dekke sikkerhetsmessige behov som dukker opp.

1.4 Kommunisere viktighet

- Ledere på alle nivå må systematisk kommunisere viktigheten av både informasjonssikkerhet, de iverksatte sikkerhetstiltakene og de systematiske aktivitetene i internkontrollarbeidet.
- Ledelsens holdning kommer til uttrykk gjennom det ledelsen sier og gjør. Kommunikasjonen bør derfor skje både muntlig, skriftlig og gjennom synlig handling.

1.5 Håndtere problemstillinger løftet gjennom linjen

- Dersom problemstillinger i internkontrollarbeidet ikke kan løses på det organisatoriske nivå de oppstår, skal de løftes gjennom linjen og håndteres på et høyere ledernivå.
- De skal løftes gjennom linjen til man når et ledernivå som har økonomisk handlingsrom eller myndighet til å finne budsjettdekning, akseptere aktuelle risikoer eller ta andre nødvendige beslutninger.
- Årsaken kan bl.a. være manglende finansiering, at akseptkriteriene sier at kun ledere på et visst nivå kan akseptere store restrisikoer, uenighet mellom ulike oppgaveeiere som benytter samme IKT-system, arbeidslokaler e.l., uenighet i virksomheten om hvilke tiltak som skal inngå i virksomhetens fellessikring og gjelde alle, og hvilke som bør være tilleggssikring for de som har ekstra behov.

Anbefalt dokumentasjon:

- Problemstillinger av vesentlig betydning og tilhørende beslutninger journalføres og arkiveres.

1.6 Beredskap og krisehåndtering

- Ledere på ulikt nivå vil være sentrale aktører i det meste av beredskap og krisehåndtering.
- Det er avgjørende at virksomheten har gode prosedyrer med klare ansvarslinjer og nødvendig samordning.
- Virksomheten må også ha systematiske øvelser for å sikre etterlevelse på alle ledernivå.

Anbefalt dokumentasjon:

- Beredskaps- og kriseplaner på virksomhetsledernivå og for ulike virksomhetskritiske arbeidsoppgaver og funksjoner.

2 Risikovurdering

- Alle delaktivitetene under Risikovurdering gjennomføres av eller på oppdrag for risikoeiere og systemeiere fellessystemer.
- Ledere som er ansvarlige for å nå mål og få utført tilhørende arbeidsoppgaver er normalt virksomhetens risikoeiere. Dette er oftest alle lederne på ulike nivå rundt om i virksomheten.
- Risikoene er potensielle avvik fra mål risikoeierne helt eller delvis er ansvarlig for å nå.
- Risikoeierne er normalt systemeiere for egne IKT-system, og disse er en del av deres ansvarsområde.
- Systemeiere fellessystem skal ivareta interessene til alle risikoeierne som benytter fellessystemene til sine oppgaver. IKT-infrastruktur er et fellessystem. Det samme er typisk e-postsystem og arkivsystem.
- Risikoeiere som bruker fellessystem er også risikoeiere for egen informasjonsbehandling i fellessystemene. De skal derfor i tilstrekkelig grad og hensiktsmessig måte involveres i risikovurderingsarbeid mv. som utføres på fellessystemene.
- Ledere på virksomhetsnivå, avdelingsnivå o.l. må passe på å selv gjennomføre disse delaktivitetene rundt egne lederoppgaver. De er normalt selv risikoeiere for disse.

2.1 Få oversikt og prioritere

- Gjennomføres av risikoeiere rundt om i virksomheten og av systemeiere fellessystem. Det er viktig med en prosessleder ved første gangs gjennomføring. Hele eller deler av gjennomføringen kan gjerne gjøres for en ledergruppe i en organisatorisk enhet samlet, og alle oppgavene de har ansvaret for.
- Risikoeiere skal på et overordnet nivå identifisere arbeidsoppgaver de har ansvaret for, sentral informasjon som behandles, regelverk som må følges og hvilke IKT-system som benyttes.
- De skal deretter anslå potensielt konsekvensnivå ved brudd på konfidensialitet, integritet og tilgjengelighet rundt egne arbeidsoppgaver, benyttede IKT-system og spesielle hjelpemidler.
- Systemeiere fellessystem skal som første trinn anslå potensielt konsekvensnivå ved brudd på konfidensialitet, integritet og tilgjengelighet rundt fellessystemene de har ansvar for. De kartlegginger og vurderinger som er gjort av risikoeiere som benytter fellessystemene er viktig bakgrunnsinformasjon.
- Alle skal deretter gjøre en overordnet vurdering av nivået på relevante trusler, farer og sårbarheter rundt eget ansvarsområde og merke seg de som peker seg spesielt ut.
- For å få fokus på det viktigste, behandle like ting sammen og få målrettet tidsbruk på konkrete risikovurderinger, skal alle deretter gruppere det som anses enkelt og oversiktlig og dele opp og skille ut det som anses kritisk eller som det er knyttet spesiell usikkerhet til. Det gjelder både arbeidsoppgaver, IKT-system og deler av disse.
- Alle skal så systematisk vurdere behovet for oppdaterte eller nye risikovurderinger for de ulike delene av eget ansvarsområde. De skal også prioritere mellom nødvendig risikovurderinger. Virksomhetens retningslinje for dette skal gi føringer.
- Risikoeiere og systemeiere fellessystem skal ut fra ovennevnte og de risikovurderinger som faktisk gjennomføres, vedlikeholde en oversikt over planlagte og gjennomførte risikovurderinger innen eget ansvarsområde.

