Resultatet af undersøgelse af status på implementering af ISO27001-principper i staten

2017

INDHOLD

RESULTAT AF MÅLING AF IMPLEMENTERINGSGRADEN AF ISO27001-PRINCIPPER

INDLEDNING
INDHOLD, FORMÅL OG METODE

Indhold og formål

Dette materiale konkluderer på resultatet af undersøgelse af status på implementering af ISO27001-principper i staten.
Spørgerammen bygger på best practise og har taget udgangspunkt i de fire sikkerhedstiltag fra ”Cyberforsvar der virker” samt de fællesoffentlige målepunkter defineret i regi af den fællesoffentlige digitaliseringsstrategi (FODS) initiativ 7.1.

Formålet med spørgerammen er at skabe overblik over tilstanden på informationssikkerheden i staten og identificere forbedringstiltag, som understøtter yderligere forhøjelse af informationssikkerhedsniveauet.

Metode – et generisk rammeværk

Konklusionen er baseret på kvalitative og kvantitative analyser af data genereret igennem et generisk spørgeskema.

Analysen og spørgerammen har været en selvevaluering. Dette for at danne det mest realistiske indblik i de respektive organisationers tilstand. Ydermere er metoden og spørgerammen generiske med henblik på fremadrettet brug. Dette er fordelagtigt for at monitorere og spore forbedringen af informationssikkerheden i ministerierne.

Spørgeskemaet er udsendt til alle statens departementer. Tidsrammen for svar af spørgeskemaet har været tre uger. 87 myndigheder har responderet på spørgeskemaet.

KONKLUSION AF UNDERSØGELSE

SAMMENFATNING AF SPØRGERAMMENS TRE AFSNIT

God ledelsesstøtte men stor spredning i modenhed på flere målepunkter

Resultatet af målingen bekræfter, at der er stor spredning på modenheden i arbejdet med informationssikkerhed. Der er en stor andel af respondenter (67%) som anser ledelsesstøtten til at være god (modenhedstrin 3 og 4), hvilket bekræftes af, at der er få, som indikerer, at her findes udfordringer.

Forbedringsmuligheder findes

I forhold til forbedringsmuligheder viser målingen, at særligt arbejdet med risikovurdering og leverandørstyring er mindre modent og opfattes generelt som mere vanskeligt arbejde. Særligt her ønskes også mere ekstern støtte og vejledning. Til denne kategori kan også arbejdet med beredskabsplaner tilføjes, hvor særligt øvelser og test af disse vurderes som udfordrende.

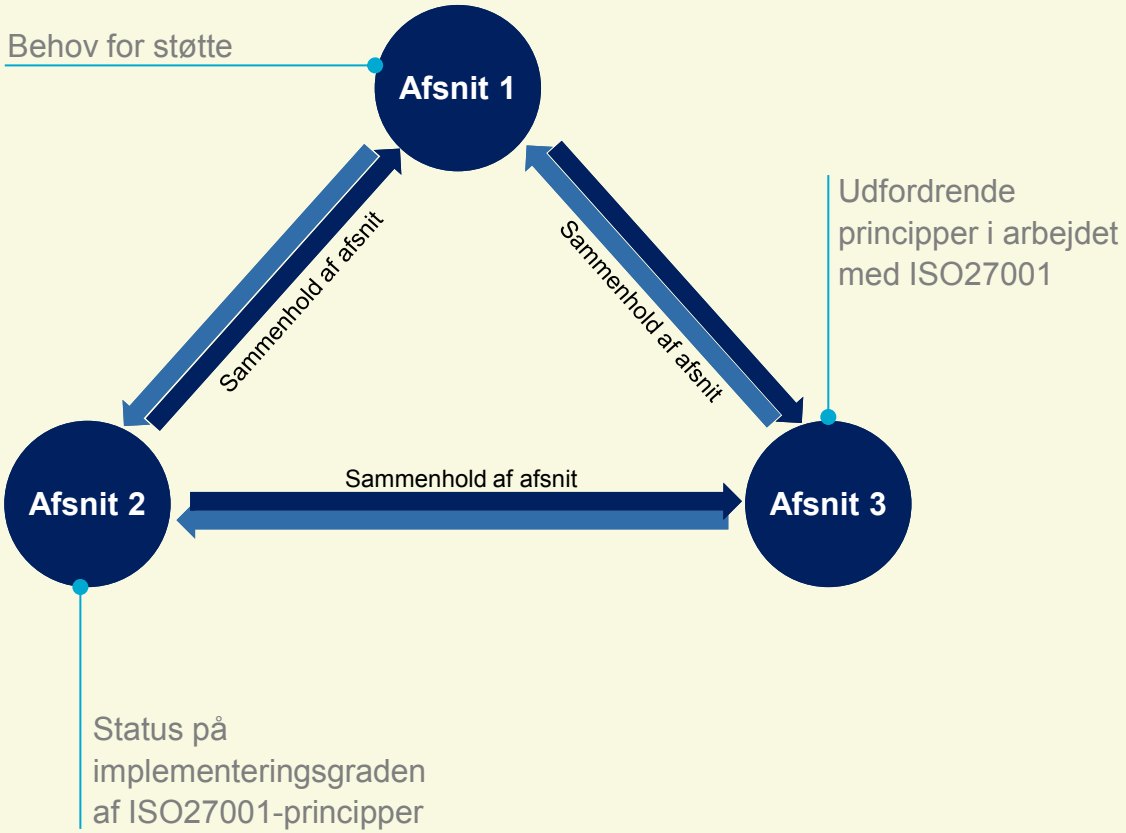
En anden vigtig konklusion fra målingen er, at få af respondenterne vurderer, at de fuldt udfører evaluering og opfølgning på informationssikkerhedsarbejdet. Eksempelvis er der meget få, som evaluerer det faktiske awareness-niveau i organisationen. Relateret til dette peger målingen også på, at arbejdet med planer for sikkerhedsaktiviteter er umodent.

