FOLKETINGET
RIGSREVISIONEN

Evalueringer af Rigsrevisionens beretninger fra 2022 af Professor Jan Pries-Heje

Januar 2023

Evaluator Jan Pries-Heje

Evaluering af beretning 9/2021
5 statslige myndigheders efterlevelse af 20 tekniske minimumskrav til it-sikkerheden

1. Er beretningens emne og formål klart motiveret og afgrænset?

Beretningen ser på hvorvidt 5 samfundsvigtige statslige myndigheder efterlever 20 tekniske minimumskrav til it-sikkerhed.

Der er tale om en evaluering som Rigsrevisionen selv har taget initiativ til i juni 2021, og gennemført i perioden marts-september 2021

Motivationen for at foretage evalueringen fremgår på side 1: ”Cybertruslen mod statslige myndigheder vokser i takt med den øgede digitalisering af samfundet … Cyberangreb er ikke ualmindelige, og flere statslige myndigheder er gennem tiden blevet udsat for dem”.

På den baggrund har Center for Cybersikkerhed, der hører under Forsvarsministeriet, defineret 20 tekniske minimumskrav til it-sikkerhed, som skal ”beskytte statslige arbejdspladser mod ondsindede cyber- og informationssikkerhedshændelser” (side 1).

Formålet med undersøgelsen er at vurdere, om fem udvalgte statslige myndigheder - Statens It, Kriminalforsorgen, Sundhedsdatastyrelsen, Energistyrelsen og Fødevarestyrelsen - efterlever de 20 tekniske minimumskrav.

De 20 krav blev vedtaget i efteråret 2019 og meldt ud per 1. januar (17 af kravene) og 1. juni 2020 (3 yderligere krav). I tabel 1 side 7-8 i beretningen findes en god forklarende oversigt over kravene.

Første del af undersøgelsen handler om, hvorvidt de enkelte myndigheder efterlever de tekniske minimumskrav, som de selv er forpligtet til at efterleve (jf. figur 2, side 11).

Anden del af undersøgelsen handler om, hvorvidt Statens IT og deres kunder - Energistyrelsen og Fødevarestyrelsen - efterlever de tekniske minimumskrav i henhold til den aftalte ansvarsdeling (figur 2).

Alt i alt er beretningens emne og formål klart motiveret og afgrænset.

2. Er det tydeligt, hvorfor de valgte revisionskriterier er egnede til at belyse formålet?

De 20 minimumskrav er valgt som revisionskriterier. Det er ikke specielt tydeligt hvorfor disse minimumskriterier er særligt egnede? Det kritiske revisorblik synes ikke at være faldet på Center for Cybersikkerhed, som har defineret de 20 minimumskriterier. Kravene tages umiddelbart for gode varer, uden nogen diskussion eller refleksion; det savnes.

Før de 20 minimumskrav er egnede til revision skal flere af dem præciseres, fordi de indeholder det man kunne kalde "elastikord", dvs. ord eller vendinger der efterlader meget rum til fortolkning. Dette gøres på glimrende vis, og der demonstreres ganske megen teknisk indsigt i denne diskussion. Det er godt.

Man kunne have valgt, eller i det mindste diskuteret, om man skulle have revideret andre eller yderligere kriterier, f.eks. set på den relative forbedring det seneste år, talt hvor mange angreb der er registreret seneste måned, perspektiveret hjemmeside-sikkerheden med antal besøg. Men ingen mulige yderligere kriterier diskuteres.

Så et mere kritisk og reflekteret valg af revisionskriterier savnes.

3. Er det tydeligt forklaret, hvorfor den valgte metode er velegnet til at belyse formålet (metodeovervejelser/beskrivelser i kap 1 og metodisk tilgang i bilaget)?

Undersøgelsen bygger på 5 it-revisioner. I forbindelse med disse fem it-revisioner, gennemført i perioden marts-september 2021, fandt Rigsrevisionen ud af, at det var nødvendigt at præcisere 4 af kravene. De fire krav der fortolkes forskelligt er dels krav 6 om begrænset tildeling af lokaladministratorrettigheder, desuden krav 13 om regelmæssig opdatering af mobile enheder, dertil krav 15 om logning, samt krav 18 om kryptering af kommunikation til hjemmesider.

