# Arbeidet med informasjonssikkerheit i statsforvaltninga

Kunnskapsgrunnlag

*Kjelde til forsidebilete: Wombo Dream – AI Art Generator*

# Innhaldsliste

# 1. Samandrag og konklusjon

Når ein ser på resultata frå undersøkinga under eitt, meiner vi det er riktig å seie at dei fleste verksemdene har etablert eit godt grunnlag for kontinuerleg forbetring. Årets undersøking viser at verksemdene held oftare øvingar, og fleire har prosedyrar for å handtere hendingar enn tidlegare.

Likevel ser vi at utviklinga går sakte på andre område. For eksempel har verksemdene i liten grad oversikt over kostnader knytt til hendingar. Det er også utfordrande for verksemdene å ha oversikt over eige kompetansebehov, og å sette i verk nødvendige kompetansehevingstiltak.

Vår vurdering er derfor at det totalt sett framleis er utfordringar med korleis statlege verksemder arbeider med styring av informasjonssikkerheit. Men fleire av verksemdene seier dei er bevisst på eigne manglar og jobbar aktivt for å forbetre dei områda der ein ikkje har komme like langt.

Regjeringa har gjennom digitaliseringsstrategien tydeleggjort målsettingar for arbeidet med informasjonssikkerheit i stat og kommune. Innan 2030 skal alle statlege verksemder, og 90 prosent av kommunane, ha forbetra eller fornya styringssystemet for informasjonssikkerheit. Ein kan nytte konklusjonane frå denne rapporten til å prioritere tiltak verksemda må gjere for å nå måla i strategien.

Vi har i denne undersøkinga ikkje spurt verksemdene om kva dei sjølv ser på som årsaker til at arbeidet på nokre område ikkje har komme lengre. Undersøkinga er ei vurdering frå fagpersonar i verksemdene om korleis arbeidet med informasjonssikkerheit vert gjennomført i deira verksemd. Presentasjonen av hovudfunn er ei oppsummering av resultata frå denne undersøkinga.

## 1.1 Våre hovudfunn

- Det er framleis utfordringar med korleis statlege verksemder arbeider med informasjonssikkerheit. Dei fleste verksemdene har etablert eit godt grunnlag for kontinuerleg forbetring, men på nokre område går utviklinga feil veg.
- I spørjeundersøkinga fann vi at 90 prosent av dei fagansvarlege svarer at dei enten i stor eller moderat grad får tydelege føringar frå leiinga. I intervjua fortel om lag ein tredjedel av respondentane at dei opplever auka fokus i leiinga for å prioritere arbeidet med informasjonssikkerheit i verksemdene.
- 44,3 prosent av respondentane oppgir at dei i stor grad ser risikostyring av informasjonssikkerheit i samanheng med resten av risikostyringa i verksemda. 12,8 prosent svarer likevel at dei i liten eller ingen grad gjer det.
- Intervjua viser at det er stor variasjon i korleis verksemdene organiserer og prioriterer ressursar i arbeidet med informasjonssikkerheit. Også om fordeling av tydelege roller og ansvar. Det er likevel positivt at 89 prosent av verksemdene seier dei i stor eller moderat grad har definerte roller og ansvar i arbeidet med informasjonssikkerheit.
- Berre ei av fem verksemder seier dei i stor grad har tydelege retningslinjer for å akseptere risiko. Dette er ein nedgang frå førre undersøking. Samtidig seier nesten ein av fire dei i liten eller ingen grad har det. Når ein ikkje har klare kriterium for å akseptere risiko vert det både vanskeleg å vite kva risiko som er kritisk å prioritere, og å styre ressursbruken.
- Undersøkinga og intervjua viser at verksemdene vurderer og handterer risiko på ulike nivå. 60 prosent av verksemdene meiner dei er i god stand til å etablere dei sikkerheitstiltaka dei har behov for. Tek vi med dei som svarer i moderat grad er talet over 92 prosent.

- Ei av fem verksemder har i liten grad vurdert om etablerte sikkerheitstiltak er formålstenlege.[1]
- Nesten ei av fire verksemder kartlegg ikkje sine behov for kompetanseheving på informasjonssikkerheitsområdet. Verksemdene arbeider med sikkerheitskultur og kompetanse, men mange har tilsette med eit sprikande kompetansebehov, og det kan vere utfordrande å sette i verk nødvendige kompetansehevingstiltak.
- Fleire enn tidlegare gjennomfører årlege øvingar. Likevel er det ei av fem verksemder som ikkje øver minst éin gong i året. Det er også fleire verksemder som oppgir at berre delar av organisasjonen jobbar systematisk med øvingar.
- Verksemdene har i liten grad oversikt over kostnadene som informasjonssikkerheitshendingar kan føre til. I spørjeundersøkinga fann vi at 46 prosent i liten eller ingen grad har oversikt over kostnadene som følger av informasjonssikkerheitshendingar.

## 1.2 Konklusjon

Vi ser ei positiv utvikling på fleire område, og det er viktig at verksemdene held fram det gode arbeidet. Samla sett tyder resultata i undersøkinga på eit behov for å forbetre systematikk i evalueringa og implementeringa av sikkerheitstiltak. Dette er ein viktig føresetnad for å sikre heilskapleg og effektiv handtering av risiko.

Intervjua, og kommentarar til spørjeundersøkinga, viste at fleire var medvitne på kvar dei har forbetringspotensiale. Fleire verksemder har ein plan med tiltak, og arbeider med det.

Vi anbefaler alle verksemdene å

- etablere tydelege retningslinjer for å akseptere risiko
- etablere rutinar for å vurdere om etablerte sikkerheitstiltak fungerer etter formålet
- halde fram arbeidet med å styre informasjonssikkerheit og -risikoar i samanheng med annan risikostyring i verksemda
- framleis fokusere på arbeidet med kompetanse og sikkerheitskultur. Særleg kartlegge kva behov for kompetanseheving dei treng, for alle tilsette og ikkje berre utvalde grupper
- halde fram fokuset på øvingar og sikre at dei riktige delane av verksemda øver
    - At alle relevante deler av organisasjonen øver årleg på sine roller og relevante scenario

I undersøkinga har vi erfart at det er utfordrande å få anbefalingane til i praksis. Dette har fleire årsaker, og biletet kan sjå annleis ut i ulike verksemder. Mange seier informasjonssikkerheit har fått større fokus og leiinga er medviten at informasjonssikkerheit er viktig for verksemda og samfunnsoppdraget. Leiinga må sørge for at punkta over vert ført vidare, og legge til rette for at organiseringa av arbeidet med sikkerheit understøttar punkta.

Vi anbefaler at leiinga sørger for

- Tilstrekkeleg med kompetanse for å kunne utføre oppgåva.

[1] Retting: Ved ein feil sto det her først at «om lag halvparten av verksemdene har i stor eller moderat grad evaluert om etablerte sikkerheitstiltak er formålstenlege». Det riktige er at ei av fem verksemder i liten grad har vurdert om etablerte sikkerheitstiltak er formålstenlege. Feilen blei retta 21.01.2025, klokka 15:05.

- Nok tid og/eller ressursar til å utføre og følge oppgåvene systematisk, både operativt og i leiinga.
- Egna organisering av sikkerheit tilpassa verksemda, og fordele tydelege roller og ansvar.

For at verksemdene skal kunne oppnå heilskapleg tilnærming til sikkerheit meiner vi at verksemdene må få tydelegare tilrådingar og rettleiing frå styresmaktene på informasjonssikkerheitsområdet.

I digitaliseringsstrategien tek regjeringa til orde for betre samordning av råd- og rettleiingsressursar innanfor digital sikkerheit. Dette skal føre til at forvaltninga får eit klarare bilete av samla råd og rettleiing frå relevante myndigheiter, og sette verksemdene i stand til å gjennomføre eige arbeid med informasjonssikkerheit på ein formålstenleg måte. Digdir er gjennom *statens kompetansemiljø for informasjonssikkerheit* ansvarleg for å gi råd og anbefalingar til verksemder i statleg og kommunal sektor om gjennomføring av internkontroll på informasjonssikkerheitsområdet. Vi skal arbeide for samordna og brukarretta rettleiing og hjelp til offentleg sektor om å ivareta informasjonssikkerheit i verksemdene.[2]

For å lukkast med samordning av råd- og rettleiingsressursar må aktørar som rettleier i sikkerheit endre måten dei jobbar på. Anbefalingar, råd og rettleiing må i større grad utviklast i samarbeid mellom dei sentrale aktørane som rettleier verksemdene om informasjonssikkerheit, personvern og digital sikkerheit. Slik samordning krev ressursar, og bør prioriterast. Vi anbefaler at ein brukar etablerte samarbeidsforum for å styrke samordning av arbeidet med råd og rettleiing. "Felles sikkerhet i forvaltningen", kor Digdir er ein pådrivar, er eit eksempel på slikt initiativ.

# 2. Bakgrunn og behov

## 2.1 Om undersøkinga

Digdir sende spørjeskjema til fagpersonar i eit utval på 91 statlege verksemder (sjå vedlegg) med ulik storleik og organisering. 18 verksemder deltok i djupneintervju for å supplere med kvalitativ informasjon. Samla gir svara eit godt bilete på korleis statsforvaltninga arbeider med informasjonssikkerheit.

Rapporten viser korleis verksemdene arbeider med informasjonssikkerheit, men ho er ikkje ei kartlegging av sjølve sikkerheitstilstanden i den enkelte verksemda. Les heile analysen her: Analyse av dei enkelte vurderingstema | Digdir. Denne rapporten, som bygger på Digdir sitt rollemandat, kan bidra til effektiv politikkutvikling, tilrådingar og rettleiing innan informasjonssikkerheit.

