5/2016

STATSREVISORERNE
RIGSREVISIONEN

Rigsrevisionens beretning om

# styring af it-sikkerhed hos it-leverandører

afgivet til Folketinget med Statsrevisorernes bemærkninger

November 2016

5 /
2016

# Beretning om styring af it-sikkerhed hos it-leverandører

Statsrevisorerne fremsender denne beretning med deres bemærkninger til Folketinget og vedkommende minister, jf. § 3 i lov om statsrevisorerne og § 18, stk. 1, i lov om revisionen af statens regnskaber m.m.

*København 2017*

Denne beretning til Folketinget skal behandles ifølge lov om revisionen af statens regnskaber, § 18:
Statsrevisorerne fremsender med deres eventuelle bemærkninger Rigsrevisionens beretning til Folketinget og vedkommende minister.
Finansministeren, erhvervs- og vækstministeren, skatteministeren, justitsministeren og beskæftigelsesministeren afgiver en redegørelse til beretningen.
Rigsrevisor afgiver et notat med bemærkninger til ministrenes redegørelser.
På baggrund af ministrenes redegørelser og rigsrevisors notat tager Statsrevisorerne endelig stilling til beretningen, hvilket forventes at ske i marts 2017.
Ministrenes redegørelser, rigsrevisors bemærkninger og Statsrevisorernes eventuelle bemærkninger samles i Statsrevisorernes Endelig betænkning over statsregnskabet, som årligt afgives til Folketinget i februar måned – i dette tilfælde Endelig betænkning over statsregnskabet 2016, som afgives i februar 2018.

Henvendelse vedrørende
denne publikation rettes til:

Statsrevisorerne
Folketinget
Christiansborg
1240 København K
Telefon: 33 37 59 87
Fax: 33 37 59 95
E-mail: statsrevisorerne@ft.dk
Hjemmeside: www.ft.dk/statsrevisorerne

Yderligere eksemplarer kan
købes ved henvendelse til:

Rosendahls-Schultz Distribution
Herstedvang 10
2620 Albertslund
Telefon: 43 22 73 00
Fax: 43 63 19 69
E-mail: distribution@rosendahls.dk
Hjemmeside: www.rosendahls.dk

ISSN 2245-3008
ISBN 978-87-7434-508-4

# Statsrevisorernes bemærkning

## BERETNING OM STYRING AF IT-SIKKERHED HOS IT-LEVERANDØRER

Finansministeriet stiller krav om, at statslige myndigheder følger it-sikkerhedsstandarden ISO 27001 til styring af it-sikkerheden, herunder it-sikkerheden hos eksterne it-leverandører. Myndighederne skal sikre en balanceret indsats, der vægter hensynet til brugervenlighed, sikkerhed og økonomi. Indsatsen skal være proportional med de risici, der er på det konkrete område.

Beretningen handler om, hvordan 5 myndigheder: Rigspolitiet (Det Centrale Pasregister), SKAT (TastSelv Borger og Nyt TastSelv Erhverv), Styrelsen for Arbejdsmarked og Rekruttering (Det fælles datagrundlag), Digitaliseringsstyrelsen (NemID) og Søfartsstyrelsen (Skibsregistret) styrer it-sikkerheden hos deres eksterne it-driftsleverandører.

**Statsrevisorerne bemærker, at statslige myndigheder generelt kan outsource it-driften til eksterne it-leverandører, men ikke ansvaret for it-sikkerheden.**

**Statsrevisorerne finder det utilfredsstillende, at 4 ud af de 5 myndigheder ikke har udarbejdet en tilstrækkelig risikovurdering.**

**Statsrevisorerne finder det bekymrende, at myndighederne – med undtagelse af Rigspolitiet – ikke i tilstrækkelig grad stiller krav til it-leverandørernes sikkerhedsniveau. Kravene bør være klare og baseret på risikovurderinger, og myndighederne bør følge op herpå.**

**Statsrevisorerne finder det væsentligt, at Finansministeriet præciserer ansvaret for tilsynet med it-sikkerheden for de it-systemer, som drives af Statens It.**

**STATSREVISORERNE,**
den 9. november 2016

Peder Larsen
Henrik Thorup
Klaus Frandsen
Lennart Damsbo-Andersen
Søren Gade
Simon Emil Ammitzbøll

# INDHOLDSFORTEGNELSE

Rigsrevisionen har selv taget initiativ til denne undersøgelse og afgiver derfor beretningen til Statsrevisorerne i henhold til § 17, stk. 2, i rigsrevisorloven, jf. lovbekendtgørelse nr. 101 af 19. januar 2012.

Beretningen vedrører finanslovens § 7. Finansministeriet, § 8. Erhvervs- og Vækstministeriet, § 9. Skatteministeriet, § 11. Justitsministeriet og § 17. Beskæftigelsesministeriet.

I undersøgelsesperioden har der været følgende ministre:

*Finansministeriet:*
Claus Hjort Frederiksen: juni 2015 -

*Erhvervs- og Vækstministeriet:*
Troels Lund Poulsen: juni 2015 -

*Skatteministeriet:*
Karsten Lauritzen: juni 2015 -

*Justitsministeriet:*
Søren Pind: juni 2015 -

*Beskæftigelsesministeriet:*
Jørn Neergaard Larsen: juni 2015 -

Beretningen har i udkast været forelagt Finansministeriet, Erhvervs- og Vækstministeriet, Skatteministeriet, Justitsministeriet og Beskæftigelsesministeriet, hvis bemærkninger er afspejlet i beretningen.

# 1. Introduktion og konklusion

## 1.1. FORMÅL OG KONKLUSION

1. Denne beretning handler om en række statslige myndigheders styring af it-sikkerheden hos deres eksterne it-driftsleverandører. Beretningen har et fremadrettet perspektiv og giver anbefalinger til at forbedre myndighedernes styring af it-sikkerheden hos leverandørerne. Rigsrevisionen har selv taget initiativ til beretningen, der bygger på it-revisioner, som Rigsrevisionen har udført i 1. halvår 2016.

2. Beretningen handler om følgende 5 myndigheder og 6 it-systemer: Rigspolitiet (Det Centrale Pasregister – herefter Pasregistret), SKAT (TastSelv Borger og Nyt TastSelv Erhverv), Styrelsen for Arbejdsmarked og Rekruttering – herefter STAR (Det fælles datagrundlag – herefter DFDG), Digitaliseringsstyrelsen (NemID) og Søfartsstyrelsen (Skibsregistret).

- Rigspolitiet hører under Justitsministeriet.
- SKAT hører under Skatteministeriet.
- Styrelsen for Arbejdsmarked og Rekruttering hører under Beskæftigelsesministeriet.
- Digitaliseringsstyrelsen hører under Finansministeriet.
- Søfartsstyrelsen hører under Erhvervs- og Vækstministeriet.

3. En stor del af statens it-drift er outsourcet til eksterne it-leverandører. Outsourcing kan give staten en række fordele i forhold til økonomi, kvalitet og organisering. Der har dog i de seneste år været eksempler på alvorlige it-sikkerhedshændelser hos statens eksterne it-leverandører. Fx blev flere af Rigspolitiets systemer i 2012 kompromitteret ved et hackerangreb på it-leverandøren CSC.

4. Myndighederne er ansvarlige for at styre it-sikkerheden, selv om driften af it-systemerne varetages af eksterne it-leverandører. Det er derfor vigtigt, at myndighederne foretager risikovurderinger og på baggrund heraf stiller relevante krav til og følger op på it-sikkerheden i de outsourcede it-systemer. Risikovurderingerne er grundlaget for en tilstrækkelig og velbegrundet styring af it-sikkerheden. Uden en aktiv, risikobaseret styring ved myndighederne ikke, om it-sikkerheden i de outsourcede systemer svarer til myndighedernes behov for sikkerhed.

It-systemer består af forskellige tekniske lag/dele, der tilsammen udgør it-systemernes it-infrastruktur. Det beskrives nærmere i pkt. 10. Der er som udgangspunkt potentielt risici i alle disse lag. Det er derfor vigtigt, at myndighedernes risikovurderinger tager højde for risici i alle lagene i it-infrastrukturen – ofte med input fra leverandørerne. Herved kan myndighederne vurdere, om der er behov for at stille krav til og følge op på it-sikkerheden i alle lagene.

5. Formålet med beretningen er at vurdere, hvordan myndighederne har *styret* it-sikkerheden hos de eksterne leverandører på udvalgte områder, med henblik på at give anbefalinger til, hvordan myndighederne fremadrettet kan forbedre deres styring af it-sikkerheden hos it-leverandører. Konkret har vi undersøgt, om myndighederne har udarbejdet risikovurderinger som grundlag for deres styring. Med afsæt i disse resultater har vi som en "temperaturmåling" undersøgt, om myndighederne har stillet krav om revisorerklæringer og mulighed for at foretage kontrol af it-sikkerheden hos leverandørerne, samt om myndighederne har stillet krav til og fulgt op på leverandørernes adgangsstyring og logning.

Det skal understreges, at beretningen handler om myndighedernes styring af it-sikkerhed og ikke om, hvordan it-sikkerheden er i praksis hos it-leverandørerne i de undersøgte systemer.

## KONKLUSION

Når driften af myndighedernes it-systemer varetages af eksterne leverandører, har myndighederne ikke længere direkte kontrol over it-sikkerheden, men er fortsat ansvarlige for at styre it-sikkerheden. Hvis myndighederne ikke foretager en aktiv, risikobaseret styring af it-sikkerheden, herunder stiller krav til og følger op på it-sikkerheden, har de ikke vished om, hvorvidt leverandørernes it-sikkerhed er tilstrækkelig i forhold til at sikre myndighedernes systemer og data.

Rigsrevisionen vurderer, at hovedparten af de undersøgte myndigheder skal forbedre deres risikovurderinger, som bør danne grundlag for myndighedernes styring af it-sikkerheden hos it-leverandørerne. Rigsrevisionen vurderer desuden, at hovedparten af de undersøgte myndigheder kan forbedre deres krav til og opfølgning på adgangsstyring og logning.

For det første finder Rigsrevisionen det ikke tilfredsstillende, at ingen af myndighederne – på nær Rigspolitiet – har foretaget tilstrækkelige risikovurderinger for de undersøgte it-systemer. Risikovurderingerne er meget overordnede og omfatter ikke alle dele af systemernes it-infrastruktur. Endvidere begrunder myndighederne i deres risikovurderinger ikke deres fravalg i forhold til adgangsstyring og logning i it-infrastrukturen og har derfor ikke dokumenteret deres overvejelser om, at det ikke er nødvendigt at stille krav til og følge op på adgangsstyring og logning i alle dele af it-infrastrukturen. Når myndighederne ikke baserer deres styring af it-sikkerheden på tilstrækkelige risikovurderinger, er der risiko for, at deres styring ikke tager udgangspunkt i myndighedernes dokumenterede behov for sikring af tilgængelighed, fortrolighed og integritet i deres systemer og data.

For det andet finder Rigsrevisionen, at hovedparten af de undersøgte myndigheder fremadrettet kan forbedre deres krav til leverandørerne om adgangsstyring og logning. Myndighederne har enten ikke stillet krav om adgangsstyring og logning eller har stillet generelle, upræcise krav eller krav, der kun omfatter dele af it-infrastrukturen.

Manglende krav eller generelle, upræcise krav, der giver rum for fortolkning i forhold til leverandørens forpligtelser, indebærer en risiko for, at leverandøren ikke har det tilstrækkelige og/eller forventede sikkerhedsniveau.

For det tredje finder Rigsrevisionen, at hovedparten af myndighederne fremadrettet kan forbedre deres opfølgning på leverandørernes adgangsstyring og logning, da de enten ikke har fulgt op på dette eller kun har fulgt op herpå i dele af it-infrastrukturen. I den forbindelse viser revisionen, at nogle af myndighederne kan blive mere bevidste om, hvad deres revisorerklæringer dækker.

For Søfartsstyrelsen og STAR, som er kunder hos Statens It, viser revisionen, at der er uklarhed om ansvars- og opgavefordelingen i forhold til tilsynet med Statens It mellem Finansministeriet og de 2 styrelser. STAR og Erhvervs- og Vækstministeriet, herunder Søfartsstyrelsen, har oplyst, at de 2 styrelser ikke har været opmærksomme på deres forpligtelser i forhold til krav til og opfølgning på it-sikkerhed i de undersøgte it-systemer, da de har en anden opfattelse af ansvars- og opgavefordelingen og finder, at det er dækket af Finansministeriets tilsyn.

Finansministeriet har oplyst, at ministeriet vil tage initiativ til at præcisere omfanget af sit tilsyn med Statens It.

På baggrund af beretningen anbefaler Rigsrevisionen:

- at myndighederne på baggrund af egne risikovurderinger stiller klare krav til leverandørernes sikkerhedsniveau i kontrakten eller i tillæg, allonger eller bilag hertil og tydeliggør, hvilke dele af it-infrastrukturen kravene gælder
- at myndighederne følger op på leverandørernes it-sikkerhed og efterlevelse af krav i alle dele af it-infrastrukturen, medmindre myndighederne i deres risikovurderinger har dokumenteret, at det ikke er nødvendigt.

## 1.2. BAGGRUND

6. Beretningen sætter fokus på den risiko, der er, hvis myndighederne ikke har en aktiv, risikobaseret styring af it-sikkerheden hos de eksterne it-leverandører, herunder at de ikke stiller klare krav til og følger op på it-sikkerheden.

### Styring af it-sikkerhed

7. Finansministeriet stiller krav om, at statslige myndigheder følger it-sikkerhedsstandarden ISO 27001 til styring af it-sikkerheden, herunder også it-sikkerheden hos eksterne it-leverandører. Desuden fremgår det af *National strategi for cyber- og informationssikkerhed,* at myndighederne skal arbejde risikobaseret med sikkerhed og løbende foretage risikovurderinger. Myndighederne skal prioritere indsatsen efter behov og sikre en balanceret indsats, der vægter hensynet til brugervenlighed, sikkerhed og økonomi. Indsatsen skal være proportional med truslerne på det konkrete område. Myndighederne skal fastlægge sikkerhedstiltagene på baggrund af en konkret vurdering af, hvilket sikkerhedsniveau der er nødvendigt.

