




Erfaring



Erfaringer fra implementeringen af DS 484
Standard for informationssikkerhed i statslige organisationer



IT- og Telestyrelsen
Ministeriet for Videnskabs
Teknologi og Udvikling



Erfaringer fra implementeringen af
DS 484 Standard for
informationssikkerhed i statslige
organisationer

Udgivet af:
IT- & Telestyrelsen

IT- & Telestyrelsen
Holsteinsgade 63
2100 København Ø

Telefon: 3545 0000
Fax: 3545 0010

Erfaringer fra implementeringen af DS 484 Standard for informationssikkerhed i statslige organisationer

Rapport udarbejdet af Dansk Standard
for IT- og Telestyrelsen

Indhold

>

1	Forord	5
2	Baggrund og formål	6
2.1	Rapportens opbygning	6
3	Konklusioner	8
3.1	Politikker, planer og procedurer	8
3.2	Fremgangsmåde og metode	8
3.3	Kompetencer og forudsætninger	10
3.4	Ansvar og beføjelser	11
3.5	Målsætning og opfølgning	12
3.6	Opmærksomhed og kommunikation	13
4	Anbefalinger	15
5	Datagrundlag og metode	17
5.1	Datagrundlag	17
5.2	Metode	17
5.2.1	Dataindsamling	17
5.2.2	Databearbejdning og analyse	18
6	Analyse af interviewresultaterne	19
6.1	Indledende generelle spørgsmål	19
6.2	Organisering og forberedelse	22
6.3	Strategi og politik for informationssikkerhed	26
6.4	Projektorganisering	28
6.5	Gennemførelse af implementeringen	29
6.6	Informationsaktiver og informationsejere	32
6.7	Risikoanalyse og beredskab	35
6.8	Awareness	39
6.9	Opfølgning på implementeringen	43
	Bilag 1: Interviewguide og spørgeramme	48
	Bilag 2: Indledning i DS 484 standarden	50
6.10	Hvad er informationssikkerhed?	50
6.11	Hvorfor er informationssikkerhed nødvendig?	50

1 Forord

>

Dansk Standard har for IT- og Telestyrelsen gennemført en kvalitativ interviewundersøgelse blandt statslige organisationer for at tage temperaturen på, hvordan implementeringen af DS 484:2005 Standard for informationssikkerhed er gået¹. Denne rapport opsamler og analyserer de erfaringer, man har gjort, sådan som de er kommet til udtryk under interviewene.

¹ Informationssikkerhed defineres som den samlede mængde af beskyttelsesforanstaltninger, der skal sikre virksomhedens daglige drift, minimere skader, beskytte virksomhedens investeringer og sikre grundlaget for nye forretningsmuligheder, se også Bilag 2.

2 Baggrund og formål

>

Økonomiudvalget tilsluttede sig den 12. januar 2004 Videnskabsministeriets anbefaling om at gøre det obligatorisk for statens institutioner at følge en fælles standard for informationssikkerhed. Udgangspunktet skulle være de basale krav i DS 484:2005 Standard for informationssikkerhed. Det satte et stort arbejde i gang i de statslige organisationer, og de har over de sidste 3-4 år høstet en mængde erfaringer.

En standard som DS 484 implementeres ikke via et enkelt gennemløb af en udvalgt implementeringsproces. Det kræver etablering af en tilbagevendende proces, der sikrer, at man hele tiden optimerer processer, organisation og tekniske foranstaltninger for at tilpasse arbejdet med informationssikkerheden til det stadigt foranderlige risikobillede.

Undersøgelsen har haft til formål:

- at opsamle de erfaringer, der er gjort på tværs af de statslige organisationer, til brug for det videre arbejde med overholdelse af kravene i DS 484
- at formidle disse erfaringer til gavn og inspiration for alle offentlige institutioner, da også mange kommuner og regioner arbejder med at indføre standarden
- at evaluere de anvendte metoder, organisationsformer, værktøjer og øvrige implementeringstiltag for at afdække dels bedste praksis, dels eventuelle behov for forbedringer og andre tilgange til implementeringen af informationssikkerhed.

2.1 Rapportens opbygning

I rapportens **Bilag 1** gengives den interviewguide og spørgeramme, som interviewundersøgelsen har taget udgangspunkt i.

Spørgerammen har to dimensioner: Områder og Emner. Områderne kan ses som hovedoverskrifter på de spørgsmål, der blev stillet, mens spørgerammens emner svarer til de temaer, man gennemgående ville have fokus på.

Rapportens konklusioner (kap. 3) og dens analyseafsnit (kap. 6) er struktureret ud fra disse to dimensioner.

Kap. 3 præsenterer konklusionerne baseret på de gennemførte interview og den efterfølgende databearbejdning og analyse. Kapitlet er bygget tematisk op efter spørgerammens emner, jf. Bilag 1: spørgerammens horisontale dimension. De enkelte temaer med tilhørende opsummeringer og konklusioner

ledsages af nogle udledte anbefalinger til inspiration for andre, der arbejder med informationssikkerhed.

Kap. 4 samler rækken af anbefalinger - baseret på konklusionerne og den bedste praksis, der kan udledes af interviewundersøgelsen, jf. kap. 3 – i en liste, der angiver et naturligt projektførløb ved implementering af informationssikkerhed.

Kap. 5 gør rede for undersøgelsens datagrundlag og metode.

Kap. 6 rummer analysen, der dykker ned i spørgerammens områder (jf. Bilag 1: spørgerammens vertikale dimension) og tager fat i svarene på de enkelte spørgsmål. Analysen danner belæg og grundlag for de udledte konklusioner og anbefalinger i kap. 3.

Analysen er krydret med en hel del citater fra interviewene, udvalgt som selvforklarende og sigende læsefrugter.

Begrebet 'informationssikkerhed' belyses kort i **Bilag 2**, hvor de første afsnit af DS 484:2005 standardens kap. 0 gengives: 0.1 Hvad er informationssikkerhed? og 0.2 Hvorfor er informationssikkerhed nødvendig?

Rapporten er opbygget som et samlet hele og kan læses som et sådant.

Men det er også tanken, at man fx kan nøjes med at læse kap. 1-3, hvis man har behov for et hurtigt indblik i undersøgelsen og dens resultater. Mens man kan gå videre til analysen, hvis man er yderligere interesseret. Man skal også afhængigt af behov kunne foretage punktnedslag i rapporten, fx kan en projektleder her og nu have gavn af at slå op på listen over anbefalinger i kap. 4.

I et forsøg på at imødekomme de forskellige behov har det været nødvendigt at indarbejde visse gentagelser undervejs i rapporten.

3 Konklusioner

>

Konklusionerne i dette kapitel er struktureret ud fra spørgerammens emner, dvs. de temaer undersøgelsen overordnet har haft fokus på, jf. Bilag 1: spørgerammens horisontale dimension.

De enkelte temaer med tilhørende opsummeringer og konklusioner ledsages af nogle udledte anbefalinger til inspiration for andre, der arbejder med informationssikkerhed. En samlet liste over disse anbefalinger findes i kap. 4.

3.1 Politikker, planer og procedurer

I de allerfleste af organisationerne startede man implementeringen fra bunden af. Man havde ikke eller havde kun delvis sikkerhedsstrategier og –politikker, ligesom der typisk ikke fandtes en informationssikkerhedsorganisation i forvejen.

Organisationerne havde kun i få tilfælde en delvis komplet oversigt over informationsaktiver at tage udgangspunkt i, og man stod også på bar bund i forbindelse med dokumenterede nød- og beredskabsplaner.

Ingen af de mindre organisationer indgår i det mindretal, der faktisk havde sikkerhedsstrategier og –politikker. Flere af de mindre organisationer havde heller ikke en sikkerhedsorganisation, hverken før eller efter projektet.

Det anbefales, at man:

- Sikrer sig ledelsens fokus
- Etablerer en informationssikkerhedsorganisation, der også kan tage over, når projektet overgår til drift

3.2 Fremgangsmåde og metode

Der er tilsyneladende ingen, som har gennemført en foranalyse forud for selve projektet. Der er heller ingen, der har foretaget en cost benefit vurdering i kølvandet på risikoanalysen. Man har med andre ord ikke systematisk vurderet omkostningerne og prioriteret eventuelle foranstaltninger til imødegåelse af de identificerede risici.

For temmelig mange har manglen på foranalyse og på cost benefit vurdering bl.a. betydet, at projektets omfang - med hensyn til indhold, tid, ressourcer og økonomi - er kommet bag på dem.

For manges vedkommende har der ikke været anvendt nogen specifik arbejds metode til gennemførelse af projektet.

De, der har haft en mere struktureret og metodisk tilgang, har bl.a. gjort brug af projekt- og arbejdsgrupper, workshops med undervisning og hands on,

implementeringsudvalg, skabeloner, informationsmøder og vejledninger. De har således haft fokus på det pædagogisk formidlende og forankrende aspekt i projektet. Og det er derfor ikke overraskende, at hovedparten af disse organisationer har deres rod i forsknings-, uddannelses- og kulturverdenen.

Som løftestænger for projektet nævner flere:

- Økonomiudvalgets beslutning
- IT- og Telestyrelsens benchmark-undersøgelse
- Rigsrevisionens besøg

Beslutningen fra centralt hold om at implementere DS 484 har hjulpet projektet på vej ved at gøre diskussioner overflødige: man skulle det her. Benchmark-resultaterne og Rigsrevisionens besøg har været motiverende og skærpende faktorer og øjenåbnere ikke mindst for ledelsen. Begge dele har bidraget til at sikre ledelsens fokus på projektet.

De fleste af organisationerne har benyttet ekstern konsulentbistand i dele af projektførelsen. Det skal dog bemærkes, at dette kun gælder halvdelen af de mindre organisationer.

Selve standarden DS 484 betragtes som et nyttigt redskab, som en god, uundværlig manual i processen.

Brugen af et it-værktøj dedikeret til arbejdet med informationssikkerhed har derimod ikke i sig selv givet et løft til implementeringen. Tværtimod synes det at have været en hæmsko i forbindelse med både risikoanalysen og gennemførelsen af kampagner og test.

En del af organisationerne nævner eksplicit ITIL² som noget, der et langt stykke hen ad vejen går hånd i hånd med informationssikkerhed, og at metoderne gensidigt beriger hinanden. Ved at integrere arbejdet med informationssikkerhed og ITIL har man fået forbedret sine it-processer.

Med hensyn til risikoanalysen giver mange udtryk for, at de har haft en forretningsmæssig tilgang til denne med deltagelse af system- og dataejerne. Disse ejerskaber har typisk været placeret i forretningen og ikke i it-afdelingen. Desuden er man gået pragmatisk til værks og har brugt sin egen risikovurderingsmodel afstemt efter situationen. Det har dog ikke nødvendigvis

² ITIL: IT Infrastructure Library. En samling anbefalinger af, hvordan man bedst driver sin it-virksomhed. Et internationalt anerkendt bedste praksis-rammeverk for it-leverancer og – services.

>

været nemt at få taget hul på risikoanalysen, og det er bl.a. i denne sammenhæng, man har brugt ekstern konsulenthjælp.

Hvad angår opfyldelsen af kravene i DS 484, har langt de fleste indgået kompromisser undervejs. Det kan igen tages som udtryk for den pragmatiske tilgang, om end den har været mere eller mindre 'frivillig'. Man har været nødt til at gå på kompromis på områder som fx kravet om logning. Og især de mindre organisationer har haft svært ved at opfylde kravet om funktionsadskillelse. Med få ansatte må man leve med, at samme person har flere roller.