Svarresultata kan tyde på at det generelt har vore lite utvikling i arbeidet med informasjonssikkerheit sidan 2018, då vi gjorde ei liknande undersøking. Det er likevel betring på enkelte område, mens andre område framleis verkar utfordrande for verksemdene å gjennomføre på ein tilfredsstillande måte.

I 2018 fann vi at statlege verksemder må styrke arbeidet med styring og kontroll av informasjonssikkerheit slik at verksemdene vert tilstrekkeleg modne og betre rusta til å følge endringar i trusselbiletet.

[2] Tildelingsbrev 2024, Digitaliseringsdirektoratet

## 2.1 Målgruppe

I denne rapporten har vi samla kunnskap om tilstand, trendar og behov i arbeidet med informasjonssikkerheit i statsforvaltninga. Eit slikt kunnskapsgrunnlag er viktig for fleire partar i offentleg sektor. Det er viktig for verksemdene sjølve å få kunnskap om dei største utfordringane i arbeidet. Samtidig vil det vere eit nyttig verktøy for etatsstyrarar og andre som har behov for å forstå korleis det vert arbeidd med informasjonssikkerheit i statsforvaltninga. Vi meiner også at eit kunnskapsgrunnlag av denne typen er eit viktig verktøy for aktørar som skal rettleie arbeidet med informasjonssikkerheit.

## 2.2 Formål

Statens kompetansemiljø for informasjonssikkerheit har som ei av sine hovudoppgåver å samle kunnskapsgrunnlag for å vurdere tilstand og trendar innan informasjonssikkerheit i offentleg sektor. Dette kunnskapsgrunnlaget tek utgangspunkt i ei undersøking frå 2018 knytt til informasjonssikkerheitsarbeidet i statsforvaltninga. Behovet for nytt kunnskapsgrunnlag er gjort tydeleg i Digdir sitt tildelingsbrev for 2023, der målet er at kunnskap produsert av Digdir skal ha høg fagleg kvalitet, vere lett tilgjengeleg, oppdatert, kjent og nytta. Digdir rapporterer på effektmålet "Status for informasjonssikkerheten i forvaltningen", som legg premissar for offentleg sektor sitt arbeid med førebyggande informasjonssikkerheit.

## 2.3 Situasjonsbiletet – frå 2018 til 2024

Omgjevnadane påverkar korleis ein arbeider med informasjonssikkerheit i statsforvaltninga, og denne dynamikken påverkar også svara frå respondentane og vår analyse av informasjonen. Derfor er det avgjerande å sjå på korleis situasjonsbiletet har endra seg frå 2018 til 2024, og kva påverknad dette kan ha for arbeidet med informasjonssikkerheit.

Frå 2018 til 2024 har trussel- og risikobiletet for Noreg vorte meir komplekst og dynamisk. Offentlege trussel- og risikovurderingar, som Risiko 2024 (NSM) og Fokus 2024 (Etterretningstenesta), skildrar eit meir skjerpa sikkerheitspolitisk bilete for Noreg. Det skjer som ei følge av krigen i Ukraina og eit meir anstrengt forhold mellom stormaktene. I Nasjonalt digitalt risikobilete 2023 beskriv Nasjonalt tryggingsorgan (NSM) korleis den teknologiske utviklinga påverkar utfordringsbiletet. Eit digitalisert samfunn aukar sårbarheita når hendingar inntreffer og konsekvensane vert større. Å ivareta sikkerheit og beredskap i digitaliseringa av Noreg er derfor ein føresetnad for at enkeltverksemder, sektorar og landet som heilskap skal kunne levere dei tenestene og oppgåvene som er forventa. Den nye sikkerheitspolitiske situasjonen krev at norske verksemder har god styring og kontroll på informasjonssikkerheitsområdet.

Norske verksemder opplever i dag ei rekke utfordringar for å få til tilstrekkeleg systematisk og kostnadseffektivt arbeid med sikkerheit. God informasjonssikkerheit er ein føresetnad for god verksemdsstyring og vellykka digitalisering. Ei offentleg verksemd arbeider med informasjonssikkerheit for å utføre oppgåvene sine og levere sine tenester på ein god måte – for å nå måla sine og ivareta lovpålagde forpliktingar. Sikkerheitsbrot kan få konsekvensar for verksemder sine leveransar, økonomi og evne til å utføre oppgåver og yte tenester. Slike sikkerheitsbrot kan også få følger for innbyggarar og tilsette, andre verksemder og samfunnsfunksjonar. Som til dømes offentlege digitale fellesløysingar eller nasjonale sikkerheitsinteresser.

I rapporten *Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor* fann Riksrevisjonen at mangelfull og fragmentert regulering, saman med tilrådingar og rettleiingar som ikkje er samordna, bidreg til at brukare opplever dagens arbeid med informasjonssikkerheit i forvaltninga som utfordrande.

Endringane i trusselbiletet og funna frå denne undersøkinga, viser behovet for å forsterke arbeidet med informasjonssikkerheit dei kommande åra, om vi skal klare å møte måla satt i Digitaliseringsstrategien.

# 3 Metode og gjennomføring

I denne delen vil vi kort greie ut om val av metode, utvalet av verksemder og dei ulike vurderingstema som undersøkinga tek for seg. Vi forklarar også sentrale omgrep som er brukt i rapporten og deira tyding i denne samanheng.

## 3.1 Om datainnsamling og val av metode

Undersøkinga er gjennomført ved bruk av spørjeundersøkingar og intervju. Kombinasjonen av kvantitativ og kvalitativ informasjonsinnhenting er lik den som vart nytta i Digdir si undersøking "Arbeidet med informasjonssikkerhet i statsforvaltningen" i 2018. Spørjeundersøkingane gir brei informasjon frå mange verksemder, mens intervjua gir djupare forståing av arbeidet med informasjonssikkerheit i nokre utvalde verksemder. Kombinasjonen av desse metodane gir eit oppdatert bilete av arbeidet med informasjonssikkerheit i statsforvaltninga, samtidig som det tek vare på moglegheita til å sjå utviklingstrekk frå undersøkinga i 2018.

### 3.1.1 Utval

Dei same verksemdene som vart nytta for undersøkinga i 2018 er nytta igjen. Årsaka er at denne rapporten bygger på tidlegare arbeid frå 2018 og ser på utviklinga sidan den gong. Det er gjort eit utval på 91 statlege verksemder frå teknisk og operativt nivå. Undersøkinga er anonym, og Digdir kan derfor ikkje samanlikne svara frå dei same verksemdene.

Hovuddelen av undersøkinga består av ei spørjeundersøking. Fagansvarleg for informasjonssikkerheit, eller tilsvarande rolle i verksemda (t.d. informasjonssikkerheitsleiar eller CISO) skulle svare på spørjeundersøkinga. Sjølv om andre også kan ha svart på spørjeundersøkinga, er dette ikkje eit problem så lenge dei har god kunnskap om informasjonssikkerheitsarbeidet i verksemda. Vi har også ønske om å forstå korleis arbeidet med informasjonssikkerheit vert utført på leiarnivå, derfor vart spørsmål om dette inkludert. Svara her må sjåast i samanheng med at svara kjem frå fagpersonane og ikkje leiinga sjølv.

### 3.1.2 Endringar frå undersøkinga gjennomført i 2018

Spørjeundersøkinga er nedskalert frå 2018. I 2018 vart det sendt ut to spørjeundersøkingar med fleire spørsmål, retta mot både verksemdsleiar og fagansvarleg informasjonssikkerheit.

Vi har valt å nedskalere omfanget på spørjeundersøkinga for å oppnå høgare svarprosent. Vi har stilt færre spørsmål og omformulert eller slått saman nokre av spørsmåla. Vi har fjerna ein del av fritekstfelta som følgde nokre av spørsmåla i 2018. Dette vert omtalt vidare i teksten under. Spørjeskjema som vart sendt ut kan du sjå her: Vedlegg | Digdir.

Denne rapporten kan du lese utan å ha lese rapporten frå 2018.

### 3.1.3 Spørjeundersøking

Verksemdene fekk tilsendt ei spørjeundersøking via Google Forms. Skjemaet inneheldt 26 spørsmål og eit fritekstfelt. Spørjeundersøkinga hadde ei estimert svartid på seks minutt.

Dei fleste spørsmåla som er nytta i spørjeundersøkinga har vorte svart på ved å nytta ein Likert-skala. Skalaen inneber at respondentane oppgir i kva grad påstanden/spørsmålet er gjeldande for verksemda. Vi valde å forme spørsmåla på denne måten fordi det er likt dei opphavlege spørsmåla frå

2018. Dessutan gir det eit enkelt grunnlag for å presentere resultata samla for dei inkluderte verksemdene.

Svarprosenten i spørjeundersøkinga var på ca. 77 prosent. Fordelinga etter storleiken på verksemdene står i tabellen under:

| Tilsette | 1-99 | 100-499 | 500-999 | 1000 og fleire |
|---|---|---|---|---|
| svar | 6 | 34 | 14 | 16 |

#### 3.1.4 Intervju

I spørjeundersøkinga vart respondentane spurde om dei ville delta på intervju for å utdjupe sikkerheitsarbeidet i verksemda deira. Det vart gjennomført 18 digitale intervju, som svarer til 25,7 prosent av respondentane. Intervjua var semistrukturelle for å få eit større innblikk i organiseringa for verksemdene, kommunikasjon, prioritering hos leiinga, handtering av hendingar, vurderingar og tiltak, avvik, og dessutan øvings- og beredskapsplanar. Respondentane kjende seg ofte tryggare på å dele sensitiv informasjon gjennom samtale enn via ei nettbasert spørjeundersøking. Dette var spesielt viktig for verksemder med kritiske samfunnsfunksjonar.

