Dette er ei liste med punkt som kan vere aktuelle å ha med i eit saksnotat som grunnlag for toppleiinga vi avgjersle om etablering/forbetring av internkontroll på informasjonssikkerheitsområdet, etter at ein analyse av status har vore gjennomført. Lista kan brukast som støtte til arbeidet med å lage eit slikt saksnotat for di verksemd.

Sentrale punkt i avgjerdsgrunnlag

# Bakgrunn

* Korleis informasjonssikkerheit påverkar måloppnåing
* Behovet for god informasjonssikkerheit
* Eit system av aktivitetar for styring og kontroll er leiinga sitt reiskap i arbeidet med informasjonssikkerheit
* Det er snakk om systematikk og formalisering som gjev verksemdsleiinga og linja elles **tillit** til at verksemda på ein akseptabel måte identifiserer og handterer risiko
* Regelverk
	+ eForvaltningsforskrifta § 15 og generelt i økonomiregelverket i staten/kommunelova
	+ Sikkerheitslova stiller krav til styring og kontroll (sikkerheitsstyring) i samband med arbeidet med å sikre skjermingsverdig informasjon og skjermingsverdige informasjonssystem (og objekt og infrastruktur) mot sikkerheitstruande verksemd
	+ Personopplysningslova/personvernforordninga stiller krav til informasjonssikkerheit ved behandling av personopplysningar, og internkontroll på personvernområdet
	+ Sektorregelverk
* Forståing for at internkontroll langt i frå berre handlar om å etterleve regelverk, men å
	+ Nå måla til verksemda
	+ Arbeide effektivt
	+ Etterleve lover og regler
	+ Ha påliteleg rapportering
* Kort skildring av Digitaliseringsdirektoratet sitt rettleiingsmateriell, og sentrale anbefalingar om
	+ Analyse av status med Digitaliseringsdirektoratet sitt rettleiingsmateriell som referanse
	+ Planlegge etablering/forbetring av internkontroll på informasjonssikkerheitsområdet

# Oppsummering av analysen

* Hovudinntrykk
	+ Er vi til dømes gjennomgåande på 0-1 eller 2-3 i analyseskjemaet?
	+ Kor er vi evt. gode eller rimeleg bra?
	+ Kor ser det ut til å vere størst utfordringar?
	+ Er det sentrale område som må forbetrast?
* Kva endringar bør vi gjere?
	+ Fordeling mellom nye aktivitetar som må på plass og formalisering og justering av eksisterande
	+ Behov for grunnopplæring av leiarar og anna kompetanseutvikling
* Oppsummeringa bør inkludere omtale av samanheng med andre internkontrollområde
	+ Verksemdsstyring, risikostyring og internkontroll generelt, til dømes i tråd med DFØ si rettleiing
	+ Risikostyring generelt i samsvar med til ISO 31000
	+ Personvern
	+ HMS
	+ Nasjonal sikkerheit (sikkerheitslova sitt område)
	+ Styring av verksemdskontinuitet
* Dersom det er relevant bør oppsummeringa spesielt omtale utfordringar ved organisering og rolleforståing, til dømes at
	+ leiarar i linja ikkje forstår behovet for informasjonssikkerheit for å understøtte arbeidsprosessane/-oppgåvene
	+ ein ikkje har gode støttefunksjonar og fagkompetanse som kan støtte linjeleiarar på ein god måte (merk: det er skilnad på å vere støtte, og å ta over ansvaret)
	+ det manglar forståing for ansvarsdelinga mellom «risikoeigarar» og «tiltaksleverandørar»
	+ plassering av systemeigarskap til fagsystem ikkje er forankra i fagavdelingane

# Anbefalingar

* Grov plan for heile planperioden
	+ Varigheit over fleire år
	+ Etableringsaktivitetar, informasjon, opplæring, og fyrste runde av styringsaktivitetar
* Detaljplan for ein avgrensa periode
	+ Bruk av ulike einingar som pilotar for sentrale aktivitetar
* Kven som bør involverast
	+ Fagpersonar frå andre internkontrollområde
	+ Interne tiltaksleverandørar (personal, bygg, IKT-drift, IKT-utvikling …)
	+ Leiarar/einingar som er aktuelle for pilot
* Anbefalingar om prioriteringar
* Overordna estimat av omfang og tidsperspektiv
	+ At verksemda treng tid til å ta inn over seg nye prosessar, samtidig som nødvendige endringar må drivast fram (for mange vil det vere snakk om ei organisasjonsendring der kultur og kompetanse står sentralt)
* Poengtere at dette er leiinga sitt reiskap, og kor viktig det er med god og tydeleg leiarforankring og støtte