Finansudvalget 2023-24
FIU Alm.del - Bilag 60
Offentligt

FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

December 2023
– 5/2023

Rigsrevisionens beretning afgivet til Folketinget med Statsrevisorernes bemærkninger

Statens it-beredskab II

5/2023

Beretning om

statens it-beredskab II

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

København 2023

Denne beretning til Folketinget skal behandles ifølge lov om revisionen af statens regnskaber, § 18:

Statsrevisorerne fremsender med deres bemærkning Rigsrevisionens beretning til Folketinget og vedkommende minister.

Ministrene afgiver en redegørelse til beretningen.

Rigsrevisor afgiver et notat med bemærkninger til ministrenes redegørelser.

På baggrund af ministrenes redegørelser og rigsrevisors notat tager Statsrevisorerne endelig stilling til beretningen, hvilket forventes at ske i marts 2024.

Ministrenes redegørelser, rigsrevisors bemærkninger og Statsrevisorernes eventuelle bemærkninger samles i Statsrevisorernes Endelig betænkning over statsregnskabet, som årligt afgives til Folketinget i februar måned – i dette tilfælde Endelig betænkning over statsregnskabet 2023, som afgives i februar 2025.

Statsrevisorernes bemærkning tager udgangspunkt i denne karakterskala:

Karakterskala	
Positiv kritik	• finder det meget/særdeles positivt • finder det positivt • finder det tilfredsstillende/er tilfredse med
Kritik under middel	• finder det ikke helt tilfredsstillende
Middel kritik	• finder det utilfredsstillende/er utilfredse med • påpeger/understreger/henstiller/forventer • beklager/finder det bekymrende/foruroligende
Skarp kritik	• kritiserer/finder det kritisabelt/kritiserer skarpt/indskærper • påtaler/påtaler skarpt
Skarpeste kritik	• påtaler skarpt og henleder særligt Folketingets opmærksomhed på

Henvendelse vedrørende denne publikation rettes til:
Statsrevisorerne
Folketinget
Christiansborg
1240 København K

Tlf.: 3337 5987
statsrevisorerne@ft.dk
www.ft.dk/statsrevisorerne

ISSN 2245-3008
ISBN online 978-87-7434-826-9

Statsrevisorernes bemærkning

Beretning om statens it-beredskab II

Center for Cybersikkerhed under Forsvarets Efterretningstjeneste vurderer, at truslen i Danmark fra cyberkriminalitet og cyberspionage er meget høj, og at truslen fra cyberaktivisme er høj.

Denne beretning omhandler it-beredskabet for 12 samfundskritiske it-systemer i henholdsvis Indenrigs- og Sundhedsministeriet, Erhvervsstyrelsen, Søfartsstyrelsen og 4 andre anonymiserede myndigheder[1)].

Dette er den anden undersøgelse af it-beredskabet for statens samfundskritiske it-systemer, som i alt udgøres af ca. 90 it-systemer. Den første undersøgelse, *beretning nr. 3/2022 om statens it-beredskab,* fra november 2022 omhandlede 13 samfundskritiske it-systemer. Statsrevisorerne kritiserede dengang, at der for ingen af de 13 it-systemer var sikret et tilfredsstillende it-beredskab. Statsrevisorerne sendte efterfølgende en opfordring til alle ministre om at identificere ministerområdets samfundskritiske it-systemer og styrke it-beredskabet. Derudover har Rigsrevisionen afholdt et informationsmøde for alle ministerier om, hvordan man kan styrke it-beredskabet.

Statsrevisorerne kritiserer, at der for 7 af de 12 undersøgte samfundskritiske it-systemer ikke er sikret et tilfredsstillende it-beredskab. Det indebærer risiko for, at staten ikke kan opretholde eller markant får forstyrret løsningen af samfundskritiske opgaver i tilfælde af større it-nedbrud, hackerangreb, fysiske skader e.l.

Statsrevisorerne finder det særdeles nødvendigt, at de undersøgte myndigheder hurtigst muligt får rettet op på de mangler i it-beredskabet, som Rigsrevisionen har påpeget. Det gælder især test af it-beredskabsplanerne og kvaliteten af planerne.

Statsrevisorerne

4. december 2023

Mette Abildgaard
Leif Lahn Jensen
Mikkel Irminger Sarbo
Serdal Benli
Lars Christian Lilleholt
Monika Rubin

[1)] Alle 12 samfundskritiske it-systemer og 4 ud af 7 myndigheder er anonymiseret i beretningen, da myndighederne vurderer, at oplysninger om myndighedernes it-beredskab er fortrolige, jf. forvaltningsloven og straffeloven.

Statsrevisorerne konstaterer, at Indenrigs- og Sundhedsministeriet har etableret et it-beredskab, der i overvejende grad er tilfredsstillende. Statsrevisorerne konstaterer også, at Erhvervsstyrelsen og Søfartsstyrelsen delvist har etableret et tilfredsstillende it-beredskab, dog med visse mangler.

Indholdsfortegnelse

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

Rigsrevisionens mandat til at gennemføre undersøgelsen følger af § 2, stk. 1, nr. 1, jf. § 3 i rigsrevisorloven.

Beretningen har i udkast været forelagt de undersøgte ministerier, hvis bemærkninger i videst muligt omfang er afspejlet i beretningen.

1. Introduktion og konklusion

Anonymisering af myndigheder og systemnavne

Beretningen indeholder vurderinger af sikkerhedsmæssige procedurer i relation til offentlige it-systemer, der indgår i den samfundskritiske it-infrastruktur. Nogle af de undersøgte myndigheder og alle systemnavne er anonymiseret i beretningen. Det skyldes, at myndighederne konkret vurderer, at oplysninger om myndighedernes it-beredskab er fortrolige oplysninger, jf. forvaltningslovens § 27 og straffelovens § 152. Da Rigsrevisionen ikke har grundlag for at tilsidesætte denne vurdering, vil 4 myndigheder og alle systemnavne være anonymiseret i beretningen. Anonymiseringen betyder, at de 4 myndigheder omtales som myndighed 1, 2, 3 og 4, og at it-systemerne omtales som system A-L, i beretningen.

1.1. Formål og konklusion

1. Denne beretning handler om statens it-beredskab for udvalgte samfundskritiske it-systemer.

Offentlige myndigheder er afhængige af it-systemer for at kunne løse deres opgaver. Større it-nedbrud og tab af data i myndighedernes samfundskritiske it-systemer kan have store konsekvenser for både staten, borgere og virksomheder. Det er derfor afgørende, at myndighederne har et tilstrækkeligt it-beredskab på plads, så de ved et større it-nedbrud kan videreføre driften og minimere konsekvenserne af nedbruddet.

2. I staten er der ca. 90 it-systemer, som ministerierne vurderer er samfundskritiske. Rigsrevisionen afgav i november 2022 en beretning til Statsrevisorerne, som handlede om it-beredskabet for 13 af statens samfundskritiske it-systemer. Undersøgelsen viste, at der for ingen af de 13 it-systemer var implementeret et tilfredsstillende it-beredskab, og at det for størstedelen af systemerne ikke var testet, om systemerne kunne reetableres ved et stort it-nedbrud. Rigsrevisionen har i oktober 2023 fulgt op på beretningen. Opfølgningen viser, at der er sket forbedringer i it-beredskabet for de 13 undersøgte it-systemer.

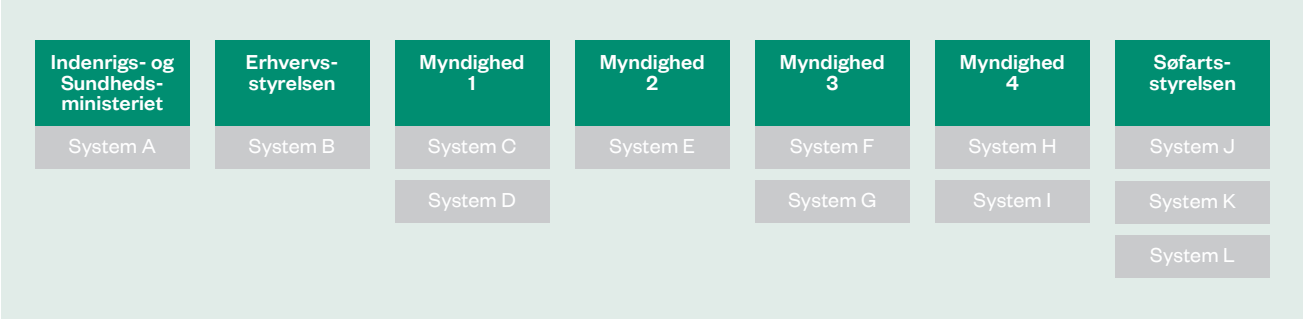
Rigsrevisionen afdækker i denne nye beretning it-beredskabet for yderligere 12 samfundskritiske it-systemer.

Samfundskritisk it-system
Et samfundskritisk it-system er et it-system, hvor større driftsforstyrrelser resulterer i væsentlige udfordringer for samfundet som helhed, fx:

- økonomiske tab for staten, borgere eller virksomheder
- længerevarende nedbrud af kritisk infrastruktur
- trusler mod den nationale sikkerhed.

3. Figur 1 viser de myndigheder og antallet af it-systemer, som indgår i undersøgelsen.

Figur 1
Myndigheder og it-systemer i Rigsrevisionens undersøgelse



Større it-hændelser, hvor myndighederne har brug for et it-beredskab
Større it-hændelser kan være situationer, hvor et it-system bliver utilgængeligt, fx ved hackerangreb, fysiske skader på datacentre eller fejl på servere.

Større it-hændelser kan også indebære tab af data i et it-system. Datatab kan opstå ved, at data ikke kan genskabes ud fra en backup, fx efter et it-nedbrud eller hackerangreb.

Typer af it-beredskabsplaner

- **Krisestyringsplan:** Plan for myndighedernes interne krisestyring og kommunikation til eksterne parter.
- **Nødplan:** Plan for, hvordan myndigheden viderefører de opgaver, som påvirkes, hvis der er nedbrud på kritiske it-systemer.
- **Reetableringsplan:** Plan for, hvordan et it-system skal reetableres efter et nedbrud.

4. 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. Vi besvarer følgende spørgsmål i beretningen:

- Har staten et tilfredsstillende grundlag for at etablere et it-beredskab for de udvalgte samfundskritiske it-systemer? *(kapitel 2)*
- Har staten implementeret tilfredsstillende krisestyringsplaner for de udvalgte samfundskritiske it-systemer? *(kapitel 3)*
- Har staten implementeret tilfredsstillende nødplaner for de udvalgte samfundskritiske it-systemer? *(kapitel 4)*
- Har staten sikret, at der er implementeret tilfredsstillende reetableringsplaner for de udvalgte samfundskritiske it-systemer? *(kapitel 5)*

I kapitel 3, 4 og 5 har vi både undersøgt, om de 3 typer af it-beredskabsplaner er udarbejdet, og om planerne er testet.

Rigsrevisionen har selv taget initiativ til undersøgelsen i februar 2023. Undersøgelsen dækker perioden fra januar 2020 til og med marts 2023.

Hovedkonklusion

Indenrigs- og Sundhedsministeriet har for sit samfundskritiske it-system sikret et it-beredskab, der i overvejende grad er tilfredsstillende. Dele af it-beredskabet for Erhvervsstyrelsens og Søfartsstyrelsens 4 samfundskritiske it-systemer er ligeledes i overvejende grad tilfredsstillende, men der er dog mangler. For de resterende 7 samfundskritiske it-systemer er der ikke et tilfredsstillende it-beredskab. Særligt er it-beredskabet mangelfuldt for 5 af it-systemerne (*system C, D, E, F* og *G*). Konsekvensen af manglerne i it-beredskabet er, at der er risiko for, at it-nedbrud og datatab medfører, at staten ikke kan opretholde eller markant får forstyrret løsningen af samfundskritiske opgaver.

For halvdelen af it-systemerne har myndighederne etableret et tilstrækkeligt grundlag for it-beredskabet i form af risikovurderinger og overblik over, hvilke andre it-systemer der er afgørende for, at de udvalgte it-systemer kan fungere.

For hovedparten af it-systemerne har myndighederne udarbejdet it-beredskabsplaner, men der er stor variation i planernes kvalitet. Enkelte af it-beredskabsplanerne er tilfredsstillende, mens andre har betydelige mangler. Det gælder særligt for reetableringsplanerne. Fx mangler der i over halvdelen af planerne beskrivelser af, hvordan it-systemerne teknisk kan reetableres efter et større it-nedbrud. For enkelte it-systemer er der ikke udarbejdet it-beredskabsplaner.

