FOLKETINGET
RIGSREVISIONEN

Maj 2022

Rigsrevisionens notat om
beretning om

universiteternes beskyttelse af forskningsdata

Opfølgning i sagen om universiteternes beskyttelse af forskningsdata (beretning nr. 8/2018)

3. maj 2022

RN 1407/22

1. Rigsrevisionen følger i dette notat op på sagen om universiteternes beskyttelse af forskningsdata, som blev indledt med en beretning i 2019. Vi har tidligere behandlet sagen i notat til Statsrevisorerne af 11. april 2019.

Konklusion

Uddannelses- og Forskningsministeriet, Aalborg Universitet, Aarhus Universitet, Danmarks Tekniske Universitet, Syddansk Universitet og Københavns Universitet har siden Rigsrevisionens beretning fra 2019 arbejdet med initiativer for at forbedre beskyttelsen af forskningsdata. Rigsrevisionen har gennemgået initiativerne og vurderer, at dele af sagen kan afsluttes. Det drejer sig om Uddannelses- og Forskningsministeriets arbejde med at inddrage universiteternes implementering af ISO 27001 i det systematiske tilsyn og ministeriets arbejde med at etablere en tværgående trusselsvurdering for universiteterne samt universiteternes identificering af kritiske it-sikkerhedsbrister.

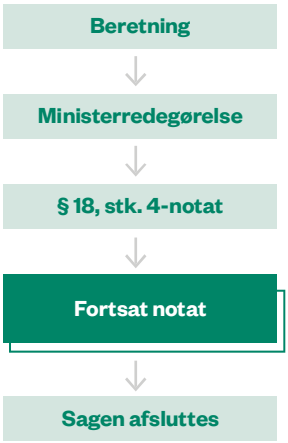
Rigsrevisionen baserer denne konklusion på følgende:

- Uddannelses- og Forskningsministeriet har inddraget universiteternes implementering af ISO 27001 i ministeriets systematiske tilsyn med universiteterne.
- Uddannelses- og Forskningsministeriet har sikret, at universiteterne har etableret en tværgående trusselsvurdering.
- Universiteterne har identificeret kritiske it-sikkerhedsbrister.

Rigsrevisionen konstaterer på baggrund af skriftlige redegørelser fra universiteterne, at de 5 universiteter har iværksat en række tiltag, men at ikke alle universiteter endnu er i mål med at reducere risikoen for, at forskningsdata ikke beskyttes i tilstrækkelig grad.

Uddannelses- og Forskningsministeriets bestræbelser har således endnu ikke ført til, at alle universiteterne har rettet op på kritiske it-sikkerhedsbrister. Henset til universiteternes høje trusselsniveau finder Rigsrevisionen, at tempoet for arbejdet med at rette op på kritiske it-sikkerhedsbrister ikke har været tilfredsstillende.

Sagsforløb for en større undersøgelse



Du kan læse mere om forløbet og de enkelte step på www.rigsrevisionen.dk

Forkortelser af afdelinger og institutter og under Københavns Universitet

I notatet anvendes følgende forkortelser om afdelinger og institutter under Københavns Universitet:

Københavns Universitets centrale it-afdeling: KU-IT
Institut for Nordiske Studier og Sprogvidenskab: NORS
Biomedicinsk Institut: BMI
Niels Bohr Instituttet: NBI.

Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om:

- resultatet af Uddannelses- og Forskningsministeriets bestræbelser i forhold til, at universiteterne får rettet op på kritiske it-sikkerhedsbrister, der medfører, at forskningsdata ikke beskyttes i tilstrækkelig grad.

Ovenstående opfølgningspunkt vil bl.a. blive baseret på it-revision hos hver af de 5 universiteter. It-revisionen forventes udført af Rigsrevisionen i 2023.

I. Baggrund

Forkortelser
I notatet anvendes følgende forkortelser om universiteterne:

Københavns Universitet: KU
Aalborg Universitet: AAU
Aarhus Universitet: AU
Danmarks Tekniske Universitet: DTU
Syddansk Universitet: SDU.

