FOLKETINGET
RIGSREVISIONEN

Evalueringer af Rigsrevisionens beretninger fra 2023 af Professor Jan Pries-Heje

Januar 2024

Evaluator Jan Pries-Heje

Evaluering af beretning 13/2022 Porteføljestyring af statens kritiske it-systemer

1. Er beretningens emne og formål klart motiveret, og er afgrænsningen relevant?

Beretningen omhandler styringen af porteføljen af kritiske it-systemer for 11 myndigheder, og yderligere mere i dybden for 4 myndigheder. Der er tale om en evaluering som Rigsrevisionen selv har taget initiativ til i oktober 2022, og gennemført i 2023.

Formålet med beretningen er at afdække om myndighedernes styring af kritiske it-systemer følger en model for porteføljestyring af statslige it-systemer, indført af Finansministeriet i 2018, og gjort obligatorisk for myndigheder at følge. Fra december 2022 er det Økonomistyrelsen der har ansvar for modellen (s. 4).

Første del af undersøgelsen omhandler 11 myndigheders kortlægning af kritiske it-systemer, handlingsplaner og statusnotater til It-rådet.

Anden del af undersøgelsen handler om 4 myndigheder, hvor man har efterspurgt og gennemgået yderligere dokumentation vedrørende handlingsplanerne og de initiativer, som myndighederne har opstillet.

Formålet med beretningen er klart motiveret fx i afsnit 4, samt i reference til Statens Digitaliserings-strategi, 2022 (manchet/sidetekst, side 4).

Beretningen er afgrænset til alene at se på om modellen for porteføljestyring følges. Der ses alene på samfunds- og forretningskritiske systemer, samt myndighedernes arbejde inden for rammerne af modellen.

I afsnit 18 fremgår det at flere myndigheder har oplyst at de anvender yderligere styringsdokumenter ud over modellens. Dette afgrænser man sig fra at medtage.

Jeg synes godt man kan diskutere denne valgte afgrænsning. Det antages at modellen er komplet og omfatter alt relevant, men at der anvendes yderligere styringsdokumenter af nogle myndigheder kunne jo tyde på at det ikke er tilfældet.

I afsnit 13 fremgår det, at modellen har udviklet sig fra dens fødsel i 2008 til 2022, og bl.a. er gået fra 80 spørgsmål, som myndighederne skulle besvare for hvert system, til ca. 25. Det oplyses eller diskuteres ikke noget steds hvad det er for 55 spørgsmål der ikke skønnes relevante? Her mener jeg en god revision kunne have gravet lidt dybere.

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

Der er stillet tre undersøgelsesspørgsmål (side 21):

- Giver myndighedernes kortlægninger overblik over deres kritiske it-systemers tilstand?
- Understøtter myndighedernes handlingsplaner deres arbejde med de kritiske it-systemer?
- Har myndighederne fulgt op på fremdriften i handlingsplanernes initiativer?

Disse tre spørgsmål virker egnede til at belyse formålet om hvorvidt porteføljestyringsmodellen følges og virker.

I paragraf 36 findes at kun ca. 30% anvender målbare succeskriterier i deres planer. Dette kritiseres, selv om nogle myndigheder argumenterer for at det ikke er et krav i modellen for porteføljestyring. Ser man på litteraturen om klassisk projektledelse så foreskrives det ganske enigt at man skal formulere SMART´e mål og succeskriterier, hvor SMART er en forkortelse for Specifikt, Målbart, Accepteret, Realistisk og Tidsfastsat. Rigsrevisionen kunne derfor være endnu mere kritisk over for planer der ikke indeholder nogle målbare succeskriterier. Man kunne også kritisere at de andre dele af 'SMART' mangler, og man kunne kritisere hvis der ikke var SMART formulerede mål i de undersøgte handlingsplaner.

I paragraf 36 findes ydermere, at der kun for ca. 20% af handlinger er sat ressurser af. Det er klart at opgaver i en plan, hvortil der ikke afsættes resurser, aldrig vil blive til noget. Det er elementær lærdom om projekter. Flere myndigheder fremfører, at det er svært at afsætte resurser over flere år, når man er meget afhængig af 1-årige budgetter (Finansloven). Her havde jeg gerne set lidt refleksion om, at hvis man virkelig ønsker at beskytte Danmarks kritiske infrastruktur, så er det næppe noget der gøres med en 1-årig horisont. Så her kunne Rigsrevisionen have markeret, at der var behov for flerårige budgetter og resursetildeling.

