Finansudvalget 2020-21
FIU Alm.del - Bilag 191
Offentligt

FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

September 2021
– 20/2020

Rigsrevisionens beretning afgivet
til Folketinget med Statsrevisorernes
bemærkninger

Skatteministeriets it-beredskab

20/2020

Beretning om

Skatteministeriets it-beredskab

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 2021

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.

Skatteministeren afgiver en redegørelse til beretningen.

Rigsrevisor afgiver et notat med bemærkninger til ministerens redegørelse.

På baggrund af ministerens redegørelse og rigsrevisors notat tager Statsrevisorerne endelig stilling til beretningen, hvilket forventes at ske i januar 2022.

Ministerens redegørelse, 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 2020, som afgives i februar 2022.

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

Yderligere eksemplarer kan købes ved henvendelse til:
Rosendahls Lager og Logistik
Vandtårnsvej 83A
2860 Søborg

Tlf.: 4322 7300
distribution@rosendahls.dk
www.rosendahls.dk

ISSN 2245-3008
ISBN trykt 978-87-7434-723-1
ISBN online 978-87-7434-724-8

Statsrevisorernes bemærkning

Beretning om Skatteministeriets it-beredskab

Skatteministeriet er afhængig af en lang række it-systemer for at varetage sine opgaver med at opkræve og inddrive skatter og afgifter, refundere moms mv. Disse opgaver løses via forretningsprocesser, som består af en række it-systemer, der arbejder sammen. Større it-nedbrud og tab af data i Skatteministeriets kritiske forretningsprocesser og underliggende it-systemer kan have store konsekvenser for staten, borgere og virksomheder. Det er derfor afgørende, at Skatteministeriet har et dækkende it-beredskab, der hurtigt kan håndtere it-nedbrud og datatab.

Rigsrevisionens undersøgelse omfatter 9 it-systemer, der vedrører 3 kritiske forretningsprocesser for personskat, moms og selskabsskat, som står for knap 80 % af statens indtægter.

Statsrevisorerne finder Skatteministeriets it-beredskab for kritiske forretningsprocesser utilfredsstillende og utilstrækkeligt. Skatteministeriet har kun kortlagt it-beredskabet for 7 ud af ministeriets ca. 230 it-systemer, hvoraf de 45 vurderes som kritiske for ministeriets opgaveløsning.

Det utilstrækkelige it-beredskab kan medføre, at it-nedbrud og datatab kan blive mere omfattende med risiko for, at staten ikke kan opkræve skatter og afgifter, tilbagebetale tilgodehavender eller udbetale løn, SU, sociale ydelser, pension mv. til borgere og virksomheder. Det vil være særdeles kritisk for en i forvejen meget udfordret skatteforvaltning i Danmark.

Statsrevisorerne

17. september 2021

Henrik Thorup
Klaus Frandsen
Frank Aaen
Britt Bager
Mette Abildgaard
Leif Lahn Jensen

Statsrevisorerne hæfter sig bl.a. ved følgende resultater fra undersøgelsen:

- Skatteministeriet har kun kortlagt it-beredskabet for 7 ud af de 45 it-systemer, som ministeriet vurderer som enten samfundskritiske eller forretningskritiske for ministeriets opgaveløsning.
- Skatteministeriet har ikke et dækkende it-beredskab, idet ministeriet ikke har overblik over it-beredskabet for de resterende 38 kritiske it-systemer og ministeriets øvrige ca. 185 it-systemer.
- Skatteministeriet har udarbejdet risikovurderinger af de kritiske it-systemer. Risikovurderingerne udgør imidlertid et utilstrækkeligt grundlag for et dækkende it-beredskab, da de bl.a. mangler vurderinger af relevante risici.
- Skatteministeriet har reetableringsplaner for, hvordan 8 af de 9 undersøgte it-systemer skal reetableres efter nedbrud. Testene af de 8 reetableringsplaner er utilstrækkelige. Ministeriet har heller ikke koordineret kravene til fx maksimal reetableringstid og datatab i reetableringsplanerne.
- Skatteministeriet har ikke indsatsplaner for den interne krisestyring for 8 af de 9 undersøgte it-systemer.
- Skatteministeriet har kun udarbejdet én nødplan på hele Skatteforvaltningens område. Nødplanen er dog utilstrækkelig, da den kun forholder sig til nedbrud på ét af de 5 it-fagsystemer, som er nødvendige for at opretholde forretningsprocessen.

Statsrevisorerne finder det kritisabelt, at Skatteministeriet ikke har fastlagt, hvilken styrelse der har ansvaret for at koordinere arbejdet med it-beredskabet for kritiske forretningsprocesser på tværs af ministerområdet.

Statsrevisorerne bemærker i den forbindelse, at Skatteministeriets organisationsstruktur i styrelser ikke bør stå i vejen for den nødvendige tværgående koordination af opgaver - hverken når det gælder it-beredskab eller andre af ministeriets opgaver.

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.

Rigsrevisionen har revideret regnskaberne efter § 2, stk. 1, nr. 1, jf. § 3 i rigsrevisorloven.

Beretningen vedrører finanslovens § 9. Skatteministeriet.

I undersøgelsesperioden har der været følgende ministre:

Karsten Lauritzen: juni 2015 - juni 2019
Morten Bødskov: juni 2019 -

Beretningen har i udkast været forelagt Skatteministeriet, hvis bemærkninger er afspejlet i beretningen.

1. Introduktion og konklusion

1.1. Formål og konklusion

1. Denne beretning handler om Skatteministeriets it-beredskab for kritiske forretningsprocesser. Skatteministeriet er afhængig af en lang række it-systemer, for at ministeriet kan varetage sine opgaver med at opkræve og inddrive skatter og afgifter, refundere moms mv. Ministeriet løser opgaverne gennem såkaldte forretningsprocesser, som består af en række it-systemer, der arbejder sammen. Beretningen har fokus på it-beredskabet for forretningsprocesserne for personskat, moms og selskabsskat, som står for knap 80 % af statens indtægter.

2. Antallet af it-hændelser er stigende. 6 ud af 10 danske virksomheder har i 2020 oplevet it-sikkerhedshændelser, fx hackerangreb, hvilket er det højeste niveau i 4 år. Center for Cybersikkerhed vurderer endvidere, at alle danske myndigheder, virksomheder og borgere er udsat for en vedvarende trussel fra cyberkriminalitet. Myndighedernes it-beredskab skal gøre myndighederne i stand til effektivt at håndtere større it-hændelser, herunder hackerangreb, som kan medføre it-nedbrud eller tab af data.

3. Større it-nedbrud og tab af data i Skatteministeriets kritiske forretningsprocesser og underliggende it-systemer kan have store konsekvenser for staten, borgere og virksomheder. For det første kan det betyde, at Skatteforvaltningen ikke kan opkræve skatter og afgifter. For det andet kan det medføre, at staten ikke kan udbetale overskydende skatter til borgere og virksomheder, hvilket kan give likviditetsmæssige udfordringer for virksomheder ved fx forsinkelse i udbetaling af negativ moms. For det tredje kan større it-nedbrud betyde, at offentlige myndigheder ikke kan udbetale SU, sociale ydelser, pension mv., da myndighederne er afhængige af data fra Skatteforvaltningens it-systemer for at kunne beregne og udbetale ydelserne. Endelig kan det medføre, at Skatteministeriet ikke kan gendanne data eller får store omkostninger til at genskabe data på ny, hvis Skatteforvaltningens data går tabt eller bliver fejlbehæftede.

Større it-hændelser, hvor der er brug for et it-beredskab

Større it-hændelser kan omhandle situationer, hvor et it-system går ned, fx ved hackerangreb, fysiske skader på datacentre eller fejl på serveren. Større it-hændelser kan også omhandle tab af data i et it-system. Datatab handler fx om, at data ikke kan genskabes ud fra en backup, fx efter et it-nedbrud eller et hackerangreb. Datatab kan også handle om, at fejlbehæftede data kopieres til flere it-systemer eller servere.

Skatteministeriets 3 typer af it-beredskabsplaner

Nødplan
En nødplan er en plan for, hvordan Skatteministeriet håndterer og viderefører de opgaver og forretningsprocesser, som påvirkes i en it-beredskabssituation.

Indsatsplan
En indsatsplan er en plan for den interne krisestyring i Skatteministeriet i en it-beredskabssituation for hvert it-system.

Reetableringsplan
En reetableringsplan er en plan for, hvordan et it-system skal reetableres i en it-beredskabssituation.

4. Det er derfor afgørende, at Skatteministeriet hurtigt kan håndtere større it-nedbrud og datatab i it-systemerne ved at have et it-beredskab. It-beredskabet skal være på plads, før skaden sker. It-beredskabet skal sikre, at alternative forretningsprocesser kan iværksættes, så ministeriet kan videreføre sine opgaver, mens it-systemerne er ude af drift. Det indebærer bl.a., at ministeriet har overblik over, hvilke it-systemer der indgår i forretningsprocesserne, og har udarbejdet it-beredskabsplaner for, hvad ministeriet skal gøre i en it-beredskabssituation. Beredskabsplanerne skal hjælpe ministeriet med hurtigt at komme tilbage til normal it-drift og minimere konsekvenserne af større it-nedbrud og datatab. Skatteministeriet skal som offentlig myndighed implementere den internationale sikkerhedsstandard ISO 27001, som bl.a. indebærer, at ministeriet skal udarbejde og teste it-beredskabsplaner. Skatteministeriet har fastlagt, at ministeriets it-beredskab skal bestå af 3 typer af it-beredskabsplaner: nødplaner, indsatsplaner og reetableringsplaner.

5. De it-systemer, der indgår i Skatteministeriets kritiske forretningsprocesser, er afhængige af hinanden. Fx overføres der data mellem it-systemerne, og nogle systemer skal være funktionsdygtige, før andre kan fungere. Et samlet velfungerende it-beredskab er derfor afhængigt af, at ministeriet koordinerer it-beredskabet for de enkelte it-systemer i forretningsprocesserne.

6. Formålet med undersøgelsen er at vurdere, om Skatteministeriet har et tilfredsstillende it-beredskab for kritiske forretningsprocesser. Vi besvarer følgende spørgsmål i beretningen:

- Har Skatteministeriet et tilstrækkeligt grundlag for at etablere et it-beredskab?
- Har Skatteministeriet sikret, at der er implementeret tilfredsstillende it-beredskabsplaner?
- Har Skatteministeriet koordineret it-beredskabet for it-systemerne?

Rigsrevisionen har selv taget initiativ til undersøgelsen i juni 2020.

Hovedkonklusion

Skatteministeriet har et utilfredsstillende it-beredskab for kritiske forretningsprocesser. Konsekvensen er, at der er risiko for, at it-nedbrud og datatab medfører, at Skatteministeriet ikke kan opkræve skatter og afgifter, og at borgere og virksomheder ikke kan få udbetalt tilgodehavender fra staten.

Skatteministeriet har et utilstrækkeligt grundlag for at etablere et it-beredskab

Skatteministeriet har kortlagt it-beredskabet for 7 af de 45 it-systemer, som ministeriet vurderer som kritiske. Ministeriet har ikke overblik over it-beredskabet for de resterende 38 kritiske it-systemer og ministeriets øvrige ca. 185 it-systemer.

Skatteministeriet har udarbejdet risikovurderinger af de kritiske it-systemer. Risikovurderingerne udgør dog ikke et tilstrækkeligt grundlag for, at ministeriet kan etablere et dækkende it-beredskab. Det skyldes bl.a., at ikke alle risikovurderinger indeholder vurderinger af risici, som er relevante for it-beredskabet.

Skatteministeriet har ikke implementeret nødplaner og indsatsplaner for kritiske forretningsprocesser, men har sikret, at der i overvejende grad er implementeret tilfredsstillende reetableringsplaner

Skatteministeriet har kun udarbejdet én nødplan på hele Skatteforvaltningens område, som vedrører forretningsprocessen for moms. Nødplanen er dog ikke tilfredsstillende, da den kun forholder sig til nedbrud på ét af de 5 it-fagsystemer, som indgår i forretningsprocessen for moms. Ministeriet har ikke indsatsplaner for den interne krisestyring for 8 af de 9 undersøgte it-systemer, som løser centrale opgaver vedrørende personskat, moms og selskabsskat. Ministeriet har hverken testet nødplanen for momsprocessen eller den ene indsatsplan, som ministeriet har udarbejdet.

Skatteministeriet har sikret, at der er udarbejdet reetableringsplaner for, hvordan 8 af de 9 undersøgte it-systemer rent teknisk skal reetableres efter et nedbrud. Det betyder, at ministeriet for ét af de kritiske it-systemer ikke har en plan for, hvordan systemet skal reetableres. 6 af de 8 reetableringsplaner er i overvejende grad tilfredsstillende, da planerne indeholder de fleste af de centrale elementer, der bør indgå i en reetableringsplan. 2 af reetableringsplanerne mangler derimod flere centrale elementer. De 8 reetableringsplaner er blevet testet. Testene har imidlertid ikke været tilstrækkelige, da de ikke omfatter alle centrale elementer, som er relevante ved en test.

Skatteministeriet har i forbindelse med undersøgelsen haft vanskeligt ved at fremskaffe de eksisterende it-beredskabsplaner. Det er afgørende, at ministeriet hurtigt kan finde de relevante it-beredskabsplaner i en beredskabssituation.

Kritiske forretningsprocesser
Undersøgelsen vedrører 3 kritiske forretningsprocesser for:

- personskat
- moms
- selskabsskat.

Undersøgelsen vedrører 9 it-systemer, som indgår i de 3 forretningsprocesser. Nogle af it-systemerne indgår i flere af de 3 processer.

It-fagsystem
Et it-fagsystem er et it-system, der løser en faglig opgave, i modsætning til et støttesystem, der understøtter it-fagsystemerne.

Skatteministeriet har ikke koordineret it-beredskabet for de it-systemer, der indgår i de kritiske forretningsprocesser
Skatteministeriet har ikke systematisk kortlagt afhængighederne mellem de it-systemer, der indgår i forretningsprocesserne for personskat, moms og selskabsskat. Endvidere har ministeriet hverken taget stilling til eller aftalt med leverandørerne, i hvilken rækkefølge ministeriets it-systemer skal reetableres, hvis alle eller flere systemer går ned samtidigt. Det betyder, at ministeriet i en it-beredskabssituation kan have vanskeligt ved hurtigt at minimere skaderne af et større nedbrud.

Skatteministeriet har ikke koordineret kravene til, hvor lang tid det må tage at reetablere de enkelte it-systemer i forretningsprocesserne. Ministeriet har heller ikke koordineret kravene til it-systemernes maksimale datatab. Det kan betyde, at ministeriet kan lide større datatab, og at det tager længere tid at reetablere it-systemerne end forventet.

Skatteministeriet har ikke afklaret, hvilken styrelse der har til opgave at koordinere it-beredskabet på tværs af it-systemerne. Koordinering af it-beredskabet er afgørende for, at ministeriet kan etablere et tilfredsstillende it-beredskab.

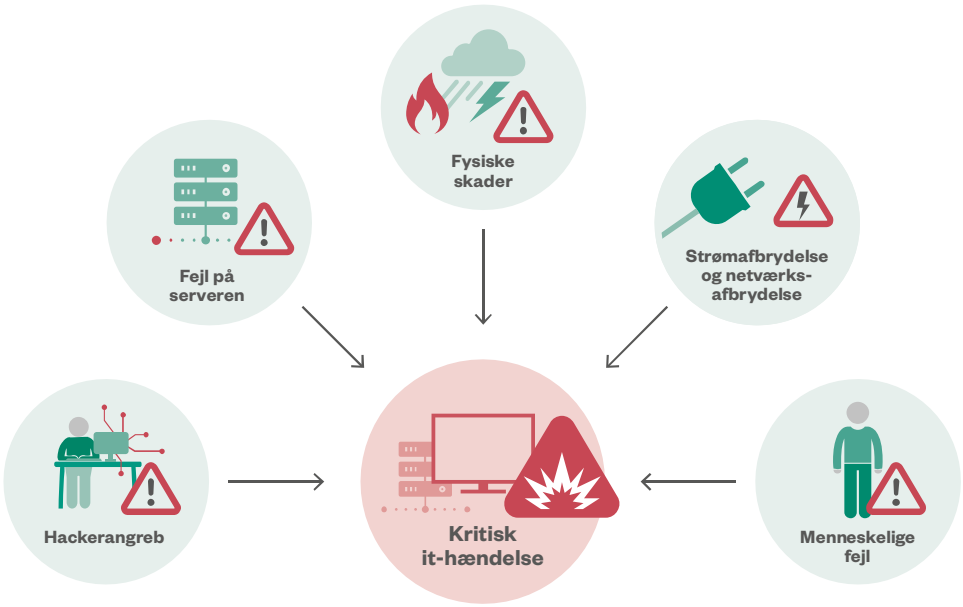
1.2. Baggrund

Krav til myndighedernes it-beredskab

7. It-beredskabet er en del af myndighedernes overordnede beredskab for at kunne håndtere ekstraordinære hændelser, der ikke kan klares ved hjælp af almindelige ressurser og rutiner. Skatteministeriets it-beredskab handler om, hvordan ministeriet kan opretholde og reetablere en lang række it-systemer, som sikrer statens indtægter. It-beredskabet er sammen med en række andre beredskaber – fx reallokering af personale eller reetablering af bygninger – en del af Skatteministeriets samlede beredskab. Figur 1 viser eksempler på hændelser, hvor det kan være nødvendigt for myndigheder at have et it-beredskab.

Figur 1

Eksempler på hændelser, hvor myndigheder kan have behov for at aktivere it-beredskabet



Kilde: Rigsrevisionen.

Figur 1 illustrerer, at hændelser som fx hackerangreb, fejl på serveren eller fysiske skader på hardware kan medføre, at der opstår en kritisk it-hændelse, hvor der kan være behov for at aktivere it-beredskabet.

8. Offentlige myndigheder har siden 2016 skullet følge den internationale standard for informationssikkerhed ISO 27001. ISO 27001 fastsætter standarderne for de offentlige myndigheders it-beredskab. De 3 overordnede standarder for it-beredskabet er, at myndighederne skal planlægge it-beredskabet, implementere it-beredskabet samt teste og evaluere it-beredskabet.

Hackerangreb på A.P. Møller - Mærsk

A.P. Møller – Mærsk blev i 2017 udsat for et hackerangreb, som ramte Mærsks adgangsstyringssystem. Adgangsstyringssystemet giver medarbejderne adgang til Mærsks it-systemer og computere. Hackerangrebet betød, at alle telefoner og interne it-systemer var ude af drift. Mærsks medarbejdere havde dermed ikke adgang til informationer om kunder og ordrer, fx hvor kundernes fragt befandt sig. Mærsk har måttet geninstallere 4.000 nye servere, 45.000 nye pc'er og 2.500 applikationer for at reetablere it-systemerne efter hackerangrebet. Mærsk vurderer, at hackerangrebet har kostet mellem 1,6 mia. kr. og 1,9 mia. kr.

Kilde: Version2 og Computerworld.

It-nedbrud hos Royal Bank of Scotland

I 2012 betød en softwareopdatering af it-systemerne hos Royal Bank of Scotland, at 6,5 mio. kunder ikke havde adgang til at benytte pengeautomater, netbank eller betale regninger og lån mv. i op til 20 dage. I 2015 betød en anden it-fejl, at 600.000 indbetalinger, fx lønindbetalinger og sociale ydelser til bankens kunder, ikke kunne modtages i flere dage.

Kilde: The Guardian.

