DIGITALISERINGSSTYRELSEN

Hovedresultater: ISO 27001-modenhed i staten

December 2018

2018

Indhold

1. Indledning

Rapporten behandler resultatet af modenhedsmåling af de statslige myndigheders implementering af den internationale informationssikkerhedsledelses-standard ISO 27001.

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 mod 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 standarden fuldt ud. Dog kan der være områder, hvor den enkelte myndighed som følge af en risiko- og væsentlighedsbetragtning har vurderet, at modenhedsniveau 3 er tilstrækkeligt.

Rapporten beskriver henholdsvis resultatet af modenhedsmålingen for 2018 og resultatet af målingen for 2017.

2. Resultat af ISO-målingen for 2018

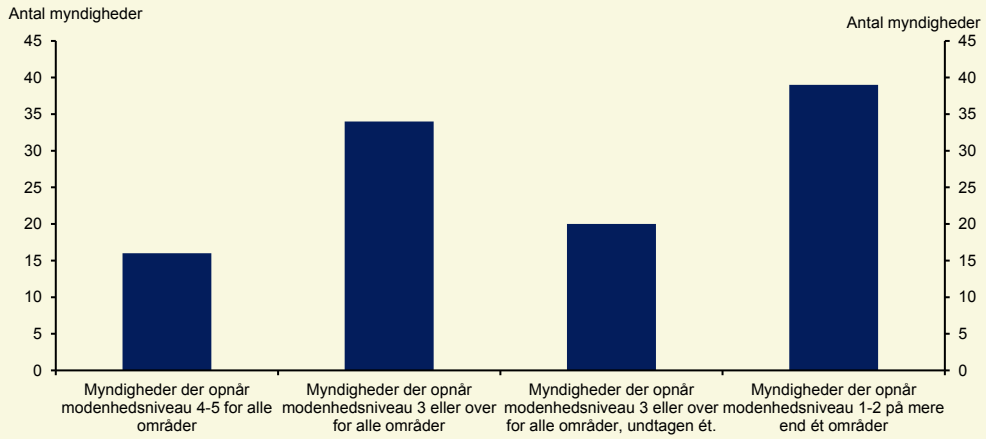
ISO 27001-modenhedsmålingen for 2018 viser, at myndighederne arbejder aktivt med ISO-standardens områder. Dog udestår der fortsat et arbejde med implementeringen af standarden i staten.

Digitaliseringsstyrelsen gennemførte i august en modenhedsmåling af de statslige myndigheder implementering af ISO 27001. Målingen blev besvaret af alle 19 ministerområder og i alt 109 statslige myndigheder. Blandt de 109 besvarelser findes både små og store myndigheder med meget forskellig grad af afhængighed af it-systemer. Behandlingen af resultatet for ISO-målingen 2018 er sket uanset myndighedernes størrelse eller kritikalitet af it- systemerne.

Resultatet af målingen viser, at myndighederne arbejder aktivt med ISO-standardens områder, men at der fortsat er en række udeståender i implementeringen.

Figur 1 viser myndigheders modenhed. Det fremgår, at 16 myndigheder (15 pct.), har implementeret standarden fuldt ud, svarende til niveau 4 eller 5 på alle syv områder. Yderligere er der 34 myndigheder (31 pct.), der har opnået minimum modenhedsniveau 3 på alle syv områder. 20 myndigheder (18 pct.) har opnået modenhedsniveau 3 eller over for alle områder, undtagen ét. Til gengæld er der 39 myndigheder (36 pct.), som fortsat har en modenhed på 1 eller 2 på mere end ét område, og hvor der derfor udestår en væsentlig implementeringsopgave.

