ISO 27001-modenhed i staten

November 2020

2020

Indhold

1. Indledning

Rapporten behandler resultatet af modenhedsmålingen af de statslige myndigheders implementering af den internationale standard for styring af informationssikkerhed, ISO 27001, gennemført i september 2020.

ISO 27001 er en international standard, der fastsætter bedste praksis for etablering, drift og løbende vedligehold af et ledelsessystem for styring af informationssikkerhed. 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 frem til 2021. 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.

ISO 27001- spørgeskema

Til brug for de halvårlige opfølgninger har Digitaliseringsstyrelsen udarbejdet et spørgeskema til at foretage ISO 27001-modenhedsmålinger. I målingen angiver myndighederne en egenvurdering på en modenhedsskala fra 1-5 på syv væsentlige områder af ISO-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 være på modenhedsniveau 4 på en skala fra 1-5 på alle syv områder for at have implementeret ISO 27001-standarden fuldt ud. Dog kan der være områder, hvor den enkelte myndighed som følge af en risikovurdering har valgt, at modenhedsniveau 3 er tilstrækkeligt for at opnå implementering.

Første modenhedsmåling for 2020 viste en overordnet fremgang i arbejdet med implementeringen af ISO 27001-standarden i staten. En række myndigheder havde nedjusteret deres modenhed, mens en del myndigheder havde registreret en fremgang i deres modenhed. Samlet set viste målingen, at der fortsat udestår et arbejde med implementering af standarden for største delen af myndighederne, og dermed i staten. Nærværende rapport behandler resultatet af målingen, der blev gennemført i september 2020.

2. Resultat af målingen for september 2020

ISO 27001-modenhedsmåling for september 2020 viser fortsat fremgang i arbejdet med implementeringen af ISO 27001-standarden i staten. Meget få myndigheder har nedjusteret deres modenhed siden seneste måling, mens en del myndigheder har registreret en fremgang i deres modenhed. Samlet set viser målingen, at der fortsat udestår et arbejde med implementering af standarden for lidt under halvdelen af de statslige myndigheder, og dermed i staten.

ISO 27001-modenhedsmålingen er gennemført af Digitaliseringsstyrelsen i september 2020. Målingen blev besvaret af 18 ministerområder og i alt 119 statslige myndigheder. Blandt de 119 besvarelser findes både små og store myndigheder med forskellig anvendelse af it-systemer. Alle myndigheder er i forbindelse med målingen behandlet ens og med samme vægt, uafhængigt af den enkelte myndigheds størrelse og brug af it-systemer.

Modenhedsmålingen for september 2020 viser tre centrale resultater *jf. boks 1*. Generelt viser målingen fremgang i implementeringen af standarden hos myndighederne. Der er en stigning fra 41 pct. til 53 pct. af myndighederne, der har opnået fuld implementering af standarden ift. første måling for 2020.

Målingen for september 2020 viser ligeledes, at det er de samme områder, der udfordrer myndighederne, som ved første måling for 2020. Det er fortsat området "Måling, audit og evaluering", der udfordrer myndighederne mest til trods for en mindre fremgang i modenheden inden for dette område. Myndighederne er også fortsat mest modne inden for områderne "Risikostyring", "Ledelsessystem for informationssikkerhed" og "Politik for informationssikkerhed".

Boks 1
Centrale resultater af målingen

- Der er en stigning fra 41 pct. til 53 pct. af myndighederne, der har opnået fuld implementering af standarden ift. første måling for 2020.
- 6 pct. af myndighederne har vurderet sig selv lavere i modenhed i anden måling for 2020 end ved første måling 2020.
- 59 pct. af myndighederne har vurderet sig selv på samme niveau i anden måling for 2020 som ved første måling for 2020.

Boks 2
Mest og mindst modne områder

- Myndighederne er mest modne inden for spørgeområderne: "Risikostyring", "Ledelsessystem for informationssikkerhed" og "Politik for informationssikkerhed".
- Myndighederne er mindst modne inden for spørgeområdet "Måling, audit og evaluering".

Fremgang i implementeringen af standarden i staten

Figur 1 neden for viser gennemsnittet af myndighedernes besvarelse fordelt på spørgeområderne i februar 2020 og september 2020. Det fremgår, at der er sket en mindre fremgang på samtlige af spørgeområderne, med undtagelse af området "Risikostyring", som er på samme niveau af implementering.

