DIGITALISERINGSSTYRELSEN

ISO 27001-modenhed i staten

August 2022

2022

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. Senest blev det med den nationale strategi for 2022-2024 besluttet, at der fremadrettet følges op på myndighedernes ISO 27001-implementering årligt, hvorfor der er én måling for 2022.

Nærværende rapport beskriver resultaterne af målingen for 2022. For at undersøge udviklingen i implementeringen sammenlignes resultaterne også med data fra tidligere målinger.

Spørgerammen for ISO 27001-modenhedsmålingen

Til brug for de årlige ISO 27001-modenhedsmålinger har Digitaliseringsstyrelsen udarbejdet en spørgeramme. I målingen selvevaluerer myndighederne deres implementering af standarden 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". Der er 124 myndigheder, som har besvaret nærværende måling.

Se *bilag 1* for nærmere forklaring af målemetoden.

Sammenfattede resultater af målingen fra 2022

Begrænset fremgang i implementeringen
Ved forrige måling fra november 2021 havde 38 pct. af de statslige myndigheder ikke opnået fuld implementering. Ved denne måling er andelen faldet til 36 pct., hvilket svarer til, at 3 myndigheder har opnået fuld implementering i perioden fra november 2021 til august 2022.

Forventninger til fuld implementering
10 myndigheder har oplyst, at de forventer at opnå fuld implementering inden udgangen af 2022. 28 myndigheder har oplyst, at de forventer at opnå fuld implementering inden udgangen af 2023, og 3 myndigheder har oplyst, at de forventer at opnå fuld implementering inden udgangen af 2024.

32 pct. af de statslige myndigheder har rapporteret fremgang, mens 20 pct. har rapporteret tilbagegang i modenhed.

Niveauet på spørgeområder
I nærværende måling er de statslige myndigheder mindst modne på spørgeområderne "Måling, audit og evaluering" (22 pct. af myndighederne har ikke opnået fuld implementering) og "Leverandørstyring" (22 pct. har ikke opnået fuld implementering). Myndighederne er mest modne på området "Politik for informationssikkerhed" (15 pct. har ikke opnået fuld implementering).

2. Resultat af måling for 2022

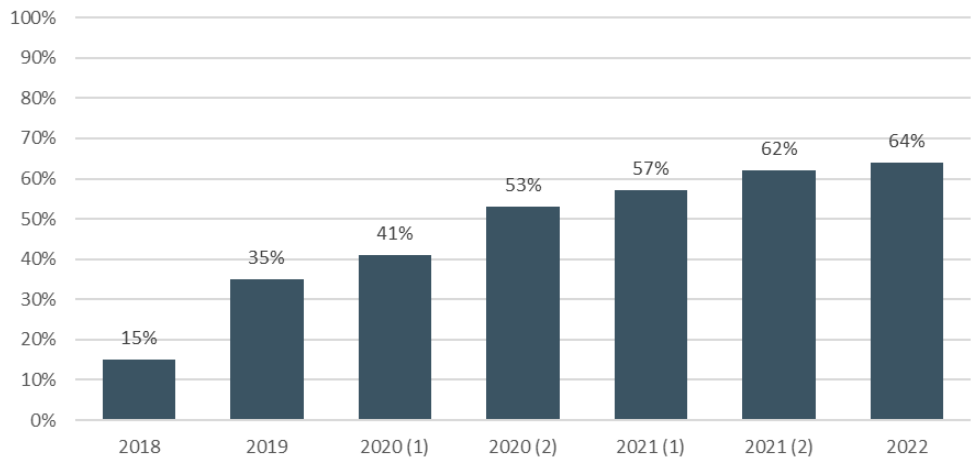
ISO 27001-modenhedsmålingen fra 2022, der er den 8. måling, danner grundlag for denne rapport udarbejdet af Digitaliseringsstyrelsen. Spørgeskemaet der ligger til grund for måleresultaterne blev besvaret af 20 ministerområder og i alt 124 statslige myndigheder i august 2022. De 124 myndigheder er af forskellig størrelse, risikoprofil og med forskellig anvendelse af it. For nærværende måling har 10 ud af de 124 statslige myndigheder via deres risikovurderinger fastlagt en implementeringsnorm på 3 på et eller flere spørgeområder.

