FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

Maj 2024
– 14/2023

Rigsrevisionens beretning afgivet til Folketinget med Statsrevisorernes bemærkninger

Finanstilsynets it-tilsyn

14/2023

Beretning om

Finanstilsynets it-tilsyn

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 2024

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.

Erhvervsministeren 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 september 2024.

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 2023, som afgives i februar 2025.

Statsrevisorernes bemærkning tager udgangspunkt i denne karakterskala:

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

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

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

ISSN 2245-3008
ISBN online 978-87-7434-836-8

Statsrevisorernes bemærkning

Beretning om Finanstilsynets it-tilsyn

Statsrevisorerne har anmodet om denne undersøgelse af, om Finanstilsynet har ført et tilfredsstillende tilsyn med finansielle virksomheders it-sikkerhed.

Finanstilsynet skal føre tilsyn med virksomhederne i den finansielle sektor. Tilsynet omfatter bl.a. tilsyn med it-sikkerhed. Siden 2018 har Finanstilsynet vurderet, at it-sikkerhed er et af de væsentligste risikoområder for den finansielle sektor, og Center for Cybersikkerhed har vurderet, at trusselsniveauet mod den danske finansielle sektor er meget højt.

Finanstilsynet er fuldt finansieret af afgifter fra de virksomheder, der er underlagt tilsynet. I 2023 udgjorde udgifterne til Finanstilsynet 465,5 mio. kr. Der er i alt ca. 325 finansielle virksomheder, som er underlagt Finanstilsynets it-tilsyn.

Statsrevisorerne finder Finanstilsynets tilsyn med finansielle virksomheders it-sikkerhed utilfredsstillende. Det utilfredsstillende tilsyn øger risikoen for it-nedbrud, økonomiske tab og tab af tillid fra kunder og omverden.

Statsrevisorerne finder det bekymrende, at Finanstilsynet ikke har inspiceret it-sikkerheden i en tredjedel af de systemisk vigtige finansielle virksomheder inden for det 4-årige interval, som de skal ifølge deres retningslinjer. Der er i gennemsnit gået 4½ år mellem inspektionerne, og for nogle af virksomhederne er der gået over 7 år.

Statsrevisorerne

13. maj 2024

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

Statsrevisorerne har bl.a. hæftet sig ved disse undersøgelsesresultater:

- Finanstilsynet har stort set ikke risikovurderet it-sikkerheden for investeringsforvaltningsselskaber og heller ikke for de e-penge- og betalingsinstitutter og datacentraler, der ikke er systemisk vigtige.
- På områder som fx adgangsstyring og fysisk sikkerhed har Finanstilsynet ikke gennemført it-inspektioner i flere år, selv om Finanstilsynet selv vurderer, at en del virksomheder har høje risici på områderne.
- Finanstilsynet har kun i meget begrænset omfang inspiceret investeringsforvaltningsselskaber samt e-penge- og betalingsinstitutter. Den begrænsede inspektion er sket uden foregående risikovurdering af it-sikkerheden i virksomhederne. Finanstilsynet har derfor ikke haft et grundlag for at vide, om fravalget af tilsyn med it-sikkerheden er hensigtsmæssigt.
- Finanstilsynet har fastsat frister for virksomhedernes efterlevelse af påbud om at rette op på mangler i deres it-sikkerhed. Virksomhederne har i gennemsnit overskredet fristerne med 2 år, og Finanstilsynet har aldrig anvendt deres hjemmel til at sanktionere virksomheder, der ikke efterlever de påbud, de har fået.
- Finanstilsynet har ikke udstedt administrative bødeforlæg til virksomheder, som overtræder reglerne for it-sikkerhed, eller som ikke efterlever Finanstilsynets påbud inden for fristen. Dette skyldes ifølge Finanstilsynet, at bødesatserne ved administrative bødeforlæg er så små, at bøderne kun kan gives for overtrædelser, der kan karakteriseres som bagatelagtige.

Statsrevisorerne kan tilslutte sig Rigsrevisionens anbefaling om, at Finanstilsynet supplerer offentliggørelsen af påbud med en vurdering af, hvilke konsekvenser virksomhedernes utilstrækkelige it-sikkerhed kan have for kunderne, så de kan se det i de offentlige redegørelser.

Statsrevisorerne anbefaler, at Finanstilsynet skærper praksis for anvendelse af sanktioner over for virksomheder, der ikke efterlever lovkravene til it-sikkerhed eller overskrider fristerne for efterlevelse af påbud.

Indholdsfortegnelse

Undersøgelsen er en statsrevisoranmodning, og Rigsrevisionen afgiver derfor beretningen til Statsrevisorerne i henhold til § 8, stk. 1, og § 17, stk. 2, i rigsrevisorloven, jf. lovbekendtgørelse nr. 101 af 19. januar 2012.

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

Beretningen vedrører finanslovens § 8. Erhvervsministeriet.

I undersøgelsesperioden 1. januar 2017 - 31. december 2023 har der været følgende ministre:

Brian Mikkelsen: november 2016 - juni 2018
Rasmus Jarlov: juni 2018 - juni 2019
Simon Kollerup: juni 2019 - december 2022
Morten Bødskov: december 2022 -

Beretningen har i udkast været forelagt Erhvervsministeriet og Finanstilsynet, hvis bemærkninger i videst muligt omfang er afspejlet i beretningen.

1. Introduktion og konklusion

1.1. Formål og konklusion

1. I Danmark foregår næsten alle økonomiske aktiviteter digitalt. Det gælder alt fra lønudbetalinger, lån og almindelige indkøb til handel med værdipapirer. Derfor kan it-nedbrud og hackerangreb i finansielle virksomheder få store praktiske og økonomiske konsekvenser for både borgere og virksomheder. Nogle finansielle virksomheder er i kraft af deres størrelse eller karakteren af deres ydelser tilmed så væsentlige for den finansielle sektor og for samfundsøkonomien, at brud på it-sikkerheden vil kunne true den samlede finansielle stabilitet. Disse virksomheder kaldes *systemisk vigtige virksomheder*. Virksomheder, der ikke er systemisk vigtige benævnes i beretningen *øvrige virksomheder*.

Der er stor risiko for brud på it-sikkerheden. Finanstilsynet har siden 2018 vurderet, at it-sikkerhed er et af de væsentligste risikoområder for den finansielle sektor, og Center for Cybersikkerhed har i deres strategi for den finansielle sektors cyber- og informationssikkerhed vurderet, at trusselsniveauet mod den danske finansielle sektor er meget højt. Desuden viser en spørgeskemaundersøgelse fra 2023, som Finanstilsynet har foretaget blandt finansielle virksomheder, at risikoen på it-området er noget af det, der bekymrer virksomhederne mest, og også er noget af det, virksomhederne finder mest udfordrende at håndtere.

2. Det er Erhvervsministeriet, der udarbejder lovgrundlaget for finansielle virksomheder. I den gældende lovgivning har Finanstilsynet fået forholdsvis frie rammer til at tilrettelægge it-tilsynet. For det første har Finanstilsynet ifølge loven hjemmel til at fastlægge de regler, som virksomhederne skal efterleve i forhold til it-sikkerhed, og som Finanstilsynet dermed skal føre tilsyn med. For det andet er det op til Finanstilsynet at fastlægge niveauet for tilsynsaktiviteten inden for lovens rammer, der foreskriver, at tilsynet skal være baseret på væsentlighed og risiko. For det tredje er Finanstilsynet uafhængige af Erhvervsministeriet i udøvelsen af tilsynet. Dette indebærer ifølge ministeriet, at ministeriet ikke har instruktionsbeføjelser over for Finanstilsynet, hverken i forhold til den konkrete behandling af tilsynssager eller i forhold til den generelle tilrettelæggelse af tilsynsvirksomheden på området for it-sikkerhed.

Krav til virksomhedernes it-sikkerhed
Finanstilsynet har inden for rammerne af den europæiske banktilsynsmyndigheds retningslinjer fastsat de krav, der er gældende for virksomhedernes it-sikkerhed. Kravene fastlægger, hvordan virksomhederne skal styre og lede deres forretning, så de bedst muligt forebygger it-hændelser og hurtigst muligt får reetableret driften og minimeret skadevirkningerne, hvis der har været it-nedbrud.

3. Formålet med undersøgelsen er at vurdere, om Finanstilsynet har ført et tilfredsstillende tilsyn med finansielle virksomheders it-sikkerhed. Vi besvarer følgende spørgsmål i beretningen:

- Har Finanstilsynet tilrettelagt it-tilsynet tilfredsstillende?
- Har Finanstilsynet gennemført it-tilsynet tilfredsstillende?
- Har Finanstilsynet understøttet, at it-tilsynet får størst mulig virkning?

4. Rigsrevisionen har igangsat undersøgelsen i april 2023 på baggrund af en anmodning fra Statsrevisorerne, jf. bilag 1, hvor Statsrevisorernes spørgsmål fremgår.

Hovedkonklusion

Finanstilsynets tilsyn med finansielle virksomheders it-sikkerhed er ikke tilfredsstillende. Konsekvensen er, at der er risiko for, at virksomhedernes it-sikkerhed ikke er tilstrækkelig til at forhindre brud på it-sikkerheden til skade for kunderne og samfundet.

Finanstilsynets tilrettelæggelse af it-tilsynet er ikke helt tilfredsstillende

Finanstilsynet har siden 2019 vurderet de systemisk vigtige virksomheders risiko på it-området, men har kun delvist anvendt vurderingerne, når de har udvalgt virksomheder til tilsyn. Derudover har Finanstilsynet stort set ikke risikovurderet it-sikkerheden for investeringsforvaltningsselskaber og heller ikke for de e-penge- og betalingsinstitutter og datacentraler, der ikke er systemisk vigtige. Dette svarer til ca. halvdelen af de øvrige virksomheder.

Finanstilsynets gennemførelse af it-tilsynet er ikke tilfredsstillende

Finanstilsynet har i overensstemmelse med intentionerne i loven ført mere tilsyn med de systemisk vigtige virksomheder end med de øvrige virksomheder. Finanstilsynet har dog ikke inspiceret it-sikkerheden i en tredjedel af de systemisk vigtige virksomheder inden for det 4-årige interval, som de skal ifølge deres retningslinjer. I gennemsnit er der gået 4½ år mellem inspektionerne, og for nogle af virksomhederne er der gået over 7 år. Dermed kan de systemisk vigtige virksomheder, herunder de fælles datacentraler, som varetager it-opgaverne i næsten alle banker, have mangler i it-sikkerheden i adskillige år, uden at det bliver afdækket af Finanstilsynet.

Fælles datacentraler
Fælles datacentraler er virksomheder, der står for drift og udvikling af it-løsninger til banker og realkreditinstitutter.

Finanstilsynet har siden 2021 gennemført smallere inspektioner for til gengæld at kunne inspicere de systemisk vigtige virksomheder oftere. Det har haft den konsekvens, at der er områder, fx *adgangsstyring* og *fysisk sikkerhed*, som Finanstilsynet ikke har gennemført it-inspektioner af i flere år, selv om Finanstilsynet selv vurderer, at en del virksomheder har høje risici på områderne.

Finanstilsynet har kun i meget begrænset omfang inspiceret investeringsforvaltningsselskaber samt e-penge- og betalingsinstitutter, fordi Finanstilsynet har vurderet, at virksomhedernes risiko er lav. Finanstilsynet har dog ikke risikovurderet it-sikkerheden i virksomhederne og har derfor heller ikke et grundlag for at vide, om fravalget af tilsyn med it-sikkerheden er hensigtsmæssigt.

It-tilsyn og inspektioner
Finanstilsynets it-tilsyn består af forskellige aktiviteter. En væsentlig del gennemføres som inspektioner i virksomheder, men tilsynet omfatter også møder, risikovurderinger, overvågning, opfølgning på påbud mv.

Vi bruger betegnelsen *inspektioner*, når det alene drejer sig om tilsynsbesøg, og betegnelsen *tilsyn*, når det enten omfatter tilsynet i sin helhed eller flere aktiviteter end blot inspektioner.

Finanstilsynet understøtter ikke i tilstrækkelig grad, at it-tilsynet får størst mulig virkning

Finanstilsynet har i forbindelse med deres tilsyn givet hovedparten af de systemisk vigtige virksomheder påbud om at rette op på mangler i deres it-sikkerhed. Finanstilsynet har også sat frister for virksomhedernes efterlevelse af påbuddene og har fulgt systematisk op på, om virksomhederne efterlever dem. Virksomhederne har dog overskredet fristerne med 2 år i gennemsnit. Rigsrevisionen kan konstatere, at Finanstilsynet aldrig har anvendt deres hjemmel til at sanktionere virksomheder, der ikke efterlever de påbud, de har fået.