Behov for støtte

Der er identificeret et stort behov for ekstern støtte på tværs af alle måleområder, hvilket understøttes af spredningen i svarene i afsnit 2 (modenhed) og afsnit 3 (udfordringer).

OMRÅDER MED BEHOV FOR STØTTE ER GENNEMGÅENDE I SPØRGERAMMENS TRE AFSNIT

METODE: SAMMENHOLD AF SPØRGERAMMENS TRE AFSNIT



Aggregeret og nuanceret status

Svarene er blevet aggregeret således, at de afdækker behovet for støtte på baggrund af de mest almindelige udfordringer

Ligeledes er svarene sammenholdt for at skabe en mere nuanceret konklusion samt for at identificere, hvilket områder der er gennemgående i de tre afsnit

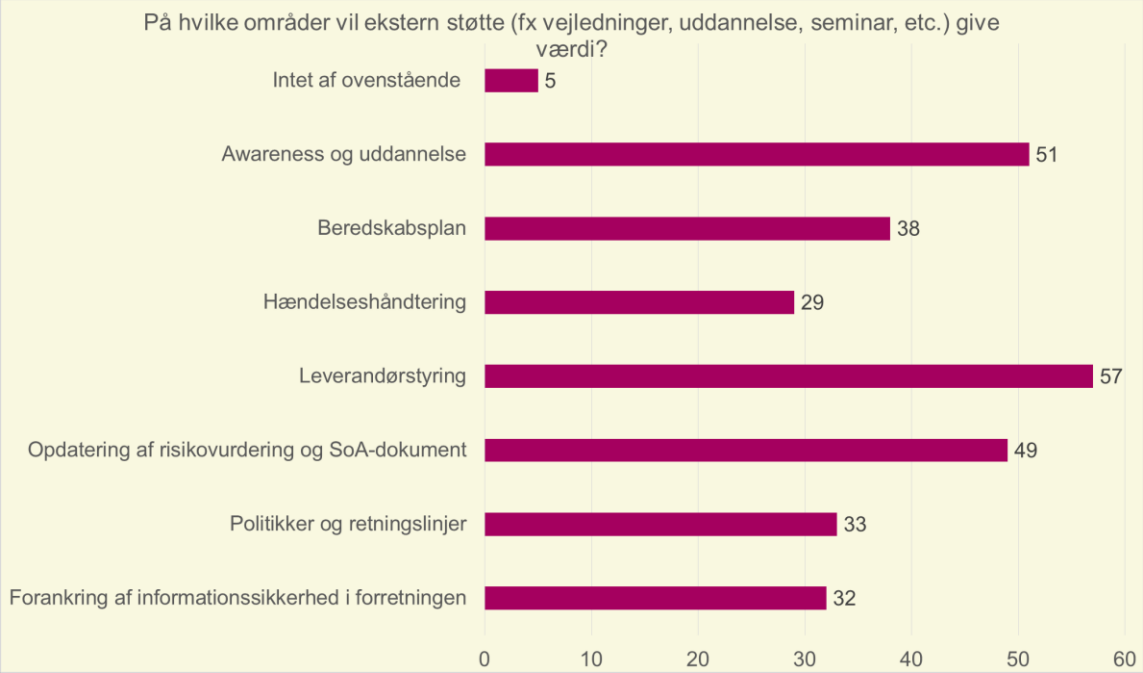
Spørgerammen har haft til formål at afdække status, herunder hvad organisationen finder vanskeligt, og derfor har spørgsmålene en mere overordnet best-practice-karakter og bygger på selvevaluering.