De fem it-revisioner førte til konstateringen af, at Sundhedsdatastyrelsen efterlevede 12 krav, Energistyrelsen efterlevede 15 krav, Kriminalforsorgen efterlevede 16 krav, Fødevarestyrelsen efterlevede 17 krav, og Statens IT 18 af kravene. Denne information fremgår af figur 4, side 19

Det er ikke alle krav der direkte skal opfyldes af 5 undersøgte myndigheder. Af figur 2 side 11 fremgår det, at de myndigheder der har Statens IT som leverandør kun selv skal opfylde 7 henholdsvis 8 krav.

Metodisk diskuteres valget af de fem styrelser ud fra en argumentation om, at de er kritiske for samfundet, og derfor vigtige. Det diskuteres ikke om der er andre styrelser der er lige så vigtige. For en uden for stående betragter undrer det f.eks. at Beredskabsstyrelsen ikke medtages?

Det beskrives at man har anvendt dokument-analyse, interviews og stikprøver.

Side 15, paragraf 26, står der at "Vi har taget udgangspunkt i system-værktøjer og udtaget stikprøver med henblik på at teste, om myndighederne har implementeret eller foretaget en række sikkerhedshandlinger". Der henvises til bilag 1 metode for yderligere uddybning, men her står "Der er desuden udtaget stikprøver" (side 36), og på side 38 står " Vi har bl.a. udtaget stikprøver for at undersøge …". Det fremgår ikke hvordan det er sikret at de udtagne stikprøver har været repræsentative? Altså hvilken metode til udtagning der er anvendt? Er der anvendt tilfældig udvælgelse, stratificeret udvælgelse, eller noget tredje. Endvidere fremgår det heller ikke hvor mange stikprøver der er udtaget i forhold til populationen? Der i mod er der en vældig god beskrivelse af hvad de der udtaget til stikprøve er blevet spurgt om (side 38).

Metodisk kunne det også have været ønskeligt med lidt mere diskussion af hvordan man har afgjort om et givent krav – af de 20 – er opfyldt eller ej. Her savnes både et eksempel, og en lidt nærmere redegørelse for hvordan vurderingen er foregået. Har det været en enkelt (rigs)revisor? Et hold på to? Har der været en repræsentant med fra myndigheden? Det sidste er næppe tilfældet, idet der har været mange kommentarer til kravopfyldelsen fra de udvalgte myndigheder.

Alt i alt er beretningen metodisk på niveauet tilfredsstillende, men med plads til forbedring, f.eks. ifm. mangler som angivet oven for.

4. Fremstår beretningens konklusioner balancerede i forhold til de revisionsresultater, der er fremhævet i undersøgelsens analyse og resultater?

I tabel 2 side 20, fremgår det hvilke krav der ikke opfyldes, af de fem undersøgte statslige myndigheder. Det fremgår at ingen af de fem har opfyldt krav 13, regelmæssig opdatering af mobile enheder, samt at krav 18 ikke opfyldes af fire undersøgte myndigheder.

Resultatet af undersøgelserne er, at ingen af myndighederne på revisionstidspunktet efterlevede alle de minimumskrav til it-sikkerheden, som de var

forpligtet til at efterleve. ”Det finder Rigsrevisionen utilfredsstillende, idet de fleste af kravene skulle være implementeret den 1. januar 2020” (side 31)

Undersøgelsen viser også, at den manglende efterlevelse er særligt udbredt i forhold til 3 krav. Eksempelvis er der som sagt ingen af de 5 myndigheder, der efterlever minimumskrav 13 om regelmæssig opdatering af mobile enheder,

Endelig viser undersøgelsen, at der ikke har været en tilstrækkelig koordinering mellem Statens It og henholdsvis Energistyrelsen og Fødevarestyrelsen i forhold til at sikre minimumskrav 18 om kryptering af kommunikation til hjemmesider.

Konklusionerne er fint sporbare til beretningen og de foretagne analyser. Der er hverken over- eller under-konkluderet. Glimrende.

