

Pressemeddelelse

Jyske Bank A/S
Vestergade 8-16
8600 Silkeborg
Telefon 89 89 89 89
www.jyskebank.dk
E-mail: jyskebank@jyskebank.dk
CVR-nr. 17616617

6. juli 2017

Finanstilsynets redegørelse om IT-inspektion

Bankdirektør Leif Larsen udtaler i denne forbindelse:

”Vi har noteret os Finanstilsynets konklusioner på deres 2016-inspektion, som banken i flere tilfælde allerede har taget hånd om.

Det er betryggende, at inspektionen ikke konstaterede alvorlige brister i Jyske Banks faktuelle IT-sikkerhed, idet Finanstilsynets kritiske bemærkninger primært påpeger behovet for en øget formalisering og kontrol i forbindelser med bankens identifikation, vurdering og rapportering af IT-sikkerhedsmæssige risici. Vi anerkender, at korrekt håndtering af de påpegede forhold, herunder en professionalisering af samarbejdet med outsourcingpartnere, vil være med til at sikre, at Jyske Bank altid opretholder et højt IT-sikkerhedsmæssigt niveau, hvilket har bankens allerhøjeste prioritet”.

Venlig hilsen

Jyske Bank

Kontaktperson: Bankdirektør Leif F. Larsen, telefon 89 89 20 05

Redegørelse om IT-inspektion i Jyske Bank A/S

1. Indledning

Finanstilsynet gennemførte i løbet af 2016 en IT-inspektion hos Jyske Bank A/S.

Finanstilsynet gennemgik udvalgte dele af IT-området, herunder den generelle IT-sikkerhedsstyring, IT-strategi, organisation, beredskabsplaner, sikkerhedspolitikker og retningslinjer. Endvidere gennemgik Finanstilsynet Jyske Banks procedurer for styring af adgange til systemer og data, ændringshåndtering, systemrevision, kontrol med outsourcete IT-funktioner samt krav og procedurer til kontrol og rapportering.

2. Sammenfatning og risikovurdering

Det er Finanstilsynets vurdering, at Jyske Bank ikke har etableret tilstrækkelig styring og rapportering på IT-sikkerhedsområdet. Dette har medført risiko for, at direktionen og bestyrelsen ikke i tilstrækkeligt omfang er bekendte med det reelle IT-risikobillede. Det er også Finanstilsynets vurdering, at Jyske Bank ikke fuldt ud efterlever lovgivningens krav på IT-området, herunder i relation til bankens outsourcing af væsentlige IT-aktiviteter.

Finanstilsynet har påbudt Jyske Bank at styrke IT-sikkerhedsstyringen og ledelsesrapporteringen samt at forbedre den løbende kontrol og opfølgning med den faktiske IT-sikkerhedsimplementering både i banken og hos IT-leverandørerne. Endvidere skal ledelsens krav og forventninger til IT-sikkerhedsarbejdet mv. i højere grad præciseres og dokumenteres.

Finanstilsynet har endvidere påbudt Jyske Bank at etablere en tilstrækkelig metode for IT-risikostyring dækkende både banken og opgaveløsningen hos de IT-leverandører, der outsources til. Der skal bl.a. etableres en bedre dokumentation af sammenhængen mellem IT-risici og de imødegående kontrol-

og sikringsforanstaltninger, der danner grundlag for bankens IT-sikkerhedsstyring. Endvidere skal Jyske Bank sikre, at der er etableret tilstrækkelige krav til roller og ansvarsplacering i IT-risikoarbejdet.

Jyske Bank er ligeledes blevet påbudt at sikre, at bankens interne forretningsgange og krav i henhold til bekendtgørelsen om outsourcing af væsentlige aktivitetsområder bliver tilstrækkeligt efterlevet.

Finanstilsynet har endvidere påbudt Jyske Bank at forbedre krav til ændringsstyring, herunder tilstrækkelig opfølgning og kontrol med ændringer til produktionssystemerne, funktionsadskillelse samt adgange til fortrolige data.

Jyske Bank er blevet påbudt at sikre, at der udarbejdes tilstrækkelige risiko- og konsekvensvurderinger som grundlag for beredskabsmålsætninger og beredskabsplaner. Endvidere skal Jyske Bank forbedre krav og forretningsgange til beredskabskoordineringen i banken og hos væsentlige outsourcing-leverandører. Forretningsgange og krav til test af beredskabsplaner skal styrkes, og det skal endvidere sikres, at beredskabsplaner og relevante test-scenarier bliver tilstrækkeligt testet.

Finanstilsynet har ligeledes påbudt Jyske Bank at forbedre adgangs- og rettighedsstyringen til systemer og data. Samtidigt skal det sikres, at der er etableret tilstrækkelige krav til IT-sikkerhedslogning med afsæt i en risikobaseret tilgang.