2. Rigsrevisionen afgav i januar 2019 en beretning om universiteternes beskyttelse af forskningsdata. Beretningen handlede om universiteternes beskyttelse af forskningsdata på Uddannelses- og Forskningsministeriets område. I beretningen kortlagde Rigsrevisionen de 5 største danske universiteters (KU, AAU, AU, DTU og SDU) risikoprofil i forhold til beskyttelse af forskningsdata mod ukendt it-udstyr. Dernæst gik beretningen i dybden med at undersøge, hvordan det største universitets, KU's, centrale it-afdeling og 3 udvalgte institutter arbejdede med it-sikkerheden i forhold til beskyttelse af forskningsdata.

3. Da Statsrevisorerne behandlede beretningen, fandt de det utilfredsstillende, at de 5 største universiteter i Danmark ikke beskyttede forskningsdata i tilstrækkelig grad, fx mod ukendt it-udstyr.

4. På baggrund af beretningen og Statsrevisorernes bemærkninger har vi fulgt op på følgende punkter:

Et opfølgningspunkt afsluttes, når Statsrevisorerne på baggrund af indstilling fra Rigsrevisionen vurderer, at myndighedernes initiativer er tilfredsstillende.

Opfølgningspunkt	Status
1. Uddannelses- og Forskningsministeriets arbejde med at inddrage universiteternes implementering af ISO 27001 i det systematiske tilsyn.	Behandles i dette notat.
2. Uddannelses- og Forskningsministeriets arbejde med at etablere en tværgående trusselsvurdering for universiteterne.	Behandles i dette notat.
3. Resultatet af Uddannelses- og Forskningsministeriets bestræbelser i forhold til, at universiteterne får identificeret og rettet op på eventuelle kritiske it-sikkerhedsbrister.	Behandles i dette notat.

5. Vi redegør i dette notat for resultaterne af opfølgningen på ovenstående punkter samt opfølgningen på kortlægningen af de 5 største universiteters risikoprofil og de kontrolmål, der var afrapporteret som ikke opfyldt (røde) eller var delvist opfyldt (gule) hos KU i beretningen fra 2019

Hele sagen og dens dokumenter kan følges på www.rigsrevisionen.dk og på www.ft.dk/Statsrevisorerne.

II. Initiativer fra Uddannelses- og Forskningsministeriet, KU, AAU, AU, DTU og SDU

6. Vi gennemgår i det følgende initiativer fra Uddannelses- og Forskningsministeriet, KU, AAU, AU, DTU og SDU i forhold til opfølgningspunkterne. Gennemgangen af Uddannelses- og Forskningsministeriets initiativer og arbejde er baseret på brevveksling, indhentet dokumentation og dialog med ministeriet. Opfølgningen på kortlægningen hos AAU, AU, DTU og SDU er baseret på skriftlige redegørelser fra universiteterne. Opfølgningen på kortlægningen hos KU er baseret på Rigsrevisionens gennemførte it-revision samt på KU's skriftlige redegørelse.

Rigsrevisionens it-revision hos KU er foretaget hos KU-IT (den centrale it-afdeling på KU) og 3 udvalgte institutter BMI (Biomedicinsk Institut på Det Sundhedsvidenskabelige Fakultet), NORS (Institut for Nordiske Studier og Sprogvidenskab) på Det Humanistiske Fakultet) og NBI (Niels Bohr Instituttet på Det Natur- og Biovidenskabelige Fakultet). KU-IT leverer it-services til bl.a. NORS og BMI. NBI har sin egen it-afdeling og benytter derfor ikke KU-IT som leverandør af it-services. It-revisionen er baseret på stedlig revision og skriftlig dokumentation.