5. Hvad er den samlede vurdering af beretningen?

En god beretning med mange fine detaljer. Beretningen demonstrerer fin teknisk indsigt. Visse steder fremstår beretningen lidt ureflekteret, og metodisk er der nogen (mindre) mangler.

Vurdering af beretningens faglige kvalitet (sæt x)

Meget tilfredsstillende*	
Tilfredsstillende	*X*
Mindre tilfredsstillende	

**Gives til beretninger, der skiller sig positivt ud, og som derved kan fungere som inspiration og læring*

Evaluering af beretning 10/2021 Projekteringsfasen for Femern Bælt-forbindelsen

1. Er beretningens emne og formål klart motiveret og afgrænset?

Beretningen omhandler Femern Bælt-forbindelsens projekteringsfase, der oprindeligt var sat til at vare 4 år, men hvor der gik 11½ år fra projekteringsfasens start, til anlægsarbejderne kunne starte. Femern Bælt har et samlet budget på ca. 53 mia. – et af de største projekter i Danmark nogensinde.

I figur 1, side 6, er vist en tidslinje fra 2009 og frem til november 2021. På tidslinjen savner man at kunne se hvordan den forventede afslutningstid – fra 4 år til 11,5 år – af projekteringsfasen udvikler sig. I den efterfølgende tabel 1 er vist finansieringsforløbet. Her savner man en kobling mellem figur og tabel. Det kræver nogen bladren frem og tilbage for at se figur og tabel i sammenhæng. I figur 2 side 18 kan man dog få et overblik over hvordan de tyske myndigheders estimater udvikler sig

Så emnet for beretningen er klart, og emnet er vel motiveret, i medfør af den lange forsinkelse, og det meget store budget.

Formålet med undersøgelsen er at vurdere, om Transportministeriet og Femern A/S har styret projekteringsfasen for Femern Bælt-forbindelsen tilfredsstillende. Der fokuseres på risikovurdering ifm. tysk myndighedsgodkendelse, samt på kvalitetssikringen af de tidsplaner, der så markant er blevet overskredet.

Så formålet med beretningen er også klart.

2. Er det tydeligt, hvorfor de valgte revisionskriterier er egnede til at belyse formålet?

Først ses på om Femern A/S har haft robuste tidsplaner, der løbende har taget højde for aktuel viden om den tyske myndighedsproces. En robust tidsplan defineres som havende (side 9 – mine kursiveringer):

- ”afsat den *nødvendige tid til kendte processer* og aktiviteter i forbindelse med den tyske myndighedsproces

- *afspejlet usikkerhed* og manglende viden om varigheden og indholdsmæssige krav til den tyske myndighedsproces ved fx at afsætte tidsmæssige buffere til processen i tidsplanen
- *afspejlet afhængighederne* mellem den tyske myndighedsproces og de øvrige opgaver i projekteringsfasen."

Altså om der bag projektplaner ligger gode estimater, beregning af usikkerhed, og højdetagen for afhængigheder.

Dette første sæt af revisionskriterier har meget fokus på projektplanlægning. Men god projektstyring vil typisk også omfatte andre områder så som interessenthåndtering og underleverandørstyring ("procurement management"), jf. PMI's 10 vidensområder (se fx: The **6th edition** of the **PMBOK**® Guide). Men overvejelser om disse områder mangler I beretningen. Ud over projektplanlægning ses der dog på risikostyringen i projektet, et andet af de 10 vidensområder. Det er godt.

Dernæst ses på hvorvidt Transportministeriet har varetaget sine opgaver i projekteringsfasen tilfredsstillende. Hertil anvendes tre revisionskriterier:

- om ministeriet har taget højde for varigheden af den tyske myndighedsproces, da projekteringsloven blev fremsat
- om ministeriet har gennemført en tilstrækkelig kvalitetssikring af Femern A/S' tidsplaner
- om ministeriet har gennemført en tilstrækkelig kvalitetssikring af Femern A/S' bidrag til beslutningsgrundlagene for udbudsprocessen

Dette andet sæt af revisionskriterier har meget fokus på kvalitet. Kvalitet defineres ikke nærmere i beretningen, men ISO (den internationale standardiseringsorganisation) definerer det som graden af opfyldelse af forventninger. I revisionskriterierne tales der primært om kvalitetssikring, altså de aktiviteter hvor man sikrer sig kvaliteten fx i form af kvalitets-reviews eller inspektion af dokumenter.

