THE DANISH FINANCIAL SUPERVISORY AUTHORITY

MEMORANDUM 15 August 2016

Statement on IT inspection at Sydbank

1. Introduction

In the latter half of 2015 the Danish Financial Supervisory Authority (FSA) conducted a functional inspection of the IT area at Sydbank.

The FSA reviewed selected parts of the IT area, including general IT security management, IT strategy, organisation, contingency plans, security policies and guidelines. In addition the FSA reviewed Sydbank's procedures for managing access to systems and data, systems audit, control of outsourced IT functions as well as control and reporting requirements and procedures.

2. Summary and risk assessment

It is the FSA's assessment that Sydbank is making a focused effort to strengthen and develop business procedures and processes in relation to general IT security management, including lifting the overall IT security level. Moreover the FSA assesses that Sydbank has presented a good understanding of IT risks and a good security culture to the FSA. In several areas the bank has established improved IT security measures and set up the overall framework for IT security management. In the FSA's assessment, however, Sydbank still needs to strengthen and implement several of the planned and presented improvement measures in relation to IT security management and the bank must retain focus on improving IT security and risk management.

The FSA has ordered Sydbank to improve the method for IT risk management and to provide better documentation of the correlation between IT risks and established control and security measures.

In addition the FSA has ordered Sydbank to strengthen procedures and business procedures regarding IT security management, including to arrange for documented follow-up and monitoring of the implementation of IT security policies, business procedures and controls, and to include and present the results in management reporting.

The FSA has also ordered Sydbank to establish documented requirements, follow-up and control of outsourcing suppliers and to ensure to a greater extent that outsourcing suppliers comply with Sydbank's requirements and expectations in relation to IT security as well as to contingency planning. Furthermore IT risks of suppliers must be identified to a higher degree and must form part of Sydbank's overall IT security management and management reporting.

Moreover the FSA has ordered Sydbank to elaborate on and document central elements of the IT contingency plan as well as to strengthen documentation and requirements in relation to test planning and identification of relevant test activities.

The FSA has ordered Sydbank to improve the management of access to systems and data. For example the bank must ensure a sufficient overview of assigned authorisations and adequate supervision of the use of access as well as ensure that critical access and critical combinations of authorisations are documented and assessed in terms of risk. Finally the FSA has ordered Sydbank to ensure that adequate requirements for IT security logging and monitoring are defined on the basis of a risk assessment.