RESULTAT
FRA UNDERSØGELSE

RESULTAT

EKSTERN STØTTE VED FLERE PUNKTER EFTERLYSES AF MERE END 56% AF RESPONDERNE

AFSNIT 1: ORGANISATIONENS BEHOV FOR FORBEDRENDE TILTAG OG EKSTERN STØTTE



Antal respondenter: 87

"…er modenhedsmæssigt et sted, hvor der mindre er brug for generelle vejledninger eller skabeloner, men konkrete cases og erfaringer eller workshops."

Kommentar fra respondent

Behov for støtte på tværs af punkter

- På tværs af alle områder påviser selvevalueringen et behov for ekstern støtte for at sikre et højt informationssikkerhedsniveau
- 51 af alle respondenter vurderer, at der er behov for ekstern støtte mht. "Awareness og uddannelse" For "leverandørstyring" og "Opdatering af risikovurdering og SoA-dokument" er det hhv. 57og 47
- **5 respondenter har i selvevalueringen vurderet, at ekstern støtte ikke vil være værdiskabende** på nogle af de angivet områder.

STOR SPREDNING I MODENHED PÅ TVÆRS AF DE OTTE IDENTIFICEREDE PUNKTER

AFSNIT 2: STATUS PÅ IMPLEMENTERINGSGRADEN AF ISO27001-PRINCIPPER

	Organisationen har ikke opnået nogen af nedenstående trin	Definering af principper og processer	Implementering af principper	Eksekvering som konsekvens af principper	Evaluering af efterlevelse af effektivitet (evaluering og opfølgning)
Forankring af informationssikkerhed i forretningen	1%	7%	24%	28%	40%
Politikker og retningslinjer	3%	6%	37%	25%	29%
Leverandørstyring	13%	26%	30%	18%	13%
Hændelseshåndtering	3%	9%	15%	41%	31%
Beredskabsplan	11%	14%	44%	17%	14%
Awareness og uddannelse	10%	6%	29%	21%	34%
Opdatering af risikovurdering og SoA-dokument	7%	29%	25%	17%	22%
Planer for sikkerhedsaktiviteter	43%	15%	18%	11%	13%

Moden proces med forbedringsmuligheder

Spørgerammen indikerer relativ god ledelsesmæssigt fokus og forankring

Ved flere punkter er der stor spredning på tværs af de fire trin.

Områder med relativ lav modenhed:

- Beredskabsplan
- Leverandørstyring
- Opdatering af risikovurdering og SoA-dokument

Største behov for indsats er ”Planer for sikkerhedsaktiviteter”, hvor 43% har indikeret, at organisationen er på laveste modenhedsniveau.

BEHOV FOR STØTTE, MODENHED OG UDFORDRINGER

AFSNIT 3: UDFORDRINGER VED ARBEJDET MED INFORMATIONSSIKKERHED

Adspurgt har respondenterne peget på leverandørstyring, som det højest prioriterede indsatsområde:

Flest respondenter har disse opgaver som de højest prioriterede

- Validering af leverandørers overholdelse af krav
- Definition af kravspecifikation til leverandører

Og følgende som mest udfordrende områder:

Flest respondenter har prioriteret disse udfordringer som de største

- Risikovurdering
- Opdatering af instrukser samt kontroller
  Validering af leverandørs overholdelse af krav
- Øvelser og test af interne beredskabsplaner
- Eksekvering af kontroller og tiltag
- Definition af kravspecifikation til leverandører
- Tilstrækkelig tid afsat til arbejdet med informationssikkerhed

Gennemgående udfordringer

Mens den ledelsesmæssige opbakning er moden og synlig i organisationen, er nedenstående områder mere udfordrende:

- Arbejdet, der knytter sig til leverandører; kravspecifikation og validering af overholdelse af krav
- Øvelser og test af beredskabsplaner
- Risikovurderinger og opdatering af instrukser samt kontroller
- Tilstrækkelig tid afsat til arbejdet med informationssikkerhed

Delkonklusioner er baseret på de punkter, som en overvejende stor andel respondenter har identificeret som mest udfordrende. Dette er for at identificere synergi på tværs af alle tre afsnit samt fælles udfordringer.