Uddannelses- og Forskningsministeriets arbejde med at inddrage universiteternes implementering af ISO 27001 i det systematiske tilsyn

7. Statsrevisorerne bemærkede, at der på Københavns Universitet var uklarhed om, hvorvidt ansvaret for at beskytte forskningsdata lå centralt hos universitetets ledelse, på institutterne eller hos den enkelte forsker. Statsrevisorerne bemærkede videre, at undersøgelsen indikerede, at opgaven med at beskytte forskningsdata heller ikke blev løst tilfredsstillende på centralt og decentralt niveau på de øvrige universiteter.

ISO 27001
ISO 27001 er en international informationssikkerhedsstandard til styring af it-sikkerheden. ISO 27001 opstiller bl.a. krav til risikostyring, dokumentation af processer samt fordeling af roller og ansvar for informationssikkerhed.

Det fremgik af beretningen, at ingen af de 5 undersøgte universiteter fra centralt hold sikrede, at forskningsdata blev beskyttet tilfredsstillende. Det fremgik videre af beretningen, at universiteterne som selvejende offentlige institutioner ikke er pålagt at følge ISO 27001, men at Københavns Universitet havde valgt at følge ISO 27001-standarden, men ikke havde udarbejdet en trusselsvurdering eller en risikovurdering, som ISO 27001 foreskriver. Uddannelses- og forskningsministeren oplyste i sin redegørelse af 18. marts 2019, at universiteterne skal håndtere og imødegå beskyttelse af forskningsdata med passende tiltag, fx med udgangspunkt i ISO 27001-standarden. På den baggrund oplyste ministeren i sin redegørelse, at ministeriet som led i det systematiske tilsyn ville bede hvert enkelt universitet om en status på implementering af ISO 27001-standarden.

8. Rigsrevisionens opfølgning viser, at Uddannelses- og Forskningsministeriet siden beretningens afgivelse har ført tilsyn med, om universiteterne har sikret implementering af ISO 27001-standarden. Ministeriet førte i 2019 første gang tilsyn med implementeringen af ISO 27001-standarden på universiteterne. Det skete via fremsendelse af mail til universiteterne med information om hensigtsmæssigheden ved at implementere standarden samt anmodning om skriftlig redegørelse og udsendelse af spørgeskema om status for implementering. Ministeriet gentog dette skriftlige tilsyn i 2021. Rigsrevisionen har set dokumentation for, at ministeriet aktivt har forholdt sig til universiteternes redegørelser fra 2019 og 2021 og har givet universiteterne tilbagemelding herpå.

Tilsynet fra 2019 viste, at universiteterne generelt havde politikker og procedurer, der understøttede implementering af ISO 27001. Dog havde enkelte universiteter ikke fået ledelsesgodkendt samtlige politikker og procedurer.

Tilsynet i 2021 viste igen, at universiteterne generelt havde sikret politikker og procedurer, der understøtter implementering af ISO 27001. Tilsynet viste ydermere, at politikkerne og procedurerne var ledelsesmæssigt forankret og havde ophæng i årshjul mv.

Ny national strategi for cyber- og informationssikkerhed
Regeringen har i december 2021 lanceret en ny national strategi for cyber- og informationssikkerhed for perioden 2022-2024. Strategien bygger videre på den forrige strategi for 2018-2021 og sigter efter at løfte den digitale sikkerhed på tværs af samfundet. Strategien skal øge den tekniske robusthed og sikre bedre beskyttelse af statens kritiske it-systemer, øge viden og kompetencer hos borgere, virksomheder og myndigheder samt styrke den nationale koordinering og samarbejdet om informationssikkerhed.

9. Uddannelses- og Forskningsministeriet har oplyst, at et tilsvarende tilsyn ikke vil blive gentaget i 2022. Det skyldes, at ministeriets fortsatte fokus på universiteternes arbejde med informationssikkerhed forankres i ministeriets videre arbejde med implementering af den nye nationale cyber- og informationssikkerhedsstrategi. Af strategien følger, at Uddannelses- og Forskningsministeriet skal formulere en sektorstrategi for ministerområdets samfundsvigtige funktioner, der i særlig grad er it-understøttet, og etablere en decentral cyber- og informationssikkerhedsenhed.