I paragraf 39 nævnes det, at det er uklart om risikovurderinger er anvendt til prioritering af handlingsplaner. Det vil oplagt være en god idé fremgår det,

hvilket er i overensstemmelse med ”klassisk” projektledelsesteori. Denne indsigt, samt flere andre kunne det have været fint at opsamle i en form for feedback på modellen. Det fremgår dog intet sted om noget sådant er foregået.

3. Er de valgte metoder velegnede til at belyse formålet og undersøgelsesspørgsmålene?

I metode-bilaget side 22 gøres der rede for, at der er valgt 11 myndigheder fordelt på 5 ministerier, og at der valgt nogen myndigheder der ”har gennemført kortlægningen og har været i review ved It-rådet 2 gange”.

En sådan udvælgelsesmetode giver risiko for et positivt bias. En myndighed der helt har ignoreret at kortlægge og intet har afleveret til it-rådet vil potentielt have kunnet snige sig uden om at indgå

Der er valgt en kombination af interviews/møder og dokumentstudier. De fremtagne dokumenter er kodet med samme ”kodebog” for ”…at understøtte en ensartet behandling af myndighedernes dokumentation. For yderligere at sikre kvaliteten af resultaterne er der foretaget blindkodning af dokumentationen. Dette er gjort ved, at alle myndighedernes dokumentation er gennemgået og kodet af 2 personer fra projektgruppen, hvorefter de 2 personer har sammenholdt resultater med henblik på at sikre kvaliteten af kodningen.”

Denne proces er rigtig god og sikrer på bedste vis, at der ikke optræder bias eller forskelsbehandling.

Det ville have været godt at se et eksempel på kodning, og også lidt refleksion om hvorvidt denne ”blindkodning” havde givet anledning til at man have fundet nogen ting som ellers kunne have været gledet forbi.

4. Er beretningens resultater og konklusioner tilstrækkeligt underbygget?

Det konkluderes at myndighedernes porteføljestyring ikke har været ”helt tilfredsstillende”. Der peges senere i rapporten på, at det især er fraværet af målbare succeskriterier, samt den manglende allokering af resurser til planen, der ligger til baggrund for denne konklusion.

Det er uklart hvilken skala der anvendes med brugen af ”ikke helt tilfredsstillende”. Er helt tilfredsstillende f.eks. bedre eller dårligere end meget tilfredsstillende? Og hvor langt er der fra ”ikke helt tilfredsstillende” til ”mindre tilfredsstillende”. Det kunne have været fint med en præcisering af den anvendte skala.

Men bortset fra denne – trods alt – detalje så giver beretningen en fin underbygning af resultater og konklusioner.

5. Er beretningens konklusioner balancerede?

Ja, beretningens konklusioner fremstår balancerede og der er tydelig sporbarhed mellem det der diskuteres i kapitlerne og det der står i konklusionerne

6. Hvad er den samlede vurdering af beretningen?

En god beretning med god sammenhæng mellem analyse og konklusioner. Visse steder fremstår beretningen lidt ureflekteret, f.eks. ved aldrig at forholde sig kritisk til om modellen for porteføljestyring er adækvat.

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 5/2023
It-sikkerhed i Statens It's servere

1. Er beretningens emne og formål klart motiveret, og er afgrænsningen relevant?

Beretningen emne er sikkerhed, med fokus på Statens It, der har ansvar for It til 151 myndigheder på tværs af 21 ministerområder. Der er tale om en beretning som Rigsrevisionen selv har taget initiativ til i marts 2023, efter at en anden undersøgelse hos 2 myndigheder viste at serverne hos Statens It ikke længere kunne sikkerhedsopdateres. Så formålet er at vurdere, om Statens It har sikret, at Statens It's servere kan sikkerhedsopdateres.

Motivationen er, at uden en sikkerhedsopdatering kan følsomme personoplysninger og forretningskritiske data blive udsat for en unødig risiko for kompromittering. Det er en klar, præcis og forståelig motivation

Så svaret på om emne og formål er klart motiveret er ja.

Der er foretaget en afgrænsning til de 46 myndigheder som ved undersøgelsesstart i marts 2023 ifølge Statens It brugte servere, der ikke længere kunne sikkerhedsopdateres. Da der er 151 myndigheder der anvender Statens It, har man altså afgrænset sig fra 2/3 af myndighederne.

Man afgrænser sig til en ret simpel "sort-hvid" vurdering; kan serveren sikkerhedsopdateres, ja eller nej. Her kunne man med fordel have taget stilling til hvad god "Governance" ville være. Det kunne f.eks. være at man har en form for årshjul der sikrer en opdatering hvert 4.-5. år af alle applikationer. Det ville tage fat om problemet rod, frem for symptomet, at der ikke sikkerhedsopdateres.