- Resultatet fra det å få oversikt og prioritere skal revurderes og eventuelt oppdateres minst en gang årlig. Relevante deler av aktiviteten skal alltid gjennomføres og oppdateres før nye typer arbeidsoppgaver starter, eller før nye IKT-system anskaffes og tas i bruk.

Anbefalt dokumentasjon:

- Risikoeiernes oversikter over arbeidsoppgaver, informasjon, regelverk og IKT-system.
- Risikoeiere og systemeiere fellessystem sine
  - oversikter over potensielle konsekvensnivå på arbeidsoppgaver, IKT-system m.v.
  - overordnede vurderinger av nivået på relevante trusler, farer og sårbarheter rundt eget ansvarsområde
  - oppdelinger i grupper og delområder og oversikt over hvilket behov det er for oppdaterte risikovurderinger på dem
  - oversikter over planlagte og gjennomførte risikovurderinger

2.2 Analysere eksterne krav

- Gjennomføres ved behov av risikoeiere rundt om i virksomheten og av systemeiere fellessystem.
- Identifisere og tydeliggjøre konkrete krav i regelverk og avtaler som man må ta hensyn til i arbeidet.
- Gjennomføres for de regelverk og avtaler som ikke er tydeliggjort nok på virksomhetsnivå (jf. pkt. 8.4).

Anbefalt dokumentasjon:

- Oversikt over konkrete tiltak eller typer tiltak som kreves i avtaler eller regelverk for aktuelle arbeidsoppgaver eller IKT-system. Detaljeringsnivå er avhengig av behov.

2.3 Planlegge risikovurdering

- Systematisk planlegging av gjennomføringen av hver enkelt risikovurdering.
- Gjennomføres i samarbeid mellom den aktuelle risikoeier/systemeier fellessystem og den som pekes ut som prosessleder for risikovurderingen.

Anbefalt dokumentasjon:

- Tydelige mandat for risikovurderingen.

2.4 Gjennomføre risikovurdering

- Systematisk gjennomføring av risikovurderinger det er identifisert behov for slike.
- Gjennomføres under ledelse av en utpekt prosessleder.
- Følger en systematisk metode, som f.eks. den Difi foreslår i dette veiledningsmateriellet.
- Omfang og innretning på arbeid og metodebruk må tilpasses det som risikovurderes.

Anbefalt dokumentasjon:

- Risikonotat som kort oppsummerer vesentlige deler fra arbeidet.
- En vedlagt risikotabell som minimum viser risikobeskrivelse, konsekvensnivå, tilhørende sannsynlighetsnivå og risikonivå for de identifiserte risikoene.
- Eventuelt andre vedlegg som ved behov utdyper analyser som er gjennomført.

2.5 Risikovurdere i hendelseshåndteringen

- Systematisk behovsvurdering og eventuell gjennomføring av avgrensede risikovurderinger når informasjonssikkerhetshendelser blir rapportert til en oppgaveeier eller systemeier.

Anbefalt dokumentasjon:

- Et kort situasjonstilpasset risikonotat.

2.6 Risikovurdere ved anskaffelser og utvikling

- Systematisk behovsvurdering og ev. gjennomføring av tilpassede risikovurderinger ved anskaffelser og systemutvikling.

Anbefalt dokumentasjon:

- Behovs- og kravlister til anskaffelses- eller utviklingsprosessen. Disse kan utformes i forkant av anskaffelsen eller gradvis i anskaffelses- eller utviklingsprosessen, avhengig av hvilken fremgangsmåte man benytter.

