DIGITALISERINGSSTYRELSEN

ISO 27001-modenhed i staten

November 2021

2021

Indhold

1. Indledning

ISO 27001 er en international standard, der fastsætter bedste praksis for styring af informationssikkerhed. Alle statslige myndigheder er pålagt at implementere denne standard. I medfør af den nationale strategi for cyber- og informationssikkerhed fra 2018 blev det besluttet at følge op på myndighedernes ISO 27001-implementering hvert halve år. Det blev samtidig besluttet, at myndigheder, der ikke er i mål med ISO 27001-implementeringen, skal forelægge en handleplan for regeringen med henblik på at sikre fuld implementering.

Nærværende rapport beskriver resultaterne af den seneste måling, der gennemførtes i september 2021. Desuden sammenlignes de seneste resultater med tidligere målinger.

Spørgerammen for ISO 27001-modenhedsmålingen

Til brug for de halvårlige ISO 27001-modenhedsmålinger har Digitaliseringsstyrelsen udarbejdet en spørgeramme. I målingen angiver myndighederne en egenvurdering af deres implementering på en modenhedsskala fra 1 til 5 fordelt på syv væsentlige områder af ISO 27001-standarden:

1. Ledelsessystem for informationssikkerhed
2. Politik for informationssikkerhed
3. Ressourcer, kompetencer og bevidsthed
4. Leverandørstyring
5. Risikostyring
6. Måling, audit og evaluering
7. Beredskabsplaner

Der er i målingen fastlagt en norm om, at myndighederne som udgangspunkt skal befinde sig på modenhedsniveau 4 på alle 7 områder for at kunne siges at have opnået "fuld implementering" af ISO 27001-standarden. Dog kan der være spørgeområder, hvor den enkelte myndighed som følge af en risikovurdering har valgt, at modenhedsniveau 3 er tilstrækkeligt til at opnå "fuld implementering". For nærværende måling har 15 ud af de 123 statslige myndigheder via deres risikovurderinger fastlagt en implementeringsnorm på 3 på et eller flere spørgeområder.

Se *bilag 1* for nærmere omtale af scoresystemet.

Sammenfattede resultater

38 pct. af de statslige myndigheder har endnu ikke opnået fuld implementering af standarden i nærværende måling fra september 2021. I forrige måling fra september 2020 havde 43 pct. af de statslige myndigheder ikke opnået fuld implementering.

9 myndigheder har oplyst, at de forventer at opnå fuld implementering inden udgangen af 2021. 27 myndigheder har oplyst, at de forventer at opnå fuld implementering inden udgangen af 2022.

23 pct. af de statslige myndigheder har rapporteret fremgang, mens 10 pct. har rapporteret tilbagegang i modenhed.

I nærværende måling er de statslige myndigheder mindst modne på spørgeområderne "Måling, audit og evaluering" (28 pct. af myndighederne har ikke opnået fuld implementering), "Leverandørstyring" (25 pct. har ikke opnået fuld implementering) og "Risikostyring" (20 pct. har ikke opnået fuld implementering) og mest modne på området "Politik for informationssikkerhed" (15 pct. har ikke opnået fuld implementering).

Der er sket en fremgang i det gennemsnitlige modenhedsniveau på områderne "Ledelsessystem", "Ressourcer, kompetencer og bevidsthed" og "Måling, audit og evaluering" og stagnation på områderne "Politik for informationssikkerhed" og "Risikostyring". På et enkelt spørgeområde, "Leverandørstyring", har de statslige myndigheder gennemsnitligt set vurderet tilbagegang i modenhed.

2. Resultat af måling for september 2021

ISO 27001-modenhedsmålingen fra september 2021, der er den 7. måling, danner grundlag for denne rapport udarbejdet af Digitaliseringsstyrelsen. Spørgeskemaet der ligger til grund for måleresultaterne blev besvaret af 20 ministerområder og i alt 123 statslige myndigheder. Blandt de 123 respondenter findes myndigheder af forskellig størrelse, risikoprofil og med forskellig anvendelse af it.

