Digitaliseringsdirektoratet
Norwegian Digitalisation Agency

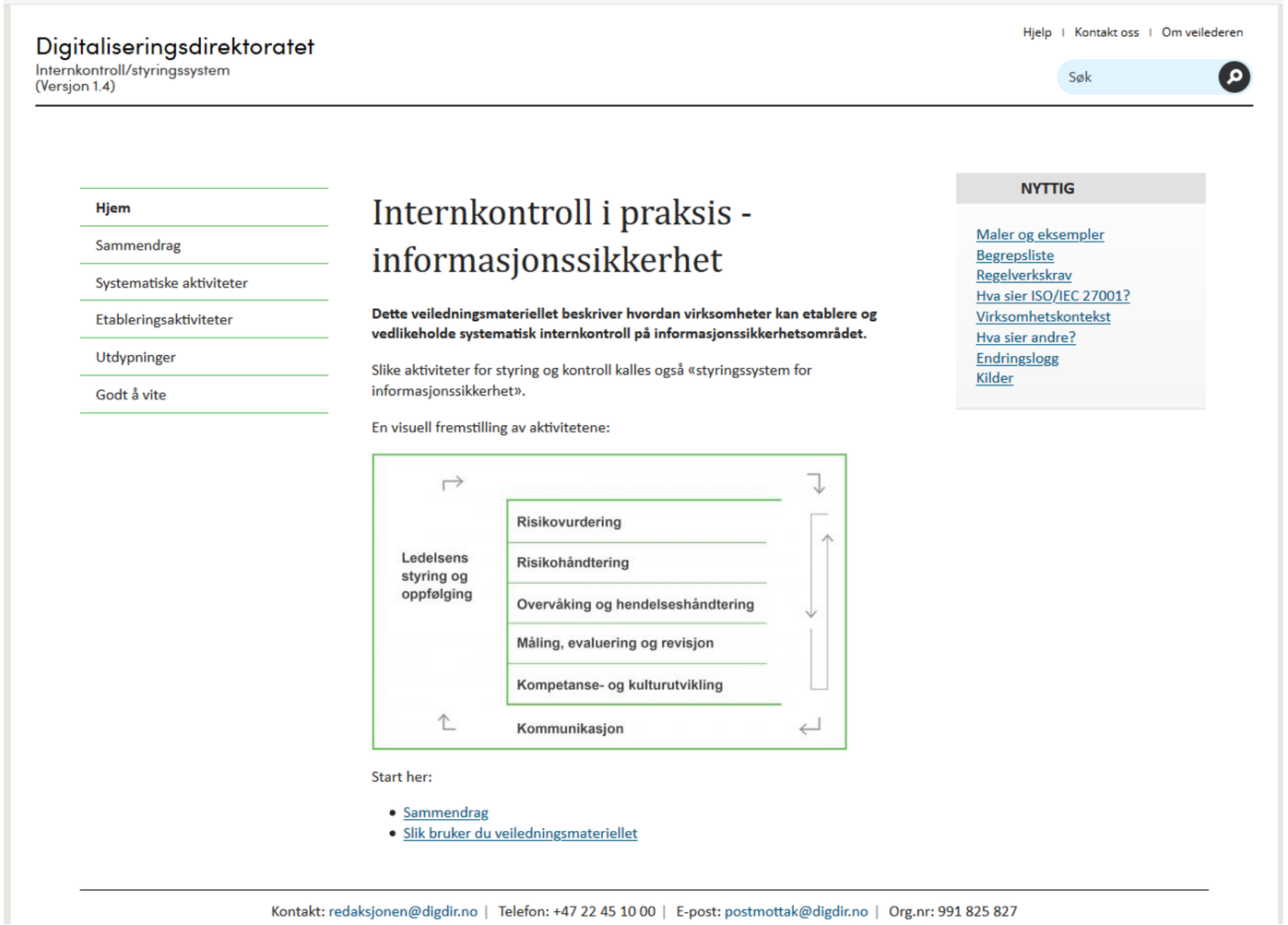
# Nytt fra Digitaliseringsdirektoratet

Kjetil Korslien
Seksjonssjef

# Seksjon for informasjonssikkerhet

- Digitaliseringsstrategien
- Nasjonal strategi for digital sikkerhet
  - Styring og kontroll på informasjonssikkerhet
    - Både stat og kommuner
  - Gi veiledning og anbefalinger på styring og kontroll av informasjonssikkerhet
  - Samordning / helhetlig tilbud til forvaltningen på veiledning
  - Anbefalingene fra evalueringen i 2018 skal følges opp

