Group Compliance Policy

SEPTEMBER 2018

Purpose

This Group Compliance Policy (the Compliance Policy) sets out the principles and standards for compliance and management of compliance risks in Danske Bank Group (the Group).

The objective of this Compliance policy is to ensure compliance risks are identified, and adequately mitigated. The Group seeks to reduce compliance risks taking into account the nature, scale and complexity of the business. This is in alignment with the Group strategy and The Essence, which sets the Group's vision to be recognised as the most trusted financial partner, and is deeply connected to treating customers fairly and conducting business with high integrity.

The Compliance policy is designed to meet the requirements of the Danish Executive Order on Management and Control of Banks no. 1026 of 30 June 2016 and additional applicable legislation.

Scope and application

The Compliance Policy applies to all employees, all functions, all units in the Group, and all regulated legal entities once adopted by Senior Management.

In case the Compliance Policy conflicts with local requirements, senior management of the subsidiary can approve the Compliance Policy with deviations. Any material deviations from the Compliance Policy must be reported to the Board of Directors of Danske Bank A/S, as well as the administrator of the Information Management Policy, and informed to Group Compliance.

Definitions

Compliance is defined as the adherence to laws, including the spirit of the law, regulations, generally accepted practices, standards, and financial industry codes of conduct.

Compliance risk is defined in this Compliance Policy as the risk of legal or regulatory sanctions, material financial loss, or loss of reputation which the Group may suffer as a result of its failure to comply with laws, including the spirit of the law, regulations, generally accepted practices, standards, and financial industry codes of conduct applicable to Group's activities.[1]

[1] This definition is in accordance with the Basel Committee on Bank Supervision.

Governance

The Board of Directors has the overall responsibility for compliance and management of compliance risks in the Group. The Board of Directors and the Executive Board must ensure that appropriate and adequate resources, sufficient internal procedures and systems are in place. The identification of compliance risks, their assessment and appropriate risk management shall be elements to consider in any process and form the basis for a risk based approach, when establishing appropriate and applicable countermeasures to mitigate the risk.

In order to ensure appropriate risk management, the Group has established three lines of defence and control governance model:

- Business units and group functions constitute the 1st line of defence, and have primary responsibility for identifying, managing and mitigating the Group's compliance risks by having sufficient controls in place.
- Group Compliance is an independent risk control function headed by the Head of Group Compliance and constitutes the 2nd line of defence for compliance risk. Group Compliance is responsible for having an independent oversight of the Group's Compliance risks, by performing risk assessment, monitoring activities, advisory work and providing independent report to senior management. Additionally, Group Compliance serves as the Group Data Protection Officer (DPO) function and the Designated Group Conflicts Officer (DGCO) function.

- Group Internal Audit constitutes the 3rd line of defence and is responsible for auditing both the 1st and 2nd line of defence in terms of validating that a robust framework is in place, sufficiently implemented and assess the effectiveness of internal controls.

Compliance risk and risk tolerance

Compliance risks exists as an inherent part of doing business. Hence, compliance risk management in the Group is considered to be of key importance. The identification of compliance risks, their assessment and appropriate risk management shall be elements to consider in any process and form the basis for a risk based approach, when establishing appropriate and applicable countermeasures to mitigate the risk; including escalation of problematic cases according to the Group's Escalation Policy. Monitoring complaints handling processes in the Group and using complaints as a relevant source of information for compliance reporting is one of the elements for the basis of risk based approach.

Group Compliance must oversee the development and periodic review of the product governance arrangements. In this regard, information about products that are manufactured and distributed by the Group, including their distribution strategies, shall be systematically included in the compliance reports to the management body and made available to National Competent Authorities on request. The relevant Product Committee must assist Group Compliance by providing information about all products when they are developed or reviewed. To the extent required by applicable legislation, subsidiaries must allocate necessary resources to monitor relevant product governance arrangements.

Compliance with the data protection regulation is supported by and follows the provisions of this Compliance Policy. In the role as DPO, Group Compliance must oversee compliance with the General Data Protection Regulation (GDPR) and applicable national data protection laws.

The Group does not tolerate breaches of applicable laws, including the spirit of the law, regulations, generally accepted practices and standards and financial industry codes of conduct applicable to the Group's activities, significant fines or other significant enforcement actions.

Compliance Framework

The Group's Compliance framework and strategy is embedded across the three lines of defence. This Compliance policy describes the principles for risk mitigation of compliance risk, in order to have a comprehensive overview of the Group's compliance framework. Other governing documents within, but not limited to, financial crime, conflicts of interest, market abuse, data protection, whistleblowing and code of conduct should be considered.

As the control function, Group Compliance is responsible for designing, implementing and maintaining a group wide framework for compliance risk identification, assessment, monitoring and reporting. Group compliance follows a risk-based approach to identify, and prioritise the monitoring activities.

In addition, Group Compliance is responsible for providing advice to business units and group functions related to compliance risk management and mitigation.

Reporting

Group Compliance must provide a semi-annual compliance report to the Executive Board, to the Audit Committee and to the Board of Directors. As a minimum, the compliance report must include findings of non-compliance.

The Head of Group Compliance has a day-to-day reporting line to the Chief Financial Officer, and escalation lines to the Executive Board and the CEO of the Executive Board. In the event of need for escalation outside Group compliance reporting period, the Head of Group Compliance will escalate in the appropriate channels. The Head of Group Compliance has a right and an obligation to escalate any material or systemic breaches to the Audit Committee.

Review

The policy is managed and updated by Group Compliance and approved by the Board of Directors.

The Policy must be reviewed and updated at least annually. Any changes to the policy must be endorsed by the Audit Committee and approved by the Board of Directors.