1.2. Baggrund

Finanstilsynet

5. Ifølge finansloven er det Finanstilsynets opgave at medvirke til finansiel stabilitet og til, at borgere og virksomheder har tillid til den finansielle sektor. Det indebærer, at Finanstilsynet skal:

- udarbejde regler på det finansielle område
- belyse udviklingen i den finansielle sektor gennem statistik og løbende information
- føre tilsyn med de finansielle virksomheder og markeder.

Denne undersøgelse handler om Finanstilsynets tilsyn med finansielle virksomheder, nærmere bestemt deres tilsyn med virksomhedernes it-sikkerhed.

Tilsynet med finansielle virksomheder

Foruden tilsynet med virksomhedernes it-sikkerhed omfatter tilsynet også:

- tilsyn med virksomhedernes likviditet
- tilsyn med udlån
- tilsyn med håndtering af hvidvaskrisici.

6. Finanstilsynet er fuldt finansieret af afgifter fra de virksomheder, der er underlagt tilsynet. I 2023 udgjorde udgifterne til Finanstilsynet 465,5 mio. kr., og der var ultimo 2023 i alt 423 ansatte, hvoraf 12 førte tilsyn med de systemisk vigtige virksomheders it-sikkerhed. It-tilsynet med de øvrige virksomheder er en del af Finanstilsynets generelle tilsyn, og de kan derfor ikke opgøre, præcis hvor mange ansatte der fører it-tilsyn med disse virksomheder.

Finansielle virksomheder

7. Der er i alt ca. 325 finansielle virksomheder, som er underlagt Finanstilsynets it-tilsyn. Denne undersøgelse omfatter it-tilsynet med 112 virksomheder, der fordeler sig på 8 typer virksomheder. Virksomhederne er udvalgt, så undersøgelsen bl.a. omfatter alle de systemisk vigtige virksomheder.

Tabel 1 viser de typer af finansielle virksomheder, der indgår i undersøgelsen.

Tabel 1
Typer af finansielle virksomheder, der indgår i undersøgelsen

Pengeinstitutter (banker) Omfatter både store banker, fx Danske Bank, og mindre lokale sparekasser, fx Sparekassen for Nørre Nebel og Omegn.	**Realkreditinstitutter og andre kreditinstitutter** Udlåner til køb af ejendomme. Omfatter fx Nykredit.
Fælles datacentraler Leverer it-løsninger til banker og realkreditinstitutter. Eksempler er JN Data og Gensam Data.	**Markedspladser** Regulerede markeder og multilaterale handelsfaciliteter, hvor der kan handles med værdipapirer. Omfatter kun Nasdaq, der driver de 2 danske markedspladser.
E-penge- og betalingsinstitutter Virksomheder, der formidler elektroniske betalinger mellem 2 parter. Omfatter fx Nets og Forbrugsforeningen.	**Værdipapircentraler** Værdipapircentralens system anvendes af deltagerne (primært banker) til udstedelse, opbevaring og afvikling af handler med værdipapirer. Omfatter kun VP Securities.
Investeringsforvaltningsselskaber Forvalter og administrerer danske investeringsforeninger. Et eksempel er Formuepleje.	**It-operatører af detailbetalingsselskaber** Driver de systemer, som afvikler betalinger mellem fysiske personer, virksomheder og offentlige myndigheder. I Danmark er der kun Mastercard.

Kilde: Rigsrevisionen på baggrund af oplysninger fra Finanstilsynet.

Virksomhederne varierer, både hvad angår størrelse og kompleksitet og i deres anvendelse af it-systemer.

Kravene til finansielle virksomheders it-sikkerhed

8. Det fremgår af lov om finansiel virksomhed (§ 71), lov om betalinger (§ 25) og lov om kapitalmarkeder (§ 180), at virksomhederne skal have betryggende kontrol- og sikringsforanstaltninger på it-området. Det er ikke nærmere specificeret, hvad det indebærer, men det fremgår, at Finanstilsynet kan fastsætte nærmere regler på området.

Finanstilsynet har i en bekendtgørelse om ledelse og risikostyring af pengeinstitutter m.fl. (ledelsesbekendtgørelsen) præciseret, hvordan pengeinstitutter, realkreditinstitutter og andre kreditinstitutter, investeringsforvaltningsselskaber og fælles datacentraler skal sikre betryggende kontrol- og sikringsforanstaltninger. Kravene er, at virksomhederne skal arbejde og være organiseret på en måde, der gør dem i stand til at opdage mangler i it-sikkerheden og iværksætte tiltag, der mindsker risikoen for brud på it-sikkerheden. Det skal de fx gøre ved at udarbejde it-strategier og forretningsgange, opbygge interne, uafhængige kontroller med it-sikkerheden og udarbejde planer for at genoprette systemerne, hvis der sker nedbrud.

Ledelsesbekendtgørelsen
Kravet om effektiv ledelse og risikostyring har været gældende siden 2010, men bestemmelserne i bekendtgørelsen er blevet udbygget og gjort mere detaljerede i løbet af undersøgelsesperioden. I den gældende bekendtgørelse er der flere end 100 bestemmelser, men det fremgår, at de skal overholdes på en måde, der står i rimeligt forhold til virksomhedens størrelse og til, om virksomheden har outsourcet it-systemerne til en fælles datacentral.

Outsourcing af it-området til en datacentral
De fleste banker, der ikke er systemisk vigtige, har outsourcet driften og udviklingen af deres it-systemer til en datacentral. I investeringsforvaltningsselskaberne samt de e-penge- og betalingsinstitutter, der ikke er systemisk vigtige, varetages it-driften af virksomhederne selv.

For de andre typer af finansielle virksomheder, som indgår i undersøgelsen, har Finanstilsynet ikke udstedt bekendtgørelser, der præciserer, hvordan virksomhederne skal sikre betryggende kontrol- og sikringsforanstaltninger. For værdipapircentraler reguleres kravene til it-sikkerhed af en EU-forordning om værdipapircentraler.

Finanstilsynet har desuden udstedt en bekendtgørelse, som pålægger fælles datacentraler og it-operatører af detailbetalingssystemer at udpege en ekstern revisor som en ekstra kontrolforanstaltning på it-området. Den eksterne revisor skal hvert år erklære sig om, hvorvidt virksomhedens it-sikkerhed er betryggende. Derudover skal virksomheder, der outsourcer til datacentraler, kontrollere, at datacentralernes arbejde er tilfredsstillende, og fx også have it-beredskabsplaner i tilfælde af nedbrud hos datacentralerne.

DORA-forordningen og NIS2-direktiv
DORA-forordningen skærper kravene til finansielle virksomheder i forbindelse med cyberangreb og stiller bl.a. krav om langt hurtigere genopretning efter eventuelle cyberangreb.

NIS2-direktivet øger bl.a. kravene til virksomhedernes risikostyring og indberetning af it-hændelser.

9. Lovkravene til de finansielle virksomheders it-sikkerhed forventes ændret i løbet af 2024 og 2025 som følge af implementeringen af EU's DORA-forordning og NIS2-direktiv. Finanstilsynet har oplyst, at de i løbet af 2024 vil fastlægge, hvilken betydning det skal have for deres it-tilsyn.

1.3. Vurderingskriterier, metode og afgrænsning

Vurderingskriterier

10. Vi forudsætter, at tilsynet skal være baseret på væsentlighed og risiko. Dette følger af lov om finansiel virksomhed, § 344, som de fleste virksomheder i undersøgelsen er underlagt. For de virksomheder, der ikke er underlagt lov om finansiel virksomhed, fremgår det af Finanstilsynets retningslinjer og politik for it-tilsynet, at Finanstilsynet også for disse virksomheder tilstræber, at tilsynet skal baseres på væsentlighed og risiko. Lovgivningen indeholder ingen bestemmelser om omfanget af tilsynet, og det er dermed op til Finanstilsynet selv at fastlægge, hvor ofte og hvordan, de skal føre tilsyn med virksomhederne, herunder hvor hyppigt de skal inspicere virksomhedernes it-sikkerhed.

Den europæiske banktilsynsmyndighed
Den europæiske banktilsynsmyndighed er et EU-agentur, hvis formål er at skabe en fælles ramme for regulering og tilsyn i hele EU's banksektor.

I forhold til Finanstilsynets tilrettelæggelse af it-tilsynet (afsnit 2.1) bør Finanstilsynet som forudsat i loven tilrettelægge it-tilsynet på en måde, der understøtter, at der føres mest tilsyn med de systemisk vigtige virksomheder. Derudover lægger vi til grund, at Finanstilsynet skal vurdere alle virksomheders it-risici, hvilket også anbefales af den europæiske banktilsynsmyndighed. Til sidst lægger vi til grund, at Finanstilsynet bør sikre, at de udvælger de systemisk vigtige virksomheder til inspektion, hvor de har vurderet, at der er størst risiko for utilstrækkelig it-sikkerhed.

I forhold til Finanstilsynets gennemførelse af it-tilsynet (afsnit 2.2) forudsætter vi, at de overholder deres egne retningslinjer for, hvor ofte de som minimum skal inspicere it-sikkerheden i systemisk vigtige virksomheder. Det gør vi, fordi Finanstilsynet selv har bemyndigelse til at tilrettelægge tilsynet og fastlægge inspektionsfrekvensen. Da de ikke har fastlagt nogen minimumsfrekvens for de øvrige virksomheder, har vi ikke noget grundlag for at vurdere, om tilsynsfrekvensen er tilstrækkelig.

I forhold til virkningen af tilsynet (afsnit 2.3) forudsætter vi, at Finanstilsynet skal understøtte, at deres tilsyn får størst mulig virkning. Dels ved i overensstemmelse med deres retningslinjer at sætte frister for, hvornår virksomhederne skal rette op på de mangler i it-sikkerheden, Finanstilsynet har fundet under inspektionerne. Dels ved at overvåge, om virksomhederne retter op. Vi undersøger i den forbindelse også, om Finanstilsynet anvender deres hjemmel til at give bøder til virksomheder, der overtræder reglerne for it-sikkerhed, eller som efterfølgende ikke efterlever de udstedte påbud.

Metode

11. Undersøgelsen er baseret på gennemgang af lovgrundlaget, internationale retningslinjer samt Finanstilsynets politikker, strategier og retningslinjer. Desuden er den baseret på gennemgang af Finanstilsynets risikovurderinger og inspektionsrapporter samt på materiale vedrørende Finanstilsynets opfølgning på virksomhedernes efterlevelse af påbud. For at understøtte analysen har vi holdt møder med Finanstilsynet.

12. Statsrevisorernes spørgsmål og angivelse af, i hvilke afsnit spørgsmålene bliver besvaret, fremgår af bilag 1. Undersøgelsens metode uddybes i bilag 2, og bilag 3 viser, hvilke finansielle virksomheder der indgår i undersøgelsen.

13. Revisionen er udført i overensstemmelse med standarderne for offentlig revision, jf. bilag 2.

Afgrænsning

14. Undersøgelsen omfatter perioden 2017-2023. Vi har ikke undersøgt, om virksomhederne efterlever lovkravene til it-sikkerhed, da Rigsrevisionen ikke har revisionsadgang til private virksomheder. Vi belyser i stedet, hvordan Finanstilsynet arbejder for at sikre, at virksomhederne har betryggende kontrol- og sikringsforanstaltninger på it-området.

Undersøgelsen omfatter Finanstilsynets it-tilsyn med 112 finansielle virksomheder. Virksomhederne repræsenterer 8 ud af 14 typer af finansielle virksomheder og udgør ca. en tredjedel af de finansielle virksomheder, som er underlagt it-tilsynet. Baggrunden for udvælgelse af virksomhederne er nærmere begrundet i bilag 2.

2. Finanstilsynets it-tilsyn

Dette kapitel handler om Finanstilsynets it-tilsyn. Vi har undersøgt:

- Finanstilsynets tilrettelæggelse af it-tilsynet (2.1)
- Finanstilsynets gennemførelse af it-tilsynet (2.2)
- Virkningen af Finanstilsynets it-tilsyn (2.3)
- Finanstilsynets it-tilsyn med udenlandske bankers danske filialer (2.4).

2.1. Tilrettelæggelse af it-tilsynet

15. Vi har undersøgt, om Finanstilsynet har tilrettelagt it-tilsynet ud fra vurderinger af virksomhedernes væsentlighed og risici.

16. Undersøgelsen viser, at it-tilsynet er tilrettelagt på baggrund af virksomhedernes væsentlighed, men i mindre grad ud fra vurderinger af virksomhedernes risici. Vi vurderer derfor, at tilrettelæggelsen af tilsynet ikke er helt tilfredsstillende.

Virksomhedernes væsentlighed

17. Vi har undersøgt, om Finanstilsynet løbende har vurderet virksomhedernes væsentlighed og tilrettelagt tilsynsaktiviteten derefter.