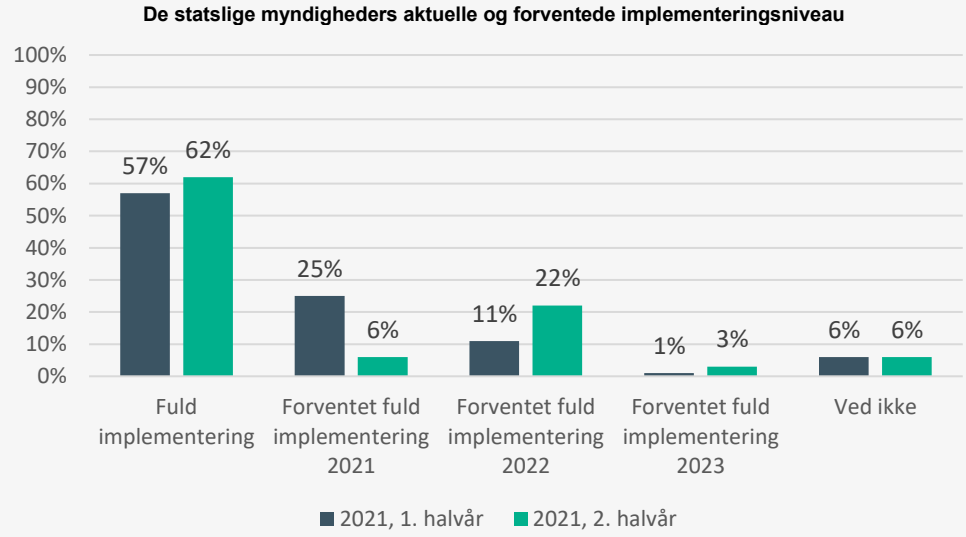
2.1 De statslige myndigheders nuværende og forventede implementeringsniveau

I *figur 1* ses både hvor stor en andel af de statslige myndigheder, der har opnået fuld implementering af ISO 27001 samt hvilke forventninger, de ikke fuldt implementerede myndigheder har til fremtidig implementering. Figuren indeholder både tal fra 7. måling fra september 2021 samt 6. måling fra marts 2021.

Det ses i *figur 1*, at 62 pct. af de statslige myndigheder har vurderet at have opnået fuld implementering af ISO 27001 i seneste måling. Dette udgør et fremskridt i forhold til den forrige måling fra marts 2021, hvor 57 pct. af de statslige myndigheder vurderede at have opnået fuld implementering. Fremskridtet modsvarer imidlertid ikke de 22 pct. af myndighederne, der ved forrige måling forventede fuld implementering ultimo 2021. De 22 pct. svarer til, at 27 myndigheder (der på daværende tidspunkt ikke havde opnået fuld implementering) forventede fuld implementering i 2021, i praksis har kun 8 myndigheder fuldt den implementeringsplan ved 7. ISO-måling. 9 myndigheder, der ved måletidspunktet ikke har vurderet at have opnået implementering, forventer fortsat at opnå implementering i 2021.

For en stor andel af de myndigheder, der endnu ikke har opnået fuld implementering, gælder, at de har skubbet tidsfristen for forventet implementering i deres respektive handleplaner. Det drejer sig om i alt 17 myndigheder. Justeringen af tidsfristerne sker som følge af forsinkelser eller udeståender i arbejdet med ISO-implementeringen. Sammenholdt med forventningen til fuld implementering på tværs af de statslige myndigheder ved 6. måling i marts 2021, viser nuværende måling, at der fortsat forventes fuld implementering af ISO 27001 standarden hos de statslige myndigheder i 2023, for de myndigheder, der har angivet en tidsfrist. 7 myndigheder har ikke fundet det muligt at fastsætte en konkret tidsfrist for at opnå fuld implementering.

Figur 1



Anm.: n = 122 (2021H1), n = 123 (2021H2), tallene er afrundede
Kilde: ISO 27001-modenhedsmåling 2021H1 og 2021H2

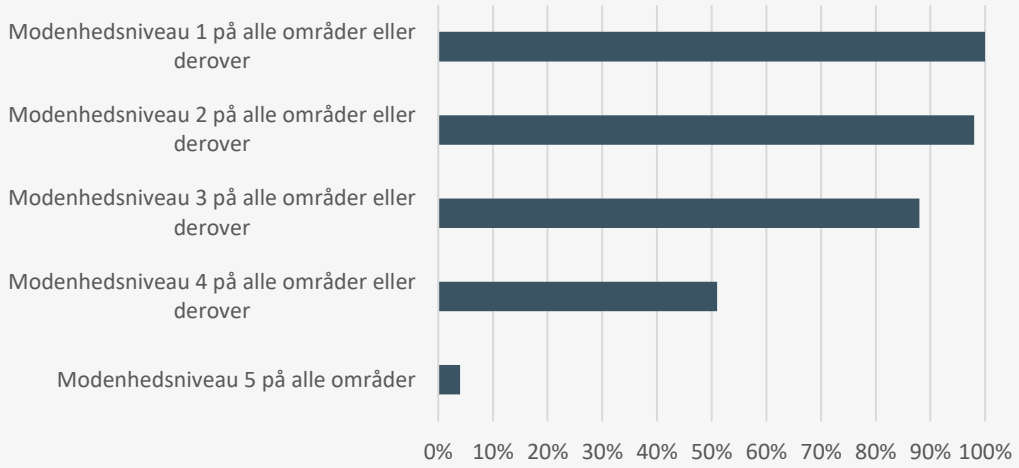
2.2 De statslige myndigheders modenhedsniveau

Figur 2 viser andelen af de statslige myndigheder, der har opnået et givent samlet modenhedsniveau. Fordi scoren 1 er den lavest mulige på den anvendte skala, har 100 pct. af de statslige myndigheder nødvendigvis opnået dette implementeringsniveau.