8. På baggrund af risikovurderingen beslutter myndighederne, hvordan de skal håndtere de identificerede risici. Myndigheden skal ifølge *Guide til implementering af ISO 27001* beskrive de sikkerhedsforanstaltninger, ledelsen har besluttet at gennemføre, i et såkaldt SoA-dokument. Beskrivelsen skal begrunde eventuelle fravalg af kontroller. SoA-dokumentet bruges til at verificere, at myndigheden ikke har undladt vigtige kontroller.

Myndighederne har fra januar 2014 skullet følge ISO 27001 og have færdigimplementeret den primo 2016.

Ifølge *National strategi for cyber- og informationssikkerhed* fra 2014 skal de statslige myndigheder blive bedre til at følge op på sikkerhedsniveauet hos eksterne leverandører. Myndighederne skal således ifølge strategien foretage risikovurderinger af it-sikkerheden samt stille relevante krav til og løbende følge op på it-sikkerheden hos leverandørerne. Dette gælder også, hvor leverandøren er en anden offentlig myndighed, fx Statens It.

**SOA-DOKUMENT**

SoA-dokument (Statement of Applicability) er et centralt dokument i sikkerhedsarbejdet efter ISO 27001.

SoA-dokumentet skal omhandle ledelsens prioritering af sikkerheden, herunder beslutninger om valg og fravalg af sikkerhedsforanstaltninger, i forhold til forretningens mål og risikoprofil.

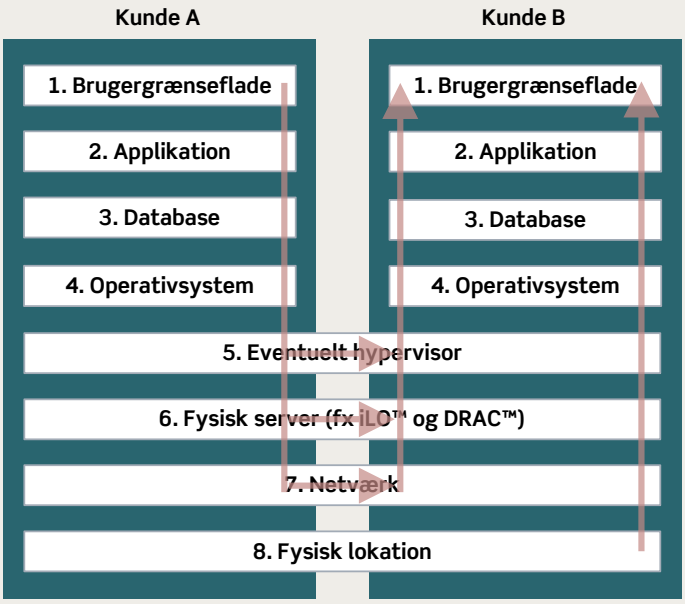
9. Myndighedernes risikovurderinger bør ifølge Digitaliseringsstyrelsens og Center for Cybersikkerheds *Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift* fra 2014 tage udgangspunkt i et opdateret trusselsbillede. Myndighederne bør desuden vurdere risici ud fra karakteren og værdien af data og systemer, som myndighederne er ansvarlige for, herunder hvor kritiske de er.

## Sikkerhedsrisici i it-infrastrukturen

10. It-systemer består af forskellige tekniske lag/dele, der tilsammen udgør it-systemernes it-infrastruktur. Figur 1 viser en forenklet illustration af it-infrastrukturen, som den ofte er sammensat hos en leverandør, hvor kunderne deler services. De undersøgte it-systemer deler i varierende omfang services med andre kunder – som minimum lag 8 (fysisk lokation).

FIGUR 1

**IT-INFRASTRUKTUREN I IT-SYSTEMER**




Kilde: Rigsrevisionen.

Det fremgår af figur 1, at it-infrastrukturens lag 1-4 (brugergrænseflade, applikation, database og operativsystem) typisk vil være adskilt mellem de forskellige kunder i leverandørens it-miljø. Lag 5-8 (hypervisor, fysisk server, netværk og fysisk lokation) vil derimod oftest være fælles services og faciliteter, som flere kunder deles om hos leverandøren.

11. Der er som udgangspunkt potentielt risici og sårbarheder i hvert af lagene i it-infrastrukturen for et it-system. Lagene i it-infrastrukturen hænger indbyrdes sammen.

Derfor vil risici og sårbarheder i ét lag som udgangspunkt kunne få konsekvenser for sikkerheden i hele systemet. En person, der har adgang til ét eller flere lag, kan ved at udnytte tekniske sårbarheder skaffe sig adgang til andre lag. Fx kan en hacker, som udnytter en sårbarhed i it-infrastrukturen til at kompromittere sikkerheden i ét lag, have mulighed for derigennem at skaffe sig adgang til andre lag (illustreret med pilen til højre hos kunde B i figur 1).

Afhængigt af den tekniske opbygning kan der også være risiko for, at en hacker, som udnytter en sårbarhed i it-infrastrukturen hos kunde A, ad den vej kan skaffe sig adgang til it-infrastrukturen hos kunde B og derved kan kompromittere sikkerheden i kunde B's it-system, hvis de har samme leverandør (illustreret med pilen til venstre i figur 1).

Det er derfor vigtigt, at myndighederne sikrer sig, at leverandørerne har truffet de fornødne sikkerhedsforanstaltninger i systemets it-infrastruktur, så dette ikke er muligt. Det betyder, at myndighederne bør stille krav til og følge op på leverandørernes sikkerhed og efterlevelse af krav i hvert af de enkelte lag i it-infrastrukturen, medmindre myndighederne i deres risikovurderinger har dokumenteret, at det ikke er nødvendigt.

For kunder, der ikke deler services, indeholder it-infrastrukturen typisk de samme 8 lag som i figur 1. Her er det dog i forhold til risici blot pilen til højre, der er relevant.

12. Leverandørerne har typisk implementeret en række forskellige sikkerhedsforanstaltninger. Disse foranstaltninger begrænser risikoen i de enkelte lag i it-infrastrukturen og betyder, at der ikke er "fri adgang" for fx en hacker igennem hele it-infrastrukturen fra det ene lag til det andet. Jo flere sikkerhedsforanstaltninger, desto vanskeligere er det at trænge ind i it-infrastrukturen og komme igennem de forskellige lag. Desuden kan myndigheder og leverandører have forskellige kompenserende foranstaltninger, der reducerer konsekvenserne, hvis it-systemer og data bliver kompromitteret. Disse bør indgå i myndighedernes risikovurderinger, for at myndighederne kan have vished om, at leverandørens håndtering af risici og sikkerhedsniveauet er tilstrækkelig.

## De udvalgte myndigheder og it-systemer

13. De udvalgte myndigheder og it-systemer, som beretningen handler om, dækker tilsammen en bred vifte af forskellige myndigheder og it-systemer med forskellige typer af data.

De udvalgte it-systemer understøtter forskellige væsentlige opgaver og services på 5 forskellige ministerområder. Systemerne repræsenterer både ældre og nyere systemer og kontrakter. Nogle af systemerne er rettet mod borgere og virksomheder og forbinder borgere og virksomheder til digitale services. Andre systemer er afgrænsede fagsystemer, som anvendes af medarbejdere. Høj it-sikkerhed er vigtig for alle de udvalgte systemer i form af tilgængelighed, fortrolighed og/eller integritet af data og systemer.

14. Tabel 1 viser de udvalgte it-systemer, de ansvarlige myndigheder og de it-leverandører, som varetager driften af systemerne.

**TABEL 1**

**DE UDVALGTE IT-SYSTEMER**

| System | Myndighed | It-driftsleverandør | Indgåelse af driftskontrakt | Beskrivelse af systemet |
|---|---|---|---|---|
| Det Centrale Pasregister (Pasregistret) | Rigspolitiet | CSC | 2014 | Indeholder pasoplysninger, som bl.a. benyttes af politiet, kommuner, Udenrigsministeriet og Udlændingestyrelsen. |
| Nyt TastSelv Erhverv | SKAT | CSC | 2014 | Er et it-system, hvor virksomheder indberetter deres skatteoplysninger. |
| TastSelv Borger | SKAT | CSC | 1992 | Er et it-system, hvor borgerne indberetter deres skatteoplysninger. |
| Det fælles datagrundlag (DFDG) | Styrelsen for Arbejdsmarked og Rekruttering (STAR) | KMD | 2012 (2015) | Er STAR's tekniske indgang til fælles it på beskæftigelsesområdet. It-systemet understøtter sagsbehandlernes arbejde i kommuner og jobcentre samt borgervendt selvbetjening på Jobnet. |
| NemID | Digitaliseringsstyrelsen | Nets | 2008 | Er et fælles log-in til både offentlige og private selvbetjeningsløsninger og til den enkelte borgers netbank. |
| Skibsregistret | Søfartsstyrelsen | Statens It | 2009 | Er et register, hvor skibe kan registreres. |

Kilde: Rigsrevisionen på baggrund af oplysninger fra de undersøgte myndigheder.

15. Myndighederne har forskellige rammebetingelser for styringen af it-sikkerheden hos it-leverandørerne i de udvalgte systemer.

Skibsregistrets data er i modsætning til de øvrige systemers data offentligt tilgængelige. Erhvervs- og Vækstministeriet har på den baggrund oplyst, at der efter ministeriets opfattelse ikke er behov for samme sikkerhedsniveau som for de andre undersøgte systemer.

Rigsrevisionen konstaterer, at det fremgår af Søfartsstyrelsens risikovurdering, at Skibsregistret understøtter styrelsens kritiske forretningsprocesser, og at integritet og tilgængelighed i forhold til Skibsregistret har stor betydning.

SKATs TastSelv Borger er en del af et systemkompleks, der understøtter borgernes skatteberegning og årsopgørelse. Systemkomplekset består grundlæggende af 2 dele: Mainframe-delen, der udfører beregningen af borgerens skat mv., og TastSelv Borger, der er det system, borgeren benytter til indtastning og godkendelse af forskuds- og årsopgørelsesoplysninger. Revisionen har omfattet TastSelv Borger-delen.

16. Driften af alle de udvalgte it-systemer varetages af eksterne it-leverandører. Dog er NemID og TastSelv Borger ikke outsourcet på samme måde som de andre undersøgte it-systemer. It-systemet bag NemID ejes af Nets. Digitaliseringsstyrelsen køber services, som Nets udbyder. SKAT har kun brugsret til systemet TastSelv Borger. Det er CSC, som ejer systemet. TastSelv Borger hører under en rammekontrakt med CSC fra 1992 sammen med andre af SKATs systemer. Med de valgte løsninger er Digitaliseringsstyrelsen og SKAT dog – ligesom de andre myndigheder – ansvarlige for at foretage risikovurdering samt stille krav til og følge op på it-sikkerheden hos leverandøren.

17. Både STAR og Søfartsstyrelsen er kunder hos Statens It, men på 2 forskellige måder.

Driften af STAR's system DFDG varetages af en ekstern it-driftsleverandør (KMD). STAR er omfattet af Statens It's rammeaftale med eksterne leverandører.

Erhvervs- og Vækstministeriet, herunder Søfartsstyrelsen, er tilsluttet Statens It, som varetager driften af styrelsens it-systemer, herunder Skibsregistret. Styrelsen kan derfor ikke frit vælge driftsleverandør, men skal benytte Statens It som it-driftsleverandør.

Statens It varetager it-driften af Skibsregistret, herunder afvikling af software og drift af fysisk udstyr i lag 1-8 i systemets it-infrastruktur. Søfartsstyrelsen har en vedligeholdelses- og udviklingsaftale med en softwareleverandør. Softwareleverandøren varetager såkaldt application management (dvs. bl.a. fejlsøgning, fejlrettelse og videreudvikling i lag 1, 2 og dele af lag 3 i Skibsregistrets it-infrastruktur). Revisionen omhandler alene Søfartsstyrelsens it-driftskontrakt med Statens It. Vi har således kun undersøgt Søfartsstyrelsens krav og opfølgning i forhold til it-driftsleverandøren Statens It.

At STAR og Søfartsstyrelsen er tilsluttet Statens It har betydning for den måde, hvorpå de skal styre it-sikkerheden hos it-driftsleverandørerne (henholdsvis Statens It og KMD).

### Styring af it-sikkerheden hos Statens It's it-driftsleverandør (KMD) for STAR

18. Aftalen med it-driftsleverandøren stiller krav om revisorerklæring, som omfatter leverandørens kundefælles ydelser. Statens It fører tilsyn (audit) med it-driftsleverandøren på vegne af kunderne, herunder STAR. Tilsynet tager udgangspunkt i de kundefælles ydelser, som revisorerklæringen omfatter (lag 5-8 i it-infrastrukturen).

Det er Rigsrevisionens opfattelse, at STAR har ansvaret for at foretage risikovurderinger, der tager højde for risici i alle 8 lag i deres fagsystem DFDG, og via Statens It stille krav til den eksterne it-driftsleverandør, hvis der på baggrund af risikovurderingen er behov for det.

Desuden skal STAR forholde sig til revisorerklæringen og det tilsyn, som Statens It udfører på vegne af STAR. STAR skal supplere dette med øvrig opfølgning hos it-driftsleverandøren, så STAR samlet set følger op i alle dele af it-infrastrukturen for DFDG.

Statens It har oplyst, at det er Statens It, der er juridisk kontraktpart over for KMD og derfor har ansvaret for, at kontraktens krav til it-sikkerhed opfyldes. Statens It har endvidere oplyst, at STAR har haft mulighed for at stille yderligere krav i forbindelse med kravspecifikationen til it-driftsleverandøren, da STAR har siddet med i styregruppen for udbuddet.

Statens It har oplyst, at Statens It har ansvaret for driftsaftalen med den eksterne leverandør, men at STAR som systemejer har godkendt den kravspecifikation, der ligger til grund for kontrakten med leverandøren. STAR har desuden haft mulighed for løbende at stille supplerende it-sikkerhedsmæssige krav til leverandøren via Statens It.

**FINANSMINISTERIETS TILSYN**

Ifølge Finansministeriet omfatter tilsynet som udgangspunkt ikke kundernes fagspecifikke systemer. Dog bemærkes det, at Finansministeriets tilsyn med Statens It dækker generelle it-kontroller og efterlevelse af ISO-standarden, hvilket udgør et væsentligt grundlag for driften af kundernes fagspecifikke systemer, jf. standardkundeaftalen og tilhørende bilag.

