Danske Bank

Group Compliance Policy

25 June 2020

1. Objective

The Group provides a wide range of financial services and products and, as a result, operates in a highly regulated environment. The Group takes its obligations to comply with applicable laws, rules and regulations extremely seriously, including the spirit of the law. Demonstrating compliance is a core part of building and sustaining the trust of our customers, and protecting the interests of our stakeholders.

The Group Compliance Policy (the "Policy") sets the principles and standards for managing Compliance Risks across the Group in order to realise the Group's vision of being recognised as the most trusted financial partner. Furthermore, it describes the role the independent second line oversight function Group Compliance has in supporting the Group to remain compliant with applicable laws, rules and regulations.

The Policy is designed to meet the requirements of the Danish Executive Order on Management and Control of Banks No. 1026, dated 30 June 2016, EBA Guidelines on Internal Governance EBA/GL/2017/11, dated 21 March 2018, Basel Committee on Banking Supervision guidance for Compliance and the Compliance Function in Banks, dated April 2005, ESMA/2012/388 Guidelines on certain aspects of the MiFID compliance function requirements, dated 28 September 2012, and other applicable legislation and guidelines.

Lack of adherence to the Policy may lead to disciplinary actions.

2. Definitions

The below definitions apply to the terms used throughout the Policy.

Compliance Culture	A culture where all employees, managers and members of the Board of Directors feel empowered to take positive steps to ensure the Group remains compliant with applicable laws, rules and regulations. A strong Compliance Culture is reinforced through the role-modelling and rewarding of positive behaviours; implementing appropriate governance and reporting mechanisms; relevant policies, instructions and systems; as well as, ongoing training and awareness. [1]
Compliance Risk	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, rules and standards applicable to the Group's activities. [2]
Conduct Risk	The risk that the Group's behaviour, in supplying financial services, causes customer detriment, damages the integrity of financial markets, reduces competition or erodes society's trust in the Group.[3]
Financial Crime Risk	The risk of internal or external parties using the Group's infrastructure and services to steal, defraud, manipulate or circumvent established rules, laws and regulations, particularly in the areas of money laundering, terrorist financing, economic sanctions as well as bribery and corruption.[4]
Group	Danske Bank A/S including all subsidiaries.

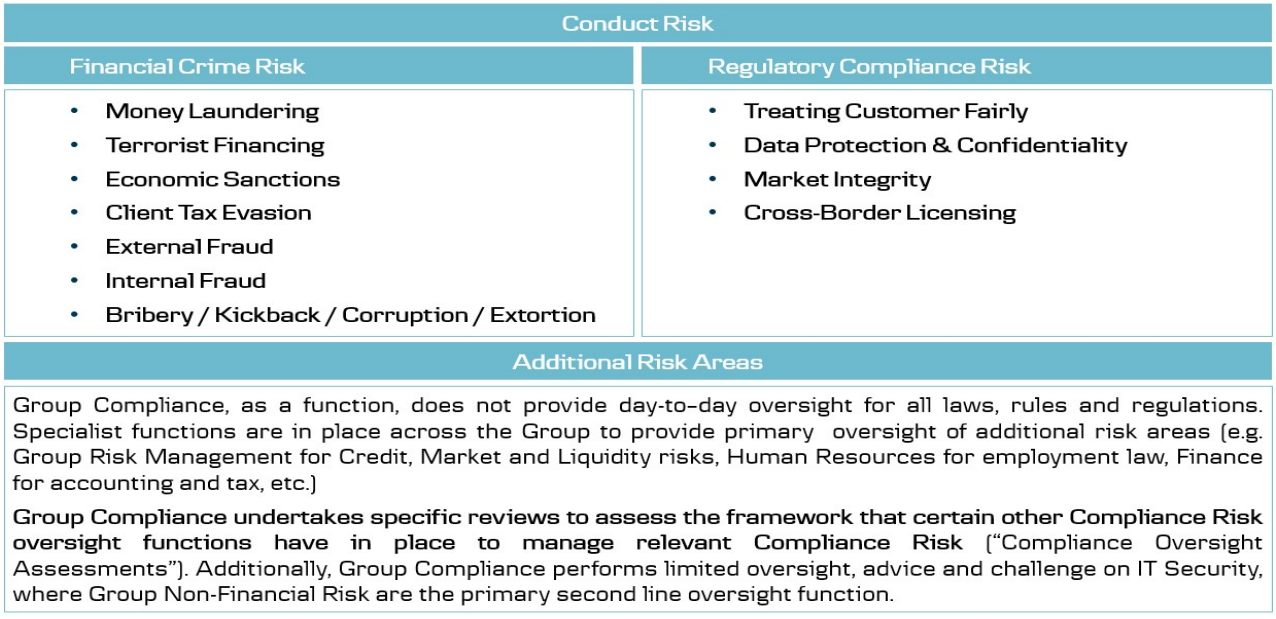
[1] A strong Compliance Culture is a core part of the Group's sound business culture, as outlined in the Code of Conduct Policy.
[2] Based on the definition of compliance risk in the guidance of the Basel Committee on Banking Supervision for *Compliance and the Compliance Function in Banks*.
[3] As defined by the ERM strategy.
[4] As defined by the ERM strategy.