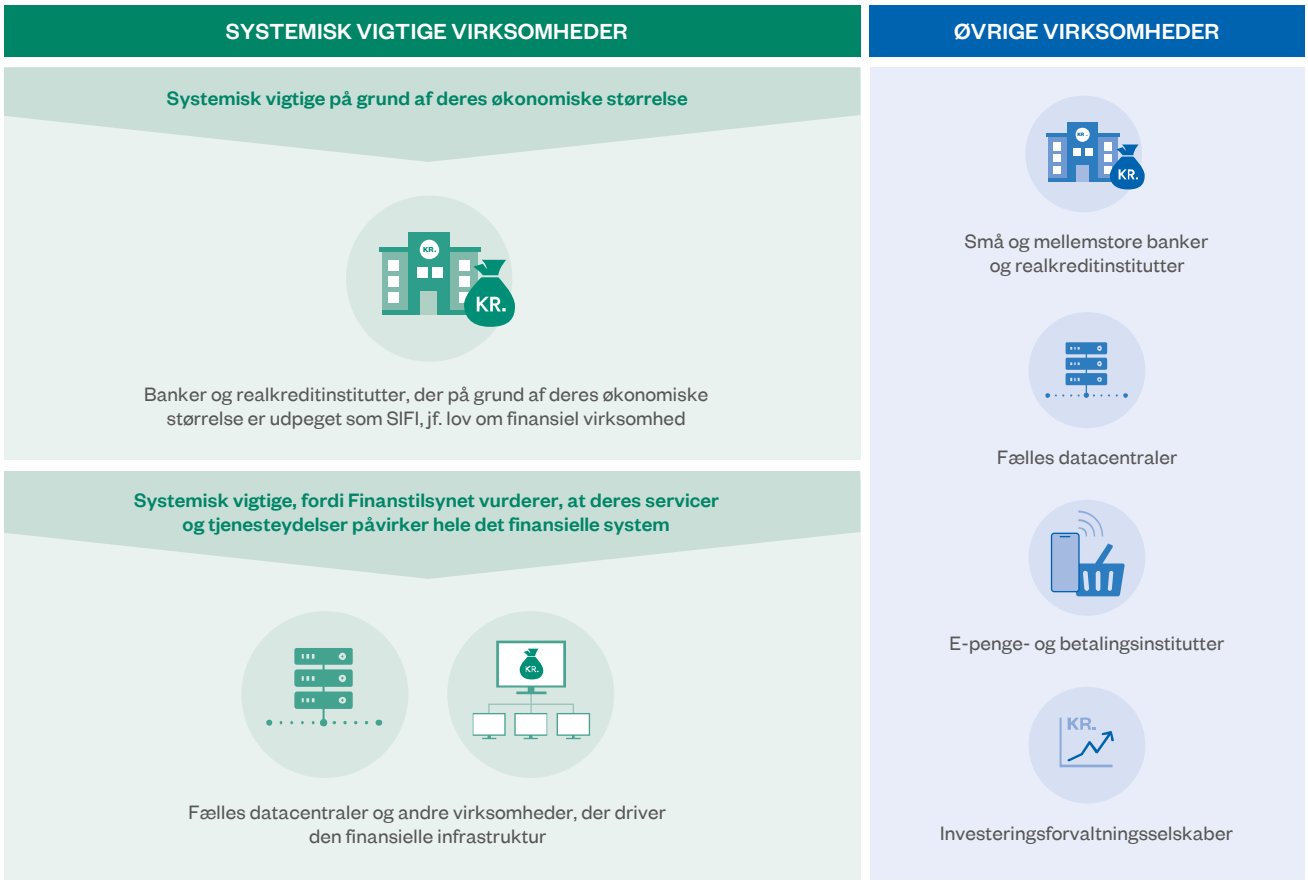
18. Undersøgelsen viser, at Finanstilsynet siden 2019 løbende har vurderet alle virksomhedernes væsentlighed ud fra en vurdering af, om brud på it-sikkerheden vil kunne påvirke den finansielle stabilitet. Finanstilsynet har desuden opdelt virksomhederne i 4 grupper efter, hvor store konsekvenser der vil være ved eventuelle it-nedbrud i virksomhederne. Alle de systemisk vigtige virksomheder udgør gruppe 1, mens de resterende virksomheder er fordelt på gruppe 2-4 efter væsentlighed. For overskuelighedens skyld sondrer vi kun mellem systemisk vigtige virksomheder og øvrige virksomheder i beretningen.

Gruppe 1 omfatter 18 virksomheder, herunder de 9 banker og realkreditinstitutter, der alene på grund af deres økonomiske størrelse er udpeget som systemisk vigtige, jf. lov om finansiel virksomhed, og som Finanstilsynet derfor ifølge loven skal føre et intensiveret tilsyn med. Derudover omfatter gruppen virksomheder, som Finanstilsynet vurderer som systemisk vigtige i forhold til it-sikkerhed, fordi de driver betalingssystemer, infrastruktur for værdipapirmarkedet eller står for drift og udvikling af it-systemer til banker og realkreditinstitutter Det gælder fx visse datacentraler, der driver kritiske systemer og opbevarer data for næsten alle banker i Danmark, samt en række virksomheder, der driver kritisk finansiel infrastruktur.

De øvrige virksomheder, som indgår i undersøgelsen, tæller i alt 94 virksomheder, som Finanstilsynet ikke vurderer er væsentlige i forhold til at sikre finansiel stabilitet. Det skyldes, enten at virksomhederne er forholdsvis små i økonomisk forstand, eller at de har outsourcet deres it-systemer til en af de systemisk vigtige fælles datacentraler, som Finanstilsynet også fører it-tilsyn med. Dette gælder for de fleste banker på nær de allerstørste.

Figur 1 viser, hvilke typer virksomheder der indgår i gruppen af systemisk vigtige virksomheder, og hvilke typer øvrige virksomheder der indgår i undersøgelsen.

Figur 1
Virksomhedstyper blandt de systemisk vigtige og de øvrige virksomheder



Note: Bilag 3 viser, hvilke virksomheder der indgår i undersøgelsen.

Kilde: Rigsrevisionen på baggrund af oplysninger fra Finanstilsynet.

Udvælgelsen af inspektioner i de øvrige virksomheder
Ifølge Finanstilsynets retningslinjer skal de først udarbejde en samlet risikovurdering af virksomheden, som de anvender til at udvælge, hvilke virksomheder der skal inspiceres. Når Finanstilsynet har valgt de virksomheder, hvor der samlet er størst risici, skal de derefter vælge, hvilke områder, fx it-sikkerhed, der skal undersøges i inspektionen. Om it-sikkerheden bliver inspiceret, afhænger altså først af virksomhedens samlede risiko i forhold til de andre virksomheders. Dernæst afhænger det af, om risikoen på it-området er høj, hvis der sammenlignes med risikoen på virksomhedens øvrige områder.

19. Undersøgelsen viser endvidere, at Finanstilsynet siden 2019 har tilrettelagt tilsynsaktiviteten efter, hvilken gruppe virksomhederne er placeret i, så Finanstilsynet fører mere it-tilsyn med de systemisk vigtige virksomheder end med de øvrige virksomheder.

For de systemisk vigtige virksomheder har Finanstilsynet valgt, at der skal gennemføres inspektioner, som kun vedrører it-området (it-inspektioner). Finanstilsynet har derudover fastlagt en minimumsfrekvens for, hvor ofte de skal gennemføre it-inspektioner. For de øvrige virksomheder har Finanstilsynet ikke fastsat en minimumsfrekvens, men i stedet tilrettelagt en udvælgelsesproces, hvor de kun skal inspicere it-området i visse tilfælde.

Det fremgår ikke af Finanstilsynets retningslinjer, hvordan inspektionerne af it-sikkerheden i de systemisk vigtige virksomheder adskiller sig metodemæssigt og indholdsmæssigt fra inspektionerne af it-sikkerheden i de øvrige virksomheder. Vores gennemgang af inspektionsrapporter viser dog, at både krav og behandlingsdybde er større ved en inspektion i en systemisk vigtig virksomhed, hvilket medfører, at inspektionen bliver mere omfattende og tager længere tid at gennemføre.

Virksomhedernes risici

20. Vi har undersøgt, om Finanstilsynet har tilrettelagt it-tilsynet ud fra vurderinger af virksomhedernes risici på it-området.

Risici
Finanstilsynet skal føre tilsyn med, at virksomhederne overholder lovkravene vedrørende it-sikkerhed. Derfor forstås risici i denne sammenhæng som risikoen for, at virksomhederne ikke har tilstrækkelig it-sikkerhed, fordi de ikke efterlever de krav til it-sikkerhed, som Finanstilsynet har fastsat i de relevante bekendtgørelser.

Det følger af lov om finansiel virksomhed og af Finanstilsynets retningslinjer, at Finanstilsynets tilsyn skal stå mål med de potentielle risici. Derudover anbefaler den europæiske banktilsynsmyndighed, at Finanstilsynet løbende vurderer de risici, den enkelte virksomhed kan blive eksponeret for med henblik på at tilpasse tilsynsaktiviteten.

Vi lægger til grund, at Finanstilsynet skal risikovurdere it-sikkerheden i alle virksomheder. For de systemisk vigtige virksomheder, hvor risici ved mangelfuld it-sikkerhed ifølge Finanstilsynet altid er væsentlige, bør de udarbejde særskilte it-risikovurderinger. For de øvrige virksomheder behøver der ikke blive udarbejdet særskilte risikovurderinger af it-området, idet vurderingerne også kan ske som led i en samlet risikovurdering af virksomheden.

21. Undersøgelsen viser, at Finanstilsynet kun delvist har tilrettelagt tilsynet på baggrund af vurderinger af virksomhedernes risici på it-området.

De systemisk vigtige virksomheder

22. Undersøgelsen viser, at Finanstilsynet siden 2019 har udarbejdet it-risikovurderinger for de systemisk vigtige virksomheder. Det har de gjort på baggrund af virksomhedernes egne risikovurderinger, halvårlige it-statusmøder med systemiske virksomheder, revisionsprotokollater og -erklæringer, indberetning af it-hændelser og på baggrund af viden fra tidligere inspektioner samt eventuel igangværende opfølgning på påbud i virksomheden.

Undersøgelsen viser også, at Finanstilsynet ikke alene har udvalgt virksomheder til it-inspektion på baggrund af risikovurderingerne. Boks 1 viser nogle af de kriterier, Finanstilsynet bruger til at udvælge virksomhederne.

Boks 1

Kriterier for Finanstilsynets udvælgelse af systemisk vigtige virksomheder til it-inspektion

1. Finanstilsynets vurdering af virksomhedens risiko på it-området.
2. Overholdelse af den fastlagte minimumsfrekvens for it-inspektioner.
3. Om virksomheden for nyligt er udpeget som systemisk vigtig, eller der tidligere er gennemført it-inspektioner.
4. Om virksomheden har åbne påbud. Hvis virksomheden stadig har åbne påbud fra sidste it-inspektion, vil Finanstilsynet i udgangspunktet ikke prioritere at udtage virksomheden til en ny it-inspektion.

Kilde: Finanstilsynets retningslinjer for planlægning af inspektioner.

Det fremgår af Finanstilsynets retningslinjer, at der skal være en minimumsfrekvens for it-inspektioner i systemisk vigtige virksomheder, og at den skal fastlægges ud fra virksomhedernes risiko. Dette skal ifølge retningslinjerne sikre, at der oftere gennemføres inspektioner i de virksomheder, hvor Finanstilsynet vurderer, at risikoen for at overtræde reglerne er højere sammenlignet med andre virksomheder af samme størrelse eller væsentlighed.

Undersøgelsen viser dog, at Finanstilsynet ikke tilpasser minimumsfrekvensen for it-inspektioner ud fra vurderinger af virksomhedernes risiko på it-området. Finanstilsynet har i stedet fastlagt en fast minimumsfrekvens på 4 år for it-inspektioner i systemisk vigtige virksomheder, uanset om virksomhedernes risiko på it-området er høj eller lav. Dette adskiller sig fra andre områder af Finanstilsynets tilsynsvirksomhed, fx tilsynet med virksomhedernes kapitalsituation og solvensbehov. Her fremgår det af retningslinjerne, at Finanstilsynet skal bruge risikovurderinger til at fastlægge minimumsfrekvenser på 1 og 2 år for inspektioner, hvis virksomhederne har en risiko, som er over middel eller høj.

Rigsrevisionen vurderer, at det ikke er tilfredsstillende, at Finanstilsynet ikke tilpasser minimumsfrekvensen for it-inspektioner i systemisk vigtige virksomheder til de enkelte virksomheders risici på it-området.

