FINANSTILSYNET

Finanstilsynet

20. november 2019

J.nr. 6941-0008

Redegørelse om IT-inspektion i Danske Bank A/S

1. Indledning

Finanstilsynet har gennemført en IT-inspektion i Danske Bank A/S ultimo 2018 og primo 2019. Inspektionen blev gennemført i samarbejde med en række af de udenlandske tilsynsmyndigheder, som fører tilsyn med Danske Banks udenlandske datterselskaber og filialer. Inspektionen omfattede følgende områder:

- Styring af IT-sikkerhed og -risici, herunder sikkerhedspolitikken
- Outsourcing
- IT-driftsafvikling og -udvikling
- Adgangsstyring
- Beredskabsplanlægning og cyberrobusthed
- Systemrevision

2. Sammenfatning

Finanstilsynet vurderer, at Danske Bank A/S (herefter banken) har væsentlige svagheder i sin styring af IT-sikkerhed og -risici. Banken har desuden ikke fulgt tilstrækkeligt op på påbuddene fra den seneste IT-inspektion i 2015. Disse forhold medfører forhøjet IT-risiko i banken.

På baggrund af inspektionen har Finanstilsynet givet banken en række påbud.

Grundlæggende skal banken forbedre sin generelle styring af IT-sikkerhed og -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.

Derudover skal en række specifikke områder styrkes. I forhold til outsourcing skal banken sikre, at de interne retningslinjer på alle områder stemmer overens med lovgivningens krav, og at de interne retningslinjer efterleves i

praksis. 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.

Svaghederne er samlet set på niveau med, hvad Finanstilsynet har fundet i IT-inspektioner i andre større pengeinstitutter og datacentraler de senere år, dog er der variationer på de forskellige områder.

Finanstilsynet har i samarbejde med de øvrige tilsynsmyndigheder, som fører tilsyn med banken, vurderet, at inspektionen giver anledning til, at søjle II-tillægget til solvensbehovet skal øges med minimum 2 mia. kr. for at tage højde for den forhøjede IT-risiko. Det har banken gjort pr. 3. kvartal 2019.