Kun et fåtal af it-beredskabsplanerne er blevet testet. Det finder Rigsrevisionen utilfredsstillende, da det betyder, at myndighederne ikke har trænet beredskabet og dermed ikke ved, om it-beredskabsplanerne virker efter hensigten. Fx har myndighederne for hovedparten af it-systemerne ikke testet, om systemerne kan reetableres efter et større it-nedbrud.

Hovedparten af ministerierne har ført tilsyn med it-beredskabet. På trods heraf viser undersøgelsen, at der er betydelige mangler i myndighedernes it-beredskabsplaner og i myndighedernes tests af planerne.

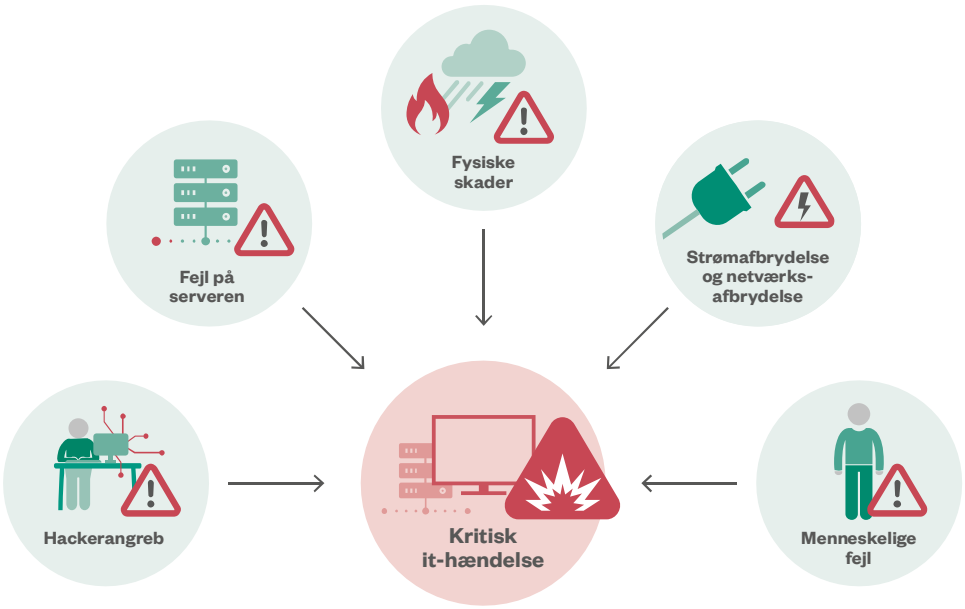
1.2. Baggrund

Eksempel på it-nedbrud
I juni 2022 var der et stort nedbrud på NemID. Nedbruddet varede i ca. 5 dage og betød, at 30 % af brugerne ikke kunne bruge tjenesten til at tilgå fx e-Boks, borger.dk og netbank.

Kilde: Digitaliseringsstyrelsen.

5. It-beredskabet er en del af myndighedernes samlede beredskab. Beredskabet skal kunne håndtere ekstraordinære hændelser, der ikke kan klares gennem de normale arbejdsgange og den daglige drift. It-beredskabet handler om, hvordan myndighederne kan opretholde eller reetablere de it-systemer, som myndighederne er afhængige af for at kunne varetage deres kritiske funktioner. Figur 2 viser eksempler på hændelser, hvor det kan være nødvendigt for myndighederne at aktivere deres it-beredskab.

Figur 2
Eksempler på hændelser, hvor myndigheder kan aktivere it-beredskabet



Kilde: Rigsrevisionen.

6. Det overordnede princip for beredskabet (herunder it-beredskabet) i Danmark er sektoransvarsprincippet. Det betyder, at den myndighed, som til daglig har ansvaret for en opgave og de tilhørende it-systemer, også har ansvaret under en større it-hændelse eller katastrofe. Det er derfor den enkelte myndighed, der har ansvaret for at sikre et tilstrækkeligt it-beredskab på sit område.

Krav til it-beredskabet

7. Offentlige myndigheder har siden 2016 skullet følge den internationale standard for informationssikkerhed ISO 27001. ISO 27001 består af en række kontrolmål inden for informationssikkerhed. Flere af kontrolmålene vedrører it-beredskabet.

Ifølge ISO 27001 skal myndighederne planlægge it-beredskabet ved at vurdere, hvilke forhold og elementer der er relevante at tage højde for i it-beredskabet, herunder kortlægge systemafhængigheder og væsentlige risici for it-systemerne. Myndighederne skal udarbejde it-beredskabsplaner på baggrund af den viden, som myndighederne har kortlagt. Endvidere skal myndighederne teste it-beredskabsplanerne for at vurdere, om procedurerne for beredskabet er på plads, og for at træne relevante medarbejdere i beredskabshåndteringen. Testen skal evalueres, og på baggrund heraf skal it-beredskabsplanen eventuelt justeres.

8. Vi har valgt at fokusere på 3 typer af it-beredskabsplaner i undersøgelsen af statens it-beredskab: *krisestyringsplaner*, *nødplaner* og *reetableringsplaner*, som skal håndtere forskellige opgaver inden for it-beredskabet. Myndighederne kan strukturere it-beredskabet på forskellige måder og kan derfor have en anden opdeling af it-beredskabsplanerne eller have andre betegnelser for planerne. Det er vigtigt, at it-beredskabsplanerne er på plads, før en beredskabssituation opstår, for at minimere eventuelle følgevirkninger af et større it-nedbrud eller datatab.

Krisestyringsplaner beskriver myndighedens interne krisestyring ved et større it-nedbrud. En krisestyringsplan fastlægger, hvordan myndigheden skal håndtere et nedbrud og sikre, at alle relevante personer bliver informeret og kender deres roller i en beredskabssituation. Krisestyringsplanen omfatter også myndighedens plan for kommunikation til eksterne parter, som er afhængige af at anvende de it-systemer, der utilgængelige. Det kan fx være borgere, virksomheder og andre offentlige myndigheder som fx kommuner og regioner.

Nødplaner beskriver, hvilke nødprocedurer myndigheden eventuelt kan tage i brug i tilfælde af et nedbrud på de it-systemer, som normalt varetager opgaverne. Det kan fx betyde, at myndigheden må bruge manuelle procedurer eller alternative it-systemer for at løse sine opgaver.

Reetableringsplaner beskriver, hvordan it-systemer teknisk reetableres efter et nedbrud. Ved it-systemer, der er driftet af myndigheden, er det myndigheden selv, som skal udarbejde og teste reetableringsplanerne. Hvis et it-system er driftet af en ekstern leverandør, er det typisk leverandøren, som står for at reetablere systemet og udarbejde en reetableringsplan. Det er myndighedens ansvar at sikre, at der er reetableringsplaner, og at stille krav til leverandørernes reetableringsplaner.

Informationssikkerhed
It-beredskabet er en del af informationssikkerheden, som bl.a. har til formål at sikre informationer i forhold til fortrolighed, integritet (ændring af data) og tilgængelighed.

Eksempel på it-nedbrud
I juli 2023 blev 12 ud af 16 norske ministerier, herunder det norske sundhedsministerium og det norske finansministerium, ramt af et stort hackerangreb. Hackerangrebet betød, at ministerierne ikke kunne arbejde som normalt. Hackerne havde fået adgang til en it-platform, som de fleste af ministerierne anvender.

Ifølge Norges nationale sikkerhedsmyndighed har hackerne udnyttet en svaghed i systemerne, som leverandøren eller producenten ikke kendte til på forhånd.

Kilde: Politiken og Nasjonal sikkerhetsmyndighet.

1.3. Revisionskriterier, metode og afgrænsning

Revisionskriterier

9. Undersøgelsens revisionskriterier tager udgangspunkt i den internationale standard for informationssikkerhed ISO 27001:2017, som myndighederne skal følge. Revisionskriterierne tager desuden udgangspunkt i Digitaliseringsstyrelsens vejledninger og skabeloner, der konkretiserer, hvordan myndighederne i praksis kan implementere ISO 27001. Enkelte steder har vi operationaliseret, hvordan ISO 27001 eller vejledninger kan forstås i forhold til samfundskritiske it-systemer. Dette er nærmere beskrevet i bilag 1 og bilag 2, hvor der også er en oversigt over de kriterier, som vi har anvendt til at vurdere myndighedernes it-beredskabsplaner (krisestyringsplaner, nødplaner og reetableringsplaner) og myndighedernes tests af planerne.

Undersøgelsen tager udgangspunkt i, at myndighederne skal indtænke ekstraordinære hændelser i planlægningen af it-beredskabet for samfundskritiske it-systemer – også selv om sandsynligheden for hændelsen kan forekomme at være lille.

I *kapitel 2* har vi undersøgt myndighedernes grundlag for at etablere et tilfredsstillende it-beredskab. Det har vi gjort ved at undersøge, om myndighederne har kortlagt it-systemernes afhængigheder til andre it-systemer, og om myndighederne har udarbejdet risikovurderinger af de udvalgte it-systemer. Vi har også undersøgt, om ministerierne har ført tilsyn med myndighedernes it-beredskab.

I *kapitel 3* har vi undersøgt, om myndighederne har udarbejdet krisestyringsplaner, som skal bruges, hvis der er nedbrud på et af myndighedernes samfundskritiske it-systemer. Vi har også undersøgt, om krisestyringsplanerne indeholder en række centrale elementer, som tager udgangspunkt i ISO 27001 og i Digitaliseringsstyrelsens vejledning i it-beredskab. Derudover har vi undersøgt, om krisestyringsplanerne er testet.

I *kapitel 4* har vi undersøgt, om myndighederne har udarbejdet nødplaner for de udvalgte samfundskritiske it-systemer, og om nødplanerne indeholder centrale elementer, som tager udgangspunkt i ISO 27001 og i Digitaliseringsstyrelsens vejledning i it-beredskab. Vi har også undersøgt, om nødplanerne er testet.

I *kapitel 5* har vi undersøgt, om myndighederne har sikret, at der er tilfredsstillende reetableringsplaner for de udvalgte samfundskritiske it-systemer. Det har vi gjort ved at undersøge, om der er reetableringsplaner, som indeholder en række centrale elementer, der tager udgangspunkt i ISO 27001 og i Digitaliseringsstyrelsens vejledning i it-beredskab. Derudover har vi undersøgt, om reetableringsplanerne er testet.

Metode

10. Vi har udvalgt 12 it-systemer, der understøtter forskellige samfundskritiske funktioner og opgaver i staten. Ansvaret for de 12 it-systemer er placeret hos Indenrigs- og Sundhedsministeriet, Erhvervsstyrelsen, Søfartsstyrelsen og 4 andre myndigheder, som er anonymiseret i beretningen. De 4 myndigheder benævnes myndighed 1, 2, 3 og 4.

11. Vi har som grundlag for undersøgelsen indhentet og gennemgået dokumenter om it-beredskabet for de 12 it-systemer. For it-systemerne har vi gennemgået myndighedernes kortlægning af systemafhængigheder og risikovurderinger samt it-beredskabsplaner (krisestyringsplaner, nødplaner og reetableringsplaner) og testrapporter for at vurdere, om planerne og rapporterne indeholder de mest centrale elementer. Derudover har vi for de it-systemer, som er driftet af eksterne leverandører, indhentet kontraktbilag, som vedrører it-beredskabet.

Vi har holdt møder med relevante medarbejdere i myndighederne for at stille spørgsmål til it-beredskabet for de udvalgte it-systemer.

12. Revisionen er udført i overensstemmelse med standarderne for offentlig revision, jf. bilag 1.

Afgrænsning

13. Undersøgelsen handler om planlægning og udarbejdelse af it-beredskabsplaner i form af krisestyringsplaner, nødplaner, reetableringsplaner og test af planerne i perioden januar 2020 - marts 2023. Det betyder, at vi fx ikke har undersøgt, hvordan it-beredskabet rent faktisk har fungeret i en beredskabssituation. Derudover har vi afgrænset os fra at undersøge myndighedernes forebyggelse af, at der opstår et større it-nedbrud, men har kun fokus på det it-beredskab, som myndighederne skal iværksætte, hvis der opstår et større it-nedbrud.

14. Vi har som udgangspunkt ikke undersøgt myndighedernes generelle beredskabsplaner, som også kan omfatte beredskabssituationer såsom brand og naturkatastrofer. Myndighedernes generelle beredskabsplaner har dog indgået i undersøgelsen, hvis de omfatter it-beredskabssituationer vedrørende større nedbrud, datatab mv. i myndighedernes it-systemer.