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

Der vælges tre undersøgelsesspørgsmål:

1. Har Statens It opgraderet eller nedlagt servere for de 46 myndigheder, der indgår i undersøgelsen, inden leverandøren er ophørt med at udvikle sikkerhedsopdateringer?
2. Har Statens It gennemført kompenserende foranstaltninger for servere, der ikke længere kan sikkerhedsopdateres?
3. Har Statens It etableret procedurer, der sikrer, at de løbende og rettidigt kan opgradere eller nedlægge servere, der ikke længere kan sikkerhedsopdateres?

Ja, spørgsmål 1 følger direkte af formålet. Der refereres også til ISO 27001 og "*Cyberforsvar der virker*" (afsnit 14). Men spørgsmål 2 om kompenserende handlinger, og spørgsmål 3 om hvorvidt der er etableret procedurer der sikrer løbende opgradering og/eller nedlæggelse af servere, følger ikke lige så klart af formålet. Dog kan spørgsmål 3 siges at være forankret i ISO 27001, der som rigtig mange andre ISO-standarder foreskriver at processer og procedurer skal være på plads.

Med hensyn til kompenserende handlinger så fremgår det af beretningen, at en af grundene til en manglende opgradering af servere hos nogle myndigheder er, at vigtige fagsystemer i så fald ville ophøre med at fungere (s fx boks 3, side 11). Der gives ingen detaljer om hvor mange af de manglende opgraderinger der kan forklares af dette? Der mangler også detaljer om hvorvidt der er lavet planer for at gøre noget ved dette drilske problem? Igen, som jeg også nævnte under afgrænsningen oven for, kan dette problem relateres til manglen på god Governance.

Med hensyn til manglen på detaljer så står der på side 2 at " Da beskrivelsen af sårbarhederne ifølge Finansministeriet potentielt kan udgøre en risiko for statens sikkerhed, gengiver vi ikke disse detaljer i beretningen". Det er selvsagt umuligt at sige hvilke detaljer der er udeladt, og hvilke man ikke har dykket ned i – om nogen.

3. Er de valgte metoder velegnede til at belyse formålet og undersøgelsesspørgsmålene?

Som metode er valgt at gennemgå materiale fra Statens It. Dertil kommer et dataudtræk fra en database over servere hos Statens It. Desuden har man haft hjælp af en cybersikkerhedsekspert Jacob Herbst, der bl.a. har gennemgået beretningen og rådgivet konsekvenser og alvorsgrad.

Det fremgår ikke om man på nogen måde har sikret datakvaliteten af den database man har lavet udtræk af. Og da mange konklusioner bygger på de udtræk der er lavet finder jeg det betænkeligt, at der intet står om hvordan Statens It har sikret kvaliteten af data.

Ligeledes er det betænkeligt, at der blot står, at man gennemgået dokumenterne. Har der været anvendt en eller anden systematik i gennemgangen, ja så får vi det ikke at vide.

4. Er beretningens resultater og konklusioner tilstrækkeligt underbygget?

Det er nogle stærke konklusioner statsrevisorerne drager på baggrund af beretningen; ”Statsrevisorerne finder det utilfredsstillende, at Statens It ikke har sikret, at alle Statens It’s servere kan sikkerhedsopdateres”, og ”Statsrevisorerne finder det bekymrende, at Statens It’s utilstrækkelige sikkerhedsopdateringer og utilstrækkelige kompenserende foranstaltninger indebærer risiko ...”

Det første udsagn, der jo også er besvarelsen af undersøgelsesspørgsmål 1, findes fuldt ud underbygget i de fremdragne tal.

I forbindelse med det andet udsagn kunne jeg ønske flere præciseringer af hvad kompenserende foranstaltninger kunne være. Det beskrives kort, men rent teknisk findes der mange løsninger der kan kompensere. Med hensyn til servere så har rigtig mange private virksomheder lagt deres services i en sky (”clouden”) og øget ”virtualiseringen”. Statens It har oprettet en statslig sky kaldet GovCloud (https://govcloud.dk/). En god modernisering indebærer at man opgraderer applikationer så de bliver operativsystem uafhængige. Eksempelvis ved at løfte ”virtualiseringen” til PAAS (platform-as-a-service) eller SAAS (software as a service). Dette vil særligt være relevant ved services der går på tværs af myndigheder så som rejseafregning, journalisering og lign. Derfor undrer det, at det slet ikke omtales som en mulighed at servere kan lægges i skyen, og heller ikke kan fremgå af den database der er hentet oplysninger fra, jf. de felter der angives som indhentet på side 15. Men fordi man har valgt en relativt sort-hvid afgrænsning kommer man slet ikke på denne problemstilling om virtualiseringen af servere. Det synes jeg er en mangel.