# Styring og kontroll



Digitaliseringsdirektoratet
Internkontroll/styringssystem
(Versjon 1.4)

Hjelp | Kontakt oss | Om veilederen

Søk

- Hjem
- Sammendrag
- Systematiske aktiviteter
- Etableringsaktiviteter
- Utdypninger
- Godt å vite

## Internkontroll i praksis - informasjonssikkerhet

**Dette veiledningsmateriellet beskriver hvordan virksomheter kan etablere og vedlikeholde systematisk internkontroll på informasjonssikkerhetsområdet.**

Slike aktiviteter for styring og kontroll kalles også «styringssystem for informasjonssikkerhet».

En visuell fremstilling av aktivitetene:



Start her:

- Sammendrag
- Slik bruker du veiledningsmateriellet

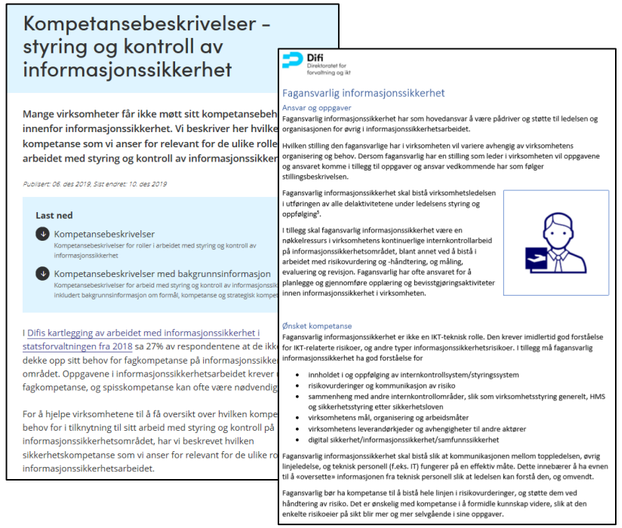
**NYTTIG**

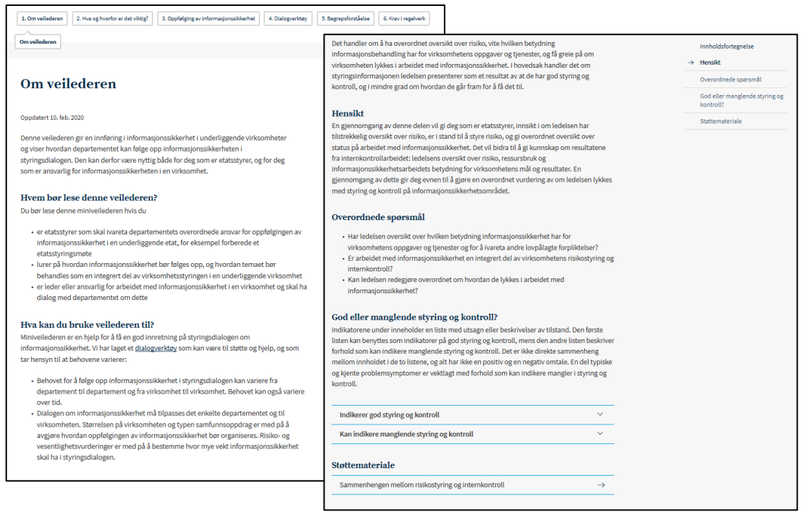
- Maler og eksempler
- Begrepsliste
- Regelverkskrav
- Hva sier ISO/IEC 27001?
- Virksomhetskontekst
- Hva sier andre?
- Endringslogg
- Kilder