### Styring af it-sikkerhed hos Søfartsstyrelsens it-driftsleverandør (Statens It)

19. Finansministeriet fører tilsyn med Statens It's it-sikkerhed på vegne af de kunder, hvor Statens It varetager driften af deres it-systemer (herunder Søfartsstyrelsen). Finansministeriet løfter dermed tilsynsopgaven for at undgå, at alle ministerier bruger resurser på at føre tilsyn med Statens It.

Det er Rigsrevisionens opfattelse, at ansvaret for at foretage risikovurdering af fagsystemer ligger hos de enkelte kunder, herunder Søfartsstyrelsen. Finansministeriet er enig med Rigsrevisionen heri.

Desuden er de enkelte kunder ansvarlige for at stille krav til Statens It, hvis der på baggrund af deres risikovurdering er behov for det. Endelig er kunderne forpligtede til aktivt at forholde sig til det tilsyn, Finansministeriet fører på vegne af kunderne, fx ved at spørge ind til det eller stille krav til emner, der skal være særligt fokus på. Dette bør ske med udgangspunkt i myndighedernes risikovurdering, så tilsynet afspejler myndighedernes specifikke behov for it-sikkerhed.

Finansministeriet er enig med Rigsrevisionen og vil derfor tage initiativ til at præcisere omfanget af sit tilsyn med Statens It.

Det er Rigsrevisionens opfattelse, at Søfartsstyrelsen således skal foretage en risikovurdering, der tager højde for risici i alle 8 lag i it-infrastrukturen i Skibsregistret og på den baggrund vurdere, om der er behov for at stille krav til og følge op på it-sikkerheden i alle 8 lag i it-infrastrukturen.

STAR og Erhvervs- og Vækstministeriet, herunder Søfartsstyrelsen, har oplyst, at de har en anden opfattelse af ansvars- og opgavefordelingen i forhold til tilsynet med Statens It mellem Finansministeriet og de 2 styrelser, herunder omfanget af deres forpligtelser og Finansministeriets tilsyn.

Bilag 2 beskriver, hvordan Finansministeriet betragter ministeriets tilsyn med Statens It og kundernes forpligtelser. Desuden beskriver bilaget STAR's og Erhvervs- og Vækstministeriets, herunder Søfartsstyrelsens, opfattelse af ansvars- og opgavefordelingen mellem dem og Finansministeriet.

## 1.3. REVISIONSKRITERIER, METODE OG AFGRÆNSNING

### Revisionskriterier

20. Vi har til brug for it-revisionen opstillet revisionskriterier. Beretningen omhandler 16 revisionskriterier, som er en del af en større it-revision. De udvalgte kriterier dækker 4 emner: risikovurdering, revisorerklæringer og kontrol af sikkerhed, adgangsstyring samt logning. Vi har udvalgt disse emner og kriterier, da vi anser dem for at være væsentlige for styring af it-sikkerhed.

### De valgte emner og kriterier

21. Vi har undersøgt myndighedernes risikovurderinger, som er grundlaget for en tilstrækkelig og velbegrundet styring af it-sikkerheden. På baggrund af risikovurderingerne skal myndighederne beslutte, hvordan de kan håndtere de identificerede risici, og hvilke foranstaltninger de vil implementere, herunder hvilke sikkerhedsmæssige aspekter det er relevant at stille krav om og følge op på.

I forlængelse heraf har vi undersøgt myndighedernes krav til revisorerklæringer, herunder hvad erklæringerne dækker, og myndighedernes krav om mulighed for at foretage kontrol/inspektion hos leverandørerne. Revisorerklæringerne spiller en vigtig rolle i myndighedernes styring af it-sikkerheden, da de giver myndighederne information om, hvorvidt it-sikkerheden er i orden på de områder, erklæringerne omfatter. Myndighedernes kontrol/inspektion (fx via tredjepart) spiller også en vigtig rolle, da den kan give myndighederne information om forhold, der ikke er omfattet af revisorerklæringerne.

Adgangsstyring og logning er 2 vigtige aspekter af it-sikkerhed, som begge indgår som kontroller i ISO 27001. Vi har derfor – med afsæt i resultaterne om risikovurderinger og som en "temperaturmåling" på myndighedernes krav og opfølgning – undersøgt, om myndighederne har stillet krav til og fulgt op på leverandørernes adgangsstyring og logning.

22. De emner og kriterier, beretningen omhandler, omfatter blot en del af den samlede it-sikkerhed. De udgør derfor ikke en udtømmende liste for, hvordan myndighederne skal styre it-sikkerheden hos leverandørerne, herunder hvilke krav myndighederne bør stille. Opfyldelse af kriterierne er derfor ikke ensbetydende med en tilstrækkelig styring af it-sikkerheden. Det fremgår af bilag 1, hvad kriterierne er baseret på.

23. Som det fremgår af tabel 1, er flere af kontrakterne for de undersøgte systemer indgået, før den nationale strategi fra 2014 og vejledninger mv. udkom. På baggrund af grundprincipperne i ISO 27001 finder Rigsrevisionen det vigtigt, at myndighederne foretager risikovurderinger løbende, og at myndighederne på baggrund heraf stiller nye relevante krav til sikkerhedstiltag, selv om kontrakterne er indgået på et tidligere tidspunkt. Dette kan fx ske i form af allonger, tillægsaftaler og/eller bilag.

### Metode

24. Beretningen bygger på it-revisioner, som vi har udført i 1. halvår 2016. Som en del af it-revisionen har vi været på revisionsbesøg hos hver myndighed – enten hos myndigheden med deltagelse af leverandøren og/eller hos leverandøren. Endvidere har vi afholdt opfølgende møder med myndigheder/leverandører. For at sikre sammenlignelighed på tværs af myndighederne har vi taget udgangspunkt i den samme spørgeramme, dog tilpasset de konkrete systemer.

Vores dokumentation bygger bl.a. på relevant skriftligt materiale fra myndighederne, fx risikovurderinger, kontrakter, materiale, som understøtter kontrakterne, og revisorerklæringer.

Herudover har vi været i dialog med Center for Cybersikkerhed og gjort brug af konsulentbistand fra Rambøll Management.

Den metodiske tilgang er nærmere beskrevet i bilag 1.

25. Revisionen er udført i overensstemmelse med god offentlig revisionsskik, der er baseret på de grundlæggende revisionsprincipper i rigsrevisionernes internationale standarder (ISSAI 100-999).

## Afgrænsning

26. Beretningen giver et øjebliksbillede af, hvordan myndighederne på revisionstidspunktet har styret it-sikkerheden hos it-leverandørerne på en række væsentlige områder.

27. Beretningen handler om myndighedernes styring af it-sikkerheden hos it-driftsleverandørerne. Beretningen handler ikke om, hvordan it-sikkerheden er i praksis hos leverandørerne, og hvilke konsekvenser en eventuel manglende sikkerhed kan have. Vi har dog beskrevet et par anonymiserede eksempler på praksis. De viser vigtigheden af myndighedernes styring, men indgår ikke i vurderinger og resultater. Vi har desuden ikke vurderet kvaliteten af den revision, de private revisorer har udført.

28. Vi har undersøgt myndighedernes krav til og opfølgning på it-driftsleverandørernes adgangsstyring og logning i forhold til medarbejderne hos driftsleverandørerne. Vi har ikke undersøgt adgangsstyring og logning i forhold til brugerne af applikationen (fx sagsbehandlere eller borgere).

Vi har desuden kun undersøgt myndighedernes styring af it-sikkerheden hos *it-driftsleverandører* og ikke hos leverandører eller eksterne konsulenter, der varetager vedligehold og udvikling mv. Vi har derfor kun gennemgået myndighedernes driftskontrakter med it-driftsleverandører.

29. Bilag 3 indeholder en ordliste, der forklarer udvalgte ord og begreber.

# 2. Myndighedernes styring af it-sikkerheden

## 2.1. MYNDIGHEDERNES RISIKOVURDERINGER

30. Vi har undersøgt, om myndighederne har foretaget risikovurderinger af it-sikkerheden i systemernes it-infrastruktur, der bl.a. omfatter adgangsstyring og logning.

31. Der er som udgangspunkt potentielt risici og sårbarheder i hvert af de enkelte lag i it-infrastrukturen for et it-system. ISO 27001 giver imidlertid ikke konkrete anvisninger til, hvad der skal være omfattet af risikovurderingen for at give et præcist billede af it-sikkerhedsrisici, og ISO 27001 forholder sig fx ikke til begrebet it-infrastrukturen.

Det er dog på baggrund af principperne i ISO 27001 og vejledninger mv. (jf. bilag 1) Rigsrevisionens opfattelse, at det er den enkelte myndigheds ansvar at sikre, at myndighedens risikovurdering dækker alle lagene i it-infrastrukturen for it-systemet, og at risikovurderingen tager udgangspunkt i myndighedens behov i forhold til at sikre tilgængelighed, fortrolighed og/eller integritet i it-systemet og data. De seneste års sikkerhedshændelser viser vigtigheden heraf. Navnlig i forhold til lag 5-8 vil myndighederne dog ofte være afhængige af input fra leverandørerne for at identificere risici i disse lag og vurdere, hvad de betyder for systemet.

Det er endvidere Rigsrevisionens opfattelse, at hvis myndighederne ikke har foretaget en risikovurdering af systemerne og sikret, at risikovurderingen dækker de enkelte lag i it-infrastrukturen og ikke har taget stilling til risici heri, så ved myndigheden ikke, i hvilket omfang der er risici i de enkelte lag i it-infrastrukturen, og i hvilket omfang leverandørens sikkerhedsforanstaltninger tager hånd om disse risici. Myndighederne ved heller ikke, hvilke sikkerhedskrav det er relevant at stille til leverandøren, og hvilke der eventuelt kan undlades, hvis der ikke er behov. Det er derfor Rigsrevisionens opfattelse, at myndighederne bør foretage risikovurderinger, der tager højde for risici i alle lagene i it-infrastrukturen.

32. Revisionen viser, at Rigspolitiet har foretaget en risikovurdering af sine vigtigste forretningsmæssige processer og de understøttende it-systemer (herunder Pasregistret) og har gennemført omfattende sikkerhedsanalyser hos leverandøren. Rigspolitiet har i sit SoA-dokument aktivt tilvalgt at implementere alle kontroller fra ISO 27001, herunder adgangsstyring og logning. Rigsrevisionen vurderer, at Rigspolitiets risikovurdering, sikkerhedsanalyser og SoA-dokument tilsammen omfatter alle dele af it-infrastrukturen for Rigspolitiets centrale systemer, herunder Pasregisteret.

SKAT har udarbejdet en risikovurdering af et større systemkompleks, som TastSelv Borger er en del af. TastSelv Borger fremgår ikke eksplicit af risikovurderingen. Rigsrevisionen vurderer på den baggrund, at SKAT ikke har foretaget en egentlig risikovurdering af TastSelv Borger.

SKAT (for Nyt TastSelv Erhverv), Digitaliseringsstyrelsen, STAR og Søfartsstyrelsen har foretaget risikovurderinger, der kun generelt eller i nogen grad omfatter adgangsstyring og logning i it-infrastrukturen.

SKAT (for Nyt TastSelv Erhverv) og Digitaliseringsstyrelsen har udarbejdet systemspecifikke risikovurderinger, der bl.a. omhandler adgangsstyring og logning. Risikovurderingerne er imidlertid meget overordnede og mangler begrundelser. Derfor giver de ikke et dækkende billede af risici i forhold til bl.a. adgangsstyring og logning i it-infrastrukturen.

STAR og Søfartsstyrelsen har udarbejdet risikovurderinger, som omfatter myndighedernes vigtige forretningsprocesser og de understøttende it-systemer, herunder de undersøgte systemer. Risikovurderingerne er dog overordnede, da de ikke forholder sig detaljeret til bl.a. adgangsstyring og logning i de undersøgte systemers it-infrastruktur.

Revisionen viser således, at de myndigheder, der ikke har tilstrækkelige risikovurderinger, ikke har begrundet deres fravalg på baggrund af deres risikovurderinger i forhold til adgangsstyring og logning i it-infrastrukturen for de undersøgte it-systemer.

Revisionen viser videre, at myndighedernes risikovurderinger – med undtagelse af Rigspolitiet – ikke omfatter alle dele af it-infrastrukturen.

## RESULTATER

Rigsrevisionen vurderer, at myndighederne – bortset fra Rigspolitiet – ikke har udarbejdet tilstrækkelige risikovurderinger, hvilket er en forudsætning for, at myndighederne kan vurdere, begrunde og prioritere, hvilke krav der er relevante at stille til leverandørernes it-sikkerhed, herunder bl.a. i forhold til adgangsstyring og logning i it-infrastrukturen.

Revisionen viser, at Rigspolitiet har valgt at implementere alle kontroller fra ISO 27001, herunder om adgangsstyring og logning. Ingen af de øvrige myndigheder har i deres risikovurderinger dokumenteret, at det ikke er nødvendigt at stille krav til og følge op på adgangsstyring og logning i alle dele af it-infrastrukturen. Desuden er risikovurderingerne – med undtagelse af Rigspolitiet – overordnede og omfatter ikke alle dele af it-infrastrukturen i de undersøgte systemer.

Når myndighedernes styring af it-sikkerheden ikke er baseret på tilstrækkelige risikovurderinger, er der risiko for, at deres styring af it-sikkerheden ikke tager udgangspunkt i myndighedernes dokumenterede behov i forhold til beskyttelse af tilgængelighed, fortrolighed og integritet af deres systemer og data.

## 2.2. MYNDIGHEDERNES KRAV OM REVISORERKLÆRINGER OG KONTROL AF IT-SIKKERHED

33. Vi har undersøgt, om myndighederne har stillet krav om at modtage en årlig revisorerklæring om leverandørens it-sikkerhed og krav om adgang til at foretage kontrol af it-sikkerheden hos leverandørerne i systemernes it-infrastruktur (fx via tredjepart).

34. Ifølge *Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift* bør myndighederne sikre sig, at leverandørerne i relevant omfang er underlagt uafhængig ekstern it-sikkerhedsrevision, og at revisionsrapporterne løbende gøres tilgængelige for myndighederne.