Group Compliance	Is a permanent and independent function within the Group, which constitutes the 2nd line of defence with primary oversight responsibilities for Regulatory Compliance Risk, Financial Crime Risk and Conduct Risk as defined in Section 3.
Governing Information	Written governing information that instructs and/or guides employees across the Group in performing their daily tasks, including and limited to the Essence, strategies, policies, instructions and standard operating procedures.
Regulatory Compliance Risk	The risk of or incurring regulatory, criminal or administrative sanctions, material financial loss, or loss of reputation, which the Group may suffer as a result of its failure to comply with laws, rules and standards applicable to the Group's activities in the areas of treating customers fairly, market integrity, data protection and confidentiality and cross border licensing.[5]
Subsidiary	Any undertaking over which Danske Bank A/S effectively exercises a dominant influence.

3. Scope

The Policy is applicable to the management of all Compliance Risks in the Group, as well as the specific roles and responsibilities of Group Compliance. In the context of the Policy, Group Compliance is responsible for the oversight of the following Level 1 risk types, as defined by the Enterprise Risk Management (the "ERM") strategy: Financial Crime Risk, Regulatory Compliance Risk as well as the cross-taxonomy risk – Conduct Risk, and all associated underlying Level 2 and Level 3 risk types. Group Compliance also plays a role in the oversight of other risk areas, including IT Security Risk (see Figure 1).

Figure 1 – Scope of Group Compliance



3.1. Target Group

The Policy is established by the Board of Directors of Danske Bank A/S (the "BoD") and applies to all employees, contractors, outsourced relationships, business units, group functions, Subsidiaries and branches of the Group.

The management body of any Subsidiary may approve the Policy with deviations in case the Policy conflicts with local regulatory requirements. The policy administrator in the Subsidiary should justify the rationale behind the deviation and ensure that the administrator of the Group Policy is consulted and endorses any deviation.

The administrator of the Policy must document and report any deviations from the Policy to the Policy owner and ultimately to the Executive Leadership Team of Danske Bank A/S (the "ELT") via the administrator of the Steering Policy. The ELT shall report all deviations from Group Policies to the BoD.

[5] As defined by the ERM strategy.

4. Policy Content

Principle 1: Activities in the Group are conducted compliantly

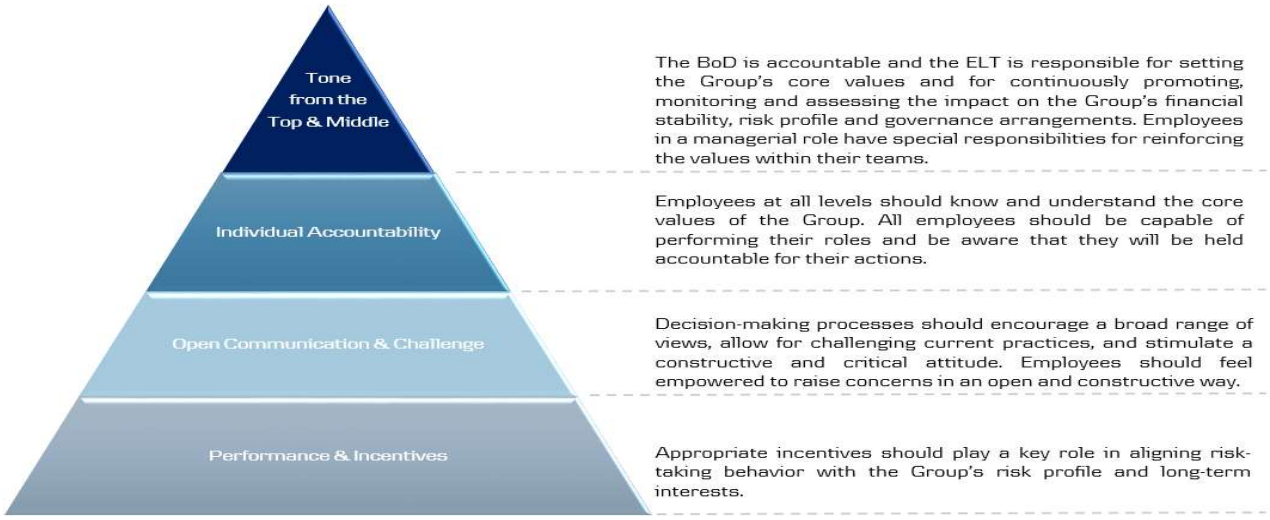
The BoD is ultimately accountable for the Compliance Risks undertaken by the Group, where the ELT retains management responsibility. The ELT is responsible for implementation of and adherence to the Policy, supported and advised by Group Compliance.