Kontakt: redaksjonen@digdir.no | Telefon: +47 22 45 10 00 | E-post: postmottak@digdir.no | Org.nr: 991 825 827

# Oppfølging Difi-rapport 2018:4

| Delprosjekt | Leder | Bidrar |
|---|---|---|
| Etatsstyring | Ø | Difi, NSM |
| Øvelser for bedre informasjonssikkerhet | dsb | Difi, NSM |
| Sikkerhetskultur | NorSIS | Difi |
| Kompetanse | Difi | NorSIS |
| Risikostyring av informasjonssikkerhet | Ø, Difi | NSM |

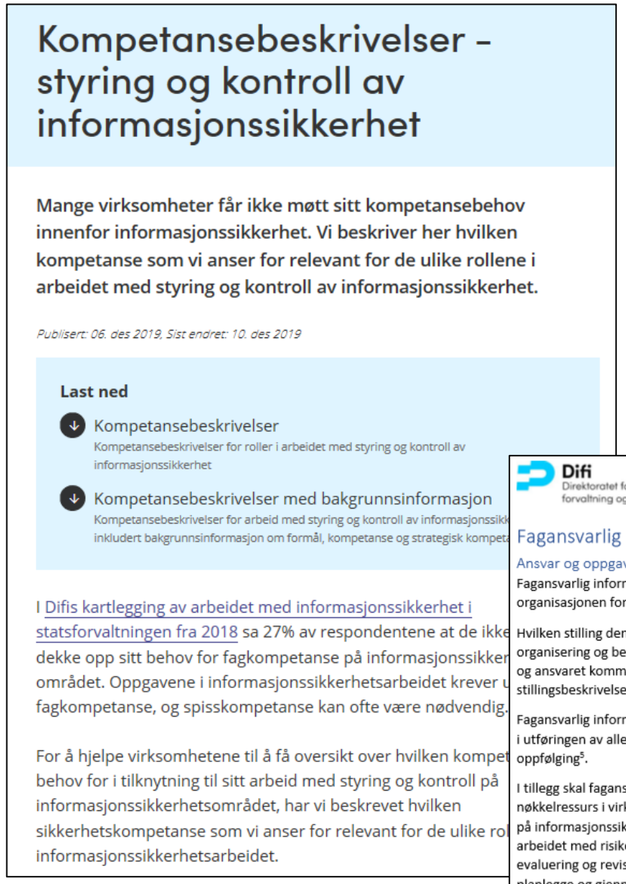


# Kompetanse

- Veileder
- Kompetanseutvikling
- Ansettelser
- Medarbeidersamtaler
- Basert på roller i Veileder for internkontroll

https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet/veiledere/kompetansebeskrivelser-styring-og-kontroll-av-informasjonssikkerhet



Kompetansebeskrivelser – styring og kontroll av informasjonssikkerhet

Mange virksomheter får ikke møtt sitt kompetansebehov innenfor informasjonssikkerhet. Vi beskriver her hvilken kompetanse som vi anser for relevant for de ulike rollene i arbeidet med styring og kontroll av informasjonssikkerhet.