Myndighederne bør desuden ifølge anbefalingerne aftale og formulere en ret til at foretage kontrol af efterlevelsen af aftalte sikkerhedskrav. Når myndighederne indgår kontrakt, bør de således ifølge anbefalingerne overveje, om det er anført i kontrakten, at myndigheden (oftest via en uafhængig revisor) skal have adgang til fx én gang årligt at foretage en passende inspektion af håndtering af data hos leverandøren. Alternativt, at leverandøren via en uafhængig revisor redegør for, hvordan leverandørens it-infrastruktur, herunder sikkerhedsspecifikationer, håndteres.

### Myndighedernes krav om en årlig revisorerklæring om leverandørernes it-sikkerhed

35. Flere af myndighederne har oplyst, at leverandørerne er ISO 27001-certificerede, og at det efter myndighedernes opfattelse betyder, at leverandørernes it-sikkerhed er i orden.

Rigsrevisionen finder, at ISO-certificeringen er vigtig, idet certificeringen viser, at den pågældende leverandør har etableret hensigtsmæssige processer for styring af it-sikkerheden. Imidlertid tager ISO-certificeringen udgangspunkt i leverandørens risikovurdering og ikke i myndighedens risikovurdering. Det er derfor vigtigt, at myndighederne stiller krav om revisorerklæringer og adgang til at foretage kontrol/inspektion af it-sikkerheden hos leverandøren. Det er ligeledes vigtigt, at myndighederne løbende følger op på it-sikkerheden (jf. afsnit 2.3 og 2.4).

Kriteriet om revisorerklæring er ikke relevant for Søfartsstyrelsen, da Rigsrevisionen er revisor for både Statens It og Søfartsstyrelsen.

36. Revisionen viser, at Rigspolitiet, SKAT (for Nyt TastSelv Erhverv), STAR og Digitaliseringsstyrelsen har stillet krav om at modtage en årlig revisorerklæring om leverandørens it-sikkerhed. Revisionen viser også, at der er forskel på, hvilken form for revisorerklæring der er tale om og dermed, hvad erklæringerne dækker.

Rigspolitiet har stillet krav om revisorerklæring, der specifikt dækker deres systemer hos leverandøren, herunder Pasregistret, og som bl.a. forholder sig til adgangsstyring og logning.

SKAT (for Nyt TastSelv Erhverv) har i forbindelse med en ny kontrakt stillet krav om fremover at modtage en systemspecifik revisorerklæring. SKAT har modtaget denne, efter revisionen er afsluttet. SKAT har hidtil modtaget en generel revisorerklæring.

STAR modtager ligeledes en generel revisorerklæring.

Generelle revisorerklæringer er ikke kunde- og systemspecifikke. De omhandler leverandørernes generelle it-kontroller og dækker leverandørernes fælles it-miljø, der normalt kun dækker lag 5-8 i it-infrastrukturen. Hvis myndighederne følger op på it-sikkerheden hos leverandørerne alene ved hjælp af en generel revisorerklæring, dækker myndighedernes opfølgning derfor ikke alle dele af it-infrastrukturen – og muligvis heller ikke kontroller, som myndighederne måtte finde relevante på baggrund af risikovurderingen.

Digitaliseringsstyrelsen har stillet krav om at modtage en systemspecifik revisorerklæring fra leverandørens uafhængige revisor og et revisionsprotokollat (herefter samlet benævnt revisorerklæring). Tilsynskonceptet for NemID fremgår af boks 1.

**BOKS 1**

### TILSYNSKONCEPTET FOR NEMID

Digitaliseringsstyrelsen har oplyst, at NemID er omfattet af den såkaldte OCES-standard og det deri beskrevne tilsyn. Styrelsen har oplyst, at tilsynet blev etableret fuldstændig i overensstemmelse med tilsyn for kvalificerede certifikater i den daværende lov om elektroniske signaturer, og at de samme rammer omkring tilsyn er fastholdt i den såkaldte eIDAS-forordning (EU nr. 910/2014). Digitaliseringsstyrelsen har videre oplyst, at styrelsen følger tilsynsrammerne i forordningen tæt og desuden fører tilsyn hvert år frem for hvert andet år, som kravet lyder. Styrelsens opfølgning og tilsyn er baseret på en statsautoriseret revisors erklæring om, hvorvidt Nets lever op til kravene i OCES-certifikatpolitikken (CP) og følger den praksis, der er beskrevet i Certification Practice Statement (CPS). Endelig har Digitaliseringsstyrelsen oplyst, at den statsautoriserede revisor udfører sin revision i overensstemmelse med den såkaldte ISAE 3000-standard.

Som det fremgår af boks 1, er Digitaliseringsstyrelsens tilsynskoncept baseret på en revisorerklæring, som udføres af en statsautoriseret revisor i overensstemmelse med ISAE 3000-standarden. Digitaliseringsstyrelsen finder derfor, at de har levet op til kravet ved at følge tilsynsrammerne og standarden. Det er Rigsrevisionens opfattelse, at revisorerklæringen er formuleret meget overordnet og ikke indeholder informationer om, hvilke kontroller og tests revisorerklæringen er baseret på, og hvilke lag i it-infrastrukturen revisionen har dækket. Ved at modtage informationer herom kan tilsyn og opfølgning styrkes yderligere.

Revisionen viser, at de øvrige undersøgte myndigheder, som modtager revisorerklæringer, modtager informationer om de udførte kontroller og tests, hvilket skaber gennemsigtighed om, hvad revisorerklæringerne er baseret på, og giver myndighederne mulighed for at vurdere, om der eventuelt er behov for yderligere, supplerende opfølgning.

SKAT (for TastSelv Borger) har valgt ikke at få en årlig revisorerklæring.

### Myndighedernes krav om adgang til at foretage kontrol/inspektion af it-sikkerhed hos leverandørerne

37. Ved at stille krav om adgang til at foretage kontrol/inspektion hos leverandøren (fx via tredjepart) kan myndighederne supplere den ovennævnte opfølgning, så den dækker alle dele af it-infrastrukturen og alle relevante kontroller. Adgang til at foretage kontrol giver desuden mulighed for at kontrollere it-sikkerheden hos leverandøren, hvis myndigheden finder behov for det. Det er derfor et vigtigt krav, uanset om myndighederne modtager en generel eller en systemspecifik revisorerklæring.

Kriteriet om adgang til at foretage kontrol/inspektion hos leverandøren er ikke relevant for Søfartsstyrelsen, der som kunde hos Statens It ikke har til opgave at foretage denne kontrol/inspektion. Søfartsstyrelsen har dog som led i sin opfølgning mulighed for at bede Statens It om rapportering om konkrete sikkerhedsforhold, som er relevante for deres system.

38. Revisionen viser, at alle øvrige myndigheder – undtagen SKAT (for TastSelv Borger) – ifølge kontrakten har adgang til at foretage kontrol/inspektion hos leverandøren. De kan både selv kontrollere sikkerheden hos leverandøren, eller de kan foretage kontrol via tredjepart.

Revisionen viser også, at Rigspolitiet og SKAT (for Nyt TastSelv Erhverv) har benyttet sig af denne mulighed og har foretaget analyser af it-sikkerheden hos leverandøren via tredjepart. Rigspolitiet har desuden indført stikprøvevis kontrol af leverandørens sikkerhedsydelser, og den årlige it-revision vil fremadrettet blive foretaget af en revisor, som Rigspolitiet og leverandøren har udpeget i fællesskab.

## RESULTATER

Revisionen viser, at de fleste myndigheder har stillet krav om revisorerklæring og krav om adgang til at foretage kontrol/inspektion af it-sikkerheden hos leverandøren (fx via tredjepart).

Rigsrevisionen vurderer, at det er vigtigt, at myndighederne bliver mere bevidste om, hvad deres revisorerklæring dækker/ikke dækker, så de på anden vis kan følge op på det, revisorerklæringen ikke dækker.

## 2.3. MYNDIGHEDERNES KRAV OM OG OPFØLGNING PÅ ADGANGSSTYRING

39. Som nævnt er det vigtigt, at myndighederne foretager risikovurderinger og på baggrund heraf stiller relevante krav til og følger op på it-sikkerheden i de outsourcede it-systemer. På baggrund af myndighedernes risikovurderinger kan myndighederne vurdere, om der er behov for at stille krav til og følge op på adgangsstyring i alle lag i it-infrastrukturen.

Revisionen viser som nævnt i afsnit 2.1, at Rigspolitiet har valgt at implementere alle kontroller fra ISO 27001, herunder adgangsstyring. Ingen af de øvrige myndigheder har i deres risikovurderinger begrundet fravalg i forhold til adgangsstyring og har ikke dokumenteret, at det ikke er nødvendigt at stille krav til og følge op på adgangsstyring i alle dele af it-infrastrukturen.

Vi har derfor som en "temperaturmåling" undersøgt, om myndighederne har stillet krav til og fulgt op på leverandørernes adgangsstyring i systemernes it-infrastruktur.

### Myndighedernes krav om og opfølgning på, at leverandørerne begrænser medarbejdernes adgang og foretager brugerrettighedskontrol

40. Ifølge *Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift* er der behov for, at myndighederne bl.a. stiller krav til adgangskontroller, herunder krav til, at leverandøren vurderer behovet for medarbejderes adgang til systemer og data. Ifølge anbefalingerne skal myndighederne sikre, at leverandørerne begrænser medarbejdernes adgang til systemer og data til, hvad der er behov for. Desuden skal myndighederne sikre, at leverandørerne har passende processer for brugerrettighedsstyring og fører den nødvendige løbende kontrol hermed.

Jo flere medarbejdere, der har adgang, desto større er risikoen for misbrug og kompromittering af systemer og data. Der er dels risiko for internt misbrug, hvor medarbejdere misbruger deres rettigheder og adgang eller håndterer rettighederne uforsigtigt, dels risiko for eksternt misbrug, hvor fx en hacker, der er trængt ind i myndighedens it-systemer og it-infrastruktur, overtager og misbruger medarbejderes adgang og rettigheder.

41. Derfor har Rigsrevisionen undersøgt, om myndighederne dels har stillet krav om, at leverandøren begrænser sine medarbejderes adgang til, hvad der er et arbejdsbetinget behov for, dels har stillet krav om, at leverandøren foretager brugerrettighedskontroller (dvs. kontrol af, at kun godkendte medarbejdere med et arbejdsbetinget behov er blevet tildelt adgang).

42. Revisionen viser, at Rigspolitiet og SKAT (for Nyt TastSelv Erhverv) har stillet begge krav for alle dele af it-infrastrukturen.

Derimod har SKAT (for TastSelv Borger), STAR og Digitaliseringsstyrelsen enten stillet generelle, upræcise krav eller kun stillet krav til en del af it-infrastrukturen, mens Søfartsstyrelsen ikke har stillet disse krav.

Fx har STAR i aftalegrundlaget fastlagt, at leverandøren skal foretage adgangsstyring i de konkrete dele af it-infrastrukturen (for DFDG), som opbevarer og behandler persondata. Det er Rigsrevisionens opfattelse, at dette dækker lag 1-4, og at kravet derfor ikke gælder for resten af it-infrastrukturen.

Revisionen har vist et eksempel på, hvilken konsekvens det kan have, når myndighederne ikke gør det klart, at et krav om fx adgangsstyring omfatter alle dele af it-infrastrukturen, og der derfor er rum for fortolkning i forhold til leverandørens forpligtelse, jf. boks 2.

**BOKS 2**

### EKSEMPEL PÅ KONSEKVENSEN AF UKLARHED OM, HVORVIDT KRAV GÆLDER ALLE DELE AF IT-INFRASTRUKTUREN

En af de undersøgte myndigheder har stillet et krav om, at leverandøren begrænser sine medarbejderes adgang ud fra et arbejdsbetinget behov, og forventede, at kravet gjaldt for hele it-infrastrukturen. Vores revision viser imidlertid, at leverandøren tillod adgang for et stort antal personer, der ikke alle havde et specifikt arbejdsbetinget behov, til det serverrum, hvor myndighedens system er placeret (lag 8 i it-infrastrukturen (fysisk lokation)).

43. Rigsrevisionen har desuden undersøgt, om myndighederne har fulgt op på, at leverandørerne har foretaget brugerrettighedskontroller.

**BRUGERRETTIGHEDS-KONTROL**
Brugerrettighedskontrol er en kontrol af, at kun godkendte medarbejdere med et arbejdsbetinget behov er blevet tildelt adgang og rettigheder til systemer og data.

44. Revisionen viser, at Rigspolitiet og STAR har fulgt op på, at leverandøren har foretaget brugerrettighedskontroller i alle dele af it-infrastrukturen.

Rigspolitiet har fulgt op herpå i alle dele af it-infrastrukturen ved hjælp af systemspecifikke revisorerklæringer og har også på anden vis konkret fulgt op på adgangsstyring og logning.

STAR har fulgt op via en generel revisorerklæring, som dækker leverandørens fælles it-miljø (lag 5-8 i it-infrastrukturen) STAR har udført supplerende opfølgning på leverandørens brugerrettighedskontroller for lag 1-4 og har derfor fulgt op i alle dele af it-infrastrukturen.

Digitaliseringsstyrelsen og SKAT (for Nyt TastSelv Erhverv) har kun fulgt op på leverandørens brugerrettighedskontrol i dele af it-infrastrukturen, mens SKAT (for TastSelv Borger) og Søfartsstyrelsen ikke har fulgt op.

Fx har Digitaliseringsstyrelsen fulgt op på leverandørens brugerrettighedskontrol via en systemspecifik revisorerklæring. Som nævnt i afsnit 2.2 indeholder revisorerklæringen ikke informationer om, hvilke kontroller og tests revisorerklæringen er baseret på, eller hvilke lag i it-infrastrukturen revisor har gennemgået. Leverandørens eksterne revisor har oplyst til Rigsrevisionen, at deres revision har dækket adgangsstyring (herunder brugerrettighedskontrol) og logning i væsentlige dele af it-infrastrukturen. Digitaliseringsstyrelsen har ikke selv indhentet oplysninger om de udførte kontroller og tests og har derfor ikke med sikkerhed kunnet vide, om revisorerklæringen dækker alle dele af it-infrastrukturen.