15. I bilag 1 er undersøgelsens metodiske tilgang beskrevet. Bilag 2 er en oversigt over undersøgelsens revisionskriterier. Bilag 3 er en oversigt over myndighedernes samlede resultater.

2. Grundlaget for it-beredskabet

Delkonklusion

De undersøgte myndigheder har for halvdelen af de udvalgte it-systemer etableret et tilstrækkeligt grundlag for deres it-beredskab. Særligt har Indenrigs- og Sundhedsministeriet, myndighed 2 og Søfartsstyrelsen et tilfredsstillende grundlag for it-beredskabet. Myndighederne har generelt kortlagt, hvilke afhængigheder de udvalgte it-systemer har til andre it-systemer, men flere af myndighederne har mangler i risikovurderingerne af it-systemerne.

Alle ministerierne undtagen Indenrigs- og Sundhedsministeriet har ført tilsyn med it-beredskabet på ministerområderne. På trods af at de fleste ministerier har ført tilsyn, er der betydelige mangler i myndighedernes it-beredskab.

Eksempel på systemafhængigheder
Nedbrud på NemID i juni 2022 betød, at det ikke var muligt at tilgå en lang række andre it-systemer. Fx var det ikke muligt for sundhedsfaglige personer at logge på et it-system, som giver adgang til medicinoplysninger. Nedbruddet betød også, at domstole og advokater ikke kunne logge på hjemmesiden minretssag.dk, som anvendes til sagsbehandling af civile retssager.

Kilde: Digitaliseringsstyrelsen, Sundhedsdatastyrelsen og Danmarks Domstole.

16. Dette kapitel handler om, hvorvidt myndighederne har et tilfredsstillende grundlag for at etablere et it-beredskab for de 12 udvalgte samfundskritiske it-systemer.

17. Vi har undersøgt:

- om myndighederne har kortlagt it-systemernes afhængigheder til andre it-systemer
- om myndighederne har udarbejdet risikovurderinger
- om de ansvarlige ministerier har ført tilsyn med myndighedernes it-beredskab.

2.1. Kortlægning af it-systemernes afhængigheder til andre it-systemer

18. Vi har undersøgt, om myndighederne har kortlagt, hvilke andre it-systemer, støttesystemer, platforme mv. de udvalgte samfundskritiske it-systemer er afhængige af for at kunne fungere. Det er vigtigt at have et overblik over disse afhængigheder, da et nedbrud på støttesystemer, platforme mv. kan betyde, at de samfundskritiske it-systemer ikke fungerer. Tabel 1 viser, om myndighederne for de 12 udvalgte it-systemer har kortlagt, hvilke systemafhængigheder der er til andre it-systemer.

Tabel 1
Myndighedernes kortlægning af de udvalgte it-systemers systemafhængigheder

	Indenrigs- og Sundheds-ministeriet	Erhvervs-styrelsen	Myndighed 1		Myndighed 2	Myndighed 3		Myndighed 4		Søfarts-styrelsen		
It-system	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
Systemafhængig-hederne er kortlagt	●	●	●	●	●	●	●	●	●	●	●	●

● Ja ● Delvist ● Nej

Kilde: Rigsrevisionen på baggrund af dokumentation fra myndighederne.

Det fremgår af tabel 1, at 6 af de 7 myndigheder har kortlagt, hvilke andre it-systemer, støttesystemer, platforme mv. der er afgørende for, at de udvalgte it-systemer kan reetableres efter et nedbrud. Fx har Indenrigs- og Sundhedsministeriet for *system A* sikret, at systemarkitekturen, herunder afhængigheder og sammenhænge til andre it-systemer, er beskrevet.

Undersøgelsen viser også, at myndighed 4 har udarbejdet en rækkefølge for reetablering af sine it-systemer i tilfælde af, at flere systemer er utilgængelige samtidigt. For de 2 systemer er der dog fejl og mangler i rækkefølgen for reetablering.

2.2. Risikovurderinger

19. Ifølge ISO 27001 skal myndighederne ved planlægningen af informationssikkerheden, herunder it-beredskabet, tage udgangspunkt i risici, som skal vurderes i forhold til en række sårbarheder, trusler, konsekvenser og sandsynligheder. Vi har derfor undersøgt:

- om myndighederne har udarbejdet risikovurderinger af de udvalgte samfundskritiske it-systemer, som kortlægger sårbarheder og trusler
- om risikovurderingerne forholder sig til konsekvenserne af og sandsynligheden for, at sårbarheder og trusler bliver udnyttet eller indtræffer
- om risikovurderingerne er blevet forelagt ledelsen.

20. Undersøgelsen viser, at alle myndighederne har en nedskrevet procedure eller politik for risikovurderinger. Procesbeskrivelserne handler fx om, hvordan der skal foretages risikovurderinger, eller hvilke sårbarheder og trusler der skal vurderes for it-systemerne.

Undersøgelsen viser også, at det ikke er alle myndigheder, som har udarbejdet risikovurderinger af de udvalgte samfundskritiske it-systemer, jf. tabel 2.

Tabel 2
Myndighedernes risikovurderinger af de udvalgte samfundskritiske it-systemer

	Indenrigs- og Sundheds-ministeriet	Erhvervs-styrelsen	Myndighed 1		Myndighed 2	Myndighed 3		Myndighed 4		Søfarts-styrelsen		
It-system	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
Der er udarbejdet risikovurderinger, som indeholder vurderinger af sårbarheder, trusler, konsekvenser og sandsynligheder	●	●	●	●	●	●	●	●	●	●	●	●

● Ja ● Delvist ● Nej

Kilde: Rigsrevisionen på baggrund af dokumentation fra myndighederne.

Det fremgår af tabel 2, at Indenrigs- og Sundhedsministeriet, myndighed 2 og Søfartsstyrelsen har udarbejdet risikovurderinger af alle deres udvalgte it-systemer. Myndighed 1 og myndighed 4 har dog ikke udarbejdet risikovurderinger af henholdsvis *system D* og *system I*.

Risikovurderingerne af 3 af systemerne (*system B, F* og *G*) er kun delvist tilfredsstillende, da de kun består af talvurderinger og ikke indeholder forklarende tekst. Der er dermed risiko for, at risikovurderingerne er indforstået, og at det er svært for ledelserne at agere på baggrund af dem. Både Erhvervsstyrelsen og myndighed 3 har oplyst, at de har igangsat et arbejde med at forbedre deres risikovurderinger med en mere udbygget beskrivelse af trusler og risici for it-systemerne.

21. Risici og trusler kan løbende ændre sig, og derfor skal myndighederne i henhold til ISO 27001 jævnligt ajourføre deres risikovurderinger. Da der er tale om samfundskritiske it-systemer, har Rigsrevisionen lagt til grund for sin vurdering, at risikovurderingerne som minimum bør ajourføres årligt.

Undersøgelsen viser, at Indenrigs- og Sundhedsministeriet, Erhvervsstyrelsen og Søfartsstyrelsen årligt har ajourført deres risikovurderinger. De resterende myndigheder har ikke ajourført risikovurderingerne årligt i undersøgelsesperioden.

Mitigerende tiltag
Der er tale om mitigerende tiltag, når myndighederne reducerer en risiko ved at lave kompenserende tiltag.

22. Ifølge ISO 27001 skal myndighedernes ledelser forelægges risikovurderingerne for at være orienterede om de identificerede risici og for at kunne iværksætte mitigerende tiltag.

Undersøgelsen viser, at de seneste risikovurderinger har været forelagt ledelsen i 6 af myndighederne. Kun risikovurderingen af *system C* har ikke været forelagt ledelsen.

2.3. Ministeriernes tilsyn med it-beredskabet

Tilsyn med it-beredskabet
Tilsyn med it-beredskabet indebærer, at ministerierne har forholdt sig til, om myndighederne har udarbejdet og testet krisestyringsplaner, nødplaner og reetableringsplaner.

23. Vi har undersøgt, om ministeriernes tilsyn med informationssikkerhed inden for en 3-årig periode har omfattet it-beredskabet hos myndighederne. Det har vi undersøgt ved at gennemgå tilsynsrapporterne for de undersøgte myndigheder for perioden 2020-2022. Oftest vil det være ministeriernes departementer, der udfører tilsynet med deres underliggende myndigheder, men ministerierne kan uddelegere tilsynet til en underliggende myndighed eller oprette interne tilsynsenheder i departementerne.

24. Undersøgelsen viser, at alle ministerierne i undersøgelsen undtagen Indenrigs- og Sundhedsministeriet hvert år har ført tilsyn med informationssikkerheden hos de undersøgte myndigheder. Undersøgelsen viser også, at tilsynet i løbet af en 3-årig periode har omhandlet it-beredskabet hos de underliggende myndigheder på ministerområderne. På trods af at hovedparten af ministerierne har ført tilsyn med it-beredskabet, er der betydelige mangler i myndighedernes it-beredskab.

I undersøgelsesperioden januar 2020 -marts 2023 er der ikke blevet ført tilsyn med informationssikkerheden hos Indenrigs- og Sundhedsministeriet, som har ansvaret for *system A*. Dog er ledelsen i departementet blevet forelagt relevante dokumenter vedrørende it-beredskabet for *system A*, uden at der er tale om et egentlig tilsyn. Ministeriet har oplyst, at ministeriet er i gang med at udarbejde et koncept for det fremtidige tilsyn i ministeriets koncern.

3. Krisestyringsplaner

Delkonklusion

Myndighederne har generelt udarbejdet tilfredsstillende planer for den interne krisestyring ved større it-nedbrud. Én af krisestyringsplanerne er dog for overordnet og er ikke udarbejdet til krisestyring ved større it-nedbrud.

Kun 3 af de undersøgte myndigheder har testet deres krisestyringsplaner, og kun Erhvervsstyrelsen har testet sin plan årligt. De resterende 4 myndigheder har ikke testet deres krisestyringsplaner i løbet af undersøgelsesperioden.

25. Dette kapitel handler om myndighedernes interne krisestyringsplaner ved et større it-nedbrud. En krisestyringsplan fastlægger, hvordan myndigheden skal håndtere et it-nedbrud og sikre, at alle relevante personer bliver informeret og kender deres roller i en beredskabssituation.

26. Vi har undersøgt:

- om myndighederne har implementeret tilfredsstillende krisestyringsplaner for de udvalgte it-systemer, og om planerne indeholder en række centrale elementer
- om krisestyringsplanerne er testet.

3.1. Myndighedernes krisestyringsplaner

27. Vi har undersøgt, om myndighederne har udarbejdet krisestyringsplaner for, hvordan myndighederne internt skal håndtere større hændelser, som påvirker myndighedernes samfundskritiske it-systemer.

Vi har gennemgået myndighedernes krisestyringsplaner for at vurdere, om planerne er tilfredsstillende. Vi har lagt til grund, at en krisestyringsplan skal indeholde 5 centrale elementer, som er baseret på ISO 27001, på Digitaliseringsstyrelsens anbefalinger til beredskabsplaner og på skabeloner til it-beredskabsplaner på sikkerdigital.dk. Figur 3 viser de 5 centrale elementer, som en tilfredsstillende krisestyringsplan som minimum bør indeholde. En tilfredsstillende krisestyringsplan indeholder alle 5 centrale elementer og opnår en maksimal score på 100 point.

Sikkerdigital.dk
På sikkerdigital.dk kan myndigheder, borgere og virksomheder finde vejledninger og konkrete værktøjer til en sikker digital hverdag. Bag sikkerdigital.dk står Digitaliseringsstyrelsen og en række samarbejdspartnere.

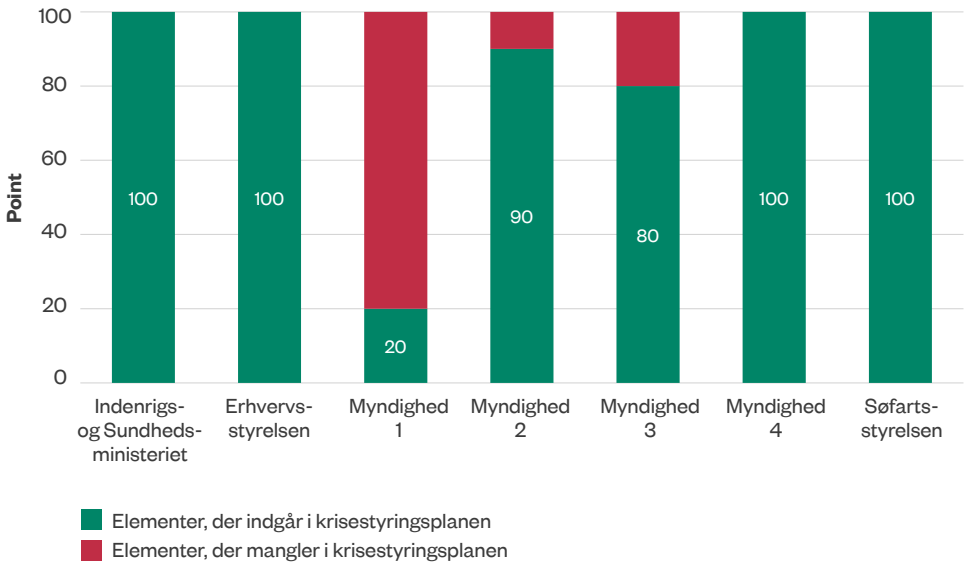
Figur 3
Centrale elementer i en krisestyringsplan

Kilde: Rigsrevisionen på baggrund af ISO 27001 og Digitaliseringsstyrelsens vejledning i it-beredskab.