The Group must conduct its activities in adherence with applicable laws, rules and regulations. In undertaking such activities, the Group is exposed to Compliance Risk, which is an inherent element of doing business and as such must be considered when developing or executing the Group's business strategy.[6] The consideration of, and response to, Compliance Risks is expected to be comprehensive and risk-based in order to develop and implement appropriate mitigation measures. All employees share the responsibility for compliance regardless of their position within the Group.

Subprinciple 1.1: All employees are responsible for maintaining a strong Compliance Culture

A strong Compliance Culture begins with the 1st line of defence and is reinforced by a framework of Governing Information set by the 2nd line of defence. Strong leadership from the BoD and ELT is fundamental in promoting awareness, giving clarity and equipping employees to do their job properly in alignment with sound risk management principles and practices.

Figure 2 – Sound Compliance Culture



The BoD and ELT, supported by Group Compliance, must play a key role in developing and embedding a strong Compliance Culture. This is achieved in a number of ways including:

- Setting and embedding an appropriate risk appetite framework and tolerances,
- Continuously and clearly advocating the components and benefits of a strong Compliance Culture "tone from the top",
- Reinforcing "tone from the top" through direct advocacy by employees in a managerial role "tone from the middle",
- Maintaining effective incentive and reward practices that reinforce positive conduct,
- Removing barriers to positive conduct (e.g. speaking up, systems and tools and other workplace hygiene factors),
- Setting clear expectations for compliance through comprehensive requirements in Governing Information,
- Maintaining effective governance for the oversight and challenge of Compliance Risks,
- Developing and maintaining effective risk management tools to identify, prioritise, manage and report Compliance Risks,

[6] Execution of the Group's business strategy includes, but is not limited to, decisions and/or actions that materially affect the Group's risk profile (for example, entering new jurisdictions; undertaking new regulated activities; launching or amending products, processes or systems).

- Providing suitable training and awareness programmes that empower managers and employees to remain, and help each other to remain compliant.

Subprinciple 1.2: A sound risk taking approach informs all decisions impacting the Regulatory Compliance, Financial Crime and Conduct Risk profile of the Group

In keeping with sound compliance risk management principles, each business unit and Group function is expected to properly consider the impact of their activities on the risk profile of the Group.

Financial Crime Risk

- By providing products and services to customers there is an inherent risk that the Group may be used to conduct dishonest or unlawful activities (e.g. money laundering, terrorist financing, breaches of economic sanctions and tax evasion).
- The Group does not condone financial crime or any other criminal activity and has implemented, and continues to invest in systems, processes and controls to reduce the residual impact and likelihood of Financial Crime Risk.
- The Group's approach is to 'avoid' undertaking business activities that exposes the Group to Financial Crime Risk that cannot be appropriately controlled. The Group strongly disassociates itself from such activities. Action must be taken to mitigate immediately any such impacts, if identified.

Regulatory Compliance Risk

- The Group is subject to the laws, rules and regulations of the jurisdictions within which it operates. This includes having a physical presence (e.g. branch or Subsidiary) in a jurisdiction; holding the rights to transact business in that jurisdiction as a result of existing agreements (e.g. passporting); having customers or business interests in and conducting permissible cross-border activity.
- The Group is committed to compliance with applicable laws, rules and regulations and undertakes due diligence and ongoing monitoring of its regulatory compliance obligations in all areas of operation.
- The Group's position is to 'limit' the potential for non-compliance through having robust systems and controls to identify, implement and monitor ongoing compliance with applicable laws, rules and regulations.
- The Group does not accept systemic or persistent breaches of laws, rules and regulations (including any failure to implement new regulations) and must take immediate action to mitigate any such identified issues.

