*Translation from Danish by Danske Bank of a statement dated 20 November 2019 from the Danish Financial Supervisory Authority (*Finanstilsynet*). In case of discrepancies, the Danish version prevails.*

The Danish Financial Supervisory Authority
20 November 2019
File no. 6941-0008

Statement on IT inspection at Danske Bank A/S

1. Introduction

The Danish Financial Supervisory Authority (the FSA) conducted an IT inspection at Danske Bank A/S at the end of 2018 and at the beginning of 2019. The inspection was carried out in cooperation with a number of the foreign supervisory authorities that supervise Danske Bank's foreign subsidiaries and branches. The inspection covered the following areas:

- Management of IT security and IT risks, including security policy
- Outsourcing
- IT operations and development
- Access management
- Contingency management and cyber resilience
- System audit

2. Summary

The FSA assesses that Danske Bank A/S (the bank) has significant weaknesses in its management of IT security and IT risks. Furthermore, the bank has failed to sufficiently follow up on the orders issued after the IT inspection in 2015. These issues have resulted in an elevated IT risk at the bank.

On the basis of its inspection, the FSA has issued a number of orders to the bank.

Fundamentally, the bank must improve its general management of IT security and IT risks. For example, the bank must ensure that the lines-of-defence model is adequately implemented in relation to the management of IT risks. The bank must also ensure that its control and security measures match risks at all times and that the bank's management has a sufficient and documented basis for making decisions about the bank's IT security.

In addition, a number of specific areas must be strengthened. In terms of outsourcing, the bank must ensure that the internal guidelines in all areas meet the statutory requirements and that they are followed in practice. As regards IT operations, the bank must centralise and strengthen its management of IT assets and implement adequate monitoring, especially in relation to privileged users. The bank must also strengthen its access management requirements and ensure that the requirements are implemented. Finally, the bank must improve its IT contingency management. The objectives of the contingency planning must be based on analyses of the consequences of breakdown for the business, and management must be sufficiently informed of the objectives. The requirements for the contents of the contingency plans and their testing must be clear to ensure that the objectives of the contingency planning can be fulfilled in practice.

On balance, the weaknesses correspond to what has been uncovered by the FSA in its inspections at other large banks and data centres in recent years, although there are differences in the various areas.

In cooperation with the other supervisory authorities that supervise the bank, the FSA has assessed that the inspection gives rise to an additional Pillar II add-on of a minimum of DKK 2 billion to the bank's solvency need to allow for the elevated IT risk. Danske Bank increased its Pillar II add-on as of the third quarter of 2019.