2.1 Udvikling i de statslige myndigheders implementeringsgrad

I 2018 blev det besluttet at følge op på myndighedernes ISO 27001-implementering. Nedenstående afsnit viser beskriver udviklingen i de statslige myndigheders implementeringsgrad fra 2018 til 2022.

Figur 1 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, som har opnået fuld implementering af standarden. Ved målingen i 2. halvår 2021 var der 62 pct., der havde opnået fuld implementering, mens der i 2022 er 64 pct. af de statslige myndigheder, der har opnået fuld implementering.

Figur 1: Udvikling i andel af statslige myndigheder, der har opnået fuld implementering af ISO 27001



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), n 2022 = 124 (79). Bemærk at

nogle myndigheder kan opnå fuld implementering med et modenhedsniveau på 3 på et eller flere områder pba. risikovurdering.
Kilde: ISO 27001-modenhedsmålinger 2018, 2019, 2020H1, 2020H2, 2021H1, 2021H2 og 2022.

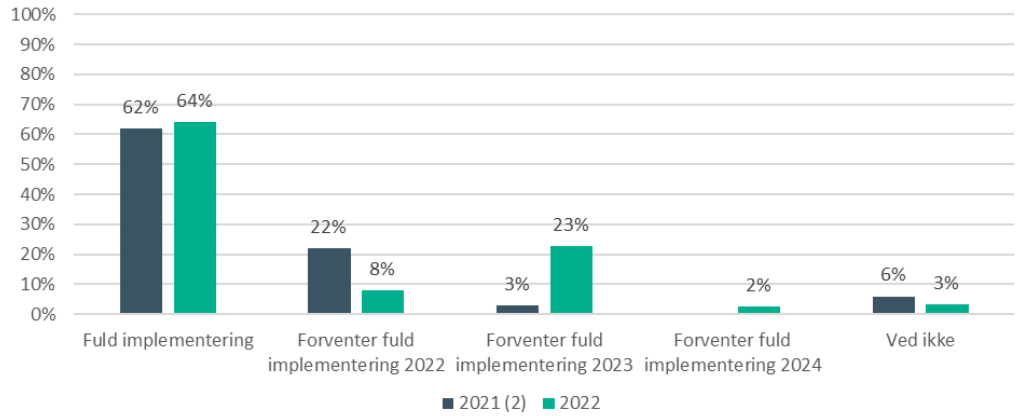
2.2 De statslige myndigheder nuværende og forventede implementeringsniveau

Alle statslige myndigheder skal implementere ISO 27001-standarden. Som både forrige målinger og indeværende måling viser, er der fortsat myndigheder, som ikke er fuld implementeret. Nedenstående afsnit beskriver myndighedernes aktuelle og forventede implementeringsniveau.

I figur 2 ses både hvor stor en andel af de statslige myndigheder, der har opnået fuld implementering af ISO 27001 samt deres forventninger til hvornår, de har opnået fuld implementering. Figuren indeholder både tal fra målingen i 2022 og 2021.

Det ses i figur 2, at 64 pct. af de statslige myndigheder har vurderet at have opnået fuld implementering af ISO 27001 i den seneste måling. Dette udgør et fremskridt i forhold til den forrige måling fra 2021, hvor 62 pct. af de statslige myndigheder vurderede at have opnået fuld implementering. Dog bemærkes, at der endvidere er 10 myndigheder, som ud fra en risikobaseret tilgang har vurderet ved denne måling, at værdien 3 er tilstrækkelig for deres myndighed ift. at opnå fuld implementering.

Figur 2: De statslige myndigheders aktuelle og forventede implementeringsniveau



Anm.: n = 124 (2022), 123 (2021H2), tallene er afrundede
Kilde: ISO 27001-modenhedsmåling 2022, 2021H2.

Fremskridtet fra sidste måling modsvarer imidlertid ikke de 22 pct. af myndighederne, der ved forrige måling forventede fuld implementering ultimo 2022. De 22 pct. svarer til, at 27 myndigheder (der på daværende tidspunkt ikke havde opnået fuld implementering) forventede fuld implementering i 2022. Det er kun 6 ud af de 27 myndigheder, der har fulgt deres implementeringsplan.

Ligesom tidligere rapporter også viser, har en stor andel af de myndigheder, der endnu ikke har opnået fuld implementering, har skubbet tidsfristen for forventet implementering i deres respektive handleplaner. 23 pct. af myndighederne har rykket deres forventning til, hvornår de opnår fuld implementering til 2023, mens 2 pct. har rykket deres forventede implementering til 2024. Samtidig er der 8 pct. af myndighederne, som forventer at opnår fuld implementering i indeværende år.

