Executive Order No. 710 of 8 July 2019 (Current)	Printing date: 9 July 2019
Ministry: Ministry of Industry, Business and Financial Affairs Reference number.: Min. of Ind., Bus. and Fin. Affairs, The Danish Financial Supervisory Authority, ref. no. 1912-0033	**Subsequent amendments to the regulation** None

Executive Order on the amendment of the Executive Order on Management and Control of Banks, etc.

Part 1

The following changes are made to Executive Order no. 1026 of 30 June 2016 on the management and Control of Banks, etc., as amended by Executive Order No. 461 of 9 May 2018:

1. The introduction to the *Executive Order* is worded as follows:
'Pursuant to Section 65 (2), Section 70 (7), Section 71 (3), Section 152 (2), and Section 373 (4) of the Financial Business Act, cf. Consolidated Act no. 457 of 24 April 2019, as amended by Act No. 552 of 7 May 2019, and Section 21 and Sections 39 (3) of the Danish Act on mortgage credit loans and mortgage credit bonds, etc., cf. Consolidated Act no. 1188 of 19 September 2018, the following is established:'

2. *Section 4 (2), no. 6,* is worded as follows:
'6) IT security policy and IT risk management policy, cf. Appendix 5.'

3. *Appendix 5* is worded as Appendix 1 to this Executive Order.

Part 2

This Executive Order enters into force on 1 September 2019.

The Danish Financial Supervisory Authority, 8 July 2019

J*esper* B*erg*

/ Anders Kragsnæs Balling

Appendix 1

'Appendix 5

Scope and definitions

1) This appendix contains provisions on the matters covered by the Executive Order relating the IT area, including IT security management.

Tasks and responsibilities of the Board of Directors

2) Based on a risk assessment, the Board of Directors must decide on an IT security policy for the company.

3) The IT security policy must, based on the desired risk profile in the IT area, contain an overall assessment of all essential matters concerning IT security. What is essential depends, among other things, on the size of the company and the extent and complexity of the company's IT use.

The following factors must be considered, taking into account the size, complexity, business model and business scope of the company:

a) Organisation of the IT work, including separation of functions between

- system development/maintenance
- IT operations and
- the business management of the company.

b) Regular risk assessments.
c) Protection of systems, data, hardware and communication paths.
d) System development and maintenance of systems.
e) Operating performance.
f) Logging and monitoring.
g) Separation of functions.
h) Backup.
i) Objectives for contingency plans.
j) Quality assurance.
k) Access control.
l) Principles for implementing the policy in detailed guidelines, procedures and instructions.
m) Precautions in case of breach of IT security policy and security rules.
n) Compliance with relevant legislation.
o) Reporting, control and follow-up.
p) Any exemptions from the IT security policy.

4) If the company is a SIFI or a G-SIFI, the IT security policy, cf. no. 3, must include a position on the need to establish multi-centre operations for all business-critical IT systems, cf. Section 2 (3).

5) The Board of Directors must regularly and at least once a year re-evaluate the IT security policy based on an updated risk assessment, including assessing whether the IT security policy is sufficient to ensure that the risks IT use entails and is expected to entail in the future are at a level acceptable to the company.

6) The IT security policy must as far as possible be independent of the technology used.

Tasks and responsibilities of the Executive Board

7) The Board of Management must ensure compliance with the company's IT security policy. The Executive Board must elaborate the IT security policy in procedures, etc. to help ensure that

a) responsibilities, including ownership of IT processes and resources, are placed,
b) the separation of functions is continuously monitored and reviewed,
c) maintenance of the desired IT security level is monitored and any weaknesses are managed,
d) systems and data are classified and prioritised, cf. no. 19,
e) critical systems, data and multidisciplinary dependencies are continuously identified and risk-assessed, cf. no. 19,
f) systems (both basic and user systems) and configuration (hardware) as well as changes to them are documented,
g) backup of systems and data takes place, including storage of the backups,
h) sufficient IT resources are acquired,
i) system development, configuration and maintenance, as well as testing of new and changed systems, are adequate,
j) tests and other quality assurance are carried out,
k) change management and problem management take place,
l) there is access control to systems and data, cf. nos. 16-19,
m) there is sufficient physical security, including physical access control,
n) there are sufficient IT contingency plans and testing of IT preparedness, cf. nos. 20-23, and
o) appropriate measures are implemented to educate employees in IT and cyber security.

8) The Board of Management must ensure that monitoring and control of compliance with the IT security policy are established.

9) The Board of Management must regularly report to the Board of Directors on non-compliance with the IT security policy.

10) If the company is a SIFI or a G-SIFI, which has several operating centres, the Board of Management must ensure that the distance between the operating centres is sufficient for an incident that puts one operating centre out of service to be unable to affect other operating centres at the same time. Sufficient distance between operating centres must be established on the basis of a specific risk assessment.