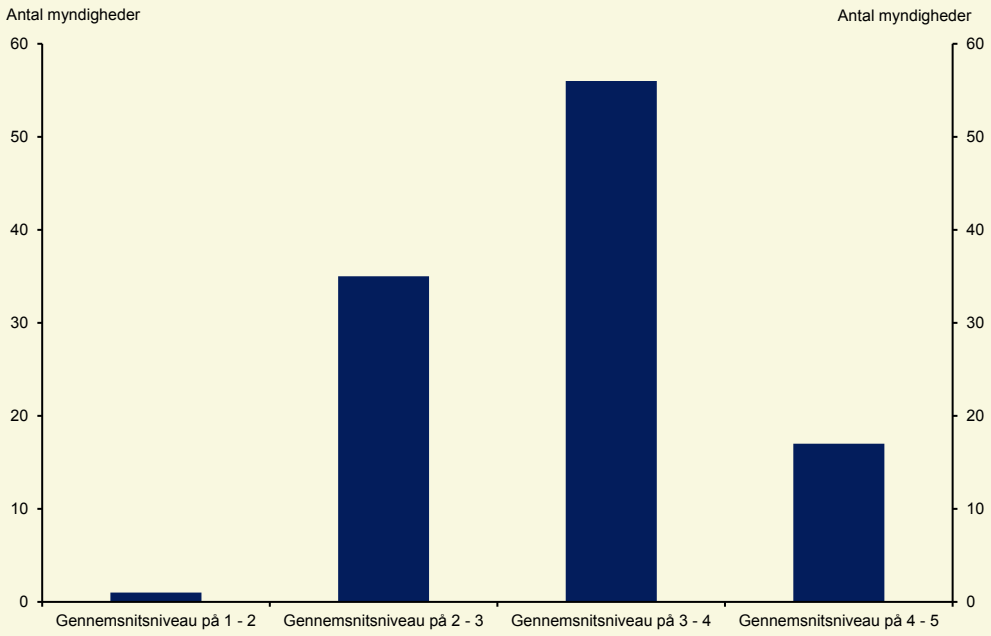
Figur 1
Resultat af ISO-målingen 2018: Myndighedernes modenhed



Der kan være områder, hvor den enkelte myndighed som følge af en risiko- og væsentlighedsbetragtning har vurderet, at modenhedsniveau 3 er tilstrækkeligt.

Figur 2 viser myndighedernes gennemsnitlige modenhed. Det fremgår, at størstedelen af myndighederne, i alt 56 myndigheder (51 pct.), har opnået en gennemsnitlig modenhed på de syv områder på mellem 3 og 4 i målingen, og at yderligere 17 myndigheder (16 pct.) har en gennemsnitlig modenhed på over 4. Til gengæld er der fortsat 36 myndigheder (33 pct.), som har en gennemsnitsmodenhed på under tre, når der ses på tværs af de syv områder.

Figur 2
Resultat af ISO målingen: Myndighedernes gennemsnitsresultat



Der kan være områder, hvor den enkelte myndighed som følge af en risiko- og væsentlighedsbetragtning har vurderet, at modenhedsniveau 3 er tilstrækkeligt.