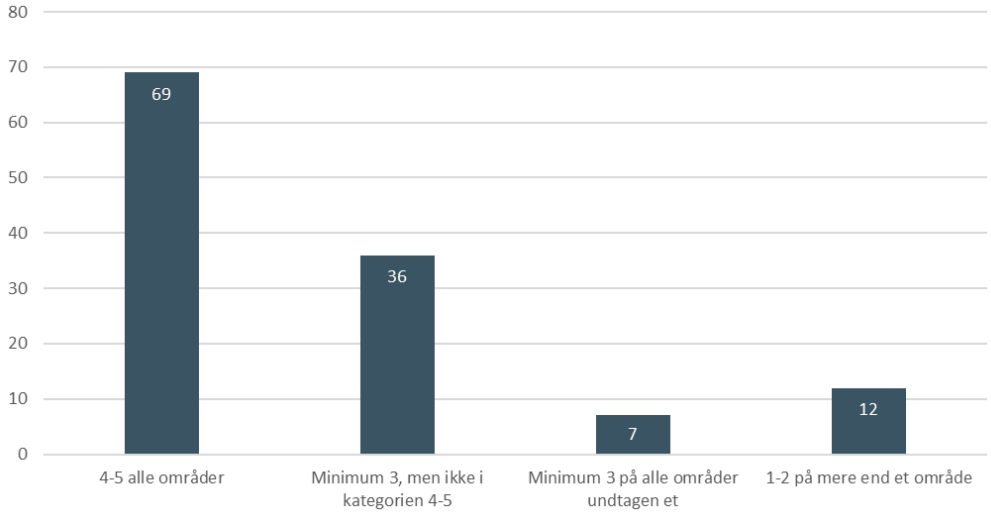
Myndighedernes udfordringer for fuld implementering
De myndigheder, som ikke har opnået fuld implementering, skal forelægge en handleplan for, hvornår og hvordan de opnår fuld implementering. I handleplanerne til modenhedsmålingen for 2022 peger myndighederne primært på, at den manglende implementering skyldes ressourcemæssige årsager. Flere myndigheder peger også på, at deres manglende implementering skyldes, at myndighederne har foretaget en ny gennemgang af sikkerheden i deres organisation, hvilket har givet anledning til en mere grundig og præcis gennemgang af de specifikke områder fra ISO-standarden. Endeligt peger flere myndigheder på, at deres manglende implementering skyldes transition til Statens It.

2.3 Fordeling af modenhedsniveau

Når de statslige myndigheder har opnået værdien 4 på alle spørgeområderne, har de opnået fuld implementering. Nedenstående afsnit beskriver hvordan myndighederne fordeler sig på modenhedsniveauerne 1-5.

Figur 3 illustrer, hvordan myndighederne fordeler sig på skalaen for modenhedsniveauet 1-5. Som det ses, er der 69 statslige myndigheder, som har opnået niveau 4 eller 5 på alle områder, hvorfor de har opnået fuld implementering. Der er 36 myndigheder, som har opnået niveau 3 på alle spørgeområderne. Ud af de 36 myndigheder har 10 myndigheder, ud fra en risikobaseret tilgang, vurderet, at værdien 3 er tilstrækkelig ift. at opnå fuld implementering. Disse myndigheder forventes derfor ikke at rykke til et højere niveau på modenhedsskalaen, idet de allerede er fuldt implementeret ved niveau 3. Figuren viser endvidere, at 7 myndigheder har opnået niveau 3 på minimum alle områder undtagen ét, mens 12 myndigheder har opnået niveau 1-2 på mere end ét område.

Figur 3: Antallet af myndigheder fordelt på modenhedsniveau



Anm.: 10 myndigheder er som følge af deres risikovurderinger alene forpligtet på at implementere ISO 27001 svarende til modenhedsniveau 3 på et eller flere spørgeområder. n = 124.
Kilde: ISO 27001-modenhedsmålinger 2022.

Det viser således, at der er en relativ stor andel af myndighederne som på mere end ét område ligger lavt på modenhedsskalaen, og det tyder på, der er behov for en mere målrettet og vedvarende indsats, hvis disse myndigheder skal løfte deres modenhedsniveau.