Planlægning af it-beredskabet indebærer, at Skatteministeriet skal vurdere, hvilke forhold og elementer der er relevante at tage højde for i it-beredskabet. Det er i planlægningen relevant, at ministeriet bl.a. har overblik over, hvilke forretningsprocesser og it-systemer ministeriet vurderer er kritiske. Det er også relevant, at ministeriet har overblik over de risici, hvor konsekvenserne for ministeriet er størst. Planlægningen har til formål at danne et grundlag for, at ministeriet kan implementere et dækkende it-beredskab.

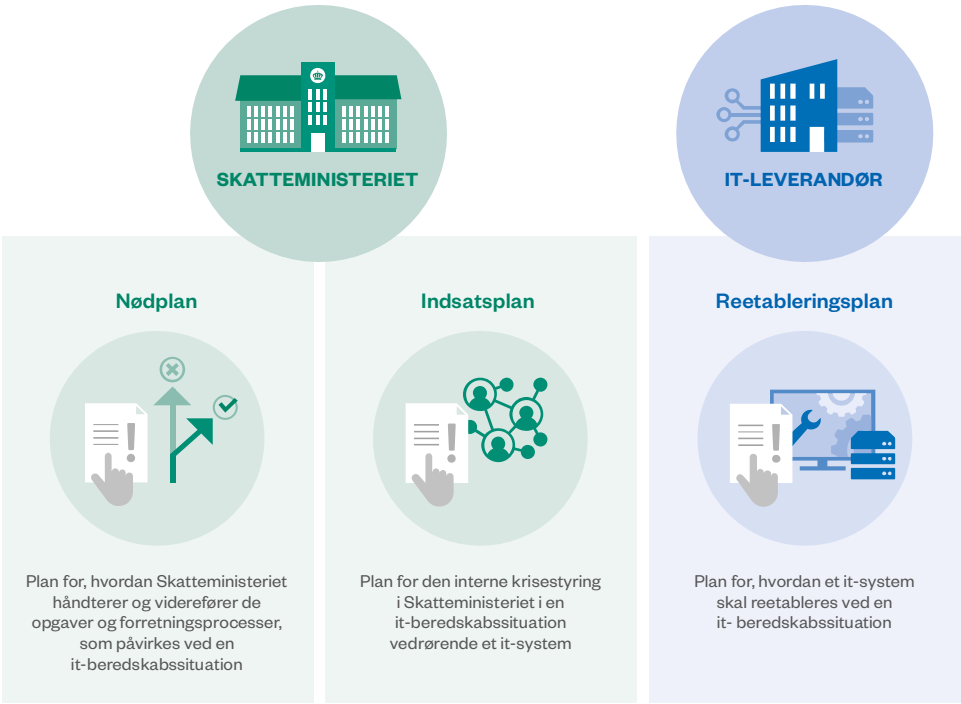
Implementering af it-beredskabet indebærer, at Skatteministeriet udarbejder og iværksætter it-beredskabsplaner.

Test og evaluering af it-beredskabet indebærer, at Skatteministeriet skal vurdere it-beredskabet og dermed ministeriets evne til at håndtere it-nedbrud og datatab. Ministeriet skal teste it-beredskabsplanerne og efterfølgende evaluere resultaterne af testen for at forbedre it-beredskabet og justere beredskabsplanerne.

Forskellige typer af it-beredskabsplaner

9. Når der opstår en it-beredskabssituation, er der behov for handling på forskellige områder – og dermed også behov for forskellige typer af it-beredskabsplaner. Som det fremgår af figur 2, har Skatteministeriet fastlagt, at ministeriets it-beredskab skal bestå af 3 typer af it-beredskabsplaner.

Figur 2
Skatteministeriets 3 typer af it-beredskabsplaner



Kilde: Rigsrevisionen på baggrund af oplysninger fra Skatteministeriet.

Nødplaner beskriver, hvilke nødprocedurer Skatteministeriet eventuelt kan tage i brug i tilfælde af et nedbrud på de it-systemer, som normalt varetager opgaverne. Det kan fx betyde, at ministeriet må bruge manuelle procedurer eller alternative it-systemer for at løse opgaverne. Ministeriet har fastlagt, at nødplaner skal udarbejdes for den enkelte forretningsproces.

Indsatsplaner beskriver Skatteministeriets interne krisestyring. Planen fastlægger, hvordan ministeriet skal håndtere et nedbrud og sikre, at alle relevante personer bliver informeret og kender deres roller i en it-beredskabssituation. Indsatsplaner omfatter også ministeriets plan for kommunikation til eksterne parter, som er afhængige af at anvende de it-systemer, der er gået ned. Det kan fx være borgere og virksomheder, men også andre offentlige myndigheder, fx kommuner, ATP, Udbetaling Danmark, a-kasser og FerieKonto. Offentlige myndigheder anvender oplysninger om borgernes indkomst fra it-systemet elndkomst, når de skal beregne og udbetale ydelser. Ministeriet har fastlagt, at indsatsplanerne skal udarbejdes for det enkelte it-system.

Reetableringsplaner er tekniske beredskabsplaner, som beskriver, hvordan it-systemet reetableres efter et nedbrud. Det er ofte eksterne leverandører, som står for at reetablere Skatteministeriets it-systemer, og derfor også leverandørerne, som udarbejder reetableringsplanerne. Det skyldes, at hovedparten af ministeriets it-systemer er driftet af eksterne leverandører. Ministeriet udarbejder reetableringsplanerne for ministeriets internt driftede it-systemer. Reetableringsplanerne udarbejdes for det enkelte it-system.

Organisering

10. Udviklings- og Forenklingsstyrelsen står for drift og vedligeholdelse af Skatteforvaltningens it-systemer. Det indebærer, at styrelsen indgår aftaler og fører tilsyn med de eksterne leverandører, som drifter en stor del af Skatteforvaltningens it-systemer. Styrelsen varetager desuden selv driften af nogle af Skatteforvaltningens it-systemer.

Udviklings- og Forenklingsstyrelsen har den rammesættende og understøttende opgave med at udarbejde og implementere processer og skabeloner for it-beredskabet. Endvidere har styrelsen ansvaret for det tekniske it-beredskab, herunder ansvaret for, at eksterne leverandører eller styrelsen selv udarbejder reetableringsplaner for it-systemerne.

Skattestyrelsen står for forretningsprocesserne for personskat, moms og selskabsskat, som it-systemerne indgår i. Det er Skattestyrelsen, som har opgaven med at udarbejde nødplaner for alternative forretningsgange, i tilfælde af at den almindelige it-understøttelse ikke er til rådighed. Det er ligeledes Skattestyrelsen, som har ansvaret for at udarbejde indsatsplaner for den interne opgavefordeling og krisestyring i Skatteministeriet.

Både Udviklings- og Forenklingsstyrelsen og Skattestyrelsen har således opgaven med at udarbejde de relevante it-beredskabsplaner for forretningsprocesserne for personskat, moms og selskabsskat samt de underliggende it-systemer.

1.3. Revisionskriterier, metode og afgrænsning

Revisionskriterier

Informationssikkerhed
Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger til at sikre informationer i forhold til fortrolighed, integritet (ændring af data) og tilgængelighed. I arbejdet indgår bl.a. organisering af sikkerhedsarbejdet, processer for behandling af data, styring af leverandører, tekniske sikringsforanstaltninger og it-beredskab.

11. Undersøgelsens revisionskriterier tager udgangspunkt i de internationale standarder for informationssikkerhed ISO 27001 og ISO 27002, som fastsætter standarderne for it-beredskabet. Offentlige myndigheder har siden 2016 skullet følge ISO 27001. ISO 27001 er bredt formuleret. Hver myndighed skal tage stilling til, hvordan de vil implementere sikkerhedsforanstaltningerne, så de er passende for den enkelte myndighed. Skatteministeriet har oplyst, at ministeriet har vurderet, at det er relevant, at ministeriet implementerer alle sikkerhedsforanstaltninger fra ISO 27001, herunder de sikkerhedsforanstaltninger, der vedrører it-beredskabet. Mens ISO 27001 beskriver standarderne for informationssikkerhed, herunder standarderne for it-beredskabet, er ISO 27002 en vejledning i den praktiske udmøntning af standarderne. Digitaliseringsstyrelsen og Erhvervsministeriet vejleder på hjemmesiden sikkerdigital.dk offentlige myndigheder i, hvordan de i praksis skal implementere ISO 27001. Derudover har Digitaliseringsstyrelsen udarbejdet vejledninger og skabeloner for myndighedernes it-beredskab, fx *Vejledning til it-beredskab*, *Guide til kommunikation i en beredskabssituation* og skabeloner til it-beredskabsplaner. Disse vejledninger og skabeloner samt vejledningen på sikkerdigital.dk er ligeledes udgangspunktet for vores revisionskriterier.

Rammerne for offentlige myndigheders it-beredskab er det såkaldte helhedsorienterede beredskab, som er en overordnet paraply for beredskabsarbejdet defineret af Beredskabsstyrelsen. Beredskabsstyrelsen opstiller en række anbefalinger om god praksis for myndighedernes it-beredskab. Digitaliseringsstyrelsens vejledning i at implementere ISO 27001 ligger i tråd med Beredskabsstyrelsens anbefalinger. Beredskabsstyrelsens anbefalinger er dog på nogle punkter mere specifikke, fx i forhold til, hvad der karakteriserer en god beredskabsplan. Rigsrevisionen vil derfor også anvende Beredskabsstyrelsens anbefalinger som revisionskriterier til revisionen af it-beredskabsplanernes indhold. I bilag 2 findes en liste over ophænget til de revisionskriterier, som vi har anvendt til at vurdere Skatteministeriets it-beredskabsplaner og ministeriets test af beredskabsplanerne.

12. I *kapitel 2* undersøger vi Skatteministeriets grundlag for at etablere et dækkende it-beredskab. Herunder undersøger vi, om ministeriet har fastsat en overordnet ramme for it-beredskabet, om ministeriet har identificeret de kritiske forretningsprocesser og tilhørende it-systemer, og om ministeriet har overblik over det eksisterende it-beredskab. Endelig undersøger vi, om ministeriet har udarbejdet risikovurderinger af ministeriets kritiske forretningsprocesser og underliggende it-systemer som grundlag for at kunne etablere og tilpasse it-beredskabet.

I *kapitel 3* undersøger vi, om Skatteministeriet har sikret, at der er udarbejdet it-beredskabsplaner, og om beredskabsplanerne indeholder udvalgte centrale elementer. Dette undersøger vi med udgangspunkt i it-systemerne for de 3 forretningsprocesser for personskat, moms og selskabsskat. Derudover undersøger vi, om it-beredskabsplanerne er blevet testet, og om testene indeholder udvalgte centrale elementer. Undersøgelsen vedrører både Skatteministeriets egne it-beredskabsplaner og leverandørernes it-beredskabsplaner. I kapitlet undersøger vi, om der er nødplaner for forretningsprocesserne, indsatsplaner for den interne krisestyring og reetableringsplaner for den tekniske reetablering af it-systemerne, da alle 3 planer er vigtige dele af it-beredskabet.

I *kapitel 4* undersøger vi, om Skatteministeriet har koordineret it-beredskabet for de it-systemer, som er afhængige af hinanden for at kunne fungere i de 3 kritiske forretningsprocesser. Vi har fokus på koordineringen af it-systemernes reetablering og således på den del af it-beredskabet, der vedrører reetableringsplanerne. Koordineringen af it-beredskabet er ikke en standard, der fremgår direkte af ISO 27001. Ministeriets koordinering af den tekniske reetablering af de it-systemer, der indgår i forretningsprocesserne, er imidlertid helt central for, at ministeriet kan opretholde kritiske forretningsprocesser. Det skyldes, at der i de enkelte forretningsprocesser indgår mange it-systemer, som er afhængige af hinanden. Koordineringen af reetableringen af de it-systemer, der indgår i de enkelte forretningsprocesser, er derfor en forudsætning for, at ministeriet kan have et tilfredsstillende it-beredskab.

Vi undersøger derfor i kapitel 4, om Skatteministeriet har kortlagt, hvilke sammenhænge og afhængigheder der er mellem it-systemerne i de 3 undersøgte forretningsprocesser. Derudover undersøger vi, om ministeriet har taget stilling til og beskrevet, hvilke it-systemer der skal først op at køre, i tilfælde af at flere eller alle systemer har større nedbrud. Endelig undersøger vi, om ministeriet har koordineret it-systemernes maksimale reetableringstid og maksimale datatab for de it-systemer, der er afhængige af hinanden i forretningsprocesserne.

Metode

13. Vi har undersøgt, om Skatteministeriets it-beredskab er tilfredsstillende for 3 kritiske forretningsprocesser. Vi har udvalgt processerne for personskat, moms og selskabsskat, som er særligt væsentlige både med hensyn til statens indtægter og potentielle konsekvenser for borgere og virksomheder ved større it-nedbrud. Skatteforvaltningen opkræver gennem de 3 processer knap 80 % af statens indtægter, svarende til ca. 850 mia. kr. Boks 1 beskriver de 3 forretningsprocesser.

Boks 1

De 3 undersøgte forretningsprocesser

Personskat (A-skat og arbejdsmarkedsbidrag) udgjorde i 2020 samlet set ca. 547 mia. kr., svarende til ca. 50 % af statens indtægter.

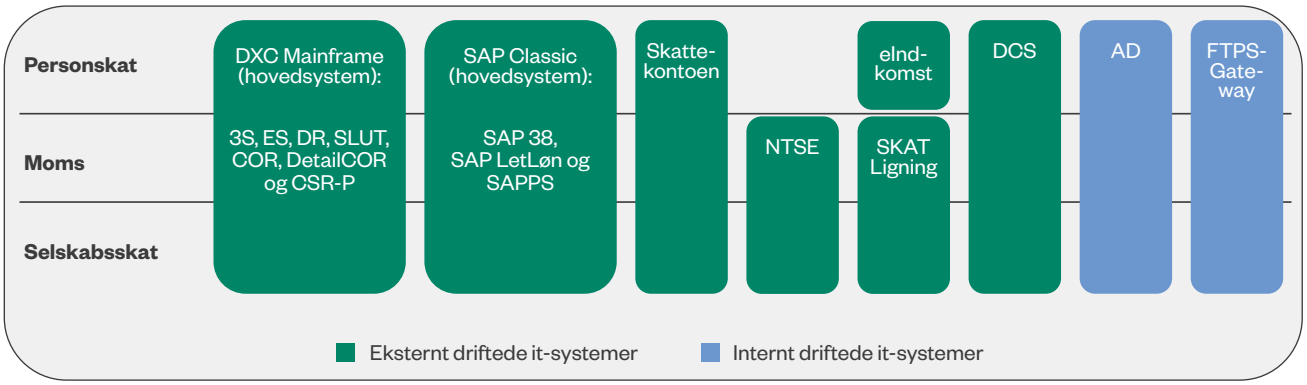
Moms udgjorde i 2020 samlet set ca. 230 mia. kr., svarende til ca. 21 % af statens indtægter. Virksomheder angav i 2020 positive momsangivelser for ca. 536 mia. kr. og negative momsangivelser for ca. 306 mia. kr.

Selskabsskat udgjorde i 2020 samlet set ca. 70 mia. kr., svarende til ca. 6 % af statens indtægter.

Kilde: Skatteministeriets årsregnskab 2020 for § 38. Skatter og afgifter samt Skatteministeriets indtægtlister for 2020.

14. Figur 3 viser de forretningsprocesser og de it-systemer, der indgår i undersøgelsen.

Figur 3
It-systemer i forretningsprocesserne for personskat, moms og selskabsskat



Kilde: Rigsrevisionen på baggrund af oplysninger fra Skatteministeriet.

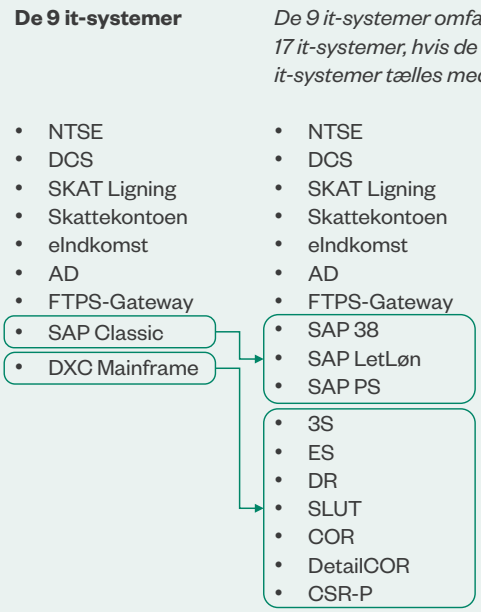
Det fremgår af figur 3, at mange af it-systemerne indgår i alle 3 forretningsprocesser. Disse it-systemer er derfor særligt kritiske. Det drejer sig fx om Skattekontoen, som er en samlet indgang til betalinger og opkrævninger for virksomheder, og SAP 38, der anvendes til regnskabsaflæggelse af statens indtægter. Skattekontoen og SAP 38 indgår i næsten alle Skatteministeriets forretningsprocesser. Nedbrud på SAP 38 vil betyde, at Skatteministeriet ikke kan opkræve told, skatter og afgifter fra borgere og virksomheder, og at borgere og virksomheder ikke kan få udbetalt tilgodehavender.

I figuren indgår også de støttesystemer og platforme, som er afgørende for, at de 3 kritiske forretningsprocesser kan fungere. Det vedrører fx brugeradgangssystemerne Active Directory (AD) og DCS. AD giver Skatteforvaltningens medarbejdere adgang til forvaltningens it-systemer, mens DCS giver borgere og virksomheder adgang til Skatteforvaltningens brugerrettede systemer, fx TastSelv Erhverv (NTSE). Betegnelsen it-system dækker i beretningen både over it-fagsystemer, støttesystemer og platforme.

I undersøgelsen indgår 2 hovedsystemer, hvor flere af it-systemerne for de 3 forretningsprocesser ligger. Som det fremgår af figur 3, ligger 7 it-systemer under hovedsystemet DXC Mainframe, mens 3 it-systemer ligger under hovedsystemet SAP Classic. Hovedsystemerne og de underliggende it-systemer indgår i en samlet kontrakt med leverandøren og har en fælles reetableringsplan. De behandles derfor som ét it-system i undersøgelsen, når vi i kapitel 3 gennemgår it-beredskabsplanerne og test af beredskabsplanerne. I kapitel 4, hvor vi undersøger koordineringen mellem de enkelte it-systemers it-beredskab, tager vi udgangspunkt i de enkelte systemer i forretningsprocesserne. Samlet set indgår der 9 it-systemer (2 hovedsystemer og 7 øvrige systemer) i undersøgelsen. Under de 2 hovedsystemer er der en række underliggende it-systemer. Det betyder, at der i undersøgelsen indgår i alt 17 enkeltstående it-systemer. I bilag 3 findes en liste over de undersøgte it-systemer med en kort beskrivelse af it-systemernes funktion. Boks 2 viser de 9 it-systemer, som indgår i undersøgelsen, og de i alt 17 enkeltstående it-systemer.

Boks 2

It-systemer i forretningsprocesserne for personskat, moms og selskabsskat



De undersøgte it-systemer omfatter ca. halvdelen af de såkaldte legacy-systemer. Det er it-systemer, som regeringens legacy-udvalg vurderer har særlige udfordringer, bl.a. fordi systemerne er meget gamle, og fordi der er få nøglepersoner i Skatteministeriet, der har kendskab til systemerne.

15. Skatteministeriet har ikke et fuldstændigt overblik over alle de it-systemer, der indgår i forretningsprocesserne for personskat, moms og selskabsskat. Vi har derfor i dialog med Udviklings- og Forenklingsstyrelsen og Skattestyrelsen forsøgt at danne os et overblik over alle it-systemer, der indgår i de 3 forretningsprocesser. Skatteministeriet har vurderet, at vi har identificeret de it-systemer, som er de væsentligste for forretningsprocesserne for personskat, moms og selskabsskat.

