FOLKETINGET
RIGSREVISIONEN

Evalueringer af Rigsrevisionens beretninger fra 2025 af professor Jan Pries-Heje

Januar 2026

Evaluator Jan Pries-Heje

Evaluering af beretning om Regionernes beskyttelse af sundhedsdata mod cyberangreb

Er undersøgelsen igangsat efter anmodning fra Statsrevisorerne?	Nej
Har fortrolige oplysninger haft betydning for beretningen?	Nej

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

Beretningen undersøger, om regionerne beskytter sundhedsdata på hospitalerne tilstrækkeligt mod cyberangreb. Truslen fra cyberkriminalitet vurderes som *meget høj*. Fokus er på regionernes arbejde med både at forhindre angreb og at begrænse skaderne, hvis et angreb lykkes. Analysen bygger på 15 vurderingskriterier hentet fra ISO 27001-standarden og Center for Cybersikkerheds anbefalinger.

Beretningen konkluderer, at beskyttelsen samlet set "ikke er helt tilfredsstillende". Regionerne har gjort en indsats for at forhindre adgang udefra, men ikke nok for at forhindre, at angreb spreder sig internt. Det kan i værste fald føre til driftsstop på hospitaler og utilgængelige patientdata.

Beretningens emne og formål er klart motiveret af den stigende cybertrussel mod sundhedssektoren, hvor både kriminelle og fremmede stater udgør en risiko. Sundhedsdata er særligt attraktive, fordi de er følsomme og kan bruges til afpresning eller spionage. Samtidig er sundhedsvæsenet stærkt digitaliseret, hvilket er godt for effektiviteten, men øger sårbarheden.

Beretningen er afgrænset til regionernes arbejde med at beskytte sundhedsdata i hospitalsvæsenet og omfatter ikke primærsektoren, fx praktiserende læger. Fokus er på netværk og IT-systemer, som regionerne selv vurderer som kritiske for hospitalsdriften. Særligt de elektroniske patientjournaler er prioriteret, fordi de er ret centrale for behandlingen af patienter. Der ses ikke på fysisk sikkerhed, såsom adgang til serverrum. Den foretagne afgrænsning vurderer jeg er relevant.

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

Beretningen opstiller 3 undersøgelsesspørgsmål:

1. Har regionerne et tilstrækkeligt grundlag for at beskytte sundhedsdata mod cyberangreb (overblik, sårbarhedsskanninger, risikovurderinger, politikker)?
2. Har regionerne iværksat tilstrækkelige tekniske tiltag til at beskytte sundhedsdata mod cyberangreb (ekstern og intern sikring af netværk og systemer)?
3. Har regionerne et beredskab til at håndtere konsekvenserne af cyber-angreb, der rammer de elektroniske patientjournaler?

Det er tydeligt for mig som evaluator, at de tre undersøgelsesspørgsmål tilsammen dækker hele sikkerhedskæden: forudsætninger (styring og risikogrundlag), forebyggelse (konkrete tekniske kontroller) og robusthed, når skaden sker (beredskab og backup). Samtidig er spørgsmålene eksplicit knyttet til formålet om at vurdere, "om regionerne i tilstrækkeligt omfang beskytter sundhedsdata i hospitalsvæsenet mod cyberangreb".

Ydermere er de opstillede spørgsmål afledt af både ISO 27001 og Center for Cybersikkerheds anbefalinger, hvilket styrker deres relevans og faglige legitimitet.

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

Beretningen anvender primært en historisk-dokumentarisk undersøgelsesmetode, hvor man indhenter og gennemgår (reviderer) en række dokumenter. Konkret er der tale om en systematisk gennemgang af regionernes planer, retningslinjer og politikker, herunder risikovurderinger, it-beredskabsplaner, politikker for it-sikkerhed, passwords og backup. Derudover gennemgås rapporter over status for sikkerhedsopdateringer.

Revisionen er struktureret omkring 15 vurderingskriterier, der kommer fra ISO 27001 og Center for Cybersikkerheds vejledning "*Cyberforsvar der virker"*. Desuden anvendes ISO 27002 til at uddybe og detaljere nogle af de mere overordnede punkter i ISO 27001.

Bilag 1 til beretningen indeholder en meget fin metodebeskrivelse, hvor man også i detaljer kan se hver af de 15 punkter. Det fremgår endvidere, at der udover dokumentgennemgang har været holdt møder med regionernes it-afdelinger for at få uddybet materiale og anvendelsespraksis. På disse møder er regionerne blevet bedt om "at demonstrere udvalgte tekniske tiltag i praksis på møderne, herunder implementeringen af sikre passwords, multifaktorlogin og ændringer i firewallregler".