Det anbefales, at man:

- Sikrer sig ledelsens fokus
- Udarbejder en foranalyse med henblik på at bedømme opgavens indhold og vurdere omfanget i tid, ressourcer og økonomi
- Organiserer projektet med en projektgruppe, evt. i form af et sikkerhedsudvalg, og en styregruppe. Det hjælper på forankringen af informationssikkerhed i organisationen, stor som lille, når projektet ikke kører isoleret fra den
- Fokuserer mindre på at anvende et it-værktøj til informationssikkerhed og mere på at planlægge implementeringen og procesoptimeringen
- Definerer, identificerer og forankrer ejerskab til informationsaktiverne
- Foretager en cost benefit vurdering i tilknytning til risikoanalysen
- Får samlet op på risikoanalysen og holder ledelsen fast på at drage konklusioner ud fra den

3.3 Kompetencer og forudsætninger

Forståelsen af projektbegreber som 'foranalyse' og 'cost benefit vurdering' forekommer at være uklar. Og man har som nævnt tilsyneladende hverken gennemført en foranalyse forud for projektet eller en cost benefit vurdering i forbindelse med risikoanalysen.

Jf. ovenfor betragter mange selve standarden DS 484 som et nyttigt, uundværligt redskab. Samtidig er det påfaldende, hvor enslydende kommentarerne er om, hvordan det har været at arbejde med dens ordlyd. Man har oplevet den som vanskelig og tung at gå til, hvad angår både dens terminologi og dens struktur. Den har været svær at læse, svær at forstå og derfor også svær at formidle. Det har fx været vanskeligt at skulle arbejde med et begreb som 'ejerskab'.

I forlængelse af, at man har haft problemer med at forholde sig til teksten, og i det hele taget har haft svært ved at spore sig ind på projektets omfang og indhold, jf. også afsnit 3.2, giver man udtryk for, at man har savnet hjælpeværktøjer i form af konkrete, operationelle vejledninger, standard

>

skabeloner og paradigmer, praktiske køreplaner og eksempler til brug for projektet.

Dette sammenholdt med, at organisationerne indledningsvis stod på bar bund i projektet, jf. afsnit 3.1, gør, at forudsætningerne for at starte projektet må siges at have været ringe.

Flere af de mindre organisationer har følt standardens omfang som en belastning og kunne godt have tænkt sig, at den var fleksibel og kunne tilpasses i forhold til organisationens størrelse.

Det anbefales, at man:

- Genbruger, hvad andre har haft gavn af, fx låner sig frem til skabeloner og andre hjælpeværktøjer
- Udveksler erfaringer med andre, fx Hvad gik godt? Hvorfor? Hvilke faldgruber skal man forsøge at navigere udenom?

3.4 Ansvar og beføjelser

Flertallet af organisationerne har udført projektet i it-afdelingens regi, ligesom majoriteten af interviewpersonerne har eksplicit tilknytning til it. De, der udtaler sig om betydningen af projektets placering, siger enten, at det ikke skulle have ligget i it's regi, eller at det var positivt, at det ikke blev et it-projekt.

Men der er også i interviewundersøgelsen eksempler på, at det er den forretningsorienterede holdning og tilgang til projektet, der er det afgørende. Dvs. at det er muligt at undgå, at det bliver et rent 'it-projekt', også selv om det er placeret i it-afdelingen.

Der er ikke nogen nævneværdige kommentarer til spørgsmålet om, hvorvidt man havde de nødvendige beføjelser i forhold til ansvaret for projektet. Det kan hænge sammen med det gennemgående træk, at projektlederen har trukket et stort læs enten helt alene eller i samarbejde med få andre. Der tales om 'lonely rider', enmandsopgave og enmandshær.

Til gengæld er der en lille overvægt, der svarer, at de fik de nødvendige ressourcer, herunder også ekstern hjælp. Samtidig mener hovedparten, at der ikke blev allokeret den fornødne tid til projektdeltagerne. I den kategori ses igen en del af de mindre organisationer. Man kan altså have fået tildelt de nødvendige ressourcer i form af fx økonomi og personer, og samtidig have oplevet, at personerne – projektdeltagerne – ikke har fået tilstrækkelig tid til projektarbejdet.

Det anbefales, at man:

- Får allokeret nødvendige ressourcer og fornøden tid
- Fokuserer på at have en forretningsorienteret - og ikke en snæver it-mæssig - tilgang til sikkerhed

3.5 Målsætning og opfølgning

Det er væsentligt at hæfte sig ved, at alle giver udtryk for, at arbejdet med informationssikkerhed har været umagen værd. Det har ganske vist haft sin pris, men ingen siger, at prisen har været for høj i forhold til udbyttet.

Svarene på spørgsmålet om, hvordan man har oplevet selve implementeringsprocessen, fordeler sig nogenlunde ligeligt mellem dem, der har oplevet processen som svær og tung, og dem, der ser meget positivt på den. Det er bemærkelsesværdigt, at de mindre organisationer udtrykkeligt nævner deres størrelse, som årsag til at processen har været tung for dem. Og de understreger, at det har givet dem mere arbejde.

Men uanset hvordan man har oplevet processen, så peger man entydigt på disse resultater som de væsentligste udbytter:

- Bevidsthed, erkendelse, opmærksomhed
- Forbedring af sikkerhed, struktur på processer, dokumentation
- Ledelsesforankring og -fokus

Den øgede forståelse, erkendelse og opmærksomhed går hånd i hånd med det forbedrede, strukturerede sikkerhedsarbejde og dermed det højnede sikkerhedsniveau.

Langt hovedparten af de ændringer og tilpasninger, man har foretaget i kølvandet på arbejdet med informationssikkerhed, omfatter arbejdsprocesser og -procedurer. Det drejer sig ikke så meget om it-mæssige ændringer.

Flere udtaler, at de i virkeligheden gjorde mange af tingene i forvejen, men at sikkerhedsarbejdet er blevet mere struktureret, formaliseret og bevidst med DS 484 som løftestang, krumtap og manual.

Og både det at få kortlagt informationsaktiverne og det at få gennemført en risikoanalyse har for mange haft stor værdi og medført konkrete og håndgribelige resultater.

Det er også værd at bemærke, at relativt mange har oplevet ledelsesforankringen som et væsentligt udbytte hen ad vejen.

De allerfleste er opmærksomme på at følge op på implementeringen. Man tænker i vedligeholdelse og nævner et bredt spektrum af virkemidler til det formål. Set udefra er det vanskeligt at afgøre, om der er tale om planer for fremtiden, eller om virkemidlerne rent faktisk er i brug.

De fleste vurderer, at deres implementeringsgrad ligger i intervallet 70-80%. Det harmonerer godt med, at der er gjort en relativt stor indsats for at øge bevidstheden i organisationerne (se afsnit 3.6). Samtidig er det udtryk for en realistisk vurdering: Der er stadig et stykke vej, før man er helt i hus med implementeringen.

Typisk er man ikke så langt med nød- og beredskabsplanlægningen. Beredskab opleves generelt som et svært område, og flere har endnu ingen nød- og beredskabsplaner. Hos nogle er man heller ikke helt i mål med risikoanalyserne.

Med hensyn til behovet fremover - også i lyset af Statens It - nævner flere, at gryden skal holdes i kog, at der ligger en udfordring i at tænke sikkerhed ind i SLA-arbejdet (arbejdet med Service Level Agreements), og man foreslår at gentage benchmark-undersøgelsen.

I tråd med at man i implementeringsprocessen har savnet konkrete hjælpeværktøjer, jf. afsnit 3.3, ser man frem til en central styring som mulig løftestang for det videre arbejde med informationssikkerhed. Man forventer sig mere standardisering i form af en fælles opfattelse og forståelse af sikkerhedsbegrebet, fælles regelsæt og politikker, som kan genbruges, operationelle driftshåndbøger, skabeloner og et fælles risikostyringsværktøj.

Det anbefales, at man:

- Løbende vedligeholder, forbedrer og videreudvikler informationssikkerheden i et stadigt samspil med de ændrede forretningsmæssige risici
- Fra centralt hold leverer konkrete, operationelle hjælpeværktøjer som fx standard skabeloner, vejledninger og køreplaner samt til brug for selvevalueringer: en model for temperatur-/modenhedsmåling

3.6 Opmærksomhed og kommunikation

Det er de færreste, der indledningsvis har lagt vægt på at informere og kommunikere om projektet. Man henviser til, at det jo var obligatorisk, jf. også afsnit 3.2. Igen fremgår det, at de, der bevidst har anvendt forskellige former for information, formidling og kommunikation også i starten af projektet, hører hjemme i forsknings-, uddannelses- og kulturverdenen.

I lyset af, hvor få der til en start har gjort noget for at ”sælge” projektet, er det bemærkelsesværdigt, hvor mange der undervejs i projektet har taget hånd om at skabe bevidsthed om informationssikkerhed. Man har generelt anvendt en bred vifte af informations- og kommunikationskanaler i bestræbelserne på at bevidstgøre organisationen om sikkerhedsspørgsmålene. Kun et mindretal har ikke fundet det nødvendigt at fokusere på at skabe bevidsthed om informationssikkerhed.

Det er et gennemgående træk, at organisationerne har fundet de indførte foranstaltninger irriterende og besværlige, men at der samtidig er forståelse for nødvendigheden af dem. Flere steder har medarbejderne ikke bare accepteret, men ligefrem ”adopteret” og taget sikkerhedsudfordringerne til sig.

Mange svarer også bekræftende på spørgsmålet om, hvorvidt ansvaret som ejer efterleves nu. Flere peger dog på, at den fulde forståelse og bevidsthed ikke er helt på plads, men at den er undervejs.

Det er karakteristisk, at flere af de interviewede peger på eksemplets magt som et tungtvejende pædagogisk middel til bevidstgørelse om informationssikkerhed. Eksempler på hændelser fra dagligdagen, hvor sikkerheden kompromitteres, er noget, man kan forholde sig til.

Det anbefales, at man:

- Identificerer ildsjælene i organisationen, og evt. ’omvender’ de vrangvillige til at blive projektets ambassadører
- Udleder og kommunikerer ’what’s in it for me?’
- Anvender et bredt udsnit af informations- og kommunikationskanaler for at øge bevidstheden om informationssikkerhed og dermed adfærden i organisationen
- Løbende registrerer, opsamler og formidler ’de gode historier’ i organisationen. ’De gode historier’ handler vel at mærke både om eksempler på hændelser, der gik godt pga. stor opmærksomhed på sikkerhed og strukturerede processer, og om eksempler på hændelser, der gik skidt, fordi man et øjeblik glemte sikkerhedsspørgsmålet

4 Anbefalinger

>

Følgende, samlede række af anbefalinger baserer sig på konklusionerne og den bedste praksis, der kan udledes af interviewundersøgelsen. I parentes efter hver anbefaling angives det relevante, underbyggende afsnit i kap. 3.