16. Vi har som grundlag for revisionen indhentet og gennemgået materiale om Skatteministeriets it-beredskab, ministeriets kortlægning af forretningsprocesser og it-systemer samt ministeriets risikovurderinger af it-systemer. For de 9 undersøgte it-systemer har vi gennemgået it-beredskabsplaner og testrapporter for perioden 2018-2020 for at vurdere, om de indeholder centrale elementer. Derudover har vi for de eksternt driftede it-systemer indhentet de kontraktbilag, som vedrører it-beredskabet. For at vurdere, om Skatteministeriet har koordineret it-beredskabet for de it-systemer, der indgår i de 3 forretningsprocesser, har vi bl.a. sammenlignet kravene til it-systemernes maksimale reetableringstid og maksimale datatab, som er fastsat i kontraktbilag eller i anden dokumentation. Vi har for hvert af de 9 it-systemer holdt møde med medarbejdere i Skatteministeriet, som er ansvarlige for systemerne, leverandørstyring og kontraktforhold. Møderne havde bl.a. til formål at få afklaret spørgsmål til materialet.

Legacy-systemer

Legacy-systemer er ældre it-systemer, der stadig er i brug. Skatteministeriet ønsker at udskifte legacy-systemerne, da de er komplekse og bygger på forældet teknologi.

Skatteforvaltningens legacy-systemer understøtter centrale dele af skatteopkrævningen og bidrager samlet set til at opkræve ca. 800 mia. kr. årligt.

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

Afgrænsning

18. Undersøgelsen omhandler perioden 2018-2020 og dermed tiden efter, at Skatteforvaltningen blev omorganiseret, og de nye styrelser blev etableret.

It-beredskabet handler om den del af informationssikkerhed, som vedrører tilgængeligheden af it-systemerne og større datatab. Undersøgelsen vedrører derfor ikke andre dele af informationssikkerhedsområdet, fx adgangsstyring. Undersøgelsen af it-beredskabet for forretningsprocesserne for personskat, moms og selskabsskat belyser den del af processen, som vedrører opkrævning af skatter mv. Vi har for at afgrænse antallet af it-systemer fravalgt den del af forretningsprocesserne, som vedrører Skatteforvaltningens inddrivelse af gæld.

Undersøgelsen er afgrænset til at handle om planlægning og test af it-beredskabet. Det betyder, at vi fx ikke har undersøgt, hvordan it-beredskabet rent faktisk fungerer i en beredskabssituation. En god beredskabsplanlægning øger sandsynligheden for, at myndigheder i en beredskabssituation kan handle hurtigt og minimere skaderne, men det er ikke nogen garanti for, at alt forløber, som det er planlagt i it-beredskabsplanerne. Vi har ikke undersøgt, om it-beredskabsplanerne for de undersøgte it-systemer er fysisk tilgængelige for de relevante personer i Skatteministeriet. Det har ikke været muligt på grund af COVID-19-situationen.

19. I bilag 1 er undersøgelsens metodiske tilgang beskrevet. Bilag 2 indeholder en liste over ophænget til de revisionskriterier, som vi har anvendt til at vurdere Skatteministeriets it-beredskabsplaner og test af beredskabsplanerne. I bilag 3 beskrives de undersøgte it-systemers funktion. Bilag 4 indeholder en ordliste, der forklarer udvalgte ord og begreber.

2. Grundlaget for it-beredskabet

Delkonklusion

Skatteministeriet har et utilstrækkeligt grundlag for at etablere et it-beredskab.

Skatteministeriet har fastlagt en overordnet ramme for beredskabet, herunder it-beredskabet. Ministeriet har udarbejdet en koncernfælles beredskabspolitik, generelle beredskabsplaner for Skattestyrelsen og Udviklings- og Forenklingsstyrelsen samt skabeloner for it-beredskabsplaner.

Skatteministeriet har udpeget 45 it-systemer, som ministeriet vurderer som enten samfundskritiske eller forretningskritiske for ministeriets samlede opgavevaretagelse, da de har en central betydning for statens opkrævning af bl.a. personskat og selskabsskat.

Skatteministeriet har ikke overblik over det eksisterende it-beredskab. Ministeriet har således kun kortlagt, hvilket it-beredskab der eksisterer for 7 ud af 45 af ministeriets samfundskritiske og forretningskritiske it-systemer. Ministeriet har dermed ikke overblik over it-beredskabet for de resterende 38 kritiske it-systemer og ministeriets øvrige ca. 185 it-systemer.

Skatteministeriet har i 2019 og i 2020-2021 udarbejdet risikovurderinger af kritiske it-systemer. Risikovurderingerne udgør dog ikke et tilstrækkeligt grundlag for, at ministeriet kan etablere et dækkende it-beredskab. Det skyldes, at risikovurderingerne for 2019 ikke indeholder vurderinger af, hvilke konsekvenser det har for ministeriet, hvis de påpegede risici opstår, og at risikovurderingerne for 2020-2021 kun indeholder vurderinger af konsekvenser på et overordnet niveau. Desuden er det ikke alle risikovurderingerne af it-systemerne, som indeholder risici, der er relevante for it-beredskabet. I risikovurderingerne for 2020-2021 indgår der 4 risici, som er relevante for it-beredskabet, og som skal vurderes for alle it-systemer. De 4 risici er dog ikke blevet vurderet for alle de 9 it-systemer, som indgår i Rigsrevisionens undersøgelse. Den samlede risikovurderingsrapport for 2020-2021 påpeger dog, at Skatteministeriet mangler it-beredskabsplaner for en lang række it-systemer.

20. Dette kapitel handler om Skatteministeriets grundlag for at kunne etablere et dækkende it-beredskab for ministeriets forretningsprocesser. Vi undersøger, om ministeriet har fastsat nogle rammer for it-beredskabet, om ministeriet har kortlagt ministeriets kritiske forretningsprocesser og underliggende it-systemer, og om ministeriet har overblik over det eksisterende it-beredskab. Endelig undersøger vi, om ministeriet har foretaget risiko- og konsekvensvurderinger for kritiske forretningsprocesser og underliggende it-systemer som grundlag for at etablere et dækkende it-beredskab.

2.1. Rammerne for it-beredskabet

21. Vi har undersøgt, om Skatteministeriet har fastsat en overordnet ramme for it-beredskabet på ministeriets område. Da it-beredskabet er en del af myndighedernes generelle beredskab, er planlægningen af det generelle beredskab også med til at sætte rammerne for it-beredskabet.

22. Vores undersøgelse viser, at Skatteministeriet i 2018 har udarbejdet en koncernfælles beredskabspolitik, som fastlægger den overordnede ramme for koncernens generelle beredskab, herunder ansvarsfordeling, målbillede og vision på tværs af koncernen. Politikken er senest opdateret i juni 2020. Derudover har ministeriet fastlagt, at departementet og de enkelte styrelser skal udarbejde en beredskabsplan og et beredskabsprogram med udgangspunkt i en koncernfælles skabelon.

Udviklings- og Forenklingsstyrelsen og Skattestyrelsen udarbejder årligt et beredskabsprogram, som beskriver, hvilke aktiviteter styrelserne skal gennemføre på beredskabsområdet i løbet af året. Derudover har Udviklings- og Forenklingsstyrelsen og Skattestyrelsen udarbejdet en generel beredskabsplan for hver styrelse. Beredskabsplanerne er senest opdateret i henholdsvis april og marts 2021. Skattestyrelsen har ikke testet sin beredskabsplan. Skattestyrelsen har oplyst, at styrelsen har haft aktiveret beredskabet 2 gange. Først ved sprængningen af en bombe i Østbanegade i 2019 og senere i forbindelse med hjemsendelsen af medarbejdere på grund af COVID-19 i foråret 2020. Udviklings- og Forenklingsstyrelsen har oplyst, at styrelsen i august 2021 for første gang har testet beredskabsplanen og er i gang med at udarbejde en evaluering af testen, som vil indeholde en række forbedringspunkter. Styrelsen har endvidere oplyst, at styrelsen i forbindelse med COVID-19 nedsatte en krisestab og har evalueret dette krisestyringsforløb.

23. Undersøgelsen viser, at Skatteministeriet i forhold til it-beredskabet har fastlagt, at departementets og styrelsernes generelle beredskabsplaner i relevant omfang skal suppleres med nødplaner, indsatsplaner og reetableringsplaner for forretningsprocesser og underliggende it-systemer. Derudover har Udviklings- og Forenklingsstyrelsen oplyst, at det er fastlagt, at alle it-systemer skal have en reetableringsplan.

Udviklings- og Forenklingsstyrelsen har udarbejdet skabeloner for nødplaner, indsatsplaner og reetableringsplaner. Skatteministeriet har fastlagt, at skabelonerne skal anvendes ved nyudvikling og nyanskaffelser af it-systemer.

Resultater

Skatteministeriet har fastlagt en overordnet ramme for beredskabet, herunder it-beredskabet. Ministeriet har således udarbejdet en koncernfælles beredskabspolitik, og Udviklings- og Forenklingsstyrelsen og Skattestyrelsen har udarbejdet en generel beredskabsplan og et beredskabsprogram for hver styrelse. Udviklings- og Forenklingsstyrelsen har endvidere udarbejdet skabeloner for de it-beredskabsplaner, der skal foreligge for de enkelte it-systemer (nødplaner, indsatsplaner og reetableringsplaner).

2.2. Kortlægning af kritiske forretningsprocesser og it-systemer

24. Vi har undersøgt, om Skatteministeriet har kortlagt ministeriets kritiske forretningsprocesser og tilhørende it-systemer. Formålet med kortlægningen er, at Skatteministeriet skal have gjort sig klart, hvilke opgaver ministeriet ønsker at kunne opretholde i en beredskabssituation, hvor der er større nedbrud på ét eller flere it-systemer. Derfor skal ministeriet også have overblik over, hvilke it-systemer der er nødvendige, for at forretningsprocessen kan fungere. Ministeriet skal således anvende kortlægningen til at fokusere it-beredskabet mod de kritiske forretningsprocesser og tilhørende it-systemer. Vi har derudover undersøgt, om Skatteministeriet har overblik over det eksisterende it-beredskab for Skatteforvaltningens it-systemer.

25. Figur 4 viser, på hvilket grundlag myndighederne kan etablere et fokuseret it-beredskab.

Figur 4
Etablering af et fokuseret it-beredskab

Kilde: Rigsrevisionen på baggrund af oplysninger fra sikkerdigital.dk.

Som det fremgår af figur 4, kan kortlægningen af kritiske forretningsprocesser og tilhørende it-systemer anvendes til, at myndighederne kan vurdere risici og konsekvenser for de væsentligste forretningsprocesser og tilhørende it-systemer. Dette kan hjælpe myndighederne til at vurdere, hvilket it-beredskab de har behov for. Myndighederne kan på den baggrund udarbejde dækkende it-beredskabsplaner, som efterfølgende skal testes.

26. Undersøgelsen viser, at Udviklings- og Forenklingsstyrelsen i juni 2020 har kortlagt, hvilke af Skatteministeriets it-systemer der er henholdsvis samfundskritiske og forretningskritiske. Styrelsen identificerede 15 samfundskritiske og 30 forretningskritiske it-systemer ud af ministeriets i alt ca. 230 it-systemer. Styrelsen begrunder udvælgelsen af de samfundskritiske it-systemer med, at de har en central betydning for opkrævning af personskat, selskabsskat, told, import og afgifter samt betydning for virksomheders muligheder for ind- og udbetalinger. De samfundskritiske it-systemer omfatter kun it-fagsystemer og ikke de støttesystemer og platforme, som de samfundskritiske it-systemer er afhængige af for at kunne fungere. Udviklings- og Forenklingsstyrelsen har valgt at betragte støttesystemer, platforme mv. som forretningskritiske for at minimere antallet af samfundskritiske it-systemer. Rigsrevisionen finder, at det bør være it-systemets kritikalitet og ikke antallet af it-systemer, der afgør, om Skatteministeriet vurderer et it-system til at være samfundskritisk eller forretningskritisk.

Skatteministeriet har ikke systematisk kortlagt og prioriteret, hvilke forretningsprocesser ministeriet vurderer er kritiske for ministeriet, dvs. er vigtige for ministeriets kerneopgaver.

27. Udviklings- og Forenklingsstyrelsen har på baggrund af kortlægningen af de samfundskritiske og forretningskritiske it-systemer afdækket, hvilket it-beredskab der eksisterer for 7 af de 15 samfundskritiske it-systemer. Styrelsen har ikke afdækket, hvilket it-beredskab der eksisterer for de resterende 8 samfundskritiske og 30 forretningskritiske it-systemer samt for ministeriets øvrige it-systemer.

Skatteministeriets kortlægning af it-beredskabet for 7 samfundskritiske it-systemer resulterede i en række anbefalinger til at styrke ministeriets it-beredskab. Ministeriet har udarbejdet en plan for implementeringen af disse anbefalinger. Ministeriet har oplyst, at implementeringen af anbefalingerne vil begynde i 2. halvår 2021.

Resultater

Skatteministeriet har kortlagt, hvilke it-systemer ministeriet betragter som henholdsvis samfundskritiske og forretningskritiske. Ministeriet har dog ikke systematisk kortlagt, hvilke forretningsprocesser der er kritiske for ministeriet, og dermed hvilke opgaver ministeriet ønsker at kunne opretholde i en beredskabssituation. Ministeriet har ikke overblik over det eksisterende it-beredskab, da ministeriet kun har afdækket, hvilket it-beredskab der eksisterer for 7 af de 45 samfundskritiske og forretningskritiske it-systemer. Ministeriet har dermed ikke overblik over it-beredskabet for de resterende 38 kritiske it-systemer og ministeriets øvrige ca. 185 it-systemer.

2.3. Risiko- og konsekvensvurderinger

28. Vi har undersøgt, om Skatteministeriet anvender risiko- og konsekvensvurderinger af kritiske forretningsprocesser og tilhørende it-systemer som grundlag for at udarbejde dækkende it-beredskabsplaner. Formålet med risiko- og konsekvensvurderinger er at understøtte arbejdet med at etablere et dækkende it-beredskab, der hvor konsekvenserne og sandsynligheden ved et større it-nedbrud er størst.

29. Skatteministeriet har fastlagt, at der hvert år skal udarbejdes en samlet risikovurderingsrapport på informationssikkerhedsområdet på baggrund af systemspecifikke risikovurderinger af udvalgte it-systemer.

Systemspecifikke risikovurderinger
I Udviklings- og Forenklingsstyrelsens systemspecifikke risikovurderinger vurderer styrelsen en række trusler og sårbarheder for hvert it-system, fx manglende sikkerhedsprocedurer eller mangelfuld backup.

Vores undersøgelse viser, at Skatteministeriet i 2018 ikke har udarbejdet en samlet risikovurderingsrapport med systemspecifikke risikovurderinger.

Udviklings- og Forenklingsstyrelsen har udarbejdet en samlet risikovurderingsrapport for 2019 og en fælles risikovurderingsrapport for 2020 og 2021, hvor der er risikovurderinger af samfundskritiske og forretningskritiske it-systemer. De systemspecifikke risikovurderinger for 2019 og for 2020-2021 udgør dog ikke et tilstrækkeligt grundlag for, at Skatteministeriet kan tilrettelægge et dækkende it-beredskab.

I 2019 har Udviklings- og Forenklingsstyrelsen udarbejdet risikovurderinger af 49 it-systemer. Risikovurderingerne for 2019 indeholder dog meget få vurderinger af risici, som er relevante i forhold til it-beredskabet. Endvidere indgår der ikke vurderinger af konsekvenserne af de påpegede risici for it-systemerne eller for de forretningsprocesser, som systemerne indgår i.

I 2020-2021 har Udviklings- og Forenklingsstyrelsen udarbejdet risikovurderinger af de 45 samfundskritiske og forretningskritiske it-systemer. Styrelsen har oplyst, at der i risikovurderingerne indgår 4 risici, som er relevante for it-beredskabet. Vores gennemgang af risikovurderingerne for de 9 undersøgte it-systemer viser imidlertid, at styrelsen ikke systematisk har vurderet de 4 risici. I risikovurderingerne for 2 af de 9 it-systemer er der ingen vurderinger af de 4 risici, mens der i risikovurderingerne for 3 af systemerne kun indgår nogle af de 4 risici vedrørende it-beredskabet.

I risikovurderingerne for 2020-2021 er der eksempler på, at de samme risici er vurderet forskelligt. Fx er risikoen vedrørende manglende it-beredskabsplaner vurderet meget forskelligt for de enkelte it-systemer, selv om der for ingen af systemerne foreligger indsatsplaner. Risikoen er fx vurderet til 5 på sandsynlighedsskalaen (6 er højest på skalaen) for it-systemet SKAT Ligning. Derimod er risikoen vurderet til 1 for it-systemerne NTSE og DCS.

I risikovurderingerne for 2020-2021 er der vurderinger af konsekvenserne på et meget overordnet niveau for Skatteforvaltningen. Der er ingen vurderinger af de direkte konsekvenser af de påpegede risici for it-systemet.

30. Risikovurderingerne for både 2019 og 2020-2021 afspejler, at det er vurderinger af det enkelte it-system og ikke vurderinger af de tværgående afhængigheder mellem it-systemer og støttesystemer. Fx fremgår det ikke af risikovurderingen af brugeradgangssystemet AD for 2020-2021, at en række samfundskritiske it-systemer er afhængige af AD for at kunne fungere. Skatteministeriet har oplyst, at ministeriet er enig i, at det skal fremgå af risikovurderingen af AD, og vil tilføje det til risikovurderingen.

31. Udviklings- og Forenklingsstyrelsen udpeger i den samlede risikovurderingsrapport for 2019 og 2020-2021 en række tværgående risici på baggrund af de systemspecifikke risikovurderinger. Én af de tværgående risici i rapporten for 2020-2021 omhandler mangelfulde it-beredskabsplaner, da flere af risikovurderingerne af it-systemerne vurderer, at der mangler beredskabsplaner.

De samlede risikovurderingsrapporter bygger kun på risikovurderinger af it-systemerne og ikke på konsekvens- og risikovurderinger af de forretningsprocesser, som systemerne indgår i.

32. Udviklings- og Forenklingsstyrelsen har fastlagt, at hvis risikovurderingen af et it-system viser, at et nedbrud på systemet eller de forretningsprocesser, som systemet understøtter, vil have alvorlige konsekvenser, skal Skatteministeriet udarbejde og teste en indsatsplan og en nødplan. Ministeriet har imidlertid ikke kunnet anvende risikovurderingerne for 2019 til at vurdere, om ministeriet skal udarbejde indsatsplaner og nødplaner for it-systemerne. Det skyldes, at ministeriet i risikovurderingerne for 2019 ikke har vurderet konsekvenserne af de påpegede risici for it-systemerne. Ministeriet har således ikke fastlagt, hvilke forretningsprocesser og it-systemer ministeriet skal udarbejde indsatsplaner og nødplaner for. Ministeriet har heller ikke brugt risikovurderingerne for 2019 til at tilpasse it-systemernes it-beredskab.

Risikovurderingsrapporten for 2020-2021 og de systemspecifikke risikovurderinger er udarbejdet i maj 2021. Skatteministeriet har endnu ikke fulgt op på risikovurderingerne for 2020-2021.

33. Undersøgelsen viser, at Skatteministeriets ledelse i forbindelse med risikovurderingerne af it-systemerne i 2019 og i 2020-2021 ikke har taget stilling til, hvilke risici ledelsen vil acceptere i forhold til fx datatab eller reetableringstid for it-systemerne ved større it-nedbrud. Det betyder, at den risiko, ministeriet løber i forhold til tab af data, og tidshorisonten for reetablering af it-systemerne, ikke nødvendigvis stemmer overens med ledelsens forventninger.