Til præsentation af resultater anvendes en simpel trafiklys-skala med rød, gul og grøn. Denne præsentation er let at forstå og formidle, men det fremgår ikke præcist hvad der skal til for at opnå gul frem for rød. Jeg har tidligere kritiseret (i evalueringen af rapporter fra de foregående år), at det er en meget grov skala, og har foreslået at man forholder sig mere kritisk til både skalaen og punkterne. Dette synes at være endnu mere relevant i år, hvor der nærmest pågår et 'våbenkapløb' mellem de 'gode' og de 'onde' med brug af Generativ AI til cyberkriminalitet. Men da alle punkterne, der måles på, er fra før Generativ AI fik sin opblomstring, så synes jeg det havde været på sin plads at forholde sig mere kritisk.

Der ligger også en begrænsning i, at Rigsrevisionen ikke foretager egne tekniske tests ud over regionernes egen dokumentation, og at fokus er afgrænset til udvalgte områder. Af bilag 1 fremgår f.eks. at man har undladt 5 områder, og man giver kun en forklaring på hvorfor det giver mening at undlade det ene område. Men der er ikke en god forklaring på, at f.eks. "fjernadgang til it-systemer", ikke undersøges. Det kunne ellers være særdeles relevant efter som sundhedssektoren mange steder eksperimenterer med indlæggelse og patient i eget hjem, hvilket kræver omfattende fjernadgang.

Min konklusion er, at metoderne der er anvendt, fremstår som passende og vel anvendt, med enkelte mangler.

4. Er beretningens resultater og konklusioner tilstrækkeligt underbygget?

Rigsrevisionen konkluderer i beretningen, at regionernes beskyttelse af sundhedsdata samlet set "ikke er helt tilfredsstillende". Alle regioner har politikker og foretager sårbarhedsskanninger, men flere mangler ledelsesmæssig opfølgning og systematiske risikovurderinger. Især Region Hovedstaden kommer ud med 'røde' mangler.

Ekstern netværkssikkerhed er generelt bedre end den interne, hvor manglende segmentering, utilstrækkelige sikkerhedsopdateringer og svagheder i udstyr udgør væsentlige risici. Region Hovedstaden anvender fx ikke multifaktorlogin på netværksudstyr, og har ikke segmenteret netværket.

Ja, beretningens resultater og konklusioner er tilstrækkeligt underbygget. Hvert resultat knyttes direkte til konkrete vurderingskriterier, som anvendes ensartet på alle regioner. Dokumentation, tabeller og regionale oversigter viser præcist, hvor kriterier er opfyldt, delvist opfyldt eller ikke opfyldt. Der er klar sammenhæng mellem de fremlagte fund (fx manglende segmentering og opdateringer) og konklusionen om utilstrækkelig beskyttelse. Brug af en internationale standarder ISO 27001 og 27002 styrker validiteten, ihukommende

min kritik oven for. Fraværet af uafhængige tekniske tests begrænser dog dybden på enkelte områder, men svækker efter min opfattelse ikke den samlede evidens væsentligt.

5. Er beretningens konklusioner balancerede?

Ja, beretningens konklusioner er balancerede. Rigsrevisionen anerkender, at regionerne har gjort reelle fremskridt og generelt har styr på den eksterne sikring. Samtidig lægges der tydelig vægt på de alvorlige mangler i intern sikring og beredskab, hvilket er sagligt begrundet i risikoen for driftsstop og datalæk.

Kritikken i beretningen er differentieret. Der skelnes mellem regioner og mellem typer af mangler. Beretningen fremstår med et nøgternt og klart teknisk sprog.

Med til at give balance er også, at det fremhæves at regionerne allerede har forbedret forholdene under undersøgelsen.

Samlet set synes jeg at beretningen giver et realistisk, men ikke over-alarmerende billede af situationen på beretningens område.

6. Hvad er den samlede vurdering af beretningen?

Beretningen fremstår samlet set som en solid og fagligt velfunderet undersøgelse af regionernes beskyttelse af sundhedsdata mod cyberangreb. Den er klart motiveret af en meget høj trusselsvurdering og den omfattende digitalisering af sundhedsvæsenet. Formål og tre undersøgelsesspørgsmål er tydeligt formuleret og dækker hele sikkerhedskæden: styringsgrundlag, konkrete tekniske tiltag og beredskab. Metoden er gennemsigtig, med 15 vurderingskriterier afledt af ISO 27001 og Center for Cybersikkerheds anbefalinger, og resultaterne formidles overskueligt i tabeller og figurer, som gør det let at se forskelle mellem regionerne.

En vigtig styrke ved beretningen er, at konklusionerne er balancerede: Rigsrevisionen anerkender både de fremskridt, regionerne har gjort, og peger klart og entydigt på de mest kritiske mangler, især manglende segmentering, utilstrækkelige opdateringer og svagheder i beredskabet.