Det diskuteres ikke om man skulle have set på andet end kvalitet i samspillet mellem Transportministeriet og Femern A/S. Det er her interessenthåndtering og underleverandørstyring kunne have været relevant, efter min mening.

Alt i alt synes det at være gode revisionskriterier, men koblingen til formålet fortaber sig. Der savnes en bedre og mere reflekteret diskussion af hvilke revisionskriterier man kunne have anvendt, sat lidt yderligere diskussion af valget.

3. Er det tydeligt forklaret, hvorfor den valgte metode er velegnet til at belyse formålet (metodeovervejelser/beskrivelser i kap 1 og metodisk tilgang i bilaget)?

Den valgte metode er baseret på dokumenter eller som det siges ”indhentet ved gennemgang af dokumentation” (side 11)

”Desuden undersøges Femern A/S’ styring af opnåelsen af den tyske myndighedsgodkendelse og udbudsprocessen samt Transportministeriets kvalitetssikring heraf gennem en række nedslagspunkter i perioden” (side 11). Konkret undersøges 5 tidspunkter i projekteringsfasen.

I figur A på side 47 ses at man har valgt en fremgangsmåde hvor man har 3 faser af undersøgelsen. Herefter beskrives dokumentanalysen i de enkelte faser meget omhyggeligt. Den del af metodeafsnittet er forbilledligt godt.

På side 12 fremgår at revisionen har vægtet de grafiske repræsentationer af tidsplanen og finder at ”Det er Rigsrevisionens opfattelse, at der bør være sammenhæng mellem de oplysninger, der fremgår af den grafiske fremstilling og af den medfølgende tekst”.

Modsætningsvis har Femern A/S ”oplyst, at den grafiske fremstilling af tidsplanerne er udtryk for en forenkling, som ikke kan betragtes isoleret fra de beskrivelser, der følger med”.

Denne diskurs/diskussion demonstrerer at der ville have været en fordel at supplere dokumentations-studier med flere interviews, end dem Rigsrevisionen faktisk har udført. Det kunne have uddybet de grafiske tidsplaner og en række andre ting, der kan læses for ’firkantet’ hvis man udelukkende baserer sig på dokumentation.

Der er uddrag af en interviewguide i Tabel A side 48, hvor man holder møde om tidsplaner. Det er rigtig godt med dette uddrag. Det giver en indsigt i de interviews der har komplementeret dokumentanalysen.

På side 46 står der ”Derudover har vi holdt møder med Transportministeriet og Femern A/S”. Men vi får ingen oplysning om hvilke møder, med hvilken dagsorden; er det den fra tabel A, side 48? Ej heller får vi noget begreb om sammenhængen mellem dokumenter og møder.

Senere i det egentlige analyseafsnit bliver det klart hvordan analysen er dokumenter er foregået. Der er indsamlet over 800 dokumenter og de er screenet på den samme systematiske måde, og resultaterne lagt ind i et regneark, fremgår det på side 47. Der er i øvrigt en mindre diskrepans omkring antallet af dokumenter. På side 47 står der ”800 dokumenter”, og på side 49 står der

”Samlet set bygger analysen på et materialegrundlag på knap 1.600 dokumenter – heraf er nogle dokumenter dubletter …”. Men der er vel næppe 800 dubletter?

I beretningen er der nogle metodemæssigt rigtig gode tabeller, som giver et fint overblik over usikkerheder, hvornår de opstår, og hvad Femern A/S gør i relation hertil, i tabellerne 3 og 4, side 20 og 21.

Der står også på side 48 ”Med henblik på at sikre en systematisk og ensartet gennemgang af materialet i forhold til revisionskriterierne udarbejdede vi en læseguide for hvert af vores undersøgelses-spørgsmål. Guiden indeholdt analysespørgsmål til at guide vores læsning”. Det er en god beskrivelse og fremgangsmåde.