### Myndighedernes krav om og opfølgning på, at privilegerede brugere hos leverandørerne anvender stærke passwords

45. Privilegerede brugere har omfattende adgang og rettigheder til it-systemer og data. Ved at bryde deres passwords kan uvedkommende personer overtage rettighederne og tiltvinge sig adgang til it-systemer og data.

Myndighederne kan mindske denne risiko ved at stille krav om, at de privilegerede brugere hos leverandøren anvender stærke passwords. Der findes også andre vigtige sikkerhedstiltag, som kan begrænse denne risiko, fx segmentering og to-faktorvalidering. Stærke passwords er dog en basal form for adgangsstyring.

Myndighedernes risikovurderinger har ikke dokumenteret, at leverandørerne har sikkerhedsforanstaltninger, der begrænser relevansen af stærke passwords.

46. Derfor har Rigsrevisionen undersøgt, om myndighederne har stillet krav om, at privilegerede brugere hos leverandørerne anvender stærke passwords.

47. Revisionen viser, at Rigspolitiet, STAR, Digitaliseringsstyrelsen og Søfartsstyrelsen har stillet krav herom i alle dele af it-infrastrukturen.

Derimod har SKAT (for Nyt TastSelv Erhverv) stillet et generelt, upræcist krav om, at privilegerede brugere hos leverandøren anvender stærke passwords. Det er uklart, hvilke dele af it-infrastrukturen kravet gælder. SKAT har for TastSelv Borger ikke stillet krav herom.

48. Rigsrevisionen har også undersøgt, om myndighederne har fulgt op på, at privilegerede brugere hos leverandøren anvender stærke passwords.

49. Revisionen viser, at Rigspolitiet som den eneste myndighed har fulgt op på, at privilegerede brugere hos leverandøren anvender stærke passwords, i alle dele af it-infrastrukturen.

STAR og Digitaliseringsstyrelsen har kun fulgt op herpå i dele af it-infrastrukturen, mens SKAT (for begge de undersøgte systemer) og Søfartsstyrelsen ikke har fulgt op.

#### *Uklarhed om tilsynsforpligtelsen, herunder pligten til at stille krav om og følge op på adgangsstyring*

50. Revisionen viser, at der er uklarhed om ansvars- og opgavefordelingen i forhold til tilsynet med Statens It mellem Finansministeriet samt henholdsvis Søfartsstyrelsen og STAR, som er kunder hos Statens It, jf. bilag 2.

51. STAR og Erhvervs- og Vækstministeriet, herunder Søfartsstyrelsen, har oplyst, at de 2 styrelser ikke har været opmærksomme på deres forpligtelser med hensyn til krav og opfølgning i forhold til Statens It. Det skyldes, at de har en anden opfattelse af ansvars- og opgavefordelingen i forhold til tilsynet med Statens It mellem Finansministeriet og de 2 styrelser, herunder omfanget af deres forpligtelser og Finansministeriets tilsyn.

### RESULTATER

Revisionen viser, at kun Rigspolitiet har stillet alle de undersøgte krav til adgangsstyring i alle dele af it-infrastrukturen og fulgt op herpå i alle dele af it-infrastrukturen.

De øvrige myndigheder har i større eller mindre grad forbedringsmuligheder i forhold til deres krav til adgangsstyring og/eller opfølgning herpå.

Forbedringsmulighederne i forhold til krav omfatter, at myndighederne enten ikke har stillet krav, har stillet krav, der kun omfatter dele af it-infrastrukturen, eller har stillet generelle, upræcise krav, hvor det ikke tydeligt fremgår, hvilke lag i it-frastrukturen kravene gælder. Forbedringsmulighederne i forhold til opfølgning omfatter, at myndighederne enten ikke har fulgt op eller kun har fulgt op i dele af it-infrastrukturen.

Rigsrevisionen vurderer, at manglende krav overlader det til leverandørerne at fastsætte sikkerhedsniveauet. Generelle krav giver rum for fortolkning af, hvad leverandørerne er forpligtede til. Begge dele indebærer en risiko for, at leverandørernes adgangsstyring ikke er, som myndighederne forventer og/eller har behov for.

Når myndighederne ikke følger op eller kun følger op i dele af it-infrastrukturen, ved de ikke, om sikkerheden er i orden, og om leverandørerne efterlever kravene, herunder om leverandørerne har en anden fortolkning af kravene.

Revisionen viser, at der er uklarhed om ansvars- og opgavefordelingen i forhold til tilsynet med Statens It mellem Finansministeriet samt henholdsvis STAR og Søfartsstyrelsen, som er kunder hos Statens It. STAR og Erhvervs- og Vækstministeriet, herunder Søfartsstyrelsen, har oplyst, de 2 styrelser ikke har været opmærksomme på deres forpligtelser med hensyn til krav og opfølgning i forhold til Statens It. Det skyldes, at de har en anden opfattelse af ansvars- og opgavefordelingen i forhold til tilsynet med Statens It mellem Finansministeriet og de 2 styrelser, herunder omfanget af deres forpligtelser og Finansministeriets tilsyn.

Finansministeriet har oplyst, at ministeriet vil tage initiativ til at præcisere omfanget af sit tilsyn med Statens It, herunder i forhold til de 8 lag i it-infrastrukturen og i forhold til driftsmodellerne i Statens It.

## 2.4. MYNDIGHEDERNES KRAV OM OG OPFØLGNING PÅ LOGNING

52. Som nævnt er det vigtigt, at myndighederne foretager risikovurderinger og på baggrund heraf stiller relevante krav til og følger op på it-sikkerheden i de outsourcede it-systemer. På baggrund af myndighedernes risikovurderinger kan myndighederne vurdere, om der er behov for at stille krav til og følge op på logning i alle lag i it-infrastrukturen.

Revisionen viser som nævnt i afsnit 2.1, at Rigspolitiet har valgt at implementere alle kontroller fra ISO 27001, herunder logning. Ingen af de øvrige myndigheder har i deres risikovurderinger begrundet fravalg i forhold til logning og har ikke dokumenteret, at det ikke er nødvendigt at stille krav til og følge op på logning i alle dele af it-infrastrukturen.

Vi har derfor som en "temperaturmåling" undersøgt, om myndighederne har stillet krav til og fulgt op på leverandørernes logning i systemernes it-infrastruktur.

Kriterierne om logning er baseret på *Cyberforsvar der virker* fra 2013. Center for Cybersikkerhed har opstillet en række anbefalinger i *Logning – en del af et godt cyberforsvar* (herefter logningsvejledningen) fra april 2016. Vi har gengivet nogle af disse anbefalinger nedenfor til fremtidig inspiration (jf. boks 3, 5, 6 og 7), men kriterier og vurderinger er ikke baseret herpå, da vejledningen udkom, mens vi gennemførte revisionen.

### Myndighedernes krav om og opfølgning på, at leverandøren foretager logning

53. Ifølge *Cyberforsvar der virker* fra 2013 øger god logning sandsynligheden for at opdage og opklare angreb. Mange myndigheder gemmer dog ikke de rigtige logs eller undlader vigtige detaljer.

Myndighederne bør på baggrund af risikovurderingerne fastlægge, hvad der er relevant at logge og i hvilke dele af it-infrastrukturen. Loggen kan indeholde forskellige informationer til brug for opklaring (fx tid, handlinger og brugere).

**BOKS 3**

**ANBEFALING FRA CENTER FOR CYBERSIKKERHED OM RISIKOBASERET LOGNING**

Det fremgår af logningsvejledningen fra 2016, at Center for Cybersikkerhed fortsat ofte ser, at vigtige logs til at analysere hackerangreb ikke er til rådighed, når myndigheder bliver ramt af angreb. Ifølge logningsvejledningen kan det bl.a. skyldes, at myndighederne ikke har stillet krav til de eksterne it-leverandører om myndighedernes behov for logning. Ifølge Center for Cybersikkerhed vil mange leverandører som udgangspunkt kun foretage logning, hvis der er indgået specifikke aftaler herom.

Center for Cybersikkerhed anbefaler derfor, at myndighederne på baggrund af en risikovurdering afgør, hvilke typer af logs der bidrager mest i forebyggelsen af trusler eller bedst reducerer konsekvenserne. Herved kan myndigheden identificere, hvilken logning der skal foretages, herunder i hvilke dele af it-infrastrukturen.

54. Rigsrevisionen har derfor undersøgt, om myndighederne har stillet krav om, at leverandørerne foretager logning.

55. Revisionen viser, at Rigspolitiet, SKAT (for Nyt TastSelv Erhverv) og Digitaliseringsstyrelsen har stillet krav herom for alle dele af it-infrastrukturen.

Omvendt har SKAT (for TastSelv Borger), STAR og Søfartsstyrelsen enten kun stillet krav, der omfatter dele af it-infrastrukturen, eller stillet generelle, upræcise krav, der ikke klart definerer, hvilke lag i it-infrastrukturen kravene omfatter.

Revisionen har vist et eksempel på konsekvensen af at stille generelle krav og ikke klart definere, at leverandøren fx skal foretage logning i alle dele af it-infrastrukturen, jf. boks 4.

**BOKS 4**

### EKSEMPEL PÅ KONSEKVENSEN AF GENERELLE, UPRÆCISE KRAV OM LOGNING

En af de undersøgte myndigheder forventede, at deres generelle krav om logning omfattede privilegerede brugeres handlinger i databasen. Vores revision viste imidlertid, at leverandøren ikke tolkede kravet på samme måde som myndigheden og derfor ikke foretog den forventede logning.

56. Rigsrevisionen har desuden undersøgt, om myndighederne har fulgt op på, at leverandørerne har foretaget logning.

57. Revisionen viser, at det kun er Rigspolitiet, der har fulgt op på, om leverandøren foretager logning i alle dele af it-infrastrukturen.

SKAT (for Nyt TastSelv Erhverv), STAR og Digitaliseringsstyrelsen har fulgt op herpå i dele af it-infrastrukturen, mens SKAT (for TastSelv Borger) og Søfartsstyrelsen ikke har fulgt op.

## Myndighedernes krav om og opfølgning på, at leverandørerne regelmæssigt gennemgår loggen

58. Ifølge *Cyberforsvar der virker* fra 2013 prioriterer myndigheder – selv med gode logs – ofte ikke at undersøge deres logs for angreb.

**BOKS 5**

### ANBEFALING FRA CENTER FOR CYBERSIKKERHED OM GENNEMGANG AF LOGS

Det fremgår af logningsvejledningen fra 2016, at det fortsat er Center for Cybersikkerheds opfattelse, at logs primært anvendes reaktivt.

Ifølge logningsvejledningen kan visse typer af logs med fordel anvendes præventivt, fx i forbindelse med en regelmæssig gennemgang af loggen. Afhængigt af hvad de enkelte logs skal anvendes til, skal myndighederne på forhånd beslutte, om loggen skal gennemgås regelmæssigt eller blot gennemgås, når der er indtruffet en sikkerhedshændelse.

59. Rigsrevisionen har derfor undersøgt, om myndighederne har stillet krav om, at leverandørerne regelmæssigt gennemgår loggen.

Revisionen viser, at Rigspolitiet, SKAT (for Nyt TastSelv Erhverv) og Digitaliseringsstyrelsen har stillet krav herom for alle dele af it-infrastrukturen.

Omvendt har SKAT (for TastSelv Borger), STAR og Søfartsstyrelsen ikke stillet krav herom.

STAR har oplyst, at de mener, at de har stillet krav om regelmæssig gennemgang af loggen for lag 1-3 i it-infrastrukturen, og har fremsendt dokumentation herom.

Det er Rigsrevisionens vurdering, at dokumentationen ikke viser, at de krav, STAR henviser til, omfatter regelmæssig gennemgang af loggen.

60. Rigsrevisionen har desuden undersøgt, om myndighederne har fulgt op på, at leverandørerne regelmæssigt gennemgår loggen.

61. Revisionen viser, at Rigspolitiet og SKAT (for Nyt TastSelv Erhverv) har fulgt op herpå i alle dele af it-infrastrukturen.

Digitaliseringsstyrelsen har fulgt op i dele af it-infrastrukturen, mens SKAT (for TastSelv Borger), STAR og Søfartsstyrelsen ikke har fulgt op.

### Myndighedernes krav om og opfølgning på, at leverandørerne beskytter loggen, så den hverken kan ændres eller slettes

62. Ifølge *Cyberforsvar der virker* er logs et vigtigt redskab til at opdage og opklare eventuelle sikkerhedshændelser.

Hvis fx en hacker har kompromitteret it-systemer eller data, vil vedkommende typisk forsøge at sløre sine spor i loggen. Derfor er det vigtigt at beskytte loggen, så den hverken kan ændres eller slettes.

**BOKS 6**

**ANBEFALING FRA CENTER FOR CYBERSIKKERHED OM BESKYTTELSE AF LOGGEN**

Det fremgår af logningsvejledningen fra 2016, at myndighederne bør sikre, at det ikke er muligt at foretage uautoriserede ændringer eller slette i loggen. Det kan fx gøres ved at opbevare logs centralt og begrænse adgangen til logs.

63. Rigsrevisionen har derfor undersøgt, om myndighederne har stillet krav om, at leverandørerne beskytter loggen, så den hverken kan ændres eller slettes.

64. Revisionen viser, at Rigspolitiet, SKAT (for Nyt TastSelv Erhverv) og Digitaliseringsstyrelsen har stillet krav herom for alle dele af it-infrastrukturen.

Omvendt har SKAT (for TastSelv Borger), Søfartsstyrelsen og STAR ikke stillet krav om at beskytte loggen.

STAR har oplyst, at de mener, at de har stillet krav om beskyttelse af loggen, dog ikke for alle lag i it-infrastrukturen, og har fremsendt dokumentation herfor.

Det er Rigsrevisionens vurdering, at dokumentationen ikke viser, at de krav, STAR henviser til, omfatter beskyttelse af loggen.

65. Rigsrevisionen har endvidere undersøgt, om myndighederne har fulgt op på, at leverandørerne beskytter loggen, så den hverken kan ændres eller slettes.

66. Revisionen viser, at det kun er Rigspolitiet, der har fulgt op på, om leverandøren beskytter loggen mod ændring og sletning i alle dele af it-infrastrukturen.