Står man over for at skulle implementere informationssikkerhed på basis af DS 484, kan det anbefales, at man som projektleder:

- Sikrer sig ledelsens fokus (afsnit 3.1, 3.2)
- Udarbejder en foranalyse med henblik på at bedømme opgavens indhold og vurdere omfanget i tid, ressourcer og økonomi (afsnit 3.2)
- Får allokeret nødvendige ressourcer og fornøden tid (afsnit 3.4)
- Fokuserer på at have en forretningsorienteret - og ikke en snæver it-mæssig - tilgang til sikkerhed (afsnit 3.4)
- Identificerer ildsjælene i organisationen, og evt. 'omvender' de vrangvillige til at blive projektets ambassadører (afsnit 3.6)
- Organiserer projektet med en projektgruppe, evt. i form af et sikkerhedsudvalg, og en styregruppe. Det hjælper på forankringen af informationssikkerhed i organisationen, stor som lille, når projektet ikke kører isoleret fra den (afsnit 3.2)
- Etablerer en informationssikkerhedsorganisation, der også kan tage over, når projektet overgår til drift (afsnit 3.1)
- Fokuserer mindre på at anvende et it-værktøj til informationssikkerhed og mere på at planlægge implementeringen og procesoptimeringen (afsnit 3.2)
- Udleder og kommunikerer 'what's in it for me?' (afsnit 3.6)
- Anvender et bredt udsnit af informations- og kommunikationskanaler for at øge bevidstheden om informationssikkerhed og dermed adfærden i organisationen (afsnit 3.6)
- Løbende registrerer, opsamler og formidler 'de gode historier' i organisationen. 'De gode historier' handler vel at mærke både om eksempler på hændelser, der gik godt pga. stor opmærksomhed på sikkerhed og strukturerede processer, og om eksempler på hændelser, der gik skidt, fordi man et øjeblik glemte sikkerhedsspørgsmålet (afsnit 3.6)
- Definerer, identificerer og forankrer ejerskab til informationsaktiverne (afsnit 3.2)
- Foretager en cost benefit vurdering i tilknytning til risikoanalysen (afsnit 3.2)
- Får samlet op på risikoanalysen og holder ledelsen fast på at drage konklusioner ud fra den (afsnit 3.2)
- Genbruger, hvad andre har haft gavn af, fx låner sig frem til skabeloner og andre hjælpeværktøjer (afsnit 3.3)
- Udveksler erfaringer med andre, fx Hvad gik godt? Hvorfor? Hvilke faldgruber skal man forsøge at navigere udenom? (afsnit 3.3)

>

- Løbende vedligeholder, forbedrer og videreudvikler informationssikkerheden i et stadigt samspil med de ændrede forretningsmæssige risici (afsnit 3.5)

Herudover kan det anbefales, at man fra centralt hold leverer konkrete, operationelle hjælpværktøjer som fx standard skabeloner, vejledninger og køreplaner samt til brug for selvevalueringer: en model for temperatur-/modenhedsmåling (afsnit 3.5).

5 Datagrundlag og metode

>

5.1 Datagrundlag

Der er i alt gennemført 23 interview, repræsenterende 21 statslige organisationer (i.e. departementer, direktorater, styrelser og diverse institutioner). Af de 21 organisationer har IT- og Telestyrelsen og Dansk Standard i samarbejde udpeget nogle som værende 'mindre' organisationer i denne sammenhæng. De er i det følgende identificeret som A, C, G, H, M, S og T.

Det har været relevant, fordi det har vist sig, at de mindre organisationer har stået over for en række særlige udfordringer, jf. konklusionerne i kap. 3.

26 personer har medvirket i interviewene. Langt hovedparten af de interviewede har deltaget under hele implementeringen af DS 484 (spm. 1.2³): 20 personer har været med hele vejen, og 3 har været med i næsten hele forløbet, blot ikke til en start.

Deres roller i implementeringsforløbet fordeler sig sådan (spm. 1.1 og 1.3):

Rolle	Antal
Projektleder – overordnet eller lokal	13
Projektejer / repræsentant for projektejer	4
Projektejer og –leder (under en hat)	4
Projektdeltager	3
Resten	2

Tabel 1 - Roller

17 af de 26 svarpersoner har eksplicit tilknytning til it-delen af organisationen.

9 organisationer gik i gang i 2006, 5 i 2005, 7 før 2005 (spm. 2.1).

5.2 Metode

5.2.1 Dataindsamling

Data er indsamlet via en kvalitativ interviewundersøgelse.

I samtlige interview blev der taget udgangspunkt i den samme interviewguide og spørgeramme, se Bilag 1. Det skete for at sikre en vis konsistens og ensartethed i erfaringsopsamlingen og dermed også for at sikre, at datagrundlaget for den efterfølgende bearbejdning blev tilstrækkeligt validt.

³ Tal i parentes med foranstillet "spm." henviser til det konkrete spørgsmål, der blev stillet.

Som det fremgår af bilaget, blev interviewguiden indledningsvis læst op, og der blev i overensstemmelse med den kvalitative metode gjort opmærksom på, at alle interviewpersonerne i undersøgelsen blev interviewet ud fra de samme spørgsmål, men at:

”Interviewet skal ses som en samtale, således at viden om dine erfaringer og konstateringer er vigtigere, end at hvert enkelt spørgsmål bliver besvaret specifikt.”

Det vigtige var ikke, om man kom igennem samtlige spørgsmål under spørgerammens områder, men at man fik fokuseret på interviewpersonernes erfaringer inden for spørgerammens emner, jf. Bilag 1.

Hvert enkelt interview blev optaget og sidenhen transskriberet.

5.2.2 Databearbejdning og analyse

Analysen af interviewresultaterne (kap. 6) er baseret på de transskriberede interview. Databearbejdningen følger nøje spørgerammens områder. Et kriterium for udvælgelse af spørgsmål/svar til behandling har været, om der har tegnet sig et tydeligt svarmønster, sådan at svarene har kunnet kategoriseres. Et andet har været, om der tegnede sig et diffust svarmønster, hvilket der også i visse tilfælde kan være en pointe i.

Der er som hovedregel set bort fra manglende svar, og svar, der ikke umiddelbart er svar på det stillede spørgsmål. Da ikke alle spørgsmål er blevet stillet slavisk til de enkelte interviewpersoner, skal man ikke forvente, at de kvantificerede resultater kan opsummeres til at gå op med fx antal interviewpersoner eller antal organisationer. Omvendt hænder det også ret hyppigt, at den samme organisation optræder i flere svarkategorier på en gang (jf. den kvalitative metode).

Under analysen har det været nødvendigt at kunne identificere den enkelte organisation for at kunne uddrage et eventuelt mønster på kryds og tværs af interviewene.

Af hensyn til andres mulighed for dels at bedømme rimeligheden af analysens resultater, bl.a. kvantificeringerne, dels at finde øvrige mønstre, fremgår organisationerne af rapporten, dog naturligvis i anonymiseret form med benævnelserne A-X. Der henvises til svarmønstrene med romertal i fed skrift.

Analysen rummer en hel del citater fra interviewene. De udgør i sig selv en form for dokumentation, men de er ikke mindst udvalgt som selvforklarende læsefrugter.

6 Analyse af interviewresultaterne

>

Analysen i dette kapitel er bygget op om spørgerammens områder, dvs. de hovedoverskrifter, som interviewundersøgelsens spørgsmål falder ind under, jf. Bilag 1: spørgerammens vertikale dimension.

Om databearbejdningen og analysemetoden: se afsnit 5.2.2.

6.1 Indledende generelle spørgsmål

Hvordan har du oplevet implementeringsprocessen? (spm. 1.4)

Svar	I	II	III
	Svært at komme i gang	Tung proces for en lille organisation	God, positiv, sund proces
Antal	C, I, N, P	A, G, H, M, S	B, F, J, L, N, R, T, U

Tabel 2 - Implementeringsprocessen

Svarene på spørgsmålet fordeler sig nogenlunde ligeligt mellem dem, der har oplevet processen som svær og tung (**I+II**), og dem, der ser meget positivt på den (**III**).

Det er bemærkelsesværdigt, at hele 5 mindre organisationer eksplicit peger på, at processen har været tung for dem netop pga. organisationens størrelse (**II**). De nævner bl.a. ressourcer som et problem, og en enkelt stiller spørgsmålstegn ved relevansen af DS 484 for en lille organisation.

De, der ser positivt på processen, taler bl.a. om, at der har været stor lydhørhed og ledelsesopbakning i organisationen, og at processen har været velorganiseret.

Af de organisationer, der havde været i gang tidligere (med 2000-versionen af DS 484), udtaler 2 (O, X), at det var nemt at komme op på den nye version. Der var ikke tale om noget kvantespring med den nye standard, og det store arbejde var lavet. Andre 2 oplevede versionsændringen som irriterende (P) og besværligt (Q). Værktøjsmæssigt var det problematisk at skulle skifte over til den nye version midt i forløbet pga. tekniske konverteringsproblemer.

>

**Hvad vurderer du som det væsentligste udbytte ved implementeringen?
(spm. 1.5)**

Svar	I	II	III
	Bevidsthed, erkendelse, forståelse, holdninger, opmærksomhed	Forbedring af sikkerhed, Sikkerhed tænkes ind i processer, Metodik, Struktur i sikkerhedsbeslutninger, Formaliseret procedure	Skub i nogle beslutninger Ledelsesforankring og -fokus
Antal	A, B, D, H, I, K, L, M, O, P, S, T	B, C, F, E, H, I, K, N, Q, R, T	F, G, H, M, P, V

Tabel 3 - Udbytte ved implementeringen

Svarene på dette spørgsmål falder også her i 3 kategorier. I 5 tilfælde svarer interviewpersonen med både svar **I** og **II**. Den øgede forståelse, erkendelse og opmærksomhed går i disse tilfælde hånd i hånd med det forbedrede, strukturerede sikkerhedsarbejde og dermed sikkerhedsniveauet.

Det er også værd at bemærke, at relativt mange har oplevet ledelsesforankringen som det væsentligste udbytte.

Selve standarden DS 484 får nogle ord med på vejen som en løftestang:

En (U) siger:

”Med 484 er det meget nemt at kommunikere med leverandørerne. Og ingen tilbudsgivere spørger: Hvorfor har I skrevet det?”

En anden (N) udtaler:

”Hvis der ikke var en 484 (...) ville jeg have været på Herrens mark og ville ikke være kommet så langt omkring, jeg ville ikke selv kunne proppe de relevante ting ind (...) 484 altså krumtappen i vores arbejde”

Og en tredje (Q):

”Og vi fik nogle tanker, som vi ikke havde fået uden 484”

En nævner, at standarden bruges som international reference.

Som et virksomt middel til at få sat skub i tingene i forhold til ledelsens fokus og erkendelsesprocessen nævnes IT- og Telestyrelsens benchmarkundersøgelse (V):

”Da vi fik benchmark fra IT- og Telestyrelsen, så fik vi øjnene op.”

>

Hvordan opleves det at skulle efterleve et normativt grundlag? (spm. 1.6)

Svar	I	II	III	IV
	Mere arbejde	For interviewperson: OK For organisationen: Svært	Dagligdag ikke sværere Ingen forandring Ingen problemer	Fint, god sikkerhedsmæssig skik, Fantastisk værktøj, Redskab, værktøj, hjælp
Antal	A, G, N, S	J, L, M, O, Q	B, C, F, H, K, P, U	E, R, T, V

Tabel 4 - At efterleve et normativt grundlag

Hovedparten af de interviewede udtrykker, at det ikke er anderledes end normalt at arbejde med DS 484 (**III**). Man er vant til at være underlagt regelsæt:

”Vi har (...) en række direktiver, som vi i forvejen skal efterleve”

Nogle er eksplicit positive og betragter DS 484 som et nyttigt værktøj (**IV**).

3 ud af de 4, der udtaler, at det har givet mere arbejde (**I**), repræsenterer mindre organisationer.

Svarkategori **II** udgør dem, der på egne vegne er positive, samtidig med at de giver udtryk for, at det har været svært for organisationen at acceptere.

En (J) udtrykker det sådan:

”(...) opfattes som en bureaukratisk belastning, men er det ikke i virkeligheden”

En repræsentant (M) for en af de mindre organisationer siger:

”Det er nok svært især at acceptere kravet, at man skal (...) Men der er også meget godt i 484, gode råd. Godt, at man ikke selv skal opfinde...”