3 Risikohåndtering

3.1 Foreslå håndtering av risikoer

- Systematisk oppfølging av forutgående risikovurdering der det er identifisert risikoer som ikke kan aksepteres uten nærmere tiltaksvurdering.
- Gjennomføres ofte direkte i forlengelsen av en risikovurdering.
- Gjennomføres under ledelse av en prosessleder utpekt av aktuell risikoeier eller systemeier fellessystem. Det vil ofte være den samme som ledet tilhørende risikovurdering.
- Følger en systematisk metode, som f.eks. den Difi foreslår i dette veiledningsmateriellet.

Anbefalt dokumentasjon:

- Et eget risikohåndteringsnotat eller en forlengelse av risikonotatet fra risikovurderingen, som kort oppsummerer vesentlige deler fra arbeidet.
- Et vedlagt risikohåndteringsskjema som viser hvilke tiltak som anbefales for de risikoene som bør håndteres.
- En kopi av den opprinnelige risikotabellen med oppdatering av hvilke tiltak som er foreslått for hver risiko og hva det betyr for konsekvensnivå, tilhørende sannsynlighetsnivå og risikonivå (restrisiko).
- Eventuelt andre vedlegg som ved behov utdyper analyser, nytte-/kostvurderinger e.l. som er gjennomført.

3.2 Godkjenne forslag til risikohåndtering

- Gjennomføres av aktuell risikoeier eller systemeier fellessystem.
- En systematisk vurdering av forslaget til håndtering av risikoer.

Anbefalt dokumentasjon:

- Beslutning med aksept av risikoene og tiltakene, retur til forrige delaktivitet for mer arbeid med tiltaksforslag eller løfting av uavklarte problemstillinger gjennom linjen.

3.3 Iverksette godkjente tiltak

- Gjennomføres av en håndteringsansvarlig utpekt av aktuell risikoeier eller systemeier fellessystem.
- Utformer konkret handlingsplan for gjennomføringen, inngår avtaler med de som skal gjennomføre aktivitetene i handlingsplanen, får planen godkjent av oppdragsgiver og følger opp gjennomføringen.

Anbefalt dokumentasjon:

- Handlingsplan med tilhørende fremdriftsrapportering.

3.4 Utforme og implementere tiltakene

- Konkrete tiltak utformes, settes i verk og vedlikeholdes av tiltaksleverandører.
- Dette kan være felles tiltaksleverandører internt eller eksternt med ansvar som IT-drift, IT-utvikling, eiendom/bygninger, felles personalrutiner o.l.

- Det kan også være personer hos aktuell risikoeier eller systemeier fellessystem som får ansvar for utvikling av prosedyrer, rutiner, opplæring o.l.
- Testing av tiltakene må gjennomføres som avtalt.

Anbefalt dokumentasjon:

- Dokumentasjon av det enkelte tiltaket avhengig av tiltakets egenart.
- Avtalt rapportering til aktuelle håndteringsansvarlige.
- Samlet oversikt over alle tiltak i henhold til overordnede føringer.

3.5 Oppdatere fellessikringen

- Initieres og gjennomføres dersom tiltaksleverandører mener nye tiltak best kan implementeres som del av virksomhetens fellessikring, og dermed skal gjelde alle i virksomheten.
- Vurderingen koordineres systematisk på virksomhetsnivå og gjennomføres som forenklet utgave av pkt. 8.5 *Etablere fellessikring og synliggjøre tilleggssikring*.

Anbefalt dokumentasjon:

- Oppdatering av oversikten over virksomhetens fellessikring (jf. pkt. 8.5).

4 Overvåking og hendelseshåndtering

4.1 Overvåke i henhold til avtale

- Gjennomføres systematisk av tiltaksleverandører for de områder der overvåking er et avtalt sikkerhetstiltak.

Anbefalt dokumentasjon:

- Eventuelt krav om dokumentasjon av at overvåking gjennomføres, skal være en del av kravene til overvåkingen.

4.2 Rapportere hendelser, avvik og informasjonssikkerhetsbrudd

- Gjennomføres systematisk av alle ansatte.
- Systemet etablert for hendelses- og avvikshåndtering (jf. pkt. 8.6) benyttes.

Anbefalt dokumentasjon:

- Nødvendig dokumentasjon skal være integrert i systemet for hendelses- og avvikshåndtering.

4.3 Følge opp hendelser, avvik og informasjonssikkerhetsbrudd

- De som er ansvarlig for oppfølging av hendelser håndterer disse i henhold til gjeldende rutiner i hendelses- og avvikshåndteringen.

Anbefalt dokumentasjon:

- Dokumentasjon av oppfølgingen skal være integrert i systemet for hendelses- og avvikshåndtering.

