Støttespørsmål til verksemdsleiinga sin gjennomgang

**Dette er ei liste med støttespørsmål som kan brukast i samband med førebuing og gjennomføring av Verksemdsleiinga sin gjennomgang, inkludert utarbeiding av saksnotat til ein slik gjennomgang.**

# Om lista

Punkta i lista er formulerte som spørsmål som verksemda (leiing og fagpersonar) kan spørje seg, ønske å ha svar på til gjennomgangen, eller ønske å vurdere som ein del av gjennomgangen. Meininga er å gje detaljerte tips til kva som **kan** inngå i gjennomgangen. Alt som er lista opp her vil ikkje vere aktuelt for alle verksemder, og i alle fall ikkje i kvar einaste gjennomgang.

Nokre av punkta er ganske like, men skil seg i ordbruk eller detaljeringsgrad. Det er medvite. Og understrekar berre at det ikkje er ei autorativ sjekkliste over innhaldet i gjennomgangen, men kan nyttast til å få i gang refleksjon og tankeverksemd om desse emna.

Rekkjefølgja på punkta i lista indikerer inga prioritering, og er ikkje meint å gje føringar for kor viktige dei ulike emna er.

Denne lista er ikkje meint å skulle brukast til ein grundig og heilskapleg gjennomgang av omfang og kvalitet på internkontrollarbeidet. Om det er behov for det bør de bruke etableringsaktiviteten Analysere status.

# Rammevilkår

* Har det vore endringar i interne eller eksterne tilhøve som har noko å seie for informasjonssikkerheitsarbeidet?
* Gjennomførte eller planlagde endringar i kva vi driv med?
* Endringar i kven vi yter tenester til?
* Trugsmålsutvikling nasjonalt og internasjonalt, eller i verksemda vår?
* Gjennomførte eller føreståande endringar i regelverk?
* Utvikling elles, t.d. teknologi?

# Generelt om styringsaktivitetane

* Har vi tilstrekkeleg oversikt over status, mogenheit og effektivitet i aktivitetane for styring og kontroll?
* Blir styringsaktivitetane gjennomførte?
* Er vi i stand til å gjennomføre dei effektivt, med fornuftig ressursbruk?
* Fungerer dei bra? Får vi det til? Kva fungerer ikkje bra nok?
* Blir det arbeidd målretta med kontinuerleg forbetring av aktivitetane og informasjonssikkerheitsarbeidet elles?
* Fungerer styring av informasjonssikkerheit godt i samanheng med den andre risikostyringa i verksemda?
* Er styring og kontroll føremålstenleg lagt opp med tanke på krav og tilrådingar som t.d. eForvaltningsforskrifta § 15 og rettleiinga til Digitaliseringsdirektoratet?

# Leiinga si styring og oppfølging

* Har vi tydelege og gode føringar for aktivitetane (kven, kva, korleis)?
* Har vi gode og tydelege føringar for roller og ansvar?
* Har vi tydelege føringar for innhaldet i styringsaktivitetane?
* Har leiarane våre tilstrekkeleg støtte og rettleiing? T.d. frå «fagansvarleg informasjonssikkerheit» og «sikkerheitskoordinatorar» som stør leiinga i arbeidet. Tykkjer leiarane at det fungerer bra?
* Er leiarane i linja i stand til å ta hand om ansvaret for å vurdere og handtere risiko innan informasjonssikkerheit på ein god måte?
* Er det tilstrekkeleg med ressursar til arbeid med informasjonssikkerheit?
* Er arbeidet med styring og kontroll og tryggingstiltak synleg i verksemdsplanane?

# Vurdering av risiko

* Har alle einingar tilstrekkeleg oversikt over informasjonsbehandlinga, og kva denne har å seie for måloppnåinga?
* Har vi tilstrekkeleg oversikt over arbeidsoppgåver (-prosessar), kva informasjonstypar vi behandlar og kva informasjonssystem, IKT-system og IKT-tenester vi nyttar til behandlinga?
* Er vi i stand til å prioritere arbeidet med risiko til dei områda der dei potensielle konsekvensane ved informasjonssikkerheitshendingar er høgast?
* Dekkjer vi alle typar informasjon, IKT-system og uønskte hendingar? (T.d. ikkje berre personopplysningar; ikkje berre tilsikta hendingar, men også uhell, aktløyse, tilfeldig svikt i utstyr og naturhendingar.)
* Har vi oversikt over kor avhengige vi er av eksterne løysingar og tenester? Kor avhengige er vi av nasjonale felleskomponentar? Har vi tilstrekkeleg oversikt over verdikjeder?
* Vurderer vi regelbunde behov for risikovurdering?
* Gjennomfører vi vurdering av risiko der det er behov for det?
* Vurderer vi informasjonssikkerheitsrisiko ved oppstart og gjennomføring av utviklings- og anskaffingsprosjekt?
* Fungerer kriterium for å akseptere risiko godt?
  + Blir dei brukte i risikovurderingsaktivitetane?