SKAT (for Nyt TastSelv Erhverv), STAR og Digitaliseringsstyrelsen har kun fulgt op herpå i dele af it-infrastrukturen, mens SKAT (for TastSelv Borger) og Søfartsstyrelsen ikke har fulgt op.

SKAT har i forhold til Nyt TastSelv Erhverv oplyst, at SKAT har sikret, at loggen opbevares på en måde, så den ikke kan ændres og slettes. SKAT mener derfor, at det ikke er relevant at følge op på, om leverandøren beskytter loggen.

Rigsrevisionens vurdering er baseret på, at SKAT via revisorerklæringen følger op på, at de logs fra Nyt TastSelv Erhverv, som opbevares i leverandørens centrale logserver, er beskyttet, så de ikke kan ændres eller slettes. SKAT følger ikke op på de logs, som opbevares decentralt, fx logs på den fysiske server. Det er Rigsrevisionens opfattelse, at de logs, der opbevares decentralt, ikke er omfattet af den sikring af loggen, som SKAT henviser til, og at det er vigtigt at følge op på, om leverandøren fortsat beskytter loggen mod ændring og sletning, da det, der anses for at være sikre løsninger, ikke nødvendigvis vedbliver at være sikre løsninger.

### Myndighedernes krav om og opfølgning på, hvor længe leverandøren skal gemme loggen med henblik på opklaring af sikkerhedshændelser

67. Ifølge *Cyberforsvar der virker* gemmer mange myndigheder ikke de rigtige logs.

**BOKS 7**

#### ANBEFALING FRA CENTER FOR CYBERSIKKERHED OM, HVOR LÆNGE LOGS BØR GEMMES

En årsag til, at der ofte mangler logs til at analysere og opklare angreb, er ifølge logningsvejledningen fra 2016, at logs ikke gemmes i tilstrækkelig lang tid.

Det er derfor ifølge Center for Cybersikkerhed væsentligt, at myndighederne i risikovurderingen tager stilling til, hvor lang tid de enkelte logs skal gemmes. Center for Cybersikkerhed påpeger, at der kan gå lang tid, fra et angreb er sket, til det bliver opdaget. På opdagelsestidspunktet er det vigtigt, at de relevante logs ikke er blevet slettet.

Ifølge Center for Cybersikkerhed bør myndighederne gemme de enkelte logs så lang tid, det giver mening under hensyntagen til de gældende regler. Center for Cybersikkerhed henviser desuden til, at National Institute of Standards and Technology (NIST) foreslår forskellige opbevaringsperioder afhængig af de enkelte logs betydning.

**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**

National Institute of Standards and Technology (NIST) er en amerikansk offentlig institution, som bl.a. udvikler standarder inden for it-sikkerhed.

68. Rigsrevisionen har derfor undersøgt, om myndighederne har stillet krav om, hvor længe leverandørerne skal gemme loggen med henblik på opklaring af sikkerhedshændelser.

69. Revisionen viser, at Rigspolitiet, SKAT (for Nyt TastSelv Erhverv) og Digitaliseringsstyrelsen har stillet krav om, hvor længe leverandøren skal gemme loggen, for alle dele af it-infrastrukturen.

STAR har kun stillet krav herom for dele af it-infrastrukturen, mens SKAT (for TastSelv Borger) og Søfartsstyrelsen ikke har stillet krav herom.

70. Rigsrevisionen har videre undersøgt, om myndighederne har fulgt op på, hvor længe leverandørerne gemmer loggen med henblik på opklaring af sikkerhedshændelser.

71. Revisionen viser, at det kun er Rigspolitiet, der har fulgt op på, hvor længe leverandøren gemmer loggen, i alle dele af it-infrastrukturen.

SKAT (for Nyt TastSelv Erhverv), STAR og Digitaliseringsstyrelsen har fulgt op herpå i dele af it-infrastrukturen, mens SKAT (for TastSelv Borger) og Søfartsstyrelsen ikke har fulgt op herpå.

***Uklarhed om tilsynsforpligtelsen, herunder pligten til at stille krav om og følge op på logning***

72. Revisionen viser som nævnt i afsnit 2.3, at der er uklarhed om ansvars- og opgavefordelingen i forhold til tilsynet med Statens It mellem Finansministeriet samt henholdsvis Søfartsstyrelsen og STAR, som er kunder hos Statens It.

73. STAR og Erhvervs- og Vækstministeriet, herunder Søfartsstyrelsen, har som nævnt oplyst, de 2 styrelser ikke har været opmærksomme på deres forpligtelser i forhold til krav og opfølgning i forhold til Statens It. Det skyldes, at de har en anden opfattelse af ansvars- og opgavefordelingen i forhold til tilsynet med Statens It mellem Finansministeriet og de 2 styrelser, herunder omfanget af deres forpligtelser og Finansministeriets tilsyn.

## RESULTATER

Kun Rigspolitiet har stillet alle de undersøgte krav til logning i alle dele af it-infrastrukturen og fulgt op herpå i alle dele af it-infrastrukturen. De andre myndigheder har i større eller mindre grad forbedringsmuligheder i forhold til krav til og/eller opfølgning på logning.

Forbedringsmulighederne i forhold til krav til logning omfatter, at myndighederne enten ikke har stillet krav, har stillet generelle, upræcise krav, hvor det ikke tydeligt fremgår, hvilke lag af it-frastrukturen kravene gælder, eller har stillet krav, der kun omfatter nogle af lagene i it-infrastrukturen.

Forbedringsmulighederne i forhold til opfølgning omfatter, at myndighederne enten ikke har fulgt op eller kun har fulgt op i dele af it-infrastrukturen.

Rigsrevisionen vurderer, at manglende krav til logning overlader det til leverandørerne at beslutte, hvad der skal logges, hvor længe loggen skal gemmes, om den skal beskyttes, og om loggen skal gennemgås regelmæssigt. Generelle og upræcise krav om logning giver rum for fortolkning af, hvad leverandørerne er forpligtede til. Det indebærer en risiko for, at leverandørernes logning ikke er, som myndighederne forventer.

Når myndighederne ikke følger op, ved de ikke, om logningen er i orden, og om leverandøren efterlever kravene, herunder om leverandøren har en anden fortolkning af kravene. Når myndighederne alene følger op ved hjælp af en generel revisorerklæring, omfatter myndighedernes opfølgning ikke system- og kundespecifikke forhold hos leverandøren.

Revisionen viser, at der er uklarhed om ansvars- og opgavefordelingen i forhold til tilsynet med Statens It mellem Finansministeriet samt henholdsvis STAR og Søfartsstyrelsen, som er kunder hos Statens It. STAR og Erhvervs- og Vækstministeriet, herunder Søfartsstyrelsen, har oplyst, at de 2 styrelser ikke har været opmærksomme på deres forpligtelser i forhold til krav og opfølgning i forhold til Statens It. Det skyldes, at de har en anden opfattelse af ansvars- og opgavefordelingen i forhold til tilsynet med Statens It mellem Finansministeriet og de 2 styrelser, herunder omfanget af deres forpligtelser og Finansministeriets tilsyn.

Finansministeriet har oplyst, at ministeriet vil tage initiativ til at præcisere omfanget af sit tilsyn med Statens It, herunder i forhold til de 8 lag i it-infrastrukturen og i forhold til driftsmodellerne i Statens It.

Rigsrevisionen, den 2. november 2016

Lone Strøm

/Mads Nyholm Jacobsen

# BILAG 1. METODISK TILGANG

## Revisionens forløb og aktiviteter

Beretningen bygger på it-revisioner, som Rigsrevisionen har udført i 1. halvår 2016. It-revisionen har omfattet 6 it-systemer fordelt på 5 myndigheder. Revisionen har bestået af revisionsbesøg hos hver myndighed – enten hos myndigheden med deltagelse af leverandøren og/eller hos leverandøren. Endvidere har vi afholdt opfølgende møder med myndigheder/leverandører.

For at sikre sammenlignelighed på tværs af myndighederne har vi taget udgangspunkt i den samme spørgeramme, dog tilpasset de konkrete systemer.

Vores dokumentation bygger bl.a. på relevant skriftligt materiale fra myndighederne, fx risikovurderinger, kontrakter, materiale, som understøtter kontrakterne, og revisorerklæringer. Vi har også gennemgået kopier af skærmbilleder og dataudtræk fra systemerne for at se eksempler på fx adgangsstyring og logning, men vi har ikke foretaget en revision af it-sikkerheden hos leverandørerne. It-revisionen og beretningen handler om myndighedernes styring af it-sikkerhed hos leverandørerne og ikke om, hvordan it-sikkerheden er i praksis hos leverandørerne.

Herudover har vi været i dialog med Center for Cybersikkerhed og gjort brug af konsulentbistand fra Rambøll Management.

## Revisionskriterier

Vi har til brug for revisionen opstillet revisionskriterier. Beretningen omhandler 16 revisionskriterier, som er en del af en større it-revision. De udvalgte kriterier dækker 4 emner: risikovurdering, revisorerklæringer og kontrol af sikkerhed, adgangsstyring samt logning. Vi har udvalgt disse emner og kriterier, da vi anser dem for at være centrale for styringen af it-sikkerhed.

### *De valgte emner og kriterier*

Vi har valgt at undersøge myndighedernes risikovurdering, da risikovurderingen er fundamentet for at styre it-sikkerheden. Myndighederne bør på baggrund af risikovurderingerne beslutter, hvordan de kan håndtere de identificerede risici, og hvilke foranstaltninger de vil implementere.

Vi har undersøgt kriteriet om myndighedernes risikovurderinger ud fra følgende målepunkter:

- Myndigheden har ikke foretaget en risikovurdering af systemet.
- Myndigheden har foretaget en generel eller systemspecifik risikovurdering af systemet, som i nogen grad omfatter adgangsstyring og logning i systemets it-infrastruktur, og/eller som kun omfatter nogle lag/dele af it-infrastrukturen.
- Myndigheden har foretaget en risikovurdering af systemet, der omfatter adgangsstyring og logning for alle lag/dele af systemets it-infrastruktur.

Revisorerklæringer spiller en vigtig rolle i myndighedernes styring af it-sikkerheden, da de giver myndighederne information om, hvorvidt it-sikkerheden er i orden på de områder, erklæringerne omfatter. Myndighedernes kontrol/inspektion (fx via tredjepart) spiller også en vigtig rolle, da den kan give myndighederne information om forhold, der ikke er omfattet af revisorerklæringerne. Derfor har vi valgt at undersøge myndighedernes krav om revisorerklæringer og krav om mulighed for at foretage kontrol/inspektion hos leverandørerne.

Vi har undersøgt kriterierne om myndighedernes krav til revisorerklæringer og adgang til at foretage kontrol/inspektion ud fra følgende målepunkter:

- Myndigheden har ikke stillet krav om henholdsvis revisorerklæring og adgang til at foretage kontrol/inspektion.
- Myndigheden har stillet krav om henholdsvis revisorerklæring og adgang til at foretage kontrol/inspektion.

Adgangsstyring, herunder passwords, er et vigtigt aspekt af it-sikkerhed. Jo flere medarbejdere, der har adgang til systemet, desto større er risikoen for misbrug af rettigheder og adgang. Logning er et andet vigtigt aspekt af it-sikkerhed, vi har valgt at undersøge. God logning øger chancen for at opdage og opklare angreb, jf. *Cyberforsvar der virker*. Både adgangsstyring og logning indgår som kontroller i ISO 27001.

Vi har derfor – med afsæt i resultaterne om risikovurderinger og som en "temperaturmåling" på myndighedernes krav og opfølgning – undersøgt, om myndighederne har stillet krav til og fulgt op på leverandørernes adgangsstyring og logning.

Vi har undersøgt de enkelte kriterier om myndighedernes krav om adgangsstyring og logning ud fra følgende målepunkter:

- Myndigheden har ikke stillet krav.
- Myndigheden har stillet et generelt, upræcist krav, eller myndigheden har kun stillet krav for nogle lag/dele af it-infrastrukturen.
- Myndigheden har stillet krav for alle lag/dele af it-infrastrukturen, eller der foreligger risikovurderinger, der dokumenterer, at dette ikke er nødvendigt for alle lag/dele af it-infrastrukturen.

Vi har undersøgt de enkelte kriterier om myndighedernes opfølgning på adgangsstyring og logning ud fra følgende målepunkter:

- Myndigheden har ikke fulgt op.
- Myndigheden har kun fulgt op i nogle lag/dele af it-infrastrukturen.
- Myndigheden har fulgt op i alle lag/dele af it-infrastrukturen, eller der foreligger risikovurderinger, der dokumenterer, at dette ikke er nødvendigt for alle lag/dele af it-infrastrukturen.

Rigsrevisionen gør opmærksom på, at der er en række juridiske aspekter i forbindelse med logning, som myndighederne skal forholde sig til. De relevante bestemmelser kan variere på tværs af systemer og afhænger fx af, hvilken type data systemerne indeholder. Det er ikke omfattet af denne beretning.

De emner og kriterier, beretningen omhandler, omfatter blot en del af it-sikkerheden. De udgør derfor ikke en udtømmende liste over, hvordan myndighederne skal styre it-sikkerheden hos leverandørerne, herunder hvilke krav myndighederne bør stille. Opfyldelse af kriterierne er derfor ikke ensbetydende med en tilstrækkelig styring af it-sikkerheden.

Da risikobilledet ændrer sig løbende, ændrer det sig over tid, hvilke sikkerhedskrav der er relevante at stille, og hvilket sikkerhedsniveau det er tilstrækkeligt at kræve. Samtidig vil det afhænge af de enkelte myndigheders risikovurderinger for de enkelte systemer og skal ses i sammenhæng med de samlede sikkerhedsforanstaltninger i de enkelte systemer. Derfor er de valgte kriterier formuleret overordnet fremfor at angive specifikke niveauer.