De øvrige virksomheder

23. Undersøgelsen viser, at Finanstilsynet siden 2020 har foretaget systematiske vurderinger af it-sikkerheden i ca. halvdelen af de øvrige virksomheder, nemlig bankerne. Finanstilsynet har således for alle banker udarbejdet risikovurderinger forud for udvælgelsen af inspektioner. I risikovurderingen indgår virksomhedernes risiko for mangelfuld it-sikkerhed som en obligatorisk og selvstændig del af vurderingen.

I forhold til investeringsforvaltningsselskaberne samt de-penge- og betalingsinstitutter og datacentraler, der ikke er systemisk vigtige, har Finanstilsynet derimod ikke på systematisk vis vurderet it-sikkerheden, inden de har udvalgt virksomheder til inspektion. Det svarer til ca. halvdelen af de øvrige virksomheder, der indgår i undersøgelsen. Finanstilsynet har oplyst, at deres vurdering af e-penge- og betalingsinstitutters it-sikkerhed indgår i den samlede risikovurdering af virksomhederne.

Undersøgelsen viser dog, at virksomhedernes it-sikkerhed kun i meget begrænset omfang og kun for enkelte virksomheder er omtalt i risikovurderingerne. Vi vurderer derfor, at Finanstilsynet ikke har tilrettelagt inspektionerne ud fra en systematisk vurdering af virksomhedernes risiko for mangelfuld it-sikkerhed.

2.2. Gennemførelse af it-tilsynet

24. Vi har undersøgt, om Finanstilsynets gennemførelse af it-tilsyn er tilfredsstillende. For at vurdere dette har vi fokuseret på inspektionerne i virksomhederne.

Undersøgelsen viser, at Finanstilsynets gennemførelse af it-inspektioner i finansielle virksomheder ikke er tilfredsstillende. Det skyldes for det første, at Finanstilsynet ikke har overholdt deres egen minimumsfrekvens for it-inspektioner for en tredjedel af de systemisk vigtige virksomheder, og for det andet, at der er risikofyldte områder, som Finanstilsynet ikke har gennemført inspektioner af i flere år. For det tredje, at Finanstilsynet stort set ikke har inspiceret it-sikkerheden i investeringsforvaltningsselskaberne samt de e-penge- og betalingsinstitutter, der ikke er systemisk vigtige.

It-inspektioner i systemisk vigtige virksomheder

25. Vi har undersøgt, hvor mange it-inspektioner Finanstilsynet har gennemført, og om de har overholdt minimumsfrekvensen for it-inspektioner. Vi har i den forbindelse også undersøgt, hvor lang tid der er gået mellem it-inspektionerne i virksomhederne. Endelig har vi undersøgt, om Finanstilsynet sikrer, at deres it-inspektioner dækker alle risikofyldte it-sikkerhedsområder i virksomhederne.

Cyberstresstest
Stresstest af cyberrobusthed og it-beredskab simulerer et it-nedbrud for at undersøge, hvor hurtigt virksomheden kan genoprette it-systemerne, og hvilke konsekvenser nedbruddet har for forretningsprocesser og virksomhedens kunder.

Foruden it-inspektionerne har Finanstilsynet fra og med 2023 suppleret inspektionerne med stresstests af virksomhedernes cyberrobusthed og it-beredskab. Finanstilsynet har udført tests i 7 virksomheder og forventer, at testresultaterne offentliggøres medio 2024. Finanstilsynets cyberstresstests indgår ikke i opgørelsen af minimumsfrekvensen og tidsintervallet mellem it-inspektionerne og heller ikke i opgørelsen af inspektionernes dækning af it-områder.

Overholdelse af minimumsfrekvensen for it-inspektioner

26. Undersøgelsen viser, at Finanstilsynet har gennemført 20 it-inspektioner i de systemisk vigtige virksomheder i perioden 2017-2023.

I perioden 2017-2023 har i alt 19 virksomheder på et tidspunkt været kategoriseret som systemisk vigtige. Én af virksomhederne er i løbet af perioden blevet opkøbt og er ikke længere systemisk vigtig. 13 af virksomhederne har været kategoriseret som systemisk vigtige i hele perioden, mens 5 af dem er blevet udpeget i løbet af perioden. Pr. 31. december 2023 var der 18 systemisk vigtige virksomheder.

27. Finanstilsynet har i deres retningslinjer fastsat en minimumsfrekvens for, hvor ofte de skal gennemføre it-inspektioner i systemisk vigtige virksomheder. Ifølge retningslinjerne må der højst gå 4 år, uanset om virksomhederne har høj eller lav risiko på it-området.

Det fremgår ikke af Finanstilsynets retningslinjer, hvordan intervallet mellem inspektionerne skal opgøres. Vi har derfor brugt den metode, som Finanstilsynet har oplyst, at de selv anvender.

Figur 2 viser, i hvilket omfang Finanstilsynet har overholdt minimumsfrekvensen i perioden 2017-2023 for de virksomheder, der var systemisk vigtige pr. 31. december 2023.

Figur 2

Finanstilsynets overholdelse af minimumsfrekvensen for it-inspektioner

Note: Perioden er regnet fra tidspunktet, hvor virksomheden modtager den afsluttende rapport fra den første inspektion, til Finanstilsynet sender virksomheden et indkaldelsesbrev til næste inspektion. Én virksomhed kan ikke vurderes, da den er udpeget som systemisk vigtig i 2023 og endnu ikke er inspiceret.

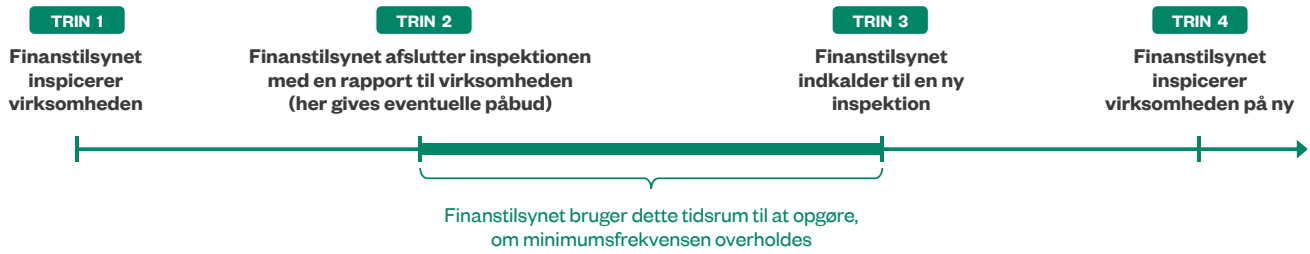
Kilde: Rigsrevisionens på baggrund af Finanstilsynets opgørelse af overholdelsen af minimumsfrekvensen.

Det fremgår af figur 2, at Finanstilsynet har overholdt minimumsfrekvensen for it-inspektioner i 11 ud af de 18 systemisk vigtige virksomheder, men har overtrådt den i 6 virksomheder. 2 ud af de 6 virksomheder er fælles datacentraler, der varetager driften og udviklingen af it-systemer for mange små og mellemstore banker og derudover også leverer it-ydelser til hovedparten af de systemisk vigtige banker. Det betyder, at eventuelle mangler i it-sikkerheden i datacentralerne kan få betydning for mange virksomheder.

28. Figur 3 viser, hvilke trin der er i Finanstilsynets inspektioner, og hvordan Finanstilsynet har opgjort, om de har overholdt deres minimumsfrekvens for en inspektion i en systemisk vigtig virksomhed.

I opgørelsen over overholdelsen af minimumsfrekvensen har Finanstilsynet beregnet tidsrummet, fra virksomhederne modtager den afsluttende rapport fra Finanstilsynets første inspektion (trin 2), til tidspunktet, hvor Finanstilsynet sender virksomheden et indkaldelsesbrev til den næste inspektion (trin 3).

Figur 3
Trin i inspektionsprocessen og Finanstilsynets opgørelse af overholdelsen af minimumsfrekvensen



Kilde: Rigsrevisionen på baggrund af Finanstilsynets oplysninger om deres opgørelsesmetode.

Som det fremgår af figur 3 tager Finanstilsynets opgørelse af minimumsfrekvensen ikke højde for, hvor lang tid der går, fra Finanstilsynet inspicerer den enkelte virksomhed og dermed afdækker eventuelle mangler i virksomhedens it-sikkerhed, til inspektionen afsluttes med en rapport. Vores gennemgang af Finanstilsynets inspektionsrapporter viser, at der er betydelig forskel på, hvor lang tid der er gået, fra inspektionerne bliver udført i virksomhederne, til virksomhederne har modtaget den afsluttende rapport. For 5 inspektioner er den afsluttende rapport sendt mere end ét år efter, at inspektionen blev udført i virksomhederne. Derudover er der også forskel på, hvor lang tid der er gået, fra Finanstilsynet sender indkaldelsesbrevene, til de inspicerer virksomhederne. I 5 tilfælde er der gået mere end 6 måneder.

Vi har derfor også opgjort, hvor lang tid der er gået mellem, at Finanstilsynet har været til stede i virksomhederne og udført inspektioner (dvs. tidsrummet mellem trin 1 og trin 4 i figur 3).

Tabel 2 viser tidsintervallet mellem it-inspektionerne.

Tabel 2
Tidsintervallet mellem it-inspektionerne

Interval mellem inspektioner	Antal virksomheder
Mindre end 4 år mellem inspektioner	6
4-5 år mellem inspektioner	5
5-6 år mellem inspektioner	3
6-7 år mellem inspektioner	0
7 år eller derover mellem inspektioner	3

Note: Perioden er regnet fra tidspunktet for gennemførelsen af den forrige it-inspektion til tidspunktet for gennemførelsen af den næste inspektion. En af de 18 systemisk vigtige virksomheder indgår ikke i tabellen, fordi den endnu ikke er inspiceret, da den først er udpeget som systemisk vigtig i 2023.

Kilde: Rigsrevisionens beregninger på baggrund af Finanstilsynets inspektionsrapporter.

Tabel 2 viser, at der ved udgangen af 2023 i 11 virksomheder er gået mere end 4 år mellem, at inspektionerne er udført. Det gælder også for virksomheder, hvor Finanstilsynet i løbet af undersøgelsesperioden har vurderet, at risikoen på it-området var over middel eller høj. Desuden viser tabellen, at der for 3 virksomheder er gået over 7 år mellem inspektionerne. Samlet set er der i gennemsnit gået 4½ år mellem inspektionerne.

29. Rigsrevisionen finder det ikke tilfredsstillende, at der i gennemsnit er gået 4½ år, og at der for nogle af virksomhederne er gået over 7 år mellem inspektionerne.

Inspektionernes dækning af it-områder

30. Finanstilsynet har inddelt virksomhedernes it-sikkerhed i 7 forskellige it-områder, jf. boks 2.

Boks 2

IT-områder

Risiko- og sikkerhedsstyring: Om virksomhedens strategier, processer og organisering sikrer, at sårbarheder i it-sikkerheden kan opdages og udbedres.

It-beredskab: Om virksomheden har opdateret sine it-beredskabsplaner og tester dem.

Outsourcing: Om virksomheden kontrollerer, at leverandører efterlever virksomhedens it-sikkerhedskrav.

It-revision: Om virksomhedens styring og systemer på it-sikkerhedsområdet revideres af en uafhængig revisor.

Driftsstyring: Virksomhedens arbejde med at styre driften og beskyttelsen af bl.a. systemer, netværk, data og enheder.

Adgangsstyring og fysisk sikkerhed: Om virksomheden sikrer systemer mod misbrug af adgangsrettigheder, sikrer den fysiske adgang og sikrer elforsyningen til følsomme områder som serverrum mv.

Anskaffelse, udvikling og vedligehold: Om virksomheden fx i tilstrækkelig grad styrer it-projekter og anskaffelsen af nye it-systemer.

Kilde: Finanstilsynets retningslinjer.

I perioden 2017-2020 dækkede Finanstilsynets inspektioner de fleste it-områder i de enkelte virksomheder. Siden 2021 har Finanstilsynet gennemført smallere inspektioner for til gengæld at kunne inspicere virksomhederne hyppigere og målrette inspektionerne mod de områder, hvor Finanstilsynet har vurderet, at risikoen er størst.

For at understøtte udvælgelsen af it-sikkerhedsområder til inspektion udarbejdede Finanstilsynet i perioden 2021-2022 en risikovurdering for hver af de systemisk vigtige virksomheder, der opgjorde virksomhedernes risici på de enkelte it-sikkerhedsområder. Det fremgår af disse risikovurderinger, at Finanstilsynet vurderede, at de mest risikofyldte it-sikkerhedsområder var *risiko- og sikkerhedsstyring*, *it-beredskab*, *adgangsstyring og fysisk sikkerhed* samt *driftsstyring*. Finanstilsynet vurderede for disse områder, at en del virksomheder havde høj risiko for mangler i it-sikkerheden.