*Publisert: 06. des 2019, Sist endret: 10. des 2019*

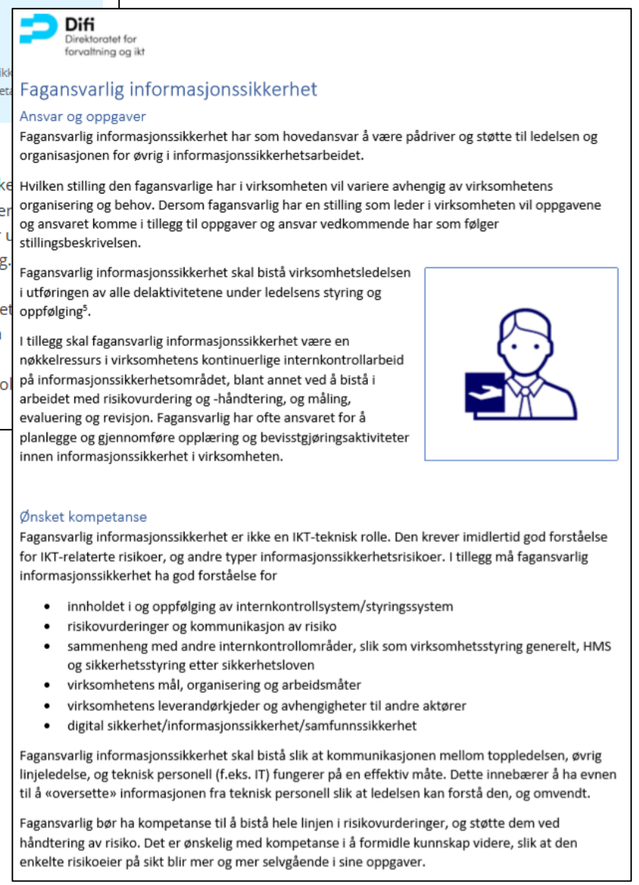
**Last ned**

Kompetansebeskrivelser
Kompetansebeskrivelser for roller i arbeidet med styring og kontroll av informasjonssikkerhet

Kompetansebeskrivelser med bakgrunnsinformasjon
Kompetansebeskrivelser for arbeid med styring og kontroll av informasjonssikk
inkludert bakgrunnsinformasjon om formål, kompetanse og strategisk kompet

I Difis kartlegging av arbeidet med informasjonssikkerhet i statsforvaltningen fra 2018 sa 27% av respondentene at de ikke
dekke opp sitt behov for fagkompetanse på informasjonssikker
området. Oppgavene i informasjonssikkerhetsarbeidet krever u
fagkompetanse, og spisskompetanse kan ofte være nødvendig.

For å hjelpe virksomhetene til å få oversikt over hvilken kompet
behov for i tilknytning til sitt arbeid med styring og kontroll på
informasjonssikkerhetsområdet, har vi beskrevet hvilken
sikkerhetskompetanse som vi anser for relevant for de ulike rol
informasjonssikkerhetsarbeidet.



Difi
Direktoratet for forvaltning og ikt

Fagansvarlig informasjonssikkerhet

Ansvar og oppgaver

Fagansvarlig informasjonssikkerhet har som hovedansvar å være pådriver og støtte til ledelsen og organisasjonen for øvrig i informasjonssikkerhetsarbeidet.

Hvilken stilling den fagansvarlige har i virksomheten vil variere avhengig av virksomhetens organisering og behov. Dersom fagansvarlig har en stilling som leder i virksomheten vil oppgavene og ansvaret komme i tillegg til oppgaver og ansvar vedkommende har som følger stillingsbeskrivelsen.

Fagansvarlig informasjonssikkerhet skal bistå virksomhetsledelsen i utføringen av alle delaktivitetene under ledelsens styring og oppfølging[5].

I tillegg skal fagansvarlig informasjonssikkerhet være en nøkkelressurs i virksomhetens kontinuerlige internkontrollarbeid på informasjonssikkerhetsområdet, blant annet ved å bistå i arbeidet med risikovurdering og -håndtering, og måling, evaluering og revisjon. Fagansvarlig har ofte ansvaret for å planlegge og gjennomføre opplæring og bevisstgjøringsaktiviteter innen informasjonssikkerhet i virksomheten.

Ønsket kompetanse

Fagansvarlig informasjonssikkerhet er ikke en IKT-teknisk rolle. Den krever imidlertid god forståelse for IKT-relaterte risikoer, og andre typer informasjonssikkerhetsrisikoer. I tillegg må fagansvarlig informasjonssikkerhet ha god forståelse for

- innholdet i og oppfølging av internkontrollsystem/styringssystem
- risikovurderinger og kommunikasjon av risiko
- sammenheng med andre internkontrollområder, slik som virksomhetsstyring generelt, HMS og sikkerhetsstyring etter sikkerhetsloven
- virksomhetens mål, organisering og arbeidsmåter
- virksomhetens leverandørkjeder og avhengigheter til andre aktører
- digital sikkerhet/informasjonssikkerhet/samfunnssikkerhet

Fagansvarlig informasjonssikkerhet skal bistå slik at kommunikasjonen mellom toppledelsen, øvrig linjeledelse, og teknisk personell (f.eks. IT) fungerer på en effektiv måte. Dette innebærer å ha evnen til å «oversette» informasjonen fra teknisk personell slik at ledelsen kan forstå den, og omvendt.