2.4 De statslige myndigheders modenhedsniveau opgjort på spørgeområder

Nedenstående afsnit beskriver de statslige myndigheders modenhedsniveau opgjort på de syv spørgeområder for at se hvilke områder, myndighederne er mest og mindst modne på.

Figur 3 viste, at 69 statslige myndigheder havde opnået et samlet modenhedsniveau på 4 eller derover. Med "samlet modenhedsniveau" forstås, at en statslig myndighed har opnået mindst niveau 4 på alle spørgeområder. Hvis en myndighed fx har opnået værdien 3 på blot ét spørgeområde, har myndigheden ikke opnået et samlet modenhedsniveau på 4 ud fra denne opgørelsesmetode.

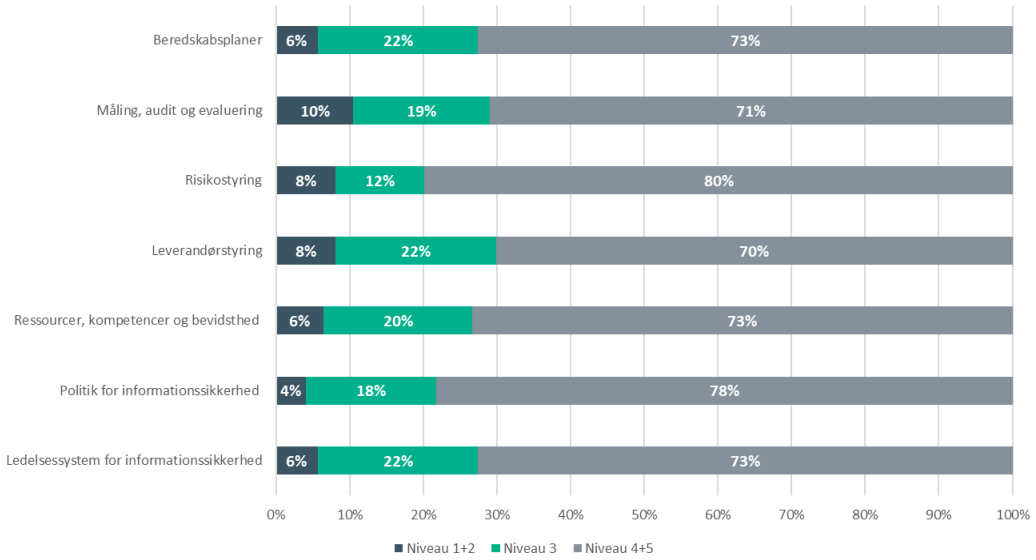
Figur 4 illustrerer, hvilke andele af de statslige myndigheder, der befinder sig på givne trin på ISO 27001-modenhedsskalen opgjort på de enkelte spørgeområder.

Det ses i den seneste måling, at 70 pct. af de statslige myndigheder har opnået modenhedsniveau 4 eller 5 på området "Leverandørstyring". For området "Måling, audit og evaluering" har 71 pct. af myndighederne et modenhedsniveau på 4 eller 5.

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

For alle de oplistede tal i figur 4 gælder det således, at de er markant højere end den samlede andel af myndigheder, som har opnået fuld implementering, hvilket 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 syv spørgeområder.