### 3.2 Vurderingstema

Rapporten er delt inn i fire område. Områda som er vektlagde er sentrale i arbeidet med informasjonssikkerheit i alle verksemder.

Rapporten består av følgande tema:

- Styring av informasjonssikkerheit
- Risikostyring
- Øvingar og handtering av hendingar
- Kultur og kompetanse

Vi har teke utgangspunkt i dei elleve indikatorane som vart nytta i Difi-undersøkinga frå 2018 i vedlegg 1. For å redusere omfanget har vi denne gongen ikkje henta informasjon frå etatsstyrarar og verksemdsleiarar.

### 3.3 Omgrepsskildringar

Denne rapporten viser til Digdir si eiga omgrepsskildring, sjå Begrepsliste | Digdir.

#### 3.3.1 Informasjonssikkerheit

Arbeidet med informasjonssikkerheit i ei verksemd handlar om å styre risiko i bruk av informasjonssystem til å utføre oppgåver og levere tenester. Det handlar om å sikre all informasjonsbehandling som inngår i oppgåver og tenester, eller støttar opp under dei.

Det betyr å sikre at informasjon i alle former

- ikkje vert kjend for uvedkomande (konfidensialitet)
- ikkje vert endra utilsikta eller av uvedkomande (integritet)
- er tilgjengeleg ved behov (tilgjengelegheit)

Det handlar om å sikre informasjonssystema som vert nytta – inkludert alle IKT-system, IKT-tenester og IKT-komponentar som inngår i informasjonssystema.

### 3.3.2 Styring og kontroll

Med styring og kontroll meiner vi dei sentrale aktivitetane som normalt inngår i styring og kontroll på informasjonssikkerheitsområdet. Vi nyttar det synonymt med styringssystem, leiingssystem eller internkontroll. Jamfør ISO/IEC 27001:2022 kapittel fire til ti, og aktivitetane som er beskrivne i Digdir si rettleiing «Internkontroll i praksis – informasjonssikkerheit».

I denne rapporten har vi valt å bruke omgrepet styring og kontroll (internkontroll) av informasjonssikkerheit.

### 3.3.3 Sikkerheitstiltak

Med sikkerheitstiltak meiner vi varige tiltak som reduserer risiko, slik at verksemda kan utføre oppgåvene sine og levere tenester på ein god måte. Sikkerheitstiltaka vert etablert for å ivareta konfidensialitet, integritet eller tilgjengelegheit i informasjonsbehandlinga. Tiltaka vert valt og etablert ved bruk av aktivitetane og ved å vurdere og handtere risiko.

### 3.3.4 Statleg verksemd

I denne rapporten er ei verksemd avgrensa til statlege verksemder, i tråd med definisjonen i økonomiregelverket.

Ei verksemd er ei organisatorisk eining i statsforvaltninga som har eit sjølvstendig ansvar for å vareta informasjonssikkerheita knytt til deira oppgåver og tenester. Dei underliggande verksemdene i statsforvaltninga vert kalla forvaltningsorgan, og nokon har større grad av fridom enn andre i form av faglege og budsjettmessige fullmakter.

### 3.3.5 Fagansvarleg informasjonssikkerheit

Vi brukar omgrepet fagansvarleg informasjonssikkerheit for å skildre rolla som har hovudansvar for å vere pådrivar og støtte til leiinga og organisasjonen elles i informasjonssikkerheitsarbeidet. Fagansvarleg informasjonssikkerheit er ofte det same som informasjonssikkerheitsansvarleg, informasjonssikkerheitsleiar eller Chief Information Security Officer (CISO).

# 4. Analyse av dei enkelte vurderingstema

Analysen er delt opp i fire område som er sentrale i arbeidet med informasjonssikkerheit. Kvart område er delt inn i skildring av vurderingstema, observasjonar, og vurderingar av utvikling frå 2018.

I «utvikling frå 2018» har vi berre samanlikna svara frå fagansvarleg informasjonssikkerheit (ikkje verksemdsleiar og etatsstyrar).

## 4.1 Styring av informasjonssikkerheit

Leiar av ei offentleg verksemd har ansvaret for å styre verksemda. Dette inkluderer å styre risiko knytt til oppgåvene og tenestene i verksemda. Arbeidet med informasjonssikkerheit er ein del av dette.
Vi har sett på følgande faktorar når vi har vurdert korleis verksemdene arbeider med styring og kontroll:

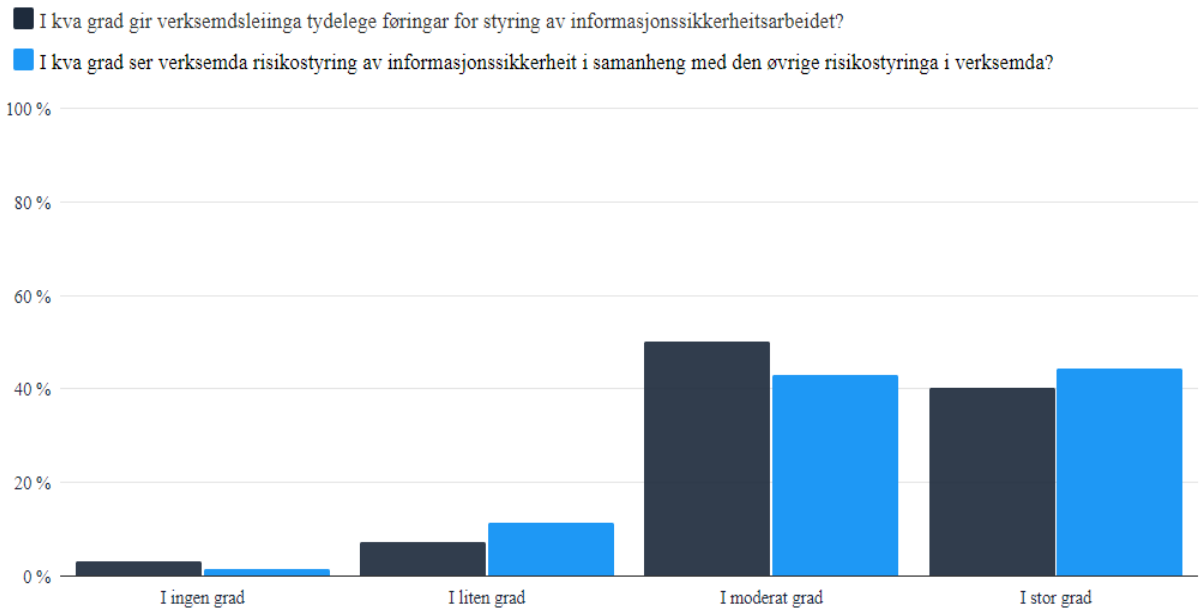
- **Leiinga si styring og oppfølging** (forankring i leiinga/ «tonen på toppen»). Kva føringar har leiinga gitt? Kva roller er definerte?
- **Heilskapleg styring og kontroll.** Jobbar verksemda heilskapleg med informasjonssikkerheit? Er informasjonssikkerheit ein del av styringa av verksemda?
- **Organisering.** Korleis er arbeidet med informasjonssikkerheit organisert i verksemda? Følger dette arbeidet linja, og er det etablert nødvendige støttefunksjonar? Er roller og ansvar tydelege?
- **Oppfølging og kontinuerleg forbetring**. Følger leiinga opp arbeidet med revisjonar og evalueringar? Vert det lagt til rette for forbetringar? Og vedtek leiinga endringar på dei områda der vurderingar viser det er nødvendig?

### 4.1.1 Skildring

Formålet med informasjonssikkerheit, og tilhøyrande styring og kontroll, er å medverke til at informasjonsbehandlinga i verksemda på ein best mogleg måte realiserer det samla målet for verksemda, er kostnadseffektiv og er i samsvar med lover og reglar. I praksis betyr det at internkontrollen bør sjåast i samanheng med den generelle styringa av verksemda. Digdir er utpeika til å gi tilrådingar på området jamfør Digitaliseringsrundskrivet 1.4. I Referansekatalogen tilrår vi å basere seg på ISO/IEC 27001:2022 og Digdir sitt rettleiingsmateriell «Internkontroll i praksis – informasjonssikkerheit».

Spørsmåla som har vorte analysert i denne delen er spørsmål 4, 6, 7, 9, 11 og 12 (sjå vedlegg 1).

### 4.1.2 Observasjonar




*Figur 1*

**Leiinga si styring og oppfølging – «tonen på toppen»**

- 90 prosent svarer at dei har tydelege føringar for styring av informasjonssikkerheitsarbeidet (i moderat eller stor grad). 40 prosent av respondentane svarer i stor grad, 50 prosent i moderat grad, og 10 prosent i liten eller ingen grad.
- I intervjua kjem det også fram at verksemdene i stor grad har føringar frå leiinga. Fleire av desse respondentane opplever at leiinga er medviten om informasjonssikkerheit og at dei prioriterer området. Eit fåtal oppgir å ikkje ha nokon tydelege føringar.