Fagansvarlig bør ha kompetanse til å bistå hele linjen i risikovurderinger, og støtte dem ved håndtering av risiko. Det er ønskelig med kompetanse i å formidle kunnskap videre, slik at den enkelte risikoeier på sikt blir mer og mer selvgående i sine oppgaver.

# Etatsstyring

- Veileder for etatsstyring av informasjonssikkerhet i underliggende virksomhet
- Veileder
- Dialogverktøy


1. Om veilederen | 2. Hva og hvorfor er det viktig? | 3. Oppfølging av informasjonssikkerhet | 4. Dialogverktøy | 5. Begrepsforståelse | 6. Krav i regelverk

Om veilederen

## Om veilederen

Oppdatert 10. feb. 2020

Denne veilederen gir en innføring i informasjonssikkerhet i underliggende virksomheter og viser hvordan departementet kan følge opp informasjonssikkerheten i styringsdialogen. Den kan derfor være nyttig både for deg som er etatsstyrer, og for deg som er ansvarlig for informasjonssikkerheten i en virksomhet.



### Hvem bør lese denne veilederen?

Du bør lese denne miniveilederen hvis du

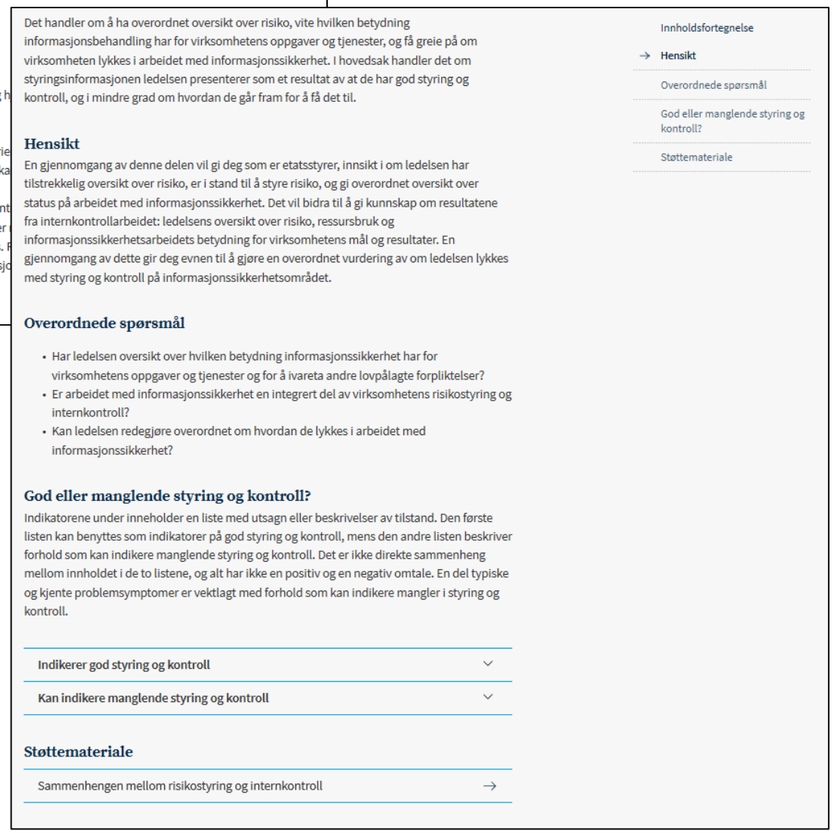
- er etatsstyrer som skal ivareta departementets overordnede ansvar for oppfølgingen av informasjonssikkerhet i en underliggende etat, for eksempel forberede et etatsstyringsmøte
- lurer på hvordan informasjonssikkerhet bør følges opp, og hvordan temaet bør behandles som en integrert del av virksomhetsstyringen i en underliggende virksomhet
- er leder eller ansvarlig for arbeidet med informasjonssikkerhet i en virksomhet og skal ha dialog med departementet om dette

