

Group Compliance Policy

22 June 2023

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, including the spirit of the law extremely seriously. Demonstrating compliance is a core part of how we do business, which is critical to maintaining the trust of our customers and protecting the interests of our stakeholders.

The Group Compliance Policy (this "Policy") sets the principles and standards for managing Compliance Risks across the Group and describes key roles and responsibilities of the independent Group Compliance function in supporting the Group to remain compliant with applicable laws, rules and regulations.

This Policy is designed to meet laws, rules, regulations and sound practice applicable to the compliance function and the management of Compliance Risks. These include: the Danish Financial Supervisory Authority's Executive Order on Management and Control of Banks no. 1103 from 30 June 2022, Executive Order on Management and Control of UCITS No. 865, Executive Order on Management and Control of Insurance Companies and Multi-Employer Occupational Pension Funds No. 1723, European Banking Authority Guidelines on Internal Governance EBA/GL/2021/05 2 July 2021, Basel Committee on Banking Supervision guidance for Compliance and the Compliance Function in Banks, European Securities and Market Authority Guidelines on certain aspects of the MiFID compliance function requirements.

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

2. Definitions

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

Board of Directors	the Board of Directors of Danske Bank A/S. When this Policy is adopted by a Subsidiary, references to the Board of Directors may be understood to mean the respective roles and responsibilities of the management body responsible for setting the strategy, objectives and overall direction of the Subsidiary.
Branch	foreign establishment through which Danske Bank A/S provides banking or other financial services within a host country (either within the EEA or otherwise within a third country) based on its home country registration with the Danish Financial Supervisory Authority.
Compliance Culture	a culture where all Employees, managers and members of the Board of Directors feel empowered to take active steps to ensure that the Group remains compliant with applicable laws, rules and regulations.
Compliance Oversight Assessments	specific reviews undertaken by Group Compliance to assess the frameworks put in place by Group Risk Management and 1 st Line Specialist Functions to manage Compliance Risks.
Compliance Risk	the risk of incurring legal and regulatory sanctions, or material financial loss, causing adverse outcomes for customers, markets or society, or loss of reputation, as a result of the Group's failure to comply with laws, rules, regulations and Governing Documents applicable to the Group's activities.
Compliance Breach	non-compliance with applicable laws, rules, regulations and/or Governing Documents within Group Compliance's primary oversight mandate and where there are no registered exemptions.

Compliance Risk Profile	a point in time view of the Group's aggregate Compliance Risk exposures across each Enterprise Risk Management Policy ("ERM") category within Group Compliance's primary oversight mandate, based on a combination of factors including, but not limited to, risk assessments, risk/control indicators, outcome of applicable monitoring and oversight activities, and identified emerging risks.
Conduct Risk	the risk that the Group's behaviour, in supplying financial services, causes customer detriment and/or damages the integrity of financial markets. the Executive Leadership Team of Danske Bank A/S.
Executive Leadership Team	When this Policy is adopted by a Subsidiary, references to the Executive Leadership Team may be understood to mean the respective roles and responsibilities of the board of management ¹ or such person as appointed to undertake the responsibility for that Subsidiary.
Employee	a permanent or temporary Employee of the Group, a contingent worker, or an individual which is working for the Group but is not directly employed by the Group (including officers, consultants, contractors, agency workers, etc.)
Financial Crime Risk	the risk of internal or external parties using the Group's infrastructure, products and services to move and conceal proceeds of criminal conduct, defraud, manipulate or circumvent applicable rules, laws and regulations, particularly in the areas of money laundering, terrorist financing, economic sanctions as well as bribery and corruption, fraud and tax evasion.
Group	Danske Bank A/S including its Branches and Subsidiaries.
Group Compliance	a permanent and independent function within the Group, which forms part of the 2 nd line of defence with primary oversight responsibilities for Regulatory Compliance Risk, Financial Crime Risk, Conduct Risk and Sustainability Compliance Risk
Governing Documents	documents through which the Board of Directors, Executive Leadership Team or the relevant Subsidiary Board and Subsidiary Executive Management set out policies principles, strategy, guidelines, instructions and business procedures for the proper operation of the Group.
Regulator	a financial supervisory authority, competition authority or data protection authority that oversees the Group's activities and that has the authority to initiate regulatory issues.
Regulatory Compliance Risk	The risk of incurring legal and regulatory sanctions, material financial loss, causing serious/systemic unfair customer outcomes, detriment to data subjects, damaging the integrity of financial markets or suffering loss of reputation, as a result of the Group's failure to comply with laws, rules, regulations and Governing Documents, applicable to the Group's activities in the areas of treating customers fairly, market integrity, data protection and confidentiality and breach of licensing, accreditation and registration requirements.
1st Line Specialist Functions	Functions in the 1 st line of defence that are responsible for designing and maintaining effective risk management frameworks within their respective areas of responsibility (e.g. Group HR, Group Legal, CFO Area and Technology & Services).
Subsidiary	any undertaking over which Danske Bank A/S exercises control ² .
Sustainability Compliance Risk	Sustainability Risk (as defined in the ERM) to the extent that it relates to Financial Crime Risk, Regulatory Compliance Risk and Conduct Risk.
Subsidiary Compliance	a permanent and independent function responsible for compliance matters within a Subsidiary (this function may be undertaken by Group Compliance where so agreed with the Subsidiary and where this does not contravene local law).