5 Måling, evaluering og revisjon

5.1 Vurdere status på eget ansvarsområde

- Minst en gang i året skal følgende vurdere status for sine ansvarsområder:
  - Ledere som delegerer og skal følge opp gjennom linjen
  - Risikoeiere
  - Systemeiere fellessystem
  - Tiltaksleverandører
  - Ansvarlige for tjenestenivåavtaler eller andre avtaler

  - Ansvarlige for egne deler av internkontrollaktivitetene, som f.eks. hendelseshåndteringssystemet og internrevisjon
- Statusvurderingen skal omfatte vurderinger av om man selv, egne ansatte og leverandører
  - følger gjeldende lov- og regelverk
  - gjennomfører internkontrollaktivitetene slik man er pålagt
  - etablerer og følger opp vedtatte eller avtalte sikkerhetstiltak
  - etterlever gjeldende sikkerhetstiltak
- I tillegg skal de som har ansvar for tiltak vurdere om tiltakene fungerer som forutsatt.
- Alle skal i første omgang vurdere hvor stor tillit de har til at status er slik den skal være. Dersom tilliten er lav, skal nærmere undersøkelser gjennomføres. Dersom tilliten er moderat, skal behovet for nærmere undersøkelser vurderes ut fra hvor viktig saken anses å være, både for virksomheten og egen enhet. Er tilliten høy, er det normalt ingen grunn til ytterligere undersøkelser. Det betinger at tillitsnivået bygger på kritisk refleksjon om egen kunnskap.
- Den ansvarlige må sørge for at nærmere undersøkelser blir gjort i tilstrekkelig omfang og med tilstrekkelig kvalitet. Dersom undersøkelser avdekker avvik, må disse utbedres slik at ting fungerer og tilliten økes til et tilfredsstillende nivå.

Anbefalt dokumentasjon:

- Resultatet av statusvurderingen sammen med hvilke undersøkelser og oppfølgingstiltak som er gjennomført, bør dokumenteres i et kort notat.

5.2 Måle tilstanden på definerte indikatorer

- Virksomhetsledelsens kan beslutte at de vil følge sikkerhetstilstanden over tid på enkelte områder, jf. pkt. 1.1.
- De skal da peke ut noen ansvarlige som skal utarbeide forslag til systematiske målinger, herunder områder, indikatorer, metoder, frekvens, ansvarlige og rapportering. Beslutning skal tas av virksomhetsledelsen.
- Målingene skal gjennomføres av de som blir pekt ut til det gjennom linjebeslutninger.
- Resultatene skal sammenstilles av fagansvarlig informasjonssikkerhet og presenteres for virksomhetsledelsen, normalt som del av virksomhetsledelsens gjennomgang.

Anbefalt dokumentasjon:

- Sammenstilte resultatet av målingene sammenlignet over tid.

5.3 Gjennomføre evalueringer

- Virksomhetsledelsens kan beslutte at det skal gjennomføres evalueringer, jf. pkt.1.1. Evalueringer kan omfatte hele eller deler av arbeidet med internkontroll og informasjonssikkerhet i virksomheten.
- Ledere på ulikt nivå kan i tillegg beslutte at de skal få gjennomført evalueringer på deler av sine ansvarsområder. Noe av dette kan være lovpålagt, f.eks. krav om «sikkerhetsrevisjoner» e.l.. Slike krav vil normalt dekkes av målrettede evalueringer.
- Oppdragsgiver skal peke ut de som skal være ansvarlig for en evaluering. Det skal alltid gjøres en vurdering av behovet for uavhengighet. Ved særskilt behov for uavhengighet eller kompetanse, kan man hente inn eksterne til å gjennomføre evalueringen.
- Evalueringsoppdrag skal være spesifisert og avgrenset og gjennomføres på en profesjonell måte. Resultatet skal presenteres for oppdragsgiver. Eventuelle avvik skal følges opp.

Anbefalt dokumentasjon:

- Evalueringsrapporter

5.4 Gjennomføre internrevisjon

- Formålet med en internrevisjon er å få en formell vurdering av om virksomheten følger bestemte krav, og om kravene er implementert og vedlikeholdt på en formåls- og kostnadseffektiv måte.
- Virksomhetsledelsens kan beslutte at det skal gjennomføres internrevisjon, jf. pkt. 1.1. En internrevisjon kan omfatte hele eller deler av arbeidet med internkontroll og informasjonssikkerhet i virksomheten.
- Internrevisjonen skal gjennomføres etter anerkjente revisjonsstandarder. Arbeidet kan utføres av interne eller eksterne, men reell uavhengighet skal sikres.
- Resultatet av en internrevisjon skal presenteres for virksomhetsledelsen. Avvik skal følges opp på en systematisk måte.