På side 23 fremgår det, at Femern A/S ikke opdaterede sin tidsplan frem mod vedtagelsen af anlægsloven i 2014, selv om der var opstået forsinkelser. På bestyrelsesmødet forud drøftedes tidsplanen, og det ”fremgik af drøftelserne, at det ikke kunne anbefales at udmelde nye tidsplaner for det samlede projekt før vedtagelsen af anlægsloven, jf. tabel 4. Begrundelsen var, at der var behov for at opretholde et pres på forskellige aktører”. Dette er et meget tydeligt eksempel på at en egentlig interessentanalyse kunne have været meget nyttig, og der er som tidligere nævnt en af de 10 kernekompetencer for projektledere (jf. PMBOK og PMI).

I kapitel 3 startende side 31 vurderes kvalitetssikringen i projektet. Det defineres ikke nærmere hvad der menes med kvalitetssikring. Indirekte kan man se af teksten, at det handler om hvorvidt ministeriet forholdt sig kritisk og var opmærksom på mangler. På side 32 står: ”Ministeriet forholdt sig i 2010/2011 ikke kritisk til Femern A/S’ bidrag til beslutningsgrundlaget … Ministeriet reagerede ikke på, at der manglede oplysninger om de risici, som Femern A/S præsenterede, og ministeriet søgte ikke at få afklaret, om der var yderligere risici…”. Samme definition, at det handler om at forholde sig kritisk ses på side 35, afsnit 71.

Man kunne også have anvendt ISO 9000 definitionen af kvalitetssikring der siger ”… that quality assurance is part of quality management focused on providing confidence that quality requirements will be fulfilled”. Endelig kunne man have undersøgt om Ministeriet anvendte nogen af de normale kvalitetssikrings-teknikker så som review, inspektion, definition af kvalitetsmål m.v.

Alt i alt er der mange rigtig gode elementer og detaljer mht. metode. Dele af metodeafsnittet er ligefrem forbilledlige. Det er kun den helt overordnede sammenknytning af metode og formål der fremstår en smule svagt. Formålet var jo at vurdere, om Transportministeriet og Femern A/S har styret projekteringsfasen for Femern Bælt-forbindelsen tilfredsstillende. Men styring kan

foregå på mange måder og på mange områder. Men her i beretningen fokuseres alene på planer og risici. Det er en lidt snæver opfattelse af styring som der ikke argumenteres for.

4. Fremstår beretningens konklusioner balancerede i forhold til de revisionsresultater, der er fremhævet i undersøgelsens analyse og resultater?

Beretningen konkluderer at Transportministeriets og Femern A/S' styring af Femern Bælt projekteringsfasen ikke har været "helt tilfredsstillende". Der peges også på, at der undervejs er "taget unødige økonomiske risici" i forhold til tunnelentrepriserne

I opsummeringen af konklusioner på side 3 peges også på, at "Ministeriet vidste, at der var opstået forsinkelser i projektet … Alligevel fastholdt ministeriet målet om at åbne Femern Bælt-forbindelsen i 2018."

Ligeledes peges på side 3 på, at Transportministeriet ikke gennemførte en tilstrækkelig kvalitetssikring af Femern A/S' tidsplaner. Dette udbygges i et helt kapitel senere. Det konstateres at der i Ministeriet forelå information om den tyske myndighedsproces, der havde et sådant indhold, at det burde have ført til, "at ministeriet forholdt sig mere kritisk til tidsplanerne".

Disse konklusioner er fint sporbare til beretningen og de foretagne undersøgelser. Jeg mener dog godt at man kunne have konkluderet lidt skarpere en "ikke helt tilfredsstillende". Jeg mener beretningen og de foretagne undersøgelser giver baggrund for at tale om "utilfredsstillende" risikostyring og kvalitetssikring.

5. Hvad er den samlede vurdering af beretningen?

En kort og præcis beretning, med fokus på samspillet mellem Transportministeriet og Femern A/S. Der afdækkes mange relevante problemer, på en god måde, med rigtig fin sporbarhed til analyserne. Beretningen har også meget fine metodevalg og -beskrivelser, nogle af dem helt forbilledlige. Derfor har jeg valgt at give scoren "meget tilfredsstillende", selv om der også er dele der kunne have været bedre, eksempelvis koblingen mellem revisionskriterier og formål.