Conduct Risk

- The Group, in accordance with its vision to be recognised as the most trusted financial partner, requires that all employees act in accordance with applicable laws, rules and regulations at all times and place the interests of customers first. Only by acting with integrity and using the expertise of the Group, can we achieve our aim to provide sustainable value to customers and keep the trust of our stakeholders and the wider society.
- The Group's position is to 'avoid' undertaking business that results in negative outcomes for customers or that erodes the trust placed in the Group by stakeholders and society.
- The Group must take action to mitigate immediately any negative customer, regulatory or reputation impacts, if this occurs.

Principle 2: The BoD and ELT provide appropriate and adequate resources to enable Group Compliance to undertake its legal and regulatory responsibilities

The BoD appoints a Chief Compliance Officer, who is a member of the ELT and Head of Group Compliance. The Chief Compliance Officer ensures that an adequate governance setup is in place within the area of his/her responsibility. This setup should at all times be designed in such a way that enables adequate and diligent management decision-making and appropriate oversight of the function. This implies solid collaboration with all parts of the Group and the capability to support and challenge business units and Group functions in the efforts to do the right thing for our customers, colleagues and society.

The ELT must ensure that adequate resources are available to achieve the BoD's objective of having sufficient internal procedures, systems and controls to allow the Group to meet regulatory requirements.

Group Compliance is responsible for overseeing Regulatory Compliance, Financial Crime and Conduct[7] risks and for providing advice, guidance and challenge to the 1st line of defence as described in Subprinciple 4.4. This includes

[7] The oversight of Conduct risk potential impacts is undertaken by the Group's Conduct & Reputational Committee.

providing support and fostering ongoing awareness. These activities should be seen as part of an ongoing process that is adjusted to regulatory changes and requirements and to business activities.

To support its oversight role on Compliance Risks, the BoD has established the Conduct & Compliance Committee, which is responsible for the preparatory work for the BoD with respect to conduct and reputational risk, compliance, financial crime and any other matters, which the BoD may want to have examined by the Conduct & Compliance Committee.

Additionally, the Chief Compliance Officer (or delegate cf. Principle 3 below) should be a permanent member of all committees where there are matters relevant to Regulatory Compliance, Financial Crime or Conduct Risks.

Principle 3: The Chief Compliance Officer can delegate his or her mandate to ensure the efficient operation of the Group Compliance where he or she is not limited by law or by instruction of the BoD

The Chief Compliance Officer has the right to delegate his/her mandate to support the effective functioning of Group Compliance and the oversight of day-to-day business operations.

Delegation can only be provided to a qualified person with sufficient competence and experience to undertake the activity. For this purpose, it is expected to establish appropriate procedures for supervision and control (i.e. follow-up, review and reporting processes) to determine that delegated responsibilities are being exercised properly.

In managing Compliance Risks, the ELT and/or the Chief Compliance Officer, within the limits of his/her mandate, can delegate duties and responsibilities to sub-committees and other relevant fora to provide:

- Adequate and coordinated oversight of all relevant Compliance Risk types as defined by the ERM strategy,
- Coordinated control of all decisions made on compliance matters across the Group to enhance accountability and transparency.

The Chief Compliance Officer may not delegate any responsibilities that must, by law or by instruction of the BoD, be undertaken directly.

Principle 4: Group Compliance provides primary oversight of Regulatory Compliance Risk, Financial Crime Risk and Conduct Risk and performs its responsibilities independently

Group Compliance is a permanent and independent function, which constitutes the 2nd line of defence with primary oversight responsibilities for Regulatory Compliance Risk, Financial Crime Risk and Conduct Risk. Group Compliance also provides specific assessments to understand the framework in place across other 2nd line of defence and independent oversight/control functions to ensure their adherence to laws, rules and regulations, relevant to their functions (as defined in Section 3).

Group Compliance is responsible for control testing and assessing whether methods and procedures that are suitable for identifying and reducing the risk of non-compliance with laws, rules and regulations, as well as measures taken to address any deficiencies, are effective. Group Compliance also undertakes specific assessments across other 2nd line of defence and independent oversight/control functions to confirm processes for adherence to laws, rules and regulations are appropriate for these functions.

In order to fulfil the independence requirements:

- The Chief Compliance Officer should be free from any conflicts of interest that may impede the independent and objective performance of his/her duties or subject him/her to undue or inappropriate influence.
- The Chief Compliance Officer must have a direct access to the BoD to maintain independence. Additionally, direct reports of the Chief Compliance Officer, where specifically mandated, may approach the BoD on matters where the defined escalation route presents a potential conflict of interest or where such access is prescribed by regulation (e.g. Swap Dealer Chief Compliance Officer, Data Protection Officer).
- Group Compliance must be provided with sufficient and skilled resources required to perform the core duties of the function.
- Group Compliance must have access to all relevant information to enable the function to carry out its responsibilities (see Subprinciple 4.9 for more details).