28. Undersøgelsen viser, at alle myndighederne med undtagelse af én myndighed (myndighed 1) har udarbejdet krisestyringsplaner, der gælder på tværs af myndighedernes it-systemer. Myndighed 1 har en generel beredskabsplan, som ifølge myndigheden ikke er designet specifikt til it-krisestyring. Enkelte dele af den generelle beredskabsplan kan dog tages i brug ved it-hændelser, og derfor indgår myndighedens generelle beredskabsplan i vores vurderinger.

29. Figur 4 viser vores gennemgang af myndighedernes krisestyringsplaner.

Figur 4
Samlet vurdering af myndighedernes krisestyringsplaner



Kilde: Rigsrevisionen vurdering på baggrund af dokumentation fra myndighederne.

Sammenligning af krisestyringsplaner
For at vi kan sammenligne myndighedernes krisestyringsplaner, har vi tildelt planerne point efter, hvor mange af de 5 centrale elementer der indgår i planerne. En krisestyringsplan opnår en score på 100 point, hvis planen indeholder alle 5 elementer. Vi har vægtet de 5 elementer ligeligt, og myndighederne kan derfor opnå en score på maks. 20 point for hvert element.

Det fremgår af figur 4, at 4 af krisestyringsplanerne (Indenrigs- og Sundhedsministeriet, Erhvervsstyrelsen, myndighed 4 og Søfartsstyrelsen) indeholder alle de relevante elementer. Vi gennemgår nedenfor undersøgelsens resultater for de resterende myndigheder.

Krisestyringsplanen for myndighed 1 mangler størstedelen af de elementer, der skal fremgå af en krisestyringsplan. Både aktivering af krisestyringsplanen og kommunikationsrammerne er delvist beskrevet i planen. Myndighed 1 har oplyst, at myndigheden på baggrund af Rigsrevisionens undersøgelse er gået i gang med at udarbejde en it-krisestyringsplan, som dog ikke dækker hele myndigheden, men ét af de udvalgte samfundskritiske it-systemer.

Krisestyringsplanerne for myndighed 2 og myndighed 3 indeholder hovedparten af de centrale elementer. Krisestyringsplanerne mangler dog kontaktoplysninger på interne og eksterne nøglepersoner.

Årlig ajourføring

30. Vi har undersøgt, om krisestyringsplanerne er ajourført årligt. Krisestyringsplanerne skal ajourføres for at sikre, at planerne indeholder de korrekte oplysninger.

31. Undersøgelsen viser, at krisestyringsplanerne for Indenrigs- og Sundhedsministeriet, Erhvervsstyrelsen og Søfartsstyrelsen er blevet ajourført årligt. Krisestyringsplanen for myndighed 4 er først blevet udarbejdet i 2021 og er derefter blevet ajourført årligt. Krisestyringsplanerne for de øvrige 3 myndigheder (myndighed 1, 2 og 3) er ikke blevet ajourført i undersøgelsesperioden.

3.2. Test af krisestyringsplaner

32. Vi har undersøgt, om myndighederne har testet deres krisestyringsplaner i perioden januar 2020 - marts 2023. Krisestyringsplanerne skal med jævne mellemrum testes og trænes af relevante personer for at sikre, at planerne understøtter en effektiv intern krisestyring, hvis der er nedbrud på et af myndighedens it-systemer.

Vi har undersøgt, om krisestyringsplanerne er testet tilstrækkeligt, herunder:

- om krisestyringsplanen er testet årligt – enten ved en planlagt test eller ved, at planen har været aktiveret ved en hændelse
- om testrapporten indeholder testresultater
- om testrapporten beskriver eventuelle forbedringsforslag.

33. Tabel 3 viser vores gennemgang af myndighedernes tests af krisestyringsplanerne i perioden januar 2020 - marts 2023.

Tabel 3
Rigsrevisionens gennemgang af myndighedernes tests af krisestyringsplanerne

	Indenrigs- og Sundheds-ministeriet	Erhvervs-styrelsen	Myndighed 1	Myndighed 2	Myndighed 3	Myndighed 4	Søfarts-styrelsen
Krisestyringsplanen er testet årligt	●	●	●	●	●	●	●
Resultater af testen fremgår af testrapporten	-	●	-	-	-	●	●
Testrapporten beskriver eventuelle forbedringsforslag	-	●	-	-	-	●	●

● Ja ● Delvist ● Nej

Note: Ved "-" er kriteriet ikke vurderet, da krisestyringsplanen ikke er blevet testet.

Kilde: Rigsrevisionen på baggrund af dokumentation fra myndighederne.

Det fremgår af tabel 3, at Erhvervsstyrelsen, myndighed 4 og Søfartsstyrelsen har testet deres krisestyringsplaner i undersøgelsesperioden. Indenrigs- og Sundhedsministeriet og 3 myndigheder (myndighed 1, 2 og 3) har ikke testet deres krisestyringsplaner i undersøgelsesperioden.

Kun Erhvervsstyrelsen har testet sin krisestyringsplan hvert år i undersøgelsesperioden. Myndighed 4 har testet sin krisestyringsplan i 2021 og 2022, da planen først blev udarbejdet i 2021.

Søfartsstyrelsens krisestyringsplan har været aktiveret 2 gange i undersøgelsesperioden og er i den forbindelse blevet testet.

Testrapporterne for Erhvervsstyrelsen og myndighed 4 indeholder både resultater og forbedringsforslag. Søfartsstyrelsen har i forbindelse med én af it-hændelserne udarbejdet en evaluering, hvor der fremgår forbedringsforslag, men ikke resultater af myndighedens krisehåndtering af hændelsen.

4. Nødplaner for it-systemerne

Delkonklusion

Myndighederne har udarbejdet tilfredsstillende nødplaner for størstedelen af de udvalgte it-systemer. For *system C, D* og *E* er der ikke udarbejdet nødplaner. Erhvervsstyrelsen har for *system B* kun haft en dækkende og tilfredsstillende nødplan i den sidste måned af undersøgelsesperioden.

Kun 2 af de nødplaner, der er blevet udarbejdet, er blevet testet. Det er kun Erhvervsstyrelsens nødplan, der er blevet testet tilstrækkeligt.

34. Dette kapitel handler om myndighedernes nødplaner. En nødplan beskriver, hvilke nødprocedurer myndigheden eventuelt kan tage i brug i tilfælde af et nedbrud på de it-systemer, som normalt varetager opgaverne. Fx kan myndigheden bruge manuelle procedurer eller alternative it-systemer til at løse opgaverne.

35. Vi har undersøgt:

- om myndighederne har implementeret tilfredsstillende nødplaner for de udvalgte samfundskritiske it-systemer
- om nødplanerne er testet.

36. Ansvaret for at udarbejde nødplaner ligger hos de aktører, som anvender it-systemerne. For 11 af de 12 udvalgte it-systemer er det myndighederne selv, der anvender systemerne og derfor har ansvaret for at udarbejde nødplaner. Indenrigs- og Sundhedsministeriet anvender ikke selv *system A*, men ministeriet stiller systemet til rådighed for en lang række eksterne aktører. *System A* indgår derfor ikke i denne del af undersøgelsen.

4.1. Nødplaner

37. Vi har undersøgt, om myndighederne har udarbejdet nødplaner for de udvalgte it-systemer. Vi har med udgangspunkt i ISO 27001 undersøgt:

- om myndighedernes nødplaner beskriver de procedurer, der skal iværksættes for at opretholde kritiske opgaver og forretningsprocesser ved nedbrud på it-systemerne
- om det er beskrevet i nødplanerne, hvor planerne er tilgængelige
- om nødplanerne er ajourført årligt.

38. Tabel 4 viser vores gennemgang af myndighedernes nødplaner.

Tabel 4
Rigsrevisionens gennemgang af myndighedernes nødplaner

	Indenrigs- og Sundheds-ministeriet	Erhvervs-styrelsen	Myndighed 1		Myndighed 2	Myndighed 3		Myndighed 4		Søfarts-styrelsen		
It-system	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
Nødplanen beskriver, hvilke procedurer der skal iværksættes for at opretholde kritiske opgaver og forretningsprocesser	●	●[1)]	Ingen plan	Ingen plan	Ingen plan	●	●	●	●	●	●	●
Det er beskrevet i nødplanen, hvor den er tilgængelig	●	●[1)]	-	-	-	●	●	●	●	●	●	●
Nødplanen er ajourført årligt	●	●	-	-	-	●	●	●	●	●	●	●

● Ja ● Delvist ● Nej ● Ikke relevant

[1)] Erhversstyrelsens nødplan for *system B*, som ligger til grund for vurderingen, er fra marts 2023. Nødplanen har dermed først været gældende fra den sidste måned af undersøgelsesperioden.

Note: Ved "-" er kriteriet ikke vurderet, da der ikke er udarbejdet en nødplan.

Kilde: Rigsrevisionen på baggrund af dokumentation fra myndighederne.

Det fremgår af tabel 4, at Søfartsstyrelsen har udarbejdet tilfredsstillende nødplaner for de 3 udvalgte it-systemer. Myndighed 1 og myndighed 2 har ikke udarbejdet nødplaner for *system C, D* og *E*. Myndighed 1 har oplyst, at myndigheden er ved at udarbejde en nødplan for *system C*, som forventes at være færdig i 4. kvartal 2023. Rigsrevisionens vurderinger af de øvrige nødplaner gennemgås nedenfor.

Erhvervsstyrelsen

39. Undersøgelsen viser, at Erhvervsstyrelsens nødplan fra marts 2023 for *system B* indeholder de procedurer, der skal iværksættes for at opretholde kritiske opgaver og forretningsprocesser. Frem til marts 2023 har en tidligere version af nødplanen kun indeholdt procedurer for nedbrud på understøttende it-systemer, som *system B* er afhængig af. Nødplanen frem til marts 2023 har derfor ikke været tilfredsstillende. Det fremgår af Erhvervsstyrelsens generelle beredskabsplan, hvor styrelsens beredskabsplaner skal være tilgængelige. Det er Rigsrevisionens vurdering, at det er uhensigtsmæssigt, at det ikke også fremgår af selve nødplanen fra marts 2023. Erhvervsstyrelsen har oplyst, at styrelsen vil angive i nødplanen, hvor den skal være tilgængelig.

Myndighed 3

40. Undersøgelsen viser, at myndighed 3 har udarbejdet en nødplan for *system F*. Nødplanen forelå ved undersøgelsestidspunktet i en foreløbig version og var ikke blevet forelagt ledelsen. I forlængelse af undersøgelsen har myndighed 3 oplyst, at myndigheden stiller systemet til rådighed for en anden offentlig myndighed, som anvender systemet. Myndigheden vil derfor overveje, om det fremover er myndigheden selv eller andre aktører, som skal udarbejde en nødplan for systemet.

Nødplanen for *system G* er udarbejdet i november 2022, og der har derfor ikke været en nødplan for systemet i hovedparten af undersøgelsesperioden.

Ingen af nødplanerne for *system F* og *G* beskriver, hvor planerne skal være tilgængelige. Myndighed 3 har opdateret nødplanen for *system G,* efter undersøgelsen er afsluttet, så det fremgår, hvor planen opbevares.

Myndighed 4

41. Myndighed 4 har udarbejdet nødplaner for myndighedens 2 it-systemer (*system H* og *I*). Det første udkast til en nødplan for *system H* er dog først udarbejdet i oktober 2022 og i en endelig version i marts 2023. Der har dermed ikke været en nødplan for *system H* i hovedparten af undersøgelsesperioden. Det fremgår ikke af nødplanen, hvor planen er tilgængelig. Nødplanen for *system I* er blevet ajourført, dog ikke hvert år i undersøgelsesperioden.