Vurdering af beretningens faglige kvalitet (sæt x)

Meget tilfredsstillende*	*X*
Tilfredsstillende	
Mindre tilfredsstillende	

Gives til beretninger, der skiller sig positivt ud, og som derved kan fungere som inspiration og læring

Evaluering af beretning 14/2021 Energinets outsourcing af driften af forsyningskritisk it-infrastruktur

1. Er beretningens emne og formål klart motiveret og afgrænset?

Beretningens emne er Energinets beslutning om at outsource driften af forsyningskritisk it-infrastruktur.

Energinet indgik i juni 2020 en kontrakt med KMD, som bl.a. indebar outsourcing af driften af den forsyningskritiske it-infrastruktur. Outsourcingen omfatter ca. 90 % af Energinets it-systemer (side 5)

Motivationen fremgår tydeligt; Energinet står for en meget stor del af det danske el- og gas-net. Så et angreb på denne it-infrastruktur ville i værste fald kunne afbryde forsyningen af el og gas til mange danske husstande.

Formålet med undersøgelsen er at vurdere, om både Klima-, Energi- og Forsyningsministeriet på den ene side, og Energinet på den anden side, har håndteret outsourcing af driften af den forsyningskritiske it-infrastruktur ansvarligt.

Beretningen fokuserer på perioden fra 2018 til slutningen af 2021. Begrundelsen for denne afgrænsning er, at Ministeren på det tidspunkt, april 2018, understreger over for Energinet, at de skal have fokus på it-sikkerhed, fordi Energinets it-sikkerhed spiller en afgørende rolle i forhold til it-sikkerhed i hele el- og naturgassektoren.

Så beretningens emne og formål er klart formuleret, vel motiveret og passende afgrænset.

2. Er det tydeligt, hvorfor de valgte revisionskriterier er egnede til at belyse formålet?

Der opstilles 4 revisionskriterier for at besvare undersøgelsens formål (side 6-7):

1. Har Energinet har orienteret Klima-, Energi- og Forsyningsministeriet rettidigt om outsourcingen?
2. Har Energinet sikret sikkerheden i forbindelse med outsourcingen

3. Har Klima-, Energi- og Forsyningsministeriet har sikret tydelige rammer for tilsynet med Energinets it-forhold?
4. Har Ministeriet har ført et tilstrækkeligt løbende tilsyn med Energinets it-sikkerhed?

Det står hurtigt klart at Ministeriet ikke blev orienteret om outsourcingen. Derfor kan formålet, om outsourcingen er håndteret ansvarligt, ikke umiddelbart undersøges. Det fører til revisionskriterierne 3. og 4. oven for. De synes umiddelbart velegnede til at belyse formålet.

I forbindelse med at Ministeriet ikke blev orienteret om outsourcingen står der på side 11 at "Energinet har oplyst, at Energinet ikke vurderer, at der er tale om en strategisk beslutning". Det bruges som forklaring på ikke at have orienteret ministeriet. Den vurdering mener jeg er ganske kritisabel. I alle de lærebøger jeg har anvendt til undervisning i IT-strategi er outsourcing altid med som et meget strategisk emne. Det vedrører topledelsen hvor der skal sources, og det er en beslutning der rækker år ind i fremtiden. Så per definition er outsourcing en strategisk beslutning, fordi det er topledelsen der træffer de langsigtede beslutninger der defineres som strategiske. Som følge heraf kunne Rigsrevisionen godt have været endnu hårdere i sin kritik af Energinet.

Alt i alt finder jeg, at det er tydeligt at de valgte revisionskriterier er velegnede til at belyse formålet.

3. Er det tydeligt forklaret, hvorfor den valgte metode er velegnet til at belyse formålet (metodeovervejelser/beskrivelser i kap 1 og metodisk tilgang i bilaget)?

Undersøgelsen bygger på en gennemgang af dokumenter, som der står i metodeafsnittet og bilag om metode. Det diskuteres ikke noget sted om det er den bedste metode. Vi får heller ingen indsigt hvordan dokumenterne er gennemgået.