10. Rigsrevisionen finder på baggrund af ovenstående, at Uddannelses- og Forskningsministeriets har inddraget universiteternes implementering af ISO 27001 i det systematiske tilsyn tilfredsstillende. Rigsrevisionen finder det ligeledes tilfredsstillende, at ministeriets fokus på universiteternes arbejde med informationssikkerhed fremover forankres i ministeriets sektorstrategi for samfundsvigtige funktioner. Rigsrevisionen vurderer derfor, at denne del af sagen kan afsluttes.

Uddannelses- og Forskningsministeriets arbejde med at etablere en tværgående trusselsvurdering for universiteterne

11. Statsrevisorerne bemærkede, at Center for Cybersikkerhed fandt truslen fra cyberspionage mod de danske offentlige forskningsinstitutioner høj.

Uddannelses- og forskningsministeren oplyste i sin redegørelse af 18. marts 2019, at ministeriet havde aftalt med universiteterne at igangsætte en dialogproces, bl.a. med henblik på at etablere en opdateret tværgående trusselsvurdering for hele universitetssektoren og at aftale en kadence for opdatering.

12. Rigsrevisionens opfølgning viser, at Uddannelses- og Forskningsministeriet har sikret, at universiteterne i marts 2020 har etableret en tværgående trusselsvurdering, som blev opdateret i oktober 2021. Ministeriet oplyser, at trusselsvurderingen er baseret på den nationale trusselsvurdering af Center for Cybersikkerhed. Ligeledes har universiteterne inddraget internationale trusselsvurderinger, herunder inddraget USCERT (den amerikanske operative cybersikkerhedstjeneste) og erfaringer med konkrete sikkerhedshændelser på universiteterne. Ministeriet oplyser videre, at universiteterne i forbindelse med udarbejdelsen af trusselsvurderingen og en risikoanalyse har konsulteret Center for Cybersikkerhed, Sundhedsdatastyrelsen og DKCert (Danish Computer Security Incident Response Team), som overvåger sikkerheden på forskningsnettet.

Uddannelses- og Forskningsministeriet har i forbindelse med opfølgningen oplyst, at universiteterne fremover vil udarbejde en årlig status for ændringer i den tværgående trusselsvurdering samt sikkerhedsmæssige tiltag.

13. Rigsrevisionen finder det tilfredsstillende, at Uddannelses- og Forskningsministeriet har sikret, at universiteterne har etableret en tværgående trusselsvurdering. Rigsrevisionen vurderer på den baggrund, at denne del af sagen kan afsluttes.

Resultatet af Uddannelses- og Forskningsministeriets bestræbelser i forhold til, at universiteterne får identificeret og rettet op på eventuelle kritiske it-sikkerhedsbrister

14. I forbindelse med beretningen oplyste Uddannelses- og Forskningsministeriet, at ministeriet ville kontakte universiteterne og understrege ledelsernes ansvar for området og samtidig bede universiteterne om at identificere og rette op på eventuelle kritiske it-sikkerhedsbrister, hvilket Statsrevisorerne noterede sig i deres bemærkning til beretningen.

Universiteternes identificering af kritiske it-sikkerhedsbrister

15. Rigsrevisionens opfølgning viser, at Uddannelses- og Forskningsministeriet har sikret, at universiteterne har identificeret kritiske it-sikkerhedsbrister. Universiteternes identificering af kritiske it-sikkerhedsbrister er oplistet i forbindelse med universiteternes udarbejdelse af den tværgående trusselsvurdering og blev primo 2020 opsummeret i 6 kritiske brister: 1) lokaladministrator på universitetsejet udstyr, 2) ukendt udstyr på netværket, herunder privatejet udstyr, 3) anvendelse af ukendt eller ikke-opdateret software, 4) IT-Governance, 5) fysisk adgang til laboratorier, forskningskontorer m.m. og 6) brand, bomber, naturkatastrofer m.m.