Svaghederne ved beretningen er primært metodiske og afgrænsningsmæssige: den bygger i høj grad på dokumenter og regionernes egne oplysninger, uden egentlige uafhængige tekniske tests, og den ser kun på hospitalsområdet – ikke primærsektoren eller fysisk sikkerhed. Desuden er sproget i beretningen ret teknisk, hvilket kan gøre den tung for ikke-specialister, og der

diskuteres kun begrænset, hvad det vil kræve ressourcemæssigt at lukke de identificerede huller.

På trods af disse begrænsninger giver beretningen et klart og præcist billede af regionernes cybersikkerhed på et vigtigt område. Min samlede vurdering er derfor, at beretningen er på et tilfredsstillende niveau.

Vurdering af beretningens faglige kvalitet (sæt x)

Vurdering	**(x)**
Meget tilfredsstillende	
Tilfredsstillende	*X*
Mindre tilfredsstillende	

Evaluering af beretning om Tidsforbrug og økonomi i statslige bygge- og anlægsprojekter

Er undersøgelsen igangsat efter anmodning fra Statsrevisorerne?	Nej
Har fortrolige oplysninger haft betydning for beretningen?	Nej

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

Beretningen kortlægger tidsforbrug og økonomi i 120 statslige bygge- og anlægsprojekter på seks ministerområder, som skulle være afsluttet i årene 2018-2022. Beretningen viser, at omkring 60 % af projekterne ikke gennemføres som først planlagt; de bliver gennemsnitligt forsinket 2½ år, 20% har merforbrug, men der er også flere projekter med mindreforbrug.

Motivationen fremgår klart; Rigsrevisionen reagerer på et tilbagevendende problem med forsinkelser og fordyrelser i større statslige anlæg og vil skabe et samlet overblik, som hidtil ikke har eksisteret.

Beretningen lægger sig i forlængelse af både tidligere Rigsrevisionsberetninger og nyere tal fra Finansministeriet, der peger på udbredte problemer med tid og økonomi i statens projekter. Dertil kommer et samfundsmæssigt hensyn: Folketinget godkender projekter på grundlag af forventninger til pris og tid. Og når disse forventninger bliver skuffet, så kan Folketinget føle sig vildledt eller ført bag lyset.

Beretningen afgrænses til bygge- og anlægsprojekter under seks ministerområder. Kun projekter over et vist beløb, en såkaldt forelæggelsesgrænse, og projekter som ifølge første bevilling skulle være færdige i perioden 2018-2022, er medtaget.

Konkluderende mener jeg, at beretningen er både klart motiveret og velafgrænset.

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

Beretningen har det overordnet formål, at vurdere, om ministeriernes bygge- og anlægsprojekter gennemføres som først planlagt? Det konkretiseres i 2 undersøgelsesspørgsmål:

1. Om projekterne er blevet færdige til tiden.
2. Om projekterne er blevet færdige til prisen, dvs. inden for den oprindeligt angivne økonomiske ramme.

Det er tydeligt, hvorfor netop disse spørgsmål er valgt: de oversætter det overordnede formål til to enkle, målbare kriterier (tid og økonomi), som også er præcis de oplysninger, Folketinget godkender projekterne på baggrund af. Spørgsmålene er dermed velegnede til at belyse, om projekterne lever op til de forventninger, der oprindeligt er præsenteret for Folketinget.

I litteraturen om projekter har man i mange år diskuteret om offentlige projekter var udsat for ”strategic misrepresentation”, dvs. “the planned, systematic distortion or misstatement of fact—lying—in response to incentives in the budget process” (citeret fra side 437 I Jones & Euske (1991) "Strategic Misrepresentation in Budgeting." *Journal of Public Administration Research and Theory* (4):437-460). Men med den valgte afgrænsning, vil det desværre ikke være muligt at komme bag om tallene, og diskutere om vi har ”strategic misrepresentation” i en dansk kontekst.

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

Beretningen bygger primært på kvantitative dataanalyser kombineret med dokumentgennemgang. Man har til formålet opbygget et nyt datasæt med oplysninger om tid og økonomi for 120 projekter på tværs af 6 ministerområder. Data kommer fra ministerierne og fra aktstykker, finanslove, årsrapporter, statusrapportering m.v.

For hvert projekt sammenlignes det forventede afslutningstidspunkt og den oprindelige økonomiske ramme med det faktiske ibrugtagningstidspunkt og det faktiske forbrug. Et stort, fælles datasæt giver mulighed for et samlet, sammenligneligt overblik, som netop var et centralt formål med undersøgelsen. Sammenligningen mellem første bevilling og faktisk forløb rammer præcist den politiske problematik om Folketingets beslutningsgrundlag.

