

**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 veiledningsmaterialet 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 veiledningsmaterialet](#)

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

**NYTTIG**

- [Maler og eksempler](#)
- [Begrepsliste](#)
- [Regelverkskrav](#)
- [Hva sier ISO/IEC 27001?](#)
- [Virksomhetskontekst](#)
- [Hva sier andre?](#)
- [Endringslogg](#)
- [Kilder](#)

# 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**

- 1. Kompetansebeskrivelser
- 2. 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 arbeidet med styring og kontroll av informasjonssikkerhet, har vi beskrevet hvilken sikkerhetskompetanse som vi anser for relevant for de ulike roller i informasjonssikkerhetsarbeidet.

### Fagsvarlig informasjonssikkerhet

**Ansvar og oppgaver**  
Fagsvarlig informasjonssikkerhet har som hovedansvar å være pådriver og støtte til ledelsen og organisasjonen for øvrig i informasjonssikkerhetsarbeidet.

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

Fagsvarlig informasjonssikkerhet skal bistå virksomhetsledelsen i utføringen av alle delaktivitetene under ledelsens styring og oppfølging\*.

I tillegg skal fagsvarlig 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. Fagsvarlig har ofte ansvaret for å planlegge og gjennomføre opplæring og bevisstgjøringstiltak innen informasjonssikkerhet i virksomheten.

**Ønsket kompetanse**  
Fagsvarlig informasjonssikkerhet er ikke en IKT-teknisk rolle. Den krever imidlertid god forståelse for IKT-relaterte risikoer, og andre typer informasjonssikkerhetsrisikoer. I tillegg må fagsvarlig 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/samfunnsikkerhet

Fagsvarlig 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.

Fagsvarlig 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. Dialogverktøy | 5. Begrepsfortellere | 6. Kvit 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 **dialogverktøy** 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?**  
Indikatoren 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

# Kompetanse

- Veileder
- Kompetanseutvikling
- Ansettelses
- 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 informasjonssikkerhet inkludert bakgrunnsinformasjon om formål, kompetanse og strategisk kompetanse

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 informasjonssikkerhetsområdet. Oppgavene i informasjonssikkerhetsarbeidet krever ulike fagkompetanse, og spisskompetanse kan ofte være nødvendig.

For å hjelpe virksomhetene til å få oversikt over hvilken kompetansebehov 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 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<sup>5</sup>.

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/samfunnsikkerhet

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

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

1. Om veilederen 2. Hva og hvorfor er det viktig? 3. Oppfølging av informasjonssikkerhet 4. Dialogverktøy 5. Begrepsforståelse 6. Krav 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 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 hjalp. Det tar hensyn til at behovene varierer:

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

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 ✓

**Støttmateriale**

Sammenhengen mellom risikostyring og internkontroll →



Innholdsfortegnelse

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

Indikerer god styring og kontroll ✓

Kan indikere manglende styring og kontroll ✓

**Støttmateriale**

Sammenhengen mellom risikostyring og internkontroll →

# Sikkerhetsstandarder

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

<https://www.difi.no/fagomrader-og-tjenester/informasjonsikkerhet/veiledere/veileder-e-etterlevelse-av-fire-sikkerhetsstandarder>

Digitaliseringsdirektoratet  
Norwegian Digitalisation Agency

Kontakt oss | About us | Samspeilla

Søk

Fagområder og tjenester | Rapporter og statistikk | Opplæringstilbud | Om oss

Hjem > Fagområder og tjenester > Informasjonsikkerhet > Veiledere > Veileder for etterlevelse av forvaltningsstandardene

## Veileder for etterlevelse av forvaltningsstandardene

Denne veilederen beskriver formålet med hver av fire sikkerhetsrelaterte forvaltningsstandarder og hvordan de bør iverksettes på systemene hvor de skal brukes.

Publisert: 17. des 2019. Sist endret: 18. des 2019

De fire standardene er:

- Anbefalte standarder for sikker datakommunikasjon
- Anbefalt standard for transportsikring av e-post
- Anbefalte standarder for å motvirke falske avsendere av e-post
- Anbefalte standarder for sikker bruk av domenenavnssystemet

Vi kaller standardene i referanse katalogen forvaltningsstandarder, og hver av de fire forvaltningsstandardene viser til en eller flere tekniske standarder og har gjerne en kort beskrivelse av hvordan de tekniske standardene skal brukes sammen.