16. Rigsrevisionen vurderer, at Uddannelses- og Forskningsministeriets og universiteternes arbejde med den del af opfølgningspunktet, der omhandler identificering af kritiske it-sikkerhedsbrister, er tilfredsstillende. Rigsrevisionen vurderer på den baggrund, at denne del af sagen kan afsluttes.

Universiteternes håndtering af kritiske it-sikkerhedsbrister

17. Uddannelses- og Forskningsministeriet har oplyst, at ud over, at universiteterne har identificeret kritiske it-sikkerhedsbrister, så arbejder universiteterne kontinuerligt med at forbedre deres sikkerhedsmæssige tiltag.

Uddannelses- og forskningsministeriet har videre oplyst, at universiteterne har adresseret de centrale kritikpunkter fra Rigsrevisionens beretning. Ligeledes har ministeriet oplyst, at samtlige universiteter fremhæver, at de har taget Rigsrevisionens kritik til efterretning og har foretaget eller iværksat forskellige foranstaltninger for at opnå bedre informationssikkerhed på universiteterne.

I det materiale, som Uddannelses- og Forskningsministeriet har fremsendt til Rigsrevision, fremgår det dog, at flere af universiteterne har oplyst til ministeriet, at de ikke har rettet op på samtlige af de identificerede it-sikkerhedsbrister. Fx har universiteterne oplyst til ministeriet, at de fastholder forskernes rettigheder som lokaladministratorer, og at det er en præmis, der udgør en risiko, som universiteterne tilkendegiver og accepterer. Universiteterne oplyser, at forklaringen er, at forskerne har behov for at anvende specifikke systemer til at udføre deres daglige arbejde ved brug af systemer, der ikke tilbydes som standardvare.

Ukendt udstyr

Ukendt udstyr er i dette notat en betegnelse for udstyr, der ikke bliver styret af den centrale ledelse eller it-afdeling på universitetet. Det er et bredt begreb, der både omfatter diverse udstyr, som forskerne selv medbringer, og forsknings- og laboratorieudstyr indkøbt via universitetet, og som er en forudsætning for, at forskerne kan bedrive deres forskning.

Der kan således være tale om forsknings- og laboratorieudstyr, som det enkelte institut kender til og har behov for, men hvor de fx ikke har et samlet, centralt overblik over udstyret og risikoen herved, herunder fx om det er muligt at opdatere udstyret, om udstyret er blevet opdateret, og om udstyret alternativt er afsondret med henblik på at reducere risikoen.

Opfølgning på kortlægning af de 5 største universiteters risikoprofiler
18. I Rigsrevisionens beretning fra 2019 blev der foretaget en kortlægning af de 5 største universiteters (KU, AAU, AU, DTU og SDU) risikoprofil i forhold til beskyttelse af forskningsdata.

Rigsrevisionen har i 2021-2022 fulgt op på kortlægningen fra beretningen. Opfølgningen på kortlægningen hos AAU, AU, DTU og SDU er baseret på skriftlige redegørelser fra universiteterne. Opfølgningen på kortlægningen hos KU er baseret på vores gennemførte it-revision samt KU's skriftlige redegørelse. Rigsrevisionen konstaterer på baggrund af de skriftlige redegørelser fra universiteterne, at de 5 universiteter har iværksat en række tiltag, men at ikke alle universiteter endnu er i mål med at reducere risikoen for, at forskningsdata ikke beskyttes i tilstrækkelig grad.

19. Rigsrevisionen vil fortsat følge de 5 største universiteters risikoprofiler. Rigsrevisionen forventer, at den fremtidige opfølgning vil blive baseret på it-revision hos hver af de 5 universiteter i 2023.