- Group Compliance remuneration practices must be determined in a manner that avoids jeopardising the independence of the function or individuals within the function and must be in line with the Group's Remuneration Policy.
- Group Compliance employees, as a rule, must not be involved in the provision of services or activities of which they have direct oversight or monitoring responsibilities. In cases where Group Compliance employees are required to perform tasks not directly related to their compliance responsibilities, potential conflicts of interest must be mitigated through independent oversight provided by one or more employees not involved in those tasks or activities.
- Group Compliance is responsible for independent quarterly reporting to the ELT and the BoD on matters relating to Regulatory Compliance, Financial Crime and Conduct Risks (see Subprinciple 4.15 for more details).

Furthermore, Group Compliance is required to develop and implement a structured and well-defined compliance programme setting out its planned activities including alignment with the Group's strategic business plan. The compliance programme is risk-based and subject to oversight by the Chief Compliance Officer to ensure appropriate coverage across business areas and co-ordination with other risk and oversight/control functions.

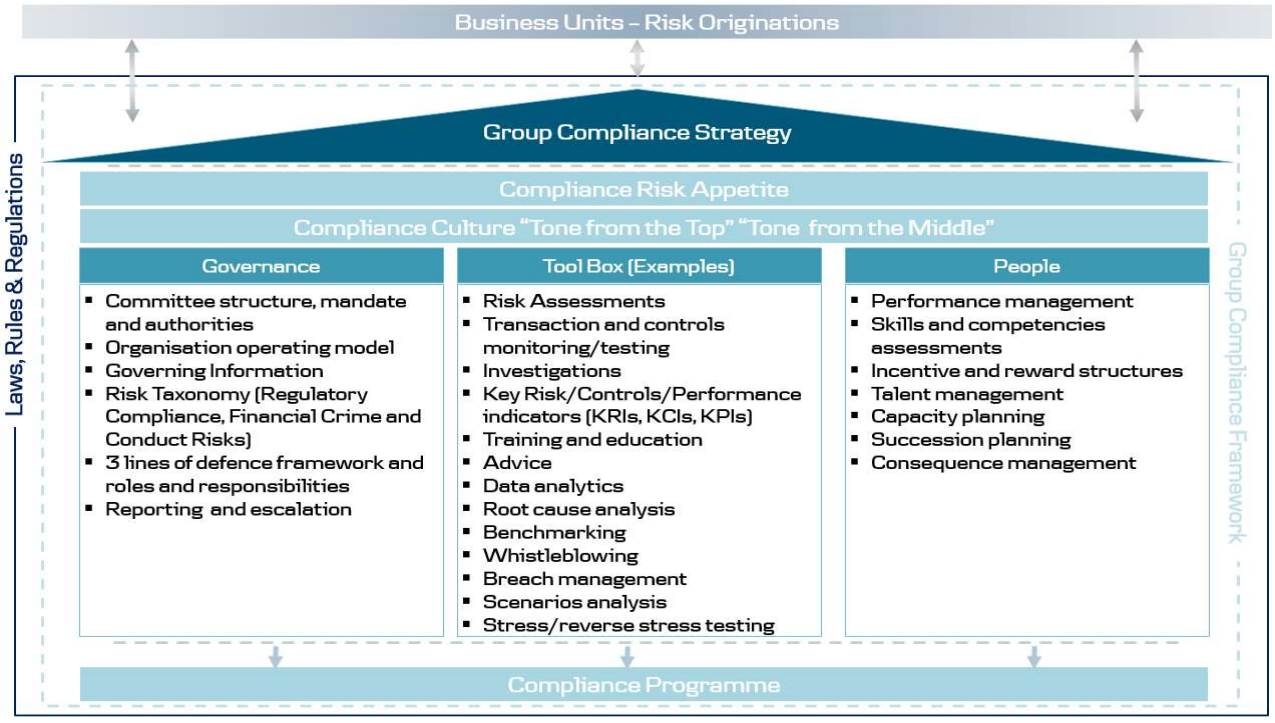
Subprinciple 4.1: Group Compliance establishes and maintains an independent governing framework for managing Regulatory Compliance, Financial Crime and Conduct Risks consistent with the ERM strategy

The Group Compliance framework articulates the function's approach to identifying, measuring, managing, reporting and escalating risks which have a material impact on the delivery of the Group's strategy. Group Compliance's approach is consistent with the ERM strategy, which defines the way the Group manages all risk types.