98 pct. af de statslige myndigheder har opnået et samlet modenhedsniveau på 2 *eller derover*. 2 pct. har et samlet modenhedsniveau på 1.

Endelig ses det at 51 pct. - dvs. lige over halvdelen - af de statslige myndigheder har implementeret ISO 27001 svarende til et modenhedsniveau 4 eller derover. At det samlede implementeringstal er højere skyldes, at en række statslige myndigheder via deres risikovurderinger fastlagt en implementeringsnorm på 3 på et eller flere spørgeområder.

Figur 2
De statslige myndigheders modenhedsniveau, pct.



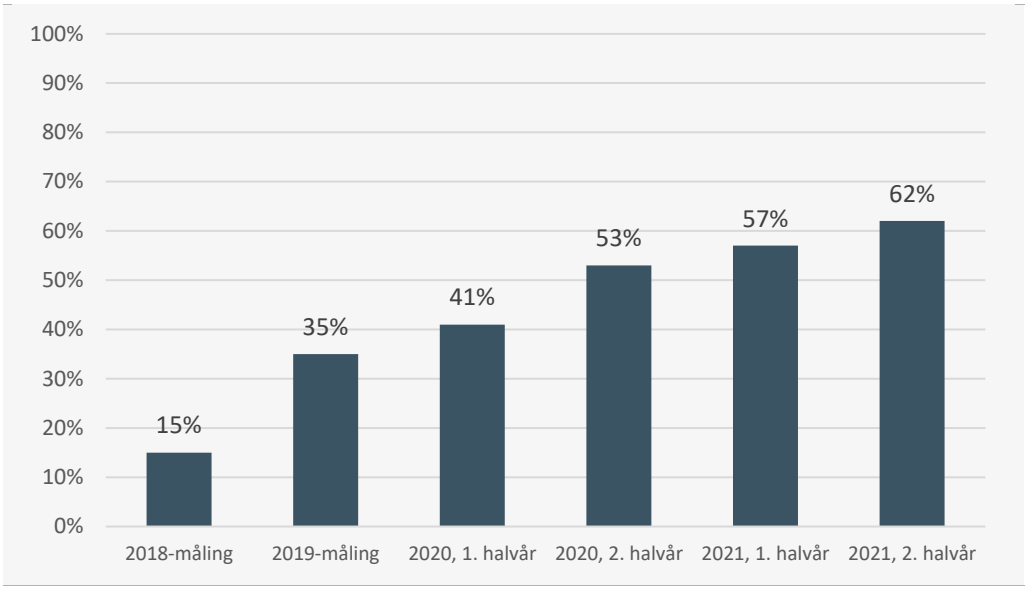
Anm.: n = 123, tallene er afrundede
Kilde: ISO 27001-modenhedsmåling 2021H2

2.3 Udvikling i de statslige myndigheders implementeringsgrad over tid

Figur 3 viser udviklingen i andelen af statslige myndigheder, der har opnået fuld implementering af ISO 27001-standarden. Der ses over tid en gradvis forøgelse af andelen af statslige myndigheder, har opnået fuld implementering af standarden.

I 2018-målingen havde kun 15 pct. opnået fuld implementering af ISO 27001. I 2019-målingen var dette tal mere end fordoblet til 35 pct. Ved 4. måling gennemført i marts 2020 – et halvt år efter 2019-målingen – havde 41 pct. opnået fuld implementering. Ved 5. måling fra september 2020 havde 53 pct. opnået fuld implementering, og i den 6. måling havde 57 pct. opnået fuld implementering. I den seneste måling er det tal steget til 62 pct. Det er ikke oplagt at konkludere fra tendensen, at de statslige myndigheders implementeringstempo reduceres over tid, da den faldende stigning skal sammenholdes med, at målingerne foretages hyppigere.

Figur 3
Udvikling i andel af statslige myndigheder, der har opnået fuld implementering af ISO 27001, pct.