Anbefalt dokumentasjon:

- Revisjonsrapporter

6 Kompetanse- og kulturutvikling

6.1 Identifisere og følge opp behov for kompetanse- og kulturutvikling

- Identifisering av behov for kompetanse- og kulturutvikling skal gjøres løpende som en del av internkontrollarbeidet i virksomheten. Dette skal gjøres av ledere på alle nivå og for alle ansvarsområder.
- Behovene kan identifiseres gjennom ulike delaktiviteter, for eksempel:
    - Medarbeidersamtaler
    - Risikovurderinger
    - Oppfølging av hendelser, avvik og informasjonssikkerhetsbrudd
    - Vurdering av status på eget ansvarsområde
    - Revisjoner og evalueringer
    - Ledelsens gjennomgang
- Når det er identifisert et behov skal det gjennomføres hensiktsmessige tiltak. Tiltakene skal
    - være tilpasset riktig målgruppe
    - ta i bruk hensiktsmessig(e) virkemidler
    - sees i sammenheng med andre opplæringstiltak i virksomheten
    - være tilrettelagt slik at man kan måle effekten av tiltaket.

Anbefalt dokumentasjon:

- Planer for opplæring- og kulturutvikling.

6.2 Følge opp lokale sikkerhetskoordinatorer

- Fagansvarlig informasjonssikkerhet og virksomhetens lokale sikkerhetskoordinatorer skal møtes jevnlig for å utveksle erfaringer og lære av hverandre.
- Aktuelle temaer for samlingene vil være
    - sikkerhetskoordinatorenes egen kompetanseheving innen informasjonssikkerhet og internkontroll
    - kompetanse- og kulturutfordringer rundt om i virksomheten og innspill og råd til sentralstyrte tiltak på området
    - innspill og råd til virksomhetsledelsens gjennomgang
    - innspill og råd rundt fellessikring i virksomheten

Anbefalt dokumentasjon:

- Oppsummeringsnotat fra møtene med sikkerhetskoordinatorene.

7 Kommunikasjon

7.1 Formidle nye føringer

- Nye eller oppdaterte føringer skal formidles raskt og effektivt til de som har eller kan få bruk for dem. Ansvaret ligger hos de som godkjenner føringene.

Anbefalt dokumentasjon:

- Dokumentasjon og formidlingskanal skal være i samsvar med virksomhetens felles krav til dokumentasjon av internkontroll.

7.2 Dokumentere gjennomførte internkontrollaktiviteter

- Gjennomføring av internkontrollaktiviteter skal som hovedregel dokumenteres skriftlig.

Anbefalt dokumentasjon:

- Et kort notat vil ofte være nok. Arkivering og journalføring bør skje i samsvar med virksomhetens felles krav til dokumentasjon av internkontroll.

7.3 Dokumentere etterlevelse av tiltak

- Dersom sikkerhetstiltak, prosedyrer eller rutiner stiller krav om det, skal etterlevelsen av dem dokumenteres skriftlig. Slike krav skal være basert på risiko og behov.
- Dokumentasjonskrav skal legges opp på en måte som gjør at de ikke oppleves som unødvendige eller vesentlig hemmende for annet viktig arbeid.

Anbefalt dokumentasjon:

- Eventuelle dokumentasjonskrav på etterlevelse skal være en del av beskrivelsen av tiltaket.

7.4 Statusrapporter som grunnlag for risikovurderinger

- Fagansvarlig informasjonssikkerhet skal en gang i året lage en rapport over status og trender på informasjonssikkerhetsområdet både internt i virksomheten og i sammenlignbare virksomheter eksternt.
- Rapporten skal være bakgrunnskunnskap for de som skal gjennomføre risikovurderinger rundt om i virksomheten. Rapporten må være tilpasset det formålet.

Anbefalt dokumentasjon:

- Statusrapport som grunnlag for risikovurderinger.

7.5 Saksnotat til virksomhetsledelsens gjennomgang

- Fagansvarlig informasjonssikkerhet skal i god tid før virksomhetsledelsens gjennomgang produsere et saksnotat til gjennomgangen. Hun skal også utarbeide og legge ved en tilpasset rapport om status på relevante områder innen informasjonssikkerhet. Notatet og rapporten skal være tilpasset de føringer virksomhetsledelsen har gitt fra tidligere gjennomganger.