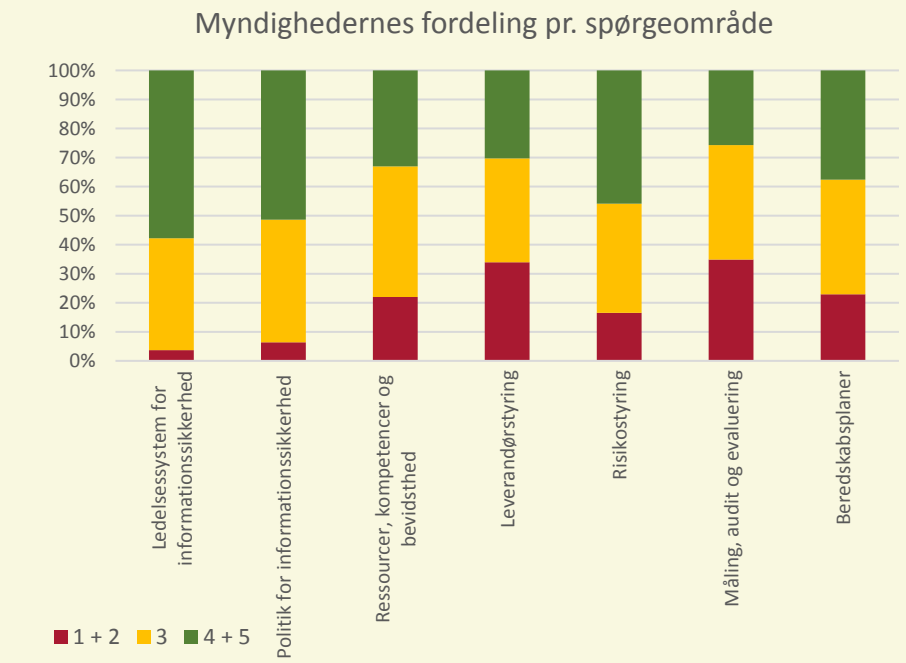
Figur 3 viser modenheden på hvert spørgeområde på tværs af myndighederne, hvor grøn markering svarer til andelen af myndigheder, der har opnået fuld implementering på det givne område, gul svarer til andelen af myndighederne, der nærmer sig fuld implementering, svarende til niveau 3, og rød svarer til andelen, der fortsat er på niveau 1 eller 2.

Figuren viser, at der er den højeste modenhed inden for området "Ledelsessystem for informationssikkerhed", der beskriver it-styringens forankring i ledelsen, hvor 57 procent af myndighederne har implementeret standarden fuldt ud. Til gengæld er der er størst udfordringer på områderne "Måling, audit og evaluering", hvor 74 procent af myndighederne ikke har implementeret standarden fuldt ud, "Leverandørstyring", hvor 70 procent af myndighederne ikke har im-

plementeret standarden fuldt ud, samt "Ressourcer, kompetencer og bevidsthed", hvor 67procent ikke har implementeret standarden fuldt ud.

Figur 3

Fordeling af myndighedernes svar pr. spørgeområde



Der kan være områder, hvor den enkelte myndighed som følge af en risiko- og væsentlighedsbetragtning har vurderet, at modenhedsniveau 3 er tilstrækkeligt.

3. Resultat af ISO-målingen for 2017

I 2017 gennemførte Digitaliseringsstyrelsen en ISO 27001-modenhedsmåling i regi af Den fællesoffentlige digitaliseringsstrategi. Resultatet af målingen viste i lighed med resultatet af målingen fra 2018, at der udestår et arbejde med implementeringen af ISO-standarden.

I 2017 gennemførte Digitaliseringsstyrelsen en ISO 27001-modenhedsmåling i regi af den fællesoffentlige digitaliseringsstrategi. 84 statslige myndigheder gennemførte målingen.

Målingen viste, at myndighederne var kommet godt i gang med arbejdet med informationssikkerhed og implementeringen af ISO-standarden, herunder at der var et godt ledelsesfokus og støtte til arbejdet med informationssikkerhed i organisationerne. Målingen viste samtidig et behov for øget fokus på fire områder: Risikovurderinger, leverandørstyring og beredskabsplaner samt retningslinjer for måling af informationssikkerhed og dermed mulighed for evaluering og forbedring. Endelig viste 2017-målingen, at der var stor spredning i ISO-modenheden hos myndighederne.

Resultatet af 2017-målingen er ikke direkte sammenlignelig med målingen for 2018. Begge målinger omhandler ISO-standarden og behandler til dels de samme spørgeområder, men spørgsmålene og metoden, hvorpå der spørges ind, har ændret sig. Ændringerne skyldes især et ønske om at gøre målingen for 2018-2021 mere vejledende og understøttende for myndighederne i deres arbejde med implementeringen. Derfor er målingen for 2018 suppleret med uddybende spørgsmål for hvert spørgeområde.

digst.dk