34. Skatteministeriet har oplyst, at ministeriet ikke finder det fuldt ud relevant at anvende risikovurderingerne som grundlag for at udarbejde it-beredskabsplaner. Det skyldes dels, at det er for omfattende for ministeriets it-portefølje, dels at ministeriet anvender risikovurderingerne i overensstemmelse med ISO 27001 til at vurdere anbefalinger og krav til informationssikkerhed samlet set og ikke kun til it-beredskabet. Ministeriet har oplyst, at ministeriet i stedet har standardiserede krav til it-beredskabet, som følger ISO 27001, fx at der skal være en teknisk reetableringsplan for alle it-systemer. Ministeriet har dog samtidig fastlagt, at hvis en risikovurdering af et it-system viser, at der er en høj sandsynlighed og konsekvens for risici vedrørende it-systemets tilgængelighed, skal ministeriet udarbejde indsatsplaner og nødplaner for it-systemet.

Resultater

Skatteministeriet har i 2019 og i 2020-2021 udarbejdet risikovurderinger af kritiske it-systemer. Risikovurderingerne udgør imidlertid ikke et tilstrækkeligt grundlag for, at ministeriet kan etablere et dækkende it-beredskab. Det skyldes, at risikovurderingerne for 2019 ikke indeholder vurderinger af konsekvenserne af de påpegede risici, og at risikovurderingerne for 2020-2021 kun indeholder vurderinger af konsekvenserne på et overordnet niveau. Endvidere indeholder risikovurderingerne for 2019 meget få vurderinger af risici, som er relevante i forhold til it-beredskabet. Udviklings- og Forenklingsstyrelsen har i risikovurderingerne for 2020-2021 udvalgt 4 risici, som er relevante for it-beredskabet, og som skal vurderes for alle it-systemer. Det er dog ikke alle risikovurderingerne for 2020-2021, som vurderer de 4 risici. Den samlede risikovurderingsrapport for 2020-2021 konkluderer dog, at Skatteministeriet mangler it-beredskabsplaner for en lang række it-systemer.

Ministeriet har ikke anvendt risikovurderingerne for 2019 til at etablere et passende it-beredskab. Ministeriet har endnu ikke fulgt op på risikovurderingerne for 2020-2021.

3. It-beredskabsplaner

Delkonklusion

Skatteministeriet har ikke implementeret nødplaner og indsatsplaner for kritiske forretningsprocesser, men har sikret, at der i overvejende grad er implementeret tilfredsstillende reetableringsplaner.

Skatteministeriet har ikke interne it-beredskabsplaner for de kritiske forretningsprocesser for personskat, moms og selskabsskat, som kan sikre, at ministeriet hurtigt kan håndtere en it-beredskabssituation og dermed reducere følgevirkningerne af hændelsen.

Skatteministeriet har kun udarbejdet én nødplan på hele Skatteforvaltningens område for, hvordan ministeriet skal iværksætte eventuelle nødprocedurer for at opretholde forretningsprocessen i en it-beredskabssituation. Nødplanen vedrører forretningsprocessen for moms. Nødplanen er dog ikke tilfredsstillende, da den kun forholder sig til nedbrud på ét af de 5 it-fagsystemer, som er nødvendige for at opretholde forretningsprocessen. Derudover har ministeriet ikke udarbejdet indsatsplaner for den interne krisestyring i ministeriet for 8 af de 9 undersøgte it-systemer. Ministeriet har for it-systemet eIndkomst udarbejdet en indsatsplan for ministeriets interne krisestyring. Planen er i overvejende grad tilfredsstillende, da den indeholder flere af de elementer, som bør indgå i en indsatsplan.

Skatteministeriet har sikret, at der for 8 af de 9 undersøgte it-systemer er udarbejdet tekniske reetableringsplaner. Ministeriet har endnu ikke udarbejdet en reetableringsplan for ét af de undersøgte it-systemer, som ministeriet har driftet siden 2016. Reetableringsplanerne for 6 af de 8 it-systemer indeholder de fleste af de elementer, der bør indgå i en reetableringsplan. 2 af reetableringsplanerne mangler dog flere af de centrale elementer, som bør indgå i en reetableringsplan, fx en beskrivelse af, hvordan nøddrift iværksættes, og kriterier for at vende tilbage til normal drift. Ministeriet har ikke kendskab til leverandørens reetableringsplan for ét af de 7 eksternt driftede it-systemer. Ministeriet har dermed ikke sikret, at leverandørens reetableringsplan er tilfredsstillende, og at reetableringsplanen hænger sammen med ministeriets eget it-beredskab.

Skatteministeriet har hverken testet nødplanen for moms eller indsatsplanen for eIndkomst. De 8 reetableringsplaner er blevet testet i undersøgelsesperioden. Testene er dog ikke tilstrækkelige, da de ikke indeholder alle de centrale elementer, som er relevante at teste, fx om it-systemets funktionalitet er testet efter reetableringen af systemet.

Det er afgørende, at Skatteministeriet i en beredskabssituation hurtigt kan finde it-beredskabsplanerne for at iværksætte beredskabet. Skatteministeriet har dog i forbindelse med undersøgelsen i flere tilfælde haft vanskeligt ved at fremskaffe de eksisterende it-beredskabsplaner.

35. Dette kapitel handler om Skatteministeriets it-beredskabsplaner for de kritiske forretningsprocesser for personskat, moms og selskabsskat.

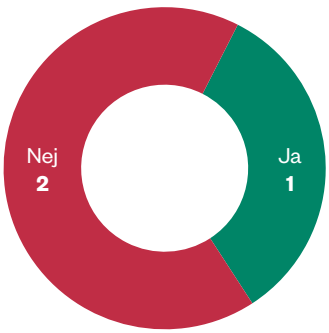
Det kan være hensigtsmæssigt at nedbryde it-beredskabet i operationelle handlingsplaner for forskellige områder. Skatteministeriet har således fastlagt, at it-beredskabet skal bestå af nødplaner for forretningsprocesserne samt indsatsplaner og reetableringsplaner for it-systemerne. Vi har derfor undersøgt, om Skatteministeriet har implementeret tilfredsstillende nødplaner, indsatsplaner og reetableringsplaner for forretningsprocesserne for personskat, moms og selskabsskat. Med tilfredsstillende planer mener vi, at ministeriet dels skal have udarbejdet it-beredskabsplaner, dels skal have testet planerne, og at planerne og testene indeholder de relevante elementer.

3.1. Skatteministeriets nødplaner for forretningsprocesser

36. Vi har undersøgt, om Skatteministeriet har udarbejdet nødplaner for ministeriets kritiske forretningsprocesser. En nødplan har til formål at beskrive, hvordan kritiske forretningsprocesser skal håndteres i en situation, hvor den almindelige it-understøttelse ikke er til rådighed.

37. Figur 5 viser resultatet af vores undersøgelse af, om Skatteministeriet har udarbejdet nødplaner for de 3 forretningsprocesser for personskat, moms og selskabsskat.

Figur 5
Er der nødplaner for forretningsprocesserne for personskat, moms og selskabsskat?



Kilde: Rigsrevisionen på baggrund af dokumentation fra Skatteministeriet.

Det fremgår af figur 5, at Skatteministeriet ikke har udarbejdet nødplaner for 2 af de 3 kritiske forretningsprocesser. Ministeriet har således kun udarbejdet én nødplan for forretningsprocessen for moms, som også omfatter processen for lønsum. Undersøgelsen viser endvidere, at nødplanen for moms og lønsum er den eneste nødplan, som ministeriet har udarbejdet på hele Skatteforvaltningens område.

38. Skatteministeriet har oplyst, at det ikke er meningsfyldt at have en nødplan for manuel drift ved nedbrud i it-systemerne for langt de fleste forretningsprocesser i Skatteforvaltningen, herunder processerne for personskat, moms og selskabsskat. Det skyldes, at forretningsprocesserne i høj grad er automatiserede, og at der er en høj kompleksitet i de understøttede it-systemer. Det medfører, at størstedelen af Skatteforvaltningens forretningsprocesser ikke vil kunne opretholdes uden adgang til it-systemernes data. På den baggrund mener Skatteministeriet, at det i en krisesituation er vigtigere, at der er planer for, hvordan it-systemerne skal reetableres, end at der er nødplaner for forretningsprocesserne.

Skatteministeriet har dog oplyst, at ministeriet vil udarbejde nødplaner for kritiske forretningsprocesser, og at det indledningsvist skal afdækkes, i hvilken grad forretningsprocesserne kan understøttes manuelt. Udarbejdelsen af nødplaner er en del af ministeriets samlede implementeringsplan for at styrke it-beredskabet, jf. pkt. 27.

Rigsrevisionen er opmærksom på, at det kan være vanskeligt at opretholde forretningsprocesserne uden adgang til it-systemerne. Det er dog afgørende, at Skatteministeriet har taget stilling til, hvordan ministeriet håndterer kritiske forretningsprocesser i en beredskabssituation, hvor den almindelige it-understøttelse ikke er til rådighed. Ud over at undersøge mulighederne for manuel drift kan det også være relevant for ministeriet at afdække mulighederne for at anvende en alternativ it-understøttelse. Desuden er det relevant, at ministeriet overvejer, hvordan ministeriet vil håndtere kortvarige og længerevarende nedbrud samt omfattende datatab.

39. Vi har undersøgt, om nødplanen for moms og lønsum er tilfredsstillende. Det har vi undersøgt ved at afdække, om planen indeholder de centrale elementer, som en nødplan skal indeholde ifølge ISO 27001, Digitaliseringsstyrelsen og Beredskabsstyrelsen. De fleste af elementerne indgår også i Skatteministeriets skabelon for nødplaner. Tabel 1 viser vores gennemgang af nødplanen for moms og lønsum.

Tabel 1

Rigsrevisionens gennemgang af Skatteministeriets nødplan for moms og lønsum

Elementer i nødplanen for moms og lønsum	
Er planen ajourført årligt?	🔴
Beskriver planen, hvornår den aktiveres?	🟢
Omfatter planen alle centrale it-systemer i forretningsprocessen?	🔴
Fremgår der kontaktoplysninger på nøglepersoner internt i Skatteministeriet?	🟢
Beskriver planen rolle- og ansvarsfordelingen internt i Skatteministeriet?	🟢
Beskriver planen konkrete nødprocedurer eller aktiviteter?	🟡
Er det besluttet, hvor planen opbevares, så man ved, hvor den er i en it-beredskabssituation?	🔴

🟢 Indgår i nødplanen 🟡 Indgår delvist i nødplanen 🔴 Indgår ikke i nødplanen

Kilde: Rigsrevisionen på baggrund af en gennemgang af nødplanen for moms og lønsum.

Det fremgår af tabel 1, at Skatteministeriets nødplan for moms og lønsum bl.a. indeholder kontaktoplysninger om nøglepersoner og rolle- og ansvarsfordelingen internt i Skatteministeriet. Nødplanen er dog ikke ajourført og indeholder ikke alle de centrale elementer, der bør fremgå af en nødplan. Nødplanen omfatter således ikke alle de it-systemer, som indgår i forretningsprocessen, men omhandler kun nedbrud på ét it-system (NTSE) i forretningsprocessen. Nedbrud på NTSE betyder, at virksomheder ikke kan indberette ordinær moms i NTSE. Nødplanen omhandler ikke nedbrud på de øvrige 5 it-fagsystemer i momsprocessen, fx nedbrud på Skattekontoen, som bl.a. giver overblik over virksomhedernes ind- og udbetalinger af moms.

Skatteministeriet har oplyst, at ministeriet endnu ikke har kortlagt de alternative forretningsprocedurer, og at nødplanen for moms og lønsum derfor ikke er udtryk for en systematisk og struktureret nødplan.

Resultater

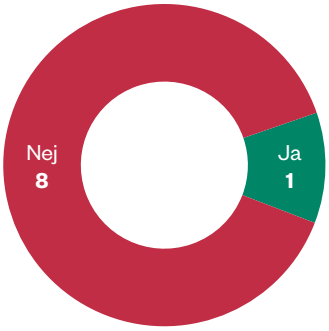
Skatteministeriet har kun udarbejdet én nødplan på hele Skatteforvaltningens område. Nødplanen vedrører forretningsprocessen for moms og lønsum. Planen er imidlertid ikke tilfredsstillende, da den ikke er ajourført og ikke indeholder alle de centrale elementer, der bør fremgå af en nødplan. Fx forholder nødplanen sig kun til nedbrud på ét af de 5 it-systemer, der indgår i forretningsprocessen for moms.

3.2. Skatteministeriets indsatsplaner for it-systemer

40. Vi har undersøgt, om Skatteministeriet har udarbejdet indsatsplaner for de it-systemer, som indgår i forretningsprocesserne for personskat, moms og selskabsskat. Formålet med indsatsplaner er at fastlægge, hvordan krisestyringen skal foregå i Skatteministeriet, og at understøtte en effektiv intern og ekstern kommunikation for at minimere eventuelle følgevirkninger af større it-nedbrud.

41. Figur 6 viser resultatet af vores undersøgelse af, om der er udarbejdet indsatsplaner for de 9 undersøgte it-systemer i forretningsprocesserne for personskat, moms og selskabsskat.

Figur 6
Er der indsatsplaner for de 9 it-systemer i forretningsprocesserne for personskat, moms og selskabsskat?



Kilde: Rigsrevisionen på baggrund af dokumentation fra Skatteministeriet.

Det fremgår af figur 6, at Skatteministeriet kun har udarbejdet én indsatsplan, som vedrører it-systemet eIndkomst. For de 8 øvrige it-systemer har Skatteministeriet ikke udarbejdet indsatsplaner.

42. Vi har i undersøgelsen efterspurgt indsatsplaner for de undersøgte it-systemer. Skatteministeriet oplyste først, at ministeriet ikke havde særskilte indsatsplaner for it-systemerne. Senere blev vi på et møde opmærksomme på, at der alligevel var en indsatsplan for eIndkomst.

43. Skatteministeriet har oplyst, at ministeriet vurderer, at indsatsplaner er mindre væsentlige end reetableringsplaner, da indsatsplaner kun vedrører kommunikation, eskalering og planlægning af driften, som ad hoc kan håndteres via styrelsernes overordnede beredskabsplaner. Reetableringsplanerne skal sikre, at it-systemerne rent faktisk kan reetableres. Rigsrevisionen er enig i, at reetableringsplaner er helt grundlæggende for, at it-systemer kan reetableres. Rigsrevisionen finder samtidig, at konkrete indsatsplaner er en forudsætning for, at ministeriet kan reagere hurtigt og effektivt i en beredskabssituation og dermed kan minimere konsekvenserne af krisen. En ad hoc-baseret løsning er ikke tilstrækkelig, da det netop i en beredskabssituation er afgørende, at ministeriet kan handle hurtigst muligt for at stoppe krisen.

Endvidere kan der være beredskabssituationer, hvor en indsatsplan er helt afgørende, fx i en situation, hvor der opstår korrupte data i ét eller flere it-systemer. Her handler det i første omgang om at få stoppet spredningen af korrupte data hurtigst muligt. Dette håndteres bl.a. ved en indsatsplan.

I forlængelse af Skatteministeriets kortlægning af it-beredskabet for 7 samfundskritiske it-systemer har ministeriet udarbejdet en implementeringsplan for at styrke it-beredskabet, jf. pkt. 27. Implementeringsplanen indebærer bl.a., at ministeriet vil udarbejde en proces og vejledning om kommunikation i en beredskabssituation, herunder fordeling af roller og ansvar i forhold til interne og eksterne interessenter. Ministeriet vil endvidere arbejde med at få inddraget alle de relevante personer for de enkelte it-systemer i beredskabsplanlægningen og uddanne dem i deres ansvar og opgaver i forhold til it-beredskabet.

44. Vi har undersøgt, om indsatsplanen for it-systemet eIndkomst er tilfredsstillende. Det har vi undersøgt ved at afdække, om indsatsplanen indeholder de centrale elementer, som ISO 27001, Digitaliseringsstyrelsen og Beredskabsstyrelsen anbefaler skal indgå i en plan for den interne krisestyring. Flere af disse elementer indgår også i Udviklings- og Forenklingsstyrelsens skabelon for indsatsplaner. Tabel 2 viser vores gennemgang af indsatsplanen for eIndkomst.

Tabel 2

Rigsrevisionens gennemgang af Skatteministeriets indsatsplan for eIndkomst

Elementer i indsatsplanen for eIndkomst	
Er planen ajourført årligt?	●
Beskriver planen, hvornår den aktiveres?	●
Beskriver planen, hvor krisestaben mødes?	●
Fremgår der kontaktoplysninger på nøglepersoner internt i Skatteministeriet?	●
Fremgår der kontaktoplysninger på eksterne interessenter?	●
Beskriver planen rolle- og ansvarsfordelingen internt i Skatteministeriet?	●
Beskriver planen, hvilke it-systemer der påvirkes af et systemnedbrud eller datatab?	●
Indgår der beskrivelser af kommunikation til eksterne og interne aktører?	●
Er det besluttet, hvor planen opbevares, så man ved, hvor den er i en it-beredskabssituation?	●

● Indgår i indsatsplanen ● Indgår ikke i indsatsplanen

Kilde: Rigsrevisionen på baggrund af en gennemgang af indsatsplanen for eIndkomst.

Det fremgår af tabel 2, at indsatsplanen for eIndkomst indeholder flere af de elementer, som bør indgå i en indsatsplan. Indsatsplanen indeholder fx en kontaktliste med nøglepersoner og en kort beskrivelse af nøglepersonernes rolle og organisatoriske placering, fx nøglepersoner fra Udviklings- og Forenklingsstyrelsen, Skattestyrelsen og leverandøren. Indsatsplanen indeholder dog ikke overvejelser om eller beskrivelser af kommunikationen til andre styrelser i Skatteministeriet eller til eksterne interessenter, ligesom den ikke indeholder kontaktoplysninger på eksterne interessenter.

45. Selv om der ikke er udarbejdet en selvstændig indsatsplan for brugeradgangssystemet AD, som er internt driftet i Skatteministeriet, viser vores gennemgang, at reetableringsplanen for AD indeholder flere af de elementer, som skal indgå i en indsatsplan. Indsatsplanen indeholder således kontaktoplysninger på forskellige relevante nøglepersoner i Udviklings- og Forenklingsstyrelsen og i andre af styrelser under Skatteministeriet. Indsatsplanen indeholder også beskrivelser af rolle- og ansvarsfordelingen internt i Udviklings- og Forenklingsstyrelsen, herunder en beskrivelse af, hvem der er kommunikationsansvarlig i en it-beredskabssituation. Indsatsplanen mangler dog centrale elementer, der bør fremgå af en indsatsplan, fx en beskrivelse af kommunikation til interne og eksterne interessenter og en beskrivelse af, hvilke øvrige it-systemer der bliver påvirket ved et nedbrud på AD.

Proces for incidents
Skatteministeriets proces for incidents håndterer ikke-planlagte afbrydelser af en it-service eller reduktion i kvaliteten af it-servicen. Fejl, der endnu ikke har haft konsekvenser for it-systemet, er også incidents.

Proces for major incidents
Skatteministeriets proces for major incidents behandler alle hændelser, som har en meget stor effekt på Skatteministeriet, og som ikke umiddelbart kan løses.

46. Skatteministeriet har oplyst, at selv om indsatsplaner og nødplaner endnu ikke er implementeret, kan it-hændelser i betydeligt omfang håndteres gennem ministeriets processer for incidents og major incidents samt gennem Udviklings- og Forenklingsstyrelsens generelle beredskabsplan.