Figur 4: Modenhedsniveau fordelt på spørgeområderne, 2022

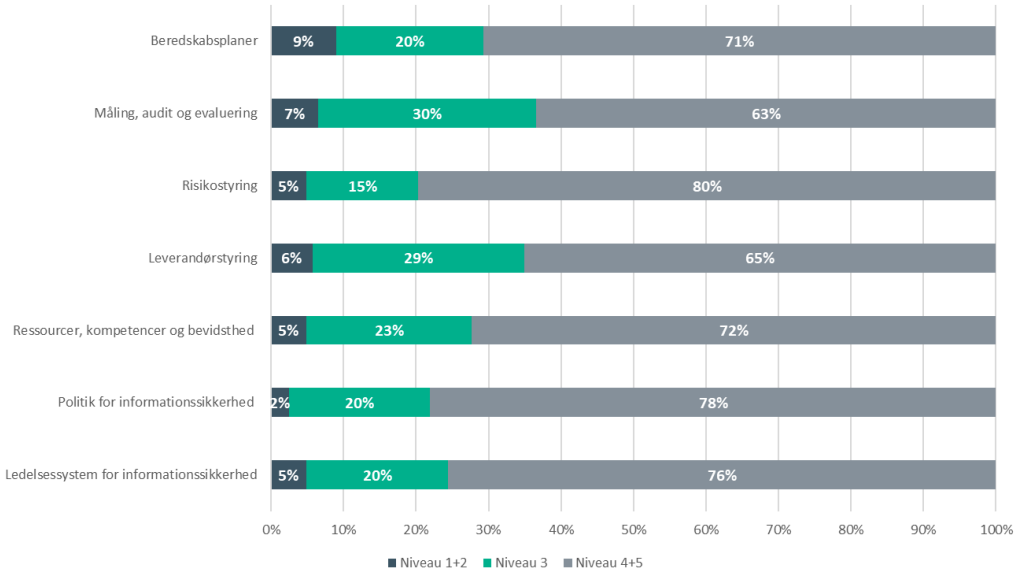


Anm.: n = 124, tallene er afrundede

Kilde: ISO 27001-modenhedsmåling 2022

Figur 5 viser den samme opgørelse som figur 4, men blot med resultatet fra forrige måling fra november 2021 i stedet for tal fra den seneste måling. Bortset fra "Måling, audit og evaluering" og "Leverandørstyring", hvor myndighederne er blevet mere modne, gælder det, at der kun er relativt få procentpoint til forskel på fordelingerne på de to målinger. Dog ses det, at myndighederne er blevet mindre modne på "Ledelsessystem for informationssikkerhed", hvor 76 pct. af myndighederne ved målingen i november 2021 var på niveau 4 eller 5, mens 73 pct. af myndighederne er på niveau 4 eller 5 ved den seneste måling.

Figur 5: Modenhedsniveau fordelt på spørgeområderne, 2021H1



Anm.: n = 123, tallene er afrundede

Kilde: ISO 27001-modenhedsmåling 2021H2

2.5 Udvikling i implementeringsgrad opgjort på spørgeområder

Nedenstående afsnit beskriver udviklingen i implementeringsgraden opgjort på spørgeområderne for at se en konkret fremgang i implementeringen.

I figur 6 og figur 7 ses udviklingen i andelen af statslige myndigheder, der har opnået fuld implementering af de enkelte spørgeområder.

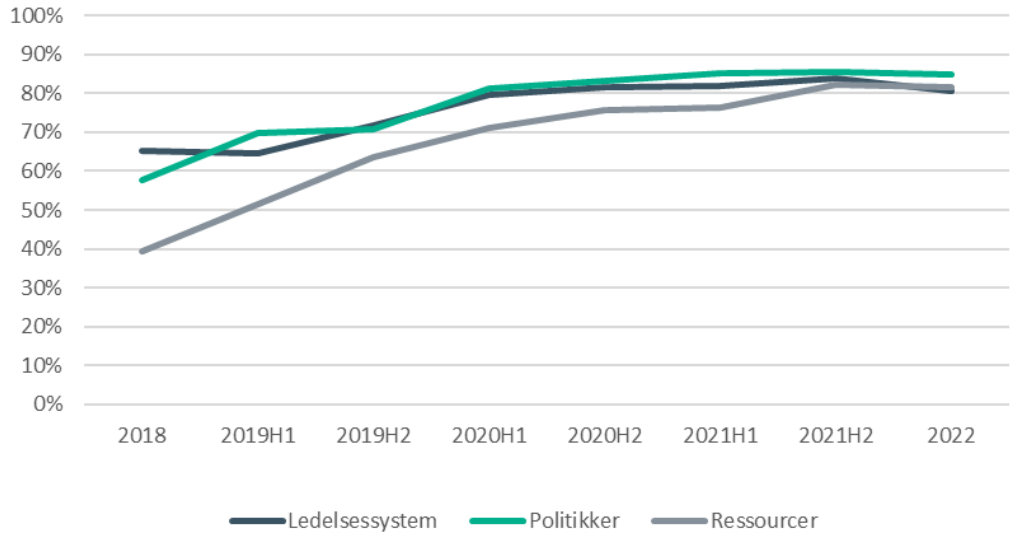
Generelt er tendensen den samme for alle områderne. Der har siden 2018 og frem til og med måling i 2022 været en stigning i implementeringsgraden. Siden 2020 er udviklingen dog for flere af områderne stagneret.