### *Kriteriernes ophæng*

Finansministeriet stiller krav om, at statslige myndigheder følger it-sikkerhedsstandarden ISO 27001 til styring af it-sikkerheden, herunder også it-sikkerheden hos eksterne it-leverandører. Myndighederne er desuden forpligtet til at følge *National strategi for cyber- og informationssikkerhed* og forskellige lov- og myndighedskrav på sikkerhedsområdet. Derfor danner ISO 27001 og *National strategi for cyber- og informationssikkerhed* den overordnede ramme for kriterierne. Derudover har vi som fortolkningsbidrag benyttet relevante anbefalinger og vejledninger fra Digitaliseringsstyrelsen og Center for Cybersikkerhed som ramme for kriterierne.

Vi har anvendt *Guide til implementering af ISO 27001* (Digitaliseringsstyrelsen, 2015), *Vejledning i it-risikostyring og -vurdering* (Digitaliseringsstyrelsen, 2015), *Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift* (Digitaliseringsstyrelsen og Center for Cybersikkerhed, 2014) og *Cyberforsvar der virker* (Digitaliseringsstyrelsen og Center for Cybersikkerhed, 2013).

Som supplement har vi inddraget *Logning – en del af et godt cyberforsvar* (Center for Cybersikkerhed, april 2016) som et fremadrettet fortolkningsbidrag til inspiration, da vejledningen er udkommet, mens revisionen blev gennemført. Derfor er kriterier og vurderinger ikke baseret herpå.

Vi har ikke opstillet kriterier på baggrund af sikkerhedsmæssige lov- og myndighedskrav. Det skyldes, at det varierer, hvilke sikkerhedsmæssige lov- og myndighedskrav de enkelte myndigheder er underlagt, afhængigt af hvilke data mv. der indgår i deres systemer. Vi har valgt at anvende samme kriterier på tværs af de myndigheder, som indgår i beretningen, for at skabe et godt sammenligningsgrundlag.

Som det fremgår af tabel 1, er flere af kontrakterne indgået, før den nationale strategi, vejledninger mv. udkom. På baggrund af grundprincipperne i ISO 27001 finder Rigsrevisionen det vigtigt, at myndighederne løbende foretager risikovurderinger, og at myndighederne på baggrund heraf stiller nye relevante krav til sikkerhedstiltag, selv om kontrakterne er indgået på et tidligere tidspunkt. Dette kan ske i form af fx allonger, tillægsaftaler og/eller bilag.

Dertil kommer, at de krav og anbefalinger, der er udgået fra Digitaliseringsstyrelsen og Center for Cybersikkerhed gennem de senere år, efter Rigsrevisionen opfattelse er gældende for statslige myndigheder, uanset hvornår myndighederne har indgået kontrakter med deres it-leverandører.

Vi har derfor valgt at anvende krav og anbefalinger, der er udkommet før revisionens påbegyndelse, som kriterier for revisionen, selv om myndighederne har indgået kontrakterne med deres it-leverandører på forskellige tidspunkter, og selv om ikke alle krav og anbefalinger, som vi baserer kriterierne på, var udkommet på det tidspunkt, hvor de enkelte kontrakter blev indgået.

### *Risikovurderinger af it-infrastrukturen*

Der er som udgangspunkt potentielt risici og sårbarheder i hvert af de enkelte lag i it-infrastrukturen for et it-system.

ISO 27001 giver imidlertid ikke konkrete anvisninger til, hvad der skal være omfattet af risikovurderingen for at give et præcist billede af it-sikkerhedsrisici, og ISO 27001 forholder sig fx ikke til begrebet it-infrastrukturen.

Det er dog på baggrund af principperne i ISO 27001 og vejledninger mv. Rigsrevisionens opfattelse, at det er den enkelte myndigheds ansvar at sikre, at myndighedens risikovurdering dækker alle lagene i it-infrastrukturen for it-systemet, og at risikovurderingen tager udgangspunkt i myndighedens behov i forhold til at sikre tilgængelighed, fortrolighed og/eller integritet i it-systemet og data. De seneste års sikkerhedshændelser viser vigtigheden heraf. Navnlig i forhold til lag 5-8 i it-infrastrukturen vil myndighederne dog ofte være afhængige af input fra leverandørerne for at identificere risici i disse lag og vurdere, hvad de betyder for systemet.

Det er Rigsrevisionens opfattelse, at hvis myndighederne ikke har foretaget en risikovurdering af systemerne og sikret, at risikovurderingerne dækker de enkelte lag i it-infrastrukturen og ikke har taget stilling til risici heri, så ved myndigheden ikke, i hvilket omfang der er risici i de enkelte lag i it-infrastrukturen, og i hvilket omfang leverandørens sikkerhedsforanstaltninger tager hånd om disse risici. Myndighederne ved heller ikke, hvilke sikkerhedskrav det er relevant at stille til leverandøren, og hvilke der eventuelt kan undlades, hvis der ikke er behov. Det er derfor Rigsrevisionens opfattelse, at myndighederne bør foretage risikovurderinger, der tager højde for risici i alle lagene i it-infrastrukturen.

Det er Rigsrevisionens opfattelse, at det følger af principperne i ISO 27001, at myndighederne bør sikre, at deres risikovurderinger forholder sig til hele systemet og de enkelte lag i den underliggende it-infrastruktur, for at kunne begrunde valg og fravalg af foranstaltninger/kontroller og få vished om, at de ikke har undladt vigtige foranstaltninger/kontroller.

Det fremgår desuden af *Anbefalinger til styrkelse af it-sikkerheden i statens outsourcede drift*, at myndigheden bør vurdere risikobilledet ved outsourcing af it-drift sammenholdt med risikobilledet ved egen drift/insourcing. Risikobilledet sammenholdes med de forretningsmæssige mål og myndighedens risikovillighed på områder, hvor der ikke er risiko for personfølsomme eller nationale data. Myndighederne skal herunder ved udbud eller indkøb af it-leverancer vurdere it-sikkerhedsrisici ved den påtænkte it-leverance og it-sikkerhedsrisici ved integrationen af leverancen i myndighedens øvrige it-miljø og beslutte passende sikringstiltag. Det er afgørende for myndighedens it-sikkerhed, at den løbende identificerer de sårbarheder, der måtte være ved at vælge en outsourcet løsning, så it-sikkerhedsforanstaltningerne kan justeres eller nye indføres.

Ifølge *Vejledning i it-risikostyring og -vurdering* bør identifikation af risici tage udgangspunkt i de såkaldte aktiver, som er omfattet af organisationens it-sikkerhedsarbejde. Aktiverne bør identificeres på et passende niveau i forhold til organisationens størrelse og det ønskede detaljeringsniveau af risikovurderingen. I mange tilfælde kan aktiverne grupperes, så antallet begrænses, men der stadig er mulighed for at knytte specifikke trusler til dem. Fx kan routere, switche og firewalls grupperes som netværksudstyr eller infrastruktur.

Desuden fremgår det af *Guide til implementering af ISO 27001*, at støtteaktiver som fx hardware og software, fysiske lokationer og interaktion med informationerne skal identificeres og medtages i vurderingen af de trusler og sårbarheder, der vil kunne aktualiseres i risiko for tab af fortrolighed, integritet og tilgængelighed.

Ifølge guiden handler arbejdet med at identificere relevante trusler om at undersøge, hvad der kan true informationssikkerheden.

Endelig fremgår det af Dansk It's guide *Sikkerhed ved it-outsourcing* fra 2012, at det er vigtigt, at virksomhederne forstår det miljø, som outsources, til bunds.

# BILAG 2. FINANSMINISTERIETS TILSYN MED STATENS IT OG KUNDERNES FORPLIGTELSER

Dette bilag beskriver, hvordan Finansministeriet betragter sit tilsyn med Statens It og forpligtelserne for de myndigheder, der er kunder hos Statens It.

Desuden beskriver bilaget STAR's og Søfartsstyrelsens opfattelse af ansvars- og opgavefordelingen mellem kunderne og Finansministeriet, som varetager tilsynet med Statens It på kundernes vegne.

## Baggrund

STAR og Søfartsstyrelsen er kunder hos Statens It på 2 forskellige måder. Erhvervs- og Vækstministeriet, herunder Søfartsstyrelsen, er tilsluttet Statens It, som varetager driften af styrelsens it-systemer, herunder Skibsregistret. Styrelsen kan derfor ikke frit vælge driftsleverandør, men skal benytte Statens It.

Driften af STAR's system DFDG er outsourcet til KMD via Statens It's rammeaftale med eksterne leverandører. Finansministeriet har oplyst, at Statens It har ansvaret for driftsaftalen med KMD, men at STAR som systemejer har godkendt den kravspecifikation, der ligger til grund for kontrakten med KMD. STAR har desuden haft mulighed for løbende at stille supplerende it-sikkerhedsmæssige krav til KMD via Statens It.

## Finansministeriets tilsyn med Statens It og kundernes forpligtelser

Finansministeriets tilsyn med Statens It har bestået af Digitaliseringsstyrelsens tilsyn og Finansministeriets Koncernrevisions revision.

Finansministeriet har oplyst, at fokus i Digitaliseringsstyrelsens tilsynsaktiviteter har været på, om ledelsen i Statens It har etableret driftsmæssige og organisatoriske procedurer, der understøtter de fællesstatslige basisleverancer til kunderne, herunder til infrastrukturen, datacenter mv., så de overordnede krav til styring af it-sikkerhed efterleves. Revisionerne går derimod i dybden omkring de tekniske løsninger og sikkerhedsforanstaltninger og efterprøver, om forretningsgangene, jf. ISO-standarderne, efterleves.

Ifølge Finansministeriet omfatter hverken tilsynet eller Koncernrevisions revisioner som udgangspunkt kundernes fagspecifikke systemer. Dog bemærkes det, at Finansministeriets tilsyn med Statens It dækker generelle it-kontroller og efterlevelse af ISO-standarden, hvilket udgør et væsentligt grundlag for driften af kundernes fagspecifikke systemer, jf. standardkundeaftalen og tilhørende bilag.

Det er Erhvervs- og Vækstministeriets opfattelse, at det er valget af driftsmodel i Statens It, der afgør, om driften af it-infrastrukturen (basisgrundlag) er omfattet af Finansministeriets tilsyn.

Finansministeriet har oplyst, at ministeriet vil tage initiativ til at præcisere omfanget af sit tilsyn med Statens It, herunder i forhold til de 8 lag i it-infrastrukturen og i forhold til driftsmodellerne i Statens It.

### *Kundernes risikovurderinger*

Kundernes risikovurderinger af fagsystemer er helt centrale ved vurderingen af, om kunderne har sikret en tilstrækkelig og dækkende sikkerhed. Hvis der ikke er lavet en tilstrækkelig risikovurdering, kan der ikke stilles de rigtige krav til Statens It, og dermed er det også umuligt efterfølgende at foretage og dokumentere en tilstrækkelig opfølgning på varetagelsen af it-driften. Finansministeriet er enig med Rigsrevisionen i, at ansvaret for at foretage en risikovurdering af fagsystemer ligger hos kunden. Hvis kunden vurderer, at det enkelte fagsystem ikke har behov for særlige sikkerhedsforanstaltninger, og det derved kan omfattes af Statens It's standardkundeaftale, bør dette eksplicit skrives i risikovurderingen.

### *Kundernes krav til Statens It*

Finansministeriet har oplyst, at som følge af risikovurderingen kan kunderne stille krav til Statens It om udførelsen af it-driften for kundernes fagsystem. De basale krav til Statens It, herunder krav til generelle it-kontroller, efterlevelse af ISO-standarden mv., vil være omfattet af standardkundeaftalen med tilhørende bilag. Hvis kunderne har ønsker, som rækker ud over det basale, vil disse være aftalt særskilt, og Statens It kan fakturere på baggrund heraf. Ifølge Finansministeriet ligger ansvaret for at stille de tilstrækkelige krav til Statens It hos kunderne, da de er de eneste, der kan vurdere behovet for sikkerhed.

### *Kundernes opfølgning*

Finansministeriet udfører tilsynet med Statens It's generelle kontroller og basale sikkerhed, hvilket driften af fagsystemerne hviler på. Finansministeriet er forpligtet til at afrapportere tilsynet til kunderne og i den forbindelse henlede kundernes opmærksomhed på større problemstillinger og risici. I tilsynsrapporten redegøres for de udførte revisioner fra såvel intern revision som fra Rigsrevisionen, så kunderne får en præcisering af, hvilke områder der har haft tilsynets og revisionens fokus. Koncernrevisionen reviderer ud fra en turnus, hvor alle områder i ISO-standarden gennemgås inden for en 4-årig periode. Ved revisionerne testes det bl.a., om forretningsgangene overholder standarder og er hensigtsmæssigt implementeret. Herudover har Rigsrevisionen gennemført supplerende revision.

Kunden er forpligtet til at forholde sig til Finansministeriets tilsyn. Hvis tilsynet viser væsentlige udfordringer i Statens It's opgavevaretagelse, bør kunden ifølge Finansministeriet eksplicit tage stilling til, om dette giver anledning til initiativer. Kunderne har desuden mulighed for at afgive ønsker til tilsynet, hvis der er særlige områder, de mener, at tilsynet skal gennemgå/efterse.

Det er Rigsrevisionens opfattelse, at kundens forpligtelser afhænger af kundens risikovurdering. Finansministeriet er enig med Rigsrevisionen heri. Hvis kunden i sin risikovurdering vurderer, at der ikke er særlige sikkerhedskrav/risici, vil det være omfattet af de krav, der er stillet i kundeaftalen, og opfølgningen vil også være omfattet af Finansministeriets tilsyn med Statens It. Kunden er dog forpligtet til at forholde sig til Finansministeriets tilsyn, herunder om det giver anledning til at bede tilsynet om at tage særlige emner op.

Hvis kunden i risikovurderingen vurderer, at der er tale om særlige risici, som rækker ud over den sikkerhed, der er opstillet i kundeaftalen, har kunden ifølge Finansministeriet en forpligtelse til at synliggøre dette krav over for Statens It. Kunden har derudover en forpligtelse til at stille krav til, hvordan Statens It afrapporterer til kunden omkring de særlige foranstaltninger. Kunden har en forpligtelse til at følge op på, at de særlige aftaler og sikringsforanstaltninger udføres. Dette omfattes ikke af Finansministeriets tilsyn. De øvrige forhold omkring systemet, som ligger i basispakken for Statens It's leverancer, vil dog være omfattet af Finansministeriets tilsyn på kundernes vegne.

Finansmisteriet har oplyst, at tilsynet og koncernrevision kun har omfattet de kunder, der har Statens It som driftsleverandør.