En anden (O) peger på, at

”Det har været lidt svært at få dem til at rette ind i forhold til en standard. Derfor kræver det ledelsesansvar”

Ud af de 5, der svarer **II**, har de 4 rollen som projektleder og den sidste rollen som projektdeltager. I de øvrige svarkategorier er rollefordelingen mere diffus.

>

6.2 Organisering og forberedelse

Hvordan blev projektet ”solgt” internt? (spm. 2.2)

Svar	I	II	III
	Ej solgt	Ej solgt – ej nødvendigt: <ul style="list-style-type: none">➤ Beslutning i regeringens Økonomiudvalg➤ ”Vi skal”➤ Benchmark➤ Rigsrevisionen	<ul style="list-style-type: none">➤ Information fra øverste ledelse til næste lag➤ Nyheder på intranet, mails til afd.ledere➤ Awareness- kampagner, interne artikler, plakater, musemåtter➤ Politikker, huskeregler, procedurer. Deltagelse på afd.ledermøder, matrix med ansvar➤ God intern accept
Antal	C, D, E, G, I, O, P, V	B, K, L, M, N, Q, U	A, F, H, J, R, T

Tabel 5 - Internt salg af projekt

I 15 af organisationerne er projektet ikke blevet ”solgt” (**I+II**), heraf henviser ca. halvdelen til, at projektet var obligatorisk (**II**). Disse nævner Økonomiudvalgets beslutning, benchmark og rigsrevisionen som løftestænger for projektet.

Som en (Q) udtrykker det:

”Først da det blev et krav, gik det nemmere med at få direktionens opmærksomhed.”

Heroverfor står 6 af organisationerne, der - måske ikke helt fra starten men undervejs - bevidst har anvendt forskellige former for information, formidling og kommunikation i projektet (**III**). Det er værd at bemærke, at 4 ud af disse 6 hører hjemme i forsknings-, uddannelses- og kulturverdenen.

>

Hvordan har ledelsen udvist deres ejerskab og ansvar? (spm. 2.3)

Svar	I	II	III	IV
	Underskrift/ godkendelse (breve, sikkerheds-politik, skriftlige oplæg)	Mere af navn end af gavn. Manglende indsigt, forståelse for opgaven. Set som et it- projekt	Højt forankret	I høj grad
Antal	A, C, P, Q,	D, E, G, L, M, T, V	B, K, L, O	F, H, I, J, N, R, S, U, X

Tabel 6 - Ledelsens ejerskab og ansvar

En enkelt udtaler uforbeholdent, at ledelsesopbakningen har fungeret:

”Ledelsen har bakket mig op i forhold til at gennemføre ting, hvor medarbejderne ikke har kunnet leve med det. Her har ledelsen jo efterlevet sit ejerskab og bakket op” (S)

Flere peger på, at Rigsrevisionens besøg har været en motiverende faktor for ledelsen:

”Det er (...) motiverende, at Rigsrevisionen kommer og giver signal om vigtighed.” (H)
”Rigsrevisionen kritiserede direktionens engagementet, og det har klart hjulpet” (T)

Andre nævner benchmark-undersøgelsen som en øjenåbner hos ledelsen:

”Vores første benchmarkresultat (...) Målet var, at det skulle implementeres, og det så ikke så godt ud i ledelsesforankringen. Det røde lys blinkede, og så tog ledelsen ansvaret.” (M)

”Da vi fik benchmark fra IT- og Telestyrelsen, så fik vi øjnene op.” (V, jf. tidligere)

Har ledelsen erkendt sin rolle? (spm. 2.3.1)

På spørgsmålet om, hvorvidt ledelsen har erkendt sin rolle (spm. 2.3.1), svarer 6 ja, mens resten ikke svarer eksplicit.

Har nødvendige beføjelser og ressourcer fulgt med ansvar? (spm. 2.3.2)

Svar	I	II
	Nej, ingen ekstra ressourcer	Ja Ja, dedikeret stilling Ja, ekstern hjælp
Antal	A, E, H, J, P, T, U, V	B, C, D, F, G, I, K, L, M, O, R, S

Tabel 7 - Beføjelser og ressourcer

>

Der er ikke mange, som svarer specifikt på spørgsmålet om beføjelser – de fleste svarer øjensynligt på ressourcedelen af spørgsmålet. En enkelt (S) nævner dog, at det havde været nemmere, hvis personaleansvaret også havde fulgt med; en anden (T) siger, at mandatet var ok.

Som det fremgår af tabellen, er der en lille overvægt af dem, der svarer, at de har fået de nødvendige ressourcer.

Modsat hvad man måske kunne forvente, fordeler de mindre organisationer sig nogenlunde ligeligt i de to svarkategorier.

13 af organisationerne nævner, at de har benyttet ekstern konsulentbistand i dele af forløbet. Det er værd at lægge mærke til, at der kun er 3 mindre organisationer (C, M, S) blandt disse 13.

Hvor har projektejerskabet og projektet organisatorisk været placeret? (spm. 2.4)

Svarene på spørgsmålet er ikke entydige. Det ser ud til, at nogle blander projektejerskab, og –ledelse, også hvor det ikke er en og samme person, der varetager de to roller. Det lader også til, at nogle opfatter den organisatoriske placering som værende identisk med et spørgsmål om, hvor selve arbejdet blev udført.

Når der tages højde for det, kan det konstateres, at flertallet af organisationerne (ca. 14) har haft projektet placeret eller har udført det i it-afdelingens regi. Dertil kommer, at 17 af de 26 interviewpersoner har eksplicit tilknytning til it, jf. tidligere.

Projektet tenderer med andre ord til at blive placeret og/eller udført i its regi.

De – i alt 6 - der direkte udtaler sig om betydningen af projektets placering, siger enten, at det ikke skulle have ligget i it's regi, eller at det var positivt, at det ikke blev et it-projekt.

”(…) projektlederen skulle ikke have været it-chefen, for så bliver det for meget it. Det skal være it for forretningens skyld.” (A)
Positivt, at ”det ikke (er) havnet som et it-projekt.” (B)

En organisation (D), hvor projektet tidligere reelt havde været forankret hos it-driftschefen, som ”(...)prioriterede driften”, har oplevet en fordel ved at projektet blev flyttet ud af it:

”(…)fordel, at (...) kom ind, (...) var udenfor – ikke en it-mand. Det var en bedre model (...)
Vi har fået styr på det nu, vi har planer, og det skrider fremad. Er nok fordi jeg ikke er it-mand, men har (...) gode erfaringer med fortolkninger.”

I en anden organisation (N) har projektet organisatorisk ”haft sin egen eksistens”:

”Denne opgave kræver engagement og interesse, så det har haft betydning, at vi har kunnet sammensætte gruppen og ikke været bundet af et eksisterende kontor. Fordel at kunne se på det som noget tværfagligt. Vi ser det lidt udefra og lettere at anskue det som informationssikkerhed og ikke kun it – altså de mere abstrakte ting – vi sidder ude i forretningen og er ikke knyttet til de fx daglige tekniske ting.”

En anden organisation (S):

”For meget it-relateret og lidt sværere at komme igennem for hele organisationen og ikke kun i it. Det har været svært med nogle af tingene. Måske bedre at placere det hos samarbejdsudvalget, så de kunne følge med løbende. Det ville være mere effektivt.”

En it-chef med en utraditionel baggrund udtaler (T):

”Man finder det logisk, at det har ligget hos mig i it. Det er vigtigt, at jeg er inde over forretningsområderne og har gode kontakter. Der må ikke være barrierer mellem forretningen og it. Jeg er (...), og det gør det lettere at blive accepteret i miljøet. Det er værdifuldt.”

Det sidste udsagn kunne tyde på, at det er irrelevant om projektet ligger i it's regi eller ej, men at det er den forretningsrelaterede tilgang, der er det afgørende. Eller med andre ord: Det er muligt at undgå, at det bliver et rent 'it-projekt', også selv om det er placeret i it-afdelingen.

Blev der gennemført en foranalyse forud for selve projektet til at bedømme opgaven og vurdere omfanget i tid og ressourcer? (spm. 2.5)

Flertallet af organisationer – i alt 14 - svarer: Nej.

Det er påfaldende, at flere af dem, der svarer ja, henviser til gap analyser, handlingsplaner og benchmark. En enkelt henviser til ”en fin kravspecifikation”.

Det giver alt i alt et indtryk af, at man ikke er helt bekendt med begrebet foranalyse, med formålet med en sådan analyse og heller ikke med at gennemføre en.

>

6.3 Strategi og politik for informationssikkerhed

Fandtes der sikkerhedsstrategier og -politikker i forvejen? (spm. 3.1)

Svar	I	II	III
	Nej	Ja	Delvis
Antal	C, D, H, K, P, S, U	I, J, L, N, R, V	A, B, E, F, G, M, O, Q, T, X

Tabel 8 - Sikkerhedsstrategier og -politikker

Langt hovedparten af organisationerne havde ikke eller havde kun delvis sikkerhedsstrategier og -politikker på forhånd. 'Delvis' dækker over, at man havde en sikkerhedshåndbog eller en gammel it- politik, men ingen sikkerhedspolitik, eller at man havde nogle forældede, ikke gennemarbejdede dokumenter.

De, der svarer ja på spørgsmålet, er i klart mindretal. Samtidig kan det konstateres, at der ikke er nogen af de mindre organisationer blandt ja-sigerne, dvs. de mindre organisationer svarer 'nej' eller 'delvis' og har dermed ikke haft opdaterede sikkerhedsstrategier og -politikker at tage udgangspunkt i.

Hvordan er arbejdet med udarbejdelsen/opdateringen af disse blevet gennemført? (spm. 3.2)

Hvem har deltaget? (spm.3.3)

Svar	I	II	III
	Startede fra scratch og/eller Stor opgave	Projektleder og få andre	Ekstern konsulentbistand
Antal	H, I, J, L, N, O, P	C, F, G, I, J, M, T, P, U	I, P, Q, U, X

Tabel 9 - Udarbejdelse og opdatering af strategi og politik

Mange svarer, dels at man startede fra scratch – også dem, der havde noget i forvejen - og/eller at det var en stor opgave, dels at projektlederen har trukket et stort læs med skrivearbejdet enten helt alene eller i samarbejde med få andre. I denne sammenhæng har nogle desuden benyttet sig af ekstern konsulentbistand. Ingen af de mindre organisationer nævner i deres svar, at de har anvendt ekstern hjælp, jf. tabel 7.

En projektleder har oplevet det sådan:

”Jeg har været 'lonely rider' og min chef" (O)

>

En projektdeltagers situation beskrives på denne måde:

”(...) kørt meget som enmandsopgave” (M) / ”enmandshær” (A)

Det påfaldende er, at de samstemmende udtalelser dels kommer fra to meget forskellige organisationer, dels fra to personer der både organisatorisk og projektmæssigt er vidt forskelligt placeret.

På spørgsmålet om, **hvorvidt processen med udarbejdelsen/opdateringen har ført andet med sig (spm. 3.4)**, henviser 4 til bedre it-processer:

En (F) nævner ansvarsplacering i forbindelse med afklaring om fx ændringsstyring og vigtigheden af at få styr på backupkoncepter.

En anden (S) siger:

”Et helt afsnit handler om it, men vi valgte ofte at tage skridtet fuldt ud – ITIL”

En (T) udtaler:

”Systematik og en større forståelse for, at vi skal behandle digitale informationer systematisk – ITIL”

ITIL og CMDB⁴ nævnes af en fjerde (under spm. 6.2) som et redskab til at skabe overblik over informationsaktiver (X).