I Skatteministeriets procesbeskrivelser for incidents og major incidents fremgår det, hvordan ministeriet skal håndtere alle typer af it-hændelser, som påvirker den daglige it-drift. It-hændelserne kan vedrøre både mindre it-forstyrrelser – fx en ikke-planlagt afbrydelse af en it-service – og større it-nedbrud. Procesbeskrivelsen for major incidents omhandler, hvilke overordnede aktiviteter ministeriet skal igangsætte ved en it-hændelse. Fx er der beskrivelser af kommunikationen til ledelse og interessenter. Det fremgår også, at der skal nedsættes en arbejdsgruppe med en hovedansvarlig (major incident manager), som skal løse it-hændelsen. Gruppen dannes ad hoc med personer, som har kendskab til it-systemerne. Det betyder, at ministeriet først i selve situationen tager stilling til, hvilke personer det er relevant at inddrage i håndteringen af it-hændelsen.

Udviklings- og Forenklingsstyrelsen har oplyst, at en major incident manager ikke har adgang til reetableringsplaner og eventuelle indsatsplaner og nødplaner for it-systemerne. I reetableringsplanerne er der fx kontaktoplysninger til leverandøren og oplysninger om fordelingen af opgaver, roller og ansvar mellem leverandøren og Skatteministeriet i en it-beredskabssituation. En major incident manager skal således først fremskaffe disse oplysninger hos de relevante medarbejdere i Udviklings- og Forenklingsstyrelsen. Det fremgår endvidere ikke af procesbeskrivelserne for incidents og major incidents eller af andet materiale, hvordan leverandørens reetableringsplaner og ministeriets eventuelle indsatsplaner og nødplaner skal indgå i processen for major incidents. Udviklings- og Forenklingsstyrelsen har oplyst, at styrelsens generelle beredskabsplan aktiveres, hvis en major incident bliver til en krise, dvs. en hændelse, der ikke kan håndteres via de normale driftsprocedurer.

Rigsrevisionen konstaterer, at Skatteministeriet med processen for major incidents har en ramme for, hvordan daglige it-problemer og større it-nedbrud skal håndteres. Ministeriet mangler dog konkrete planer, informationer mv. for, hvordan ministeriet gennem sin proces for major incidents vil håndtere en it-beredskabssituation for de enkelte it-systemer. Rigsrevisionen bemærker, at tid er en væsentlig faktor i en beredskabssituation. Det er derfor helt afgørende, at ministeriet har udarbejdet konkrete planer for, hvordan beredskabssituationen skal håndteres. Det er ligeledes afgørende, at en major incident manager har adgang til de relevante oplysninger i en beredskabssituation.

Resultater

Skatteministeriet har kun udarbejdet en indsatsplan for ét af de 9 undersøgte it-systemer. Dermed er der ikke udarbejdet indsatsplaner for ministeriets krisehåndtering i tilfælde af større nedbrud i de systemer, som er afgørende for, at forretningsprocesserne for personskat, moms og selskabsskat kan fungere.

Skatteministeriet har udarbejdet en indsatsplan for it-systemet eIndkomst, som i overvejede grad er tilfredsstillende, da den indeholder flere af de elementer, som bør fremgå af en indsatsplan. Indsatsplanen indeholder dog ikke overvejelser om eller beskrivelser af kommunikationen til andre styrelser i Skatteministeriet eller til eksterne interessenter.

Rigsrevisionens gennemgang viser, at reetableringsplanen for brugeradgangssystemet AD, som er internt driftet, indeholder nogle af de elementer, der bør fremgå af en indsatsplan. Reetableringsplanen indeholder fx kontaktlister og beskrivelser af rolle- og ansvarsfordelinger internt i Udviklings- og Forenklingsstyrelsen og i andre styrelser i Skatteministeriet. Indsatsplanen indeholder dog ikke alle de centrale elementer, der bør fremgå af en indsatsplan for ministeriets krisestyring.

Skatteministeriet har en overordnet proces til at håndtere it-hændelser, som ministeriet kan anvende i en it-beredskabssituation. Håndteringen vil dog foregå ad hoc, da ministeriet ikke har konkrete planer for at håndtere en it-beredskabssituation for de enkelte it-systemer. De personer, som skal håndtere processen, mangler desuden adgang til centrale informationer, fx kontaktoplysninger til leverandøren og øvrige interessenter, som er afgørende for, at ministeriet hurtigt og effektivt kan håndtere en it-beredskabssituation.

3.3. Reetableringsplaner for it-systemer

47. Vi har undersøgt, om Skatteministeriet har sikret, at der er udarbejdet reetableringsplaner for de 9 it-systemer, som indgår i forretningsprocesserne for personskat, moms og selskabsskat. En reetableringsplan indeholder bl.a. en teknisk beskrivelse af, hvordan et it-system skal reetableres, og skal sikre, at it-systemet kan reetableres inden for en ønsket tidsperiode. Ligesom nødplanen og indsatsplanen skal reetableringsplanen også indeholde beskrivelser af bl.a. leverandørens kriseorganisation, kontaktlister over nøglepersoner og en rolle- og ansvarsfordeling.

48. Hvis it-systemerne driftes af eksterne leverandører, er det leverandørerne, som udarbejder reetableringsplaner for systemerne. Skatteministeriet kan i kontrakten med en leverandør stille krav til leverandørens reetableringsplaner og til andre forhold i relation til reetableringsplanen. Ministeriet kan fx stille krav til, hvor lang tid det maksimalt må tage for leverandøren at reetablere it-systemet ved et nedbrud, eller krav til årlige test af reetableringsplanen.

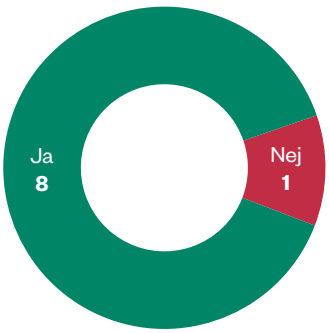
49. Skatteministeriet har i forbindelse med undersøgelsen i flere tilfælde haft vanskeligt ved at fremskaffe de gældende reetableringsplaner, som Rigsrevisionen har efterspurgt.

Ajourførte og godkendte reetableringsplaner

50. Vi har undersøgt, om der er udarbejdet reetableringsplaner for hvert af de 9 it-systemer, der indgår i forretningsprocesserne for personskat, moms og selskabsskat. Herunder har vi undersøgt, om reetableringsplanerne er ajourførte, og om Skatteministeriet har modtaget og godkendt leverandørernes reetableringsplaner.

51. Figur 7 viser resultatet af vores undersøgelse af, om der er udarbejdet reetableringsplaner for de 9 undersøgte it-systemer.

Figur 7
Er der reetableringsplaner for de 9 it-systemer i forretningsprocesserne for personskat, moms og selskabsskat?



Kilde: Rigsrevisionen på baggrund af dokumentation fra Skatteministeriet.

Det fremgår af figur 7, at der for 8 af de 9 undersøgte it-systemer er udarbejdet en reetableringsplan. Skatteministeriet har endnu ikke en reetableringsplan for it-systemet FTPS-Gateway, men er ved at udarbejde den.

52. Det er Udviklings- og Forenklingsstyrelsen, som udarbejder reetableringsplaner for AD og FTPS-Gateway, da it-systemerne er internt driftet i Skatteministeriet. Styrelsen har oplyst, at der skal udarbejdes en reetableringsplan for FTPS-Gateway for hvert af de ca. 10 it-systemer, som FTPS-Gateway har integrationer med. I 2020 har styrelsen udarbejdet det første udkast til en reetableringsplan for FTPS-Gateway og for it-systemet eKapital. Styrelsen mangler dermed at udarbejde 9 af de ca. 10 reetableringsplaner, der skal være for FTPS-Gateway. FTPS-Gateway har været internt driftet i Udviklings- og Forenklingsstyrelsen siden 2016.

53. Vores gennemgang viser, at de 8 undersøgte reetableringsplaner er blevet opdateret i løbet af 2020 og typisk bliver opdateret én gang årligt.

54. Det er Skatteministeriets opgave at føre tilsyn med leverandørernes reetableringsplaner. Det gør ministeriet fx ved at modtage og godkende leverandørernes reetableringsplaner.

Vores gennemgang viser, at Udviklings- og Forenklingsstyrelsen har modtaget og godkendt reetableringsplaner for 6 af de 7 it-systemer, som driftes af eksterne leverandører. Leverandøren har vurderet, at reetableringsplanen for elndkomst er fortrolig. Styrelsen har derfor ikke indhentet eller godkendt reetableringsplanen. Vi har dog modtaget reetableringsplanen for elndkomst i forbindelse med vores undersøgelse.

55. Ministeriet kan som en del af tilsynet med leverandørerne også stille krav om, at leverandørerne hvert år får et revisionsfirma til at udarbejde en ISAE 3402-erklæring. Revisorerklæringen har til formål at dokumentere, at leverandøren lever op til bl.a. ISO 27001, herunder at leverandøren har udarbejdet it-beredskabsplaner og testet dem.

Undersøgelsen viser, at Udviklings- og Forenklingsstyrelsen har modtaget ISAE 3402-erklæringer for alle de 7 eksternt driftede systemer for 2018 og 2019. Der har i revisorerklæringerne ikke været bemærkninger til it-beredskabet – med undtagelse af revisorerklæringen for 2019 for elndkomst, hvor det fremgår, at it-beredskabsplanen ikke er testet.

ISAE 3402-erklæring
En ISAE 3402-erklæring er en erklæring, hvor it-revisoren udtaler sig om, hvorvidt leverandørens beskrivelse af ydelser og systemer er retvisende, hvorvidt leverandørens generelle it-kontroller er hensigtsmæssigt udformet, og om disse kontroller har fungeret tilfredsstillende i regnskabsperioden.

Gennemgang af centrale elementer i reetableringsplanerne

56. Vi har undersøgt, om it-systemernes reetableringsplaner er tilfredsstillende. Det har vi undersøgt ved at afdække, om reetableringsplanerne indeholder udvalgte centrale elementer, som ISO 27001, Digitaliseringsstyrelsen og Beredskabsstyrelsen anbefaler skal indgå i en reetableringsplan. Flere af elementerne indgår også i Udviklings- og Forenklingsstyrelsens egen skabelon for reetableringsplaner. Tabel 3 viser resultaterne af vores undersøgelse.

Tabel 3
Rigsrevisionens gennemgang af reetableringsplaner for 9 it-systemer

	Eksternt driftede it-systemer							Internt driftede it-systemer	
	SAP Classic	DXC Mainframe	Skatte-kontoen	eIndkomst	DCS	NTSE	SKAT Ligning	AD	FTPS-Gateway
Beskriver planen, hvornår den aktiveres?	●	●	●	●	●	●	●	●	
Beskriver planen eller kontrakten kriterierne for at vende tilbage til normal drift?	●	●	●	●	●	●	●	●	
Er det besluttet, hvor planen opbevares, så man ved, hvor den er i en it-beredskabssituation?	●	●	●	●	●	●	●	●	
Fremgår der kontaktoplysninger på nøglepersoner hos leverandøren og Skatteministeriet?	●	●	●	●	●	●	●	●	
Beskriver planen rolle- og ansvarsfordelingen mellem leverandør og Udviklings- og Forenklingsstyrelsen?	●	●	●	●	●	●	●	-	
Fremgår der krav til RTO af planen eller kontrakten?	●	●	●	●	●	●	●	●	
Fremgår der krav til RPO af planen eller kontrakten?	●	●	●	●	●	●	●	●	
Beskriver planen nødvendige aktiviteter for at reetablere it-systemet?	●	●	●	●	●	●	●	●	
Beskriver planen, hvordan it-systemet kan køre i nøddrift?	●	●	●	●	●	●	●	●	

● Indgår i reetableringsplanen ● Indgår ikke i reetableringsplanen

Note: (-) betyder, at elementet ikke er relevant for reetableringsplanen. Det røde felt ved FTPS-Gateway markerer, at Skatteministeriet ikke har en færdig reetableringsplan for it-systemet.

Kilde: Rigsrevisionen på baggrund af en gennemgang af de seneste reetableringsplaner for de 9 it-systemer.

Nøddrift
Nøddrift betyder, at it-systemet kører med reduceret kapacitet, fx 50 % af systemets fulde kapacitet. It-systemet kan i en beredskabssituation køre på nøddrift, indtil systemet er fuldt reetableret. Nøddrift ved et it-system, der har tocenterdrift, vil typisk være, at systemet kun kører ved hjælp af det ene center og derfor må køre med reduceret kapacitet.

Reetableringsplaner for de 7 eksternt driftede it-systemer

57. Som det fremgår af tabel 3, er der enkelte mangler i reetableringsplanerne for 6 af de 7 eksternt driftede it-systemer. Reetableringsplanen for SKAT Ligning mangler 4 af de 9 centrale elementer, der bør fremgå af en reetableringsplan.

Vores undersøgelse viser, at der i 2 af reetableringsplanerne for de eksternt driftede it-systemer mangler beskrivelser af rolle- og ansvarsfordelingen mellem Udviklings- og Forenklingsstyrelsen og leverandøren i en beredskabssituation. Det drejer sig om Skattekontoen og SKAT Ligning.

Undersøgelsen viser, at der i 3 af reetableringsplanerne for de eksternt driftede it-systemer er beskrivelser af, hvordan nøddrift iværksættes ved en beredskabssituation. I de øvrige 4 planer fremgår det af reetableringsplanen, at der er reduceret kapacitet ved nøddrift, men derudover er der ingen beskrivelse af, hvordan nøddriften iværksættes.

58. Fastsættelse af krav til den maksimale reetableringstid (RTO) og det maksimale datatab (RPO) for it-systemerne er helt centrale for it-beredskabet, da de har betydning for, hvor hurtigt Skatteministeriet i tilfælde af større nedbrud og datatab kan komme tilbage til normal drift og dermed varetage sine opgaver. Undersøgelsen viser, at reetableringsplanerne for 6 af de 7 eksternt driftede it-systemer har krav til, hvor lang tid der maksimalt må gå, før systemet skal være reetableret efter et nedbrud (RTO). I reetableringsplanen for SKAT Ligning fremgår det, at kravet til den maksimale reetableringstid (RTO) er på mere end 72 timer. I leverandørens it-beredskabsplan fremgår det, at det specifikke antal dage skal aftales med kunden, når der er et krav om en maksimal reetableringstid på mere end 72 timer. Vi har i forbindelse med undersøgelsen ikke modtaget dokumentation for, at Udviklings- og Forenklingsstyrelsen har indgået nærmere aftale med leverandøren om den maksimale reetableringstid. Det betyder, at der ikke er aftalt en øvre tidsgrænse for, hvornår SKAT Ligning skal være reetableret.

Derudover viser undersøgelsen, at der for alle 7 eksternt driftede it-systemer fremgår krav til det maksimale datatab (RPO) i reetableringsplanen, kontrakten eller af anden dokumentation.

Reetableringsplaner for de 2 internt driftede it-systemer

59. Vi har kun gennemgået reetableringsplanen for brugeradgangssystemet AD, da reetableringsplanen for FTPS-Gateway stadig er under udarbejdelse. Vores gennemgang af reetableringsplanen for AD viser, at halvdelen af de centrale elementer mangler i reetableringsplanen.

Som det fremgår af tabel 3, indeholder reetableringsplanen for AD ingen beskrivelser af kriterierne for at vende tilbage til normal drift og ingen beskrivelser af mulighederne for nøddrift i en beredskabssituation. Nøddrift af it-systemet kan være relevant ved de systemer, hvor et nedbrud påvirker en kritisk forretningsproces, og hvor systemet kan køre med reduceret kapacitet. Udviklings- og Forenklingsstyrelsen har oplyst, at det vil blive præciseret i reetableringsplanen for AD, hvordan AD kan køre i nøddrift.

Gennemgangen viser endvidere, at reetableringsplanen for AD ikke indeholder krav til det maksimale datatab (RPO). Udviklings- og Forenklingsstyrelsen har oplyst, at der hver dag tages backup af AD. Det betyder, at RPO er på mindst 24 timer.

Vores gennemgang viser desuden, at reetableringsplanen for AD ikke indeholder en tilstrækkelig beskrivelse af de aktiviteter, som er nødvendige for at kunne reetablere it-systemet. Udviklings- og Forenklingsstyrelsen har oplyst, at reetableringen af AD generelt gennemføres i henhold til generelle instruktioner, som også er gældende for andre it-systemer. Rigsrevisionen vurderer dog, at der mangler en beskrivelse af, hvordan systemet kommer op at køre ved en reetablering.

RTO
Recovery Time Objective (RTO) er den tid, som det maksimalt må tage at reetablere it-systemet.

RTO omtales i beretningen som den maksimale reetableringstid.

RPO
Recovery Point Objective (RPO) er den maksimale tidsperiode, hvor der må være tab af data i it-systemet. RPO er dermed udtryk for den tid, man må gå tilbage for at finde den seneste brugbare backup.

RPO omtales i beretningen som det maksimale datatab.

Resultater

Rigsrevisionens gennemgang viser, at der for 8 af de 9 it-systemer, der indgår i forretningsprocesserne for personskat, moms og selskabsskat, er udarbejdet en reetableringsplan, som ajourføres årligt. Skatteministeriet har ikke en reetableringsplan for it-systemet FTPS-Gateway, som har været internt driftet i ministeriet siden 2016. Ministeriet er dog i gang med at udarbejde en reetableringsplan.

Skatteministeriet har godkendt reetableringsplanerne for 6 af de 7 it-systemer, som er driftet af eksterne leverandører. Ministeriet har ikke indhentet og godkendt reetableringsplanen for elndkomst, da leverandøren har vurderet, at reetableringsplanen er fortrolig. Ministeriet har dermed ikke sikret, at leverandørens reetableringsplan er tilfredsstillende, og at ministeriets eget it-beredskab hænger sammen med leverandørens reetableringsplan.

Undersøgelsen viser, at 6 af de 8 reetableringsplaner i overvejende grad er tilfredsstillende, da de indeholder de fleste af de centrale elementer, som ISO 27001, Digitaliseringsstyrelsen og Beredskabsstyrelsen anbefaler skal indgå i en reetableringsplan. 5 af reetableringsplanerne indeholder dog ikke en beskrivelse af, hvordan nøddrift iværksættes. Reetableringsplanerne for SKAT Ligning og brugeradgangssystemet AD er ikke tilfredsstillende, da de mangler ca. halvdelen af de centrale elementer, som en reetableringsplan bør indeholde.

3.4. Test af it-beredskabet

60. Vi har undersøgt, om Skatteministeriet har testet it-beredskabsplanerne tilstrækkeligt. Ifølge ISO 27001 skal it-beredskabsplanerne testes og evalueres jævnligt for at få viden om, hvordan beredskabsplanerne virker i en konkret beredskabssituation. Skatteministeriet har også fastlagt, at ministeriets indsatsplaner skal testes én gang om året.

Test af nødplan og indsatsplan

61. Skatteministeriet har udarbejdet en nødplan for forretningsprocessen moms og lønsum og en indsatsplan for it-systemet elndkomst.

Vores undersøgelse viser imidlertid, at Skatteministeriet ikke har testet nødplanen for moms og lønsum eller indsatsplanen for elndkomst. Ministeriet har dermed ikke viden om, hvordan ministeriets interne it-beredskabsplaner fungerer i en beredskabssituation.

Test af reetableringsplaner

62. Vi har undersøgt, om reetableringsplanerne for de undersøgte 9 it-systemer er blevet testet i perioden 2018-2020. Reetableringsplanerne skal testes med jævne mellemrum for at sikre, at it-systemet kan reetableres i overensstemmelse med de krav, der er opstillet for reetableringen. Det skal fx testes, at reetableringen af it-systemet sker uden fejl, og at den maksimale tid, det må tage at reetablere systemet (RTO), kan overholdes.