**Heilskapleg styring og kontroll**

- I spørjeundersøkinga svarer 44,3 prosent at dei i stor grad ser risikostyring av informasjonssikkerheit i samanheng med resten av risikostyringa i verksemda. 42,9 prosent svarer i moderat grad, og 12,8 prosent svarer i liten eller ingen grad.
- Intervjua viser at fleire verksemder har gjort større omorganiseringar for å slå saman fagmiljø. Dette har ført til meir heilskapleg risikostyring og positiv effekt på styringa av informasjonssikkerheit.

**Organisering**

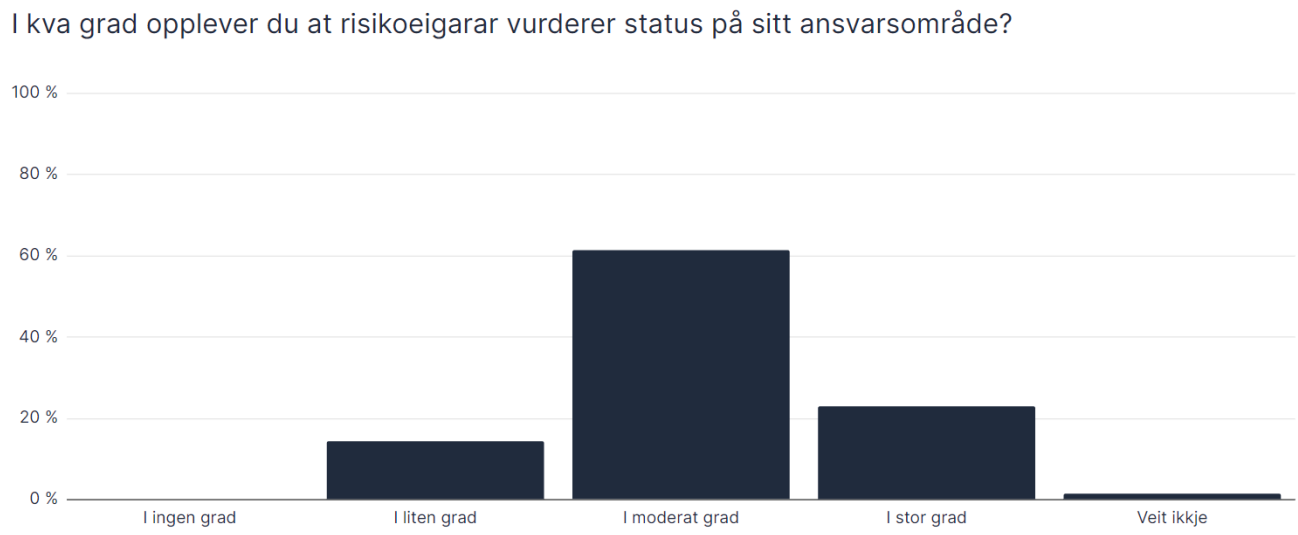
Ansvaret for informasjonssikkerheit og tilhøyrande internkontrollarbeid bør som hovudregel følge linja. For å støtte opp under leiarar på ulike nivå, må verksemda etablere nødvendige støttefunksjonar. Saman med linja utgjer dette sikkerheitsorganisasjonen i verksemda. Roller, ansvar og oppgåver må vere tydelege.

Vi har følgande observasjonar om organiseringa av arbeidet med informasjonssikkerheit:

- I spørjeundersøkinga har respondentane angitt kor mange personar i verksemda som arbeider med fagområdet informasjonssikkerheit. Talet respondentane har oppgitt varierer mellom 0 til 65 personar.

- I intervjua kjem det fram at fleire verksemder manglar ressursar og kompetanse. Fleire fagansvarlege for informasjonssikkerheit sit på dobbeltroller, eller har ei redusert stilling innan andre ansvarsområde i tillegg til rolla som fagansvarleg informasjonssikkerheit. Til dømes IT-sjef eller personvernombod. Nokon meiner at det kan vere konfliktfylt å ha fleire roller på same tid. Dei har erfart at det er nyttig å ha ein dedikert fagansvarleg informasjonssikkerheit/CISO som kan overvake og gi råd på eit overordna nivå. Dobbeltroller kan skape konflikt dersom ein ikkje er klar over rollene.
- I SSB si undersøking «Digitalisering og IKT i offentleg sektor» (2024) svarer 92,8 prosent av statlege verksemder at dei formelt har peika ut ein person som ansvarleg for informasjonssikkerheita.

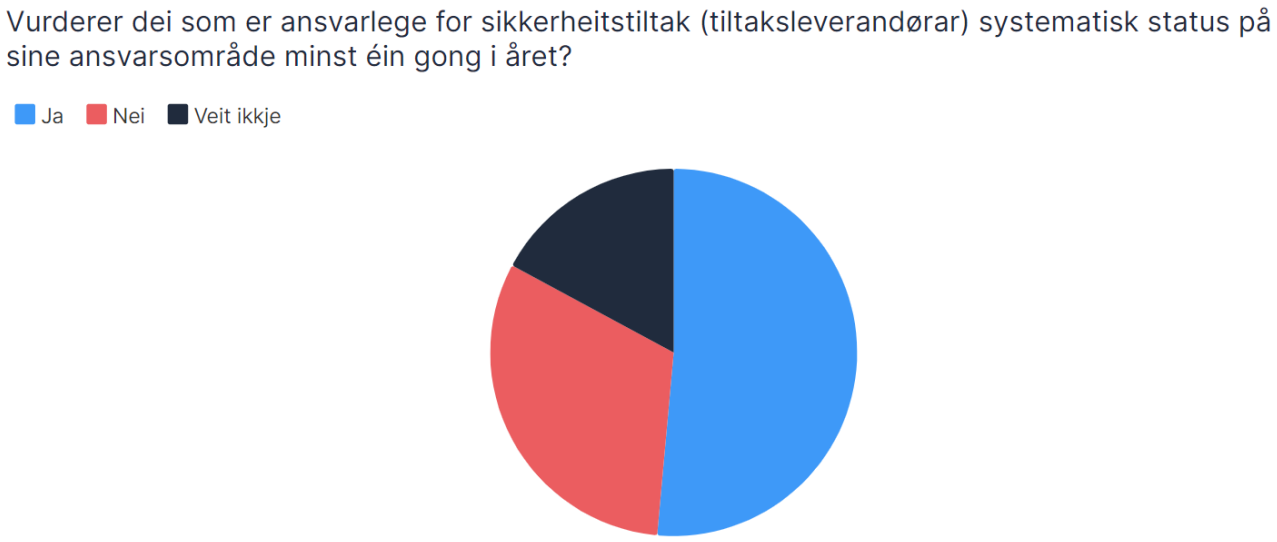
**Oppfølging og kontinuerleg forbetring**




*Figur 2*

Sentrale aspekt ved styring og kontroll er å legge til rette for å kunne forbetre, følge opp arbeid og gjere nødvendige endringar. Å handtere hendingar og gjere evalueringar og revisjonar er viktige delar i dette.

- 22,9 prosent av respondentane opplever at risikoeigarar (dei som har ansvaret for mål og resultat i verksemda) i stor grad systematisk vurderer status på ansvarsområdet sitt. Dette betyr at risikoeigarane gjer ei sjølvstendig vurdering av om internkontrollaktivitetane dei har ansvaret for vert utført forsvarleg, og at tilsette etterlever dei gjeldande retningslinjene. Vidare svarer 61,4 prosent av respondentane at dei gjer dette i moderat grad, mens 14,3 prosent gjer det i liten grad.
- Tilsvarande svarer 51,4 prosent av respondentane at dei som er ansvarlege for sikkerheitstiltak (tiltaksleverandørar) vurderer systematisk status på ansvarsområda sine minst ein gong i året. 17,1 prosent svarer «veit ikkje», og 31,4 prosent svarer «nei».
- Intervjua viser også at det er utfordrande for risikoeigar og tiltaksleverandør å få god nok oversikt, og analysere status på ansvarsområdet sitt.




*Figur 3*

### 4.1.3 Vurderingar

Det er positivt at 90 prosent av verksemdene sine fagansvarlege svarer at dei har tydelege føringar (i moderat eller stor grad). Men det å ha føringar betyr ikkje nødvendigvis at verksemdene er tilstrekkeleg moden. Intervjua viser likevel at dei fleste oppgir at informasjonssikkerheit har auka fokus og bevisstheit i leiinga, og at rollar og ansvar er beskrivne. Dei peiker likevel på fleire utfordingar. Til dømes med organisering og manglande dedikerte ressursar.

> «Vi opplever at verksemda jobbar kontinuerleg med å forbetre arbeidet med informasjonssikkerheit, og det er eit område som blir tatt alvorleg av leiinga.»
>
> *Sitat frå intervju med respondent*

Det er positivt at 87,4 prosent ser risikostyring av informasjonssikkerheit i samanheng med anna risikostyring. Samtidig er det urovekkande at heile 12,8 prosent i ingen eller liten grad gjer dette. Intervjua viser at sjølv om mange opplever ei auka forståing for å sjå informasjonssikkerheit i samanheng med andre ansvarsområde, er dette krevjande i praksis. Nokre av observasjonane i undersøkinga kan seie noko om årsakene til dette; utfordringar med organisering av sikkerheitsarbeidet, kompetanse- og ressursmangel.