31. Undersøgelsen viser, at Finanstilsynet ikke har dækket 2 af de 4 mest risikofyldte it-områder i perioden 2021-2023. Finanstilsynet har siden 2021 gennemført 9 inspektioner, som alle har dækket områderne *risiko- og sikkerhedsstyring*, *it-revision* og/eller *it-beredskab*, men har ikke gennemført inspektioner af it-områderne *adgangsstyring og fysisk sikkerhed* og *driftsstyring*, selv om det er nogle af de mest risikofyldte områder ifølge Finanstilsynets egne vurderinger.

Finanstilsynet har oplyst, at prioriteringen af områderne risiko- og sikkerhedsstyring samt it-beredskab for det første skyldes, at nye virksomheder er blevet udpeget som systemisk vigtige, og at Finanstilsynet i disse tilfælde derfor har valgt at inspicere den overordnede styring af it-sikkerheden først. For det andet skyldes prioriteringen ifølge Finanstilsynet, at de har fulgt op på en række ældre påbud vedrørende driftsstyring samt adgangsstyring og fysisk sikkerhed, som de udstedte i forbindelse med de bredere inspektioner før 2021.

Finanstilsynet har dog i slutningen af 2023 planlagt og igangsat flere smalle inspektioner af de risikofyldte områder: adgangsstyring og fysisk sikkerhed eller driftsstyring.

32. Finanstilsynets smallere fokus i inspektionerne siden 2021 har medført en risiko for, at inspektionerne ikke dækker alle risikofyldte it-områder i virksomhederne, og at mangler i it-sikkerheden på nogle områder dermed først undersøges flere år efter, at Finanstilsynet vurderer, at en virksomhed har forhøjet risiko på et område.

Inspektioner i øvrige virksomheder

33. Vi har undersøgt, hvor mange inspektioner af it-sikkerheden Finanstilsynet har gennemført i de øvrige 94 finansielle virksomheder, og om de har inspiceret de virksomheder, hvor risikoen for mangler i it-sikkerheden var størst.

Det fremgår ikke af lovgivningen, hvor ofte Finanstilsynet skal inspicere it-området i de øvrige virksomheder, og Finanstilsynet har heller ikke retningslinjer for det. Det følger dog af lovgivningen og af Finanstilsynets retningslinjer, at Finanstilsynet skal føre et risikobaseret tilsyn, og af Finanstilsynets politik for it-tilsyn, at de dermed kan føre mindre tilsyn med virksomheder, hvor konsekvenserne af it-nedbrud ikke er væsentlige.

34. Undersøgelsen viser, at Finanstilsynet i overensstemmelse med loven og deres politik for it-tilsyn fører mindre tilsyn med de finansielle virksomheder, der ikke er systemisk vigtige. Det kommer for det første til udtryk ved, at de ikke gennemfører særskilte it-inspektioner i disse virksomheder, men i stedet samlede inspektioner af virksomhederne, hvor de undersøger forskellige udvalgte områder af virksomhedens drift. For det andet ved, at Finanstilsynet kun har inspiceret it-sikkerheden i 41 % af de nuværende øvrige virksomheder.

Undersøgelsen viser, at Finanstilsynet i perioden 2017-2023 har udvalgt it-sikkerhed som ét af de områder, de skulle undersøge i forbindelse med i alt 79 inspektioner.

Figur 4 viser andelen af øvrige virksomheder, hvor Finanstilsynet har udvalgt it-sikkerheden som ét af de inspicerede områder. Figuren viser også, om Finanstilsynet har risikovurderet it-sikkerheden i virksomhederne i perioden 2017-2023.

Figur 4
Inspektioner i øvrige virksomheder i perioden 2017-2023

Tilsynsaktivitet	Banker	E-penge- og betalingsinstitutter	Investerings-forvaltningsselskaber	Fælles datacentraler
				
Inspektioner	Finanstilsynet har inspiceret it-sikkerheden i 76 % af virksomhederne.	Finanstilsynet har ikke inspiceret it-sikkerheden. Finanstilsynet har i stedet inspiceret den overordnede risikostyring i 24 % af virksomhederne.	Finanstilsynet har inspiceret it-sikkerheden i 8 % af virksomhederne.	Finanstilsynet har inspiceret it-sikkerheden i 50 % af virksomhederne.
Risikovurderinger	Finanstilsynet har siden 2020 risikovurderet it-sikkerheden.	Finanstilsynet har stort set ikke risikovurderet it-sikkerheden.	Finanstilsynet har ikke risikovurderet it-sikkerheden.	Finanstilsynet har ikke risikovurderet it-sikkerheden.

Kilde: Rigsrevisionen på baggrund af Finanstilsynets inspektionsrapporter og risikovurderinger.

Det fremgår af figur 4, at Finanstilsynet primært har ført tilsyn med it-sikkerheden i bankerne, hvor de har inspiceret it-sikkerheden i 76 % af virksomhederne. Det fremgår også af figuren, at de næsten ikke har inspiceret it-sikkerheden i investeringsforvaltningsselskaberne samt de e-penge- og betalingsinstitutter, der ikke er systemisk vigtige, selv om disse virksomheder tilsammen udgør næsten halvdelen af de øvrige virksomheder. Endelig har Finanstilsynet inspiceret it-sikkerheden i 50 % af de fælles datacentraler.

Finanstilsynet har oplyst, at de gennemfører generelle inspektioner af e-penge- og betalingsinstitutters interne kontrolprocedurer og risikostyring. Selv om inspektionerne ikke er målrettet it-området, dækker inspektionerne ifølge Finanstilsynet også virksomhedernes risici på it-området. Undersøgelsen viser, at Finanstilsynet i perioden 2017-2023 har gennemført generelle inspektioner af den overordnede risikostyring i 24 % af e-penge- og betalingsinstitutterne.

Eftersom Finanstilsynet enten slet ikke eller stort set ikke har risikovurderet it-sikkerheden i de investeringsforvaltningsselskaber og e-penge- og betalingsinstitutter, som er blandt de øvrige virksomheder, ved Finanstilsynet ikke, om der er potentielle risici eller mangler i it-sikkerheden, som virksomhederne burde rette op på. I modsætning til bankerne outsourcer investeringsforvaltningsselskaber samt e-penge- og betalingsinstitutter ikke deres it-drift og udvikling til datacentralerne, og Finanstilsynets tilsyn med de fælles datacentraler vil derfor heller ikke dække eventuelle mangler i it-sikkerheden.

35. Da Finanstilsynet siden 2020 har risikovurderet it-sikkerheden i bankerne, har vi undersøgt, om Finanstilsynet har inspiceret it-sikkerheden i de banker, der havde størst risiko for at overtræde reglerne for it-sikkerhed.

Undersøgelsen viser, at Finanstilsynet generelt har vurderet bankernes risiko på it-området som lav eller middel. Undersøgelsen viser også, at Finanstilsynet i lidt højere grad har inspiceret it-sikkerheden i de banker, hvor risikoen for brud på it-sikkerheden var middel, hvis der sammenlignes med de banker, hvor Finanstilsynet vurderede risikoen til at være lav.

2.3. It-tilsynets virkning

36. Vi har undersøgt, om Finanstilsynet har understøttet, at it-tilsynet får størst mulig virkning. Vi har i den forbindelse undersøgt, hvor mange påbud de har udstedt til virksomhederne, om de har fulgt op på, om virksomhederne efterlever påbuddene, og om de har anvendt de sanktioner, de har hjemmel til over for virksomheder, der ikke efterlever påbuddene.

Desuden har vi undersøgt, hvilke muligheder kunderne har for at blive orienteret om Finanstilsynets påbud til pengeinstitutter, og om de oplysninger, der bliver offentliggjort, giver kunderne mulighed for at orientere sig om it-sikkerhedsmæssige risici og påbud i deres bank.

Undersøgelsen viser, at Finanstilsynet ikke i tilstrækkelig grad understøtter, at it-tilsynet får størst mulig virkning.

37. Finanstilsynet har hjemmel til at udstede påbud, hvis lovgivningen på det finansielle område bliver overtrådt. Ifølge Finanstilsynets retningslinjer skal der anvendes påbud i forbindelse med en væsentlig lovovertrædelse, hvor der er behov for at pålægge en virksomhed en bestemt adfærd eller handling. Enten fordi virksomheden handler på en måde, der er i strid med loven, eller fordi virksomheden undlader at handle, hvor handling er påkrævet efter lovgivningen.

Hvis virksomheden ikke efterlever påbuddene, har Finanstilsynet flere sanktionsmuligheder. For det første kan de udstede administrative bødeforlæg. For det andet kan de anmelde virksomheden til politiet, som derefter kan idømme virksomhederne en bødestraf for brud på lovgivningen.

Omfanget af påbud

38. Vi har undersøgt, hvor mange påbud Finanstilsynet har givet pr. it-inspektion til henholdsvis systemisk vigtige og øvrige virksomheder.

Tabel 3 viser antal inspektioner og antal påbud i perioden 2017-2023 for henholdsvis systemisk vigtige virksomheder og øvrige virksomheder.

Tabel 3
Antal it-inspektioner og antal påbud i perioden 2017-2023

Virksomhed	Antal it-inspektioner	Antal påbud
Systemisk vigtige virksomheder	20	76
Øvrige virksomheder	79	53

Note: De 79 inspektioner i øvrige virksomheder dækker både inspektioner i nuværende virksomheder og inspektioner i virksomheder, der ikke længere eksisterede ved udgangen af 2023.

Kilde: Rigsrevisionen på baggrund af Finanstilsynets inspektionsrapporter.

Det fremgår af tabel 3, at Finanstilsynet i perioden 2017-2023 har givet i alt 76 påbud i forbindelse med de 20 it-inspektioner i systemisk vigtige virksomheder. Derudover har de givet 53 påbud vedrørende it-sikkerhed til de øvrige virksomheder fordelt på 79 inspektioner.

Boks 3 viser eksempler på påbud, som Finanstilsynet har givet til systemisk vigtige virksomheder på de forskellige it-områder.

Boks 3
Eksempler på påbud givet til systemisk vigtige virksomheder

Risiko- og sikkerhedsstyring: Virksomheden skal sikre klarhed om rapporteringslinjerne fra den complianceansvarlige og til bestyrelsen.

It-beredskab: Virksomheden skal udarbejde og implementere formaliserede krav og forretningsgange for, hvordan relevante testscenarier identificeres, risikovurderes og testes.

Outsourcing: Virksomheden skal kontrollere, om de outsourcede aktiviteter udføres tilfredsstillende, og om der bliver foretaget it-risikovurderinger af alle outsourcede aktiviteter.

Driftsstyring: Virksomheden skal sikre, at adgange til data kun tildeles på baggrund af et arbejdsmæssigt behov.

Anskaffelse, udvikling og vedligehold: Virksomheden skal implementere ledelsesgodkendte forretningsgange for ændringsstyring, der som minimum efterlever sikkerhedsstandarderne på området, og begrænse adgangen til fortrolige informationer til medarbejdere med et direkte arbejdsbetinget behov herfor.

Kilde: Finanstilsynets offentliggjorte inspektionsredegørelser.

Finanstilsynet har både for systemisk vigtige virksomheder og for øvrige virksomheder givet flest påbud inden for området risiko- og sikkerhedsstyring og næstflest inden for området it-beredskab. Det skal ses i lyset af, at det også er de områder, som Finanstilsynet har udtaget til inspektion flest gange.

Undersøgelsen viser også, at Finanstilsynet har givet påbud på grund af mangler i it-sikkerheden i forbindelse med 80 % af inspektionerne i de systemisk vigtige virksomheder og i forbindelse med 44 % af inspektionerne i de øvrige virksomheder. Tallene understøtter, at der er problemer med it-sikkerheden i finansielle virksomheder og behov for at føre tilsyn med deres it-sikkerhed.

Finanstilsynets opfølgning

39. Vi har undersøgt, om Finanstilsynet har fulgt op på, om virksomhederne efterlever påbuddene. Vi har i den forbindelse undersøgt, om Finanstilsynet har sat frister for, hvornår virksomhederne senest skal have efterlevet påbuddene og have rettet op på manglerne i it-sikkerheden. Vi har også undersøgt, om Finanstilsynet har overvåget, om virksomhederne har overholdt fristerne, og om de har vurderet, at virksomhederne har efterlevet påbuddene inden for fristen.

Når Finanstilsynet afslutter inspektionerne, skal de fastsætte frister for, hvornår virksomhederne skal have efterlevet påbuddene, og registrere fristerne i Finanstilsynets registreringssystem. Dette fremgår af Finanstilsynets retningslinjer. Det fremgår desuden, at de kan forlænge fristen, hvis virksomhedernes anmodning om fristforlængelse er velbegrundet.