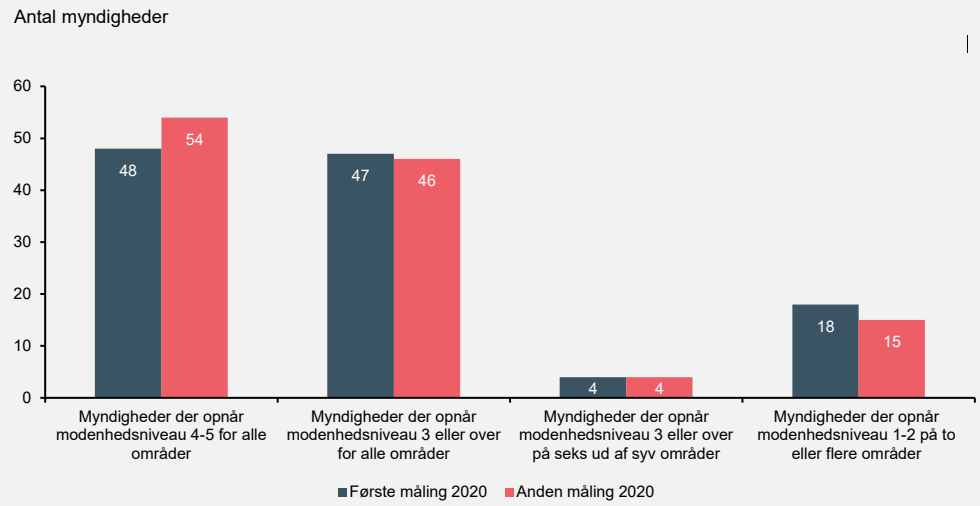
Figur 1

Gennemsnit af myndighedernes besvarelse pr. spørgeområde ved første måling 2020 og anden måling 2020

Anm.: Der kan være områder, hvor den enkelte myndighed som følge af en risikovurdering har valgt, at modenhedsniveau 3 er tilstrækkeligt for at opnå implementeirng.

Figur 2 neden for viser det samlede antal myndigheder fordelt på modenhedsniveauer ved første måling i 2020 og nærværende måling. Det fremgår, at 54 myndigheder har opnået modenhedsniveau 4 eller derover på alle områder, mod 48 myndigheder ved første måling i 2020. 46 myndigheder har opnået mindst niveau 3 på alle områder, mod 47 myndigheder ved første måling 2020. Endelig er der et fald i antallet af myndigheder, der vurderer sig selv til at ligge på modenhedsniveau 1-2 på to eller flere områder af målingen, med 15 myndigheder i september 2020, mod 18 myndigheder i februar 2020.

Figur 2
Myndighedernes ISO-modenhed ved første måling 2020 og anden måling 2020

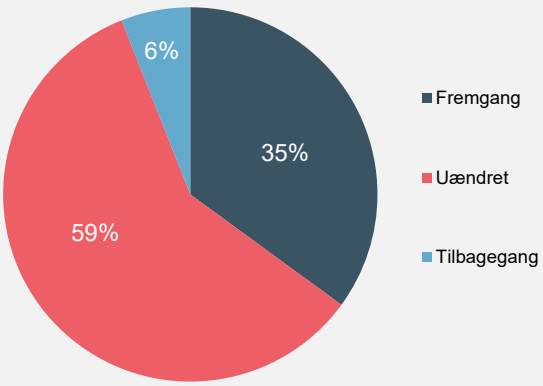


Anm.: Der kan være områder, hvor den enkelte myndighed som følge af en risikovurdering har valgt, at modenhedsniveau 3 er tilstrækkeligt for at opnå implementering.

Udviklingen i modenheden hos myndighederne

Figur 3 viser den overordnede udvikling i modenheden hos myndighederne fra februar 2020 til september 2020. Figuren viser, at 35 pct. af myndighederne oplever fremgang i implementeringen af standarden. Samtidig viser figuren, at 6 pct. af myndighederne har nedjusteret deres modenhed i målingen for september 2020 i forhold til målingen for februar 2020, og 59 pct. af myndighederne har vurderet sig selv på samme modenhedsniveau. At mange myndigheder ikke har oplevet en fremgang i modenheden, og at få har vurderet en tilbagegang, skyldes bl.a., at myndighederne ikke har gennemført planlagte aktiviteter eller, at aktiviteter er blevet forsinkede. Myndighederne har generelt udtrykt, at omorganisering og omprioritering af sikkerhedsopgaver som følge af Covid-19 har betydet væsentlige ressourcetræk for myndighedernes sikkerhedsenheder bl.a. ifm. sikring af hjemmearbejdspladser. Enkelte myndigheder har oplyst, at tilbagegangen i modenheden skyldes en øget erkendelse af opgavens omfang, hvilket har afstedkommet egenvurderinger, der i højere grad afspejler det aktuelle modenhedsniveau i myndighederne. Endelig er enkelte myndigheder fortsat i en proces med at omorganisere og tilpasse indsatserne, hvilket skal ses som en del af det fortsatte arbejde med at højne informationssikkerheden.