> «For ein liten organisasjon med ei relativt lita gruppe som jobbar med informasjonssikkerheit, ser ein det som utfordrande at ting skjer raskt og at det er relativt kostbart å halde seg oppdatert. Vi har til tider problem med å halde kompetansen oppdatert.»
>
> *Sitat frå intervju med respondent*

Vi ser at mange verksemder har plassert ansvaret som fagansvarleg informasjonssikkerheit saman med andre roller. Dette kan føre til at rolla vert utvatna, og moglege rollekonflikter i arbeidet med informasjonssikkerheit. Det er viktig at fagansvarleg informasjonssikkerheit har ei overordna og fagleg rådgivande rolle for heile organisasjonen, og kan rapportere direkte til toppleiinga utan mellomledd. I tillegg påpeika respondentane at det er positivt at verksemder kunngjer rolla som fagansvarleg informasjonssikkerheit/Chief Information Security Officer (CISO) som «verksemdskritisk», då dette gjer det tydeleg kva rolla inneber.

Når ein skal forbetre arbeidet med informasjonssikkerheit kontinuerleg er det utfordrande for risikoeigar og tiltaksleverandør å ha oversikt. Inkludert å analysere status på ansvarsområdet sitt minst éin gong årleg. Heile 49 prosent har svart «nei» eller «veit ikkje» på spørsmålet om tiltaksleverandørar vurderer status på sine ansvarsområde minst éin gong i året. Det vil seie at halvparten av verksemdene ikkje undersøker om etablerte sikkerheitstiltak er formålstenlege, eller om ein må endre sikkerheitstiltak. Det er også urovekkande at 17 prosent har svart «veit ikkje», og at fagansvarlege ikkje sit på denne oversikta. Europeiske regelverk som NIS2 og GDPR set krav til å forvalte sikkerheitstiltak, og å kontinuerleg evaluere desse.[3] Dette inneber å sette i verk sikkerheitstiltak som er tilpassa risiko, og å vurdere effekten av desse tiltaka. Ein treng tilstrekkeleg fagkunnskap for å velje, etablere, oppretthalde og forvalte gode sikkerheitstiltak – og dessutan fase ut tiltak som ikkje lenger er formålstenlege.

#### 4.1.4 Utvikling sidan 2018

I år oppgir færre respondentar at dei i stor grad har tydelege føringar for styring av arbeidet sitt. Samtidig er det fleire som seier dei har det i moderat grad. Dette kan indikere at det framleis er eit godt grunnlag for risikobasert styring, i og med at heile 90 prosent i enten moderat eller stor grad har tydelege føringar frå leiinga.

Det kan vere forskjell på korleis leiar av verksemda og fagansvarleg oppfattar kor tydeleg styringa av informasjonssikkerheitsarbeidet er. Vi har ikkje spurt leiarar i denne undersøkinga, derfor er det ukjend om oppfatninga har endra seg. I 2018 meinte 77 prosent av leiarane at dei gav tydelege føringar, mens 51 prosent av dei fagansvarlege var samde i at dei fekk tydelege føringar.

Det er størst behov for å forbetre undertemaet «kontinuerleg forbetring». Det er tydeleg nedgang i mengda som oppgir at tiltaksleverandørar og risikoeigarar analyserer status på ansvarsområdet sitt minst éin gong i året. Tala frå rapporten i år kan derimot hinte om at verksemdene i mindre grad har evne til å systematisk godkjenne og iverksette sikkerheitstiltak.

### 4.2 Risikostyring

#### 4.2.1 Skildring

Risikostyring omfattar to faktorar som kan vere ein del av vurderingstemaet styring og kontroll. Her er risikostyring trekt ut som eit eige vurderingstema fordi det er eit eige fag som også vert brukt på mange andre område, i tillegg til informasjonssikkerheit.

I denne rapporten har vi valt å analysere to faktorar for området risikostyring:

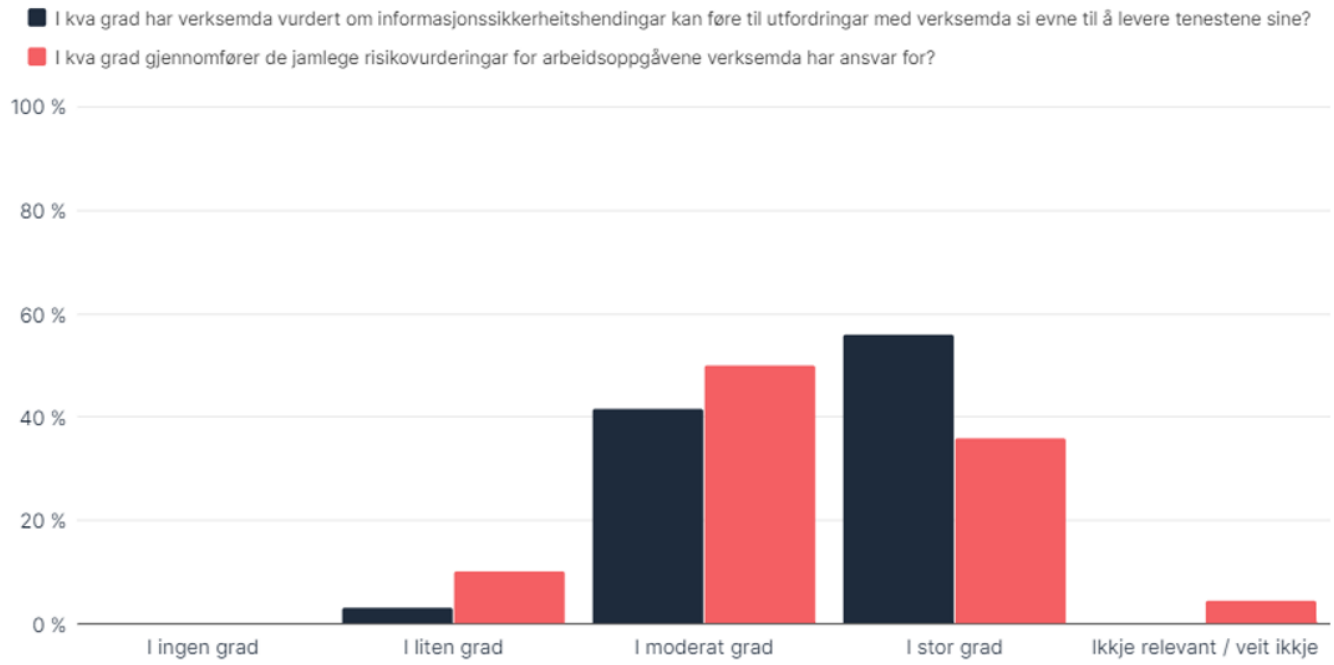
- **Vurdering av risiko** gjeld her korleis verksemdene beskriv og vurderer operativ risiko. Vi har lagt særleg vekt på tilnærminga verksemdene har til å akseptere risiko.
- **Handtering av risiko** er kva verksemdene gjer med kvar identifiserte risiko, kva som vert lagd til grunn for avgjerder om å akseptere ein risiko, og kva tilnærming verksemda har til å etablere og forvalte sikkerheitstiltak for å redusere risiko.

Spørsmåla som er analysert i denne delen er spørsmål 8, 10, 13, 14, 15, 16 og 17 (sjå vedlegg 1).

[3] Se NIS2, Article 21 Cybersecurity risk-management measures, bokstav f. og GDPR Article 32.