40. Undersøgelsen viser, at Finanstilsynet i samarbejde med virksomhederne har sat frister for, hvornår den enkelte virksomhed skal have rettet op på manglerne i it-sikkerheden og have efterlevet påbud. De frister, der er blevet fastsat i perioden 2017-2023, varierer mellem 3 måneder og 4½ år. Finanstilsynet har oplyst, at lange frister kan skyldes, at virksomhederne skal igangsætte gennemgribende projekter og investeringer, herunder fx:

- etablere og implementere nye politikker, koncepter og procedurer
- indkøbe og implementere nye systemer til risikostyring, kontroller og ledelsesrapportering, adgangsstyring, logning og overvågning af brugeraktivitet
- opkvalificere it-kompetencer på flere niveauer i virksomheden.

Da det beror på en faglig vurdering, har vi ikke vurderet, om fristerne er rimelige i forhold til de enkelte påbud.

41. Undersøgelsen viser endvidere, at Finanstilsynet løbende har overvåget, om virksomhederne har overholdt fristerne. De har desuden indhentet dokumentation for virksomhedernes tiltag, når fristerne udløb, og har haft dialog med virksomhederne om eventuelle fortsatte mangler i it-sikkerheden. I de tilfælde, hvor Finanstilsynet har vurderet, at virksomhedernes opfølgning på de enkelte påbud ikke var afsluttet eller ikke var tilstrækkelig til at sikre it-sikkerheden, har de forlænget virksomhedernes frist.

42. Undersøgelsen viser også, at de systemisk vigtige virksomheder, der har fået påbud, sjældent har efterlevet påbuddet inden for fristen, selv om virksomhederne selv har været med til at fastlægge fristerne. Således har de systemisk vigtige virksomheder i gennemsnit overskredet fristen med ca. 2 år.

Anvendelse af sanktioner

43. Vi har undersøgt, om Finanstilsynet har anvendt sanktioner over for virksomheder, der ikke har efterlevet lovkravene og/eller har overskredet fristerne for efterlevelse af påbud.

Hvis virksomheden ikke efterlever påbuddene, har Finanstilsynet flere sanktionsmuligheder. For det første kan de udstede administrative bødeforlæg. For det andet kan de anmelde virksomheden til politiet, som derefter kan idømme virksomheden en bødestraf for brud på lovgivningen.

44. Undersøgelsen viser, at Finanstilsynet ikke har udstedt administrative bødeforlæg til virksomheder, der overtræder reglerne for it-sikkerhed, eller som ikke efterlever Finanstilsynets påbud inden for fristen. Finanstilsynet har oplyst, at det skyldes, at bødesatserne ved administrative bødeforlæg er så små, at bøderne kun kan gives for overtrædelser, der kan karakteriseres som bagatelagtige, hvilket Finanstilsynet ikke vurderer er tilfældet, når det gælder påbud om forbedring af it-sikkerheden.

Bødeniveauet ved administrative bødeforlæg
Bødeniveauet er fastlagt i bemærkningerne til lov om finansiel virksomhed fra 2010. Her fremgår det, at en overtrædelse af loven som udgangspunkt vil udløse en bøde på 25.000 kr. første gang, som forhøjes med 50 % anden gang, 100 % tredje gang, 200 % fjerde gang osv. ved senere gentagelsestilfælde.

Undersøgelsen viser også, at Finanstilsynet heller ikke har anmeldt virksomheder, som ikke efterlevede påbuddene til politiet, selv om det fremgår af deres sanktionspolitik, at politianmeldelse bør overvejes ved manglende efterlevelse af påbud.

Finanstilsynet har oplyst, at det er deres generelle indtryk, at virksomhederne har givet påbuddene det rette fokus, og at Finanstilsynet derfor ikke har fundet, at der var grundlag for at politianmelde virksomheder. I de tilfælde, hvor Finanstilsynet kunne være i tvivl om, hvorvidt virksomhederne prioriterede opfølgningen på påbuddene, har de i stedet henledt virksomhedernes ledelse på problemerne.

Boks 4 viser et eksempel fra Finanstilsynets it-tilsyn med en systemisk vigtig virksomhed, hvor Finanstilsynet gentagne gange har konstateret brud på reglerne og overskridelse af fristerne, uden at det har ført til, at de har anvendt muligheden for at sanktionere virksomheden.

Boks 4

Eksempel på manglende sanktion ved fristoverskridelse

Under en inspektion i en systemisk vigtig virksomhed afdækkede Finanstilsynet, at den pågældende virksomhed havde mangelfuld styring af it-sikkerheden, og at virksomheden ikke havde fulgt op på påbuddene fra den forrige it-inspektion. Finanstilsynet gav derfor virksomheden en række påbud for mangelfuld styring af it-sikkerheden.

Pr. 31. december 2023 var hovedparten af virksomhedens påbud fortsat åbne og havde på dette tidspunkt overskredet Finanstilsynets frister med omtrent 2 år. Finanstilsynet har ikke anvendt deres mulighed for at sanktionere virksomheden.

Kilde: Finanstilsynets inspektionsrapporter og overblik over opfølgningen på påbud.

45. Rigsrevisionen anbefaler, at Finanstilsynet genovervejer deres praksis for anvendelse af sanktioner over for virksomheder, der ikke efterlever lovkravene til it-sikkerhed eller overskrider fristerne for efterlevelse af påbud.

Offentliggørelse af påbud

46. Vi har undersøgt, om Finanstilsynet har efterlevet kravene til at offentliggøre påbud til finansielle virksomheder. Desuden har vi undersøgt, om de oplysninger, Finanstilsynet og virksomhederne offentliggør, giver kunderne mulighed for at holde sig orienteret om it-sikkerhedsmæssige risici i deres bank.

Finanstilsynets forbrugeroplysende rolle

Ifølge § 333 a i lov om finansiel virksomhed skal Finanstilsynet fremme den offentlige forbrugerinformation.

Formålet er bl.a., at Finanstilsynet skal bidrage til at styrke forbrugernes viden, så de kan træffe hensigtsmæssige beslutninger og få en tillidsskabende oplevelse, når de møder den finansielle sektor.

47. Kravet om offentliggørelse af påbuddene skal ses i lyset af Finanstilsynets forbrugeroplysende rolle. Redegørelserne om inspektionerne skal ifølge Finanstilsynets retningslinjer bl.a. give eksisterende og potentielle kunder bedre indsigt i virksomhederne.

Både Finanstilsynet og de finansielle virksomheder har ifølge lov om finansiel virksomhed og lov om betalinger pligt til at offentliggøre tilsynsreaktioner, herunder bl.a. påbud, på deres hjemmesider, medmindre fx fortrolighedshensyn taler imod det. Det fremgår også, at virksomhederne kan fjerne oplysningerne fra deres hjemmeside efter 3 måneder. Dette gælder, uanset om virksomheden på det tidspunkt har rettet op på manglerne eller ej.

Reglerne for offentliggørelse fremgår af offentlighedsbekendtgørelsen, som er udstedt af erhvervsministeren. Heraf fremgår det, at Finanstilsynet efter hver inspektion skal udarbejde en redegørelse med de centrale påbud, og at det er denne redegørelse, Finanstilsynet og virksomheden skal offentliggøre. Samlet set er der altså krav om, at de påbud, Finanstilsynet udvælger som centrale påbud og derfor gengiver i redegørelsen, skal offentliggøres.

48. Undersøgelsen viser, at Finanstilsynet har offentliggjort alle redegørelserne for de gennemførte it-inspektioner i perioden 2017-2023. Da virksomhederne ifølge loven kan fjerne påbuddene efter 3 måneder, har det ikke været muligt at undersøge, om virksomhederne har offentliggjort alle de påbud, de har fået i hele perioden 2017-2023.

49. Undersøgelsen viser, at det ikke fremgår af de påbud, der er er gengivet i redegørelserne, hvilke konsekvenser den manglende it-sikkerhed kan få for virksomhedernes kunder, jf. eksemplet i boks 5.

Boks 5

Eksempel på påbud fra en inspektionsredegørelse vedrørende en systemisk vigtig virksomhed

Grundlæggende skal banken forbedre sin generelle styring af it-sikkerhed og it-risici. Banken skal bl.a. sikre, at forsvarslinjemodellen implementeres tilstrækkeligt i forhold til styring af it-risici. Banken skal også sikre, at kontrol- og sikringsforanstaltningerne til enhver tid modsvarer risiciene, og at bankens ledelse får et tilstrækkeligt og dokumenteret grundlag for at træffe beslutninger om bankens it-sikkerhed.

I forhold til outsourcing skal banken sikre, at de interne retningslinjer på alle områder stemmer overens med lovgivningens krav, og at de efterleves. På it-driftsområdet skal banken centralisere og forbedre sin styring af it-aktiver og etablere tilstrækkelig overvågning, særligt af privilegerede brugere. Desuden skal banken styrke sine krav til adgangsstyring og sikre, at kravene implementeres. Endelig skal banken forbedre sin it-beredskabsstyring. Målsætningerne for beredskabet skal basere sig på analyser af konsekvenserne af nedbrud for forretningen, og ledelsen skal være tilstrækkeligt informeret om målsætningerne. Der skal være klare krav til beredskabsplanernes indhold og til test heraf, så det sikres, at beredskabsmålsætningerne kan overholdes i praksis.

Kilde: Finanstilsynets redegørelse vedrørende en it-inspektion i en systemisk vigtig virksomhed.

Rigsrevisionen anbefaler, at Finanstilsynet overvejer at supplere påbuddene med en vurdering af, hvilke konsekvenser virksomhedernes utilstrækkelige it-sikkerhed kan have for kunderne, så de kan se det i de offentliggjorte redegørelser.

Kunderne kan også få oplysninger om risici i deres bank via de it-hændelser, virksomhederne indberetter til Finanstilsynet. Finanstilsynet har ifølge lov om finansiel virksomhed også mulighed for, efter høring i virksomhederne, at offentliggøre de it-hændelser, som virksomhederne indberetter, hvis Finanstilsynet vurderer, at offentlighedens kendskab hertil er nødvendig for at forebygge eller håndtere en igangværende hændelse. Virksomhederne har i perioden 2017-2023 indberettet 370 it-hændelser, der spænder fra midlertidige forsinkelser i betalinger til driftsforstyrrelse og angreb på servere og netværk. Finanstilsynet har oplyst, at de ikke har fundet det nødvendigt at offentliggøre nogen af it-hændelserne.

It-hændelse
En it-hændelse er en hændelse, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester. Det kan fx være, hvis en server går ned, eller hvis hackere får adgang til et netværk.

2.4. It-tilsynet i danske filialer af udenlandske banker

50. Vi har undersøgt, hvilke muligheder og pligter Finanstilsynet har i henhold til lov om finansiel virksomhed i forhold til at føre tilsyn med it-sikkerheden i danske filialer af udenlandske banker, som har en stor del af deres kritiske infrastruktur placeret i Danmark. Derudover har vi undersøgt, i hvilket omfang Finanstilsynet har ført tilsyn med it-sikkerheden. Vi har ikke vurderet, om tilsynet er tilstrækkeligt, da det ville kræve, at vi undersøgte tilsynsindsatsen over for den samlede koncern i alle involverede landes tilsynsmyndigheder, hvilket vi ikke har adgang til.

51. Lov om finansiel virksomhed sondrer mellem almindelige filialer og væsentlige filialer. Vi fokuserer i det følgende på tilsynet med de væsentlige filialer, da der ifølge Finanstilsynet ikke er nogen af de almindelige filialer, der har kritisk finansiel infrastruktur.

Væsentlige filialer
Finanstilsynet udpeger filialer som væsentlige, hvis filialen lever op til mindst ét af følgende kriterier:

1. Filialen har en markedsandel i form af indlån på mere end 2 % i Danmark.
2. Filialens balance udgør mere end 4 % af Danmarks BNP.

Finanstilsynet har udpeget 2 af de i alt 25 filialer af udenlandske banker i Danmark til at være væsentlige filialer. Den ene af de 2 banker med en væsentlig filial i Danmark har kritisk finansiel infrastruktur placeret i Danmark i form af et datacenter. Datacenteret understøtter hele bankens drift og styres fra bankens centrale it-organisation. Den anden af de 2 banker med en væsentlig filial i Danmark har indtil 2022 haft kritisk finansiel infrastruktur i Danmark, idet deres it-platform var outsourcet til en dansk fælles datacentral. Efter 2022 er filialen blevet tilknyttet bankens centrale it-platform, og banken har ikke længere kritisk finansiel infrastruktur i Danmark.

