DIGITALISERINGSSTYRELSEN

ISO 27001-modenhed i staten

November 2019

2019

Indhold

1. Indledning

Rapporten behandler resultatet af modenhedsmåling af de statslige myndigheders implementering af den internationale standard for styring af informationssikkerhed, ISO 27001, gennemført i september 2019.

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.

Til brug for de halvårlige opfølgninger har Digitaliseringsstyrelsen udarbejdet et spørgeskema til at foretage ISO 27001-modenhedsmålinger. I målingen angiver myndighederne en egen-vurdering 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.

Nærværende rapport behandler resultatet af målingen, der blev gennemført i september 2019. Den tidligere modenhedsmåling fra 2018 viste, at myndighederne arbejdede aktivt med ISO 27001-standardens områder, men at der stadig udestod et arbejde med implementeringen. Til sammenligning viser målingen fra september 2019 en overordnet fremgang i modenheden hos myndighederne. Målingen viser blandt andet en stigning fra 15 pct. til 35 pct. af myndighederne, der har opnået fuld implementering af standarden. Samtidig viser målingen, at 21 pct. af myndighederne har nedjusteret deres modenhed på et eller flere områder.

2. Resultat af målingen for 2019

ISO 27001-modenhedsmåling for september 2019 viser en overordnet fremgang i arbejdet med implementeringen af ISO 27001-standarden i staten. Samtidig viser målingen, at nogle myndigheder har nedjusteret deres modenhed siden seneste måling. Samlet set viser målingen, at der fortsat udestår et arbejde med implementering af standarden i staten.

ISO 27001-modenhedsmålingen er gennemført af Digitaliseringsstyrelsen i september 2019. Målingen blev besvaret af alle 18 ministerområder og i alt 113 statslige myndigheder. Blandt de 113 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 viser tre centrale resultater, *jf. boks 1*. Generelt viser målingen fremgang i implementeringen af standarden hos myndighederne. Der er en stigning fra 15 pct. til 35 pct. af myndighederne, der har opnået fuld implementering af standarden ift. 2018. Samtidig viser målingen, at der er et fald fra 36 pct. til 19 pct. af myndighederne, der fortsat er langt fra at opnå fuld implementering og har et modenhedniveau på 1 eller 2 på to eller flere områder af målingen.

Endelig viser målingen, at 21 pct. af myndighederne har vurderet sig selv lavere i 2019 end i 2018 på et eller flere områder af målingen. Den efterfølgende dialog med myndighederne giver indtryk af, at dette skyldes, dels en voksende erkendelse hos myndighederne af opgavens omfang og kompleksitet, dels omorganisering af informationssikkerheden hos enkelte ministerområder.

Målingen viser hvilke områder, som myndighederne er henholdsvis mest og mindst modne indenfor, *jf. Boks 2*. Til forskel fra målingen fra 2018, hvor myndighederne var mest modne inden for "Politik for informationssikkerhed" er de nu mest modne inden for "Risikostyring". Myndighederne er næstmest modne inden for områderne "Ledelsessystem for informationssikkerhed" og "Politik for informationssikkerhed". Det er fortsat områderne "Måling, audit og evaluering", "Ressourcer, kompetencer og bevidsthed" og "Leverandørstyring", der udfordrer myndighederne.

Boks 1
Centrale resultater af målingen

- Der er en stigning fra 15 pct. til 35 pct. af myndighederne, der har opnået fuld implementering af standarden ift. 2018.
- Der er fald fra 36 pct. til 19 pct. af myndighederne, der fortsat er langt fra at opnå fuld implementering med et modenhedsniveau på 1 eller 2 på to eller flere områder af målingen ift. 2018.
- 21 pct. af myndighederne har vurderet sig selv lavere i 2019 end i 2018.