Opfølgning på Københavns Universitets beskyttelse af forskningsdata
20. Ud over kortlægningen af de 5 største universiteters risikoprofil i beretningen fra 2019 gik beretningen yderligere i dybden ved at undersøge, hvordan landets største universitets, KU's, centrale it-afdeling og 3 udvalgte institutter arbejdede med it-sikkerheden i forhold til beskyttelse af forskningsdata. Vi har fulgt op på de kontrolmål i beretningen, som ikke var opfyldt eller var delvist opfyldt. Vi har fulgt op ved at foretage særskilte it-revisioner hos KU-IT og hos de 3 udvalgte institutter BMI, NORS og NBI. Nedenstående tabel 1, 2, 3 og 4 viser – ligesom i beretningen – resultaterne for KU samlet. Dvs. at resultatet på de enkelte institutter ikke fremgår. Rigsrevisionens vurdering er baseret på, at alle 3 institutter samt KU-IT skal leve op til kontrolmål, før kontrolmålet kan siges at være opfyldt.

Ledelsesmæssig opmærksomhed på styring af it-udstyr på KU
21. Rigsrevisionen har fulgt op på KU's ledelsesmæssige opmærksomhed på styring af it-udstyr. Resultatet fremgår af tabel 1, der viser beretningens resultater fra 2018 sammenlignet med opfølgningen fra 2021-2022.

Tabel 1
Ledelsesmæssig opmærksomhed på styring af it-udstyr på KU i 2018 sammenlignet med 2021-2022

	2018	2021-2022
Universitetet har ledelsesgodkendt politik og retningslinjer for styring af it-udstyr (hardware og software).	●	●
Universitetet har vurderet trusler mod sin anvendelse af it og har dokumenteret trusselsvurderingen.	●	●
Universitetet har vurderet risici ved at anvende it i forskningen og har dokumenteret risikovurderingen.	●	●

Note: For hvert revisionskriterium har Rigsrevisionen vurderet, om KU har opfyldt kriteriet. Vurderingen er angivet med grøn (opfyldt), gul (delvist opfyldt) eller rød (ikke opfyldt).

Kilde: Rigsrevisionens beretning fra 2019 og Rigsrevisionens opfølgning fra 2021-2022.

Det fremgår af tabel 1, at KU i 2021-2022 har ledelsesgodkendte politikker og retningslinjer, der omhandler styring af it-udstyr. Rigsrevisionen vurderer, at politikkerne og retningslinjerne er i overensstemmelse med ISO 27001. Det fremgår videre af tabel 1, at KU kun delvist opfylder de 2 øvrige kontrolmål. Rigsrevisionen vurderer, at KU har vurderet trusler og risici ved at anvende it i forskningen og har dokumenteret en trussels- og risikovurdering. Rigsrevisionen vurderer dog, at der er mangler i de 3 institutters trusselsvurderinger i form af manglende vurdering af sandsynlighed og konsekvens samt manglende opstilling af mitigerende handlinger. Desuden indeholder institutternes trussels-/risikovurderinger ikke/ikke i tilstrækkelig grad en vurdering af truslen/risikoen ved Bring Your Own Device (BYOD).

Mitigerende handlinger
Handlinger, som har til formål at minimere sandsynligheden eller konsekvensen af risikoen.

Bring Your Own Device (BYOD)
Begrebet Bring Your Own Device, forkortet BYOD, dækker over diverse udstyr, som forskerne selv medbringer til universiteterne.

KU's beskyttelse af forskningsdata

22. Rigsrevisionen har fulgt op på, om KU sikrer, at data beskyttes i overensstemmelse med de ledelsesgodkendte politikker og retningslinjer. Resultatet fremgår af tabel 2, der viser beretningens resultater fra 2018 sammenlignet med opfølgningen fra 2021-2022.

Tabel 2
KU's beskyttelse af forskningsdata i 2018 sammenlignet med 2021-2022

	2018	2021-2022
Universitetet sikrer, at klassificerede forskningsdata beskyttes i henhold til de ledelsesgodkendte politikker og retningslinjer herfor.	●	●

Note: For hvert revisionskriterium har Rigsrevisionen vurderet, om KU har opfyldt kriteriet. Vurderingen er angivet med grøn (opfyldt), gul (delvist opfyldt) eller rød (ikke opfyldt).