# Handtering av risiko

* Vurderer vi ulike handteringsalternativ når vi skal handtere risiko?
* Gjennomfører vi systematisk godkjenning og etablering av sikkerheitsrisiko?
* Er det dei riktige rollene som tar avgjerder om handtering av risiko?
* Vurderer vi alle relevante faktorar ved avgjerder om etablering av tryggingstiltak (kostnader, estimert effekt, negative sideeffektar)?
* Har vi tilstrekkeleg oversikt over etablerte tryggingstiltak?
* Er dei som vurderer risiko fornøgde med oversikta dei får over eksisterande tryggingstiltak?
* Er det tydeleg kven som har ansvar for forvaltning og oppfølging av alle tryggingstiltak?
* Har vi føremålstenleg organisering av drift og forvaltning av tryggingstiltak?
* Er vi i stand til å etablere dei tryggingstiltaka vi har vurdert at det er behov for?
* Kva er årsakene til at vi ikkje er i stand til å etablere alle tryggingstiltak vi har behov for? (manglande kompetanse, økonomiske prioriteringar, uklare ansvarstilhøve mv.)
* Er omfang og innhald i fellessikringa passeleg?
* Er dei som handterer risiko fornøgde med oversikt over fellessikring og tilgjengeleg tilleggssikring?
* Har vi god oversikt over anerkjende tiltaksbankar og tilrådingar om tryggingstiltak frå relevante styresmakter, og er grunnleggjande tryggingstiltak innarbeidde i fellessikringa på ein føremålstenleg måte?
* Er tryggingstiltaka våre primært etablerte for å førebyggje hendingar, eller har vi også etablert tilstrekkeleg med tiltak for å vere i stand til å oppdage og handtere hendingar?

# Overvaking og hendingshandtering

* Har vi tydeleg definerte roller, ansvar og prosedyrar for korleis vi handterer hendingar?
* Greier vi å bruke erfaringane frå hendingshandtering og øvingar til forbetring av informasjonssikkerheitsarbeidet vårt?
* Lykkast vi med å forbetre ting etter hendingar og avvik?
* Har vi god oversikt over hendingar og avvik? Er det trendar i hendingane?
* Har vi mykje/lite hendingar? Trur vi at vi oppdagar alle hendingar?
* Overvakar vi dei riktige tinga, i tilstrekkeleg omfang, for å vere i stand til å oppdage unormal aktivitet og hendingar?
* Kor stor del av hendingane i siste periode oppdaga vi sjølv, og kor mange vart oppdaga av partnarar/leverandørar, eller kanskje av andre eksterne partar?
* Har vi oversikt over kostnadene som følgje av informasjonssikkerheitshendingar?
* Vurderer vi om informasjonssikkerheitshendingar vil kunne føre til utfordringar med tanke på verksemdskontinuitet? Heng arbeidet med informasjonssikkerheit godt saman med arbeidet med verksemdskontinuitet?
* Øver vi? Arbeider vi systematisk og målretta med øvingar på informasjonssikkerheitsområdet?
* Har vi IKT-beredskapsplanar e.l. som er godkjende verksemdsleiar?

# Måling, evaluering og revisjon

* Vurderer risikoeigarar systematisk status på ansvarsområda sine minst ein gong i året?
* Vurderer dei som er ansvarlege for tryggingstiltak (tiltaksleverandørar) systematisk status på ansvarsområda sine minst ein gong i året?
* Gjennomfører vi regelmessig evaluering av etablerte tryggingstiltak for å finne ut om dei verkar etter føremålet og ikkje har utilsikta negative sideeffektar?
* Har vi vurdert nytta av å måle tilstanden på definerte indikatorar for å følgje utviklinga over tid?
* Kva er status på indikatorar vi følgjer utviklinga på?
* Har vi vurdert behovet for evaluering av delar av arbeidet med informasjonssikkerheit? Har vi vurdert behovet for internrevisjon?

# Kompetanse- og kulturutvikling

* Har leiarar mottatt naudsynt grunnopplæring for å kunne utføre oppgåvene sine på ein god måte? Dekkjer grunnopplæringa alle vesentlege roller i dei systematiske aktivitetane? Er dei som har rollene fornøgde med opplæring, rettleiing og støtte?
* Har vi kartlagt andre behov for kompetanseheving på informasjonssikkerheitsområdet?
* Er kompetansetiltak elles tilpassa ulike målgrupper og behov?
* Greier vi å dekkje behovet for fagkompetanse på informasjonssikkerheitsområdet?
* I kor stor grad er vi avhengige av eksterne tenesteleverandørar eller konsulentar for å dekkje behovet for fagkompetanse?
* Er vi fornøgde med balansen mellom intern og ekstern kompetanse?
* Har vi kartlagt eller målt sikkerheitskulturen vår?
* Er det behov for å styrke sikkerheitskulturen vår?

# Kommunikasjon

* Er gjennomgangen vår av eige arbeid god nok til å gje grunnlag for å utarbeide naudsynt styringsinformasjon til overordna, styrande organ?
* Statleg verksemd:
  + Har behandlinga av informasjonssikkerheit i styringsdialogen med departementet fungert godt i siste periode?
  + Er informasjonssikkerheit tilstrekkeleg omtalt i kapittel om styring og kontroll i årsrapporten?
* Har vi behov for å gjere endringar i kommunikasjon til interessentar utanfor verksemda?