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

onssikkerhed" og "Risikostyring". Det tyder således på, at myndighedernes implementeringsniveau fastholdes, men at der ikke arbejdes vedvarende på at løfte implementeringsniveauet yderligere.

Spørgeområderne "Måling, audit og evaluering" og "Leverandørstyring" har den laveste grad af fuld implementering, hvor 78 pct. af de statslige myndigheder har opnået fuld implementering i den seneste måling på begge spørgeområder.

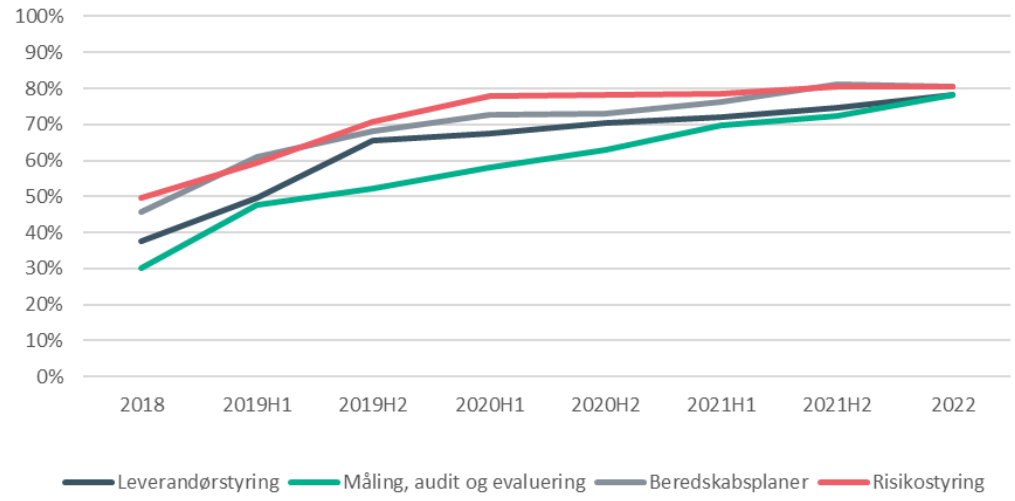
Figur 6: Andel af statslige myndigheder med fuld implementering, opgjort på spørgeområde, pct.



Anm.: Tallene er afrundede

Kilde: ISO 27001-modenhedsmåling 2018, 2019H1, 2019H2, 2020H1, 2020H2, 2021H1, 2021H2 og 2022.

Figur 7: Andel af statslige myndigheder med fuld implementering, opgjort på spørgeområde, pct.



Anm.: Tallene er afrundede

Kilde: ISO 27001-modenhedsmåling 2018, 2019H1, 2019H2, 2020H1, 2020H2, 2021H1, 2021H2 og 2022.

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 ISO-bootscamps, der indeholder ekspertoplæg, øvelser og case-oplæg omhandlende arbejdet med ISO 27001. I 2022 afholdes der ligeledes en bootcamp i efteråret. ISO-bootcamps forventes udbudt igen i 2023.

Endeligt sikres en løbende vidensdeling i statens netværk for informationssikkerhed, som samler personer, der arbejder med informationssikkerhed i det offentlige mindst to gange årligt. Alle ministerområder er repræsenteret i netværket. Netværket har til hensigt at bidrage med generel vidensdeling og erfaringsudveksling inden for den praktiske håndtering af relevante emner, herunder implementering af ISO 27001.

Med den nye nationale strategi for cyber- og informationssikkerhed 2022-2024 er nye initiativer iværksat, som skal understøtte myndighedernes cyber- og informationssikkerhedsarbejde. Målemetoden for opfølgningen på implementeringen af ISO 27001 er således ved at blive justeret, så opfølgningen i højere grad hjælper myndighederne i mål med fuld implementering på de områder, hvor der ses de største udfordringer. Samtidig arbejdes der løbende på at forbedre vejledningsindsatserne over for myndighederne, hvorfor der også blev udgivet en vejledning til de statslige myndigheder om it-beredskab i 2022.

4. Bilag 1: Målemetode

I ISO 27001-modenhedsmålingen måles de statslige myndigheder på deres implementering af ISO 27001-standarden. Myndighederne har besvaret den 8. modenhedsmåling fra juni til august 2022.

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