### 4.2.2 Observasjonar

**Vurdering av risiko**

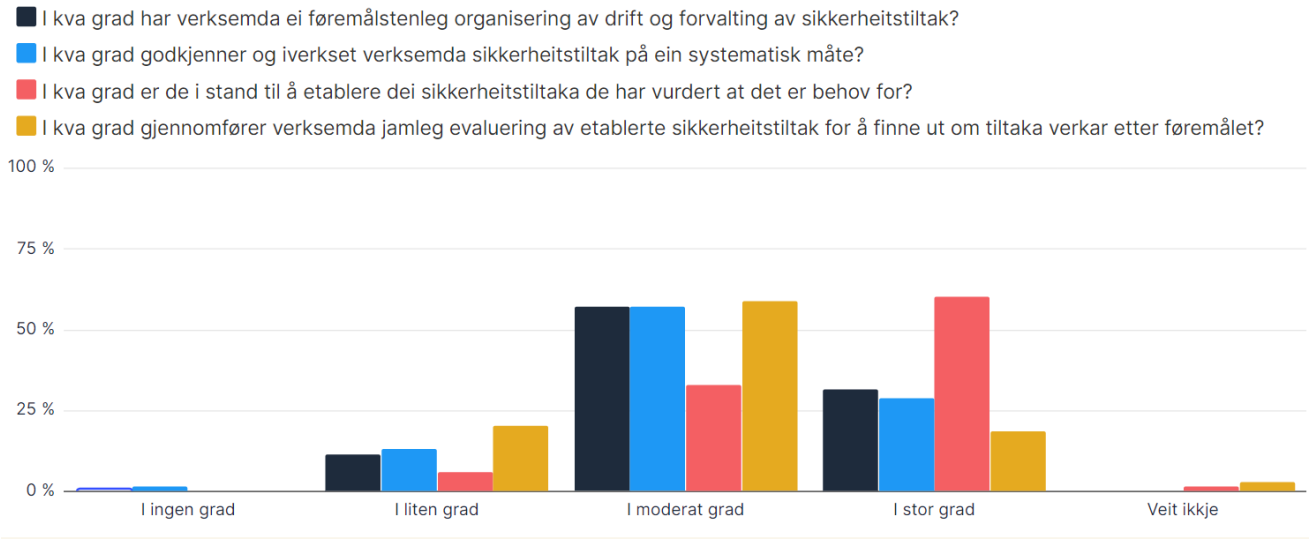



*Figur 4*

- 97,1 prosent har i stor eller moderat grad vurdert om informasjonssikkerheitshendingar kan påverka evna verksemda har til å levere sine tjenester. 44,3 prosent svarer i moderat eller liten grad. I intervjua kjem det fram at fleire av verksemdene ser informasjonssikkerheitsrisiko i samanheng med andre risikoar for verksemda.
- 35,7 prosent svarer at det i stor grad vert gjennomført regelmessige risikovurderingar for arbeidsoppgåvene i verksemda. 50 prosent svarer «i moderat grad», og 10 prosent svarer «i liten grad» på spørsmålet.
- I SSB si undersøking «Digitalisering og IKT i offentleg sektor» (2024) svarer 86,6 prosent av statlege verksemder at risikovurderingar vert gjennomført systematisk og periodisk .
- Desse resultata stemmer overeins med det som kom fram i intervjua, der dei fleste svarte at dei gjennomfører periodiske risikovurderingar på ulike nivå.
- Gjennom intervjua kjem det også fram at det er store variasjonar i korleis verksemdene arbeider med risikovurdering. Det er store forskjellar mellom verksemdene i bruken av tydelege retningslinjer for å akseptere risiko, og metodar for å gjennomføre risikovurderingar.
- Spørjeundersøkinga viser at ansvaret for å vurdere og handtere risiko følger linjeprinsippet i 83 prosent av dei spurde verksemdene. 17,1 prosent oppgir at det formelle ansvaret for avgjerder om informasjonssikkerheitsrisiko vert teke av spesialfunksjonar, slik som fagansvarleg informasjonssikkerheit eller andre.
- Intervjua viser at der er store forskjellar i frekvens på gjennomføringar av risikovurderingar, og på kva nivå dei vert gjennomført. Enkelte verksemder gjennomfører berre overordna vurderingar sentralt, nokon vert gjennomført i tilknyting til prosjekt, mens andre vert gjennomført i linja. Enkelte vurderer risiko på alle nivå.

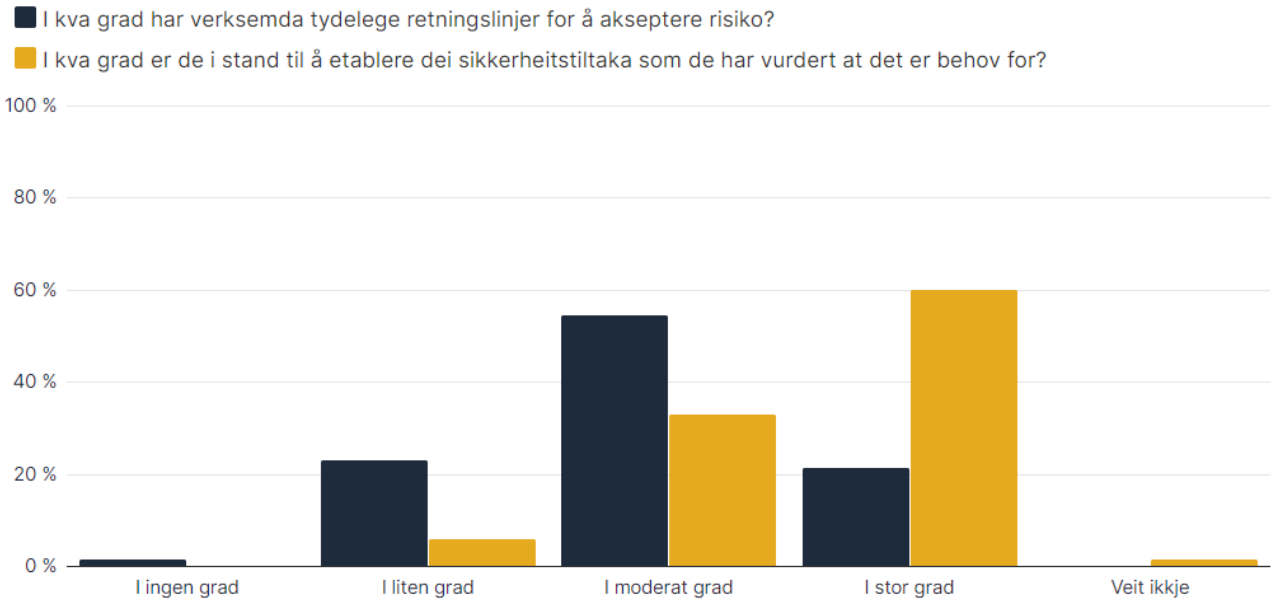
- Eit fåtal av verksemdene som er intervjua påpeikar at det vert gjennomført mange og hyppige risikovurderingar, mens nokon primært gjennomfører risikovurderingar relatert til enkelte eller alle IKT-løysingar eller -prosjekt.
- Dei fleste stiller krav til å vurdere risiko før dei tek i bruk nye IKT-system. Nokon påpeikar at sjølv om det finst slike krav, vert dei sjeldan følgde i praksis. Dette er basert på resultat frå interne spørjeundersøkingar.

**Handtering av risiko**




*Figur 5*

- 31,4 prosent har svart at verksemda i stor grad har ei formålstenleg organisering av drift og forvaltning av sikkerheitstiltak. 11,4 prosent har svart i liten grad.
- 28,6 prosent oppgir at dei i stor grad gjennomfører systematisk godkjenning og iverksetting av sikkerheitstiltak. 57,1 prosent har svart «i moderat grad». Samla sett har 14,3 prosent oppgitt at dei i liten eller ingen grad gjer dette.
- I spørjeundersøkinga oppgir 92,9 prosent at dei i stor eller moderat grad er i stand til å etablere dei sikkerheitstiltaka dei har behov for. Det er derimot 5,7 prosent som har svart at dei i liten grad er i stand til å etablere sikkerheitstiltak dei har behov for. 1,4 prosent har svart at dei ikkje veit om dei er stand til dette.




*Figur 6*

- I spørjeundersøkinga er det 18,6 prosent som oppgir at dei i stor grad regelmessig evaluerer etablerte sikkerheitstiltak. 20 prosent oppgir at dei i liten grad gjer dette. Det er ingen som svarer at dei ikkje gjennomfører evalueringar.
- Berre 21,4 prosent av respondentane oppgir at dei i stor grad har tydelege retningslinjer for å akseptere risiko. 54,3 prosent seier dei i moderat grad har det, mens 24,3 prosent seier dei i liten eller ingen grad har det

### 4.2.3 Vurderingar

Rettleiinga til Digdir slår fast at det som hovudregel ikkje er formålstenleg å gjennomføre grundige risikovurderingar på all informasjonsbehandling og alle informasjonssystem i ei verksemd. Verksemder må ha tilstrekkeleg oversikt over heilskapen og kunne prioritera, og jamleg vurdere kor det er behov for å grundig vurdere risiko. Intervjua viser at risiko i stor grad vert vurdert av risikoeigarar, og at systemeigar i mindre grad gjer det. Dette stemmer overeins med resultata frå undersøkinga som blei lagt fram i førre vurderingstema "Styring av informasjonssikkerheit". Intervjua og kommentarar i fritekstfeltet peiker på at manglande kompetanse og kapasitet har skylda for dette.

Dei statlege verksemdene har likevel eit godt grunnlag for ei risikobasert tilnærming til informasjonssikkerheit, sidan nesten 90 prosent av verksemdene oppgir at det vert utført regelmessige risikovurderingar for arbeidsoppgåvene deira. Vidare har 97,1 prosent i stor eller moderat grad vurdert om informasjonssikkerheitshendingar kan påverke evna verksemda har til å levere tenester. Intervjua viser også at fleire verksemder ser informasjonssikkerheitsrisiko i samanheng med andre typar risikoar for verksemda.

Mange verksemder er i stor grad i stand til å etablere nødvendige sikkerheitstiltak. Resultata kan derimot indikere at dei har utfordringar med å evaluere desse tiltaka effektivt. Dei fleste verksemdene har ei evne til å etablere nødvendige sikkerheitstiltak, men møter på utfordringar med organisering, forvaltning og evaluering av etablerte tiltak. Sjølv om dei fleste verksemdene har ei viss grad av formålstenleg drift og forvaltning av sikkerheitstiltak, rapporterer berre 28,6 prosent at dei i stor grad

har ei systematisk tilnærming til å godkjenne og iverksette nye tiltak. Dette betyr at mens dei fleste verksemder set i verk formålstenlege tiltak og forvaltar dei effektivt, er det ein stor del som manglar ei systematisk tilnærming til risikohandtering. Samla sett tyder det på behov for å gjere evalueringa og implementeringa av sikkerheitstiltak betre, og å sikre heilskapleg og effektiv handtering av risikoen.

> «Vi har gjort mykje arbeid innan dei områda de ønsker å avdekke, men føler likevel at vi har mykje jobb igjen før vi kan seie vi har "god kontroll".»
>
> *Sitat frå intervju med respondent*

Berre 21,4 prosent oppgir at dei i stor grad har tydelege retningslinjer for å akseptere risiko. Utan slike retningslinjer er det vanskeleg å prioritere ressursane mot dei viktigaste risikoane.

#### 4.2.4 Utvikling sidan 2018

Når det gjeld vurdering av risiko, er det noko auke (rundt 7 prosentpoeng) som oppgir at dei i "stor grad" har vurdert om hendingar vil kunne føre til utfordringar.