⁴ CMDB: Configuration Management DataBase. En hovedhjørnesten i ITIL. Holder styr på alle aktiver og deres indbyrdes relationer.

6.4 Projektorganisering

Der er ikke et entydigt mønster i svarene på, **hvilke organisationsenheder der har deltaget i projektarbejdet (spm. 4.1)**. 6 svarer ikke direkte på spørgsmålet. Af dem, der svarer, nævner 8 it-afdelingen. En enkelt af de større organisationer nævner, at også HR, Økonomi og Jura har været involveret, mens en af de mindre organisationer omtaler SU.

Fik projektdeltagerne allokeret den fornødne tid til at deltage i projektet? (spm.4.2)

Svar	I	II	III
	Nej	Ja	Intet svar
Antal	A, E, H, I, J, L, O, P, S T, V, X	D, F, N, Q	B, C, G, K, M, R, U

Tabel 10 - Projektdeltagerne til projektet

Hovedparten af de interviewede mener ikke, at der blev allokeret den fornødne tid til projektdeltagerne, 4 af dem er mindre organisationer. Blandt dem, der ikke svarer på spørgsmålet, er der meget naturligt et sammenfald med dem, der i store træk har kørt projektet alene, jf. tabel 9.

Blev der oprettet en informationssikkerhedsorganisation i forbindelse med implementeringen, eller fandtes en sådan i forvejen? (spm. 4.3)

Svar	I	II	III
	Nej	Ja – Blev oprettet	Fandtes i forvejen
Antal	C, G, S, U	A, B, D, E, H, I, M, N, Q, R, T, X	F, J, K, L, O

Tabel 11 - Informationssikkerhedsorganisation

I langt de fleste af organisationerne blev der oprettet en informationssikkerhedsorganisation i forbindelse med implementeringen (II). Det er typisk i de større organisationer, at der fandtes en i forvejen (III), mens flere af de mindre organisationer ikke havde en sikkerhedsorganisation formentlig hverken før eller efter projektet (I).

6.5 Gennemførelse af implementeringen

Hvilke arbejdsmetoder blev anvendt? (spm. 5.1)

Svar	I	II
	Intet svar eller svar: ”Ingen”	Projekt- og arbejdsgrupper, workshops med undervisning og hands on, møder i implementeringsudvalg, skabeloner, informationsmøder, vejledninger
Antal	D, E, G, J, K, U, V	F, H, I, J, L, O, Q

Tabel 12 - Arbejdsmetoder

Ca. 1/3 svarer enten ikke på spørgsmålet om, hvilke arbejdsmetoder der er anvendt, eller de nævner, at der ikke er brugt nogle specifikke metoder.

7 organisationer har tilsyneladende haft en mere struktureret tilgang og nævner bl.a.: Projekt- og arbejdsgrupper, workshops med undervisning og hands on, møder i implementeringsudvalg, skabeloner, informationsmøder, vejledninger. Det er bemærkelsesværdigt, at 5 af de 7 organisationer har deres rod i forsknings-, uddannelses- og kulturverdenen, ligesom de må siges at være vant til en projektorienteret arbejdskultur.

4 organisationer nævner, at de har brugt et egentlig værktøj (M, P, Q, R). Det kan ikke i sig selv siges at have været løftestang for implementeringen, tværtimod nævner en, at der var tekniske konverteringsproblemer i forbindelse med versionsskiftet (fra DS 484:2000 til DS 484:2005, jf. også tidligere), og en anden, at man er på udkig efter et andet værktøj (R).

Har ændringer af it-systemer eller arbejdsprocesser været nødvendige? (spm. 5.2)

Svar	I	II	III	IV
	Nej	Arbejdsprocesser ændret – lidt	Arbejdsprocesser ændret - en del/meget	It-systemer
Antal	D, G, O	E, F, I, J, M, N, Q	A, B, K, S, U, X, T	I, P, T, U

Tabel 13 - Ændringer af it-systemer eller arbejdsprocesser

14 af de interviewede svarer, at implementeringen af DS 484 har medført ændrede arbejdsprocesser. De fordeler sig nogenlunde ligeligt på, om der har været tale om enkelte (II) eller større ændringer (III).

De interviewede nævner følgende områder, der har været genstand for ændringer:

- Generelt
 - Regler for sikkerhedshændelser og for sikkerhedsbrud

>

- Systematisk logning – sporbarhed
- Brugerrettigheder
 - Kontrol med brugerrettigheder
 - Adgang til serverrum og til software
 - Indførelse af personlige kort, der bæres synligt
 - Indførelse af gæstelog
- Sikring af data
 - Ændring i backupkoncept
 - Eksterne brandskabe til sikring af data
 - Kryptering
 - Indførelse af pauseskærm styret fra centralt hold
- Driftsstabilitet
 - Organisering af testmiljø
 - Anskaffelse af stor central UPS

Langt hovedparten af ændringerne omfatter arbejdsprocesser og –procedurer, evt. i kombination med en ændring af et it-system (fx pauseskærmen, jf. ovenfor).

De 4, der decideret omtaler ændringer i et it-system, nævner alle kravet om systematisk logning – at det har skullet understøttes it-mæssigt.

Hvor meget tid/ressourcer har implementeringen af DS 484 taget? (spm. 5.3)

Svar	I	II	III	IV
	½-1½ årsværk	2-2½ årsværk	3 årsværk	6-7 årsværk
Antal	G, K, M, O, T	C, F, N, S	A, H, I, L	J, Q

Tabel 14 - Ressourcer til implementeringen

Halvdelen af de mindre organisationer (i alt 3) falder inden for svarkategori I. De har brugt 1-1½ år på implementeringen. 2 af organisationerne svarer mellem 6 og 7 årsværk. Det er ikke ensbetydende med, at der antalsmæssigt har været afsat mange ressourcer, blot at de 2 organisationer hører til dem, der har været i gang længe, dvs. før 2005.

Har det været nødvendigt at gå på kompromis i processen undervejs? (spm. 5.4)

Svar	I	II
	Nej	Ja
Antal	A, B, C, K, L, R	D, E, F, G, H, I, J, M, N, O, P, Q, S, T

Tabel 15 - Kompromis i processen

>

Majoriteten af de interviewede angiver, at det har været nødvendigt at gå på kompromis undervejs (II). I denne svarkategori ligger også de fleste af de mindre organisationer.

En repræsentant for en af de mindre organisationer (M) siger således:

”Jeg prøver at vurdere, hvilke krav der er ultimative, og hvor vi kan vælge (...) Grundlæggende har vi, der kender standarden, hele tiden følt, at det er skudt over målet i forhold til vores organisation.”

De udfordringer, der hyppigst peges på som anledning til kompromisserne, er

- Kravet om logning (D, P)
- Kravet om funktionsadskillelse (G, M, O, P, S)
- Ønske om pragmatisk tilgang med forskellige udgangspunkter (F):
 - Hvad giver værdi? (I, X)
 - Diskussioner i organisationen (J)
 - Tilpasning til virkeligheden i organisationen
 - Ressourceovervejelser – Hvad er godt nok? (N)

Herudover peger et par stykker (C, P) på udfordringerne i forbindelse med outsourcing:

”(...)system med ekstern leverandør er på vores netværk og er blevet taget med i vores system. Her kan der være ting, vi ikke kan leve op til i forhold til standarden, fx eksterne adgang og fysiske adgang.” (C)

”Jeg har brugt meget tid på outsourcing. Hvordan kan man følge op på sine outsourcingpartnere? Man skal følge op, men det er ikke nemt. Forslag: revisionserklæringer – og det er svært at få – trods kontrakt om det (...) det er en lang og sej kamp. Den slags situationer bliver til kompromisser (...) mange steder, fordi man ikke ved, hvor langt man kan/skal gå.” (P)

6.6 Informationsaktiver og informationsejere

Fandtes der en opdateret oversigt over informationsaktiver og informationsejere forud for implementeringen? (spm. 6.1)

Svar	I	II
	Nej	Ja
Antal	B, C, D, E, F, H, I, J, K, P, Q, T	A, G, L, M, N, O, R, S

Tabel 16 - Oversigt over informationsaktiver

Det fremgår af svarene, at langt hovedparten af organisationerne startede implementeringen fra bunden af, dvs. man havde ikke en oversigt over informationsaktiver at tage udgangspunkt i.

Af de 8, der svarer ja, nævner de 5, at oversigten udelukkende omfattede it systemer.

Det generelle indtryk er, at de, der havde en oversigt på forhånd, ikke nødvendigvis også havde udpeget informationsejere eller i øvrigt brugte oversigten aktivt. Følgende udtalelse forekommer at være dækkende for tingenes tilstand inden implementeringen:

”Der var en oversigt (...) den var ikke systematisk og ikke implementeret. Der manglede ting, og der var ingen klassifikation. Den bestod oprindeligt kun af it-systemer” (S)

Hvordan er overblikket over informationsaktiver blevet skabt? (spm. 6.2)

4 af organisationerne har anvendt følgende fremgangsmåde:

- Kortlægning og/eller interview med de respektive ejere (E, F, I, N)

Derudover er det lidt spredt, hvordan oversigten er blevet til:

- Kompendium med ansvar og systemejere - udarbejdet af projektleder (B)
- Decentralisering – opgaven lagt ud i de enkelte afdelinger (T)
- Afsæt i en risikovurdering (J)

Nogle har haft stor værdi ud af at få afdækket informationsaktiverne:

”(...) der findes skuffesystemer, som vi brugte, og det var hvad som helst (...) som var væsentligt, men kendtes ikke af it (...) nogle fik aha-oplevelser. Måske kom der yderligere 50% systemer frem i lyset” (L)

”Der dukkede også ting op, som vi intet anede om. Hele området med de analoge data var mere omfangsrigt, end vi vidste. Det er vores store udfordring.” (T)

”Alt har været gennemgået. Vi har tænkt og arbejdet i processer, men alligevel teknikfokuseret.” (J)

>

Hvilke former for informationsaktiver inkluderer oversigten, fx it-bårne, fysiske, medarbejdere, kontorer, beredskabsplaner? (spm. 6.3)

Svar	I	II
	Alt	It-systemer
Antal	A, B, E, I, J, M, N, S, T	D, F, G, H, O, P, Q, X

Tabel 17 - Typer af informationsaktiver inkluderet i oversigten

Svarene fordeler sig ligeligt mellem dem, der har udarbejdet en oversigt dækkende 'det hele', og dem, der har en oversigt udelukkende over it-aktiver. Det er bemærkelsesværdigt, at der er en lille overvægt af de mindre organisationer, som har valgt at udarbejde en altomfattende oversigt (I).

Hvordan er placeringen af ejerskabet foregået? (spm. 6.4)

Svar	I	II
	Ejerskab hos it	Ejerskab uden for it
Antal	G, O, T, X (system)	J, M, N, P, Q, X (data)

Tabel 18 - Placeringen af ejerskab

En hel del har fået ejerskabet placeret 'ude' i organisationen, typisk på kontorchef- eller afdelingschef-niveau.