Anbefalt dokumentasjon:

- Systematiske saksnotat til virksomhetsledelsen (jf.1.1) med tema som f.eks.
  - status på vedtatte tiltak etter tidligere gjennomganger
  - bakgrunnskunnskap om trender og utfordringer lokalt og nasjonalt
  - status på det systematiske internkontrollarbeidet innen informasjonssikkerhet
  - tilbakemeldinger på informasjonssikkerhetsnivået
  - status på risikoer eller risikoområder ledelsen er spesielt opptatt av
  - muligheter for forbedring

7.6 Kommunikasjon mellom delaktiviteter og aktører

- Alle delaktiviteter i internkontrollarbeidet forutsetter en rask og effektiv kommunikasjon med andre delaktiviteter og mellom ulike aktører.
- Det er et ansvar for alle ansatte å bidra til at riktig informasjon kommer frem til riktig person til riktig tid.
- Ivaretagelse av lovpålagt taushetsplikt ligger i begrepet riktig informasjon til riktig person.

Anbefalt dokumentasjon:

- Dokumentasjon skal være i samsvar med krav i de enkelte delaktivitetene.

7.7 Ekstern kommunikasjon

- Eventuell kommunikasjon med personer utenfor virksomheten om risikoer, tiltak, internkontroll, informasjonssikkerhet, mv., skal skje i samsvar med virksomhetens policy og retningslinjer for ekstern kommunikasjon. Det gjelder både innhold og hvem som uttaler seg om hva.

8 Etableringsaktiviteter

Etableringsaktiviteter er et sett av spesielle aktiviteter. De gjennomføres ut fra behov ved første gangs etablering av internkontroll på informasjonssikkerhetsområdet, eller ved behov for oppdatering eller vesentlig forbedring av grunnleggende deler man allerede har.

I Difis veiledningsmateriell er de to første etableringsaktivitetene *Analysere status* og *Planlegge etablering/forbedring*. De er ikke tatt med i oversikten her på grunn av deres egenart og fokus.

Analysere status er det som gjøres ved hjelp av dette støttedokumentet og tilhørende analyseskjema. *Planlegge etablering/forbedring* er det som skal gjøres dersom analysen viser vesentlige avvik fra Difis anbefalinger, og virksomhetsledelsen beslutter at virksomheten skal gjennomføre et systematisk arbeid for å rette på forholdene.

Under følger øvrige anbefalte etableringsaktiviteter man bør ta stilling til status på og behovet for.

8.1 Utforme overordnede styrende dokumenter

- Er en forutsetning for og den viktigste delen i et systematisk internkontrollarbeid på informasjonssikkerhetsområdet.
- Etablering/forbedring skal ideelt sett initieres av virksomhetsledelsen, jf. pkt. 1.1, som må eie dokumentene.
- Må utformes med god involvering og forankring både hos virksomhetsledelsen og ut i organisasjonen for øvrig.
- Deler av arbeidet og dokumentene kan med fordel integreres som fellesarbeid for flere internkontrollområder og utformes i et samarbeid med fagansvarlige på disse områdene.
- I en analyse av egen status er det svært viktig med kvalitative vurderinger av innholdet i det man har, opp mot Difis eksempler og anbefalinger på overordnede styrende dokumenter.

Anbefalt dokumentasjon:

- Gode overordnede styrende dokumenter (jf. pkt. 1.1) som tilsvarer Difis anbefalinger og eksempler for:
    - Policy for informasjonssikkerhet
    - Retningslinjene
        - Roller og ansvar i internkontroll- og sikkerhetsarbeidet
        - Forstå, vurdere og håndtere operativ risiko
        - Vurdere behov for risikovurderinger

- En retningslinje eller overordnet veiledning om aktiviteter og ansvar innen internkontroll informasjonssikkerhet, som utdyper retningslinjen om roller og ansvar

8.2 Få på plass nøkkelpersoner og aktivere sikkerhetsorganisasjonen

- Ut fra av virksomhetens status, utfordringer og egenart, samt dens egne føringene i Retningslinje: Roller i sikkerhetsorganisasjonen (jf. pkt. 8.1), må man
  - avsette ressurser til å dekke rollene når det er behov for at de blir aktivert
  - peke ut eller tilsette fagansvarlig informasjonssikkerhet eller tilsvarende – dersom man ikke har dekket rollen allerede eller ikke har nok kompetanse/ressurser p.t.
  - peke ut øvrige sentrale roller som felles tiltaksleverandører for ulike områder, prosessledere for risikovurderinger o.l., lokale sikkerhetskoordinatorer mv.
  - peke ut klare systemeiere for IKT-system – dersom det ikke er gjort tidligere (både fellessystem og system for den enkelte risikoeier)
  - etablere eventuelle nye forum
  - etablere de arbeidsgrupper man har behov for i etableringsfasen av internkontrollarbeidet
- Det meste av ovennevnte bør komme på plass gradvis og bør legges inn i planen for å etablere/forbedre internkontroll.
- Fagansvarlig informasjonssikkerhet er den viktigste rollen å få på plass tidlig. Han har en sentral rolle som lederstøtte og pådriver for det samlede internkontrollarbeidet innen informasjonssikkerhet, og vil normalt være ansvarlig for nevnte plan.