Anm.: Antallet af myndigheder varierer på tværs af målinger. For den pågældende måling er antallet af myndigheder med fuld implementering opskrevet i parentes. n 2018 = 109 (16), n 2019 =113 (39), n 2020H1 = 119 (48), n 2020H2 = 117 (63), n 2021H1 = 122 (70), n 2021H2 = 123 (76). Bemærk at nogle myndigheder kan opnå fuld implementering med et modenhedsniveau på 3 på et eller flere områder sfa. risikovurdering

Kilde: ISO 27001-modenhedsmålinger 2018, 2019, 2020H1, 2020H2, 2021H1, 2021H2

2.4 De statslige myndigheders gennemsnitlige modenhed

Figur 4 belyser, hvor langt de statslige myndigheder er i arbejdet med at implementere ISO 27001 set relativt til den i udgangspunktet fastlagte norm på 4 på ISO 27001-modenhedsskalaen. Bemærk imidlertid at i alt 15 myndigheder, baseret på en konkret risikovurdering, alene er forpligtede på at implementere et modenhedsniveau svarende til værdien 3 på ISO 27001-modenhedsskalaen på et eller flere spørgeområder.

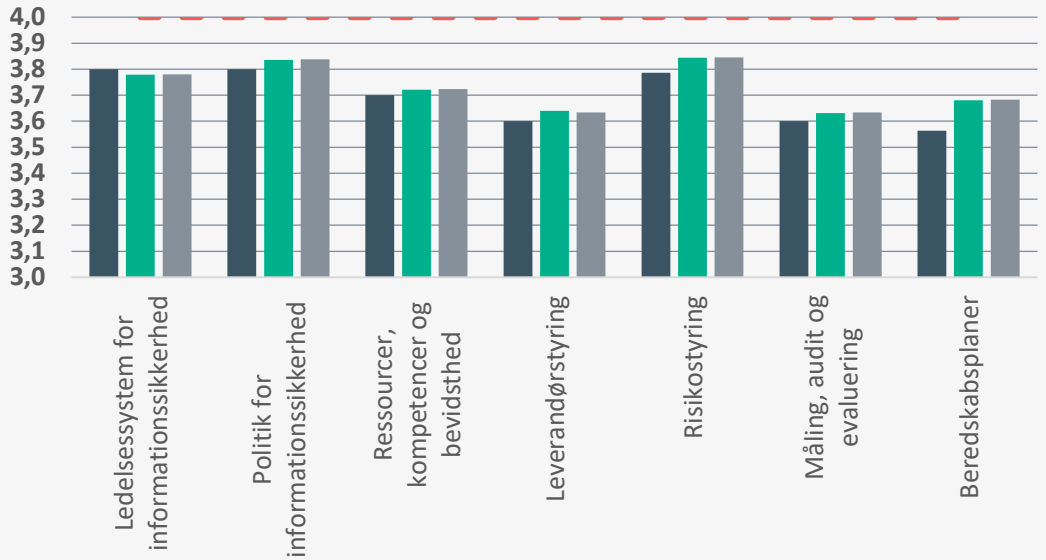
I *figur 4* ses den *gennemsnitlige modenhed* for de statslige myndigheder opgjort på de syv spørgeområder og for de tre seneste ISO 27001-målinger. I modsætning til de øvrige figurer, rapporterer denne altså gennemsnit for alle de statslige myndigheders modenhed. Bemærk, at den lodrette akse ikke viser hele modenhedsskalaen, der løber fra 1 til 5, af hensyn til læsbarhed.

Sammenlignet med 6. måling fra marts 2021 kan der konstateres fremgang i det gennemsnitlige modenhedsniveau på områderne "Ledelsessystem", "Ressourcer, kompetencer og bevidsthed" og "Måling, audit og evaluering" og stagnation på områderne "Politik for informationssikkerhed" og "Risikostyring". På et enkelt spørgeområde, "Leverandørstyring", har de statslige myndigheder gennemsnitligt set vurderet tilbagegang i modenhed. Den respektive fremgang og tilbagegang er dog af en sådan karakter, at det ikke umiddelbart giver udslag på grafen i figur 4.

I nærværende måling er den laveste gennemsnitlige modenhed at finde på spørgeområdet "Måling, audit og evaluering". Dette gjorde sig også gældende for forrige måling.

For både den aktuelle og den forrige måling gælder, at det er spørgeområdet "Politik for informationssikkerhed", hvor de statslige myndigheder er mest modne. Det er imidlertid ikke overraskende, at dette område ligger i front, da arbejdet med at udarbejde en politik for informationssikkerhed udgør én af de indledende øvelser i arbejdet med ISO 27001.

Figur 4
Gennemsnit af de statslige myndigheders ISO 27001-modenhed opgjort på spørgeområder



Anm.: 15 myndigheder er som følge af deres risikovurderinger alene forpligtet på at implementere ISO 27001 svarende til modenhedsniveau 3 på et eller flere spørgeområder. n = 123. Ikke hele modenhedsskalaen er afbilledet på den lodrette akse.
Kilde: ISO 27001-modenhedsmålinger 2020H1, 2020H2, 2021H1, 2021H2

2.5 De statslige myndigheders modenhedsniveau opgjort på spørgeområder

I *figur 2* sås det, at 51 pct. af de statslige myndigheder havde opnået et samlet modenhedsniveau på 4 eller derover. Med "samlet modenhedsniveau" forstås, at en statslig myndighed har opnået mindst et givent modenhedsniveau på alle spørgeområder. Hvis en myndighed fx har opnået værdien '4' på 6 spørgeområder, og værdien '3' på blot 1 spørgeområde, har myndigheden ikke opnået et samlet modenhedsniveau på 4 ud fra denne opgørelsesmetode.