Flere giver udtryk for, at det umiddelbart har været vanskeligt at arbejde med ejerskabsbegrebet. Det har været svært at forstå, hvad ejerskabet indebar, og dermed har processen med placeringen af ejerskabet også været tung:

"På det semantiske niveau har vi haft problemer – forklaringsproblemer, forståelsesproblemer. (...) Indimellem har det været vanskeligt at få ejerskabet på plads – rent umiddelbart – men ikke, når man taler med folk." (C)

"Jeg har samlet sammen og kategoriseret ejerskaber, men det blev for kompliceret, i stedet vigtigt at spørge: Hvem har ansvaret?" (D)

"Det har givet anledning til en række diskussioner" (J)

"Det var lidt af en kamp at få systemejerskaberne på plads. Navne (...) fungerer ikke, men funktionerne (...) det fungerer godt." (L)

"Systemejerne forstår ikke altid, hvad systemejerskabet indebærer. Nogle har fået sig noget af en overraskelse." (R)

Men der er også nogle, der har været igennem en noget nemmere proces:

"Der har været få sværdslag. 90% var oplagte ejerskaber." (E)

"Der var udpeget system- og dataejere, både af navn og af gavn. Nej (det har ikke været vanskeligt, red.)" (F)

"Vi havde systemejerskab (...) der var styr på ejerskab i forvejen" (P)

>

”Det fysiske var naturligt, og folk forstod dataejerskabsbegrebet med det samme. Systemejerskab forstod de ikke helt.” (T)

Efterleves ansvaret som informationsejer i dag? (spm. 6.5)

Svar	I	II	III
	Ja	Ikke endnu Ikke forstået Forståelse på vej Delvis	Nej
Antal	B, D, E, I, K, L, P, Q, R, T, U	C, J, M, N, S, X	G, H, O

Tabel 19 - Ansvaret som informationsejer

Det er bemærkelsesværdigt, at så mange svarer utvetydigt ja på spørgsmålet om, hvorvidt ansvaret som ejer efterleves (**I**). Ligesom rigtig mange er på vej (**II**). Kun 3 svarer entydigt nej.

2 af dem, der ligger i svarkategori **I**, nævner risikovurderingen/-analysen som et middel til erkendelse og efterlevelse af ansvaret:

”Dem der har fået lavet risikovurdering er bekendte med deres ejerskab” (Q)

”Ja, det blev meget synligt, da vi lavede risikoanalysen. Ejerne skulle jo udføre en konsekvensanalyse.” (R)

Flere i svarkategori **II** peger på, at den fulde forståelse og bevidsthed ikke er helt på plads, men at den er undervejs:

”Ja, det mener jeg. Det er under opbygning. Forståelsen er på vej.” (J)

”Det tror jeg. Vi har en sikkerhedshåndbog, men jeg er ikke sikker på, om ejerne er fuldt bevidste om indholdet.” (S)

Følgende citat udtrykker holdningen hos dem i svarkategori **III**:

”Ejerskab skal ikke blot stå på papiret, der skal handling bag, og det kniber. Der er kulturelle barrierer og manglende forståelse for, at der skal ændringer til.” (O)

>

6.7 Risikoanalyse og beredskab

Med hvilken tilgang og metode er risikoanalysen foretaget? (spm. 7.1 og 7.3)

Svar	I	II	III	IV
	Forretningsmæssigt udgangspunkt/Ejer- og brugertilgang	Simpel og pragmatisk tilgang / hjemmelavet model	Brug af standard it-værktøj til arbejdet med informationssikkerhed	Udgangspunkt i 'fortrolighed' 'integritet' 'tilgængelighed'
Antal	B, G, J, M, N, O, X	C, E, G, H, I, K, M, O, R	(H), P, Q, T	B, F

Tabel 20 - Metode til risikoanalyse

Det er tankevækkende, at så mange giver udtryk for, at de har haft en forretningsmæssig tilgang til risikoanalysen (I), og at rigtig mange fortæller, at de er gået pragmatisk til værks med udgangspunkt i en egenudviklet model (II). Der er visse gengangere i de to svarkategorier.

Flere (H, I, M, T) ytrer, at processen ikke var nem til en start. Blandt disse er der 2, som har taget udgangspunkt i værktøjets metode:

"(...) gået til opgaven ved at vælge en metode – (værktøj) har dog ikke virket. Så har vi søgt andre metoder. Men (...) for omfattende. (...) Vi har udviklet vores egen metode" (H)

"(...) vi ville bruge sikkerhedsportalen (...) for at vise vejen – den var meget besværlig. (...) Vi samlede de kritiske aktiver i bundter, og det blev samlet i et system (...) men det fungerer stadig ikke optimalt. Vi har derfor printet ud fra portalen. (...) (værktøj) er stadig ikke nem som metode" (T)

De, der typisk har deltaget i risikoanalysen, er system- og dataejerne (A, B, C, H, I, N, P, S), hvilket harmonerer med den forretningsmæssige tilgang. Flere har desuden benyttet sig af ekstern konsulenthjælp (F, I, M, P, X), og i 4 tilfælde har man involveret chefer (A, G, M, O).

>

Har det været vanskeligt at udføre cost-benefit vurderinger? (spm. 7.4)

Svar	I	II	III
	Der svares, men ikke på spørgsmålet	Ej udarbejdet C/B	Nej
Antal	B, D, F, G, H, I, J, Q, R, S, T, X	C, D, E, G, H, L, M, O, Q	U

Tabel 21 - Cost-benefit vurderinger

Svarene på dette spørgsmål forekommer ret diffuse. Kun en enkelt svarer direkte (III).

Resten svarer, men ikke på spørgsmålet, med udsagn som fx:

”Projektet lykkedes godt (...)” (B), ”Vi har intet endnu – og dog, vi har en masse procedurer...” (D), ”Nej, ikke endnu” (H), ”Ikke noget ekstraordinært” (F), ”Det har hos os ikke været så formelt (...) vi har alt på papir og kan godt tåle at gå ned” (G)

Det er påfaldende, at flere af de interviewede svarer, som om der blev spurgt om risikovurderinger og ikke om cost-benefit vurderinger (G, R, T, X).

Det giver en fornemmelse af, at forståelsen af begrebet cost-benefit vurdering er uklar - samme indtryk som svarene på spørgsmålet om foranalyse (spm. 2.5) giver.

Mange har tydeligvis ikke udarbejdet cost-benefit vurderinger (II).

Har risikoanalysen medført justeringer af sikkerhedsstrategien og virksomhedens risikovillighed? (spm. 7.5)

Svar	I	II	III
	Nej	Mangler afklaring og konklusion/ikke på niveau endnu	Ja
Antal	E, P, T, U, X	F, G, H, I, J	B, M, R, S

Tabel 22 - Justeringer af sikkerhedsstrategien og risikovillighed

De, der er kommet helt i mål med risikoanalysen (III), peger på nogle ret håndgribelige udbytter:

”(...) risikoforhold har været udløsende for de penge, der har været anvendt. Risikobeskrivelsen har udløst midler. Pengene følger med.” (B)

”(...) har fået nyt brugerstyringssystem, som gør brugerne unikke.” (M)

”Vi har også valgt at efterleve de skærpede krav, fordi med de data, vi håndterer, kan vi ikke nøjes med at håndtere de basale krav” (R)

>

”Vi fandt fx en dublering af et system, som fik backup, men hvor backup af andre systemer, som var mere kritiske, nu har fået højere prioritet (...) Vi købte ekstra backup-udstyr for at nå vores mål om at genskabe systemer (...) Vi blev opmærksomme på integritet af data, fx i vores økonomisystem, noget vi ikke kunne forstå, her forstod vi pludselig nogle data. Så vi laver nu flere løbende kontroltjek i systemerne for at dokumentere.” (S)

Mens de, der mangler afklaring og konklusion (II), forekommer mere desillusionerede:

”Der er risiko for sletning af data, men mangler afklaring” (F)

”Der mangler konklusion på risikovurderingsområdet. Altså en rapport, der viser, hvad der kom ud af denne gennemgang, og hvad vi vil prioritere. Bør afspejles i it-strategien (...) har ikke konkluderet og skabt sammenhæng til fx strategi” (I)

Fandtes der beredskabsplaner forud for projektet? (spm. 7.6)

Svar	I	II	III	IV
	Nej	Delvis: Spredt i organisationen – ikke koordineret	Ja: Non-it Brand og tyveri Forretningsprocesser	Ja: It
Antal	A, B, C, D, F, G, I, L, O, S, T, X	E, J, K	H, M, P, R	Q

Tabel 23 - Beredskabsplaner forud for projektet

Som det fremgår, har langt hovedparten af organisationerne stået på bar bund i forbindelse med beredskabsplanlægningen.

Hvilken betydning har risikoanalysearbejdet og resultatet haft på nye eller reviderede beredskabsplaner? (spm. 7.7)

Svar	I	II	III
	Beredskabsplaner er nu på plads	Beredskabsplaner endnu ikke helt udtømmende / arbejdet er stadig i gang	Stadig ingen beredskabsplaner
Antal	L, O, P, T	A, B, E, F, H, I, J, K, M, S, X	C, D, G, R

Tabel 24 - Nye eller reviderede beredskabsplaner

Det ses af svarene, at de fleste stadig er i gang med beredskabsplanlægningen.

Hermed et udpluk af sigende citater, der er karakteristiske for svarene i de 3 kategorier:

Svarkategori I:

”(...) en egentlig beredskabsplan eksisterede ikke i forvejen, dækkende alt, det har vi nu via DS 484, og den dækker hele pibetøjet” (T)

Svarkategori II:

”Vi er ikke helt med på beredskabsniveau endnu. Beredskabsplaner er det, vi er mindst parate med. Vi har dog gode nødprocedurer” (A)

”Beredskabsplaner for det daglige eksisterer også i beredskabsplanen, hvor man ved, hvem der gør hvad. (Der er) mangler i beredskabsplan (B)”

”Delvis, meget forskelligt rundt om (...). Der arbejdes videre på det. Har været nedprioriteret” (E)

”Vi har en masse i forhold til brand og tyveri. Men i forhold til it-systemer, nej, ikke på den måde. Vi tror på, vi kan få dem op. DS 484 har dog medført, at vi tænker i beredskabsplaner, fx køling ved nye servere” (H)

”Af det, vi mangler, halter det bl.a. med beredskab” (M)

”Vores svage punkt er beredskabsstyring. Også et organisatorisk problem at få forståelse for det (...) har selv skrevet på 95 % af en beredskabsplan. Den er strandet. Vi siger: Hvis vi kunne få ledelsens commitment med, så var vi færdige” (S)

Svarkategori III:

”(...) Grundlaget for at lave beredskabsplaner bliver dog bedre og bedre” (C)

”Nej, heller ikke for brand og vand. Disse procedurer er stadig et missing link (...) Det er svært, ikke?” (G)

6.8 Awareness

Hvilke midler og metoder er der anvendt for at skabe awareness omkring informationssikkerhed? (spm. 8.1)

Svar	I	II	III	IV	V
	Intranet: vejledninger procedurer Fysisk materiale: Folder, musemåtte, pixi-bog, opslag, klistermærker	Informations- møder Afd.-møder Kurser	Kampagner Konkurrencer Quiz	Orientering til nye medarbejdere	Ingen
Antal	A, C, F, J, L, M, Q, R, S, X	A, D, H, I, L, O, R, T	B, J, M, P, Q	G, L, P, Q	E, K, N, U, V

Tabel 25 - Midler og metoder anvendt til awareness

Det fremgår, at man generelt har anvendt en bred vifte af informations- og kommunikationskanaler i bestræbelserne på at skabe bevidsthed om informationssikkerhed. Og mange af organisationerne har benyttet flere forskellige midler.

Nogle af de interviewede indleder deres svar på spørgsmålet med udsagn som:

”(Vi er) ikke kommet til dette endnu” (C), ”Vi har ikke grebet det an” (F), ”Vi har ikke gjort noget særligt” (G), ”Jeg tror, der udestår awareness-delen” (O)

Når de så uddyber svaret, viser det sig, at de alligevel har gjort meget. 3 af dem ligger endda i de mere formidlingstunge svarkategorier (**I** og **II**), mens blot 1 af dem holder sig til at orientere nye medarbejdere (svarkategori **IV**).