4.2. Test af nødplaner

42. Vi har undersøgt, om myndighederne har testet nødplanerne i perioden januar 2020 - marts 2023. Nødplanerne skal testes med jævne mellemrum for at sikre, at planerne er ajourførte og indeholder de relevante informationer, samt for at sikre, at procedurerne trænes af relevante medarbejdere.

43. Vi har lagt Digitaliseringsstyrelsens vejledning i it-beredskab til grund for vurderingen af myndighedernes tests af nødplanerne. Vi har for hver nødplan undersøgt:

- om nødplanen er testet årligt – enten ved en planlagt test eller ved, at planen har været aktiveret ved en hændelse
- om testrapporten beskriver eventuelle forbedringsforslag.

44. Tabel 5 viser vores gennemgang af myndighedernes tests af nødplaner i perioden januar 2020 - marts 2023.

Tabel 5
Rigsrevisionens gennemgang af myndighedernes tests af nødplaner

	Indenrigs- og Sundheds-ministeriet	Erhvervs-styrelsen	Myndighed 1		Myndighed 2	Myndighed 3		Myndighed 4		Søfarts-styrelsen		
It-system	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
Nødplanen er testet årligt	●	●	Ingen plan	Ingen plan	Ingen plan	●	●	●	●	●	●	●
Testrapporten beskriver eventuelle forbedringsforslag	●	●	-	-	-	-	-	-	●	-	-	-

● Ja ● Delvist ● Nej ● Ikke relevant

Note: Ved "-" er kriteriet ikke vurderet, da nødplanen ikke er blevet testet.

Kilde: Rigsrevisionen på baggrund af dokumentation fra myndighederne.

Det fremgår af tabel 5, at det kun er Erhvervsstyrelsen, som har testet sin nødplan årligt. I den seneste testrapport fra Erhvervsstyrelsen er der beskrevet konkrete forbedringsforslag. Fx anbefales det, at styrelsen skal udarbejde en mere operationel nødplan for systemet. På den baggrund har Erhvervsstyrelsen udarbejdet en ny nødplan i marts 2023. Den nye nødplan er endnu ikke blevet testet. Erhvervsstyrelsen har oplyst, at styrelsen forventer at teste den nye nødplan i løbet af 2023.

DDoS-angreb
Et DDoS-angreb er et digitalt angreb, hvor en aktør med vilje fx overbelaster en hjemmeside, så siden ikke kan svare eller bryder sammen.

Kilde: Sikkerdigital.dk.

Myndighed 4 er i undersøgelsesperioden blevet ramt af et DDoS-angreb, som betød, at nødplanen for *system I* blev aktiveret. I den forbindelse blev der udarbejdet en hændelsesrapport, som dog kun beskriver den tekniske løsning. Myndighed 4 har derudover ikke testet nødplanerne for sine it-systemer.

Myndighed 3 og Søfartsstyrelsen har ikke testet nødplanerne for deres it-systemer.

5. Reetableringsplaner for it-systemerne

Delkonklusion

Hovedparten af reetableringsplanerne for it-systemerne er ikke tilfredsstillende. Fx mangler over halvdelen af reetableringsplanerne beskrivelser af, hvordan it-systemerne teknisk kan reetableres efter et større it-nedbrud. Det er kun Indenrigs- og Sundhedsministeriet, der har en tilfredsstillende reetableringsplan for sit it-system. For 2 af it-systemerne er der slet ikke udarbejdet reetableringsplaner.

Kun Indenrigs- og Sundhedsministeriet, Erhvervsstyrelsen og Søfartsstyrelsen har testet reetableringsplanerne for 3 af de udvalgte it-systemer. For de øvrige 9 it-systemer er det hverken blevet testet, om systemerne kan reetableres delvist, eller om systemerne kan reetableres fuldt efter et større it-nedbrud.

45. Dette kapitel handler om reetableringsplaner for it-systemerne. En reetableringsplan beskriver, hvordan et it-system teknisk reetableres efter et nedbrud.

46. Vi har undersøgt:

- om myndighederne for de udvalgte it-systemer har sikret, at der er implementeret tilfredsstillende reetableringsplaner, der indeholder en række centrale elementer
- om reetableringsplanerne er testet.

47. Ét udvalgt it-system hos myndighed 4 og alle udvalgte it-systemer hos Søfartsstyrelsen er ressortoverført til Statens It. Det betyder bl.a., at det er Statens It, som har ansvaret for at udarbejde reetableringsplaner for it-systemerne. Vi har derfor ikke undersøgt reetableringsplanerne for *system I, J, K* og *L*. Vi har dog undersøgt, om det er blevet testet, om it-systemerne kan reetableres, da det fortsat er myndighed 4 og Søfartsstyrelsen, der har ansvaret for at sikre, at dette bliver testet.

Statens It
Statens It leverer it-drift og servicer til ministerier, styrelser og selvejende uddannelsesinstitutioner. Statens It varetager også driftsansvaret for de it-systemer, der er ressortoverført fra statslige myndigheder.

5.1. Reetableringsplaner

48. Vi har gennemgået reetableringsplanerne for de udvalgte it-systemer for at vurdere, om planerne er tilfredsstillende. Vi har lagt til grund, at reetableringsplanerne skal indeholde 6 centrale elementer, som er baseret på ISO 27001, på Digitaliseringsstyrelsens anbefalinger til it-beredskabsplaner og på skabeloner til it-beredskabsplaner på sikkerdigital.dk. De centrale elementer kan enten fremgå af reetableringsplanen, kontrakten for systemet eller andre centrale dokumenter.

49. Figur 5 viser de 6 centrale elementer, som en tilfredsstillende reetableringsplan som minimum bør indeholde.

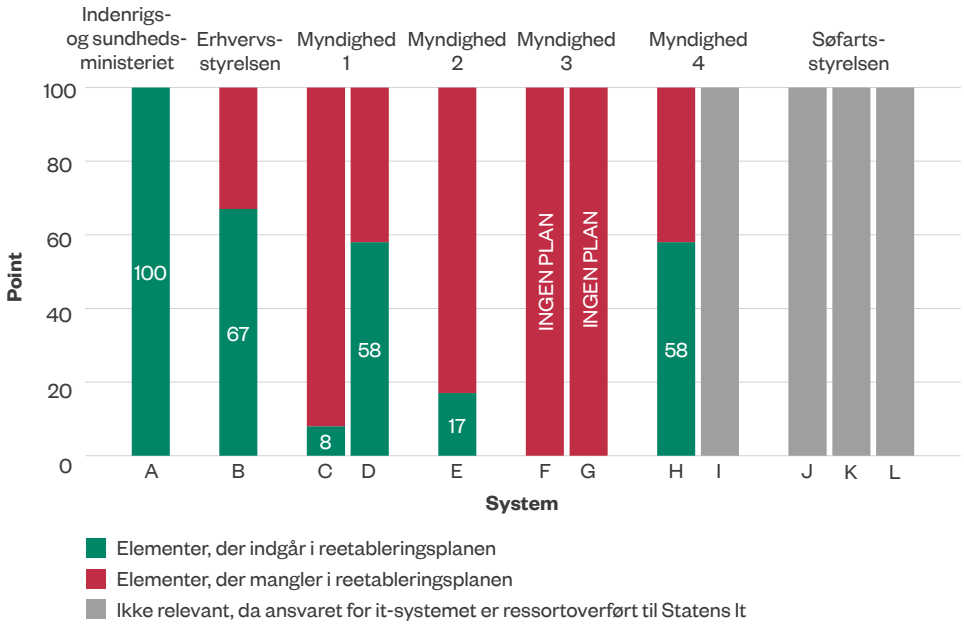
Figur 5
Centrale elementer i en reetableringsplan

Note: De centrale elementer kan enten fremgå af reetableringsplanen, kontrakten eller andre centrale dokumenter. I bilag 1 og 2 uddyber vi baggrunden for de revisionskriterier, som vi har anvendt til at vurderere reetableringsplanerne.

Kilde: Rigsrevisionen på baggrund af ISO 27001 og Digitaliseringsstyrelsens vejledning i it-beredskab.

50. Figur 6 viser Rigsrevisionens samlede vurdering af reetableringsplanerne for de udvalgte it-systemer på baggrund af de 6 centrale elementer.

Figur 6
Samlet vurdering af reetableringsplanerne for de udvalgte it-systemer



Kilde: Rigsrevisionen på baggrund af dokumentation fra myndighederne.

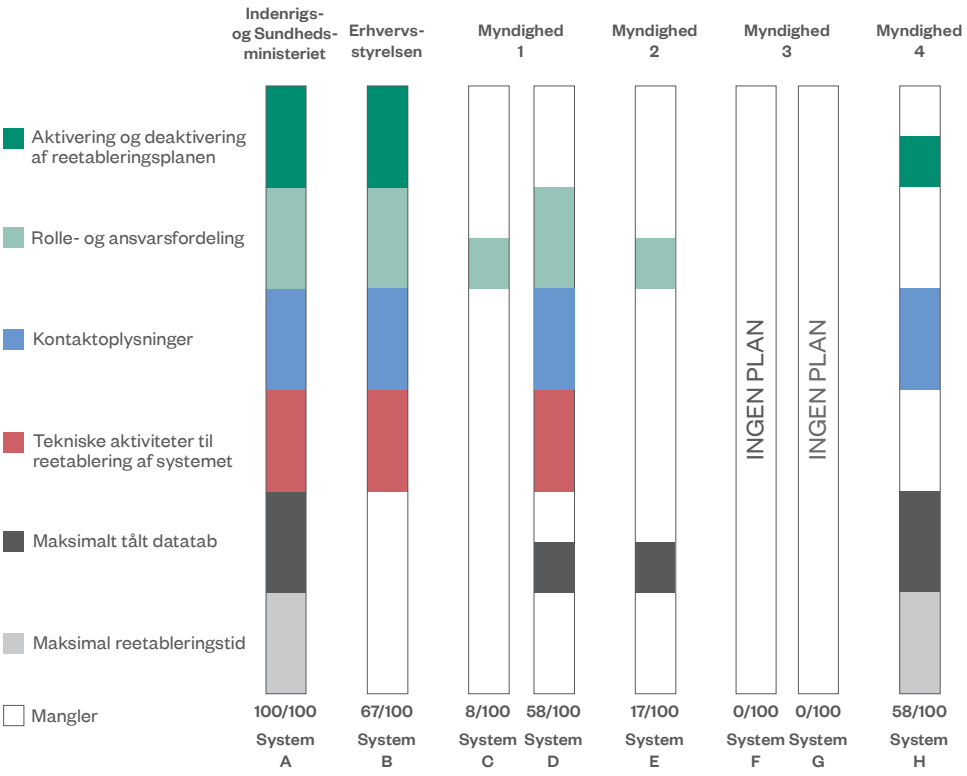
Det fremgår af figur 6, at der ikke er udarbejdet reetableringsplaner for *system F* og *G* hos myndighed 3.

51. I det følgende gennemgår vi Rigsrevisionens vurdering af reetableringsplanerne nærmere.

Sammenligning af reetableringsplaner
For at vi kan sammenligne myndighedernes reetableringsplaner, har vi tildelt reetableringsplanerne point efter, hvor mange af de 6 centrale elementer der indgår i planerne. En reetableringsplan opnår en score på 100 point, hvis planen indeholder alle 6 elementer. Vi har vægtet de 6 elementer ligeligt, og myndighederne kan derfor opnå en score på maks. 16,7 point for hvert element. I figur 6 og 7 har vi dog afrundet til nærmeste hele tal.

52. Figur 7 viser, om reetableringsplanerne indeholder de 6 centrale elementer. Manglerne i reetableringsplanerne er illustreret ved hvide felter.

Figur 7
Reetableringsplaner for myndighedernes it-systemer



Kilde: Rigsrevisionen på baggrund af dokumentation fra myndighederne.

Det fremgår af figur 7, at reetableringsplanen for Indenrigs- og Sundhedsministeriets *system A* indeholder alle de 6 centrale elementer, som bør indgå i en reetableringsplan.

Reetableringsplanerne for de øvrige it-systemer mangler flere af de centrale elementer, som bør indgå i en reetableringsplan. Som det fremgår af figuren, er det særligt 3 af de centrale elementer, som mangler i flere af reetableringsplanerne: *aktivering og deaktivering af reetableringsplanen, tekniske aktiviteter til reetablering af it-systemet* og *maksimal reetableringstid*.