Figur 5 nuancerer dette billede ved at illustrere hvilke andele af de statslige myndigheder, der befinder sig på givne trin på ISO 27001-modenhedsskalaen *opgjort på de enkelte spørgeområder*.

Det ses i den seneste måling, at 63 pct. af de statslige myndigheder har opnået modenhedsniveau 4 eller 5 på området "Måling, audit og evaluering". Det er også dette område, der har den laveste gennemsnitlige modenhed, som det sås i *figur 4*. For

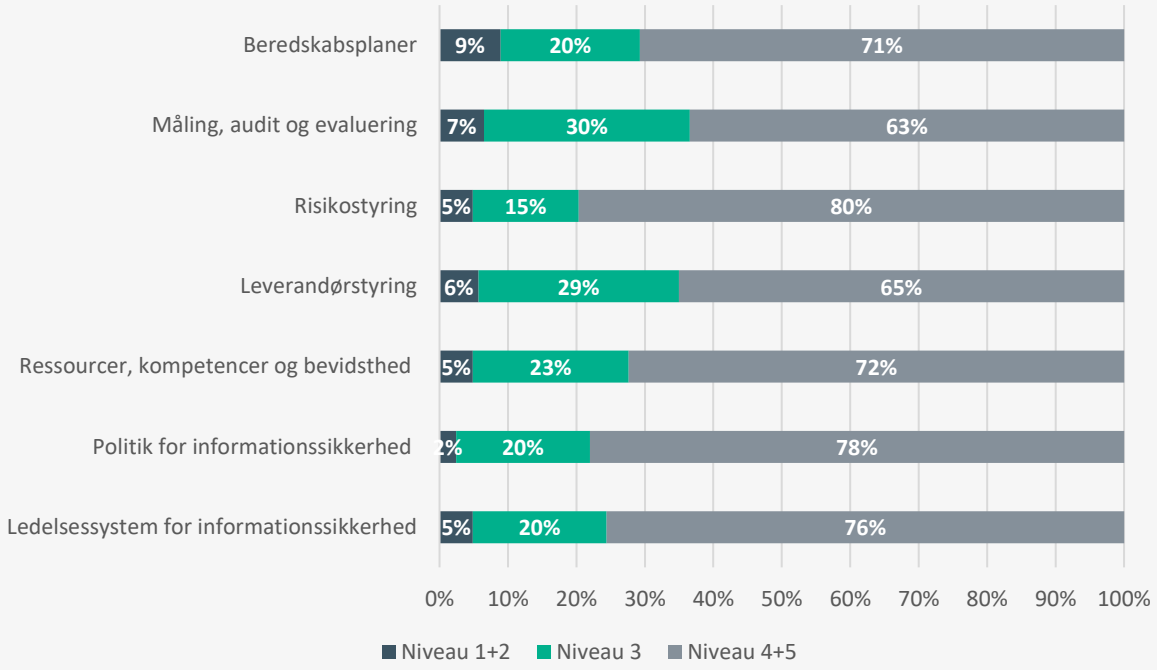
området "Leverandørstyring" har 65 pct. af myndighederne et modenhedsniveau på 4 eller 5.

På områderne hvor myndighederne klarer sig bedst, "Risikostyring", "Politik for informationssikkerhed" og "Ledelsessystem for informationssikkerhed", er det henholdsvis 80 pct., 78 pct. og 76 pct., der har et modenhedsniveau på 4 eller 5.

For alle de oplistede tal fra *figur 5* gælder det altså, at de er markant højere end de 51 pct., som figur 2 indikerede, havde opnået et samlet modenhedsniveau på 4 eller højere. Denne forskel er imidlertid forventelig og skyldes, at en del af de myndigheder, der opnår en modenhed på 4 eller højere på en række spørgeområder, ikke nødvendigvis opnår dette modenhedsniveau på alle 7 spørgeområder.

Figur 5

De statslige myndigheders modenhedsniveau fordelt på spørgeområder (2021H2), pct.

