Dette er en liste med punkter som kan være aktuelle å ha med i et saksnotat som grunnlag for toppledelsens beslutning om etablering/forbedring av internkontroll på informasjonssikkerhetsområdet, etter at en analyse av status har vært gjennomført. Listen kan brukes som støtte til arbeidet med å lage et slikt saksnotat for din virksomhet.

Sentrale punkter i beslutningsgrunnlag

# Bakgrunn

* Hvordan informasjonssikkerhet påvirker måloppnåelse
* Behovet for god informasjonssikkerhet
* Et system av aktiviteter for styring og kontroll er ledelsens redskap i arbeidet med informasjonssikkerhet
* Det er snakk om systematikk og formalisering som gir virksomhetsledelsen og linjen for øvrig **tillit** til at virksomheten på en akseptabel måte identifiserer og håndterer risiko
* Regelverk
  + eForvaltningsforskriften § 15 og generelt i økonomiregelverket i staten/kommuneloven
  + Sikkerhetsloven stiller krav til styring og kontroll (sikkerhetsstyring) ifbm. arbeidet med å sikre skjermingsverdig informasjon og skjermingsverdige informasjonssystemer (og objekter og infrastruktur) mot sikkerhetstruende virksomhet
  + Personopplysningsloven/personvernforordningen stiller krav til informasjonssikkerhet ved behandling av personopplysninger, og internkontroll på personvernområdet
  + Sektorregelverk
* Forståelse for at internkontroll langt i fra kun handler om å etterleve regelverk, men å
  + Nå virksomhetens mål
  + Arbeide effektivt
  + Etterleve lover og regler
  + Ha pålitelig rapportering
* Kort beskrivelse av Digitaliseringsdirektoratets veiledningsmateriell, og sentrale anbefalinger om
  + Analyse av status med Digitaliseringsdirektoratets veiledningsmateriell som referanse
  + Planlegge etablering/forbedring av internkontroll på informasjonssikkerhetsområdet

# Oppsummering av analysen

* Hovedinntrykk
  + Er man f.eks. gjennomgående på 0-1 eller 2-3 i analyseskjemaet?
  + Hvor er vi evt. gode eller rimelig bra?
  + Hvor ser det ut til å være størst utfordringer?
  + Er det sentrale områder som må forbedres?
* Hvilke endringer bør vi gjøre?
  + Fordeling mellom nye aktiviteter som må på plass og formalisering og justering av eksisterende
  + Behov for grunnopplæring av ledere og annen kompetanseutvikling
* Oppsummeringen bør inkludere omtale av sammenheng med andre internkontrollområder
  + Virksomhetsstyring, risikostyring og internkontroll generelt, f.eks. iht. DFØs veiledning
  + Risikostyring generelt iht. til ISO 31000
  + Personvern
  + HMS
  + Nasjonal sikkerhet (sikkerhetslovens område)
  + Styring av virksomhetskontinuitet
* Dersom det er relevant bør oppsummeringen spesielt omtale utfordringer ved organisering og rolleforståelse, f.eks. at
  + ledere i linjen ikke skjønner behovet for informasjonssikkerhet for å understøtte arbeidsprosessene/-oppgavene
  + man ikke har gode støttefunksjoner og fagkompetanse som kan støtte linjeledere på en god måte (merk: det er forskjell på å være støtte, og å ta over ansvaret)
  + det mangler forståelse for ansvarsdelingen mellom «risikoeiere» og «tiltaksleverandører»
  + plassering av systemeierskap til fagsystem ikke er forankret i fagavdelingene

# Anbefalinger

* Grov plan for hele planperioden
  + Varighet over flere år
  + Etableringsaktiviteter, informasjon, opplæring og første runde av styringsaktiviteter
* Detaljplan for en avgrenset periode
  + Bruk av ulike enheter som piloter for sentrale aktiviteter
* Hvem som bør involveres
  + Fagpersoner fra andre internkontrollområder
  + Interne tiltaksleverandører (personal, bygg, IKT-drift, IKT-utvikling …)
  + Ledere/enheter som er aktuelle for pilot
* Anbefalinger om prioriteringer
* Overordnet estimat av omfang og tidsperspektiv
  + At virksomheten trenger tid til å ta inn over seg nye prosesser, samtidig som nødvendige endringer må drives frem (for mange vil det være snakk om en organisasjonsendring hvor kultur og kompetanse står sentralt)
* Poengtere at dette er ledelsens redskap, og hvor viktig det er med god og tydelig lederforankring og støtte