Danskeren Bent Flyvbjerg (Flyvbjerg et al. (2022), The Empirical Reality of IT Project Cost Overruns: Discovering A Power-Law Distribution. *Journal of Management Information Systems* 39 (3):607-639) har sammen med et team fra Oxford University opbygget en database af mega-projekter, og har leveret den hidtil mest omfattende undersøgelse af mere end 5000 store it-projekter. De fandt, at størstedelen af projekterne kun havde beskedne budget-

overskridelser, mens en mindre andel havde usædvanligt store overskridelser. Fordelingen har en ”fat tail”, hvilket indikerer, at sådanne ekstreme overskridelser forekommer hyppigere, end man ville forvente ud fra en normalfordeling. Dette svarer fint til, at beretningen på side 3 siger, at ” Merforbruget udgør i alt ca. 4,8 mia. kr., hvoraf byggeriet af Niels Bohr Bygningen står for mere end 75 % af det samlede merforbrug”. Så tallene i beretningen bekræfter Flyvbjergs observationer.

Ja, de valgte metoder er velvalgte i forhold til formålet, fordi spørgsmålene handler om målbare forhold: tid og penge. Metoden har dog også sin begrænsning, idet man ikke går ’bag om’ den fremlagte dokumentation eller går dybere ind i årsager til forsinkelser.

4. Er beretningens resultater og konklusioner tilstrækkeligt underbygget?

Beretningen viser, at kun ca. 40 % af de 120 projekter er blevet færdige til tiden, mens ca. 60 % er forsinkede, gennemsnitligt med 2½ år. Kun 46 projekter er både færdige til tiden og inden for den økonomiske ramme, mens 19 stadig ikke er afsluttede. Ca. 20 % af projekterne er afsluttet med et merforbrug på mindst 10 % i forhold til den oprindelige økonomiske ramme, i alt ca. 4,8 mia. kr. i samlet merforbrug. Interessant nok er 40 % af de undersøgte projekter afsluttet med et mindreforbrug, samlet ca. 8 mia. kr. I disse projekter har man altså været for forsigtige og lagt for meget luft ind i estimatet. I relation til forskningsresultater fra andre lande, bl.a. ovenfornævnte Flyvbjerg, er 40% med mindreforbrug et usædvanligt stort tal

Der ses en tydelig sammenhæng mellem merforbrug og forsinkelser, samt mellem forsinkelser og projekter, hvor indholdet er ændret undervejs. Så når kravene ændrer sig så opstår overskridelser. Det er derfor der mange steder gøres forsøg med mere agil udvikling, bl.a. i Skat og STAR (Styrelsen for Arbejdsmarked og Rekruttering).

Beretningen finder ikke en entydig sammenhæng mellem entrepriseformen (udbud, tilbud, kontrakt), og om projekterne bliver færdige til tiden og inden for rammen. Det er ret interessant idet mange har angrebet entrepriseformen for at være skyld i forsinkelser og overskridelser. Men den sammenhæng findes ikke her.

Resultaterne bygger på et relativt omfattende datasæt med 120 projekter på tværs af seks ministerområder og en samlet ramme på ca. 91 mia. kr. Data stammer både fra ministeriernes egne indberetninger og fra aktstykker, finanslove, årsrapporter og Transportministeriets opgørelser. Den anvendte

metode er gennemsigtig, og der er gennemført flere runder kvalitetssikring og dialog med ministerierne om datasættet.

Den kvantitative metode, konsekvent anvendt, samt kvalitetssikringen i form af den nævnte dialog gør, at jeg finder det klart, at beretningens resultater og konklusioner er tilstrækkeligt underbygget.

5. Er beretningens konklusioner balancerede?

Ja, jeg finder at beretningens konklusioner er balancerede.

Beretningen fremhæver både problemerne med forsinkelser og merforbrug og det forhold, at en betydelig del af projekterne faktisk afsluttes til tiden og/eller med mindreforbrug. Der vises forskelle mellem ministerier og projektgrupper, uden at enkelte aktører hænges ud mere end tallene tilsiger.

Beretningen understreger, at projekterne er forskellige i størrelse, formål og rammevilkår, samt at der ikke er fælles regler for planlægning og gennemførelse, som der f.eks. er på it-området med statens it-projektmodel.

Beretningens anbefalinger rettes primært til Finansministeriet og beslutningsgrundlaget til Folketinget, og fremstår ikke som direkte kritik af enkeltprojekter.

Den eneste ubalance jeg synes man kan fremhæve er, at beretningen fokuserer ensidigt på tid og økonomi, så hele det centrale spørgsmål om den ønskede effekt eller gevinst opnås, ligger ubelyst hen. Endvidere, som også nævnt oven for, kommer vi ikke i dybden med årsagerne til hverken forsinkelser eller budget-overskridelser.