8.3 Identifisere typiske oppgave- og informasjonstyper

- Gjennomføres dersom en oversikt over typiske oppgave- og informasjonstyper mangler i virksomheten eller er svært mangelfull.
- Oversikten formål er å støtte arbeidet i delaktiviteten *Få oversikt og prioritere* (jf. pkt. 2.1) under hovedaktiviteten *Risikovurdering*.
- Difis eksempeloversikt vil kunne danne et første grunnlag for de fleste. Denne kan da bygges ut og tilpasses virksomhetens egenart.

Anbefalt dokumentasjon:

- Felles oversikt over typiske arbeidsoppgaver som utføres i virksomheten og hvilken informasjon som normalt behandles i disse
  - Både arbeidsoppgaver og informasjonstyper må være på et overordnet abstraksjonsnivå

8.4 Felles analyse av eksterne krav

- Gjennomføres på fellesnivå i virksomheten dersom viktig regelverk og avtaler gjelder for flere områder i virksomheten og flere har behov for en konkretisering av kravene.
- Identifisere og tydeliggjøre konkrete krav i regelverk og avtaler man må hensynta i arbeidet.
- Fellesarbeidet skal redusere behovet for tilsvarende arbeid rundt om i virksomheten i delaktiviteten *Analysere eksterne krav* (jf. pkt. 2.2) under hovedaktiviteten *Risikovurdering*.

Anbefalt dokumentasjon:

- Felles oversikt over konkrete tiltak eller typer tiltak som kreves i avtaler eller regelverk som gjelder for arbeidsoppgaver som utføres av flere i virksomheten. Detaljeringsnivå er avhengig av behov.

8.5 Etablere fellessikring og synliggjøre tilleggssikring

- Fellessikring er et sett av sikkerhetstiltak som etableres for å gi et felles grunnleggende sikkerhetsnivå for sentrale områder av virksomheten. De gjelder alle i virksomheten.
- Tilleggssikring er sikkerhetstiltak som kan etableres for bestemte oppgaver eller systemer som har spesielle behov.
- Formålet med denne aktiviteten er kombinasjonen av å etablere en fellessikring som er behovsorientert, forenkle risikovurderinger og risikohåndtering rundt om i virksomheten, og ta hensyn til effektiviseringsbehovet for tiltaksleverandørene.
- Aktiviteten gjennomføres dersom virksomheten mangler en systematisk etablering og synliggjøring av fellessikring og tilleggssikring.
- Aktiviteten bør gjennomføres i et fellesprosjekt med fagansvarlig informasjonssikkerhet som koordinator, virksomhetens interne tiltaksleverandører som nøkkelpersoner og noen utvalgte fagområder og risikoeiere som piloter.
- **Fase 1** handler om å få på plass et utkast til minimumsnivå på fellessikringen
- Tiltaksleverandørene bør gjennomgå egen praksis og utvalgte tiltaksbanker for å identifisere aktuelle tiltak for virksomheten.
- Tiltak som klart har vesentlig betydning for de fleste i virksomheten bør legges inn som forslag til fellessikring. Tiltak som trolig er nyttige for noen, men som kan ha vesentlige negative sideeffekter for andre, legges inn som mulig tilleggssikring. Dette gjøres uavhengig av om tiltakene i dag gjelder for store deler av virksomheten eller bare for noen få.
- **Fase 2** handler om å gjennomføre risikovurderinger og utarbeide tilhørende forslag til risikohåndtering for 2-4 pilotområder i virksomheten.
- Valgte pilotområder bør være representative for bredden i virksomhetens informasjonsbehandling, både med hensyn til kritikalitet og ressursbruk. I tillegg bør man vurdere å ta med fellessystemer som er mye brukt.
- Relevante risikoeiere, systemeiere fellessystem og sentrale tiltaksleverandører må være representert i arbeidet.
- Risikovurderingene gjennomføres med kun førsteutkast til fellessikring i bunn (jf. fase 1). Listen med potensiell tilleggssikring benyttes som hovedkilde til forslag til sikkerhetstiltak i håndteringen. Andre tiltak tas med ved behov.
- **Fase 3** handler om å utarbeide et forslag til fellessikring. Deltakere er tiltaksleverandørene og representanter for risikoeiere og systemeiere fellessystem på pilotområdene. Man bør også vurdere å inkludere en bredere referansegruppe.
- I vurderingen av hvilke av tiltakene fra fase 2 som skal være virksomhetens fellessikring og hva som skal være tilleggssikring må man balansere flere forhold. Dette gjelder kostnadseffektiv drift for tiltaksleverandørene opp mot behov, ulemper og kostnader for de ulike risikoeierne.
- **Fase 4** er en intern høring i virksomheten over forslaget til fellessikring, spesielt med tanke på å identifisere vesentlige ulemper for fagområder som ikke har vært involvert som piloter.
- **Fase 5** er en beslutning fra virksomhetsledelsen eller den hun utpeker basert på høringen.
- **Fase 6** er iverksettelse av beslutningen**.**