5. Er beretningens konklusioner balancerede?

Ja, de dragne konklusioner fremstår balancerede og velunderbyggede. Med den lille tilføjelse, at det undrer at de tekniske muligheder for at lægge serverfunktionalitet i skyen ”GovCloud” slet ikke omtales.

6. Hvad er den samlede vurdering af beretningen?

En homogen og tilfredsstillende beretning med et klart formål, tre undersøgelsesspørgsmål der ikke klart følger af formålet, men besvares fint. God sporbarhed mellem analyse og konklusioner, og balancerede og velunderbyggede konklusioner. Alt i alt en beretning på et tilfredsstillende niveau.

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 6/2023
Statens it-beredskab II

1. Er beretningens emne og formål klart motiveret, og er afgrænsningen relevant?

Ja, emnet er en undersøgelse af statens it-beredskab. Formålet med undersøgelsen er at vurdere, om staten har et tilfredsstillende it-beredskab for 12 udvalgte samfundskritiske it-systemer, så staten kan opretholde samfundskritiske funktioner i tilfælde af større it-hændelser (afsnit 4). Begge dele er klart motiveret, og der er i margin-tekst side 5 givet et eksempel på hvad der kan ske hvis man ikke har styr på beredskabet.

Som afgrænsning har man valgt at fokusere på 3 typer af it-beredskabsplaner i it-beredskabet: krisestyringsplaner, nødplaner og reetableringsplaner, i perioden januar 2020 - marts 2023. I afsnit 8 findes en god beskrivelse af hvad disse planer bør omfatte.

Man afgrænser sig fra at se på faktisk indtrufne hændelser og hvordan planerne faktisk har fungeret. Der er ikke nogen god argumentation for dette.

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

Der formuleres fire undersøgelsesspørgsmål:

1. Har staten et tilfredsstillende grundlag for at etablere et it-beredskab for de udvalgte samfundskritiske it-systemer?
2. Har staten implementeret tilfredsstillende krisestyringsplaner for de udvalgte samfundskritiske it-systemer?
3. Har staten implementeret tilfredsstillende nødplaner for de udvalgte samfunds-kritiske it-systemer?
4. Har staten sikret, at der er implementeret tilfredsstillende reetableringsplaner for de udvalgte samfundskritiske it-systemer?

Hvert af disse spørgsmål besvares i et separat kapitel (2 til og med 5). Det giver en god struktur og oversigt over svarene. Ydermere er der rigtig sporbarhed fra spørgsmål, over analyse, til de trufne konklusioner. Ydermere starter hvert af kapitlerne 2 til 5 med en kort delkonklusion, hvilket gør det meget nemt at være læser.

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

3. Er de valgte metoder velegnede til at belyse formålet og undersøgelsesspørgsmålene?

Som metode vælges dokumentgennemgang suppleret med interviews med de pågældende myndigheder. De dokumenter der gennemgås omfatter krisestyringsplaner, nødplaner og reetableringsplaner.

ISO 27001 standarden og Digitaliseringsstyrelsens vejledninger om beredskabsplaner angives som kilder til de revisionskriterier der meget omhyggeligt, og med gode referencer er angivet i bilag 2. Øverst side 32 fremgår det dog at nogen ting er fravalgt. Men vi får ikke at vide hvilke og hvorfor?

I bilag 2 er oplistet alle de elementer, som indgår i vurderingen af krisestyringsplaner, nødplaner, reetableringsplaner og testen af planerne. Det nævnes at der er nogen af de samme ting der blev set efter i del 1 (beretningen fra sidste år) for så vidt angår krisestyringsplaner og reetableringsplaner. Hermed fremgår det også indirekte at man i forhold til sidste år har tilføjet kriterier om nødplaner og test. Det er en rigtig god tilføjelse.

Til den detaljerede gennemgang har man valgt at tilføje en pointgivning. Således kan for eksempel en gennemgået krisestyringsplan få 100 point hvis den indeholder alle 5 centrale elementer. Man kan diskutere om denne kvantificering er en god idé på et grundlag der er så relativt lille (7 myndigheder, 12 systemer). Men i analysen kapitel 2 til 5 virker det faktisk rigtig godt. Og i metode-bilaget er det omhyggeligt forklaret hvad det er man gør med pointene.

Alt i alt synes de valgte metoder at være endog meget velegnede til at belyse formålet og svare på undersøgelsesspørgsmålene.