Det fremgår desuden af figuren, at Erhvervsstyrelsens reetableringsplan for *system B* mangler 2 af de centrale elementer, som en reetableringsplan bør indeholde. Undersøgelsen viser, at der først i marts 2023 er udarbejdet en reetableringsplan for systemet. Erhvervsstyrelsen har oplyst, at styrelsens eksterne it-leverandør har beskrivelser af aktiviteterne til reetablering af systemet, men at beskrivelserne er fortrolige. Rigsrevisionen har derfor ikke haft adgang til leverandørens beskrivelser i undersøgelsen.

Undersøgelsen viser desuden, at reetableringsplanerne for *system C* og *D* hos myndighed 1 og *system E hos* myndighed 2 er særdeles mangelfulde. Fx er der for 2 af systemerne ikke beskrivelser af tekniske aktiviteter til reetablering af systemerne.

Årlig ajourføring

53. Vi har undersøgt, om reetableringsplanerne for it-systemerne er ajourført årligt. Det er vigtigt, at reetableringsplanerne løbende ajourføres for at sikre, at planerne indeholder de korrekte oplysninger. Vi har lagt til grund, at reetableringsplaner for samfundskritiske it-systemer som minimum skal ajourføres én gang årligt for at sikre, at fx kontaktoplysninger på nøglepersoner er korrekte.

54. Undersøgelsen viser, at det kun er Indenrigs- og Sundhedsministeriet, der har ajourført reetableringsplanen for *system A* årligt i perioden januar 2020 - marts 2023, men den seneste reetableringsplan er dog ikke ajourført korrekt.

Reetableringsplanerne for *system C* og *E* er blevet ajourført i løbet af undersøgelsesperioden, men planerne er meget mangelfulde. For Erhvervsstyrelsens it-system er der først udarbejdet en reetableringsplan i marts 2023. Reetableringsplanen for *system D* er slet ikke opdateret i undersøgelsesperioden. Reetableringsplanen for *system H* er først blevet udarbejdet i 2021 og er derefter blevet ajourført årligt.

Myndighedernes leverandørstyring

55. *System A* hos Indenrigs- og Sundhedsministeriet, *system B* hos Erhvervsstyrelsen og *system F* hos myndighed 3 driftes af eksterne leverandører. Det er de eksterne leverandører, der udarbejder reetableringsplaner for it-systemerne og tester planerne, men det er myndighedernes ansvar at stille krav i kontrakterne til leverandørernes it-beredskab, herunder reetableringsplaner og test af planerne. Derudover bør myndighederne stille krav om, at leverandørerne får udarbejdet it-revisorerklæringer for it-systemerne, som omhandler leverandørens it-beredskab.

56. Undersøgelsen viser, at Indenrigs- og Sundhedsministeriet har sikret sig adgang til leverandørens reetableringsplaner og testrapporter for *system A*. Ministeriet har desuden årligt fået udarbejdet systemspecifikke it-revisorerklæringer.

Undersøgelsen viser også, at Erhvervsstyrelsen ikke har stillet krav til leverandørens it-beredskab og heller ikke har modtaget systemspecifikke it-revisorerklæringer for *system B*.

Myndighed 3 har ikke stillet krav i kontrakten til leverandørens it-beredskab for *system F*, og der er ikke udarbejdet systemspecifikke it-revisorerklæringer vedrørende it-beredskabet.

It-revisorerklæring
En it-revisorerklæring er et redskab for myndigheden til at få viden om leverandørens it-miljø, herunder leverandørens it-beredskab. Revisorerklæringen kan enten være en ISAE 3402-erklæring eller en ISAE 3000-erklæring og skal omhandle det specifikke it-system. I begge typer erklæringer udtaler en ekstern revisor sig om, hvorvidt leverandørens it-kontroller er hensigtsmæssigt udformet, og om kontrollerne har fungeret tilfredsstillende i en given periode.

5.2. Test af reetableringsplaner

57. Vi har undersøgt, om myndighederne har sikret, at reetableringsplanerne er testet i perioden januar 2020 - marts 2023. Beredskabsplaner skal testes, trænes og evalueres for at sikre viden om, hvordan beredskabsplanerne virker i en konkret beredskabssituation, og for at sikre, at it-systemerne kan reetableres i tilfælde af nedbrud på systemerne. Test af reetableringsplanerne er således en vigtig del af it-beredskabet. Vi har med udgangspunkt i ISO 27001 undersøgt:

- om der i undersøgelsesperioden er udført en fuld reetableringstest, herunder om der er fulgt op på, hvor lang tid det tager at reetablere it-systemet, og om systemet fungerer efter reetablering
- om der er udført delvise tests af reetableringsplanen årligt.

58. Af boks 1 fremgår de 2 typer af reetableringstests, som vi har undersøgt.

Boks 1
Forskellige tests

Fuld reetableringstest
En fuld reetableringstest er en test, hvor it-systemet reetableres på baggrund af den seneste fulde backup, fx på en tom server i et testmiljø e.l., så det almindelige driftsmiljø ikke påvirkes ved testen. En fuld reetableringstest bør omfatte tests af, at it-systemet fungerer sammen med de øvrige komponenter i it-infrastrukturen. Omfanget af tests med den øvrige it-infrastruktur vil variere, afhængigt af om it-systemet driftes internt i myndigheden eller hos en ekstern leverandør. Testen kaldes også en disaster recovery test.

Delvis reetableringstest
En delvis reetableringstest er en test af reetablering af dele af it-systemet (en delmængde af en fuld test), fx at genskabe en database. Testen kaldes også en restore test.

59. For *system I* hos myndighed 4 og for de 3 it-systemer (*system J, K* og *L*) hos Søfartsstyrelsen, som er ressortoverført til Statens It, er det de 2 myndigheders ansvar at sikre, at det er testet, om systemerne kan reetableres. Vi har derfor undersøgt, om myndighed 4 og Søfartsstyrelsen har bestilt delvise tests og fulde tests af reetablering af deres it-systemer hos Statens It.

60. Tabel 6 viser Rigsrevisionens gennemgang af myndighedernes tests af reetableringen af de udvalgte it-systemer i perioden januar 2020 - marts 2023.

Tabel 6
Rigsrevisionens gennemgang af myndighedernes tests af reetableringsplaner

	Indenrigs- og Sundheds-ministeriet	Erhvervs-styrelsen	Myndighed 1		Myndighed 2	Myndighed 3		Myndighed 4		Søfarts-styrelsen		
It-system	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
Der er udført en fuld reetableringstest	🟡	🟡	🔴	🔴	🔴	Ingen plan	Ingen plan	🔴	🔴	🔴	🔴	🔴
Der er udført en delvis reetableringstest årligt	🟢	🟡	🔴	🔴	🔴	Ingen plan	Ingen plan	🔴	🔴	🔴	🟡	🔴

🟢 Ja 🟡 Delvist 🔴 Nej

Kilde: Rigsrevisionen på baggrund af dokumentation fra myndighederne.

Fuld reetableringstest

61. Som det fremgår af tabel 6, er der kun udført fulde reetableringstests af *system A* og *B*. De 2 tests har dog ikke været fyldestgørende.

Indenrigs- og Sundhedsministeriet har udført en fuld reetableringstest af *system A*, men ministeriet har ikke testet, hvor lang tid det tager at reetablere systemet, eller om systemets funktionalitet virker, som det skal, efter reetablering.

Erhvervsstyrelsen har også udført en fuld reetableringstest af *system B*, men har ikke testet, at systemets funktionalitet fungerer, fx integrationen til andre systemer. Styrelsen har således testet, at data kan genskabes i systemet, men har ikke testet, at data kan tilgås efter en reetablering via et af de programmer, som styrelsen normalt anvender til at læse data.

For 10 ud af 12 it-systemer er der dermed ikke udført en fuld reetableringstest i undersøgelsesperioden. Det betyder, at myndighederne for de 10 it-systemer ikke har sikkerhed for, at de kan reetablere systemerne, så de virker efter et nedbrud. Søfartsstyrelsen har dog oplyst, at styrelsen efter undersøgelsesperioden har gennemført en fuld reetableringstest i forbindelse med en opgradering af *system J*.

Delvis reetableringstest

62. Det fremgår af tabel 6, at der for 3 ud af 12 it-systemer er udført en delvis reetableringstest i undersøgelsesperioden. Kun Indenrigs- og Sundhedsministeriet har hvert år udført delvise reetableringstests af *system A*. Erhvervsstyrelsen og Søfartsstyrelsen har for *system B* og *K* gennemført delvise reetableringstests i undersøgelsesperioden, dog ikke hvert år.

For de resterende 9 it-systemer er der ikke udført delvise reetableringstests. Myndighederne har dermed ikke sikkerhed for, at de kan genskabe data i it-systemerne i tilfælde af et nedbrud på et af systemerne.

Rigsrevisionen, den 23. november 2023

Birgitte Hansen

/Niels Kjøller Petersen

Bilag 1. Metodisk tilgang

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. Derfor har vi undersøgt følgende:

- Har staten et tilfredsstillende grundlag for at etablere et it-beredskab for de udvalgte samfundskritiske it-systemer?
- Har staten implementeret tilfredsstillende krisestyringsplaner for de udvalgte samfundskritiske it-systemer?
- Har staten implementeret tilfredsstillende nødplaner for de udvalgte samfundskritiske it-systemer?
- Har staten sikret, at der er implementeret tilfredsstillende reetableringsplaner for de udvalgte samfundskritiske it-systemer?

I undersøgelsen indgår 7 myndigheder: Indenrigs- og Sundhedsministeriet, Erhvervsstyrelsen og Søfartsstyrelsen under Erhvervsministeriet samt 4 andre anonymiserede myndigheder.

Undersøgelsen bygger på en gennemgang af dokumenter. Vi har desuden holdt møder med de undersøgte ministerier og myndigheder. Vi har holdt møder med:

- myndighederne om afhængigheder til andre it-systemer og risikovurderinger af de udvalgte samfundskritiske it-systemer
- systemansvarlige og forretningsansvarlige mv. fra de undersøgte myndigheder, som har ansvaret for it-beredskabet for de udvalgte samfundskritiske it-systemer
- ministerierne om tilsynet med informationssikkerhed, herunder it-beredskabet.

Formålet med møderne har været at stille spørgsmål til det udleverede materiale og at få en dybere forståelse af de forhold, vi har undersøgt.

Undersøgelsen omhandler perioden fra januar 2020 til og med marts 2023. Vi har dog primært behandlet og vurderet de seneste risikovurderinger, krisestyringsplaner, nødplaner, reetableringsplaner og tests i undersøgelsen.

Nedenfor beskrives vores kvalitetssikring og metode mere detaljeret.

Udvælgelse af samfundskritiske it-systemer

For at undersøge it-beredskabet i staten har vi valgt at gå i dybden med it-beredskabet for myndigheder, som har ansvaret for it-systemer, der er nødvendige for at kunne opretholde samfundskritiske opgaver.

På den baggrund har vi udvalgt it-systemer hos Indenrigs- og Sundhedsministeriet, Erhvervsstyrelsen og Søfartsstyrelsen samt hos 4 myndigheder (myndighed 1, 2, 3 og 4), som er anonymiseret i beretningen. For hver myndighed har vi udvalgt en række samfundskritiske it-systemer. På tværs af staten er ca. 90 it-systemer vurderet som samfundskritiske af myndighederne selv. Vi har udvalgt 12 af de 90 it-systemer.

Grundlaget for undersøgelsens revisionskriterier

Undersøgelsens revisionskriterier tager udgangspunkt i de internationale standarder for informationssikkerhed ISO 27001:2017 og ISO 27002:2017. Med *National strategi for cyber- og informationssikkerhed 2015-2016* skal alle offentlige myndigheder følge ISO 27001.

ISO 27001:2017 består af et hovedafsnit, der beskriver de ledelsesprocesser, som myndigheden skal implementere for at leve op til standarden. Hertil hører Anneks A, der beskriver en række kontrolmål inden for informationssikkerhed med underliggende kontroller. De enkelte kontroller bør implementeres, hvis myndighederne vurderer, at kontrollerne er nødvendige. Flere af kontrolmålene er relevante i forhold til it-beredskabet, og område 17 i Anneks A vedrører it-beredskabet. Under område 17 er der 3 kontroller, som fastsætter de overordnede krav til myndighedernes it-beredskab. ISO 27002:2017 er en vejledning i den praktiske udmøntning af kontrollerne i Anneks A til ISO 27001.

Der er i 1. kvartal 2022 kommet en ny og opdateret version af ISO 27001 (ISO 27001: 2022). Statslige myndigheder har fra udgivelsestidspunktet 12 måneder til at implementere den opdaterede version. Implementeringsperioden har dermed varet indtil 1. kvartal 2023. Det har derfor ikke været relevant for Rigsrevisionen at lægge denne version til grund for undersøgelsen.