Umiddelbart virker det, som om denne gruppe undervurderer deres egen indsats.

Kun et mindretal har ikke fundet det nødvendigt at fokusere på at skabe bevidsthed om informationssikkerhed (**V**). De udtrykker, at de ikke har gjort noget specielt, og for deres vedkommende passer det. Nogle af dem siger, at der ikke var nogen grund til at øge bevidstheden om informationssikkerhed:

”(...) ingen grund til at lave reklame for det som sådan, det ville nok heller ikke have haft rigtig effekt” (K), ”De ved det godt i forvejen (...) Der er ikke behov for at fortælle igen, fordi folk er pligtopfyldende, og sådan er det bare, naturligvis skal vi gøre det” (U)

>

Mens andre antyder, at der måske burde være gjort noget, men som en af dem siger:

”Hvornår er nok nok?” (N)

Spørgsmålet om awareness-tiltag (spm. 8.1, tabel 25) hænger sammen med det tidligere spørgsmål om, hvordan projektet blev ”solgt” internt (spm. 2.2, tabel 5). Det handler i begge tilfælde om projektets interne markedsføring i kommunikativ og bevidstgørende forstand. Tidsmæssigt går spm. 2.2 på projektets forberedende fase, mens spm. 8.1 drejer sig om tiltagene undervejs i projektet. Det er derfor interessant at sammenligne svarene på de to spørgsmål.

Den gruppe, der ikke har haft fokus på at skabe bevidsthed undervejs i projektet (tabel 25, V), har heller ikke koncentreret sig om at ”sælge” projektet i starten (tabel 5, I-II). De, der har nedprioriteret formidling og kommunikation i løbet af projektet, har med andre ord også gjort det indledningsvis.

Det omvendte er derimod ikke tilfældet, tværtimod. I betragtning af, at hele 15 organisationer ikke ”solgte” projektet til en start (tabel 5, I+II), er det bemærkelsesværdigt, hvor mange der undervejs har taget hånd om at skabe bevidsthed om informationssikkerhed (tabel 25, I+II+III+IV).

Flere af de interviewede påpeger, at der i forvejen i organisationen var en høj bevidsthed om sikkerhed (C, O, S, T, U). De siger fx:

”Jeg hører oftest: ”det gør vi jo” (i forvejen)” (O), ”Det fandtes i forvejen, men er nu strammet op via 484” (S), ”(Bevidstheden) er høj i forvejen (...) Men folk falder jo hen” (T), ”De ved det godt i forvejen” (U)

Men det har ikke afholdt dem fra at gøre noget for at skærpe opmærksomheden. Kun en enkelt af dem ligger i svarkategori V (tabel 25).

Ud over de informations- og kommunikationskanaler, som tabel 25 afspejler, nævner de interviewede en række redskaber, som de har brugt i bevidstgørelsesøjemed:

- It-værktøj til kampagner og test (M, P, T).
En udtaler, at det blev brugt oprindeligt, men at det ikke virkede. En anden, at det var problematisk at få lavet en fornuftig test
- Indrapporteringspligt / Kvartalsvis sikkerhedsrapport (I, R, Q)
- Risikoanalysen (I, R):
”Risikovurderingen gav awareness” (I), ”Det har været håndteret via (...) risikoanalysen (...)” (R)
- Medarbejdernes underskrift på erklæring om sikkerhedsbestemmelser (L, R)
- Benchmark (R)

>

➤ Self-assessment med 135 spørgsmål fra standarden (X)

Et par stykker peger på, at det er svært at få ressourcer til opfølgende aktiviteter (H, X).

Hvordan har organisationen reageret? (spm. 8.2)

Det gennemgående svar på dette spørgsmål er, at organisationen finder de indførte foranstaltninger irriterende og besværlige, men at der er forståelse for nødvendigheden af dem.

Et par citater til illustration af dette:

”Adgangskoder skal fx skiftes i dag, og det føles besværligt og nogle brokker sig, men det er få” (K)

”(…) det er irriterende for folk, at de ikke lige kan bruge fx nogle programmer, men de forstår godt hvorfor (…)” (S)

”(…) rollen som lokal administrator (…) skulle fjernes. Medarbejderne oplever, at man ikke frit kan downloade programmer. Folk har dog haft forståelse for det.” (F)

”De fleste forstår det, og nogle synes, der er besværligt” (P)

”Der har været god forståelse for, at sikkerhed er vigtig” (R)

Ud over regler for skift af password og manglende mulighed for at downloade programmer, nævner nogle stykker også, at organisationen har oplevet indførelsen af spam-filter som en generende restriktion.

Et fåtal nævner, at der ingen forståelse har været:

”(…) Vil helst være fri. Mener ikke, det er så vigtigt og nødvendigt (…)

Det er noget, vi skal leve med. Det er nok holdningen” (A)

”En restgruppe medarbejdere, som enten ikke kan eller vil, gav anledning til møder og ekstra information. Ledelsen har så banket i bordet: I SKAL. Alle er på plads nu, også de mest stridbare (…)” (M)

Men som nævnt er det generelle indtryk, at der er forståelse i organisationerne for sikkerhedsforanstaltningerne. Flere steder har medarbejdere ikke bare accepteret, men ligefrem indoptaget og adopteret sikkerhedsudfordringerne:

”Tog en runde hos folk, forklarede hvorfor dette og hint var interessant, altså: ’what’s in it for me’ – altså en pragmatisk vinkel. Det virkede absolut. Folk ved nu, hvordan de skal agere. Og de skulle forstå, at hvis ting ikke virkede, er det ledelsens problem. Der er absolut sket en holdningsændring hos folk. (…)

Generelt er folk flinke til at indrapportere, så det har i den grad rykket” (I)

”(…) helt klart bedre accept. Man ved, det kommer ovenfra. Men det kommer os også til gavn og tjener os alle. Men det er en stor opgave at synliggøre fordelene” (J)

”Det er interessant, når medarbejdere spontant henvender sig til os. Her mærker vi, at de tænker i sikkerhed, at de er aware. Det får de ros for, og så bliver de glade” (M)

>

”Folk er utroligt fornuftige, og dagligt får jeg henvendelser om gode råd og sikker adfærd.” (S)

Kan man yderligere øge bevidstheden hos medarbejderne? (spm. 8.3)

Det er karakteristisk, at flere af de interviewede peger på eksemplets magt som et tungtvejende pædagogisk middel til bevidstgørelse om informationssikkerhed. Eksempler på hændelser fra dagligdagen, hvor sikkerheden kompromitteres, er noget, man kan forholde sig til:

”Awareness er jo også en løbende proces, fx ud fra hændelser, som (jeg) bruger som læring – uden at løfte pegefingern.” (L)

”Eksempel på printjob, der ligger i alle udbakker. Det er læring. Jeg har vist eksempler med spam-post. Så forstår folk, hvorfor det er godt at have et filter.”

(P)

”Den bedste awareness er at benytte dagligdagens sikkerhedsspørgsmål for at få øget fokus.” (R)

”Ja, via eksempler. Det er et stærkt medie” (S)

En peger dog også på risikoen ved at ’overinformere’:

”Man skal passe på med ikke at være ’på’ for tit, for så bliver det den med Peter og ulven.” (O)

6.9 Opfølgning på implementeringen

Hvordan måles implementeringsgraden hos jer? (spm. 9.1)

De få, der svarer direkte på spørgsmålet, nævner dels Rigsrevisionens besøg dels IT- og Telestyrelsens benchmark.

Hvad skønner du den til at være p.t.? (spm. 9.2)

Svar	I	II	III	IV	V	VI
	< 50%	50-55%	70-75%	80%	90-95%	97%-100%
Antal	G	C, D	F, I, M, N	B, J, L, O, Q, R, T	K, P, S	U, X

Tabel 26 - Skøn på implementeringsgrad

Over halvdelen af de 19, der svarer, vurderer, at deres implementeringsgrad ligger i intervallet 70-80% (III+IV). Det harmonerer godt med, at der er gjort en relativt stor indsats for at øge bevidstheden i organisationerne (tabel 25). Samtidig er det udtryk for en realistisk vurdering: Der er stadig et stykke vej, før man er helt i hus med implementeringen, jf. fx de manglende beredskabsplaner, tabel 24.

En enkelt takserer implementeringsgraden til at være 100% og tilføjer:

”I princippet kan man ikke måle den slags (...) men man kan sige, at vi efterlever den 100%. Jeg har dog ingen revisorpåtegning.” (U)

Hvordan vedligeholdes implementeringen? (spm. 9.3)

I 16 af de i alt 23 interview fremgår det, at man tænker i vedligeholdelse af implementeringen. 1 svarer, at man ikke er nået til det endnu, mens der i de resterende 6 interview ikke figurerer svar på spørgsmålet.

Ligesom med tiltagene for at øge bevidstheden (tabel 25) er der også her tale om et bredt spektrum af virkemidler for at holde implementeringen ved lige.

- Planer for hvad der skal revideres (F, I, N, P)
- Revision og ajourføring af dokumentation 1 gang om året (B, F, O, T)
- Systematiske review (K)
- Løbende vedligeholdelse (L, M, S, U)
- Ved anskaffelser skal der tages stilling til informationssikkerhed (A)
- Rigsrevisionens besøg giver anledning til at tjekke forholdene (E)
- Lokale sikkerhedsudvalg (J, Q)
- Compliance tjekliste fra et it-værktøj (N, P)

>

Flere (C, J, Q) nævner også, at de har planer om at afholde kampagner.

Har nogen vundet, eller har nogen tabt som følge af implementeringen af DS 484? (spm. 9.4)

Svar	I	II	III	IV
	Ulempe: Tungere processer Besværlige krav	Ulempe: Mistet muligheder, frihed, fleksibilitet	Fordel: Større bevidsthed	Fordel: Sikkerhedsniveau højnet
Antal	A, B, I, L, M, O, Q, T, X	F, K, M, S, T	A, C, I, K, L, O	B, E, F, K, M, Q, S, T, X

Tabel 27 - Gevinster og tab ved implementeringen

Svarene på dette spørgsmål fordeler sig i to typer ulemper (**I+II**) og to typer fordele (**III+IV**).

De interviewede peger både på ulemperne og på fordelene. Der er ingen tvivl om, at arbejdet med informationssikkerhed har haft sin pris, men ingen siger, at prisen har været for høj i forhold til udbyttet. Tværtimod tipper svarene klart over til fordel for den positive vægtskål.

9 af de interviewede giver eksplicit udtryk for, at alle har vundet (D, C, F, H, J, P, R, S, T). De siger fx:

”Der er tale om en win-win.” (C)

”Vi vinder. Alle vinder” (D)

”Virksomheden samlet set vinder, der er skabt overblik og sikkerhed i sidste ende” (F)

”(…) alle har vundet noget – især på awareness. Prisen: Vi er blevet bombarderet med en række krav. Det har været irriterende og besværligt.” (I)

”(Organisationen) som sådan har vundet. Vi kunne ikke se os selv om et par år uden denne systematik. (...) Med sikkerhed mister man måske noget fleksibilitet. Vi skærper og skærper.” (T)

”Alle (...) har vundet qua den statslige beslutning, som har givet ledelsesmæssigt fokus.” (R)

”Vi skulle gerne alle have vundet (...) Nogle mener, de har tabt, fordi de har mistet fleksibilitet. Men hovedparten synes, det er supergodt.” (S)

Som et eksempel på at sikkerhedsniveauet er højnet, nævner en (B), at driftsstabiliteten er blevet bedre, og at backup virker. Desuden omtales, at ITIL og informationssikkerhed går hånd i hånd.