52. Tilsynet med væsentlige filialer af udenlandske banker er reguleret i lov om finansiel virksomhed. Lovbestemmelserne omhandler Finanstilsynets generelle tilsyn med væsentlige filialer, og der er ingen specifikke krav til Finanstilsynets tilsyn med it-sikkerheden.

Tilsynskollegier
Der skal i henhold til EU-reglerne etableres tilsynskollegier for de grænseoverskridende finansielle koncerner. Tilsynskollegierne består af de involverede tilsynsmyndigheder, som udveksler information og koordinerer tilsynsmæssige opgaver.

De væsentlige filialer, der hører under banker i andre EU-lande, skal overholde hjemlandets regler på it-området, og det er hjemlandets tilsynsmyndighed, der fører tilsyn med, om filialerne overholder reglerne. Finanstilsynet har dog pligt til at overvåge filialerne og bistå hjemlandets tilsynsmyndigheder i forbindelse med tilsynet af filialerne via deltagelse i tilsynskollegier. Derudover har Finanstilsynet mulighed for at foretage selvstændige inspektioner i de væsentlige filialer og i særligt hastende tilfælde iværksætte de nødvendige forholdsregler for at beskytte kundernes kollektive interesser mod finansiel ustabilitet.

Undersøgelsen viser, at Finanstilsynet for den ene væsentlige filial har overvåget it-sikkerheden og har bistået hjemlandets tilsyn via deltagelse i tilsynskollegiet og det underliggende kollegie, som fører tilsyn med it-området. I den forbindelse har Finanstilsynet gennemgået revisionsprotokollater, afholdt halvårlige it-statusmøder med filialen og løbende fulgt op på it-hændelser. Derudover har Finanstilsynet givet input til hjemlandets risikovurdering af koncernen og deltaget i tilsynskollegiets halvårsmøder med banken om it-risiko. Finanstilsynet har også haft mulighed for at deltage i it-inspektioner, der er foretaget af den Europæiske Centralbank, men har fravalgt denne mulighed på grund af manglende resurser.

For den anden væsentlige filial har Finanstilsynet også bistået hjemlandets tilsyn via deltagelse i tilsynskollegiet, hvor formålet bl.a. har været at drøfte hjemlandets risikovurdering af koncernens it-systemer. Med hensyn til den kritiske infrastruktur i Danmark har Finanstilsynet løbende ført tilsyn med den fælles datacentral, som filialens it-platform var outsourcet til frem til 2022.

Finanstilsynet har for ingen af de væsentlige filialer anvendt mulighederne for at foretage selvstændige inspektioner eller træffe specifikke forholdsregler, da de ikke er blevet bekendt med mangler i it-sikkerheden, som kunne begrunde det.

Rigsrevisionen, den 1. maj 2024

Birgitte Hansen

/Niels Kjøller Petersen

Bilag 1. Statsrevisorernes anmodning

Statsrevisorernes spørgsmål	Her besvares spørgsmålet
Hvor mange it-tilsyn og it-inspektioner af finansielle virksomheder har Finanstilsynet gennemført i perioden 2017-2022?	Afsnit 2.2
Hvor mange og hvilke påbud har Finanstilsynet udstedt i den forbindelse, og hvilken virkning har de haft?	Afsnit 2.3
Hvilke muligheder har Finanstilsynet for at føre tilsyn med banker i Danmark, som har adresse/hovedsæde i andre lande, men hvor en stor del af deres kritiske finansielle infrastruktur er placeret i Danmark?	Afsnit 2.4
Har Finanstilsynets it-tilsyn og inspektioner været tilfredsstillende i perioden, bl.a. i forhold til tilsynsfrekvens, rammer for tilsynet, risici og lovens hovedformål?	Afsnit 2.1, 2.2 og 2.3
Hvilke muligheder har kunderne for at blive orienteret om eventuelle it-sikkerhedsmæssige risici og påbud fra Finanstilsynet i deres pengeinstitut?	Afsnit 2.3

Bilag 2. Metodisk tilgang

Undersøgelsen baserer sig på gennemgang af lovgrundlaget, skriftligt materiale fra Finanstilsynet samt på en gennemgang af tilsynsmateriale fra Finanstilsynets it-inspektioner. Vi har derudover gennemgået den europæiske banktilsynsmyndigheds retningslinjer vedrørende tilsynet med virksomhedernes styring af it-sikkerhed. Endelig har vi holdt møder med Finanstilsynet for at understøtte analysen.

Væsentlige dokumenter

Vi har gennemgået en række dokumenter, herunder:

- Lov om finansiel virksomhed (lovbekendtgørelse nr. 406 af 29. marts 2022).
- Lov om betalinger (lovbekendtgørelse nr. 53 af 18. januar 2023).
- Lov om kapitalmarkeder (lovbekendtgørelse nr. 41 af 13. januar 2023).
- Bekendtgørelse af ledelse og styring af pengeinstitutter m.fl. (bekendtgørelse nr. 1103 af 30. juni 2022).
- Bekendtgørelse om outsourcing af kreditinstitutter m.v. (bekendtgørelse nr. 973 af 22. juni 2022).
- Bekendtgørelse om systemrevisionens gennemførelse i fælles datacentraler m.fl. (bekendtgørelse nr. 1581 af 22. december 2022).
- Bekendtgørelse om finansielle virksomheders pligt til at offentliggøre Finanstilsynets vurdering af virksomheden (bekendtgørelse nr. 857 af 14. juni 2022).
- Europa-Parlamentets og Rådets Forordning nr. 909/2014 af 23. juli 2014 om værdipapircentraler m.v. (CSDR).
- Den europæiske banktilsynsmyndigheds retningslinjer for fælles procedurer og metoder for tilsynskontrol- og vurderingsprocessen (SREP) (EBA/GL/2014/13) samt den europæiske banktilsynsmyndigheds retningslinjer for IKT-risikovurdering under tilsynskontrol- og vurderingsprocessen (SREP) (EBA/GL/2017/05).
- Finanstilsynets politik for it-tilsyn og Finanstilsynets samlede risikobilleder 2018-2023.
- Finanstilsynets retningslinjer for planlægning af inspektioner.
- Finanstilsynets årlige notater med it-inspektionsplaner for systemisk vigtige virksomheder.
- Finanstilsynets årlige overordnede risikovurderinger af systemisk vigtige virksomheder 2017-2018.
- Finanstilsynets særskilte it-risikovurderinger for systemisk vigtige virksomheder for perioden 2019-2023.
- Eksempler på den dokumentation, de finansielle virksomheder skal sende til Finanstilsynet som led i tilsynet med it-sikkerheden. Dette inkluderer virksomhedernes egne vurderinger af risici (ICAAP-rapporter), eksterne systemrevisionsprotokollater for datacentralerne og materiale fra halvårlige statusmøder med systemisk vigtige virksomheder.
- Alle inspektionsrapporter for it-inspektioner i systemisk vigtige virksomheder og de indkaldelsesbreve, Finanstilsynet har sendt til virksomhederne forud for inspektionerne.
- Alle inspektionsrapporter for inspektioner i øvrige virksomheder i de tilfælde, hvor it-området i virksomheden var blevet inspiceret.
- Risikovurderingerne for de øvrige virksomheder, som Finanstilsynet har inspiceret i perioden 2017-2023, uanset om it-området er inspiceret eller ej.

- Finanstilsynets retningslinjer vedrørende sanktioner og offentliggørelse af inspektionsredegørelser og påbud.
- Finanstilsynets overvågning af virksomhedernes efterlevelse af påbud.
- Inspektionsredegørelser på Finanstilsynets hjemmeside.
- Finanstilsynets samarbejdsaftaler med udenlandske tilsynsmyndigheder vedrørende de væsentlige filialer under kreditinstitutter i Danmark samt eksempler på virksomhedernes statusrapporter og Finanstilsynets referater i forbindelse med overvågning af filialerne.
- Finanstilsynets materiale vedrørende overvågning af virksomhedernes indberetning af it-hændelser.

Formålet med gennemgangen af dokumenterne har været at skabe klarhed om regler og retningslinjer samt undersøge, om Finanstilsynet via retningslinjer og risikovurderinger har sikret et grundlag for, at tilsynsindsatsen rettes mod væsentlige og risikofyldte virksomheder. Vi har gennemgået inspektionsmaterialet for at kortlægge, hvornår de forskellige virksomheder er blevet inspiceret, hvilke it-sikkerhedsområder inspektionerne dækkede, samt hvilke påbud og deadlines for efterlevelse Finanstilsynet har udstedt i forbindelse med inspektionerne. Vi har desuden gennemgået Finanstilsynets retningslinjer for sanktioner og offentliggørelse for at vurdere, om deres opfølgning har sikret, at tilsynet fik størst mulig virkning.

Udvælgelsen af tilsynsaktiviteter, der indgår i undersøgelsen

I vores besvarelse af Statsrevisorernes spørgsmål om, hvorvidt tilsynet er tilfredsstillende i forhold til risici, fokuserer vi på Finanstilsynets risikovurderinger, inspektioner og opfølgning på de påbud, de giver til virksomhederne. De andre aktiviteter, som Finanstilsynet foretager i forbindelse med deres it-tilsyn, fx overvågning af indberetninger om it-hændelser, gennemgang af revisionserklæringer fra virksomhederne og møder med virksomhederne om opfølgningen på påbud, indgår indirekte i undersøgelsen, da Finanstilsynet bruger aktiviteterne til at udarbejde risikovurderinger og til at understøtte, at virksomhederne efterlever påbuddene.

Udvælgelsen af virksomhedstyper, der indgår i undersøgelsen

Undersøgelsen er afgrænset, så vi undersøger it-tilsynet med alle systemisk vigtige virksomheder. Derudover inkluderer undersøgelsen it-tilsynet med alle de virksomheder, der enten er omfattet af bilag 5 til bekendtgørelsen om ledelse og styring af pengeinstitutter m.fl., som er udstedt i medfør af lov om finansiel virksomhed. Det er dette lovgrundlag, Statsrevisorerne henviser til i deres anmodning. Derudover indgår virksomheder, der er omfattet af lov om betalinger, lov om kapitalmarkeder eller af EU-forordningen om værdipapircentraler.

Udvælgelsesmetoden skal sikre, at it-tilsynet med alle de vigtigste finansielle virksomheder behandles i undersøgelsen, og at alle øvrige virksomheder af samme typer også inkluderes. Udvælgelsesmetoden tillader os for det første at belyse forskelle i it-tilsynet mellem systemisk vigtige virksomheder og de øvrige virksomheder. For det andet inkluderer undersøgelsen dermed alle typer virksomheder, som er underlagt den lovgivning, der fremgår af Statsrevisorernes anmodning. Vores kriterier for udvælgelse af virksomhedstyper medfører, at pensions- og forsikringsselskaber ikke indgår i undersøgelsen, da ingen af dem er udpeget som systemisk vigtige, og de heller ikke er omfattet af bilag 5 til bekendtgørelsen om ledelse og styring af pengeinstitutter.

Vi opererer i undersøgelsen med 2 forskellige virksomhedspopulationer: systemisk vigtige virksomheder og øvrige virksomheder. Nogle af virksomhederne er i løbet af perioden blevet udpeget som systemisk vigtige. Alle inspektioner i virksomhederne samt de eventuelle påbud, der er givet til virksomhederne, indgår i den population, som virksomheden tilhørte på tidspunktet for inspektionen eller for tildelingen af påbud.

Metode og grundlag for vores vurderinger af Finanstilsynets tilrettelæggelse, gennemførelse og opfølgning på it-tilsynet

Finanstilsynets tilrettelæggelse af it-tilsynet
Vi har gennemgået Finanstilsynets politik for it-tilsynet for at vurdere, om deres tilrettelæggelse af tilsynet tager højde for virksomhedernes væsentlighed og opstiller målsætninger, der understøtter, at der kan føres mest tilsyn med de væsentligste virksomheder. Vi har derudover gennemgået Finanstilsynets redegørelser for, hvilke principper der afgør, om virksomheder udpeges som systemisk vigtige i forhold til tilsynet med it-sikkerhed, samt gennemgået de årlige notater for planlægningen af it-inspektioner i systemisk vigtige virksomheder for at se, om Finanstilsynet løbende har opdateret deres klassificering af systemisk vigtige virksomheder.

Finanstilsynet bør ifølge den europæiske banktilsynsmyndighed vurdere risici på it-området som et led i at vurdere virksomhedernes overordnede, operationelle risiko med henblik på at tilpasse tilsynsaktiviteten. Dette gælder både for de systemisk vigtige virksomheder og for øvrige virksomheder. Den europæiske banktilsynsmyndighed anbefaler, at virksomhedernes risici vurderes særskilt i de tilfælde, hvor tilsynsmyndigheden vurderer, at it-området kan udgøre en væsentlig risiko for virksomheden. Vi lægger derfor til grund, at denne anbefaling gælder for de virksomheder, Finanstilsynet vurderer som systemisk vigtige. Derfor har vi undersøgt, om Finanstilsynet har udarbejdet særskilte it-risikovurderinger for de systemisk vigtige virksomheder.