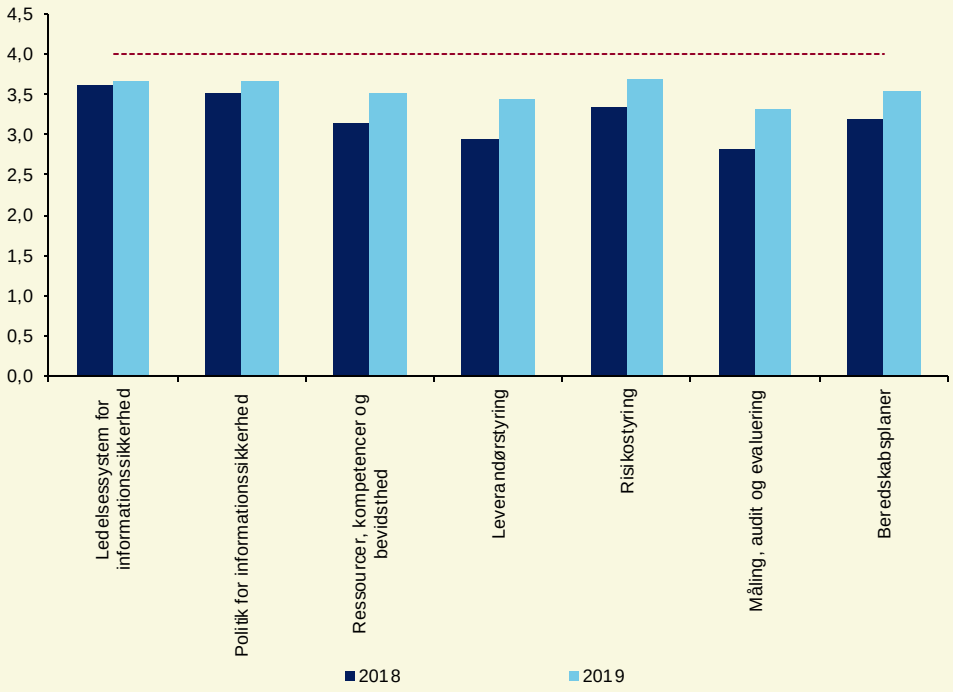
Boks 2
Mest og mindst modne områder

- Myndighederne er mest modne inden for spørgeområderne: "Risikostyring", "Ledelsessystem for informationssikkerhed" og "Politik for informationssikkerhed".
- Myndighederne er mindst modne inden for spørgeområder "Måling, audit og evaluering", "Ressourcer, kompetencer og bevidsthed" og "Leverandørstyring".

Fremgang i implementeringen af standarden i staten

Figur 1 nedenfor viser gennemsnittet af myndighedernes besvarelse fordelt på spørgeområderne i 2018 og september 2019. Det fremgår, at der er sket en fremgang på alle spørgeområder.

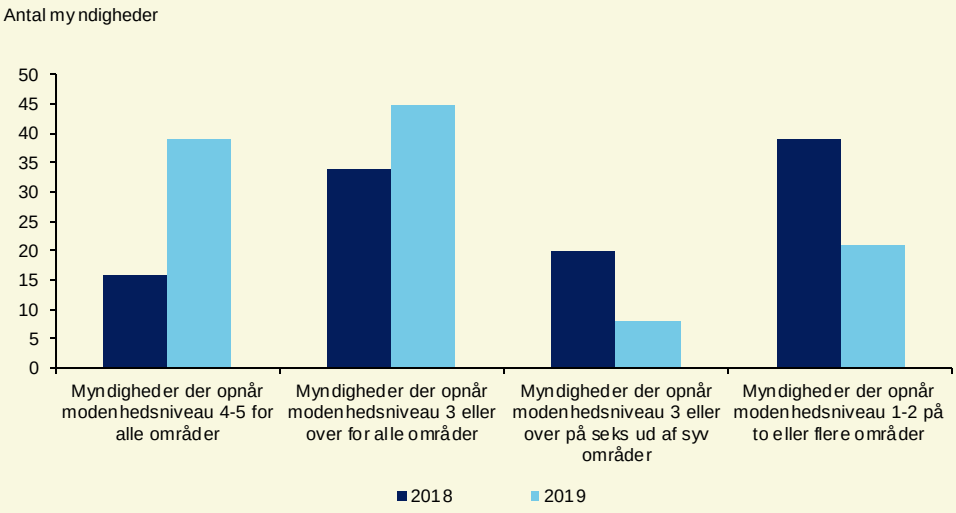
Figur 1
Gennemsnit af myndighedernes besvarelse pr. spørgeområde i 2018 og 2019



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

Figur 2 neden for viser fordelingen af myndigheder på modenhedsniveauer i 2018 og 2019. Det fremgår, at 39 myndigheder har opnået fuld implementering af standarden med modenhedsniveau 4 eller derover på alle områder, mod 16 myndigheder i 2018. 43 myndigheder har opnået mindst niveau 3 på alle områder, mod 34 myndigheder i 2018. Endelig er der et markant fald i antallet af myndigheder, der vurderer sig selv til at ligge på modenhedsniveau 1-2 på to eller flere områder af målingen, med 21 myndigheder i september 2019, mod 39 myndigheder i 2018.

Figur 3
Myndighedernes ISO-modenhed i 2018 og 2019

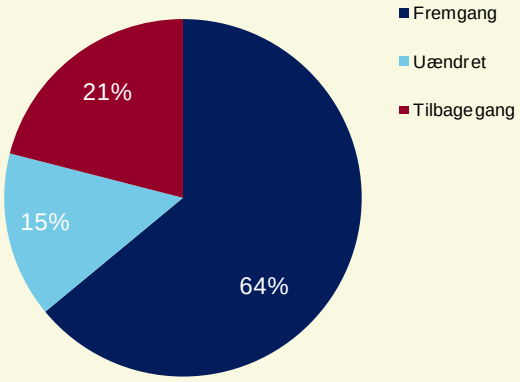


Anm.: Der kan være områder, hvor den enkelte myndighed som følge af en risikovurdering har valgt, at modenhedsniveau 3 er tilstrækkeligt .