Figur 3
Ændring i modenhed fra første måling 2020 til anden måling 2020

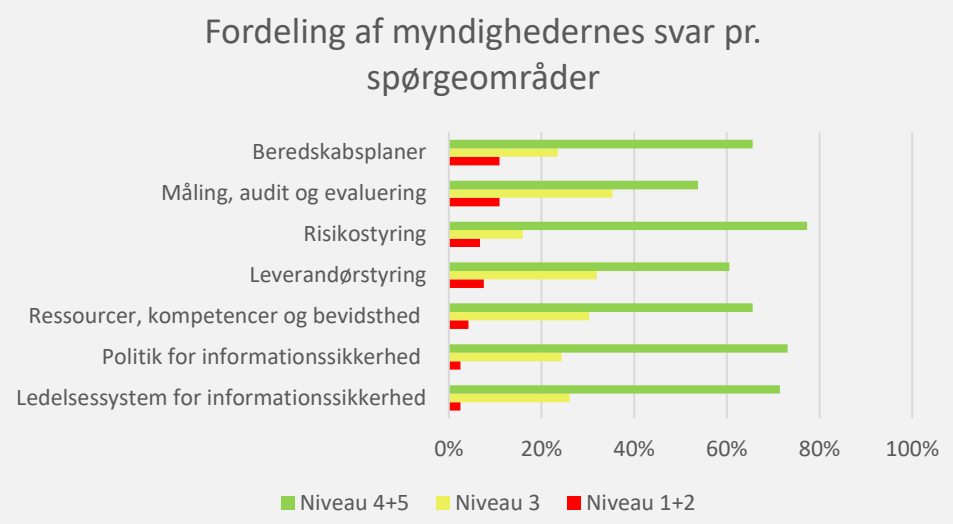


Anm.: Figuren vedrører de myndigheder, der både eksisterede i første måling for 2020 og anden måling 2020.

Standardens implementeringsgrad i staten

Figur 4 viser modenheden på hvert spørgeområde på tværs af myndighederne. Grøn markering svarer til den procentdel af myndighederne, der har opnået fuld implementering på det givne område, svarende til niveau 4 eller 5. Gul markering svarer til den procentdel af myndighederne, der nærmer sig fuld implementering, svarende til niveau 3, og rød svarer til den procentdel, der fortsat er langt fra fuld implementering, svarende til niveau 1 eller 2.

Figur 4
Fordeling af myndighedernes svar pr. spørgeområde



Anm.: Der kan være områder, hvor den enkelte myndighed som følge af en risikovurdering har valgt, at modenhedsniveau 3 er tilstrækkeligt for at opnå implementering.

Figuren viser at der fortsat udestår et arbejde med at implementere ISO 27001, særligt på området "Måling, audit og evaluering", hvor 46 pct. af myndighederne fortsat ikke har opnået fuld implementering. Måling, audit og evaluering dækker den løbende opfølgning på de politikker og processer, som implementeres i organisationen og sikrer det fortsat høje sikkerhedsniveau i organisationen. Opfølgningsarbejdet forudsætter derfor, at de processer, der skal måles og evalueres på, er etableret. Det er derfor også naturligt, at "Måling, audit og evaluering" er et af de sidste områder, der implementeres. "Måling, audit og evaluering" er sammen med "Beredskabsplaner" det område, hvor flest myndigheder er langt fra at nå i mål. Således er 11 pct. af myndighederne fortsat langt fra at opnå implementeringen, idet de er på niveau 1 eller 2.

Et andet område, hvor der udestår et arbejde, er "Leverandørstyring", hvor 40 pct. af myndighederne ikke har opnået fuld implementering af standarden. Dette område omhandler både krav til og samarbejde med leverandøren omkring sikkerheden i systemer og de processer, der omgiver disse. Udarbejdelsen af den rette politik og de rette processer, involvering af medarbejdere og ledelse samt opfølgningsarbejdet, er blandt de indsatser, der styrker informationssikkerheden i leverandørstyringen og som kræver en stor indsats fra organisationens side.

Figuren viser samtidig, at myndighederne er relativt modne inden for områderne "Risikostyring", hvor 77 pct. har opnået fuld implementering, "Politik for informationssikkerhed", hvor 73 pct. har opnået fuld implementering, og "Ledelsessystem for informationssikkerhed", hvor 72 pct. har opnået fuld implementering.

Dette er en naturlig konsekvens af, at områderne er centrale elementer i den tidlige etablering af et ledelsessystem for informationssikkerhed.

For at understøtte myndighederne i deres arbejde med implementeringen af ISO 27001-standarden arbejdes der i regi af den nationale strategi for cyber- og informationssikkerhed samt i regi af den fællesoffentlige digitaliseringsstrategi, løbende på en række initiativer. I 2020 har der bl.a. været afholdt en Masterclass for ledere i staten på cyber- og informationssikkerhedsområdet samt et møde i statens netværk for informationssikkerhed, hvor bl.a. leverandørstyring indgik som tema. Derudover blev der i oktober afholdt en ISO-bootcamp, og der udbydes en uddannelse i informationssikkerhed i regi af Digitaliseringsstyrelsens Digitaliseringsakademi. Endeligt pågår der en informationsindsats på platformen Sikkerdigital.dk rettet mod informationssikkerhedskoordinatorer og andet informationssikkerhedsfagligt personale, der blandt andet arbejder med implementering og opretholdelse af ISO-standarden i organisationer. Som en del af indsatsen opdateres vejledninger og der udarbejdes nye materialer vedrørende ISO-implementering.

digst.dk