Kilde: Rigsrevisionens beretning fra 2019 og Rigsrevisionens opfølgning fra 2021-2022.

Det fremgår af tabel 2, at KU delvist opfylder kontrolmålet om at sikre, at klassificerede forskningsdata beskyttes i henhold til de ledelsesgodkendte politikker og retningslinjer. Rigsrevisionens opfølgning viser, at KU har implementeret og er i gang med at implementere en række tekniske og organisatoriske tiltag, der skal sikre, at klassificerede forskningsdata beskyttes.

Vores opfølgning viser også, at de 3 institutter primært anvender en tillidsbaseret tilgang i forhold til de organisatoriske tiltag og ikke, fx via stikprøver, har undersøgt, om forskerne opbevarer data korrekt og sikkert. Rigsrevisionen finder, at det vil være hensigtsmæssigt, at de 3 institutter fremadrettet foretager stikprøvevis opfølgning. Dette gælder i særlig grad for NBI, da Rigsrevisionens opfølgning viser, at særligt NBI har udfordringer i forbindelse med at beskyttelse klassificerede forskningsdata i henhold til ledelsesgodkendte politikker og retningslinjer.

KU's fortegnelse over hardware

23. Rigsrevisionen har fulgt op på, om KU har fortegnelser over hardware. Resultatet fremgår af tabel 3, der viser beretningens resultater fra 2018 sammenlignet med opfølgningen fra 2021-2022.

Tabel 3

KU's overblik over anvendt hardware i 2018 sammenlignet med 2021-2022

	2018	2021-2022
Universitetet har en komplet og opdateret fortegnelse over hardware (servere og desktops), som har adgang til netværk, der indeholder systemer og data, som er vigtige for forskningen.	🟡	🟡
Universitetet anvender en metode til at opdage ukendt hardware på netværk med forskningsdata.	🔴	🟡

Note: For hvert revisionskriterium har Rigsrevisionen vurderet, om KU har opfyldt kriteriet. Vurderingen er angivet med grøn (opfyldt), gul (delvist opfyldt) eller rød (ikke opfyldt).

Kilde: Rigsrevisionens beretning fra 2019 og Rigsrevisionens opfølgning fra 2021-2022.

Det fremgår af tabel 3, at KU delvist opfylder kriteriet om, at universitetet har en komplet og opdateret fortegnelse over hardware, som har adgang til netværket, med systemer og data, som er vigtige for forskningen. Rigsrevisionens opfølgning viser, at KU samlet har opdaterede fortegnelser over det hardware, som KU styrer. Dog viser opfølgningen også, at KU ikke har fortegnelser over det udstyr, som KU ikke selv styrer (forskernes eget medbragte udstyr/Bring Your Own Device – BYOD). KU-IT har dog begrænset adgangen for BYOD-udstyr på forskellig vis på NORS og BMI, hvilket reducerer risikoen ved BYOD. KU-IT er yderligere i gang med at implementere tiltag, der vil give KU-IT mulighed for at få overblik over udstyr, som KU-IT ikke styrer, men som har adgang til netværket.

Det fremgår videre af tabellen, at KU delvist opfylder kriteriet om at anvende en metode til at opdage ukendt hardware på netværk med forskningsdata. Vores opfølgning viser, at KU-IT siden 2018 har implementeret og er i gang med at implementere forskellige værktøjer til at scanne de interne netværk med henblik på at opdage ukendt udstyr. Denne løsning fra KU-IT anvendes ligeledes af BMI. NBI anvender en anden metode til at opdage ukendt hardware på deres netværk, som Rigsrevisionen vurderer kun delvist opfylder kontrolmålet.