Udviklingen i modenheden hos myndighederne

Figur 3 viser den overordnede udvikling i modenheden hos myndighederne fra 2018 til september 2019. Figuren viser, at 21 pct. af myndighederne har nedjusteret deres modenhed i målingen for september 2019 i forhold til målingen for 2018. Efterfølgende dialog med myndighederne tegner et billede af, at det i høj grad skyldes en øget erkendelse af omfanget og kompleksiteten af implementeringen af ISO-standarden. En lavere egen-vurdering kan derfor også ses som et udtryk for en *de facto* modning af myndigheden gennem en mere nuanceret forståelse af de høje krav, der stilles til myndighedernes styring af informationssikkerheden. I tråd med dette har enkelte ministerområder omorganiseret informationssikkerheden, enten ved at samle eller decentralisere indsatser. Omorganiseringen kan ses som en del af det fortsatte arbejde med at højne informationssikkerheden og tilpasse indsatserne til den enkelte organisation, hvilket kan stille krav til politikker eller procedurer, som på ny skal formuleres, implementeres og evalueres. Både den mere nuancerede forståelse af standarden og omorganiseringer har for flere myndigheder medført nedjusteringer af resultatet.

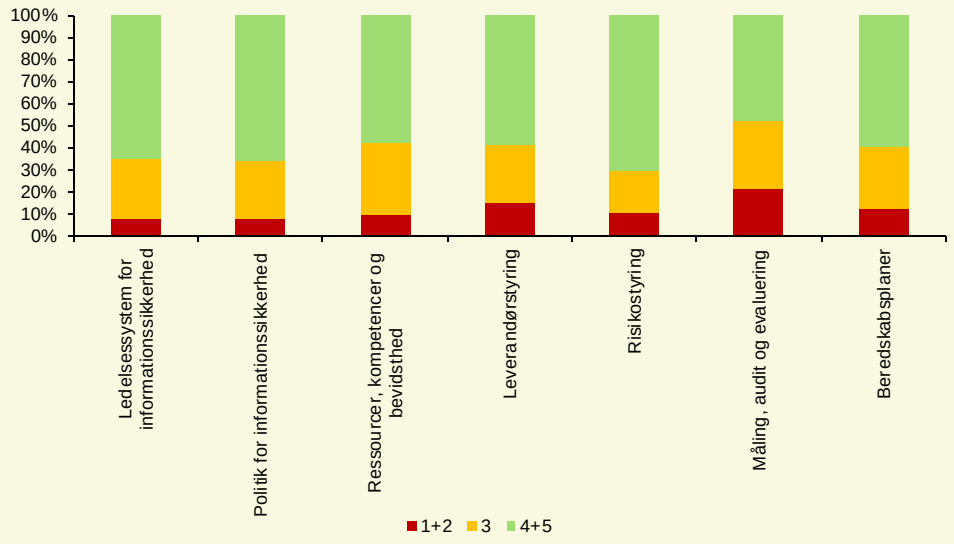
Figur 4
Ændring i modenhed fra 2018 til 2019



Anm.: Figuren vedrører de myndigheder, der både eksisterede i 2018 og 2019.

Standardens implementeringsgrad i staten
Der udestår fortsat et arbejde med implementeringen af standarden 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 5
Fordeling af myndighedernes svar pr. spørgeområde



Figuren viser, at der fortsat udestår et arbejde med at implementere ISO 27001-standarden i staten. Dette gælder særligt områderne "Måling, audit og evaluering", hvor 52 pct. af myndighederne fortsat ikke har opnået fuld implementering af standarden. 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, 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.

Et andet område, hvor der udestår et arbejde, er "Ressourcer, kompetencer og bevidsthed", hvor 43 pct. ikke har opnået fuld implementering af standarden. Dette område dækker ressourceallokeringen fra ledelsen, kompetenceudvikling af medarbejdere og awareness-aktiviteter og skabelsen af en sikkerhedskultur i organisationen. Sidstnævnte opbygges langsomt og kræver et stort engagement fra de informationssikkerhedsansvarlige og ledelsen. Det er samtidig et område, som

styrkes i takt med etableringen af et ledelsessystem og et større organisatorisk fokus på informationssikkerheden.

Endelig er der fortsat 42 pct. af myndighederne, der ikke har opnået fuld implementering af standarden inden for området "Leverandørstyring". Leverandørstyring 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 71 pct. har opnået fuld implementering, "Politik for informationssikkerhed", hvor 66 pct. har opnået fuld implementering, og "Ledelsessystem for informationssikkerhed", hvor 65 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 er der i regi af den nationale strategi for cyber- og informationssikkerhed samt i regi af den fællesoffentlige digitaliseringsstrategi, iværksat en række initiativer. Herunder udarbejdes vejledninger, eksempler og skabeloner, der afholdelse af en årlig ISO bootcamp og der udarbejdes uddannelsespakker til brug for informationssikkerhedskoordinatoren i arbejdet med at hæve informationssikkerheden i organisationen. Endelig oprettes der en uddannelse i informationssikkerhed rettet mod offentligt ansatte og med fokus på ISO implementeringen.

digst.dk