63. Undersøgelsen viser, at reetableringsplanerne for 8 af de 9 it-systemer er blevet testet i perioden 2018-2020. Udviklings- og Forenklingsstyrelsen har endnu ikke testet reetableringsplanen for FTPS-Gateway, da den er under udarbejdelse. Styrelsen ved derfor ikke, om systemet kan reetableres.

64. Vi har gennemgået den seneste test af reetableringsplanerne for de 9 it-systemer for at undersøge, om planerne er testet tilstrækkeligt. Det har vi undersøgt ved at afdække, om testene indeholder udvalgte centrale elementer, som primært fremgår af ISO 27001 og ISO 27002. Resultaterne fremgår af tabel 4.

Tabel 4
Rigsrevisionens gennemgang af testrapporter for 9 it-systemer

	Eksternt driftede it-systemer							Internt driftede it-systemer	
	SAP Classic	DXC Mainframe	Skatte-kontoen	eIndkomst	DCS	NTSE	SKAT Ligning	AD	FTPS-Gateway
Er it-systemet blevet testet årligt i perioden 2018-2020?	●	●	●	●	●	●	●	●	
Deltager Skatteministeriet i testen?	●	●	●	●	●	●	●	-	
Er funktionaliteten af it-systemet blevet testet?	●	●	●	●	●	●	●	●	
Er RTO blevet testet?	●	●	●	●	●	●	●	●	
Beskriver rapporten forbedringsforslag?	●	●	●	●	●	●	●	●	
Er test og evaluering godkendt af Skatteministeriet?	●	●	●	●	●	●	●	●	

● Indgår i testen ● Indgår ikke i testen

Note: (-) betyder, at elementet ikke er relevant, da AD er internt driftet. FTPS-Gateway er markeret med rødt, da reetableringsplanen for it-systemet er under udarbejdelse og ikke er blevet testet.

Vi har ikke undersøgt, om RPO er testet, da kontrol med, om der foretages de aftalte backups, typisk er en del af den daglige drift, som leverandørerne løbende rapporterer om til Skatteministeriet.

Kilde: Rigsrevisionen på baggrund af en gennemgang af de seneste testrapporter for de 9 it-systemer.

Det fremgår af tabel 4, at testene ikke indeholder alle de centrale elementer, som bør indgå i en test af reetableringsplanen. Ved test af reetableringsplanen er det fx vigtigt, at det ikke kun er selve it-systemet, der kan reetableres med succes, men også at systemets funktionalitet efter reetableringen testes. Vores gennemgang viser, at funktionaliteten af 5 af de 8 it-systemer ikke er blevet testet. Gennemgangen viser, at det kun fremgår af testrapporten for ét it-system (SKAT Ligning), hvor mange timer det tog at reetablere systemet ved testen. For de øvrige it-systemer fremgår det ikke af testrapporterne, om der er fulgt op på, om kravet til den maksimale reetableringstid (RTO) kunne overholdes ved testen, eller hvor lang tid det har taget at reetablere systemet ved testen.

Vores gennemgang viser også, at testrapporterne for 4 af de 8 it-systemer ikke indeholder observationer, anbefalinger eller forbedringsforslag på baggrund af testen, som kan anvendes til at forbedre it-beredskabet eller indgå som læringsperspektiv. Nogle af de få anbefalinger, der fremgår af de øvrige 4 testrapporter, er fx justeringer til reetableringsplanen og forslag til, hvilke scenarier eller dele af it-systemet der skal indgå ved næste test af reetableringsplanen.

65. Gennemgangen viser, at 2 af reetableringsplanerne ikke er blevet testet årligt. Det vedrører reetableringsplanerne for eIndkomst og AD.

Undersøgelsen viser desuden, at den første test af AD siden 2011 er udført i oktober 2020. Udviklings- og Forenklingsstyrelsen testede, om reetableringsplanen virkede i praksis, og testen viste, at der var fejl i reetableringsproceduren for AD. Styrelsen har på den baggrund testet AD igen i januar 2021, hvor testresultatet viste, at AD kunne reetableres. Rigsrevisionen vurderer dog, at opsætningen af den nye test er meget begrænset, og at testen derfor er mangelfuld. Fx har Udviklings- og Forenklingsstyrelsen ikke testet, om systemet virker som det skal efter reetableringen af systemet. Styrelsen har oplyst, at AD fremover vil blive testet hvert år, og at RTO vil blive testet ved den næste test.

Restoretest
En restoretest er en test af reetableringen af dele af it-systemet (en delmængde af en disaster recovery test), fx at genskabe en fil eller database.

Disaster recovery test
En disaster recovery test er en test, hvor hele it-systemet reetableres på baggrund af den seneste backup på en tom server.

66. Vores gennemgang af test af reetableringsplanerne i perioden 2018-2020 viser, at flere af leverandørerne skiftevis hvert 2. år udfører en restoretest af dele af it-systemet og hvert 2. år en disaster recovery test. Ved en disaster recovery test reetableres it-systemet på en tom server ud fra den seneste backup af systemet. Undersøgelsen viser, at der i undersøgelsesperioden ikke har været en disaster recovery test af reetableringsplanen for SAP Classic og Skattekontoen. Leverandøren for Skattekontoen og SAP Classic har dog udført flere restoretest af dele af it-systemerne.

67. Undersøgelsen viser, at der for ingen af it-systemerne er udarbejdet en flerårig testcyklus, som viser, hvordan hele systemet skal testes over en årrække. Der fremgår ikke krav til fastsættelse af testcyklus i kontrakterne med leverandørerne. Udviklings- og Forenklingsstyrelsen har i forbindelse med undersøgelsen identificeret en 4-årig plan for test af Skattekontoen fra leverandøren.

Resultater

Skatteministeriet har ikke testet nødplanen for moms og lønsum og indsatsplanen for eIndkomst. Ministeriet har dermed ikke viden om, hvordan ministeriets interne it-beredskabsplaner fungerer i en beredskabssituation.

Reetableringsplanerne for 8 af de 9 undersøgte it-systemer er blevet testet i perioden 2018-2020. Reetableringsplanerne er dog ikke testet tilstrækkeligt, da testene ikke indeholder alle de centrale elementer, som bør indgå i en test af reetableringsplaner. Fx er funktionaliteten af it-systemerne ved 5 af de 8 it-systemer ikke blevet testet, ligesom det kun for ét system er blevet testet, hvor mange timer det reelt tog at få reetableret systemet.

Skatteministeriet testede i 2020 for første gang siden 2011 brugeradgangssystemet AD. Testen viste fejl i reetableringsproceduren. Ministeriet udførte på den baggrund en ny test af AD i 2021. Rigsrevisionen vurderer, at testen i 2021 er mangelfuld. Ministeriet har ikke testet reetableringsplanen for det internt driftede it-system FTPS-Gateway, da planen er under udarbejdelse. Ministeriet ved derfor ikke, om systemet kan reetableres.

4. Koordinering af it-beredskabet

Delkonklusion

Skatteministeriet har ikke koordineret it-beredskabet for de it-systemer, der indgår i de kritiske forretningsprocesser.

Skatteministeriet har ikke systematisk kortlagt afhængighederne mellem de it-systemer, der indgår i forretningsprocesserne for personskat, moms og selskabsskat. Ministeriet har bl.a. ikke kortlagt, hvilke it-systemer der skal være i drift, før de øvrige it-systemer i forretningsprocesserne er funktionsdygtige. Ministeriets manglende overblik over afhængighederne mellem it-systemerne kan være problematisk i en beredskabssituation. Det skyldes, at overblik over, hvilke it-systemer og forretningsprocesser der bliver påvirket ved et større nedbrud eller datatab i ét af systemerne er afgørende for, at ministeriet kan minimere følgevirkningerne.

Skatteministeriet har endvidere ikke har taget stilling til eller aftalt med leverandørerne, i hvilken rækkefølge ministeriets it-systemer skal reetableres, i tilfælde af at alle eller flere systemer går ned samtidigt. Ministeriet har heller ikke taget stilling til, hvilke it-systemer der skal prioriteres højest i en beredskabssituation, hvor der kan være en stærkt begrænset kapacitet hos leverandøren. Ministeriets manglende stillingtagen til disse forhold kan øge følgevirkningerne af større it-hændelser for ministeriet, borgere og virksomheder. Det skyldes, at ministeriet først i en beredskabssituation skal til at tage stilling til, hvilke it-systemer der skal prioriteres, og dermed vil reagere langsommere på at få reetableret de væsentligste it-systemer.

Skatteministeriet har ikke koordineret kravene til de forskellige it-systemers reetableringsplaner. Ministeriet har således hverken koordineret, hvilke krav ministeriet har stillet til den maksimale reetableringstid (RTO) eller til det maksimale datatab (RPO) for de it-systemer, der indgår i forretningsprocesserne for personskat, moms og selskabsskat. Det betyder, at ministeriet ikke har sikret, at kravene til den maksimale reetableringstid og det maksimale datatab for de enkelte it-systemer kan efterleves i en beredskabssituation. Ministeriet ved dermed reelt ikke, hvornår ministeriets kritiske forretningsprocesser kan være oppe at køre igen efter en beredskabssituation.

Skatteministeriet har ikke afklaret, hvilken styrelse der har til opgave at koordinere it-beredskabet på tværs af ministeriets it-systemer. Koordinering af it-beredskabet er afgørende for, at ministeriet kan etablere et tilfredsstillende it-beredskab.

68. Dette kapitel handler om Skatteministeriets koordinering af it-beredskabet for de it-systemer, der indgår i forretningsprocesserne for personskat, moms og selskabsskat. I kapitel 3 undersøgte vi, om der var en plan for reetableringen af de enkelte it-systemer. I dette kapitel undersøger vi, om Skatteministeriet har koordineret reetableringsplanerne for de it-systemer, der indgår i de 3 forretningsprocesser for personskat, moms og selskabsskat. Hvert it-system indgår som et led i en forretningsproces, hvor systemerne er afhængige af at modtage data fra hinanden, for at forretningsprocessen kan fungere. Derudover er der en række støttesystemer, som it-fagsystemerne også er afhængige af, for at de er funktionsdygtige. Som følge heraf skal Skatteministeriet koordinere it-systemernes reetableringsplaner for at være sikker på, at ministeriet kan reetablere forretningsprocesserne inden for den ønskede tidsperiode.

RTO
Recovery Time Objective (RTO) er den tid, som det maksimalt må tage at reetablere it-systemet.

RTO omtales i beretningen som den maksimale reetableringstid.

RPO
Recovery Point Objective (RPO) er den maksimale tidsperiode, hvor der må være tab af data i it-systemet. RPO er dermed udtryk for den tid, man må gå tilbage for at finde den seneste brugbare backup.

RPO omtales i beretningen som det maksimale datatab.

69. Rigsrevisionen har med udgangspunkt i forretningsprocesserne for personskat, moms og selskabsskat undersøgt 3 forhold. For det første har vi undersøgt, om Skatteministeriet har kortlagt, hvilke sammenhænge og afhængigheder der er mellem de it-systemer, der indgår i forretningsprocesserne. For det andet har vi undersøgt, om Skatteministeriet har prioriteret, hvilke it-systemer der skal reetableres først i en beredskabssituation, og aftalt dette med leverandørerne. For det tredje har vi undersøgt, om Skatteministeriet har koordineret de krav, som ministeriet stiller til den maksimale reetableringstid (RTO) og det maksimale datatab (RPO) for de it-systemer, der indgår i forretningsprocesserne.

70. I forbindelse med undersøgelsen er Skatteministeriet blevet opmærksom på, at det ikke er afklaret, hvilken styrelse der har ansvaret for at koordinere it-beredskabet på tværs af it-systemerne.

4.1. Kortlægning af afhængigheder mellem it-systemer

71. Vi har undersøgt, om Skatteministeriet har kortlagt, hvilke it-systemer de 3 forretningsprocesser for personskat, moms og selskabsskat er afhængige af for at kunne fungere, og hvilke sammenhænge der er mellem systemerne. Det er relevant, da fx et nedbrud i et støttesystem, som de øvrige it-fagsystemer i forretningsprocessen er afhængige af, kan betyde, at ét eller flere af it-fagsystemerne ikke fungerer.

72. Vores undersøgelse viser, at Skatteministeriet har overordnede procestegninger over, hvilke it-systemer der indgår i forretningsprocesserne for personskat, moms og selskabsskat. Procestegningerne angiver dog kun de relevante it-fagsystemer og ikke de relevante støttesystemer, fx adgangsstyringssystemerne DCS og AD. Støttesystemerne er helt afgørende for, at it-fagsystemerne i forretningsprocesserne virker, herunder at borgere, virksomheder og Skatteforvaltningens medarbejdere kan anvende it-fagsystemerne. Desuden viser procestegningerne ikke alle afhængigheder mellem it-systemerne. Fx viser procestegningerne ikke, hvordan it-systemerne interagerer og udveksler data, ligesom det heller ikke er afdækket, hvilke it-systemer i processerne der skal være i drift, før de øvrige it-systemer i processerne kan fungere.

Udviklings- og Forenklingsstyrelsen har kun for enkelte af de undersøgte it-systemer overblik over dataudvekslingen. Styrelsen har således et netværksdiagram for regnskabssystemerne SAP 38 og SAPPS, som viser, hvilke systemer der leverer data til SAP 38 og SAPPS, og hvilke systemer SAP 38 og SAPPS leverer data til.

SAP 38 og SAPPS
SAP 38 og SAPPS indgår i hovedsystemet SAP Classic.

Udviklings- og Forenklingsstyrelsen har endvidere i en kortlægning af Skatteministeriets samfundskritiske systemer for nogle enkelte it-systemer beskrevet, at der er vigtige sammenhænge og afhængigheder. Fx er opretholdelsen af adgangsstyringssystemet DCS, som er karakteriseret som et forretningskritisk system, helt afgørende for, at 6 af de 15 samfundskritiske it-systemer kan fungere. Det gælder bl.a. NTSE, DR (DXC Mainframe), Skattekontoen og eIndkomst, som indgår i de 3 forretningsprocesser for personskat, moms og selskabsskat.

Skatteministeriet har i procestegninger og i kortlægningen af forretningskritiske og samfundskritiske it-systemer således afdækket nogle sammenhænge mellem systemer. Ministeriet har imidlertid ikke det fulde og dokumenterede overblik over, hvilke it-systemer der forudsætter, at it-fagsystemerne i de 3 udvalgte forretningsprocesser kan fungere.

Udviklings- og Forenklingsstyrelsen har oplyst, at Skatteministeriet har et internt it-værktøj med en række oplysninger om ministeriets ca. 230 it-systemer. It-værktøjet er et kartotek over ministeriets it-systemer, hvor der kan angives oplysninger om det enkelte systems integrationer og dataudvekslinger med andre systemer. Det er dog op til de medarbejdere i Udviklings- og Forenklingsstyrelsen, som er ansvarlige for de enkelte it-systemer, at udfylde og vedligeholde informationerne i it-værktøjet. Ministeriet har oplyst, at it-værktøjet for Skattekontoen giver et fyldestgørende indblik i sammenhænge og dataudveksling mellem Skattekontoen og de it-systemer, som Skattekontoen integrerer med. Værktøjet har dog ikke været anvendt til at skabe et overblik over sammenhængene mellem it-systemerne, fx i forbindelse med etablering af it-beredskabet.

Resultater

Skatteministeriet har ikke systematisk kortlagt sammenhængene og afhængighederne mellem de it-systemer, der indgår i de forretningsprocesserne for personskat, moms og selskabsskat. Ministeriet har bl.a. ikke fuldt ud kortlagt dataudvekslingen mellem it-systemerne, eller hvilke systemer der skal være i drift, før de øvrige systemer i forretningsprocesserne er funktionsdygtige. Kortlægningen af afhængighederne mellem it-systemerne i en forretningsproces er grundlaget for, at ministeriet kan tilrettelægge et dækkende it-beredskab. Den manglende kortlægning betyder bl.a., at ministeriet i en beredskabssituation ikke hurtigt kan skabe et overblik over, hvordan et større nedbrud eller datatab i ét it-system påvirker de øvrige it-systemer i forretningsprocessen.

4.2. Prioritering af it-systemer

73. Vi har undersøgt, om Skatteministeriet i it-beredskabsplanerne eller i anden dokumentation har beskrevet prioriteringen af, hvilke it-systemer der skal reetableres først, i tilfælde af at alle eller flere systemer i en forretningsproces går ned samtidigt.

Det er centralt, at Skatteministeriet har taget stilling til, i hvilken rækkefølge it-systemerne i forretningsprocessen skal reetableres, da der kan være situationer, hvor det ikke er muligt at reetablere alle systemer samtidigt. Det skyldes fx, at nogle it-systemer er afhængige af, at andre it-systemer er reetableret, før de selv kan reetableres. Det er derfor vigtigt, at Skatteministeriet har taget stilling til, hvilke it-systemer det er vigtigst at få reetableret først, og at ministeriet har aftalt dette med leverandøren, inden en beredskabssituation opstår.

74. Skatteministeriet har mange it-systemer, som er driftet hos den samme leverandør. DXC og KMD drifter langt de fleste af de it-systemer, som indgår i forretningsprocesserne for personskat, moms og selskabsskat. IBM drifter også flere af Skatteministeriets it-systemer og drifter it-systemet eIndkomst, der indgår i processen for personskat. Vi har derfor undersøgt, om Skatteministeriet har aftalt med leverandørerne, i hvilken rækkefølge leverandøren skal reetablere it-systemerne, i tilfælde af at der er nedbrud på alle eller flere systemer hos leverandøren samtidigt.

Vores undersøgelse viser, at Skatteministeriet for de enkelte forretningsprocesser ikke har beskrevet eller taget stilling til, i hvilken rækkefølge it-systemerne i forretningsprocessen skal reetableres i en beredskabssituation, hvor alle eller flere systemer ikke er funktionsdygtige.

Undersøgelsen viser, at der i it-beredskabsplanen for både SKAT Ligning og Skattekontoen, som begge driftes af KMD, er en prioriteringsliste over de it-systemer, som KMD drifter for Skatteministeriet. Prioriteringslisten oplister, i hvilken rækkefølge Skatteministeriets it-systemer hos KMD skal reetableres. Det drejer sig om i alt 13 it-systemer, som driftes af KMD. Flere af disse systemer indgår i de 3 forretningsprocesser for personskat, moms og selskabsskat.

Undersøgelsen viser dog, at prioriteringslisten ikke er opdateret, da der er it-systemer på listen, som blev taget ud af drift i 2015, mens andre it-systemer, der i dag er driftet hos KMD, ikke fremgår af listen. Endvidere har procesejerne i Skattestyrelsen, som har kendskabet til forretningsprocesserne, ikke taget stilling til prioriteringslisten, og hverken ledelsen i Udviklings- og Forenklingsstyrelsen eller Skattestyrelsen har godkendt listen.

Undersøgelsen viser desuden, at der er uoverensstemmelser mellem, hvilken prioritet it-systemerne har i it-beredskabsplanerne og i kontrakterne for systemerne. Dermed er det uklart, om leverandøren foretager en eventuel reetablering i den rækkefølge, som Skatteministeriet forventer. Ministeriet har oplyst, at uoverensstemmelsen skyldes, at kontrakterne ikke løbende bliver opdateret.

Skatteministeriet har for de it-systemer, som er driftet hos DXC og IBM, hverken udarbejdet en prioriteringsliste eller taget stilling til, i hvilken rækkefølge systemerne hos henholdsvis DXC og IBM skal reetableres.

