Støttespørsmål til virksomhetsledelsens gjennomgang

**Dette er en liste med støttespørsmål som kan benyttes i forbindelse med forberedelse og gjennomføring av Virksomhetsledelsens gjennomgang, inkludert utarbeidelse av saksnotat til en slik gjennomgang.**

# Om listen

Punktene i listen er formulert som spørsmål som virksomheten (ledelse og fagpersoner) kan spørre seg, ønske å ha svar på til gjennomgangen, eller ønske å vurdere som en del av gjennomgangen. Hensikten er å gi detaljerte tips til hva som **kan** inngå i gjennomgangen. Alt som er listet opp her vil ikke være aktuelt for alle virksomheter, og i hvert fall ikke i hver eneste gjennomgang.

Noen av punktene er ganske like, men skiller seg i ordbruk eller detaljeringsgrad. Det er bevisst. Og understreker bare at det ikke er en autorativ sjekkliste over innholdet i gjennomgangen, men kan benyttes til å få i gang refleksjon og tankevirksomhet om disse emnene.

Rekkefølgen på punktene i listen indikerer ingen prioritering, og er ikke ment å gi føringer for hvor viktig de forskjellige emnene er.

Denne listen er ikke ment å skulle benyttes til en grundig og helhetlig gjennomgang av omfang og kvalitet på internkontrollarbeidet. Dersom det er behov for det bør dere benytte etableringsaktiviteten Analysere status.

# Rammebetingelser

* Har det vært endringer i interne eller eksterne forhold som har betydning for informasjonssikkerhetsarbeidet?
* Gjennomførte eller planlagte endringer i hva vi driver med?
* Endringer i hvem vi yter tjenester til?
* Trusselutvikling nasjonalt og internasjonalt, eller vår virksomhet?
* Gjennomførte eller forestående endringer i regelverk?
* Utvikling for øvrig, f.eks. teknologi?

# Generelt om styringsaktivitetene

* Har vi tilstrekkelig oversikt over status, modenhet og effektivitet i aktivitetene for styring og kontroll?
* Gjennomføres styringsaktivitetene?
* Er vi i stand til å gjennomføre dem effektivt, med fornuftig ressursbruk?
* Fungerer de bra? Får vi det til? Hva fungerer ikke bra nok?
* Arbeides det målrettet med kontinuerlig forbedring av aktivitetene og informasjonssikkerhetsarbeidet for øvrig?
* Fungerer styring av informasjonssikkerhet godt i sammenheng med den øvrige risikostyringen i virksomheten?
* Er styring og kontroll hensiktsmessig lagt opp iht. krav og anbefalinger som f.eks. eForvaltningsforskriften § 15 og Digitaliseringsdirektoratets veiledning?

# Ledelsens styring og oppfølging

* Har vi tydelige og gode føringer for aktivitetene (hvem, hva, hvordan)?
* Har vi gode og tydelige føringer for roller og ansvar?
* Har vi tydelige føringer for innholdet i styringsaktivitetene?
* Har våre ledere tilstrekkelig støtte og veiledning? F.eks. fra «fagansvarlig informasjonssikkerhet» og «sikkerhetskoordinatorer» som støtter ledelsen i arbeidet. Synes lederne at det fungerer bra?
* Er ledere i linjen i stand til å ivareta ansvaret for å vurdere og håndtere risiko innen informasjonssikkerhet på en god måte?
* Er det tilstrekkelig med ressurser til arbeid med informasjonssikkerhet?
* Er arbeidet med styring og kontroll og sikkerhetstiltak synlig i virksomhetsplanene?

# Vurdering av risiko

* Har alle enheter tilstrekkelig oversikt over informasjonsbehandlingen, og hvilken betydning den har for måloppnåelsen?
* Har vi tilstrekkelig oversikt over arbeidsoppgaver(-prosesser), hvilke informasjonstyper vi behandler og hvilke informasjonssystemer, IKT-systemer og IKT-tjenester vi benytter til behandlingen?
* Er vi i stand til å prioritere arbeidet med risiko til de områdene hvor de potensielle konsekvensene ved informasjonssikkerhetshendelser er høyest?
* Dekker vi alle typer informasjon, IKT-systemer og uønskede hendelser? (F.eks. ikke bare personopplysninger; ikke bare tilsiktede hendelser, men også uhell, uaktsomhet, tilfeldig svikt i utstyr og naturhendelser.)
* Har vi oversikt over hvor avhengig vi er av eksterne løsninger og tjenester? Hvor avhengig er vi av nasjonale felleskomponenter? Har vi tilstrekkelig oversikt over verdikjeder?
* Vurderer vi regelmessig behov for risikovurdering?
* Gjennomfører vi vurdering av risiko der det er behov for det?
* Vurderer vi informasjonssikkerhetsrisiko ved oppstart og gjennomføring av utviklings- og anskaffelsesprosjekter?
* Fungerer kriterier for å akseptere risiko godt?
  + Blir de brukt i risikovurderingsaktivitetene?