6. Hvad er den samlede vurdering af beretningen?

Jeg synes det er en rigtig god beretning. Af stærke sider kan nævnes: (1) At den har et meget klart formål og nogle enkle, præcise undersøgelsesspørgsmål om tid og økonomi. (2) At den bygger på et relativt stort og systematisk opbygget datasæt, som muliggør et samlet overblik på tværs af ministerområder. (3) Meget fine grafiske fremstillinger hele vejen igennem. (4) Resultaterne kobles tydeligt til det politiske beslutningsgrundlag og munder ud i en konkret, realistisk anbefaling til Finansministeriet.

Beretningen har også nogle svage sider. Jeg har flere gange nævnt et meget snævert fokus på tid og økonomi, så aspekter som kvalitet og gevinstrealisering stort set ikke belyses. Årsager til forsinkelser og overskridelser

behandles kun overfladisk analyseres ikke systematisk. Beretningen, og den til grundliggende database, er helt og fuldt afhængig af ministeriernes registreringer og de projekter, der opfylder bestemte beløbs- og tidskriterier, hvilket begrænser generaliserbarheden.

Samlet vurderet er beretningen efter min opfattelse på niveauet meget tilfredsstillende.

Vurdering af beretningens faglige kvalitet (sæt x)

Vurdering	**(x)**
Meget tilfredsstillende	*X*
Tilfredsstillende	
Mindre tilfredsstillende	

Evaluering af beretning om Forsvarsministeriets beskyttelse af oplysninger om våben

Er undersøgelsen igangsat efter anmodning fra Statsrevisorerne?	Nej
Har fortrolige oplysninger haft betydning for beretningen?	Ja

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

Beretningen undersøger, om Forsvarsministeriet har beskyttet oplysninger om våben og ammunition tilstrækkeligt i ministeriets to it-systemer, kaldet system A og system B. Fokus er på, hvem der har adgang til oplysninger om våben, og om adgangen er begrundet i et reelt arbejdsmæssigt behov.

Motivationen for beretningen er tydelig, fordi oplysninger om våben anses som særligt følsomme og sikkerhedskritiske. Beretningen knytter problemet til den aktuelle sikkerhedssituation, hvor især trusler fra fremmede magter fremhæves. Der peges på, at ansatte kan udgøre en sikkerhedsrisiko, hvis tilladelse til adgang ikke gives og kontrolleres korrekt. Desuden peger undersøgelsen på tidligere sager om læk og våben, der er endt i kriminelle miljøer. Samlet giver dette en klar og relevant motivation for at gennemføre undersøgelsen.

Undersøgelsen er afgrænset til de dele af Forsvarsministeriets it-systemer, der indeholder oplysninger om våben. Anonymiseret til at blive kaldt system A og system B. Der ses udelukkende på interne adgangsforhold, ikke på forsvar mod eksterne hackerangreb, og generel cybersikkerhed er heller ikke medtaget. Der er ikke nogen god argumentation for afgrænsningen. At der er en grænseflade til en anden beretning er dog en god grænseflade-afgrænsning.

Beretningen understreger, at dele af grundlaget er hemmeligholdt af sikkerhedshensyn, hvilket har nuanceret mine forventninger som læser. Jeg synes dog ikke det virker specielt hæmmende, som det har gjort i tidligere rapporter, jeg har læst (de foregående år); man har fundet en god balance.

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

Formålet med beretningen er at vurdere, om Forsvarsministeriet har sikret en tilstrækkelig beskyttelse af ansattes adgang til oplysninger om våben i ministeriets it-systemer. Dette konkretiseres i praksis i tre undersøgelsesområder, der fungerer som undersøgelsesspørgsmål:

1) Om adgangen til oplysninger om våben er styret efter de ansattes arbejdsmæssige behov (adgangsstyring),
2) Om ministeriet logger og følger tilstrækkeligt med i, hvem der slår våbenoplysninger op (logning og overvågning), og
3) Om selve registreringerne af våbenoplysninger er tilstrækkeligt beskyttet, korrekte og ajourførte (kvalitet, integritet og teknisk sikring).

Det er forholdsvis tydeligt, hvorfor disse tre undersøgelsesspørgsmål er egnede til at belyse formålet: De dækker hele den logiske kæde fra *hvem* der kan se oplysningerne, over *hvordan* deres brug kan opdages, til *om* oplysningerne i systemerne er pålidelige og beskyttede.

Samtidig er de direkte forankret i ISO 27001 og Forsvarsministeriets egne sikkerhedsbestemmelser, som er brugt til at svare på de tre spørgsmål. Så, ja, det er tydeligt hvorfor disse spørgsmål er velegnede til at belyse formålet.