Når det gjeld handtering av risiko, er det like mange (60 prosent) som i stor grad etablerer dei sikkerheitstiltak dei har behov for. Men i 2024 er det også 7 prosent som har svart “i liten grad” eller “veit ikkje”. I 2018 var det ingen som svarte dette. Samtidig svarte 35 prosent i 2018 at dei i stor grad har tydelege retningslinjer for å akseptere risiko. I 2024 har talet sokke til berre litt over 20. Mens fleire har oppgitt at dei i moderat grad har dette, er det likevel også ein større del som i ingen eller liten grad har tydelege retningslinjer enn det var i 2018.

Færre svarer at dei i liten eller ingen grad evaluerer etablerte sikkerheitstiltak i 2024 enn i 2018. Resultata tilseier at verksemdene hadde noko betre kontroll på systematisk godkjenning og iverksetting av sikkerheitstiltak i 2018 enn i 2024.

Ved å sette tala frå årets spørjeundersøking opp mot tala frå 2018, kan ein oppleve situasjonen i statsforvaltninga som at den ikkje har endra seg noko vesentleg. Det tilseier at arbeidet med å systematisk vurdere og handtere risiko ikkje har utvikla seg mykje i dei statlege verksemdene. Det er færre som oppgir at dei har tydelege retningslinjer for aksept av risiko. Utan tydelege retningslinjer for risikoaksept er det vanskeleg å prioritere ressursbruken mot dei risikoane det er viktig å handtere. Dette er uheldig, og kan føre til svekt styring og kontroll av informasjonssikkerheit i kvar enkelt verksemd.

### 4.3 Øvingar og handtering av hendingar

#### 4.3.1 Skildring

Verksemder bør vere førebudd på at sikkerheitshendingar kan oppstå når som helst. Ei god beredskapsplanlegging er avgjerande for å handtere uønskte hendingar på ein effektiv måte. Utan klare beredskapsplanar som tydeleg definerer ansvarsfordelinga, kan det vere vanskeleg å effektivt koordinere responsen på ei hending.

Å planlegge og gjennomføre øvingar spelar ei vesentleg rolle i å førebu seg på uventa hendingar. Dei mest vellykka verksemdene er dei som trenar på risikoscenario som er identifisert ved å identifisere, vurdere og analysere risiko ein står overfor i si verksemd.[4] Dei tek også ei proaktiv tilnærming til

[4] Jøsang, Audun (2023) s. 308.

øvinga, der dei på førehand har vurdert kva som er nødvendig for ei vellykka gjennomføring av øvinga.

Etter kvar øving bør verksemder evaluere og identifisere område for forbetring. Dette kontinuerlege arbeidet vil bidra til at verksemda vert betre rusta til å handtere framtidige hendingar på ein effektiv og sikker måte. For anbefalingar og råd for gjennomføring av øvingar finst det fleire aktørar som rettleier på dette området. Hos ovelse.no får ein tilgang til diskusjonsøvingar, mens Direktoratet for samfunnssikkerhet og beredskap (DSB) rettleier for fleire type øvingar, og sektorspesifikk rettleiing.

Spørsmåla som er analysert i denne delen er spørsmål 18, 19, 20 og 21 (sjå vedlegg 1).

### 4.3.2 Observasjonar

- I spørjeundersøkinga oppgir 75,7 prosent av verksemdene at dei gjennomfører minst ei øving årleg på informasjonssikkerheitsområdet. 21,4 prosent har svart at dei ikkje øver årleg. 2,9 prosent veit ikkje. I spørjeundersøkinga svarer 41,4 prosent at dei i moderat grad arbeider systematisk med øvingar. Følgt av 35,7 prosent av verksemdene som svarer i stor grad. Vidare svarer 21,4 prosent at dei i liten grad arbeider systematisk med øvingar.
- I spørjeundersøkinga stilte vi eit fleirvalspørsmål om kva verksemdene baserer handtering av informasjonssikkerheitshendingar på. Prosentdelen differerer frå figur 6 på grunn av omrekningar gjort for ei betre grafisk framstilling.
  Her svarer verksemdene:
  - Vi har definerte roller og ansvar: 88,6 prosent
  - Vi har ein eigen funksjon for å koordinere handteringa av informasjonssikkerheitshendingar (eks: Security Incident Response Team): 78,6 prosent
  - Vi har oversikt over behov for kompetanse hos alle som er involverte i varsling, deteksjon og handtering av hendingar: 32,9 prosent
  - Vi har definerte prosedyrar for å handtere hendingar: 75,7 prosent
  - Vi har rutinar for å rapportere avvik: 87,1 prosent
  - Anna: 7,1 prosent
- 46 prosent har i liten eller ingen grad oversikt over kostnadene som følger av informasjonssikkerheitshendingar. Dette inneber at respondentane har avgrensa innsikt i kostnadene knytt til hendingar. Ein mindre del, 10 prosent, oppgir å ha stor grad av oversikt, mens 35,7 prosent oppgir å ha moderat grad av oversikt. 7,1 prosent veit ikkje.
- Frå intervjua fortalde fleire respondentar at medieomtale av hendingar som har funne stad hos andre eller eiga verksemd har bidrege til auka fokus på øvingar.
- Frå intervjua fortalde respondentane at ein endra sikkerheitspolitisk situasjon for Noreg har bidrege til at verksemdene prioriterer arbeidet med øvingar og handtering av hendingar.

### 4.3.3 Vurderingar

Hovudinntrykket frå spørjeundersøkinga er at verksemdene i stor eller moderat grad jobbar systematisk med øvingar. Eit fleirtal av verksemdene oppgir å øve minst ein gong årleg. Dette er ein auke frå 2018, då under halvparten av respondentane svarte dei øvde årleg. Svara frå spørjeundersøkinga indikerer at verksemder jobbar meir systematisk med øvingar og øver oftare enn før.

> «Erfaringane blir brukt i årshjulet for informasjonssikkerheit, og blir tatt med i neste års arbeid.»
> *Sitat frå intervju med respondent*

Sjølv om fleire oppgir i spørjeundersøkinga at dei øver årleg, så kan intervjua indikera at det ikkje er tilstrekkeleg systematikk i arbeidet. I intervjua fortalde fleire verksemder om manglande beredskapsplanar, øvingsplanar, evaluering etter hendingar og at det var eit stort forbetringspotensial. Respondentane peikar på at det er eit «etterslep» etter pandemien, der ein ikkje har komme i gang, eller ikkje har tilstrekkeleg med data frå dei siste åra å bygge på. Nokre verksemder oppgir at berre delar av organisasjonen jobbar systematisk med øvingar. Dei delane av verksemdene som jobbar meir systematisk med øvingar er vanlegvis dei som har dedikerte ressursar til arbeidet med sikkerheit på ulike nivå, både strategisk og operativt.

Svara frå spørjeundersøkinga gir ein indikasjon på at verksemdene i norsk statsforvaltning har liten oversikt over kostnadene som kan følge av informasjonssikkerheitshendingar. Kostnadene knytt til informasjonssikkerheitshendingar kan vere store, men variere i omfang og etter type hending. Det kan vere vanskeleg for verksemder å berekne omfanget av slike hendingar. Respondentar som fortel å ha opplevd hendingar i eiga verksemd, oppgir at dette har ført til at øvingar i ettertid er sett meir på dagsordenen. Verksemdene oppgir at medieomtale etter ei slik hending også fører til auka fokus frå leiinga.

Oppfatninga er likevel at norske verksemder har ei god forståing for kor viktig arbeid med øvingar er. Informasjonssikkerheitsbrot og -hendingar som har ført til negativ omtale, og dessutan krigen i Ukraina og ein ny sikkerheitspolitisk situasjon, kan ha bidratt til dette.

#### 4.3.4 Utvikling sidan 2018

Undersøkinga frå 2018 viste at verksemder øver for lite, då under halvparten hadde årlege øvingar. Det vart trekt fram som positivt at 87 prosent likevel hadde handtert hendingar basert på tydelege definerte roller, ansvar og prosedyrar.

Samanlikna med undersøkinga frå 2018 er det ein auke av verksemder som oppgir at dei jobbar systematisk med øvingar. I 2018 svara 18 prosent at verksemda i stor grad jobbar systematisk med øvingar innan informasjonssikkerheit. Dette vil seie at det har vore ein auke med over 17 prosentpoeng, som seier oss at dette har fått auka prioritering.

Det er særleg bra at vi ser at ei større grad av verksemder øver årleg. I spørjeundersøkinga oppgir 75,7 prosent av verksemdene at dei gjennomfører minst ei øving årleg på informasjonssikkerheitsområdet. Dette er ein auke frå 45 prosent i 2018.

### 4.4 Kultur og kompetanse

#### 4.4.1 Skildring

Sikkerheitskultur handlar om dei felles haldningane, åtferda og verdiane for verksemda knytt til informasjonsressursane for verksemda. Å ha god sikkerheitskultur inneber å fremme forståing for risiko, oppmuntra til å etterleve retningslinjer og prosessar for sikkerheit. Og generelt vareta eit miljø der verksemda prioriterer sikkerheit på alle nivå.

For å bygge ei robust informasjonssikkerheit og oppretthalde ein god sikkerheitskultur i ei verksemd, er kompetanse ein nøkkelkomponent. Formålstenleg sikkerheitskompetanse og nødvendig opplæring bidreg til at tilsette kan utføre dei daglege oppgåvene på ein sikker måte. Tilsette treng tilstrekkeleg kompetanse for å forstå og identifisere risiko, handtere sikkerheitstruslar og sårbarheiter i verksemda. Kompetanse er også viktig for å forstå den rolla tilsette har i å oppretthalde sikkerheita og ta nødvendige forholdsreglar.

Spørsmåla som er analysert i denne delen er spørsmål 22, 23 og 24 (sjå vedlegg 1).