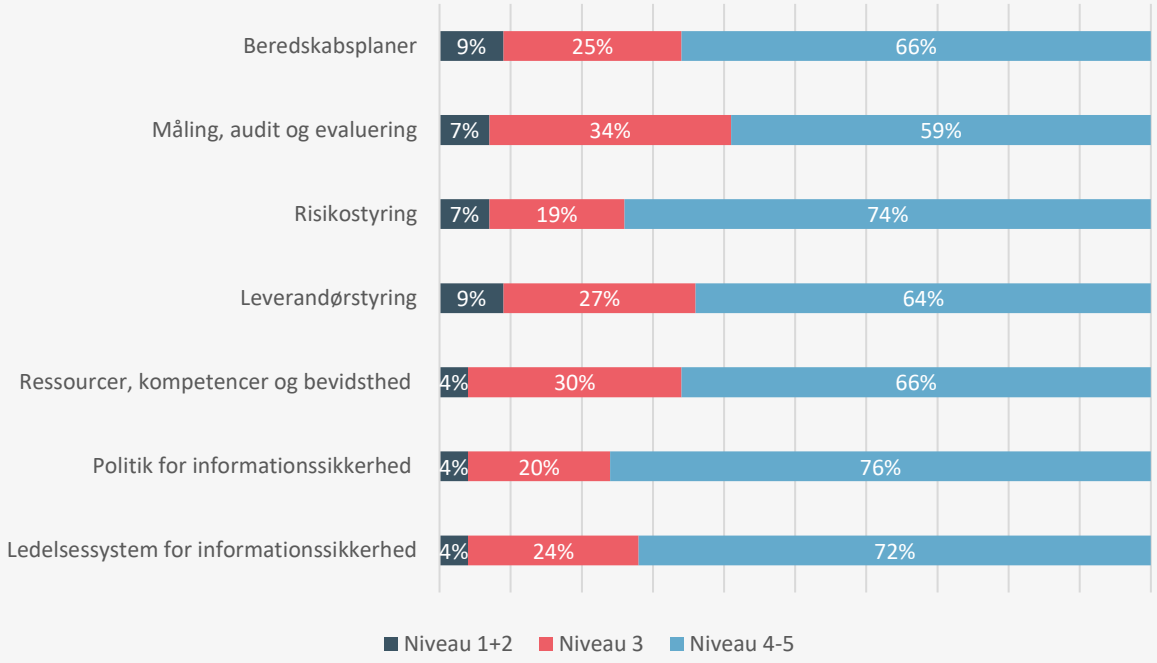


Anm.: n = 123, tallene er afrundede
Kilde: ISO 27001-modenhedsmåling 2021H2

Figur 6 viser den samme opgørelse som *figur 5*, men blot med resultaterne fra forrige måling fra marts 2021 i stedet for tal fra den seneste måling. På tværs af stort set alle kategorier gælder det, at der kun er relativt få procentpoints forskel på fordelingerne fra de to målinger.

Figur 6

De statslige myndigheders modenhedsniveau fordelt på spørgeområder (2021H1), pct.



Anm.: n = 122, tallene er afrundede
Kilde: ISO 27001-modenhedsmåling 2021H1

2.6 Udvikling i implementeringsgrad over tid opgjort på spørgeområder

I *figur 7 og figur 8* ses udviklingen i andelen af statslige myndigheder, der har opnået fuld implementering af standarden opgjort på spørgeområder og på tværs af målinger.

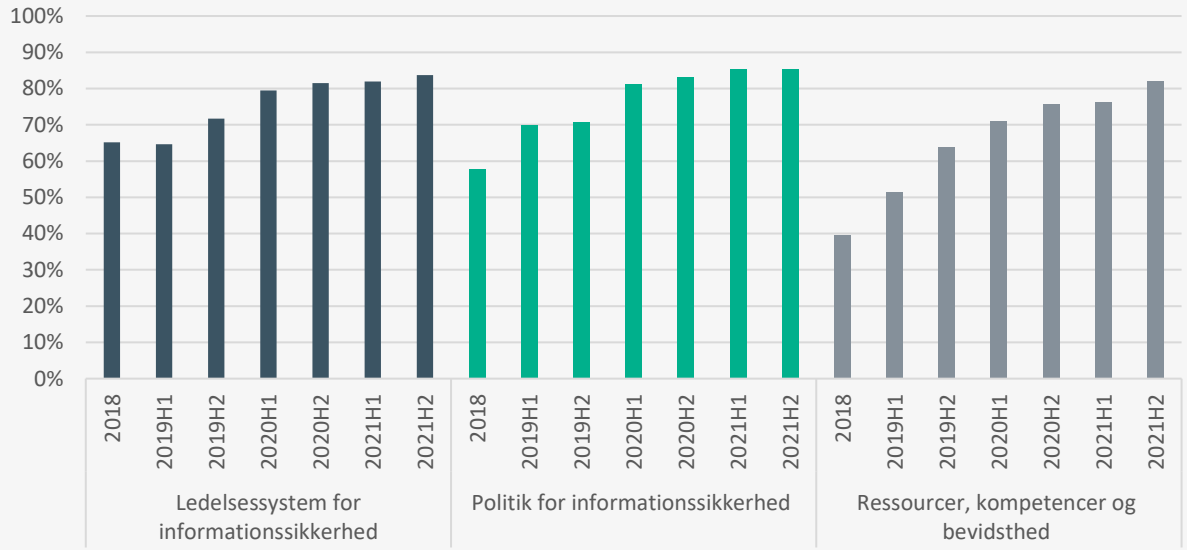
I figurerne ses det, at der har været stigning i andelen af myndigheder, der har opnået fuld implementering på alle spørgeområder.