### Hva kan du bruke veilederen til?

Miniveilederen er en hjelp for å få en god innretning på styringsdialogen om informasjonssikkerhet. Vi har laget et dialogverktøy som kan være til støtte og h
tar hensyn til at behovene varierer:

- Behovet for å følge opp informasjonssikkerhet i styringsdialogen kan varie
departement til departement og fra virksomhet til virksomhet. Behovet ka
over tid.
- Dialogen om informasjonssikkerhet må tilpasses det enkelte departement
virksomheten. Størrelsen på virksomheten og typen samfunnsoppdrag er
avgjøre hvordan oppfølgingen av informasjonssikkerhet bør organiseres. F
vesentlighetsvurderinger er med på å bestemme hvor mye vekt informasj
skal ha i styringsdialogen.

Innholdsfortegnelse
→ Hvem bør lese denne veilederen?
Hva kan du bruke veilederen til?


Det handler om å ha overordnet oversikt over risiko, vite hvilken betydning informasjonsbehandling har for virksomhetens oppgaver og tjenester, og få greie på om virksomheten lykkes i arbeidet med informasjonssikkerhet. I hovedsak handler det om styringsinformasjonen ledelsen presenterer som et resultat av at de har god styring og kontroll, og i mindre grad om hvordan de går fram for å få det til.

### Hensikt

En gjennomgang av denne delen vil gi deg som er etatsstyrer, innsikt i om ledelsen har tilstrekkelig oversikt over risiko, er i stand til å styre risiko, og gi overordnet oversikt over status på arbeidet med informasjonssikkerhet. Det vil bidra til å gi kunnskap om resultatene fra internkontrollarbeidet: ledelsens oversikt over risiko, ressursbruk og informasjonssikkerhetsarbeidets betydning for virksomhetens mål og resultater. En gjennomgang av dette gir deg evnen til å gjøre en overordnet vurdering av om ledelsen lykkes med styring og kontroll på informasjonssikkerhetsområdet.

### Overordnede spørsmål

- Har ledelsen oversikt over hvilken betydning informasjonssikkerhet har for virksomhetens oppgaver og tjenester og for å ivareta andre lovpålagte forpliktelser?
- Er arbeidet med informasjonssikkerhet en integrert del av virksomhetens risikostyring og internkontroll?
- Kan ledelsen redegjøre overordnet om hvordan de lykkes i arbeidet med informasjonssikkerhet?

### God eller manglende styring og kontroll?

Indikatorene under inneholder en liste med utsagn eller beskrivelser av tilstand. Den første listen kan benyttes som indikatorer på god styring og kontroll, mens den andre listen beskriver forhold som kan indikere manglende styring og kontroll. Det er ikke direkte sammenheng mellom innholdet i de to listene, og alt har ikke en positiv og en negativ omtale. En del typiske og kjente problemsymptomer er vektlagt med forhold som kan indikere mangler i styring og kontroll.