Der har desuden været holdt møder med både Ministeriet og Energinet. "Formålet med møderne har været at stille spørgsmål til det udleverede materiale og at få en dybere forståelse for de forhold, vi har undersøgt." (side 18)

Der er det særlige forhold, at Energinet vurderer, at "Rigsrevisionens første beskrivelse og behandling af it-sikkerhedsmæssige forhold i forbindelse med undersøgelsen af outsourcingen … er fortrolige oplysninger, som … kan kompromittere statens sikkerhed og rigets forsvar. Derfor vælger Rigsrevisionen at imødekomme ønsket om fortrolighed, så disse oplysninger er udeladt og generaliseret: "Beretningen indeholder således ingen konkrete

beskrivelser af de it-sikkerhedsbrister, som Rigsrevisionen konkluderer om", som der står på side 18.

På side 18 og 19 findes en redegørelse for hvilke dokumenter der er gennemgået. Man har f.eks. "undersøgt ministeriets ejerskabsdokumenter, retningslinjer for kommunikation mellem Energinet og ministeriet samt Energinets koncerninstruks." (side 19). Noget jeg finder underligt er, at man ikke går i detaljer med udbuds- og kontraktmateriale for outsourcingen. Det må vel være her man bedst ville have kunnet se hvordan man har "sikret sikkerheden", dvs. revisionskriterium 2. Man nøjes i stedet med at gennemgå "Energinets businesscase og risiko-vurderinger"

Det leder til en kommentar ang. side 12 hvor der står: "Der fremgår ikke overvejelser i businesscasen om outsourcingens risici for den offentlige kontrol med forsyningskritisk it-infrastruktur". Her mener jeg at man kunne have spurgt om hvad man kan lære af det? Kunne Rigsrevisionen f.eks. anbefale at man i fremtidige business cases skulle inddrage sådanne risici.

Med hensyn til risici så fremgår det ingen steder om it-projektrådet (under digitaliseringsstyrelsen/Finansministeriet) har været inden og lavet en vurdering af outsourcing-projektet og de dermed forbundne risici. Formelt skal it-projektrådet risikovurdere alle statens it-projekter over 10 mio. kr. Derfor tænker jeg at de burde have været, dels fordi det jo handler om it, dels fordi der er tale om et relativt stort beløb. Så outsourcing-projektet opfylder begge krav til at it-projektrådet skal ind over.

Så konklusionen er, at det ikke er forklaret tydeligt hvorfor den valgte metode er velegnet, og der er en række overvejelser der savnes

4. Fremstår beretningens konklusioner balancerede i forhold til de revisionsresultater, der er fremhævet i undersøgelsens analyse og resultater?

Som svar på kriterie 1 konkluderes, at Energinet ikke har orienteret Klima-, Energi- og Forsyningsministeriet rettidigt om outsourcingen.

Som svar på kriterie 2 konkluderes, at Energinet ikke har sikret sikkerheden i forbindelse med outsourcingen.

Som svar på kriterie 3 konkluderes, at Ministeriet ikke har sikret tydelige rammer for tilsynet med Energinets it-forhold.

Og som svar på kriterie 4 konkluderes, at Ministeriet har ført et løbende tilsyn med Energinets it-sikkerhed, men at man ikke har anvendt den på et givent tidspunkt til rådighed værende viden fuldt ud.

Disse konklusioner passer smukt sammen med revisionskriterierne og der er god sporbarhed til de fremlagte analyser.

5. Hvad er den samlede vurdering af beretningen?

En kort fokuseret beretning, med rigtig god balance mellem revisionskriterier og konklusioner. Desværre skæmmes beretningen af et for simpelt og ure-flekteret metodeafsnit.

Vurdering af beretningens faglige kvalitet (sæt x)

Meget tilfredsstillende*	
Tilfredsstillende	*X*
Mindre tilfredsstillende	

**Gives til beretninger, der skiller sig positivt ud, og som derved kan fungere som inspiration og læring*

Evaluering af beretning 03/2022
Statens it-beredskab

1. Er beretningens emne og formål klart motiveret og afgrænset?

Ja, emnet er en undersøgelse af statens it-beredskab. Formålet er at afdække om det er tilfredsstillende?

Ud af 3400 it-systemer udvælges 13 samfundskritiske it-systemer til undersøgelse. To ting undersøges, dels om der er beredskabsplaner, dels om der er krisestyringsplaner.