På de områder hvor de statslige myndigheder er mest modne, ses en svag tendens til stagnation i udviklingen over de seneste tre målinger. Dette gør sig gældende for områderne "Ledelsessystem for informationssikkerhed", "Politik for informationssikkerhed" og "Risikostyring".

Spørgeområdet "Måling, audit og evaluering" ser den laveste grad af fuld implementering, hvor 70 pct. af de statslige myndigheder har opnået fuld implementering i den seneste måling. Som det sås i *figur 4*, er det også området med den laveste gennemsnits-modenhed blandt de statslige myndigheder.

Figur 7

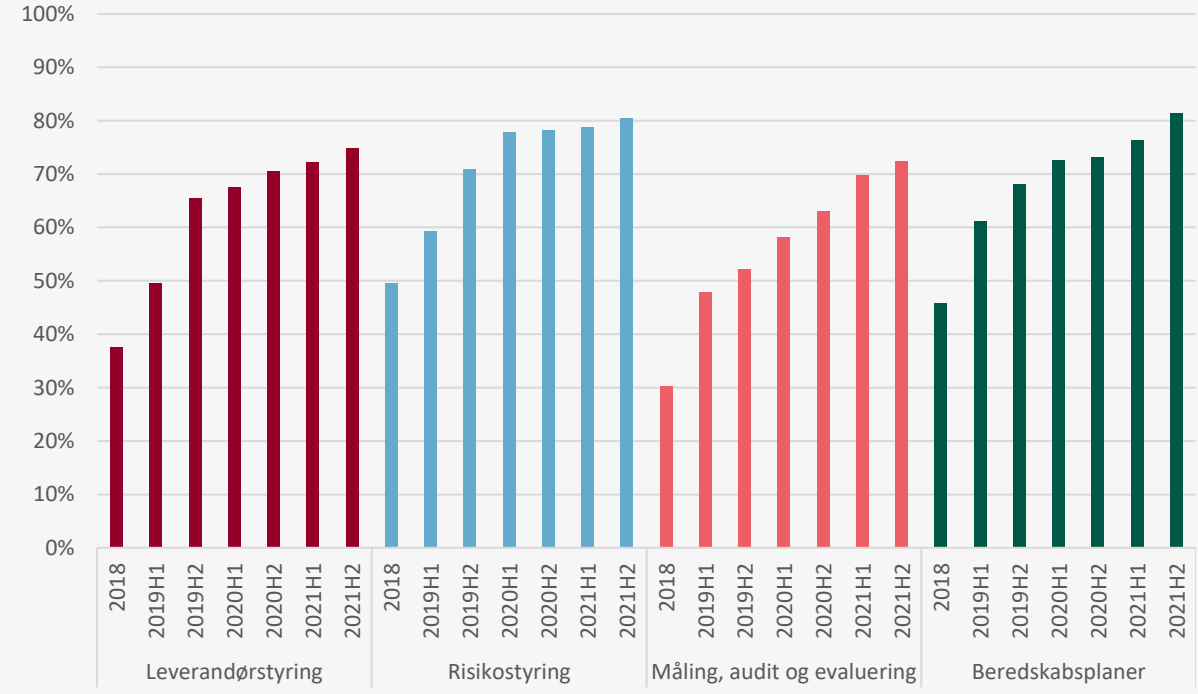
Andel af statslige myndigheder med fuld implementering, opgjort på spørgeområder, pct.



Anm.: tallene er afrundede
Kilde: ISO 27001-modenhedsmåling 2018, 2019H1, 2019H2, 2020H1, 2020H2, 2021H1, 2021H2

Figur 8

Andel af statslige myndigheder med fuld implementering, opgjort på spørgeområder, pct



Anm.: tallene er afrundede
Kilde: ISO 27001-modenhedsmåling 2018, 2019H1, 2019H2, 2020H1, 2020H2, 2021H1, 2021H2

3. Indsatser

Med henblik på at understøtte de statslige myndigheder i at implementere ISO 27001-standarden, har Digitaliseringsstyrelsen sideløbende med ISO 27001-modenhedsmålingerne iværksat en række understøttende initiativer. En række af disse nævnes nedenfor.