I kapitel 2 om myndighedernes grundlag for it-beredskabet er ISO 27001 udgangspunktet for vores revisionskriterier. Det fremgår fx af ISO 27001, at myndighederne ved planlægningen af informationssikkerheden, herunder it-beredskabet, skal tage udgangspunkt i risici, som skal vurderes i forhold til en række trusler, konsekvenser og sandsynligheder. Som det fremgår af Digitaliseringsstyrelsens *Vejledning til risikostyring inden for informationssikkerhed*, skal risikovurderinger gøre ledelsen bekendt med de aktuelle risici, så organisationen ikke udsætter sig for større risici, end hvad der er acceptabelt. Derfor har vi lagt til grund, at risikovurderingerne skal være i en form, hvor ledelsen kan forholde sig til og agere på de identificerede trusler og sårbarheder. Derfor er det ikke tilstrækkeligt alene med talvurderinger uden yderligere forklaringer i risikovurderingen.

Revisionskriteriet vedrørende ministeriernes tilsyn med informationssikkerheden på ministerområderne bygger på Digitaliseringsstyrelsens vejledning *Departementets tilsyn med informationssikkerhed på ministerområdet*. Derudover bygger revisionskriteriet også på ISO 27001, pkt. A.18.2, hvoraf det fremgår, at myndighedernes metode til styring af informationssikkerhed og implementering heraf med jævne mellemrum eller i tilfælde af væsentlige ændringer skal gennemgås af en uafhængig part. Oftest vil det være ministeriernes departementer, der udfører tilsynet med deres underliggende myndigheder, men ministerierne kan uddelegere tilsynet til en underliggende myndighed eller oprette interne tilsynsenheder i departementerne.

Af Digitaliseringsstyrelsens vejledning fremgår beredskabsplanlægning som et emne, som ministerierne kan vælge at stille spørgsmål til i forbindelse med tilsynet. Det fremgår ikke, hvor ofte de forskellige dele af informationssikkerheden skal indgå i tilsynet. I vores undersøgelse har vi lagt til grund, at ministeriernes tilsyn som minimum inden for en 3-årig periode bør omhandle myndighedernes it-beredskab for samfundskritiske it-systemer.

I kapitel 3, 4 og 5 om krisestyringsplaner, nødplaner og reetableringsplaner for it-systemerne tager vores revisionskriterier udgangspunkt i ISO 27001. Det fremgår af ISO 27001, pkt. A.17.1, at myndighederne skal udarbejde og teste processer og procedurer, herunder beredskabsplaner, for at sikre informationskontinuitet i en kritisk situation. ISO 27001 er konkretiseret i Digitaliseringsstyrelsens vejledning på sikkerdigital.dk og i Digitaliseringsstyrelsens vejledninger og skabeloner til, hvordan myndighederne i praksis skal implementere et it-beredskab. Disse vejledninger og skabeloner er ligeledes udgangspunktet for vores revisionskriterier.

For nogle af vores revisionskriterier i undersøgelsen er ISO 27001 og vejledningerne for generelle eller forholder sig til beredskabet på et mere overordnet niveau. For disse revisionskriterier har det derfor været nødvendigt at konkretisere, hvad vi har lagt til grund for vores vurderinger. Vi har derfor også fastsat revisionskriterierne ud fra en rimelighedsbetragtning og ud fra en konkret vurdering af, hvad der er god praksis på området. I bilag 2 findes en liste over ophænget til de revisionskriterier, som vi har anvendt til at vurdere de undersøgte myndigheders it-beredskabsplaner og myndighedernes tests af planerne.

Væsentlige dokumenter i undersøgelsen

Vi har gennemgået en række dokumenter, herunder:

- myndighedernes dokumentation af de udvalgte it-systemers afhængigheder til andre it-systemer
- procesbeskrivelser eller politikker for risikovurdering samt risikovurderinger af de udvalgte samfundskritiske it-systemer
- it-beredskabsplaner, herunder krisestyringsplaner, nødplaner, reetableringsplaner og tests af de 3 typer af it-beredskabsplaner
- it-revisorerklæringer (ISAE 3402-erklæringer eller ISAE 3000-erklæringer) og kontraktbilag vedrørende it-beredskabet for de udvalgte it-systemer i perioden januar 2020 - marts 2023
- tilsynsrapporter om informationssikkerhed for de undersøgte myndigheder
- ISO 27001:2017 og ISO 27002:2017 om informationssikkerhed, herunder it-beredskab
- Digitaliseringsstyrelsens og sikkerdigital.dk's vejledninger om it-beredskab.

Metode til vurdering af beredskabsplaner

Vi har i vores gennemgang af krisestyringsplaner, nødplaner og reetableringsplaner vurderet planerne ud fra en række elementer, som vi vurderer er de mest centrale elementer, der som minimum bør indgå i en it-beredskabsplan. Elementerne foreslås som kontroller i Anneks A til ISO 27001 eller i Digitaliseringsstyrelsens vejledninger om beredskabsplaner.

Vi er opmærksomme på, at myndighederne kan strukturere it-beredskabet på forskellige måder og derfor kan have en anden opdeling af it-beredskabsplanerne eller have andre betegnelser for it-beredskabsplanerne end krisestyringsplaner, nødplaner og reetableringsplaner. Vi har i undersøgelsen drøftet med de undersøgte myndigheder, hvilke af deres planer der kan karakteriseres som henholdsvis krisestyringsplaner, nødplaner og reetableringsplaner.

I ISO 27001 og i Digitaliseringsstyrelsens vejledninger indgår der flere anbefalinger til it-beredskabet end de elementer, som vi har udvalgt. Vi har vurderet, hvilke elementer der er de mest centrale, og som it-beredskabsplanerne som minimum bør indeholde for at være tilfredsstillende. I bilag 2 har vi oplistet alle de elementer, som indgår i vores vurdering af krisestyringsplaner, nødplaner, reetableringsplaner og tests af planerne, og vi har redegjort for, hvor elementerne stammer fra. For både krisestyringsplaner og reetableringsplaner har vi undersøgt de samme elementer, som blev undersøgt i Rigsrevisionens beretning om statens it-beredskab fra november 2022.

For bedre at kunne sammenligne henholdsvis krisestyringsplaner og reetableringsplaner og på en enkel måde formidle vores vurdering af indholdet af planerne, har vi valgt at tildele planerne point efter, hvor mange af de udvalgte centrale elementer der indgår i planerne. Vi har undersøgt 5 centrale elementer for krisestyringsplanerne og 6 centrale elementer for reetableringsplanerne. En krisestyringsplan opnår en score på 100 point, hvis planen indeholder alle 5 elementer, og en reetableringsplan opnår en score på 100 point, hvis planen indeholder alle 6 elementer. Vi har vægtet elementerne i både krisestyringsplanerne og reetableringsplanerne lige højt, da de alle er vigtige, for at myndighederne har tilfredsstillende krisestyringsplaner og reetableringsplaner. Hvert af de 5 elementer i krisestyringsplanerne vægter 20 point ud af 100 point, mens hvert af de 6 elementer i reetableringsplanerne vægter 16,7 point ud af 100 point. Hvis vi har vurderet, at indholdet og omfanget af et element ikke er helt tilstrækkeligt, har vi tildelt elementet halvdelen af den mulige score, dvs. en score på 10 point for krisestyringsplanerne og en score på 8,35 point for retableringsplanerne. Det kan fx være, at der mangler oplysninger i beskrivelsen af de nødvendige aktiviteter for at reetablere it-systemet eller i beskrivelsen af rolle- og ansvarsfordelingen.

For de it-systemer, der er driftet af en ekstern leverandør, har vi ud over reetableringsplanen bl.a. gennemgået kontrakten med leverandøren. Det skyldes, at nogle af de centrale elementer kan fremgå af andre dokumenter, som myndighederne og eventuelle leverandører vil benytte i en beredskabssituation.

Ifølge ISO 27001 skal myndighederne regelmæssigt overvåge, gennemgå og auditere leverandørydelser. Vi har derfor lagt til grund, at myndighederne som en del af tilsynet med leverandørerne også bør stille krav om, at leverandørerne hvert år får et revisionsfirma til at udarbejde it-revisorerklæringer for de samfundskritiske it-systemer. Revisorerklæringerne afdækker, om leverandørerne lever op til kravene i kontrakten, herunder kravene til leverandørernes it-beredskab. Revisorerklæringerne kan udarbejdes, så de omhandler et specifikt it-system.

For ét af systemerne hos myndighed 4 og for de 3 it-systemer hos Søfartsstyrelsen er driftsansvaret for it-systemerne, herunder ansvaret for reetableringsplanerne, blevet ressortoverført til Statens It. Det er derfor ikke myndighed 4 og Søfartsstyrelsen, men Statens It, der har ansvaret for at sikre en tilfredsstillende reetableringsplan. Det betyder, at de 2 myndigheder ikke er involveret i arbejdet med at udarbejde reetableringsplaner, der gælder for de systemer, som Statens It har driftsansvaret for. Derfor har vi ikke undersøgt reetableringsplanerne for disse 4 it-systemer. I forhold til test er det dog fortsat myndighed 4 og Søfartsstyrelsen, der har ansvaret for at sikre, at det er testet, om it-systemerne kan reetableres. Det sikrer de ved at bestille tests hos Statens It.

I kapitel 2, 3, 4 og 5 har vi anvendt grøn, gul og rød til at vise resultatet af vores undersøgelse. Fx har vi undersøgt indholdet af tests af krisestyringsplaner, nødplaner og reetableringsplaner. Grøn angiver, at vi har vurderet, at kriteriet er opfyldt. Rød angiver, at kriteriet ikke er opfyldt. Gul angiver, at kriteriet delvist er opfyldt. Et element er vurderet som delvist opfyldt, hvis det fx findes i testen, men ikke er tilstrækkeligt beskrevet i indhold og omfang.

Test af it-beredskabsplanerne

Ifølge ISO 27001 skal myndighederne teste beredskabsplanerne regelmæssigt. Vi har lagt til grund, at det er vigtigt, at myndighederne løbende træner it-beredskabet, herunder sikrer, at procedurer og oplysninger i beredskabsplanerne er ajour. På den baggrund har vi undersøgt, om it-beredskabsplanerne (krisestyringsplaner, nødplaner og reetableringsplaner) er blevet testet årligt.

Vurderingen af test af krisestyringsplaner, nødplaner og reetableringsplaner bygger på en gennemgang af de seneste testrapporter. Hvis der har været større it-hændelser, hvor beredskabsplanerne er blevet aktiveret, indgår hændelsesrapporter og evalueringer af hændelseshåndteringen i vores vurderinger af test af it-beredskabet.

I forhold til test af reetablering af systemerne har vi lagt til grund, at det for samfundskritiske it-systemer ikke er tilstrækkeligt at udføre tests, som kun vedrører reetablering af dele af it-systemet (restore tests), men at der også bør udføres fulde reetableringstests, hvor hele it-systemet reetableres (disaster recovery tests). Ved en fuld test reetableres hele it-systemet på baggrund af den seneste fulde backup, og den maksimale reetableringstid og systemets funktionalitet efter reetablering testes. En fuld test bør foretages på en tom server eller på ny hardware, så det almindelige driftsmiljø ikke påvirkes ved testen. Ved flere datacentre testes også switch mellem datacentre for at sikre en optimal oppetid.

Ifølge ISO 27001 skal risikovurderingerne danne grundlag for ledelsens beslutning om, hvor ofte der er behov for at teste it-beredskabet. Det fremgår ikke af risikovurderingerne af de udvalgte it-systemer, hvor ofte der bør foretages fulde reetableringstests. For enkelte af de udvalgte it-systemer følger det af risikovurderingerne eller af kontraktgrundlagene med leverandørerne, at reetableringsplanerne skal testes regelmæssigt. I Digitaliseringsstyrelsens vejledninger er der ikke anbefalinger til, hvor ofte der bør foretages en fuld reetableringstest af it-systemerne. Ved samfundskritiske it-systemer er det særligt vigtigt, at man har viden om, hvorvidt reetableringsplanerne virker efter hensigten. Da det kan være omfattende at foretage en fuld reetableringstest, og da der ikke er fastsat specifikke anbefalinger eller krav i Digitaliseringsstyrelsens vejledninger, har vi undersøgt, om der er foretaget en fuld reetableringstest inden for en 3-årig periode.

Derudover har vi undersøgt, om der som en del af en fuld test af reetableringsplanen følges op på, hvor lang tid det tager at reetablere hele it-systemet. Ligeledes har vi undersøgt, om det som led i testen tjekkes, om systemets funktionalitet virker, som det skal, efter reetablering, fx om integrationer med andre it-systemer fungerer.