The framework includes the strategy, the compliance programme, an approach to sound risk taking, Governing Information owned by Group Compliance, including this Policy, a toolkit and processes and systems aimed at managing risks overseen by Group Compliance (see Figure 3). The Group Compliance framework is underpinned by the capability of its employees and a sound Compliance Culture. A key component of the framework is the clear articulation of the roles and responsibilities for managing Regulatory Compliance, Financial Crime and Conduct Risks.

Group Compliance continuously assesses the possible impact of any changes in the legal or regulatory environment on the Group's activities and on the Group Compliance framework, and supports the 1st line of defence in implementing the changes as required. In addition, Group Compliance supports the assessment of possible impacts from changes in the legal or regulatory environment on the Group's activities.

Figure 3 - Group Compliance framework



On a wider scale, the Group operates within an internal control environment underpinned by a three lines of defence model as described by the ERM strategy. In this model, Group Compliance as the 2nd line of defence (i) sets framework for management of Regulatory Compliance Risk, Financial Crime Risk and Conduct Risk; (ii) advises on sufficient management processes and controls for these risks; (iii) challenges adherence to laws, rules and regulations; and (iv) provides independent reporting and escalation of issues and control status to the ELT and to the BoD. On the other hand, the 1st line of defence owns the management of Compliance Risks and is responsible for identifying, mitigating and reporting Compliance Risks and issues in accordance with the Group Compliance framework, (incl. reporting on Compliance Risk management activities and control effectiveness).

Subprinciple 4.2: Group Compliance undertakes risk assessments of the risks overseen by Group Compliance, providing an independent 2nd line of defence assessment

Group Compliance designs and maintains a risk assessment methodology and appropriate tools, which allows effective identification of inherent and residual risks. Group Compliance executes independent risk assessments using this methodology[8] and tools.

Risk assessments are performed on an ongoing basis (i.e. annually) and are used to determine the focus of the control testing and monitoring, training and advisory activities performed by Group Compliance.

Ad hoc risk assessments may be carried out if required, e.g. in relation to a change in regulations, or a major operational or technological change.

Subprinciple 4.3: Group Compliance performs control testing

Group Compliance designs and maintains a control testing methodology, a control testing plan, carries out control testing designed to test the Group's compliance with applicable laws, rules and regulations and requirements set in Governing Information and provides reports that describe the results of control testing.

A risk-based approach is used to prioritise control testing activities based on risk assessments and other relevant information.

Subprinciple 4.4: Group Compliance provides independent advice to the BoD and ELT and 1st line of defence

Group Compliance advises the BoD and the ELT (and by extension the 1st line of defence) on measures to be taken to ensure compliance including the allocation of responsibilities for the implementation and oversight of laws, rules and regulations as overseen by Group Compliance.

Group Compliance monitors compliance with laws, rules and regulations and requirements provided in Governing Information. Furthermore, Group Compliance provides independent advice to the 1st line of defence on whether activities and/or controls are compliant and in line with the interpretation of Governing Information, laws, rules and regulations (as overseen by Group Compliance).

Group Compliance has the authority to challenge the 1st line of defence where decisions, actions or activities are not aligned with applicable requirements in Governing Information and/or compliant with applicable laws, rules and regulations. Group Compliance officers may intervene and escalate to the Chief Compliance Officer, decisions, actions or activities undertaken by the 1st line of defence, which poses a risk of non-compliance (see Subprinciple 4.8 for details of the Chief Compliance Officer's right to access the BoD).

Subprinciple 4.5: Group Compliance provides relevant training and education for employees on Regulatory Compliance Risks, Financial Crime Risks and Conduct Risks

Group Compliance ensures that its own employees possess sufficient knowledge, expertise and skills to discharge their responsibilities, as well as undertake continuous professional development.

Group Compliance is responsible for providing targeted training to the BoD and ELT on sound practice for the management of risks overseen by Group Compliance.

Group Compliance also provides mandatory compliance training to educate all employees of the Group to fulfil their responsibilities in respect to adherence with laws, rules, regulations and requirements set in the Governing Information. Separately, Group Compliance also provides oversight and challenge on the completeness and completion of training required by 1st line of defence to meet regulatory requirements.

[8] Group-wide risk assessment is an independent methodology, but it is aligned to the ERM strategy and its taxonomy.