75. Undersøgelsen viser, at det i flere af kontrakterne for de undersøgte it-systemer fremgår, at systemerne vil have en begrænset kapacitet efter en beredskabssituation, hvor systemerne kører på nøddrift. Det fremgår fx i driftskontrakten for DXC Mainframe, at der efter en kritisk it-hændelse kan være en stærkt begrænset kapacitet, og at der skal ske en stram prioritering af, hvilke systemer der skal anvendes. Dette viser behovet for, at Skatteministeriet på forhånd tager stilling til, hvilke systemer der skal prioriteres højest i en beredskabssituation.

Udviklings- og Forenklingsstyrelsen har oplyst, at styrelsen fremadrettet ønsker at udarbejde en procedure for, hvordan styrelsen bedst muligt får udnyttet den kapacitet, der vil være til rådighed i en beredskabssituation. Styrelsen har desuden oplyst, at styrelsen vil udarbejde en prioriteringsrækkefølge for reetablering af it-systemerne i forbindelse med styrelsens arbejde med at styrke it-beredskabet, jf. pkt. 27.

Resultater

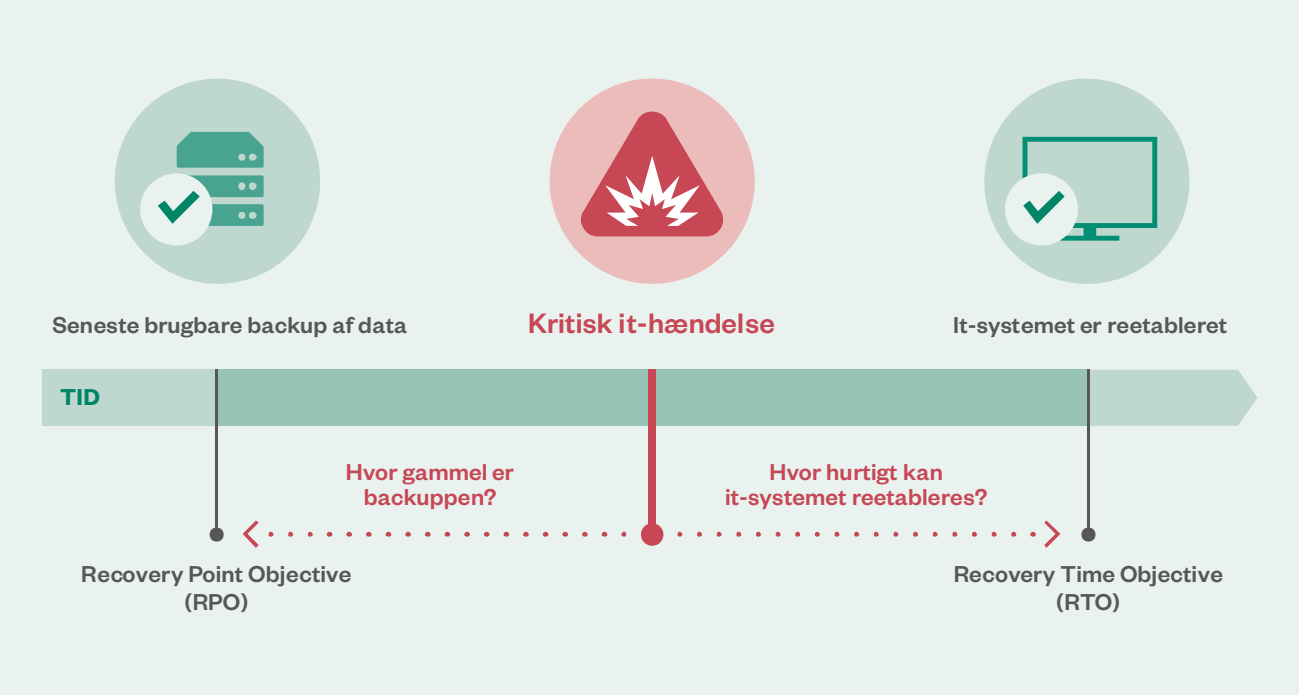
Skatteministeriet har ikke har taget stilling til eller aftalt med leverandørerne, i hvilken rækkefølge it-systemerne i forretningsprocesserne for personskat, moms og selskabsskat skal reetableres i en beredskabssituation, hvor alle eller flere systemer går ned samtidigt. Ministeriet har heller ikke taget stilling til, hvilke it-systemer der skal prioriteres højest i en beredskabssituation, hvor der kan være en stærkt begrænset kapacitet hos leverandøren.

4.3. Koordinering af kravene til it-beredskabsplaner

76. Vi har undersøgt, om Skatteministeriet har koordineret kravene til den maksimale reetableringstid (RTO) og kravene til det maksimale datatab (RPO) for de it-systemer, der indgår i de 3 forretningsprocesser for personskat, moms og selskabsskat.

77. It-systemernes maksimale reetableringstid (RTO) og maksimale datatab (RPO) er nøglebegreber i forhold til, at Skatteministeriet fortsat kan varetage kerneopgaverne i tilfælde af større it-nedbrud og datatab. Figur 8 forklarer nøglebegreberne.

Figur 8
Illustration af RPO og RTO



Kilde: Rigsrevisionen.

Det fremgår af figur 8, at RTO er den tid, det tager at få det pågældende it-system reetableret ved et større nedbrud, mens RPO er den tid, man må gå tilbage for at finde en brugbar backup af data. Datatabet svarer til tidsperioden fra it-hændelsen til den seneste brugbare backup af data. Både den maksimale reetableringstid og det maksimale datatab er centrale for, hvornår ministeriet kan forvente, at it-systemet og dermed også forretningsprocessen fungerer fuldt ud efter et større nedbrud.

78. Skatteministeriets it-systemer er indbyrdes afhængige, da nogle systemer skal være etableret, før andre kan fungere. Rigsrevisionen finder derfor, at det er centralt, at ministeriet på tværs af it-systemerne har koordineret kravene til systemernes maksimale reetableringstid (RTO). Rigsrevisionen finder det ligeledes centralt, at ministeriet har koordineret kravene til det maksimale datatab (RPO) på tværs af it-systemerne, da datatab i ét system kan påvirke data i de øvrige systemer i forretningsprocessen.

79. Skatteministeriet har ikke kortlagt, om der er sammenhæng mellem kravene til de forskellige it-systemers maksimale reetableringstid (RTO) i forretningsprocesserne. Ministeriet har heller ikke kortlagt, om der er sammenhæng mellem it-systemernes maksimale datatab (RPO). Det betyder, at ministeriet ikke har overblik over, om det vil være realistisk at opretholde kravene til RPO og RTO for de enkelte it-systemer i en it-beredskabssituation. Ministeriet ved således ikke, hvor lang tid det reelt vil tage, før ministeriet kan varetage sine væsentligste opgaver igen efter et større it-nedbrud.

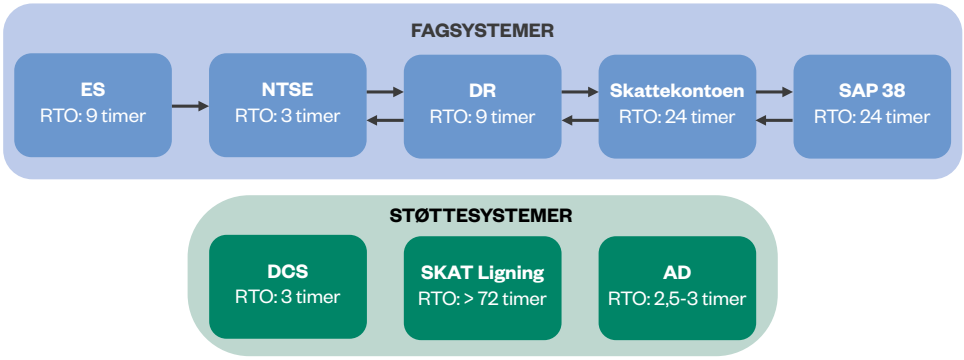
80. Vi har på baggrund af materiale fra Skatteministeriet undersøgt, hvilke krav ministeriet har stillet til RTO og RPO for de enkelte it-systemer, der indgår i forretningsprocesserne for personskat, moms og selskabsskat, for at belyse, om de er sammenhængende. I det følgende gennemgår vi som eksempel sammenhængene mellem it-systemernes RTO og sammenhængene mellem systemernes RPO i momsprocessen.

It-systemernes maksimale reetableringstid (RTO)

81. Figur 9 viser en forenklet oversigt over de it-systemer, som indgår i forretningsprocessen for moms, og kravene til systemernes maksimale reetableringstid.

Figur 9

Krav til maksimal reetableringstid (RTO) for it-systemerne i forretningsprocessen for moms



DR og ES
DR og ES indgår i hovedsystemet DXC Mainframe.

SAP 38
SAP 38 indgår i hovedsystemet SAP Classic.

Note: Pilene viser et forenklet billede af dataudveklsingen mellem it-systemerne i processen for moms.

Kilde: Rigsrevisionen på baggrund af oplysninger fra Skatteministeriet.

I figur 9 fremgår it-fagsystemerne i forretningsprocessen for moms og de støttesystemer, som it-fagsystemerne er afhængige af for at være funktionsdygtige. Som det fremgår af figuren, har de enkelte it-systemer forskellige krav til reetableringstiden (RTO). For at der skal være en sammenhæng i it-systemernes reetableringstid, skal de systemer i forretningsprocessen, som skal reetableres først, som minimum have et lavere eller samme krav til retableringstiden i forhold til de øvrige systemer i forretningsprocessen. Rækkefølgen for, hvilke it-systemer der skal reetableres først, er dermed afgørende for, hvilke krav Skatteministeriet bør stille til reetableringstiden for hvert enkelt system.

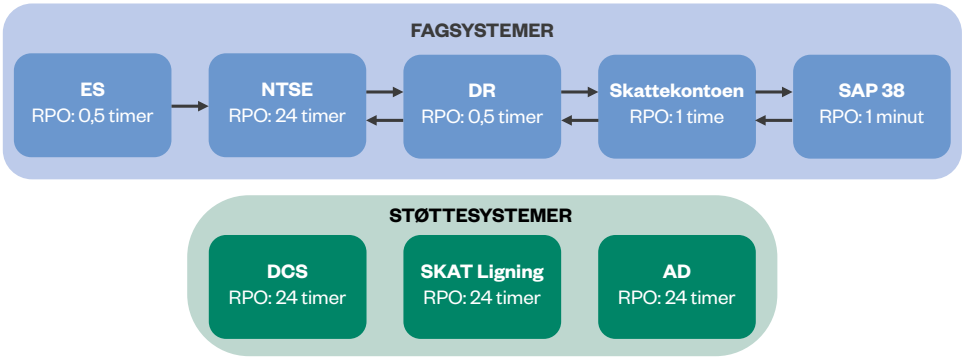
Da Skatteministeriet ikke har taget stilling til, i hvilken rækkefølge it-systemerne i forretningsprocessen skal reetableres, er det hverken muligt for ministeriet eller Rigsrevisionen at vurdere, om de fastsatte krav til den maksimale reetableringstid (RTO) for de enkelte systemer er realistiske.

It-systemernes maksimale datatab (RPO)

82. Det er nødvendigt at have overblik over, hvilken dataudveksling der er mellem it-systemerne, for at kunne afgøre, om der er den nødvendige sammenhæng mellem it-systemernes maksimale datatab (RPO) i processen for moms. Vi har derfor i figur 10 udarbejdet en forenklet model over nogle af datastrømmene mellem it-systemerne. Figuren viser også kravene til det maksimale datatab for it-systemerne i forretningsprocessen for moms.

Figur 10

Krav til maksimalt datatab (RPO) for it-systemerne i forretningsprocessen for moms



Note: Pilene viser et forenklet billede af dataudveklsingen mellem it-systemerne i processen for moms. Der fremgår ikke en RPO af reetableringsplanen for AD, men Skatteministeriet har oplyst, at der tages en backup af AD hver dag. Det betyder, at RPO er på mindst 24 timer.

Kilde: Rigsrevisionen på baggrund af oplysninger fra Skatteministeriet.

Fastsættelse af kravet til maksimalt datatab (RPO)
It-systemernes RPO er i beretningen defineret som tidsrummet mellem backups. I de kontrakter, hvor der både er angivet et krav til incremental backup og fuld backup, har vi taget udgangspunkt i kravet til incremental backup. Incremental backup kopierer i modsætning til en fuld backup kun filer, der er ændret siden den sidste backup.

Det fremgår bl.a. af figur 10, at it-systemet DR modtager data fra TastSelv Erhverv (NTSE) og leverer data til Skattekontoen. DR leverer data til Skattekontoen om positive angivelser, foreløbige fastsættelser og gebyrer til opkrævning. Hvis der i forbindelse med et nedbrud og efterfølgende reetablering af NTSE opstår et datatab i NTSE, fx at data er forældede eller korrupte, vil det også påvirke de data, som DR modtager og genererer fra NTSE samt efterfølgende videresender til Skattekontoen. Det kan fx betyde, at DR beregner moms ud fra forældede eller korrupte data, som DR modtager fra NTSE, medmindre fejlene i data udbedres.

Det fremgår desuden af figuren, at nogle af de it-systemer, som udveksler data i processen for moms, ikke har de samme krav til det maksimale datatab (RPO). Fx har NTSE et krav til RPO på 24 timer, mens DR, som modtager data fra NTSE, har et krav til RPO på 0,5 timer.

Det er ikke muligt for Rigsrevisionen at vurdere, om det maksimale datatab (RPO) for it-systemerne bør være det samme, da Skatteministeriet ikke fuldt ud har kortlagt sammenhængene og afhængighederne mellem it-systemerne. Ministeriet bør vurdere, hvordan datatab i ét af it-systemerne påvirker resten af forretningsprocessen, fx datatab i form af korrupte data. På den baggrund bør ministeriet tage stilling til, om det er hensigtsmæssigt, at de it-systemer, der løbende udveksler data i forretningsprocesserne, har forskellige krav til det maksimale datatab (RPO).

Resultater

Skatteministeriet har ikke kortlagt eller koordineret it-systemernes maksimale reetableringstid eller maksimale datatab, som er helt centrale for, at it-systemerne og dermed forretningsprocesserne kan fungere fuldt ud efter en it-beredskabssituation. Det betyder, at ministeriet ikke har overblik over, om det er realistisk, at it-systemerne kan reetableres inden for den ønskede tid (RTO), eller om det er muligt at overholde det maksimale datatab (RPO) i en beredskabssituation. Så længe ministeriet ikke har et overblik over sammenhængene og afhængighederne mellem it-systemerne, er det ikke muligt for ministeriet at vurdere, om kravene til systemernes maksimale reetableringstid og maksimale datatab er realistiske.

Rigsrevisionen, den 9. september 2021

Lone Strøm

/Niels Kjøller Petersen

Bilag 1. Metodisk tilgang

Formålet med undersøgelsen er at vurdere, om Skatteministeriet har et tilfredsstillende it-beredskab for kritiske forretningsprocesser. Vi besvarer følgende spørgsmål i beretningen:

- Har Skatteministeriet et tilstrækkeligt grundlag for at etablere et it-beredskab?
- Har Skatteministeriet sikret, at der er implementeret tilfredsstillende it-beredskabsplaner?
- Har Skatteministeriet koordineret it-beredskabet for it-systemerne?

I undersøgelsen indgår Skatteministeriet, herunder Udviklings- og Forenklingsstyrelsen og Skattestyrelsen.

Undersøgelsen omhandler perioden 2018-2020 og dermed tiden efter, at Skatteforvaltningen blev omorganiseret, og de nye styrelser blev etableret. ISO 27001, som fastsætter standarderne for it-beredskabet, har været gældende siden 2016.

Undersøgelsen bygger på en gennemgang af dokumenter. Vi har desuden holdt møder med Udviklings- og Forenklingsstyrelsen og Skattestyrelsen. Vi har således holdt møder med:

- Skattestyrelsen vedrørende udvælgelse af forretningsprocesser og underliggende it-systemer
- Udviklings- og Forenklingsstyrelsen vedrørende kortlægningen af kritiske it-systemer, Skatteministeriets it-beredskab og risikovurderinger af informationssikkerhedsområdet, herunder it-beredskabet
- systemejere og platformejere fra Udviklings- og Forenklingsstyrelsen vedrørende it-beredskabet for de 9 it-systemer, som indgår i undersøgelsen
- procesejere fra Skattestyrelsen og Udviklings- og Forenklingsstyrelsen vedrørende it-systemet elndkomst, som indgår i undersøgelsen
- procesejer for major incidents fra Udviklings- og Forenklingsstyrelsen.

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

Vi har for hvert af de 9 undersøgte it-systemer holdt et møde med de systemansvarlige i Skatteministeriet, som har ansvaret for leverandørstyring og kontraktforhold. Vi har bedt Udviklings- og Forenklingsstyrelsen udpege relevante personer til møderne, som har kendskab til it-beredskabet for de udvalgte it-systemer. Da procesejerne fra Skattestyrelsen, som har ansvaret for at udarbejde indsatsplaner og nødplaner, ikke var med til møderne om it-systemerne, har vi haft et separat møde med procesejere for ét af systemerne (elndkomst) for at få et indblik i deres rolle i forhold til it-beredskabet.

Formålet med mødet med procesejere for major incidents var at få klarhed over sammenhængen mellem Skatteministeriets interne proces for major incidents og it-beredskabet.

Nedenfor beskrives vores kvalitetssikring, data og metode i flere detaljer.

Udvælgelse af kritiske forretningsprocesser og tilhørende it-systemer

Vi har undersøgt, om Skatteministeriets it-beredskab er tilfredsstillende, ved at se på ministeriets it-beredskab for 3 kritiske forretningsprocesser. Vi har udvalgt processerne for personskat, moms og selskabsskat, som er særligt væsentlige både med hensyn til statens indtægter og potentielle konsekvenser for borgere og virksomheder ved større nedbrud. Skatteforvaltningen opkræver via de 3 forretningsprocesser knap 80 % af statens indtægter, svarende til ca. 850 mia. kr.

Da Skatteministeriet ikke har et fuldstændigt overblik over alle de it-systemer, der indgår i forretningsprocesserne for personskat, moms og selskabsskat, har det været en del af undersøgelsen at forsøge at danne os et overblik over alle it-systemer, der indgår i de 3 forretningsprocesser. Vi har haft en dialog med Skattestyrelsen, som er ansvarlig for forretningsprocesserne, om, hvilke forretningsprocesser vi skulle udvælge til undersøgelsen. På baggrund af denne dialog og procestegninger fra Skattestyrelsen af it-systemerne i forretningsprocesserne har vi udvalgt en række it-systemer til at indgå i undersøgelsen. Skattestyrelsens procestegninger over forretningsprocesserne indeholder ikke de støttesystemer, platforme mv., som er afgørende for, at de øvrige it-systemer i forretningsprocessen kan fungere. Vi har derfor anmodet Udviklings- og Forenklingsstyrelsen, som er ansvarlig for støttesystemer og platforme mv., om en oversigt over, hvilke støttesystemer der indgår i de udvalgte forretningsprocesser. Udviklings- og Forenklingsstyrelsen har dog ikke systematisk kortlagt, hvilke støttesystemer mv. der understøtter it-fagsystemerne i forretningsprocesserne. Det kan betyde, at vi ikke har fået alle de it-systemer med, der indgår i forretningsprocesserne. Vi har udvalgt it-systemer, platforme, støttesystemer mv. i samarbejde med vores kontor for it-revision. Vi har ved den endelige udvælgelse af it-systemer forelagt Skatteministeriet de it-systemer, som vi har udvalgt.