Kvalitetssikring

Denne undersøgelse er kvalitetssikret via vores interne procedurer for kvalitetssikring, som omfatter høring hos de reviderede myndigheder samt ledelsesbehandling og sparring på forskellige tidspunkter i undersøgelsesforløbet med chefer og medarbejdere i Rigsrevisionen med relevante kompetencer.

Standarderne for offentlig revision

Revisionen er udført i overensstemmelse med standarderne for offentlig revision, herunder standarderne for større undersøgelser (SOR 3). Standarderne fastlægger, hvad brugerne og offentligheden kan forvente af revisionen, for at der er tale om en god faglig ydelse. Standarderne er baseret på de grundlæggende revisionsprincipper i Rigsrevisionernes internationale standarder (ISSAI 100-999).

Bilag 2. Undersøgelsens revisionskriterier

Tabel A-D viser, hvilke revisionskriterier vi har anvendt til at vurdere indholdet af it-beredskabsplanerne og myndighedernes tests af planerne. Desuden viser tabellerne hvor revisionskriterierne stammer fra.

Tabel A
Revisionskriterier til at vurdere myndighedernes it-beredskabsplaner

Elementer, som vi har undersøgt i it-beredskabsplanerne	Krisestyringsplan	Nødplan	Reetableringsplan	Ophæng til revisionskriterier
Planen er ajourført årligt	X	X	X	• Baseret på ISO 27001 og ISO 27002 • Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet drift • Digitaliseringsstyrelsens vejledning i it-beredskab.
Planen beskriver, hvornår og af hvem it-beredskabet den aktiveres	X		X	• Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet drift • Digitaliseringsstyrelsens vejledning i it-beredskab.
Planen beskriver, hvornår it-beredskabet deaktiveres			X	• Rigsrevisionens kriterie. Det er vigtigt, at det er aftalt, hvornår man vender tilbage til normal drift.
Planen indeholder kontaktoplysninger på interne og eksterne nøglepersoner, herunder hos eventuel it-leverandør	X		X	• Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet drift • Digitaliseringsstyrelsens vejledning i it-beredskab.
Planen beskriver rolle- og ansvarsfordelingen internt i myndigheden samt for eventuel it-leverandør	X		X	• Sikkerdigital.dk (beredskabsstyring/implementering) • Digitaliseringsstyrelsens vejledning i it-beredskab.
Planen indeholder beskrivelser af, hvornår og hvordan der kommunikeres til interne og eksterne aktører	X			• Digitaliseringsstyrelsens guide til kommunikation i en beredskabssituation.
Planen er fysisk tilgængelig	X	X		• Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet drift.
Der er krav til den maksimale reetableringstid i reetableringsplanen, i kontrakten med eventuel leverandør eller i andre centrale dokumenter			X	• Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet drift • Digitaliseringsstyrelsens vejledning i it-beredskab.
Der er krav til det maksimalt tålte datatab i reetableringsplanen, i kontrakten med eventuel leverandør eller i andre centrale dokumenter			X	• Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet drift • Digitaliseringsstyrelsens vejledning i it-beredskab.
Planen beskriver, hvilke tekniske aktiviteter der er nødvendige for at reetablere it-systemet			X	• Baseret på ISO 27001 og ISO 27002.
Planen beskriver, hvilke procedurer der skal iværksættes for at opretholde kritiske opgaver og forretningsprocesser		X		• Baseret på ISO 27001 og ISO 27002.

Note: X angiver de it-beredskabsplaner, hvor elementet er undersøgt.

Tabel B

Revisionskriterier til at vurdere test af krisestyringsplaner

Elementer, som vi har undersøgt ved test af krisestyringsplaner	Ophæng til revisionskriterier
Krisestyringsplanen er testet årligt i perioden fra januar 2020 til og med marts 2023	• Baseret på ISO 27001 og ISO 27002 • Digitaliseringsstyrelsens vejledning i it-beredskab • Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet drift.
Resultater af testen fremgår af testrapporten	• Rigsrevisionens kriterie baseret på ISO 27001 og ISO 27002. Ifølge ISO 27001 skal myndighederne afprøve og teste, om beredskabsplanerne virker. For at sikre læring, som kan indgå i opdaterede planer, finder Rigsrevisionen, at resultaterne af testen skal fremgå af testrapporten.
Testrapporten beskriver eventuelle forbedringsforslag	• Digitaliseringsstyrelsens vejledning i it-beredskab.

Tabel C

Revisionskriterier til at vurdere test af nødplaner

Elementer, som vi har undersøgt ved test af nødplaner	Ophæng til revisionskriterier
Nødplanen er testet årligt i perioden fra januar 2020 til og med marts 2023	• Baseret på ISO 27001 og ISO 27002 • Digitaliseringsstyrelsens vejledning i it-beredskab • Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet drift.
Testrapporten beskriver eventuelle forbedringsforslag	• Digitaliseringsstyrelsens vejledning i it-beredskab.

Tabel D

Revisionskriterier til at vurdere test af reetableringsplanerne

Elementer, som vi har undersøgt ved test af reetableringsplaner	Ophæng til revisionskriterier
Reetablering af it-systemet er blevet testet årligt i perioden fra januar 2020 til og med marts 2023	• Baseret på ISO 27001 og ISO 27002 • Digitaliseringsstyrelsens vejledning i it-beredskab • Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet drift.
Der er udført fulde og delvise tests af reetablering af it-systemet	• Rigsrevisionens kriterie baseret på ISO 27001 og ISO 27002. Yderligere beskrivelse af Rigsrevisionens kriterie om test af reetableringen af systemerne fremgår af bilag 1 i afsnittet om test af it-beredskabsplanerne.

Bilag 3. Myndighedernes samlede resultater

Tabel E

Indenrigs- og Sundhedsministeriet

		System A
Grundlaget for it-beredskabet	Systemafhængighederne er kortlagt	●
	Der er udarbejdet risikovurderinger, som indeholder vurderinger af sårbarheder, trusler, konsekvenser og sandsynligheder	●
Krisestyringsplan	Krisestyringsplanens pointscore	100/100
	Krisestyringsplanen er testet årligt	●
Nødplan[1)]	-	-
Reetableringsplan	Reetableringsplanens pointscore	100/100
	Der er udført en fuld reetableringstest	●
	Der er udført en delvis reetableringstest årligt	●

● Ja ● Delvist ● Nej

[1)] Nødplan er ikke relevant, da myndigheden ikke selv er bruger af it-systemet.

Kilde: Rigsrevisionen på baggrund af oplysninger fra Indenrigs- og Sundhedsministeriet.

Tabel F

Erhvervsstyrelsen

		System B
Grundlaget for it-beredskabet	Systemafhængighederne er kortlagt	●
	Der er udarbejdet risikovurderinger, som indeholder vurderinger af sårbarheder, trusler, konsekvenser og sandsynligheder	●
Krisestyringsplan	Krisestyringsplanens pointscore	100/100
	Krisestyringsplanen er testet årligt	●
Nødplan	Nødplanen beskriver, hvilke procedurer der skal iværksættes for at opretholde kritiske opgaver og forretningsprocesser	●
	Nødplanen er testet årligt	●
Reetableringsplan	Reetableringsplanens pointscore	67/100
	Der er udført en fuld reetableringstest	●
	Der er udført en delvis reetableringstest årligt	●

● Ja ● Delvist ● Nej

Kilde: Rigsrevisionen på baggrund af oplysninger fra Erhvervsstyrelsen.

Tabel G

Myndighed 1

		System C	System D
Grundlaget for it-beredskabet	Systemafhængighederne er kortlagt	●	●
	Der er udarbejdet risikovurderinger, som indeholder vurderinger af sårbarheder, trusler, konsekvenser og sandsynligheder	●	●
Krisestyringsplan	Krisestyringsplanens pointscore	20/100	20/100
	Krisestyringsplanen er testet årligt	●	●
Nødplan	Nødplanen beskriver, hvilke procedurer der skal iværksættes for at opretholde kritiske opgaver og forretningsprocesser	Ingen plan	Ingen plan
	Nødplanen er testet årligt	Ingen plan	Ingen plan
Reetableringsplan	Reetableringsplanens pointscore	8/100	58/100
	Der er udført en fuld reetableringstest	●	●
	Der er udført en delvis reetableringstest årligt	●	●

● Ja ● Delvist ● Nej

Kilde: Rigsrevisionen på baggrund af oplysninger fra myndighed 1.

Tabel H

Myndighed 2

		System E
Grundlaget for it-beredskabet	Systemafhængighederne er kortlagt	●
	Der er udarbejdet risikovurderinger, som indeholder vurderinger af sårbarheder, trusler, konsekvenser og sandsynligheder	●
Krisestyringsplan	Krisestyringsplanens pointscore	90/100
	Krisestyringsplanen er testet årligt	●
Nødplan	Nødplanen beskriver, hvilke procedurer der skal iværksættes for at opretholde kritiske opgaver og forretningsprocesser	Ingen plan
	Nødplanen er testet årligt	Ingen plan
Reetableringsplan	Reetableringsplanens pointscore	17/100
	Der er udført en fuld reetableringstest	●
	Der er udført en delvis reetableringstest årligt	●

● Ja ● Delvist ● Nej

Kilde: Rigsrevisionen på baggrund af oplysninger fra myndighed 2.

Tabel I
Myndighed 3

		System F	System G
Grundlaget for it-beredskabet	Systemafhængighederne er kortlagt	●	●
	Der er udarbejdet risikovurderinger, som indeholder vurderinger af sårbarheder, trusler, konsekvenser og sandsynligheder	●	●
Krisestyringsplan	Krisestyringsplanens pointscore	80/100	80/100
	Krisestyringsplanen er testet årligt	●	●
Nødplan	Nødplanen beskriver, hvilke procedurer der skal iværksættes for at opretholde kritiske opgaver og forretningsprocesser	●	●
	Nødplanen er testet årligt	●	●
Reetableringsplan	Reetableringsplanens pointscore	Ingen plan	Ingen plan
	Der er udført en fuld reetableringstest	Ingen plan	Ingen plan
	Der er udført en delvis reetableringstest årligt	Ingen plan	Ingen plan

● Ja ● Delvist ● Nej

Kilde: Rigsrevisionen på baggrund af oplysninger fra myndighed 3.

Tabel J
Myndighed 4

		System H	System I
Grundlaget for it-beredskabet	Systemafhængighederne er kortlagt	●	●
	Der er udarbejdet risikovurderinger, som indeholder vurderinger af sårbarheder, trusler, konsekvenser og sandsynligheder	●	●
Krisestyringsplan	Krisestyringsplanens pointscore	100/100	100/100
	Krisestyringsplanen er testet årligt	●	●
Nødplan	Nødplanen beskriver, hvilke procedurer der skal iværksættes for at opretholde kritiske opgaver og forretningsprocesser	●	●
	Nødplanen er testet årligt	●	●
Reetableringsplan	Reetableringsplanens pointscore	58/100	Ikke undersøgt[1)]
	Der er udført en fuld reetableringstest	●	●
	Der er udført en delvis reetableringstest årligt	●	●

● Ja ● Delvist ● Nej

[1)] System I er ressortoverført til Statens It og indgår derfor ikke i denne del af undersøgelsen.

Kilde: Rigsrevisionen på baggrund af oplysninger fra myndighed 4.

Tabel K

Søfartsstyrelsen

		System J	System K	System L
Grundlaget for it-beredskabet	Systemafhængighederne er kortlagt	●	●	●
	Der er udarbejdet risikovurderinger, som indeholder vurderinger af sårbarheder, trusler, konsekvenser og sandsynligheder	●	●	●
Krisestyringsplan	Krisestyringsplanens pointscore	100/100	100/100	100/100
	Krisestyringsplanen er testet årligt	●	●	●
Nødplan	Nødplanen beskriver, hvilke procedurer der skal iværksættes for at opretholde kritiske opgaver og forretningsprocesser	●	●	●
	Nødplanen er testet årligt	●	●	●
Reetableringsplan	Reetableringsplanens pointscore	Ikke undersøgt[1)]	Ikke undersøgt[1)]	Ikke undersøgt[1)]
	Der er udført en fuld reetableringstest	●	●	●
	Der er udført en delvis reetableringstest årligt	●	●	●

● Ja ● Delvist ● Nej

[1)] System J, K og L er ressortoverført til Statens It og indgår derfor ikke i denne del af undersøgelsen.

Kilde: Rigsrevisionen på baggrund af oplysninger fra Søfartsstyrelsen.