

**Digitaliseringsdirektoratet**  
Norwegian Digitalisation Agency

**Nytt fra Digitaliseringsdirektoratet**

—

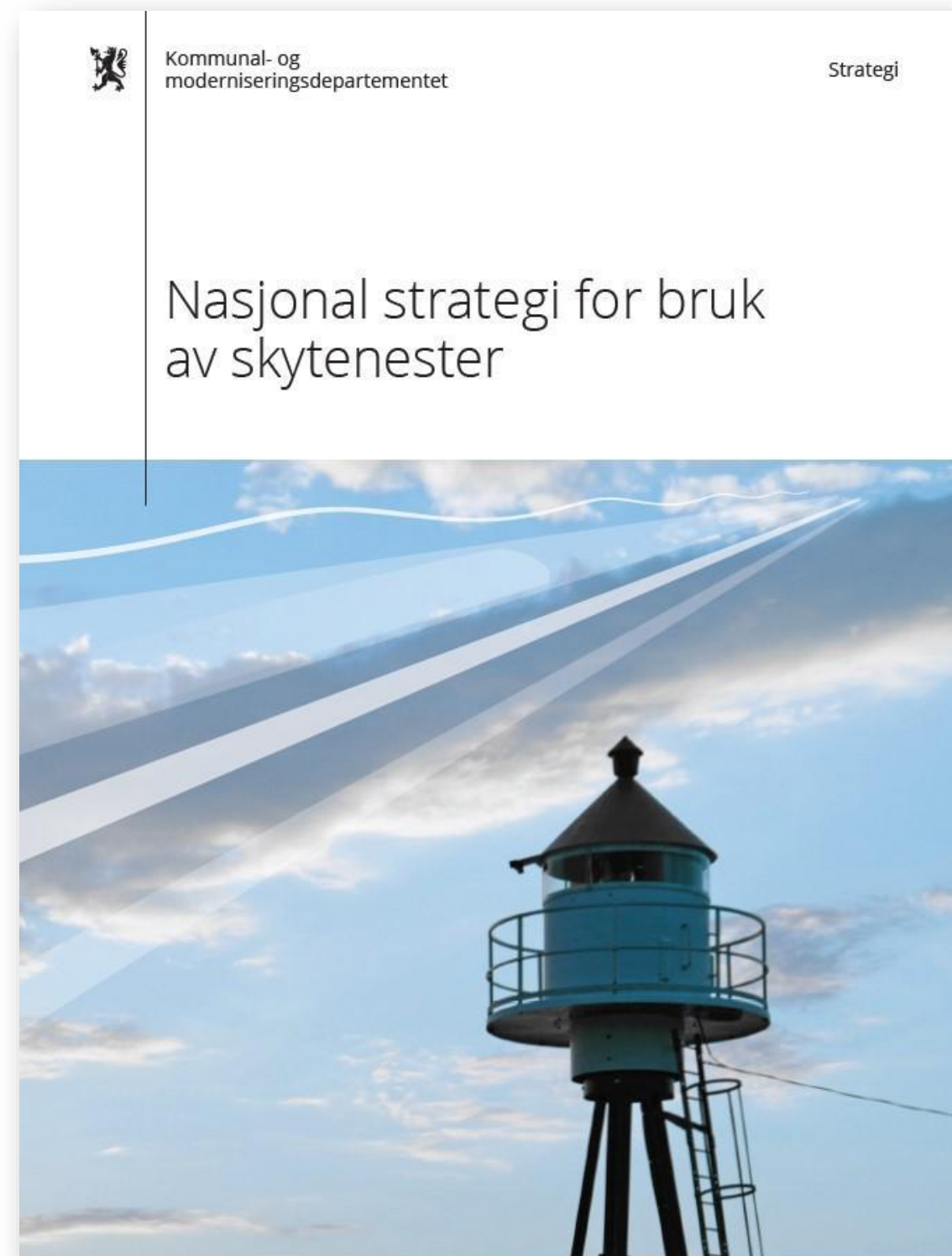
# Markeds plass for skytjenester

Det skal etableres en markeds plass for skytjenester.

Markeds plassen skal gjøre det **enklere** for virksomhetene å anskaffe **sikre**, **lovlige** og **kostnadseffektive** skytjenester.

## Anskaffelser.no

<https://www.anskaffelser.no/hva-skal-du-kjope/it/skytjenester-cloud/markeds plass-skytjenester>



# Kontroll av gratistjenester

Krav til produsent/leverandør

Minimumskrav til tjenesten

# Standardkrav til sikkerhet













Standardkrav er utarbeidet

Metode for evaluering av krav

<https://www.anskaffelser.no/hva-skal-du-kjope/it/informasjonssikkerheit-og-personvern/krav-til-sikkerheit>

R1	Trussel- og sårbarhetsvurderinger	▼
R2	Lock-In	▼
R3	Endring og avlytting av data under overføring	▼
R4	Datasenterets sikkerhet	▼
R5	Sikring av lagret informasjon	▼
R6	Separasjon mellom kunder	▼
R7	Sletting av data	▼
R8	Tilgjengelighet	▼
R9	Endringshåndtering	▼
R10	Sporbarhet	▼
R11	Tilgangskontroll / Autentisering	▼
R12	Sikkerhetsbrudd / Varsling	▼

# Oppfølging Difi-rapport 2018:4

Delprosjekt	Leder	Bidrar
Etatsstyring		 
Øvelser for bedre informasjonssikkerhet		 
Sikkerhetskultur		
Kompetanse		
Risikostyring av informasjonssikkerhet		

### Kompetansebeskrivelser – styring og kontroll av informasjonssikkerhet

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

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

**Last ned**

- Kompetansebeskrivelser
- Kompetansebeskrivelser med bakgrunnsinformasjon

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

For å hjelpe virksomhetene til å få oversikt over hvilken kompetanse de trenger for å gjennomføre sitt arbeid med styring og kontroll av informasjonssikkerhetsområdet, har vi beskrevet hvilken sikkerhetskompetanse som vi anser for relevant for de ulike roller i informasjonssikkerhetsarbeidet.

#### 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\*.

I tillegg skal fagansvarlig informasjonssikkerhet være en nøkkelperson 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 bevisstgøringstiltak 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 leverandører og avhengigheter til andre aktører
- digital sikkerhet/informasjonssikkerhet/samfunnssikkerhet

Fagansvarlig informasjonssikkerhet skal bistå slik at kommunikasjonen mellom toppledelsen, øvrig ledelse, 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 risikoer på sikt blir mer og mer selvgående i sine oppgaver.

1. Om veilederen 2. Hva og hvorfor er det viktig? 3. Oppfølging av informasjonssikkerhet 4. Dialoger/veier 5. Begrepsforståelse 6. Finn i regelverk

### 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 statsstyre, og for deg som er ansvarlig for informasjonssikkerheten i en virksomhet.

#### Hvem bør lese denne veilederen?

Du bør lese denne miniveilederen hvis du

- er statsstyre 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 **dialogveier** som kan være til støtte og hjelp, og som tar hensyn til at behovene varierer:

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

Det handler om å ha overordnet oversikt over risiko, vite hvilken betydning informasjonshandling 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 statsstyre, 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?

Indikatorne 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

#### Støttmateriale

Sammenhengen mellom risikostyring og internkontroll →

Innholdsfortegnelse

- Hensikt
- Overordnede spørsmål
- God eller manglende styring og kontroll?
- Støttmateriale

*Digitaliseringsdirektoratet*  
*Norwegian Digitalisation Agency*