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

Beretningen anvender som udforsknings-metoder primært dokumentgennemgang og møder med udvalgte medarbejdere i Forsvarsministeriet og Forsvarsministeriets Materiel- og Indkøbsstyrelse. Det er uklart hvem man har mødtes med og hvordan disse respondenter er valgt, men det fremgår at indholdet af møderne har handlet om 19 vurderingskriterier baseret på bl.a. ISO 27001. Som læser savner jeg en overvejelse om forskellige roller og en præcisering af hvilke roller man har talt med. Har man f.eks. talt med systembrugere 'ude i marken'?

Af dokumenter er der set på vejledninger, beskrivelser af brugerroller, oversigter over brugerkonti og log-politikker, og disse er analyseret. Der er ingen beskrivelse af hvordan analysen er foregået.

Metodisk er også demonstrationer af og udtræk fra de to it-systemer (system A og B) omfattet. F.eks. har man udtrukket lister over oprettede brugere og deres rettigheder. Formålet med disse udtræk har været at efterprøve, om praksis i systemerne faktisk svarer til det, der er beskrevet; en klassisk revisionsmetode.

Fra ISO 27001, suppleret med ministeriets egne regler, er der udledt 19 vurderingskriterier. Hvert kriterium er herefter vurderet som opfyldt, delvist opfyldt eller ikke opfyldt for hvert system, anvendende en trafiklys-metafor med grøn, gul og rød. Vurderingen sammenfattes i figur 1. Der gives ingen detaljer om hvordan man er nået frem til scoringen, og om der har været grænsetilfælde mellem f.eks. grøn og gul.

Metoderne der er valgt er grundlæggende velegnede til formålet, fordi de direkte tester, om ministeriet efterlever de krav, der netop definerer "tilstrækkelig beskyttelse" af oplysninger om våben. Kombinationen af dokumentgennemgang og konkrete systemudtræk giver både indblik i de formelle regler og i den faktiske praksis i it-systemerne.

En klar svaghed er, at metoden næsten udelukkende er normativ, og ikke bygger på fx interviews med bredere brugergrupper eller risikovurderinger. Metode-bilaget (bilag 1) er også meget kortfattet. Der savnes simpelthen flere detaljer, for at man som læser kan vurdere kvaliteten af beretningen.

4. Er beretningens resultater og konklusioner tilstrækkeligt underbygget?

Beretningen konkluderer, at beskyttelsen af ansattes adgang til oplysninger om våben er meget utilfredsstillende.

Man har givet mange ansatte adgang til detaljerede oplysninger om våben uden at vurdere deres arbejdsmæssige behov. Der gennemføres ikke regelmæssige gennemgange af, om adgange fortsat er nødvendige, eller om de i praksis giver mere indsigt end man har besluttet at den pågældende skal have. Ministeriet logger ikke systematisk, hvilke våbenoplysninger der søges på, og følger ikke tilstrækkeligt med i brugen af systemerne.

Til gengæld er kvaliteten af registreringer om våben og beskyttelsen mod uautoriseret ændring og sletning i de undersøgte systemer A og B overordnet tilfredsstillende.

Resultater og konklusioner er underbygget dels af de 19 vurderingskriterier udledt af ISO 27001, dels af ministeriets egne sikkerhedsbestemmelser. Metodisk er der anvendt dokumentgennemgang, systemdemonstration og møder. Jeg savner indsigt i hvordan analysen er foregået, og hvem man har mødtes med. Jeg savner også at man går tættere på de to systemer A og B og vurderer deres "affordance", altså hvilken anvendelse systemerne inviterer eller lægger op til. Så alt i alt synes jeg ikke resultater og konklusioner er helt tilstrækkeligt underbygget.

5. Er beretningens konklusioner balancerede?

Beretningen er kritisk, og bygger sin kritik på konkrete afvigelser fra etablerede standarder og ministeriets egne krav.

Beretningen fremstår balanceret på den måde at forstå, at den ikke kun fremhæver svagheder, men også styrker, så som kvalitetssikring af våbenregistreringer og beskyttelse mod uautoriseret ændring.

Som en del af kvalitetssikringen har man indhentet kommentarer fra ministeriet. Der redegøres loyalt for ministeriets synspunkter, fx om sikkerhedsgodkendelse af ansatte og sammenhængen til den fysiske beskyttelse af militære områder. Beretningen afviser dog eksplicit, at dette kan erstatte kravet om at vurdere arbejdsmæssigt behov for adgang, så her synes der at være en konstateret saglig uenighed.

Samlet set fremstår konklusionerne balancerede i forhold til materialet, de anvendte metoder og afgrænsningen.

6. Hvad er den samlede vurdering af beretningen?

Min samlede vurdering er, at beretningen opfylder sit formål, men at den er lidt snævert fokuseret.