Den europæiske banktilsynsmyndighed forudsætter ikke, at it-risici skal vurderes særskilt for virksomheder, der ikke er systemisk vigtige. Vi forventer derfor ikke, at Finanstilsynet har udarbejdet særskilte it-risikovurderinger for de øvrige virksomheder, og undersøger i stedet, om Finanstilsynet som et led i deres samlede risikovurdering på systematisk vis også har vurderet virksomhedernes it-sikkerhed.

For de systemisk vigtige virksomheder gennemgår vi derudover Finanstilsynets retningslinjer for tilrettelæggelse af inspektioner samt deres notater med it-inspektionsplaner for at se, om de anvender risikovurderinger af it-området i virksomhederne til at tilrettelægge inspektioner og inspektionsfrekvens.

Finanstilsynets gennemførelse af it-tilsynet

Systemisk vigtige virksomheder

I vores undersøgelse af gennemførelsen af inspektioner har vi har anvendt inspektionsrapporter fra Finanstilsynet til at opgøre datoerne for, hvornår Finanstilsynet har udført inspektionerne i virksomhederne, og hvornår inspektionerne efterfølgende er afsluttet. Vi har også anvendt inspektionsrapporterne til at opgøre, hvornår virksomheden modtager en rapport med eventuelle påbud. I opgørelsen af antallet af it-inspektioner i systemisk vigtige virksomheder tæller vi de inspektioner, der er afsluttet med en rapport i perioden 1. januar 2017 - 31. december 2023. Vi bruger derudover inspektionsrapporterne til at opgøre, hvilke it-områder Finanstilsynet har dækket med inspektionerne. I Finanstilsynets seneste it-risikovurderinger fremgår der for hver virksomhed en vurdering af risikoen på alle de 7 it-områder, som Finanstilsynet inddeler deres it-inspektioner i. Vi har brugt disse risikovurderinger af it-områderne til at undersøge, om Finanstilsynet efterfølgende har gennemført inspektioner på de mest risikofyldte it-områder.

Overholdelse af minimumsfrekvensen og tidsintervallet mellem inspektioner i systemisk vigtige virksomheder

Da det ikke fremgår af Finanstilsynets retningslinjer, hvordan overholdelsen af minimumfrekvensen skal opgøres, tager vores beregninger udgangspunkt i den metode, som Finanstilsynet har oplyst, at de selv anvender. Vi beregner derfor intervallet mellem 2 inspektioner ved at tælle antallet af dage fra dateringen på den afsluttende rapport fra inspektion nr. 1 til dateringen på indkaldelsesbrevet, som Finanstilsynet sender til virksomheden forud for inspektion nr. 2. Hvis intervallet mellem 2 inspektioner efter denne beregning overstiger 1.460 dage, svarende til 4 år, har vi vurderet, at minimumsfrekvensen har været overskredet for den pågældende virksomhed.

For de virksomheder, der er blevet udpeget som systemisk vigtige i løbet af perioden, har vi derfor beregnet intervallet fra tidspunktet for udpegning som systemisk vigtig til dateringen for indkaldelsesbrevet til første it-inspektion efter udpegningen. Hvis Finanstilsynet har sendt et indkaldelsesbrev til it-inspektion mindre end 4 år efter udpegningen af virksomheden som systemisk vigtig, vurderer vi, at minimumsfrekvensen er overholdt. Hvis det er mindre end 4 år siden, at virksomheden er blevet udpeget som systemisk vigtig, og Finanstilsynet endnu ikke har afsluttet en it-inspektion, kan vi ikke vurdere, om minimumsfrekvensen er overholdt.

Ud over opgørelsen af Finanstilsynets overholdelse af minimumsfrekvensen har vi også beregnet, hvor lang tid der går mellem, at Finanstilsynet er til stede i virksomhederne og udfører it-inspektioner. Vi har valgt dette tidspunkt for, hvornår Finanstilsynet udfører inspektionen af 2 årsager. For det første, fordi det er det tidspunkt, hvor Finanstilsynet får detaljeret viden om virksomhedens regelefterlevelse. For det andet er tidspunktet valgt ud fra et ønske om sammenlignelighed mellem inspektioner. Det skyldes, at der er meget stor forskel fra inspektion til inspektion i forhold til, hvor lang tid der går, fra Finanstilsynet sender indkaldelsesbrevet til virksomheden og derefter udfører inspektionen, og derudover også stor forskel på, hvor lang tid der går fra selve udførelsen af inspektionen, til Finanstilsynet afslutter inspektionen med en rapport til virksomheden.

It-inspektioner af it-sikkerhed i øvrige virksomheder
Vi har gennemgået alle inspektionsrapporter for virksomheder, hvor inspektionen er afsluttet og afrapporteret i perioden 1. januar 2017 - 31. december 2023, for at opgøre, hvor mange inspektioner af it-området Finanstilsynet har gennemført. Vi har sammenholdt inspektionerne med Finanstilsynets lister over aktive finansielle virksomheder pr. 31. december 2023 for at opgøre, hvor stor en andel af disse virksomheder, Finanstilsynet har inspiceret it-sikkerheden i, og hvilke typer virksomheder der er tale om.

For bankerne, hvor Finanstilsynet siden 2020 har risikovurderet it-sikkerheden, har vi for hver inspektion også gennemgået tilhørende risikovurderinger. Det gælder både inspektioner, hvor it-området har været undersøgt som led i inspektionen, og inspektioner, hvor Finanstilsynet har fravalgt at undersøge it-området. Vi har brugt risikovurderingerne til at se, om Finanstilsynet i højere grad har inkluderet it-området i inspektioner, når virksomhedernes risiko på it-området var høj.

Finanstilsynets opfølgning på it-tilsynet
Vi har gennemgået lov om finansiel virksomhed, lov om betalinger, bekendtgørelse om Finanstilsynets pligt til at offentliggøre Finanstilsynets vurdering af virksomheden, Finanstilsynets sanktionspolitik og deres forretningsgang vedrørende afslutning af inspektioner. Formålet har været at redegøre for Finanstilsynets hjemmel til og retningslinjer i forbindelse med at sanktionere, herunder give påbud til virksomheder, der har utilstrækkelig it-sikkerhed, og bøder til virksomheder, der ikke efterlever påbuddene, og deres retningslinjer for at offentliggøre påbud. Denne del bygger også på redegørelser fra og møder med Finanstilsynet for at få indsigt i deres praksis.

Vi har gennemgået alle rapporter for it-inspektioner i systemisk vigtige virksomheder, og alle rapporter for inspektioner i de øvrige virksomheder, hvor it-området er blevet undersøgt. Finanstilsynets påbud til virksomhederne fremgår af rapporterne, og vi har på den baggrund opgjort antallet af påbud til virksomhederne samt andelen af virksomheder, der har fået påbud for henholdsvis systemisk vigtige og øvrige virksomheder. Vi har desuden opgjort, hvilke it-områder påbuddene vedrører.

I inspektionsrapporten sætter Finanstilsynet i samarbejde med virksomhederne en frist for, hvornår virksomhederne skal efterleve påbuddene. Finanstilsynet har derudover oplyst os datoerne for, hvornår de har vurderet, at de enkelte påbud var efterlevet af virksomhederne. Disse oplysninger har vi sammen med fristerne fra rapporterne brugt til at beregne andelen af virksomheder, som har efterlevet påbuddene inden for fristen, og hvor meget virksomhedernes frist for efterlevelse af påbud i gennemsnit er blevet overskredet.

Vi har desuden kontrolleret, om de redegørelser, Finanstilsynet har sendt til de inspicerede virksomheder fra 2017 til 2023 var tilgængelige på Finanstilsynets hjemmeside.

It-tilsynet i danske filialer af udenlandske banker
Vi har gennemgået lov om finansiel virksomhed for at kortlægge Finanstilsynets muligheder og pligter i forhold til at føre tilsyn med it-sikkerheden i de udenlandske bankers danske filialer, der har en stor del af deres kritiske infrastruktur placeret i Danmark. Desuden har vi holdt møder med og indhentet redegørelser fra Finanstilsynet for deres praksis med tilsynet over for filialer samt indhentet og gennemgået dokumentation for det førte tilsyn med it-sikkerheden i væsentlige filialer.

Kvalitetssikring

Undersøgelsen er kvalitetssikret via vores interne procedurer for kvalitetssikring, som omfatter høring hos den reviderede samt ledelsesbehandling og sparring med chefer og medarbejdere i Rigsrevisionen.

Standarderne for offentlig revision

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

Bilag 3. De finansielle virksomheder, der indgår i undersøgelsen

Tabel A
De finansielle virksomheder

Virksomhedstype	Navn	
Realkreditinstitutter og andre kreditinstitutter	DLR Kredit	Nordea Kredit
	Nykredit Realkredit-koncernen (herunder Totalkredit og Nykredit Bank)	Danmarks Skibskredit[1)]
	KommuneKredit	
Pengeinstitutter (banker, sparekasser og andelskasser)	Andelskassen Fælleskassen	Arbejdernes Landsbank (herunder Vestjysk Bank)
	Borbjerg Sparekasse	Borgervennen af 1788
	Coop Bank	Danske Andelskassers Bank
	Danske Bank-koncernen (herunder Realkredit Danmark)	Djurslands Bank
	Dragsholm Sparekasse	Ekspres Bank[1)]
	Facit Bank	Faster Andelskasse
	Frørup Andelskasse	Frøslev-Mollerup Sparekasse
	Fynske Bank	Grønlandsbanken
	Hvidbjerg Bank	Jyske Bank-koncernen (herunder Jyske Realkredit)
	Klim Sparekasse	Kompasbank[1)]
	Kreditbanken	Leasing Fyn Bank[1)]
	Lollands Bank	Lunar Bank[1)]
	Lægernes Bank	Lån & Spar Bank
	Maj Bank	Merkur Andelskasse
	Middelfart Sparekasse	Møns Bank
	Nordfyns Bank	Nordoya Sparikassi
	P/F BankNordik	P/F Betri Banki
	PenSam Bank	PFA Bank
	Ringkjøbing Landbobank	Rise Sparekasse
	Rønde Sparekasse	Saxo Bank
	Skjern Bank	Spar Nord Bank
	Sparekassen Balling	Sparekassen Bredebro
	Sparekassen Danmark	Sparekassen Djursland
	Sparekassen for Nørre Nebel og Omegn	Sparekassen Kronjylland
	Sparekassen Sjælland-Fyn	Sparekassen Thy
	Stadil Sparekasse	Suduroyar Sparikassi P/F
	Sydbank	Sydjysk Sparekasse
	Sønderhå-Hørsted Sparekasse	

Tabel A (fortsat)

De finansielle virksomheder

Virksomhedstype	Navn	
E-penge- og betalingsinstitutter	4T AF 1. OKTOBER 2012	Aiia
	AMC-CONSULT	Billy
	Capuchin	Cardlay
	Clearhaus	Coop Betalinger
	Flex Funding	Forbrugsforeningen af 1886
	Inpay	Januar
	Kameo	Kontolink
	Loomis Danmark	LOYAL SOLUTIONS
	Mastercard Payment Services[2)]	Mazepay
	Monthio	Nets Denmark
	Nordea Finans Danmark	November First,
	PayProff	Pleo Financial Services
	Safenetpay	Secure Payment
	Subaio	SymblePay
	Xero Denmark	Ziglu Europe
	ZTLment	
Investeringsforvaltningsselskaber	BI Management	Danske Invest Management
	Formuepleje	Fundmarket
	Handelsinvest Investeringsforvaltning	Invest Administration
	Investeringsforvaltningsselskabet SEBinvest	Jyske Invest Fund Management
	Nykredit Porteføljе Administration	PFA Asset Management
	Syd Fund Management	Tiedemann Independent
Fælles datacentraler	BEC Financial Technologies	E-nettet
	Foreningen Bankdata	Gensam Data
	JN Data	SDC
	P/F Elektron	
It-operatører af detailbetalingssystemer	Mastercard Payment Services[2)]	
Værdipapircentraler	VP Securities	
Markedspladser	Nasdaq Copenhagen	

[1)] Penge eller kreditinstituttet er ikke tilknyttet en datacentral.

[2)] Mastercard Payment Services er både en udbyder af betalingstjenester og en it-operatører af detailbetalingssystemer og indgår derfor 2 steder i tabellen. Men er kun talt med som én virksomhed samlet i total.

Kilde: Rigsrevisionen på baggrund af oplysninger fra Finanstilsynet.