Selve DS 484 standarden får også her et par ord med på vejen:

”Havde vi ikke haft standarden, ville vi nok have brugt en konsulent” (E)

>

”Jeg har vundet ved at have en manual. Ellers ville jeg have haft svært ved at vide, hvor jeg skulle starte og slutte. Godt at have det samlet et sted” (N)

”Man slap for at opfinde den dybe tallerken. Og leverandørerne vinder såmænd også (...) 484 er fantastisk, når man skal lave udbudsmateriale” (U)

Standarden kommenteres naturligt nok også ved de næste par spørgsmål.

**Hvilke ændringer kan du foreslå til DS 484 standarden? (spm. 9.5)
Hvad savner du i DS 484 standarden? (spm. 9.5.1)**

Svar	I	II	III
	<ul style="list-style-type: none"> ➤ Tungt stof ➤ Svær at læse ➤ Svær at forstå ➤ Spring i begrebsniveau er: detaljeret teknisk vs. overordnet ➤ Omfangsrig Overvældende ➤ Mange gentagelser, mange overlap ➤ Rodet struktur 	Savner: <ul style="list-style-type: none"> ➤ Udgave for ledelsen (A) ➤ Vejledninger: Formidling og implementering (H) ➤ Overblik, sammendrag (V, X) ➤ Standard paradigmer, procedurer, skabeloner fra centralt hold (I, T) ➤ Køreplan, ’kom godt i gang’ (K) ➤ Struktur: Faser og temaer (K, X) ➤ Eksempler (K, V) ➤ Modenhedsmåling 	Savner: <ul style="list-style-type: none"> ➤ Mere plads og mulighed for lokal tilretning ➤ Fleksibilitet ➤ Alternative muligheder for / tilpasning til små organisationer
Antal	A, B, D, F, K, N, Q	A, F, H, I, K, L, P, R, T, V, X	B, G, M, P, S

Tabel 28 - Ændringer til DS 484-standarden

Det er et gennemgående træk, at man har oplevet DS 484 som svært at gå til. Man har arbejdet en hel del med selve teksten og har haft forståelses- og forklaringsproblemer (I).

Standardens terminologi og struktur er genstand for en hel del kommentarer:

”Den var svært at gå til, og vi skulle selv først forstå den. Tog derfor kapitel for kapitel (...)” (N)

”(...) oversættelsen er ikke heldig. Begrebet informationsaktiv er jo det engelske asset. Brugen af ordet informationsaktiv er en regnskabsterminologi, som slet

>

ikke passer ind i vores sprogbrug. Det påfører os en opgave med megen formidling og forklaring.” (H)

”Den er velformuleret, men ikke let forståelig. Mange ord er næsten identiske, og det virker forvirrende og tager tid at læse og forstå. DS skal tænke på, at en række forskellige brugere skal kunne læse det. Det kan godt gøres meget enklere og mere let forståeligt. Fx opdeling i kapitler. Det er også svært at få det fulde overblik – prøv at sætte cand.mag.er i dansk eller kommunikationsfolk på (...) opdel den i faser, lav en køreplan. Det ville også hjælpe med eksempler.” (K)

”Der er en række uklarheder om terminologi, og vi har forsøgt at definere (...)” (Q)

”Vi har valgt at benytte os af udtrykket ’it’ og ikke ’informations...’, som forvirrer folk. Men vores bestemmelser er forankret i informationssikkerhed.” (R)

”(…) savne(de) et kort overblik over, hvad 484 gik ud på, formuleret i menneskesprog. Jeg efterlyser et resume eller et sammendrag (...) der skal menneskesprog på, så man reelt forstår fx truslen om risiko for tab af data.” (V)

I forlængelse af, at man har haft vanskeligt ved at forholde sig til teksten, og i det hele taget indledningsvis haft svært ved at spore sig ind på projektets omfang og indhold, giver mange udtryk for, at de har savnet hjælpeværktøjer i bred forstand (II). Man efterlyser fx konkrete, operationelle vejledninger, standard skabeloner og paradigmer. Man ville også gerne have haft praktiske køreplaner og eksempler til brug for projektet.

En udtrykker det sådan:

”Der mangler mere om persondataloven og konkrete anvisninger, ITIL, man skal selv finde værktøjerne – og der er ingen best practices og ingen links.” (L)

Flere af de mindre organisationer har følt standardens omfang som en belastning og kunne godt have tænkt sig, at den var fleksibel i forhold til størrelsen af organisationen:

”Det er svært. Der er mange krav. Måske færre krav (...) på nogle af de punkter, for små virksomheder, at pege på alternative muligheder (...) når man er en lille virksomhed” (G)

”(…) man oplever, den kører på store organisationer og ikke (er) indpasset min organisations størrelse.” (M)

”Den dækker for stor en vifte af typer af organisationer og størrelser. Det er svært at være en lille organisation. Den burde være mere nuanceret og den burde indeholde anbefalinger på baggrund af fx størrelsen af organisationen. (...) Og hvor lægger man niveauet, altså hvad er nok. Er nok det, vi kan magte – og er det nok?” (S)

En enkelt af de mindre organisationer omtaler dog standarden som:

>

”(...) et fantastisk værktøj. Jeg kunne gå til direktionen og samtidig beskrive, at det var et krav. Fik direkte accept og støtte. Har ikke oplevet det som en belastning. DS 484 passer godt til (organisationens) størrelse” (T)

Flere andre ytrer sig positivt om standarden, jf. også tidligere:

”Den har været god til at løfte noget” (B)

”(...) kan godt lide den. (Der er) ikke behov for revision, den er rigtig god, fordi den er skrevet, som den er, og handler om det, den gør” (J)

En peger på en del mangler i standarden, bl.a. en klarere temaopdelte struktur, og giver udtryk for, at det havde været rart med en afgrænsning af beredskabsopgaven fx i form af et eksempel på en beredskabsplan. Men slutter alligevel af med at sige:

”Vi er glade for standarden. Den har gjort hverdagen nemmere.” (X)

Hvad er behovet fremover med hensyn til den fællesstatslige indsats inden for informationssikkerhed? (spm. 9.6)

Flere nævner, at gryden skal holdes i kog (H, C, Q), og at der ligger en udfordring i forbindelse med SLA (Service Level Agreement), hvor sikkerhed skal tænkes ind. Man foreslår også, at benchmark gentages (J, R).

Man ser frem til en central styring som en mulig løftestang og forventer sig mere standardisering på området i form af bl.a. fælles regelsæt og politikker, som kan genbruges (M, O), operationelle driftshåndbøger og skabeloner (P, T), en fælles opfattelse og forståelse af sikkerhedsbegrebet (O) og et fælles risikostyringsværktøj med opgørelse af aktiver og klassifikationer (L, O, R).

Nogle (N, X) nævner behovet for at inspirere hinanden og udveksle erfaringer, også om teknik.

Bilag 1: Interviewguide og spørgeramme

>

Interviewguide (læses op ved starten af interviewet)

De følgende emner og spørgsmål har til formål at høre om dine erfaringer fra implementeringen af DS 484 i den institution, styrelse eller det departement, du er ansat i.

Dine erfaringer, som relaterer sig til kompetencer, fremgangsmåder, projektorganisering, intern kommunikation og informationsformidling, ansvarsfordeling og målsætning, har særlig interesse.

Under interviewet kan spørgerammen på næste side anvendes som guideline.

Interviewet skal ses som en samtale, således at viden om dine erfaringer og konstateringer er vigtigere, end at hvert enkelt spørgsmål bliver besvaret specifikt.

Alle deltagere i denne erfaringsopsamling interviewes med udgangspunkt i de samme spørgsmål.

Hvert enkelt interview bliver optaget for at sikre størst mulig udbytte ved den efterfølgende bearbejdning. Optagelsen opbevares af interviewerens, gengives ikke over for andre og slettes efter transskribering.

Videregivelse af oplysninger og erfaringer fra interviewet vil ske i anonymiseret form.

SPØRGERAMME		Emner	Politikker, planer og procedurer	Fremgangsmåde og metode	Kompetencer og forudsætninger	Ansvar og beføjelser	Målsætning og opfølgning	Opmærksomhed og kommunikation
Områder								
Organisering og forberedelse								
Strategi og politik for informationssikkerhed								
Projektorganisering								
Gennemførelse af implementeringen								
Informationsaktiver og								
Risikoen analyse og beredskab								
Awareness								
Opfølgning på implementeringen								

Bilag 2: Indledning i DS 484 standarden

>

Her gengives afsnit 0.1 og 0.2 i DS 484 standardens indledende kap. 0.

6.10 Hvad er informationssikkerhed?

Information er et aktiv, der i lighed med øvrige virksomhedsaktiver er væsentlig for virksomhedens forretningsaktiviteter og derfor skal beskyttes på passende vis. Dette er specielt vigtigt med den øgede digitale informationsudveksling, som har medført en forøgelse af både trusler og sårbarheder, jf. eksempelvis OECD Guidelines.

Information kan eksistere i mange former. Det kan være skrevet på papir, lagret elektronisk, transmitteret via kabler eller gennem luften, ligge på en film eller være fremført i en konversation. Uanset formen skal information beskyttes i henhold til dens betydning for virksomheden.

Informationssikkerhed defineres som den samlede mængde af beskyttelsesforanstaltninger, der skal sikre virksomhedens daglige drift, minimere skader, samt beskytte virksomhedens investeringer og sikre grundlaget for nye forretningsmuligheder.

Informationssikkerhed opnås ved at implementere, overvåge, revurdere og løbende ajourføre et passende sæt af beskyttelsesforanstaltninger bestående af politikker, praksis, procedurer, organisatoriske tiltag og system- eller maskintekniske funktioner.

6.11 Hvorfor er informationssikkerhed nødvendig?

Information og informationsbehandlingsprocesser, -systemer og -netværk er væsentlige virksomhedsaktiver. At definere, etablere og vedligeholde en passende informationssikkerhed kan være afgørende for virksomhedens konkurrencedygtighed, rentabilitet, omdømme og efterlevelse af gældende lovgivning.

Virksomhederne udsættes for en bred vifte af trusler spændende fra svindel, industrispionage, sabotage og terror til ildebrand og oversvømmelse. Trusler som skadevoldende programmer (virus m.m.), uautoriseret indtrængen og blokering af transmissionsforbindelser bliver mere og mere almindelige og mere og mere sofistikerede.

Informationssikkerhed er væsentlig både for den offentlige og den private sektor og for at beskytte kritisk infrastruktur. En troværdig informationssikkerhed er en afgørende forudsætning for digital forvaltning og e-handel. Samtidigt giver det øgede antal adgangsmuligheder, hjemmearbejdspladser og private brugere en øget sårbarhed, da det ikke længere er muligt at forlade sig på traditionelle, centrale sikringsforanstaltninger.

Mange informationssystemer er ikke konstrueret med et forsvarligt sikkerhedsniveau. Det er derfor begrænset, hvor meget sikkerhed der kan opnås

>

med en ren teknisk indsats. Den fornødne sikkerhed må følgelig etableres ved hjælp af organisatoriske og ledelsesmæssige foranstaltninger. Etablering af disse foranstaltninger kræver omhyggelig og detaljeret planlægning.

Implementeringen af en optimal informationssikkerhed kræver som minimum en aktiv medvirken fra alle i virksomheden. Herudover kan det også kræve medvirken fra leverandører, samarbejdspartnere, kunder og andre eksterne interessenter. Det kan endvidere være påkrævet at søge yderligere ekstern bistand.

^