4. Er beretningens resultater og konklusioner tilstrækkeligt underbygget?

I kapitel 2 ses der på hvorvidt myndighederne for de 12 udvalgte systemer har et tilfredsstillende grundlag for at etablere et it-beredskab. Først ses der på om der er kortlagt sammenhænge til andre systemer (tabel 1, side 9). Dernæst ses på om der er taget udgangspunkt risici, sårbarheder og trusler, samt disses konsekvenser og sandsynligheder. Det viser sig i tabel 2 (side 10) kun at ske delvist eller slet ikke hos en række myndigheder. Til sidst i kapitel 2 ses på om ministerierne har ført tilsyn med myndighederne.

I kapitel 3 ses på om myndighederne har krisestyringsplaner til anvendelse ved et større it-nedbrud? I figur 3 (side 13) vises de fem elementer der bør indgå i en krisestyringsplan, udarbejdet på baggrund af "... ISO 27001 og Digitaliseringsstyrelsens vejledning i it-beredskab". Det viser sig at alle myndigheder har lavet krisestyringsplaner, men for den anonymiserede "Myndighed 1" indeholder den kun et af de fem elementer. Endelig ses der på om planer ajourføres årligt. I afsnit 3.2 ses der på om planerne er testet årligt, og om testresultaterne er koblet til forbedringsforslag. Det viser sig kun at være Erhvervsstyrelsen der lever op til alle revisionskriterier (tabel 3, side 15).

I kapitel 4 ses der på om myndighederne har udarbejdet tilfredsstillende nødplaner for de udvalgte it-systemer Det viser sig at være tilfældet for størstedelen, men kun 2 af nødplanerne er blevet testet (tabel 5, side 20). Af tabel 4 (side 18) ses også, at Myndighed 1, 2 og 3 mangler planer eller ikke har planer der lever op til revisionskriterierne.

Endelig i kapitel 5 fokuseres på reetableringsplaner, og hovedparten af disse er "ikke tilfredsstillende". I figur 5 fremgår seks centrale elementer af en reetableringsplan. Igen med præcis kildeangivelse (ISO 27001 og Digitaliseringsstyrelsens vejledning i it-beredskab). Og i figur 6 (side 23) fremstår det tydeligt at status er utilfredsstillende, bortset fra indenrigs- og sundhedsministeriet.

Konklusionen på beretningen (side 3) er at "Statsrevisorerne kritiserer, at der for 7 af de 12 undersøgte samfunds-kritiske it-systemer ikke er sikret et tilfredsstillende it-beredskab".

For tre navngivne enheder er der en (relativ) rosende omtale; Indenrigs- og Sundhedsministeriet; Erhvervsstyrelsen og Søfartsstyrelsen.

Med den information der findes i beretningen, bl.a. om de anvendte undersøgelsesspørgsmål og den beskrevne metode, finder jeg beretningens konklusioner fuldt ud underbyggede

5. Er beretningens konklusioner balancerede?

Emnet for beretningen er meget vigtigt for samfundet; er samfundskritiske systemer sikret fornuftigt mod personer eller grupper med ondsindede hensigter.

I lighed med sidste år, hvor 13 udvalgte samfundskritiske it-systemer blev undersøgt, fremgår det at nogle detaljer er undladt af sikkerhedsmæssige grunde, især for 4 anonymiserede myndigheder. Jeg finder dog at dybden af analyse i år er markant bedre end sidste år. Der er også langt flere detaljer

end sidste år, uden at der på nogen måde røbes noget om hvem de anonymiserede myndigheder mon kunne være. Faktisk synes jeg anonymiseringen fungerer rigtig godt; som læser får man alle detaljerne, og dermed god indsigt i hvordan Rigsrevisionen er nået frem til de dragne konklusioner. Og samtidig røbes der intet der kan identificere de anonymiserede myndigheder, så ondsindede personer har intet at gå efter.

Alt i alt finder jeg beretningens konklusioner vel balancerede.

6. Hvad er den samlede vurdering af beretningen?

En rigtig god beretning, der især udmærker sig på to områder. Dels et meget omhyggeligt beskrevet metodeafsnit og et bilag 2 der omhyggeligt redegør for de anvendte revisionskriterier, og ikke mindst med kildeangivelse (kolonnen yderst til højre i bilag 2). Dels nogle fine analyse-kapitler, der indledes med en kort og præcis delkonklusion, for derefter at "tage læseren ved hånden", og med de valgte revisionskriterier (bilag 2) gennemgår analysen bid for bid, og hele tiden med referencer angivet hvor det er relevant.

Så alt i alt har jeg valgt at vurdere den faglige kvalitet af denne beretning til at være meget tilfredsstillende.

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*