Anbefalt dokumentasjon:

- Oversikt over hvilke tiltaksområder og tilhørende sikkerhetstiltak som inngår i virksomhetens fellessikring.
- Oversikt over standardisert tilleggssikring på ulike områder som risikoeiere og systemeiere fellessystem kan velge ut fra behov.

8.6 Etablere system for hendelses- og avvikshåndtering

- Gjennomføres dersom virksomheten mangler et godt og velfungerende system for hendelses- og avvikshåndtering som også dekker informasjonssikkerhet.
- Et slikt system kan med fordel integreres og benyttes som fellessystem på tvers av flere internkontrollområder
- Systemet er ikke bare et IT-system, men like mye klargjøring av ansvar, prosedyrer og rutiner.
- Systemet bør omfatte krav om hva som skal rapporteres, hvem som skal rapportere, hvordan rapporteringen skal skje og hvem som skal håndtere hva.
- Informasjonsflyt for ulike typer hendelser bør være klart definert.
- Det må sikres at innrapporterte hendelser av ulik typer håndteres av rette vedkommende innen gitte frister.
- Ved behov må beredskapsplaner eller andre konsekvensreduserende tiltak iverksettes uten ugrunnet opphold.
- Det bør alltid vurderes om man kan lære av erfaringene fra en hendelse. Særlig bør det vurderes om hendelsene og avvikene tilsier justering av risikovurderinger og tilhørende tiltak. Kunnskapen må brukes i det videre risikovurderingsarbeidet.

Anbefalt dokumentasjon:

- Systemet bør inneholde den dokumentasjon som er nødvendig iht. ovennevnte.

8.7 Utforme og gjennomføre grunnopplæring

- Gjennomføres dersom virksomheten mangler viktig kompetanse i etableringsfasen av internkontroll på informasjonssikkerhetsområdet
- Ut fra behov bør man anskaffe eller utvikle
    - grunnleggende informasjonsmateriell eller kurs for ledere om informasjonssikkerhet
    - grunnopplæring for ledere i sentrale internkontrollaktiviteter informasjonssikkerhet
    - grunnopplæring prosessledere i *Få oversikt og prioritere* (jf. pkt. 2.1), *Gjennomføre risikovurdering* (jf. pkt. 2.4) og *Foreslå håndtering av risikoer* (jf. pkt. 3.1).
    - grunnopplæring for håndteringsansvarlige som har en sentral rolle i aktiviteten *Iverksette godkjente tiltak* (jf. 3.3)
    - grunnleggende kurs/opplæring i informasjonssikkerhet for ansatte
- Alle kursene bør være tilpasset virksomhetens internkontrollaktiviteter og sikkerhetskrav
- Opplæringen bør legges inn i planen for etablering/forbedring slik at tidspunkt for gjennomføring blir tilpasset aktivitetene der

Anbefalt dokumentasjon:

- Informasjons- og opplæringsaktiviteter integrert i planen for å etablere/forbedre internkontrollen.

8.8 Etablere rammeverk for dokumentasjon

- Gjennomføres dersom virksomheten mangler en tydelig definert struktur og føringer på dokumentasjon og gjenfinning av dokumenter, maler mv.
- Bør i størst mulig grad etableres som felles på tvers av alle internkontrollområder i virksomheten.
- Bør ta utgangspunkt i det rammeverk eller føringer virksomheten allerede har.
- Arbeidet bør inkludere fagansvarlige på alle internkontrollområder i virksomheten, samt arkivpersonell og virksomhetens kommunikasjonsenhet.

Anbefalt dokumentasjon:

- Et dokument som klargjør dokumenthierarki, maler, lagrings- og publiseringssted mv.