Subprinciple 4.6: Group Compliance engages, cooperates and communicates with supervisors, competent authorities and law enforcement agencies on matters concerning Regulatory Compliance, Financial Crime and Conduct Risks

The Group, as a provider of a wide range of financial services, is required to liaise with different supervisors and regulators, competent authorities and law enforcement agencies. In doing so, all compliance related material requests or substantial interactions must be referred without delay to Regulatory Affairs or, where relevant, the appointed Financial Supervisory Authority (the "FSA") relationship manager. The FSA relationship manager shall involve Regulatory Affairs in critical interactions with the local FSA. All employees must act professionally, with integrity and be open, transparent and forthcoming in interactions with regulators and/or competent authorities.

Subprinciple 4.7: Group Compliance provides the data protection compliance function, including the role of Group Data Protection Officer

Compliance with data protection regulation is a fundamental requirement of the Group to protect the interests of customers and employees. The Group Data Protection Officer, supported by Data Protection Compliance, oversees compliance with the General Data Protection Regulation and applicable national data protection laws. Detailed information on the management of data protection risks is outlined in a number of Governing Information documents, which can be found on the Group's policy site.

Subprinciple 4.8: Group Compliance is consulted in significant decisions, processes, major changes (including systems) and the approval of new and amended products

Major Decisions

Group Compliance must be consulted where the Group seeks to undertake significant decisions, major change projects, strategic initiatives and major transactions (altogether "*Major Decisions*"[9]). In keeping with Subprinciple 4.4, Group Compliance officers may escalate risks of non-compliance to the appropriate governance forum and to the Chief Compliance Officer, as appropriate.

The Chief Compliance Officer may refer any Major Decisions to the BoD for consideration where there is a clear risk of non-compliance or the decision is inconsistent with the risk taking approach for Regulatory Compliance, Financial Crime and Conduct Risks. Where the implementation is imminent, the Chief Compliance Officer may put a stop to such Major Decisions and demand final approval from the BoD.

New and Amended Product Approval ("NAPA")

Group Compliance provides oversight and advice on the development and periodic review of the Group's product governance arrangements in order to detect any risk of failure to comply with regulatory obligations, including known forthcoming changes. Group Compliance must also be engaged in the approval of any new products or significant changes to existing products, processes or systems, as well as the periodic review process[10]. Product reviews may be conducted independently or concurrently with Group Risk Management and/or Group Legal.

Where any features of the new or existing product causes concern, including potential reputational impact to the Group, Group Compliance officers have a right to escalate to the relevant oversight body/committee and ultimately to the Chief Compliance Officer.

Information about products that are manufactured and distributed by the Group, including their distribution strategies, must be provided to Group Compliance and included in compliance reporting and made available to national competent authorities on request. The relevant product owner (or office) must provide Group Compliance with reasonable information on new or amended products to enable Group Compliance to form a view on the level of risk taking and whether this is consistent with regulatory requirements. To the extent required by applicable legislation, Subsidiaries must allocate necessary resources to monitor relevant product governance arrangements.

Subprinciple 4.9: Group Compliance must be provided access to any and all information necessary to carry out its responsibilities

Group Compliance must have access to all relevant information to carry out its duties and to enable the function to provide independent information to the BoD and ELT. This includes access to all relevant databases and information on customer complaints.

---

[9] While *Major Decision* are not specifically defined in the Policy, Group Compliance would expect reasonable judgement to be applied to any decision, change project, strategic initiative or transaction. Where there is uncertainty about interpretation, advice should be sought from Group Compliance.

[10] See Product Governance Directive for NAPA for details of the Group's process.

Group Compliance must have the right on its own initiative to communicate with any employees and obtain access to any records or files necessary to enable it to carry out its responsibilities, where this does not contravene with existing legal limitations.

Subprinciple 4.10: The Group must have appropriate reporting structures, supported by clear roles and responsibilities, to enable aggregation and presentation of Regulatory Compliance, Financial Crime and Conduct Risks relevant to the Group as a single consolidated entity

Group Compliance must document and maintain a functional reporting structure outlining the respective roles and responsibilities in the management of Regulatory Compliance, Financial Compliance and Conduct Risks between the function, business units, branches of the Group, Subsidiaries and any other connected entities (e.g. joint ventures).

Where appropriate and consistent with local legislation, branches of the Group, Subsidiaries, or connected parties may enter into formal service level agreements with Group Compliance to detail the services received.

All agreed reporting structures must be in accordance with Danish and local law applicable to the branch or Subsidiary. Any such structure should enable Group Compliance to understand, aggregate and present relevant risks to the consolidated Group. This includes any risks or issues which might impact the Regulatory Compliance, Financial Crime or Conduct Risk profile of the consolidated Group.