Der udbydes en uddannelse i informationssikkerhed på Digitaliseringsstyrelsens Digitaliseringsakademi, der blandt andet tilbyder praksisnær indføring i ISO 27001-standarden samt råd til det daglige arbejde med at styre informationssikkerheden i sin organisation.

Digitaliseringsstyrelsen tilbyder og vedligeholder løbende et vejledningsbibliotek med vejledninger og skabeloner, der giver udførlige og praksisnære introduktioner til arbejdet med alle de centrale aktiviteter i implementeringen af ISO 27001. Dette bibliotek kan både tilgås vis Digitaliseringsstyrelsens hjemmeside og Sikkerdigital.dk.

Desuden har Digitaliseringsstyrelsen i en årrække afholdt såkaldte ISO-bootscamps, der indeholder ekspertoplæg, øvelser og case-oplæg omhandlende arbejdet med ISO 27001. I 2021har der været afholdt fire såkaldte "mini" ISO-bootcamps til efteråret i både Jylland, på Fyn og i København. ISO-bootcamps forventes udbudt igen i 2022.

Med den nye nationale strategi for cyber- og informationssikkerhed 2022-2024 vil nye initiativer med henblik på at understøtte myndighedernes cyber- og informationssikkerhedsarbejde blive udviklet og udbudt.

4. Bilag: Målemetode

I ISO 27001-modenhedsmålingen måles de statslige myndigheder på deres implementering af ISO 27001-standarden. Spørgeskemaet, der ligger til grund for målingen, spørger ind til de følgende 7 områder:

1. Ledelsessystem for informationssikkerhed
2. Politik for informationssikkerhed
3. Ressourcer, kompetencer og bevidsthed
4. Leverandørstyring
5. Risikostyring
6. Måling, audit og evaluering
7. Beredskabsplaner

For hvert spørgeområde skal de statslige myndigheder vurdere sig selv på 6 kvalitetsparametre:

1. **Ledelsesforankring**: Ledelsen skal sikre, at ansvaret for en given opgave er placeret entydigt, og at dette er gjort ud fra en strategisk stillingtagen til uddelegering af ansvaret. Dermed sikres også, at eventuelle forandringer, der skal gennemføres har tilstrækkelig organisatorisk opbakning og beslutningskraft bag sig.
2. **Kommunikation**: For at politikker, retningslinjer og målsætninger mv. knyttet til ISO 27001 kan skabe værdi, er det afgørende, at de er kendt bredt i organisationen, og at relevante medarbejdere modtager målrettet information om tilføjelser eller ændringer. Derfor skal der arbejdes struktureret med kommunikation.
3. **Roller og ansvar**: Klare definitioner af roller og ansvar sikrer, at medarbejderne både individuelt og på tværs af organisationen har kendskab til, hvem der løser hvilke opgaver. Det giver samtidig mulighed for at følge op på, at opgaver er løst.
4. **Risikobaseret**: Det er et grundlæggende princip i ISO 27001, at informationssikkerheden skal baseres på risikovurderinger. Dette sikrer, at der er fokus på væsentlige indsatsområder og giver samtidig ledelsen et struktureret grundlag til at prioritere på baggrund af.
5. **Dokumentation**: Alle de værktøjer og dokumenter, der understøtter organisationens arbejde med informationssikkerhed, skal være tilgængelige for alle relevante medarbejdere og ledelse. Dette forudsætter, at der er en fælles tilgang til opbevaring af resultater fra arbejdet.
6. **Evaluering og forbedring**: I arbejdet med informationssikkerhed bør der løbende følges op på om eksisterende procedurer og politikker følges, og om der er behov eller mulighed for at forbedre disse. Der bør således følges systematisk op på, at erfaringer opsamles og ny viden deles.

Alle modenhedsvurderinger udføres på en fempunktsskala, der er beskrevet på følgende måde:

1. **Ad hoc:** Der er indikationer af, at myndigheden i et vist omfang har erkendt et behov for politikker og/eller processer. Aktiviteter gennemføres på ad hoc basis fra aktivitet til aktivitet.
2. **Gentaget:** Der er delvist påbegyndt udarbejdelse af politikker, og der eksisterer udvalgte formelle processer. Aktiviteter gennemføres på konsistent vis, uanset om de gennemføres af forskellige personer.
3. **Procesunderstøttet:** Politikker og/eller processer eksisterer. De er dokumenterede, og der er forventning om, at de stort set følges.
4. **Styret og målbar:** Der føres tilsyn med, at politikker og/eller processer følges. Gennemførelse af aktiviteter dokumenters struktureret og er så vidt muligt målbare. Der laves forbedringer på baggrund af tilsyn eller evalueringer.
5. **Optimeret:** Processer har opnået et meget højt kvalitetsniveau. Der optimeres på baggrund af egne erfaringer og sparring med andre organisationer.

digst.dk