Vær oppmerksom på at tekniske spesifikasjoner viser til andre spesifikasjoner eller standarder, som standarder utgjør bare en delmengde av alle de relevante for å styrke sikkerheten. Vi vil derfor veiledninger fra Nasjonal sikkerhetsmyndighet omtaler sikkerhetstiltak som ikke er omtalt i referansen, publisert slike veiledere på nettsiden «Råd for sikkerhet».

De fire forvaltningsstandardene er hentet fra [«Grunnleggende datakommunikasjon»](#) i Referanse katalogen for IT-standarder. I denne veilederen har vi gjengitt



Digitaliseringsdirektoratet  
Norwegian Digitalisation Agency

Kontakt oss | About us | Samspeilla

Søk

Fagområder og tjenester | Rapporter og statistikk | Opplæringstilbud | Om oss

Hjem > Fagområder og tjenester > Informasjonsikkerhet > Veiledere > Veileder for testing av etterlevelse

## Veileder for testing av etterlevelse

Denne veilederen beskriver hvordan man kan teste etterlevelse av de fire forvaltningsstandardene som er anbefalt i Referanse katalogen for IT-standarder.

Publisert: 17. des 2019. Sist endret: 02. jan 2020

I denne veilederen har vi plukket ut fire verktøy som kan brukes til testing. De to første verktøyene, **hardenize** og **internet.nl**, er noenlunde likeverdige og gir svar som er relevante for alle standardene med unntak av DKIM. Hardenize.com sjekker ikke DKIM i det hele tatt, og internet.nl sjekker ikke TLS-RPT.

Internet.nl sjekker kun at DKIM brukes, men kan ikke validere at DKIM er satt opp riktig. Verktøyet **MECSA** gjør en litt grundigere test av e-post som også omfatter validering av DKIM dersom denne tekniske standarden er i bruk.

**Qualys SSL labs** er et verktøy som gjør en bredere analyse av nettsteders oppsett av TLS og sertifikater. Dersom verktøyene nevnt ovenfor brukes og rapporterer at resultatene er ok kan man ofte klare seg uten å bruke verktøyet til Qualys, men dette verktøyet gir en karakter på nettstedet som det kan være verd å bruke i egen oppfølging av forbedringspunkter.

Hardenize	▼
Internet.nl	▼
My Email Communications Security Assessment (MECSA)	▼
Qualys SSL Labs	▼

# Informasjonssikkerhet i kommunene

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

**INTERN RAPPORT**  
*IKT-sikkerhet på lokalt og regionalt nivå*  
Vurdering av felles arena for digital IKT-sikkerhet på regionalt og lokalt nivå, og fylkesmannens rolle i responsmiljøene og i nasjonalt rammerverk for digital helse- og omsorgstjeneste.

**Datatilsynet**  
Hva leter du etter? Q  
Lover og regler  
**Sentrale avgjørelser**  
På denne siden finner dere noen sentrale avgjørelser Datatilsynets har vedtatt de siste årene. Disse kan ha betydning for andre virksomheter også.  
År  
2019 (5)  
2017 (2)  
2016 (2)  
2015 (1)  
[Gebyr til Oslo kommune Utdanningsetaten](#)  
01.12.2019  
Datatilsynet sendte i april 2019 varsel til Oslo kommune Utdanningsetaten om et overtredelsesgebyr for brudd på personopplysningsikkerheten i mobilapplikasjonen Skolemelding. I oktober ble det vedtatt et endelig

**dsb** Det nasjonale kompetansesenteret for informasjonssikkerhet  
**Bruk av IKT i offentlig sektor**  
Forsiden > [TeknologiLog innovasjon](#) > Bruk av IKT i offentlig sektor  
Oppdatert 29. april 2019  
Neste oppdatering 4. mai 2020  
**10,5 %**  
av norske kommuner har vært rammet av virusangrep e.l. som har ført til tap av data eller arbeidstid  
IKT-sikkerhetsproblemer i løpet av det siste året. Prosent.  
Statlige virksomheter  
2019  
Sammenbrudd i forbindelsen til internett eller andre eksterne nettker 14,7  
Virusangrep, ormer eller lignende som resulterte i tap av data eller arbeidstid 1,9  
Angrep av typen 'denial of service' 14,7  
Uautorisert tilgang til systemer eller data 20,9  
Datatap pga manglende backup 2,8  
IT-misbruk av økonomisk karakter 8,5  
Forsøk på identsitetstyveri (fobistruer) 63,0

Utredning av kommunal sektors felles behov for et kompetansesenter for håndtering av IKT-hendelser (KommuneCSIRT)  
Desember 2017  
NorSIS



*Digitaliseringsdirektoratet*  
*Norwegian Digitalisation Agency*