KONKLUSION

OG FORBEDRINGSMULIGHEDER I ARBEJDET MED IMPLEMENTERING AF ISO27001-PRINCIPPER

KONKLUSION AF UNDERSØGELSE

FIRE TING AT HUSKE

Stor spredning i modenhed, hvor halvdelen af svarene er placerede på trin 3 og 4 på tværs af kategorier	Resultaterne af undersøgelsen peger på, at der er stor spredning i modenhed og hvilke udfordringer respondenterne står overfor. Dog er ca. halvdelen af svarene placererede på trin 3 og 4 i modenhedsskalaen på tværs af kategorier
Stort ønske om ekstern støtte i arbejdet med informationssikkerhed og særligt inden for kritiske områder	Der findes et stort ønske om ekstern støtte til arbejdet med informationssikkerhed. Behovet findes på tværs af alle måleområder. Dog indikerer analysen af alle tre afsnit sammenholdt, at der findes et særligt stort behov for støtte inden for risikovurdering, leverandørstyring, beredskabsplanlægning og planlægning for sikkerhedsaktiviteter
Generelt god ledelsesfokus og støtte til arbejdet med informationssikkerhed i organisationerne	Graden af implementering af informationssikkerhed er i høj grad afhængig af ledelsesfokus. Det målte modenhedsniveau tyder på, at der generelt er fokus på informationssikkerhed. Det bliver også bekræftet i undersøgelsen, hvor ledelsesstøtte er prioriteret som mindst udfordrende at få gennemført. Dog findes der organisationer, hvor der kan fokuseres mere på ledelsesstøtte
Lav modenhed i evaluering og opfølgning samt planlægning af sikkerhedsaktiviteter	Mange respondenter svarer, at de delvist evaluerer og følger op på den reelle informationssikkerhed. Dog indikerer analysen, at der er udfordringer og mangler på dette område. Desuden er der lav modenhed i planlægning af sikkerhedsaktiviteter, hvilket også er et vigtigt aspekt, når den reelle informationssikkerhed skal vurderes

FORSLAG TIL FORBEDRENDE TILTAG OG STØTTE

FOKUS PÅ KONKRETE VÆRKTØJ OG VEJLEDNINGER

Resultatet fra undersøgelsen kan bruges til at vurdere, hvor støtte vil have størst værdi i forhold til informationssikkerhed i Danmark. Fra undersøgelsen kan der konkluderes, at der er et ønske om konkrete vejledninger på en række områder. Det anbefales, at resultatet gennemgås i detaljer som baggrund for udviklingen af vejledende materiale. Nedenfor følger nogle eksempel på støtte, som kunne forbedre arbejdet.

Måleområde		Eksempel på støtte og konkrete vejledninger
Leverandørstyring	Etablering af kravspecifikation	• Proces for, hvordan en organisation kan opsamle kravene • Eksempel på lessons learned i f.h.t. kravspecifikation til leverandører
	Opfølgning af efterlevelse af krav	• Proces for, hvordan en organisation kan følge op på leverandørens overholdelse af krav • Eksempel på konkrete sager relateret til emnet
Beredskabsplaner	Øvelser og test	• Eksempel på, hvordan rollespil kan bruges til test af beredskab
Awareness	Evaluering af det reelle awareness-niveau	• Eksempel på effektiv vedligeholdelse af awareness • Indikatorer som afsløre awareness-niveau i organisationen
Opdatering af risikovurdering og SoA-dokument	Risikovurdering og håndtering	• Værktøjer og eksempel på risikoprocesser • Projektværktøjer
Planer for sikkerhedsaktiviteter	Punkter for måling	• Konkret vejledning for, hvordan en organisation kan evaluere den reelle informationssikkerhed ved at måle på en række punkter • Eksempel på værktøjer for måling af en række almindelige digitale, fysiske og menneskelige kontroller