Subprinciple 4.11: Group Compliance cooperates with Group Legal, HR Legal, Group Risk Management and Group Internal Audit

The scope and breadth of the Group Compliance activities require close engagement with Group Legal, HR Legal, Group Risk Management and, where appropriate, with Group Internal Audit.

In particular, Group Compliance and Group Risk Management cooperate and exchange information to perform their respective tasks. Sharing information on relevant incidents, breaches, findings and/or observations between Group Compliance and Group Risk Management is required to ensure completeness in reporting and decision-making processes.

Group Compliance operates as an independent function but works in close cooperation and collaboration with Group Risk Management on the development, maintenance and enhancement of the Enterprise Risk Management strategy (to the extent it impacts the effective management of Compliance Risks) in order to effectively identify, assess, manage and report relevant risks. Core elements of the current strategy, where the close collaboration is envisaged, includes development and maintenance of the risk taxonomy, risk impact methodology, risk appetite/risk tolerance and policy governance.

Subprinciple 4.12: Group Compliance is responsible for the conflicts of interest framework

The BoD is directly responsible for establishing, approving and overseeing the implementation and maintenance of an effective policy to prevent, identify, manage and record actual and potential conflicts of interest at the Group level. The framework for managing, reporting and escalating conflicts of interest is undertaken within Group Compliance and is outlined in the Conflicts of Interest Policy and related Instruction. The Group maintains a Conflicts of Interest Register for documenting inherent and live conflicts. The Designated Group Conflicts Officer is responsible for reporting conflicts of interest to the ELT and the BoD at least annually.

Subprinciple 4.13: Group Compliance is responsible for overseeing and ensuring the integrity, independence and effectiveness of the whistleblowing procedures

The Whistleblowing Policy is administered by the Head of Surveillance & Investigation in Group Compliance. The Whistleblowing Policy sets out the principles and standards for the management of whistleblower reports regarding breaches and identifies related roles and responsibilities. The whistleblowing scheme is managed by the Whistleblowing Operations Team in Group Compliance, who must have effective and robust processes in place to ensure that all reported potential breaches are properly investigated and that the confidentiality of whistleblowers is fully protected in accordance with the Whistleblowing Policy and applicable legislation.

Subprinciple 4.14: Group Compliance is responsible for conducting referred investigations within the Group relevant countries, branches and legal entities

Group Compliance is responsible for reviewing any suspicion of customer wrongdoing or employee misconduct referred to it that falls outside of the business as usual or where such suspicion could expose the Group to material financial or reputational risk, as well as regulatory scrutiny or enforcement action. All instances where employees are suspected of colluding with a customer for possible illicit activity must be referred to Group Compliance for investigation.

Subprinciple 4.15: Group Compliance is responsible for independent reporting on matters relating to Regulatory Compliance, Financial Crime and Conduct Risks

The Chief Compliance Officer as a member of the ELT has a day-to-day direct reporting line to the Chief Executive Officer and also direct access to the BoD for matters requiring escalation. The Chief Compliance Officer provides quarterly written compliance reports to the ELT and BoD.

Group Compliance reports are expected to contain an overall assessment of the primary risk areas overseen by Group Compliance and describe the implementation and effectiveness of the control environment. This includes a summary of identified risks and corrective measures. Reporting should also include insights on the potential strategic business risks (as related to the areas overseen by Group Compliance).

In addition to written reports, sound practice dictates that the Chief Compliance Officer (or delegate) also provides an oral presentation of the report to allow the ELT and BoD to ask questions and discuss relevant issues.

5. Escalation and the right of Group Compliance to conduct investigations of possible breaches of the Policy

Where a breach or potential breach of the Policy has been identified and could constitute a problematic case, as defined by the Escalation Policy, the escalation protocol as outlined in that policy must be followed.

Group Compliance retains the right to undertake an investigation into the root causes and make recommendations to address deficiencies in controls or ineffective risk management where it concerns the areas overseen by Group Compliance.

To safeguard the independence of the function it may be appropriate to appoint an independent outside expert to perform this task. Any report resulting from such investigation may need to be limited in its circulation and may be provided directly to the BoD or the Chairman of the BoD. Where required, the report may be provided to supervisors, regulators, competent authorities and/or law enforcement agencies. This does not limit the power of the Conduct & Compliance Committee to undertake its constitutional function for providing general oversight of investigations concerning regulatory and financial crime compliance, and/or litigation and enforcement.