### 4.4.2 Observasjonar


*Figur 7*

- I spørjeundersøkinga oppgir 54,5 prosent at dei i stor grad opplever at informasjonssikkerheitsarbeidet har fokus og prioritet hos leiinga, mens 44,3 prosent svarer at informasjonssikkerheit i moderat grad har fokus og prioritet. 1,4 prosent av deltakarane svarer at informasjonssikkerheit i lita grad har fokus og prioritet hos leiinga.
- Omtrent ein tredel av intervjuobjekta påpeikar eit godt fokus i leiinga når det gjeld informasjonssikkerheit. Fleire av objekta snakkar om auka prioritet, og at leiinga er på rett veg.
- Fleire av dei intervjua verksemdene uttrykkjer seg også om at sikkerheitskulturen vert rekna som å vere god, og at kulturen utviklar seg i positiv retning. Fleire presiserer likevel at sikkerheitskulturen har rom for forbetring. Nokre få verksemder rapporterer om manglande sikkerheitsskultur.
- I spørjeundersøkinga oppgir 24,3 prosent at dei enten i ingen grad eller i liten grad kartlegg verksemda sitt behov for kompetanseheving på informasjonssikkerheitsområdet. 61,4 prosent av verksemdene svarer at dei i moderat grad kartlegg behova, mens 14,3 prosent svarer at dei i stor grad kartlegg kompetansehevingsbehovet.
- I Intervjua kjem det fram frå fleire av objekta at det manglar noko kartlegging av kompetansebehov. Fleire av verksemdene har tilsette med eit sprikande behov for kompetanseheving og det kan vere utfordrande å sette i verk nødvendig sikkerheitssopplæring.
- I spørjeundersøkinga oppgir 70 prosent av deltakarane at det har vorte gjennomført tiltak for å styrke informasjonssikkerheitskulturen i verksemda for alle tilsette. 32,9 prosent av deltakarane har kryssa av at det har vorte gjennomført tiltak blant grupper av tilsette, mens 40 prosent av deltakarane svarer at tiltak har vorte gjennomført for leiargruppa. 12,9 prosent svarer at det ikkje er gjennomført tiltak for å styrke kulturen i verksemda.

- I intervjua kjem det fram at dei fleste verksemdene set i verk tiltak for å betre sikkerheitsskulturen. Men det kjem også fram at det er nokre manglar i kompetanseheving blant nyare tilsette, og at dei har ei kjensle av å vere på etterskot med tanke på utviklinga av sikkerheitssituasjonen.
- I SSB si undersøking "Digitalisering og IKT i offentleg sektor" (2024) svarer 90,4 prosent av statlege verksemder at aktivitetar for opplæring og bevisstgjering av tilsette og leiarar vert gjennomført minst éin gong per år.

### 4.4.3 Vurderingar

Det kan vere vanskeleg å seie noko konkret om sikkerheitskulturen og -kompetansen i ei verksemd. Verksemder kan i praksis ha nokre gode og nokre dårlege element i sikkerheitskultur på ei og same tid. Samtidig kan dei stille ulike krav til kultur og kompetanse basert på oppgåvene for verksemda.

Hovudinntrykket frå resultata frå både spørjeundersøkinga og intervjua er at dei fleste verksemdene kartlegg kompetansebehov og sikkerheitskultur. Majoriteten av respondentane oppgir at dei jobbar med bevisstgjering og opplæring innan informasjonssikkerheitsområdet. Rundt tre firedelar av respondentane i spørjeundersøkinga seier at dei gjennomfører kartlegging av kompetansebehov i moderat eller stor grad. På den andre sida rapporterer omtrent 23 prosent av respondentane om manglande kartlegging av sikkerheitskultur, og fleire meiner det er rom for forbetring på dette området. Samtidig påpeikar fleirtalet av respondentane at sikkerheitskulturen har vorte betre med auka fokus og bevisstgjering, og at utviklinga går i positiv retning.

> «Sjølv om augneblinksbiletet i svara tilseier i "liten" eller "moderat" grad i mange av svara så kjem det ikkje like godt fram at vi er på ei mogningsreise. Vi veit kva medisinen er, men det tar tid å skape forståing for arbeidet og endre på kulturen, både hos leiinga og dei tilsette.»
>
> *Sitat frå intervju med respondent*

Svara frå både spørjeundersøkinga og intervjua indikerer at leiinga har eit høgt fokus på og forståing for informasjonssikkerheit. Samtidig viser svara at det er behov for auka kompetanse på nokre område. Dette gir meining, sidan høgare bevisstgjering og fokus på informasjonssikkerheit vil gjere eventuelle manglar på kompetanse lettare å identifisere.

> «Leiinga er i ferd med å endre haldning til arbeidet med informasjonssikkerheit, og har det siste året gjort mykje for å auke bevisstheita hos leiarar og få informasjonssikkerheit integrert i styringssystemet. Det manglar stadig fokus på kulturbygging og kontinuerleg opplæring av tilsette.»
>
> *Sitat frå intervju med respondent*

Dei fleste verksemdene påpeikar at det vert sett i gang tiltak for å betre sikkerheitskulturen blant alle tilsette. Men nokre verksemder fortel at opplæring og bevisstgjering berre er retta mot enkelte grupper av dei tilsette. I SSB si undersøking frå 2024 svarer i overkant av 90 prosent at aktivitetar for opplæring og bevisstgjering av tilsette og leiarar vert gjennomført minst éin gong per år.[5] Desse resultata viser til eit godt fokus på bevisstgjering og opplæring. Ved å kartlegge eksisterande sikkerheitskultur og -kompetanse får ein eit godt grunnlag for formålstenleg opplæring og bevisstgjering. Ved å kartlegge sikkerheitskulturen kan verksemda identifisere område der det er

[5] SSB, Digitalisering og IKT i offentlig sektor.

behov for forbetring, og enklare vite kva kompetanse som manglar. Verksemda kan deretter implementere tiltak for å styrke sikkerheitskulturen og kompetansen over tid.

### 4.4.4 Utvikling sidan 2018

Svarresultata frå 2024 var svært like resultatet frå 2018. I 2018 svarte 52 prosent at dei i stor grad opplever at informasjonssikkerheitsarbeidet har prioritet hos leiinga, mens i år svarte 54,3 prosent at det i stor grad er prioritet hos leiinga. I 2024 har 1,4 prosent svart at arbeidet i lita grad er prioritert av leiinga. I 2018 var det ingen som svarte dette.

I spørjeundersøkinga frå 2024 svarte 14,3 prosent at dei i stor grad kartlegg behovet for kompetanseheving innan informasjonssikkerheitsområdet, ein liten nedgang frå 17,3 prosent i 2018. Det er ei positiv utvikling i andelen som i liten eller ingen grad kartlegg behov, då den er redusert mykje frå 32 prosent i 2018 til 24,3 prosent i 2024.

I år er det 3 prosentpoeng mindre som svarer at dei i stor grad kartlegg behov for kompetanseheving på informasjonssikkerheitsområdet samanlikna med 2018. Men det er og nesten 8 prosentpoeng færre som seier at det enten i liten eller ingen grad vert kartlagt behov.

Resultata frå årets spørjeundersøking viser ein nedgang av initiativ til å gjennomføre tiltak for å styrke informasjonssikkerheitskulturen i verksemdene, samanlikna med resultata frå 2018. I år har 70 prosent svart at det har vorte teke initiativ mot alle tilsette. 32,9 prosent av verksemdene har svart at initiativ har vorte retta mot grupper av tilsette, mens 40 prosent av verksemdene svarer at initiativ har vorte retta mot leiargruppa. 12,9 prosent av verksemdene svarer at det ikkje er gjennomført tiltak. I 2018 svarte 73,7 prosent av verksemdene at tiltak har vorte gjennomførte mot alle tilsette, 39,5 prosent av verksemdene kryssa av for grupper av tilsette. 44,7 prosent kryssa av for leiargruppa. 7,9 prosent svarte at det ikkje har vorte gjennomført tiltak.

# 5. Referansar

10852: Tiltak/rutiner ved administrasjon av IKT-sikkerheten, etter sysselsettingsgruppe (Statlige virksomheter) 2013 - 2024 10852: Tiltak/rutiner ved administrasjon av IKT-sikkerheten i statlige virksomheter (prosent), etter sysselsettingsgruppe, statistikkvariabel og år. Statistikkbanken (ssb.no)

10855: Tiltak for IKT-sikkerheten (Statlige virksomheter) 2004 - 2021 Digitalisering og IKT i Offentlig sektor

Begrepsliste https://www.digdir.no/informasjonssikkerhet/begrepsliste/3230#informasjonssikkerhet

Cox m.fl. (1995:9)

Datatilsynets kommunetilsyn Funn fra tilsyn i kommuner og fylkeskommuner (2023)

Difi-rapport 2018:4 Arbeidet med informasjonssikkerhet i statsforvaltningen | Digdir

Regjeringen.no, Digitaliseringsrundskrivet - regjeringen.no

Regjeringen.no, Norge får sin første lov om digital sikkerhet - regjeringen.no

Dillman (2000:326)

Jøsang, Audun (2023), «Informasjonssikkerhet: teori og praksis»

Kompetansebeskrivinger Rolle: Fagansvarlig informasjonssikkerhet | Digdir

NSM, Risiko 2018 nsm_risiko_2018_web.pdf

NSM, Risiko 2024 Risiko 2024 - Nasjonal sikkerhetsmyndighet (nsm.no)

# 6. Figurliste