2. Er det tydeligt, hvorfor de valgte revisionskriterier er egnede til at belyse formålet?

Ja, der er et ganske omfattende sæt revisionskriterier, som dog ikke i denne korte udgave af beretningen er selvstændigt præsenteret, men findes i metode-kapitlet.

Revisionskriterierne omfatter; Om der findes en kortlægning af hvad der er samfundskritiske it-systemer? Om der er afhængigheder til andre systemer? Om der er lavet risikovurderinger, og disse løbende er opdateret? Om der er lavet retableringsplaner, og om disse er testet? Om der er lavet krisestyringsplaner? Og endelig om ISO 27001-standardens kontrolmål for it-beredskabet er implementeret?

Jf. figur 2, side 7, tager beretningen også udgangspunkt i noget der kaldes ”helhedsorienteret beredskabsplanlægning”, en vejledning fra beredskabsstyrelsen.

Alt i alt virker det som om beretningens revisionskriterier dækker emne og formål godt og helhedsorienteret.

3. Er det tydeligt, hvorfor den valgte metode er velegnet til at belyse formålet

De spørgsmål der anvendes (revionskriterierne beskrevet oven for) fremgår af metode-afsnittet.

Der er ikke nogen egentlig metode-beskrivelse i metode-kapitlet. Som læser af denne korte beretning får man ingen præsentation af hvordan de 13 samfundskritiske systemer er udvalgt? Hvordan man har undersøgt om der var et beredskab? Hvordan man har undersøgt om beredskabsplaner er afprøvet? Osv.

Så det er ikke muligt at sige noget fornuftigt om metode-afsnittets kvalitet. Den korte beretning der må offentliggøres, gør det ikke muligt at lave en evaluering heraf.

4. Fremstår beretningens konklusioner balancerede i forhold til de revisionsresultater, der er fremhævet i undersøgelsens analyse og resultater?

Konklusionen på beretningen (side 3) er: ”De undersøgte myndigheder har ikke sikret et tilfredsstillende it-beredskab for de 13 udvalgte samfundskritiske it-systemer. Særligt er it-beredskabet utilfredsstillende for én af de undersøgte myndigheder, hvor undersøgelsen har omfattet flere it-systemer”.

Med den meget begrænsede information der er til rådighed i den korte offentlige beretning er det ikke muligt at afgøre om beretningens konklusioner er balancerede?

5. Hvad er den samlede vurdering af beretningen?

Det er et ekstremt samfundsvigtigt emne Statsrevisorerne har bedt Rigsrevisionen undersøge. Konklusionerne, som de fremgår af opsummeringen på de første sider, er skræmmende.

Det er fuldt forståeligt, at man vælger ikke at offentliggøre den fulde rapport, for ikke at give nogen med ondsindede hensigter let spil. Den korte udgave af rapporten yder dog ikke undersøgelsen fuld retfærdighed (tror jeg). Jeg afstår derfor fra at lave en samlet vurdering af den korte beretning.

Tværgående pointer fra de skriftlige evalueringer af beretningerne fra 2022

Jeg finder tre af de fire beretninger fra 2022 som havende en god kvalitet. Den fjerde forkortede beretning har det ikke været muligt at vurdere på linje med de andre.

Revisionskriterierne ar klare og præcise og godt knyttet an til formålet i alle de beretninger jeg har læst.

Jeg synes metode-overvejelserne over årene er blevet bedre og bedre, siden jeg første gang var med som evaluator for fem år siden. I år er der ligefrem en beretning jeg fremhæver, specifikt for de detaljerede metode-overvejelser

Beretningerne fremstår med konklusioner der har god sporbarhed til de bagvedliggende analyser. Der er ikke konklusioner som det er svært at finde solidt belæg for i data.

I lighed med sidste år savner jeg, at beretningerne også inkluderer et læringsperspektiv, dvs. et fokus på hvad der kan læres af det undersøgte og det fundne. Det er efter min opfattelse en vigtig del af ethvert beredskab, at man kan lære af sine fejl og mangler, og dermed har et fundament for at gøre tingene bedre en anden gang.