## STAR's og Erhvervs- og Vækstministeriets, herunder Søfartsstyrelsens, opfattelse af ansvars- og opgavefordelingen mellem dem, Finansministeriet og Statens It

### *STAR's opfattelse af ansvars- og opgavefordelingen*

STAR har oplyst, at det er styrelsens opfattelse, at Finansministeriet har tilsynet med og ansvaret for de 5 nederste lag i it-infrastrukturen i DFDG (dvs. lag 4-8), og at STAR har ansvaret for kundens fagspecifikke programmer og systemer (de første 2-3 lag i it-infrastrukturen – dvs. lag 1, 2 og delvist lag 3).

STAR har desuden oplyst, at det i forlængelse heraf er STAR's opfattelse, at Finansministeriet skal udarbejde risikovurderinger for lag 4-8 og føre tilsyn hermed.

Det er Rigsrevisionens opfattelse, at STAR skal foretage risikovurdering, stille krav og følge op i alle 8 lag i it-frastrukturen.

### *Erhvervs- og Vækstministeriets, herunder Søfartsstyrelsens, opfattelse af ansvars- og opgavefordelingen*

Erhvervs- og Vækstministeriet har oplyst, at det er ministeriets opfattelse, at kundernes fagspecifikke programmer kan være omfattet af Digitaliseringsstyrelsens tilsyn og Finansministeriets Koncernrevision. Hvilke dele af it-infrastrukturen som Digitaliseringsstyrelsen og Finansministeriet afløfter tilsynsforpligtelsen for, afhænger af den valgte driftsmodel for det enkelte fagsystem. Det er Erhvervs- og Vækstministeriets opfattelse, at udgangspunktet for tilsynet er fællesleverancer, fx infrastruktur. Det betyder, at Finansministeriets tilsyn – alt efter valg af driftsmodel – fører tilsyn med infrastrukturen. I de tilfælde, hvor man som kunde vurderer, at Statens It's løsning ikke er tilstrækkelig, og derfor stiller skærpede krav til sikkerheden, skal kunden påse og kontrollere, at Statens It efter aftale honorerer disse krav. Det er Erhvervs- og Vækstministeriets opfattelse, at dele af lag 3 og lag 4-8 i it-infrastrukturen i Skibsregistret er omfattet af Digitaliseringsstyrelsens tilsyn og Finansministeriets Koncernrevision.

Det er Erhvervs- og Vækstministeriets opfattelse, at Søfartsstyrelsen har en forpligtigelse til at stille supplerende krav til Statens It, hvis de vurderer, at Finansministeriets tilsyn ikke er tilstrækkeligt.

Det er desuden Erhvervs- og Vækstministeriets opfattelse, at de som kunde i Statens It er forpligtet til at holde sig opdateret i forhold til Finansministeriets tilsyn med Statens It, men at særlige krav til emner kun er nødvendige, hvis kunden vurderer, at det pågældende fagsystem har specifikke behov. Erhvervs- og Vækstministeriet er i løbende dialog med Statens It om sikkerheden i de systemer, som Statens It er driftsleverandør på.

Efter Rigsrevisionens opfattelse har Søfartsstyrelsen ikke dokumenteret, at de har gjort dette og har ikke på baggrund af en risikovurdering dokumenteret, at der ikke har været behov herfor.

Erhvervs- og Vækstministeriet har oplyst, at lag 1, 2 og dele af lag 3 i it-infrastrukturen for Skibsregistret ikke vedligeholdes af Statens It, men af et konsulentfirma, og at disse lag er omfattet af en separat leverandøraftale og leverandøropfølgning. Desuden er det Erhvervs- og Vækstministeriets opfattelse, at krav til og opfølgning i dele af lag 3 og lag 4-8 i Skibsregistret er omfattet af Digitaliseringsstyrelsens tilsyn og Finansministeriets Koncernrevision, hvorfor Søfartsstyrelsens forpligtelse hertil afløftes.

Erhvervs- og Vækstministeriet har oplyst, at Søfartsstyrelsen derfor ikke stiller krav om eller følger op på adgangsstyring særskilt for Skibsregistret. Søfartsstyrelsen stiller for så vidt angår lag 1, 2 og dele af lag 3 krav til sin anden leverandør, og Søfartsstyrelsen følger jævnligt op herpå.

Erhvervs- og Vækstministeriet har i forhold til kriteriet om at stille krav om, at leverandøren foretager logning, oplyst, at Søfartsstyrelsen kun har stillet generelle krav til logning i Statens It, da der her er tale om de krav, som er omfattet af aftalekomplekset mellem Søfartsstyrelsen og Statens It. På tidspunktet for udarbejdelsen af risikovurderingen og på revisionstidspunktet blev Skibsregistret driftet på en forældet platform, hvor det ikke var muligt at logge på enkelte niveauer i teknologistakken. Skibsregistret er efterfølgende ved at blive overført til en nutidig platform, hvor det fremadrettet er muligt at logge.

I forhold til de øvrige kriterier om krav til og opfølgning på logning har Erhvervs- og Vækstministeriet oplyst, at det er ministeriets opfattelse, at tilsynsforpligtelsen med krav til og opfølgning på logning ligger hos Digitaliseringsstyrelsen og Finansministeriets Koncernrevision for så vidt angår Skibsregistrets lag 4-8 og dele af lag 3. Skibsregistrets lag 1, 2 og dele af lag 3 er omfattet af en separat leverandørkontrakt.

Statens It varetager it-driften af Skibsregistret, herunder afvikling af software og fysisk udstyr i systemets it-infrastruktur i lag 1-8. Beretningen handler alene om Søfartsstyrelsens it-driftsleverandør – Statens It. Søfartsstyrelsen har en vedligeholdelses- og udviklingsaftale med en softwareleverandør. Softwareleverandøren varetager såkaldt applikation management (dvs. bl.a. fejlsøgning, fejlrettelse og videreudvikling i lag 1-2 og dele af lag 3 i Skibsregistrets it-infrastruktur).

Derfor finder vi, at det er relevant for Søfartsstyrelsen at foretage risikovurdering, der omfatter alle 8 lag i Skibsregistrets it-infrastruktur hos Statens It, stille krav til adgangsstyring og logning i alle 8 lag i Skibsregistrets it-infrastruktur hos Statens It, ligesom Søfartsstyrelsen i sin opfølgning skal forholde sig aktivt til Finansministeriets tilsyn med Skibsregistrets it-infrastruktur hos Statens It, herunder om det dækker de 8 lag, og om der er behov for yderligere.

Det er Rigsrevisionens opfattelse, at Finansministeriets tilsyn ikke afløfter Søfartsstyrelsens forpligtelse til at stille supplerende krav. Desuden er det Rigsrevisionens opfattelse, at hvis dette ikke var teknisk muligt, burde det fremgå af risikovurderingen.

Det er Rigsrevisionens opfattelse, at kunderne er forpligtet til aktivt at forholde sig til det tilsyn, Finansministeriet fører med Statens It på vegne af kunderne, fx ved at spørge ind til tilsynet eller stille krav til emner, der skal være særligt fokus på. Dette bør ske med udgangspunkt i myndighedens risikovurdering, så tilsynet afspejler myndighedernes specifikke behov for it-sikkerhed.

Vi har desuden gennemgået Finansministeriets tilsynsrapport for Statens It for 2013, 2014 og 2015 og vurderer, at tilsynet eller de omtalte revisioner ikke har omhandlet forhold i Skibsregistrets it-infrastruktur med betydning for adgangsstyring og logning. Finansministeriet har oplyst, at Finansministeriets Koncernrevision i henhold til sin turnusplan har gennemgået adgangsstyring og logning. Rigsrevisionen konstaterer, at disse revisioner ikke har omfattet Skibsregistret.

# BILAG 3. ORDLISTE

| | |
|---|---|
| **Aftalegrundlag/ kontraktgrundlag** | Er i denne sammenhæng anvendt i betydningen skriftligt, formelt materiale, der beskriver leverandørens forpligtelser. Det omfatter kontrakten med bilag og eventuelle ændringstillæg, tillægsaftaler mv. |
| **Applikation** | Den del af det samlede system, der "ved", hvordan informationerne i brugergrænsefladen skal behandles. |
| **Brugergrænseflade** | En webbrowser eller et dedikeret program, hvor brugerne indtaster og læser informationer til og fra systemet. |
| **Database** | Centralt opbevaringssted for systemets data. |
| **Fortrolighed** | Information og data kan kun tilgås af autoriserede personer, som har et arbejdsbetinget behov. |
| **Fysisk lokation** | Fysiske lokaler med faciliteter som fx strøm, køling og alarmer. |
| **Fysisk server** | Den enhed/komponent, der understøtter behandlingen af data mv. og fungerer som grænseflade mellem de fysiske dele og de logiske dele. I denne beretning er det den logiske adgang til den fysiske server via fx iLO™ og DRAC™. |
| **Hacker** | Betegner i denne beretning en ukendt og uautoriseret person, der foretager en ulovlig handling ved i det skjulte at skaffe sig adgang til og/eller anvende andres it-systemer eller data. Formålet med hacking og de anvendte metoder afhænger af de personer eller organisationer, der står bag, dvs. om det er fremmede stater, kriminelle organisationer eller individer, som på egen hånd misbruger institutionernes svagheder. |
| **Hypervisor** | Software, der gør det muligt at opdele den fysiske maskine i én eller flere virtuelle maskiner og derved afvikle flere operativsystemer på samme maskine. |
| **Integritet** | Informationer og data er korrekte og pålidelige. |
| **ISO27001** | En international informationssikkerhedsstandard, som afløser den tidligere sikkerhedsstandard DS 484. De statslige myndigheder har skullet følge ISO 27001 fra januar 2014 og have færdigimplementeret den primo 2016. |
| **It-infrastruktur** | It-systemer består af forskellige tekniske lag/dele (it-infrastrukturen), som tilsammen er en forudsætning for, at systemerne kan fungere korrekt. It-infrastrukturen kan opdeles i 8 lag: brugergrænseflade, applikation, database, operativsystem, eventuelt hypervisor, fysisk server, netværk og fysisk lokation. |
| **Log** | Fil, hvor institutionerne gemmer registreringer af oplysninger om anvendelse af og hændelser i institutionernes it-systemer og data. |
| **Logning** | Registrering af oplysninger om anvendelse af og hændelser i institutionernes it-systemer og data. |
| **Middleware** | En generel betegnelse for de lag i it-infrastrukturen, typisk databasen, som binder applikationen sammen med de underliggende lag. |
| **Misbrug og kompromittering af it-systemer og data** | Indebærer, at en person uretmæssigt kan få adgang til en række af institutionernes it-systemer og data.<br>Der kan fx være tale om, at personen uretmæssigt afbryder eller ændrer datakørsler. Der kan også være tale om, at personen uretmæssigt ændrer, sletter eller læser/stjæler data. |
| **Netværk** | Fysiske komponenter, der gør det muligt for et it-system at kommunikere med omverdenen/andre systemer. |
| **Operativsystem** | Den grundlæggende komponent, der styrer den fysiske eller virtuelle maskine og giver mulighed for at afvikle fx applikationer og databaser. En virtuel maskine er en delmængde af den fysiske maskine, der styres af hypervisoren. |

| | |
|---|---|
| **Outsourcet** | I denne beretning definerer vi outsourcet bredt som it-løsninger/-systemer, der drives af eller i samarbejde med eksterne it-leverandører, dvs. at eksterne it-leverandører varetager driften af it-systemer for myndighederne, eller at myndighedernes opgavevaretagelse er baseret på sådanne it-systemer, der leveres af eksterne leverandører som en tjeneste. Myndighederne er derfor ansvarlige for it-sikkerhed i forhold til de systemer eller tjenester, som de benytter i deres opgavevaretagelse. |
| **Privilegerede brugere** | Brugere, der har et højere niveau af rettigheder, adgang og kontrol over institutionens it-systemer og data end almindelige brugere. |
| **Revisorerklæring** (generel og systemspecifik) | En generel revisorerklæring er ikke kunde- og systemspecifik. Den omhandler leverandørens generelle it-kontroller og dækker leverandørens fælles it-miljø, der normalt kun dækker lag 5-8 i it-infrastrukturen.<br>En systemspecifik revisorerklæring omhandler kundens konkrete systemer og forholder sig til it-kontroller i og omkring det pågældende it-system. |
| **Revisorprotokollat** | Er en revisors rapportering om den udførte it-revision til en virksomheds bestyrelse, som i denne beretning er om it-leverandørens it-sikkerhed. |
| **Segmentering af netværk** | Myndigheden har opdelt netværket i afgrænsede områder. Det medvirker fx til at sikre, at hackerangreb ikke kan sprede sig til alle it-systemer og data, men kun rammer en begrænset del af netværket. |
| **Server (fysisk server)** | Den komponent, der udfører databehandling for fx operativsystem, database og applikation. |
| **Sikkerhedsforanstaltninger** | Sikkerhedsforanstaltninger skal bidrage til at forhindre eller opdage misbrug og kompromittering af it-systemer og data. Det er fx tekniske regler i systemerne, der kan forhindre uønskede handlinger. |
| **Sikkerhedshændelse/sikkerhedsbrud** | Sikkerhedshændelser er uventede hændelser i it-miljøet, der indikerer, at der er eller kan være noget galt.<br>Sikkerhedsbrud betyder, at en intern eller ekstern person forsætligt eller uforsætligt har foretaget en handling, der truer it-sikkerheden. |
| **SoA-dokument** (Statement of Applicability) | Er et centralt dokument i sikkerhedsarbejdet efter ISO 27001. SoA-dokumentet skal omhandle ledelsens prioritering af sikkerheden, herunder beslutninger om valg og fravalg af sikkerhedsforanstaltninger i forhold til forretningens mål og risikoprofil. |
| **Tilgængelighed** | Systemet fungerer som forventet, og brugerne kan løse deres opgaver her og nu. |
| **To-faktorvalidering** | Identifikation af en person ud fra brugernavnet og 2 elementer, som kun brugeren kan præsentere: Noget brugeren ved (password), noget, brugeren har (fx nøglekort), eller noget, brugeren er (biometri, fingeraftryk, iris, nethinde osv.). |