11) The Board of Management of a credit or mortgage credit institution designated by the FSA as the operator of essential services must ensure that the FSA and the Centre for Cyber Security are informed as soon as possible of incidents, which have significant consequences for the continuity of the essential services they deliver. The notification must contain information on

the number of users affected by the interruption of the essential service, the duration of the incident, the geographical distribution with regard to the area affected by the incident and any cross-border consequences of the incident.

IT risk management, rights management and preparedness

IT risk management

12) The Board of Directors must ensure that the company has a policy for IT risk management. The policy can be a separate policy or part of other relevant policies.

    The policy must include at least:
    a) Goals for the company's IT risk management.
    b) Identification of which IT risks the company may be exposed to.
    c) Assessment of how the company's IT risks are reduced to, or maintained at, an acceptable level.
    d) Overall principles for IT security management, in order to keep IT risks at a level acceptable to the Board.
    e) Assessment of:
        - risks related to the company's systems and data
        - risks related to the integration and suitability of the company's IT systems
        - IT risks related to dependence on external conditions, including subcontractors
        - IT risks related to the organisation of the company, including lack of separation of functions.
    f) General principles for how the company must register and categorise IT incidents.
    g) General principles for reporting IT incidents to the Board of Directors, which must ensure that the Board of Directors always has sufficient insight into the company's IT risks and how they are developing.

13) The Board of Management must ensure that the company's IT risk management policy is complied with. The Board of Management must elaborate the policy in procedures, etc. which as a minimum describe:
    a) the method for identifying, assessing and monitoring IT risks
    b) placement of responsibility and organisation
    c) the establishment and implementation of control and security measures based on IT risks, and how coherence between IT risks and controls is ensured
    d) follow-up on IT risks
    e) reporting to the Board of Directors on significant IT risks.

14) If, pursuant to section 16, the company is required to have a risk management function and a risk manager, IT risk management is included as part of the risk manager's tasks in accordance with Appendix 7.

15) For common data centres, the following applies:
    a) The Board of Management must ensure that the company's IT risk management is handled in a reassuring way by a risk manager appointed by the Board of Management .

b) The Board of Management must ensure that the IT-related tasks and responsibilities of the risk manager are clear.
c) The Board of Management must ensure that the risk manager has access to all relevant information in relation to IT and has sufficient resources.
d) The risk manager must have an overview of the company and the company's IT risks in order to be able to assess whether they are managed reassuringly.
e) The risk manager must ensure that
   - all significant IT risks are identified, measured, managed and reported correctly
   - IT risks that apply throughout the company's organisation, systems and data are included in the IT risk assessment
   - IT risks in outsourced functions/tasks are included in the assessment of the company's total IT risk assessment.

Rights management

16) The Board of Management must ensure that the company has a reassuring risk-based user and rights management, which ensures that critical systems and data are only accessed at an approved work-related need.

17) The Board of Management must elaborate the company's user and rights management in procedures, etc. which involve at least:
   a) identification and classification of critical systems and data in relation to rights management and the highlighting of risks associated with it
   b) identification of roles, rights and their combinations, as well as the highlighting of risks associated with them, including the extent to which the granting of access in accordance with a work-related need must be subject to continuous monitoring and supervision and the responsibility for this
   c) continuous control and monitoring of the use of privileged and administrative access
   d) allocation, modification and timely withdrawal of access
   e) periodic review of allocated access, as well as when unapproved access must lead to control and follow-up actions.

18) The Board of Management must ensure separation of functions in systems and in technical environments on a documented basis.

19) The Board of Management must ensure that systems and data are regularly classified, that critical access across the systems are identified, and that critical system access are logged to ensure effective monitoring and timely detection of unauthorised activity.

Preparedness

20) The Board of Management must ensure that an IT contingency plan is prepared containing an objective for restortion of normal operation in the event of errors, breakdowns, loss of data or systems, as well as full or partial destruction of buildings, hardware and communication paths in accordance with the Board of Directors' objective, cf. no. 3 (i). Depending on the circumstances of the company, the plan must include:
   a) a description of how a contingency organisation is established, including the division of roles and responsibilities in the contingency organisation

b) activity plans in relation to serious system failure, errors and disruption in IT use as well as recovery procedures.

21) The Board of Management must ensure that the contingency plan is regularly tested. The scope of the tests must, inter alia, be based on relevant scenarios and the company's threat situation.

22) The Board of Management must report significant results of the contingency tests to the Board of Directors.

23) The Board of Management must ensure that contingency plans, activity plans and recovery procedures are updated regularly and at least once a year based on test results as well as threat and risk assessments.'