Indikerer god styring og kontroll
Kan indikere manglende styring og kontroll

### Støttemateriale

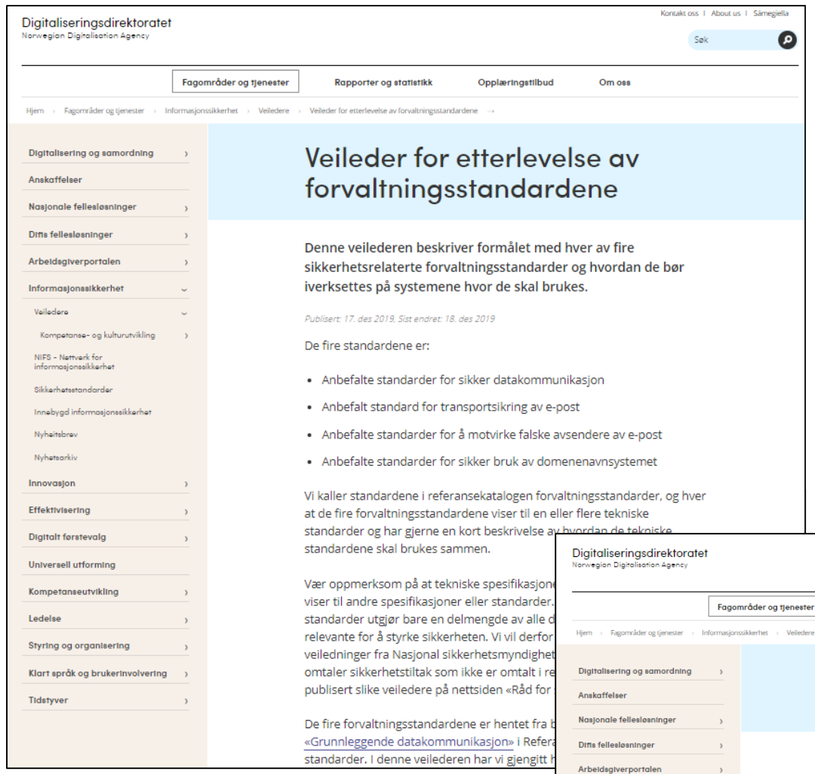
Sammenhengen mellom risikostyring og internkontroll →

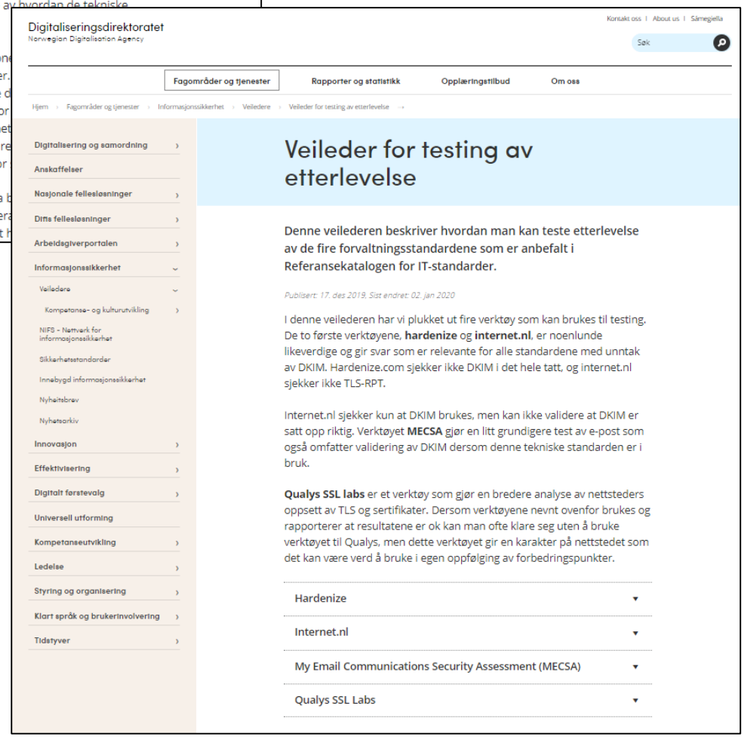
Innholdsfortegnelse
→ Hensikt
Overordnede spørsmål
God eller manglende styring og kontroll?
Støttemateriale

https://dfo.no/fagomrader/etats-og-virksomhetsstyring/etatsstyring/miniveileder-om-oppfolging-av-informasjonssikkerhet-i-styringsdialogen/om-veilederen

# Sikkerhetsstandarder

- Veiledere for etterlevelse av fire sikkerhetsstandarder
- Veileder for etterlevelse
- Veileder for testing av etterlevelse




https://www.difi.no/fagomrader-og-tjenester/informasjonssikkerhet/veiledere/veileder-etterlevelse-av-fire-sikkerhetsstandarder

# Informasjonssikkerhet i kommunene

- Kunnskapsgrunnlag om arbeidet med informasjonssikkerhet i kommunene.
- I samarbeid med KS
- Dokumentstudier


**Digitaliseringsdirektoratet**
Norwegian Digitalisation Agency


Digitaliseringsdirektoratet
Norwegian Digitalisation Agency