KU's overblik over software og softwareopdatering

24. Rigsrevisionen har fulgt op på KU's overblik over software og softwareopdatering. Resultatet fremgår af tabel 4, der viser beretningens resultater fra 2018 sammenlignet med opfølgningen fra 2021-2022.

Tabel 4

KU's overblik over software og softwareopdatering 2018 sammenlignet med 2021-2022

	2018	2021-2022
Universitetet har overblik over anvendt software på pc'er, og om den anvendte software er opdateret.	●	●
Universitetet har overblik over anvendt software på servere, og om den anvendte software er opdateret.	●	●

Note: For hvert revisionskriterium har Rigsrevisionen vurderet, om KU har opfyldt kriteriet. Vurderingen er angivet med grøn (opfyldt), gul (delvist opfyldt) eller rød (ikke opfyldt).

Kilde: Rigsrevisionens beretning fra 2019 og Rigsrevisionens opfølgning fra 2021.

Det fremgår af tabel 4, at KU delvist opfylder kontrolmålet om overblik over anvendt software på pc'er, og om den anvendte software er opdateret. Vores opfølgning viser, at KU-IT, BMI og NORS både har overblik over anvendt software på pc'er, og om den anvendte software er opdateret for så vidt angår det udstyr, der er styret af KU-IT. KU-IT har ikke mulighed for at danne overblik over anvendt software på BYOD-udstyr, da det er udstyr, som forskerne selv medbringer. KU-IT har dog begrænset adgangen for BYOD-udstyr på forskellig vis på BMI og NORS, hvilket reducerer risikoen ved BYOD. Vores opfølgning viser, at alle de adspurgte forskere på NORS anvender KU-computere og dermed er omfattet af de centrale opdateringer og det centrale overblik over software.

Vores opfølgning viser videre, at NBI fortsat ikke har overblik over anvendt software (herunder om det er opdateret) på klient-pc'er.

Det fremgår videre af tabellen, at KU opfylder kontrolmålet om overblik over anvendt software på servere, og om den anvendte software er opdateret.

Sammenfatning af resultatet af Uddannelses- og Forskningsministeriets bestræbelser i forhold til, at universiteterne får identificeret og rettet op på eventuelle kritiske it-sikkerhedsbrister

25. Rigsrevisionen finder, at Uddannelses- og Forskningsministeriet og universiteterne har foretaget et stort arbejde i forhold til at få identificeret og rettet op på kritiske it-sikkerhedsbrister. Rigsrevisionen vurderer, at ministeriets og universiteternes arbejde med den del af opfølgningspunktet, der omhandler identificering af kritiske it-sikkerhedsbrister, er tilfredsstillende. Rigsrevisionen vurderer på den baggrund, at denne del af sagen kan afsluttes.

26. Rigsrevisionen vurderer på baggrund af Uddannelses- og Forskningsministeriets redegørelser, opfølgningen på kortlægningen af universiteternes risikoprofiler og den opfølgende it-revision hos KU, at flere af universiteterne forsat har en række kritiske it-sikkerhedsbrister, hvilket har den konsekvens, at forskningsdata ikke beskyttes i tilstrækkelig grad. Henset til universiteternes høje trusselsniveau finder Rigsrevisionen ikke, at tempoet for arbejdet hermed har været tilfredsstillende.

Det bemærkes, at der i forhold til it-revisionen hos KU er individuelle forskelle på tværs af KU-IT og de 3 udvalgte institutter. Revisionen har vist, at KU-IT, NORS og BMI er nået længst i forhold til at rette op på manglerne, mens NBI ikke er nået så langt og således har væsentligt flere åbentstående kontrolmål end de 3 øvrige reviderede.

Rigsrevisionen vil derfor følge resultatet af Uddannelses- og Forskningsministeriets bestræbelser i forhold til, at universiteterne får rettet op på kritiske it-sikkerhedsbrister, der medfører, at forskningsdata ikke beskyttes i tilstrækkelig grad.

Birgitte Hansen