Af stærke sider vil jeg fremhæve, at beretningen har et meget klart og sikkerhedspolitisk relevant fokus: ansattes adgang til følsomme våbenoplysninger i to af Forsvarsministeriets it-systemer A og B. Den tager udgangspunkt i et tydeligt formål og konkrete vurderingskriterier, forankret i både ISO 27001 og ministeriets egne bestemmelser. Metoderne der er anvendt, er gennemskuelige, og resultatet sammenfattes overskueligt i tabel og figur.

Af svage sider kan nævnes metodeanvendelsen, der er ret fokuseret på 'blot' at tage nogle vurderingskriterier fra ISO 27001, uden at forholde sig kritisk til dem, og blot at mødes med nogle få – ikke alle – nøgleinteressenter. Fokus er forholdsvis snævert på to systemer og kun på udvalgte aspekter af informationssikkerhed, hvilket begrænser, hvor langt man kan generalisere konklusionerne. Endelig er beretningen meget norm- og regelbaseret og mindre optaget af en egentlig risikovurdering eller konsekvensanalyse.
På trods af disse begrænsninger fremstår beretningen samlet set fagligt solid, klart formidlet og brugbar for både Folketing og ministerium – jeg vil derfor vurdere den som på niveauet tilfredsstillende.

Vurdering af beretningens faglige kvalitet (sæt x)

Vurdering	(x)
Meget tilfredsstillende	
Tilfredsstillende	*X*
Mindre tilfredsstillende	

Evaluering af beretning om Forsvarsministeriets beskyttelse af militære områder

Er undersøgelsen igangsat efter anmodning fra Statsrevisorerne?	Nej
Har fortrolige oplysninger haft betydning for beretningen?	Ja

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

Formålet med beretningen er at undersøge, om Forsvarsministeriet har sikret en tilstrækkelig beskyttelse af Danmarks militære områder mod spionage, sabotage, indbrud og tyveri.

Beretningen er klart motiveret af et ændret og forværret trusselsbillede mod Danmark, som Forsvarets Efterretningstjeneste (FE) har dokumenteret. Truslen er blevet mere alvorlig, og ministeriet har selv erkendt behovet for bedre beskyttelse

Undersøgelsen er afgrænset til perioden 2020-2024, hvor trusselsniveauet ifølge FE netop er steget markant. Fokus er afgrænset til fysiske militære områder og omfatter de tre centrale sikringstiltag: mekanisk sikring, elektronisk overvågning og menneskelig bevogtning.

Rigsrevisionen har ikke vurderet konkrete hændelser som spionage eller tyveri, på militære områder. Dette kunne ellers have givet input til en bedre risikoanalyse. Man afgrænser sig til alene at se på beskyttelsesniveauet.

Ja, formålet er klart motiveret, mens afgrænsningen virker lidt snæver.

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

Beretningens formål er at vurdere, om Forsvarsministeriet har sikret en tilstrækkelig beskyttelse af militære områder mod spionage, sabotage, indbrud og tyveri. Det brydes i praksis ned til tre undersøgelsesområder, som fungerer som undersøgelsesspørgsmål:

1. Hvordan er den samlede sikkerhedstilstand vurderet af FE over tid (2020-2024)?

2. Hvordan vurderer de enkelte myndigheder selv sikkerheden på deres områder, og hvilke typer mangler peger de på?
3. Hvordan arbejdes der med at udbedre de konstaterede mangler, og er der tilstrækkelig fremdrift og overblik?

Ja, det er tydeligt, hvorfor disse undersøgelsesspørgsmål er egnede til at belyse formålet.

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

Ja, Samlet set er de valgte metoder velegnede til at besvare undersøgelsesspørgsmålene.

Metodisk anvender beretningen dokumentgennemgang af materiale fra ministeriet, FE, Forsvarskommandoen og Etablissement- og Terrænkommandoen (ETK). Derudover indhentes dataudtræk fra ETK om status for de projekter, der skal udbedre mangler i sikkerheden. På baggrund heraf sammenligner Rigsrevisionen FE's samlede vurderinger med myndighedernes egne vurderinger over perioden 2020-2024 og med den faktiske udbedring af mangler. Metodisk anvendes endvidere møder med de berørte parter for at få uddybet ansvar, organisering og ministeriets eget overblik over sikkerheden. Endelig har man været ude at se udvalgte militære områder for at få indblik i, hvordan sikkerhedsforanstaltninger og tilsyn ser ud i praksis.

Metoderne passer grundlæggende godt til formålet, fordi de direkte tager udgangspunkt i Forsvarsministeriets egne mindstekrav og i FE's systematiske tilsyn med sikkerheden. Dokumentgennemgangen af årsrapporter, tilsyn og årsoversigter gør det muligt at følge udviklingen i sikkerhedsniveauet over tid og på tværs af myndigheder. Data fra ETK om sikringsprojekter giver et konkret grundlag for at vurdere, om kendte mangler faktisk bliver udbedret – og hvor der mangler fremdrift. Møder og besigtigelser fungerer som kvalificerende baggrund, selv om de ikke kan betragtes som repræsentative.