Vi har valgt ikke at inddrage it-systemet DIAS, som indgår i forretningsprocessen for selskabsskat. Det skyldes, at vi på baggrund af informationer fra Skattestyrelsen vurderede, at systemet ikke er afgørende for forretningsprocessen. Senere i forbindelse med høringen af revisionsnotater har Udviklings- og Forenklingsstyrelsen oplyst, at DIAS har betydning for forretningsprocessen. Vi vurderer dog, at vi har de væsentligste it-systemer med i undersøgelsen, ligesom Skatteministeriet har vurderet, at vi har de it-systemer med, som er væsentlige for forretningsprocesserne for personskat, moms og selskabsskat.

Kvalitetssikring

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

Væsentlige dokumenter

Vi har gennemgået en række dokumenter, herunder:

- Udviklings- og Forenklingsstyrelsens dokumentation for kortlægning af kritiske it-systemer og kortlægning af Skatteministeriets it-beredskab
- Udviklings- og Forenklingsstyrelsens risikovurderinger på informationssikkerhedsområdet, herunder it-beredskabet
- Skatteministeriets beredskabspolitik samt Skattestyrelsens og Udviklings- og Forenklingsstyrelsens beredskabsplaner, beredskabsprogrammer, informationssikkerhedshåndbog og skabeloner for it-beredskabsplaner
- Skatteministeriets it-beredskabsplaner (herunder nødplaner, indsatsplaner og reetableringsplaner), test af it-beredskabsplaner, revisorerklæringer (ISAE 3402-erklæringer) og kontraktbilag for de 9 undersøgte it-systemer i perioden 2018-2020
- Skatteministeriets processer for incidents og major incidents
- ISO 27001 og ISO 27002 vedrørende it-beredskabet
- Beredskabsstyrelsens, Digitaliseringsstyrelsens og sikkerdigital.dk's vejledninger om beredskab og it-beredskab.

For at kunne afdække, om Skatteministeriet har tilvejebragt et tilstrækkeligt planlægningsgrundlag for it-beredskabet, har vi indhentet dokumentation for ministeriets kortlægning af kritiske forretningsprocesser og underliggende it-systemer samt dokumentation for ministeriets overblik over det eksisterende it-beredskab. Derudover har vi indhentet dokumentation for, om ministeriet har udarbejdet en overordnet ramme for it-beredskabet, herunder om ministeriet har udarbejdet en beredskabspolitik, og om Skattestyrelsen og Udviklings- og Forenklingsstyrelsen har udarbejdet beredskabsplaner og beredskabsprogrammer for styrelserne. Endelig har vi indhentet dokumentation for de risikovurderinger, som ministeriet har udarbejdet i perioden 2018-2020.

Vi har for at kunne vurdere, om Skatteministreret har tilfredsstillende it-beredskabsplaner, indhentet de gældende it-beredskabsplaner og test af planerne i undersøgelsesperioden 2018-2020 for de 9 undersøgte it-systemer. Derudover har vi for de eksternt driftede it-systemer indhentet de kontraktbilag, som vedrører it-beredskabet, herunder samarbejdshåndbøger mellem leverandøren og Skatteministeriet samt servicekrav om backup og reetablering af it-systemet. Endvidere har vi indhentet dokumentation, som viser, om ministeriet har ført tilsyn med leverandørernes it-beredskab. Vi har indhentet revisorerklæringer og Skatteministeriets godkendelse af leverandørernes reetableringsplaner og test af planerne.

For at kunne vurdere, om Skatteministeriet har koordineret it-beredskabet for de it-systemer, der indgår i forretningsprocesserne for personskat, moms og selskabsskat, har vi indhentet dokumentation for, om ministeriet har kortlagt sammenhængene mellem it-systemerne i de enkelte forretningsprocesser, og om ministeriet har prioriteret, hvilken rækkefølge it-systemerne skal reetableres. Endelig har vi indhentet dokumentation for, om ministeriet har koordineret kravene til it-systemernes maksimale reetableringstid og maksimale datatab for de it-systemer, som indgår i de 3 kritiske forretningsprocesser.

Fastlæggelse af it-systemernes maksimale datatab (RPO)

Vi har i undersøgelsen taget udgangspunkt i, at it-systemernes maksimale datatab (RPO) er tidsrummet mellem backups. Kravene til backups fremgår af kontrakten med leverandørerne. I de kontrakter, hvor der både er angivet et krav til incremental backup og fuld backup, har vi taget udgangspunkt i kravet til incremental backup. Incremental backup kopierer i modsætning til en fuld backup kun filer, der er ændret siden den sidste backup.

I nogle af kontrakterne for de undersøgte it-systemer fremgår det, at det maksimale datatab er 0, fordi it-systemet har 2 datacentre. Alle de eksternt driftede it-systemer i de 3 udvalgte forretningsprocesser har tocenterdrift. Det betyder, at hvis det ene datacenter går ned, kan it-systemet reetableres uden datatab på det andet datacenter, da alle data hele tiden replikeres til begge datacentre. I tilfælde af en it-beredskabssituation, hvor begge datacentre bliver ødelagt, vil det dog være den seneste backup af data, som vil være udgangspunktet for reetableringen. Derfor vil tidsperioden mellem backups udgøre det maksimale datatab (RPO).

Et andet scenarie er, at data bliver korrupte, fx på grund af malware. I det tilfælde vil de korrupte data blive kopieret fra det ene datacenter til det andet. Her vil Skatteministeriet også være afhængig af en backup for at få reetableret it-systemet med de korrekte data. Det er således også ved dette scenarie tidsrummet til den seneste backup, som vil være afgørende for, hvor meget data der går tabt. Så selv om it-systemerne har 2 datacentre, er tidsrummet mellem backups afgørende i en beredskabssituation, hvor begge datacentre går ned, eller der opstår korrupte data. Vi har derfor i undersøgelsen taget udgangspunkt i, at det maksimale datatab (RPO) for it-systemerne svarer til datatabet for perioden mellem backups.

Standarderne for offentlig revision

Revisionen er udført i overensstemmelse med standarderne for offentlig revision. 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 og tabel B viser, hvilke revisionskriterier vi har anvendt til at vurdere indholdet af Skatteministeriets it-beredskabsplaner og test af beredskabsplanerne, og hvor revisionskriterierne stammer fra.

Tabel A

Revisionskriterier anvendt til at vurdere Skatteministeriets it-beredskabsplaner

Elementer, som vi har undersøgt i it-beredskabsplanerne (X angiver de planer, hvor elementet er undersøgt)	Nødplan	Indsatsplan	Reetablerings-plan	Ophæng til revisionskriterier
Er planen ajourført årligt?	X	X	X	• ISO 27001 og ISO 27002. • Beredskabsstyrelsens helhedsorienterede beredskab. • Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet it-drift. • Digitaliseringsstyrelsens vejledning til it-beredskab.
Beskriver planen, hvornår den aktiveres?	X	X	X	• Beredskabsstyrelsens helhedsorienterede beredskab. • Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet it-drift. • Digitaliseringsstyrelsens vejledning til it-beredskab.
Omfatter planen alle centrale it-systemer i forretningsprocessen?	X			• Rigsrevisionens kriterie baseret på sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet it-drift og Digitaliseringsstyrelsens vejledning til it-beredskab.
Fremgår der kontaktoplysninger på nøglepersoner internt i Skatteministeriet? Fremgår der kontaktoplysninger på nøglepersoner hos leverandøren og Skatteministeriet?	X	X	X	• Beredskabsstyrelsens helhedsorienterede beredskab. • Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet it-drift.
Beskriver planen konkrete nødprocedurer eller aktiviteter?	X			• ISO 27001 og ISO 27002. • Beredskabsstyrelsens helhedsorienterede beredskab. • Digitaliseringsstyrelsens vejledning til it-beredskab. • Sikkerdigital.dk (beredskabsstyring/ implementering).
Beskriver planen rolle- og ansvarsfordeling internt i Skatteministeriet?	X	X		• Beredskabsstyrelsens helhedsorienterede beredskab. • Sikkerdigital.dk (beredskabsstyring/ implementering). • Digitaliseringsstyrelsens vejledning til it-beredskab.
Beskriver planen, hvor krisestaben mødes?		X		• Beredskabsstyrelsens helhedsorienterede beredskab. • Digitaliseringsstyrelsens vejledning til it-beredskab. • Sikkerdigital.dk - skabelon til it-beredskabsplan ved outsourcet it-drift.

Tabel A (fortsat)

Revisionskriterier anvendt til at vurdere Skatteministeriets it-beredskabsplaner

Elementer, som vi har undersøgt i it-beredskabsplanerne (X angiver de planer, hvor elementet er undersøgt)	Nødplan	Indsatsplan	Reetablerings-plan	Ophæng til revisionskriterier
Fremgår der kontaktoplysninger på eksterne interessenter?		X		• Beredskabsstyrelsens helhedsorienterede beredskab. • Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet it-drift.
Beskriver planen, hvilke it-systemer der påvirkes af et systemnedbrud eller datatab?		X		• Rigsrevisionens kriterie baseret på Beredskabsstyrelsens helhedsorienterede beredskab, sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet it-drift.
Indgår der beskrivelser af kommunikation til eksterne og interne aktører?		X		• Digitaliseringsstyrelsens guide til kommunikation i en beredskabssituation. • Beredskabsstyrelsens helhedsorienterede beredskab.
Beskriver planen eller kontrakten kriterierne for at vende tilbage til normal drift?			X	• Rigsrevisionens kriterie. Det er relevant, at Skatteministeriet på forhånd har aftalt med leverandøren, hvordan og hvornår beredskabet ophører, og man vender tilbage til normal drift, så der ikke opstår uenighed om det.
Er det besluttet, hvor planen opbevares, så man ved, hvor den er i en it-beredskabssituation?	X	X	X	• Beredskabsstyrelsens helhedsorienterede beredskab. • Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet it-drift.
Beskriver planen rolle- og ansvarsfordelingen mellem leverandør og Udviklings- og Forenklingsstyrelsen?			X	• Digitaliseringsstyrelsens vejledning til it-beredskab. • Beredskabsstyrelsens helhedsorienterede beredskab. • Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet it-drift.
Fremgår der krav til RTO af planen eller kontrakten?			X	• Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet it-drift. • Digitaliseringsstyrelsens vejledning til it-beredskab.
Fremgår der krav til RPO af planen eller kontrakten?			X	• Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet it-drift. • Digitaliseringsstyrelsens vejledning til it-beredskab.
Beskriver planen, hvordan it-systemet kan køre i nøddrift?			X	• ISO 27001 og ISO 27002.
Beskriver planen nødvendige aktiviteter for at reetablere it-systemet?			X	• ISO 27001 og ISO 27002. • Beredskabsstyrelsens helhedsorienterede beredskab.

Kilde: Rigsrevisionen.

Tabel B

Revisionskriterier anvendt til at vurdere test af reetableringsplanerne

Elementer, som vi har undersøgt i test af reetableringsplanerne	Ophæng til revisionskriterier
Er it-systemet blevet testet årligt i perioden 2018-2020?	• ISO 27001 og ISO 27002. • Beredskabsstyrelsens helhedsorienterede beredskab. • Digitaliseringsstyrelsens vejledning til it-beredskab. • Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet it-drift.
Deltager Skatteministeriet i testen?	• Rigsrevisionens kriterie baseret på ISO 27001 og ISO 27002.
Er funktionaliteten af it-systemet blevet testet?	• Rigsrevisionens kriterie baseret på ISO 27001 og ISO 27002.
Er RTO blevet testet?	• Sikkerdigital.dk – skabelon til it-beredskabsplan ved outsourcet it-drift.
Beskriver rapporten forbedringsforslag?	• Digitaliseringsstyrelsens vejledning til it-beredskab. • Beredskabsstyrelsens helhedsorienterede beredskab.
Er test og evaluering godkendt af Skatteministeriet?	• Rigsrevisionens kriterie. Det er relevant, at Skatteministeriet godkender testrapport og evalueringer for at sikre, at ministeriet har viden om, hvorvidt beredskabsplanerne virker, og sikre, at testene er dækkende.

Kilde: Rigsrevisionen.

Bilag 3. It-systemer, der indgår i undersøgelsen

Udvalgte it-systemer	Funktion	Udvalgte underliggende it-systemer	Leverandør
NTSE (TastSelv Erhverv)	NTSE modtager virksomhedernes indberetninger af bl.a. moms, lønsum og punkt- og miljøafgifter. NTSE modtager også selvangivelser fra selskaber og fonde.	-	DXC
DCS (Den Centrale Sikkerhedsløsning)	DCS er et fælles adgangsstyringssystem for de webservicebaserede systemer, som anvendes af borgere og virksomheder. DCS håndterer al funktionalitet, der har at gøre med login, rolle- og rettighedsdelegering og distribuering. DCS benyttes af ca. 15 af Skatteforvaltningens it-systemer.	-	DXC
SKAT Ligning	SKAT Ligning er et sagsstyringssystem og et elektronisk arkiveringssystem for skatte- og momsmedarbejdere. Systemet benyttes til understøttelse af sagsbehandlingen.	-	KMD
DXC Mainframe	DXC Mainframe er den underliggende platform, hvorpå der ligger en række af Skatteforvaltningens it-systemer.	ES, DR, 3S, DetailCOR, COR, CSR-P og SLUT	DXC
Skattekontoen	Skattekontoen giver virksomheder et samlet overblik over, hvad virksomheden har indberettet og betalt, og hvad virksomheden skylder, bl.a. i moms, lønsumsafgift, A-skat og arbejdsmarkedsbidrag, selskabsskat, acontoselskabsskat, udbytteskat og punkt- og miljøafgifter.	-	KMD
eIndkomst	eIndkomst er et samlet register, hvor alle indkomstoplysninger indberettes. Over 150 myndigheder bruger eIndkomst, når de bl.a. udbetaler offentlige ydelser. Derudover bruges systemet af private virksomheder, fx i den finansielle sektor.	-	IBM
SAP Classic	SAP 38 anvendes til regnskabsaflæggelse af statens indtægter og balanceposter for alle skatter, afgifter og told, der opkræves i henhold til finansloven. SAPPS er en kopi af SAP 38, der tager sig af punktafgifter og selskabsskat. SAP LetLøn anvendes til håndtering af virksomheders indberetninger af A-skat og arbejdsmarkedsbidrag.	SAP LetLøn, SAPPS og SAP 38	KMD
Active Directory (AD)	AD er Skatteministeriets brugeradgangssystem. AD indeholder stamoplysninger om SKATs brugere og it-systemer. Det er via AD, at Skatteforvaltningens medarbejdere får adgang til hovedparten af de kritiske systemer.	-	Internt driftet
FTPS-Gateway/SFO	FTPS-Gateway er et systemmodul, som sammen med SFO (styret filoverførsel) faciliterer filudveksling mellem Skatteforvaltningen og tredjepart (typisk virksomheder).	-	Internt driftet

Bilag 4. Ordliste

Backup	En sikkerhedskopi af data. Kopien er lavet med henblik på at genskabe data, hvis de originale data skulle gå tabt.
Disaster recovery test	En test, hvor hele it-systemet reetableres på baggrund af den seneste backup på en tom server.
DXC Mainframe	En platform, hvorpå der ligger en række af Skatteforvaltningens it-systemer, som er driftet hos DXC.
Forretningskritisk it-system	Et it-system, hvor driftsforstyrrelser kan medføre, at størstedelen af myndighedens medarbejdere ikke kan udføre deres arbejde, eller at myndigheden vanskeligt kan overholde sine forvaltningsmæssige forpligtelser.
Incremental backup	En backup, som kun kopierer filer, der er ændret siden den sidste backup.
Indsatsplan	En plan for den interne krisestyring i Skatteministeriet i en it-beredskabssituation for hvert it-system.
Informationssikkerhed	En bred betegnelse for de samlede foranstaltninger til at sikre informationer i forhold til fortrolighed, integritet (ændring af data) og tilgængelighed. I arbejdet indgår bl.a. organisering af sikkerhedsarbejdet, processer for behandling af data, styring af leverandører, tekniske sikringsforanstaltninger og it-beredskab.
ISAE 3402-erklæring	Revisorerklæring, hvor it-revisoren udtaler sig om, hvorvidt leverandørens beskrivelse af ydelser og systemer er retvisende, hvorvidt leverandørens generelle it-kontroller er hensigtsmæssigt udformet, og om disse kontroller har fungeret tilfredsstillende i regnskabsperioden.
ISO 27001	En international standard for informationssikkerhed. Standarden omfatter bl.a. principper for risikovurdering, for ledelsens aktive stillingtagen hertil og for dokumentation af arbejdet med cyber- og informationssikkerhed.
It-fagsystem	Et it-system, der løser en faglig opgave i modsætning til et støttesystem, der understøtter det faglige it-system.
Korrupte data	Korrupte data er fejlbehæftede data, som enten er beskadigede eller blevet ændret, fx at kommaer i filen er ændret til et andet tegn, eller at datafiler overskrives med vilkårlige tal. Korrupte data kan fx opstå som følge af fejl på serveren, malware eller menneskelige fejl.
Legacy-system	Et ældre it-system, der stadig er i brug. Skatteministeriet ønsker at udskifte legacy-systemerne, da de er komplekse og bygger på forældet teknologi.
Malware	En samlet betegnelse for computerprogrammer, der gør skadelige eller uønskede ting på computeren, fx ved brug af virus eller orme. Malware kan opstå på mange måder, fx ved at åbne en vedhæftet fil i en mail eller ved at åbne et link.
Nøddrift	Nøddrift betyder, at it-systemet kører med reduceret kapacitet, fx 50 % af it-systemets fulde kapacitet. It-systemet kan i en beredskabssituation køre på nøddrift, indtil systemet er fuldt reetableret.
Nødplan	En plan for, hvordan Skatteministeriet håndterer og viderefører de opgaver og forretningsprocesser, som påvirkes i en it-beredskabssituation.

Proces for incidents	Skatteministeriets proces for incidents skal håndtere ikke-planlagte afbrydelser af en it-service eller reduktion i kvaliteten af it-servicen. Fejl, der endnu ikke har haft konsekvenser for it-systemet, er også incidents.
Proces for major incidents	Skatteministeriets proces for major incidents skal håndtere alle it-hændelser, som har en meget stor effekt på ministeriet, og som ikke umiddelbart kan løses.
Reetableringsplan	En plan for, hvordan et it-system skal reetableres i en it-beredskabssituation.
Reetableringstid	Den tid, det tager at få reetableret et it-system efter et it-nedbrud.
Restoretest	En test af reetableringen af dele af et it-system (en delmængde af en disaster recovery test), fx at genskabe en fil eller database.
RPO (Recovery Point Objective)	Recovery Point Objective (RPO) er den maksimale tidsperiode, hvor der må være tab af data i it-systemet. RPO er dermed udtryk for den tid, man må gå tilbage for at finde den seneste brugbare backup. RPO omtales i beretningen som det maksimale datatab.
RTO (Recovery Time Objective)	RTO er den tid, som det maksimalt må tage at reetablere it-systemet. RTO omtales i beretningen som den maksimale reetableringstid.
Samfundskritisk it-system	Et it-system, som er vigtigt for national sikkerhed eller for kritisk infrastruktur, hvor misbrug af data vil have store konsekvenser, eller hvor driftsforstyrrelser kan have stor betydning for økonomien i staten eller for mange borgere og virksomheder.
Sikkerdigital.dk	På sikkerdigital.dk kan borgere, virksomheder og myndigheder finde viden, vejledning og konkrete værktøjer til en sikker digital hverdag. Bag sikkerdigital.dk står Digitaliseringsstyrelsen og Erhvervsstyrelsen samt en række samarbejdspartnere.
Støttesystem	Et it-system, som understøtter én eller flere funktioner i andre it-systemer.
Tocenterdrift	Tocenterdrift betyder, at it-systemet kører på 2 centre/lokationer. Det medfører, at systemet kan køre videre, selv om der skulle opstå et større driftssvigt forårsaget af fx brand, bygnings- og vandskade eller indbrud/hærværk i det ene center.