# Håndtering av risiko

* Vurderer vi forskjellige håndteringsalternativer når vi skal håndtere risiko?
* Gjennomfører vi systematisk godkjenning og etablering av sikkerhetstiltak?
* Er det de riktige rollene som tar beslutninger om håndtering av risiko?
* Vurderer vi alle relevante faktorer ved beslutninger om etablering av sikkerhetstiltak (kostnader, estimert effekt, negative sideeffekter)?
* Har vi tilstrekkelig oversikt over etablerte sikkerhetstiltak?
* Er de som vurderer risiko fornøyd med oversikten de får over eksisterende sikkerhetstiltak?
* Er det tydelig hvem som har ansvar for forvaltning og oppfølging av alle sikkerhetstiltak?
* Har vi hensiktsmessig organisering av drift og forvaltning av sikkerhetstiltak?
* Er vi i stand til å etablere de sikkerhetstiltak vi har vurdert at det er behov for?
* Hva er årsakene til at vi ikke er i stand til å etablere alle sikkerhetstiltak vi har behov for? (manglende kompetanse, økonomiske prioriteringer, uklare ansvarsforhold mv.)
* Er omfang og innhold i fellessikringen passelig?
* Er de som håndterer risiko fornøyd med oversikt over fellessikring og tilgjengelig tilleggssikring?
* Har vi god oversikt over anerkjente tiltaksbanker og anbefalinger om sikkerhetstiltak fra relevante myndigheter, og er grunnleggende sikkerhetstiltak innarbeidet i fellessikringen på en hensiktsmessig måte?
* Er våre sikkerhetstiltak primært etablert for å forebygge hendelser, eller har vi også etablert tilstrekkelig med tiltak for å være i stand til å oppdage og håndtere hendelser?

# Overvåking og hendelseshåndtering

* Har vi tydelig definerte roller, ansvar og prosedyrer for hvordan vi håndterer hendelser?
* Klarer vi å bruke erfaringene fra hendelseshåndtering og øvelser til forbedring av informasjonssikkerhetsarbeidet vårt?
* Lykkes vi med å forbedre ting etter hendelser og avvik?
* Har vi god oversikt over hendelser og avvik? Er det trender i hendelsene?
* Har vi mye/lite hendelser? Tror vi at vi oppdager alle hendelser?
* Overvåker vi de riktige tingene, i tilstrekkelig omfang, for å være i stand til å oppdage unormal aktivitet og hendelser?
* Hvor stor andel av hendelsene i siste periode oppdaget vi selv, og hvor mange ble oppdaget av partnere/leverandører, eller kanskje av andre eksterne parter?
* Har vi oversikt over kostnadene som følge av informasjonssikkerhetshendelser?
* Vurderer vi om informasjonssikkerhetshendelser vil kunne føre til utfordringer med tanke på virksomhetskontinuitet? Henger arbeidet med informasjonssikkerhet godt sammen med arbeidet med virksomhetskontinuitet?
* Øver vi? Arbeider vi systematisk og målrettet med øvelser på informasjonssikkerhetsområdet?
* Har vi IKT-beredskapsplaner e.l. som er godkjent av virksomhetsleder?

# Måling, evaluering og revisjon

* Vurderer risikoeiere systematisk status på sine ansvarsområder minst en gang i året?
* Vurderer de som er ansvarlige for sikkerhetstiltak (tiltaksleverandører) systematisk status på sine ansvarsområder minst en gang i året?
* Gjennomfører vi regelmessig evaluering av etablerte sikkerhetstiltak for å finne ut om de virker etter hensikten og ikke har utilsiktede negative sideeffekter?
* Har vi vurdert nytten av å måle tilstanden på definerte indikatorer for å følge utviklingen over tid?
* Hva er status på indikatorer vi følger utviklingen på?
* Har vi vurdert behovet for evaluering av deler av arbeidet med informasjonssikkerhet? Har vi vurdert behovet for internrevisjon?

# Kompetanse- og kulturutvikling

* Har ledere mottatt nødvendig grunnopplæring for å kunne utføre sine oppgaver på en god måte? Dekker grunnopplæringen alle vesentlige roller i de systematiske aktivitetene? Er de som har rollene fornøyd med opplæring, veiledning og støtte?
* Har vi kartlagt øvrige behov for kompetanseheving på informasjonssikkerhetsområdet?
* Er kompetansetiltak for øvrig tilpasset ulike målgrupper og behov?
* Klarer vi å dekke behovet for fagkompetanse på informasjonssikkerhetsområdet?
* I hvor stor grad er vi avhengige av eksterne tjenesteleverandører eller konsulenter for å dekke behovet for fagkompetanse?
* Er vi fornøyd med balansen mellom intern og ekstern kompetanse?
* Har vi kartlagt eller målt sikkerhetskulturen vår?
* Er det behov for å styrke sikkerhetskulturen vår?

# Kommunikasjon

* Er vår gjennomgang av eget arbeid god nok til å gi grunnlag for å utarbeide nødvendig styringsinformasjon til overordnet, styrende organ?
* Statlig virksomhet:
  + Har behandlingen av informasjonssikkerhet i styringsdialogen med departementet fungert godt i siste periode?
  + Er informasjonssikkerhet tilstrekkelig omtalt i kapittel om styring og kontroll i årsrapporten?
* Har vi behov for å gjøre endringer i kommunikasjon til interessenter utenfor virksomheten?