En svaghed er, at der ikke indgår mere dybtgående case-studier af enkeltsager eller egentlige risikovurderinger.

4. Er beretningens resultater og konklusioner tilstrækkeligt underbygget?

Ja, inden for den valgte afgrænsning fremstår konklusionerne tilstrækkeligt underbygget.

Beretningen viser, at Forsvarsministeriets beskyttelse af militære områder samlet set er kritisabel og ikke lever op til ministeriets egne sikkerhedskrav. FE har i alle år 2020-2024 vurderet sikkerheden som ”ikke tilfredsstillende”, hvilket er den dårligste kategori og indebærer krav om snarlige forbedringer. Myndighedernes egne vurderinger bekræfter dette billede; 15 ud af 18 myndigheder vurderer i 2024 deres sikkerhed som enten ”ikke tilfredsstillende” eller ”ikke helt tilfredsstillende”. Beretningen konkluderer, at sikkerheden er blevet forværret i perioden, og at Forsvarsministeriet ikke har haft tilstrækkelig fremdrift i at udbedre kendte mangler, som ofte går igen år efter år.

Som læser undrer jeg mig over, hvorfor der ikke gøres noget? Vi får kun fortalt om symptomerne og kommer aldrig ’bag om’ så vi forstår hvorfor der intet sker? I japansk kvalitets-tænkning taler man om ”five times why”, altså at man til ethvert symptom skal spørge ’hvorfor’ fem gange for at komme bagom symptomet. Det savner jeg at man gør i denne beretning.

Beretningens resultater baserer sig på FE’s årsrapporter, myndighedernes egne årsoversigter og tilsyn samt dataudtræk fra ETK om sikringsprojekter og deres fremdrift. Disse kilder giver et konsistent og flerstrenget billede af sikkerhedstilstanden. Beretningen gennemgår hele perioden 2020-2024 og kan dermed dokumentere udviklingen over tid, herunder at sikkerheden samlet set er forværret.

5. Er beretningens konklusioner balancerede?

Konklusionerne er tydeligt kritiske, men de knyttes hele tiden til konkrete krav fra f.eks. ministeriet selv. Beretningen giver plads til Forsvarsministeriets perspektiv, bl.a. ved at redegøre for ressourcemæssige begrænsninger, og ved at notere sig at der er nedsat en styregruppe til at forbedre sikkerheden. Samtidig fastholder beretningen, at kendte kritiske mangler bør udbedres straks, hvilket er en skarp, men sagligt begrundet forventning.

Myndigheder anonymiseres, og konkrete detaljer udelades af hensyn til sikkerheden. Det synes jeg er ok, da jeg ikke ved læsningen har haft brug for de anonymiserede detaljer.

Hvis man skal sige noget om balancen, så er den overvejende negativ. Mulige forbedringer eller gode eksempler belyses ikke, hvilket giver en overvejende negativ tone. Der argumenteres dog for, at den kritiske vurdering bygger på flere års gentagne konstateringer af de samme problemer.

Alt i alt er beretningens konklusioner samlet set balancerede, givet formål og afgrænsning.

6. Hvad er den samlede vurdering af beretningen?

Beretningens største styrke er, at den tager fat i et helt centralt sikkerhedspolitisk emne; den fysiske beskyttelse af militære områder i en periode med markant øget trussel. Den har et meget klart formål og en entydig konklusion. Sammenstillingen af FE's vurderinger og myndighedernes egne vurderinger er særlig stærk, fordi den viser, at problemerne er både kendte og vedvarende, men at der intet er sket.

Beretningen er balanceret, idet den gengiver ministeriets egne initiativer (f.eks. styregruppe) og forklarer de økonomiske og praktiske begrænsninger, samtidig med at den fastholder, at kritiske mangler bør udbedres straks.

Beretningens mest åbenlyse svaghed er, at fokus er snævert på tre sikringstiltag og ikke inddrager en bredere risikovurdering eller konkrete hændelsesforløb. Der gives også meget få positive eksempler på velfungerende områder, så der er ikke meget læring at hente om hvordan man kan gøre. Endelig kommer man ikke 'bag om' symptomerne, så man får ingen forståelse af hvorfor ting er sket og hvorfor det blot bliver værre og værre?

På trods af disse begrænsninger fremstår beretningen samlet set fagligt solid, metodisk velstruktureret og med klare brugbare konklusioner for ministeriet og Statsrevisorerne/Folketinget – jeg vil derfor vurdere den som på niveauet tilfredsstillende.

Vurdering af beretningens faglige kvalitet (sæt x)

Vurdering	**(x)**
Meget tilfredsstillende	
Tilfredsstillende	*X*
Mindre tilfredsstillende	