¹ Responsible for executing the strategy, objectives and overall direction of the Subsidiary set by the supervisory body.

² For the purpose of this definition "Control" means any of the following: (i) direct or indirect ownership of more than fifty per cent (50%) of the share capital or other ownership interest in any other person; (ii) the direct or indirect right to exercise more than fifty per cent (50%) of the votes in any other person; (iii) the direct or indirect contractual right to designate more than half of the members of such person's board of directors or similar executive body, (iv) direct or indirect ownership of fifty per cent (50%) or less of the share capital or other ownership interest in any other person, where such minority ownership according to local law is considered controlling interest.

3. Scope

This Policy outlines the framework for the management of all Compliance Risks in the Group, as well as the specific roles and responsibilities of Group Compliance. Group Compliance has primary responsibility for the oversight of Financial Crime Risk, Regulatory Compliance Risk, Conduct and Sustainability Compliance Risk (including, all associated underlying Level 2 and Level 3 risk types as applicable). Group Compliance is required to exercise oversight of risk areas for which primary responsibility rests with Group Risk Management and 1st Line Specialist Functions. This oversight is delivered through the Compliance Oversight Assessment framework. The scope of Group Compliance's oversight is illustrated in Figure 1.

Figure 1 - Scope of Group Compliance

Financial Crime Risk	Regulatory Compliance Risk
<ul style="list-style-type: none"> • Money Laundering • Terrorist Financing • Sanctions Violations • Tax Evasion • External Fraud • Internal Fraud • Bribery and Corruption 	<ul style="list-style-type: none"> • Treating Customer Fairly • Personal Data Protection & Confidentiality • Market Integrity • Licensing, Accreditation and Registration Requirements
Conduct Risk	
Sustainability Compliance Risk	
Additional Risk Oversight Areas	
<p>Group Risk Management and 1st Line Specialist Functions assess, control and monitor adherence to the risk management frameworks under their ownership. This includes ensuring alignment of these risk management frameworks with relevant laws, rules, regulations and Governing Documents. Group Compliance undertakes specific Compliance Oversight Assessments to evaluate the adequacy and effectiveness of these frameworks (as outlined in Principle 5).</p>	

3.1. Target group

This Policy is established by the Board of Directors and applies to all Employees, business units, group functions, Subsidiaries and Branches of the Group. All other natural persons or legal entities (such as contractors, suppliers, consultants, agents, intermediaries, introducers, brokers, business advisors, joint ventures), acting for or on behalf of the Group, must agree to comply with this Policy when acting on behalf of the Group.

The management body of a Subsidiary may approve this Policy with deviations to ensure this Policy is fit for purpose for the Subsidiary. The policy administrator in the Subsidiary should discuss the rationale behind the deviation and ensure that the administrator of the Group Policy is consulted on material deviations.

The administrator of this Policy must document and report material deviations from this Policy to the owner of this Policy.

When this Policy is adopted by a Subsidiary, references to the Board of Directors and Executive Leadership Team should be understood as meaning the responsibilities undertaken by the board of directors and board of management of that Subsidiary. When adopted by Subsidiaries, references to the Chief Compliance Officer should be read, as meaning the Head of Subsidiary Compliance or equivalent appointed person with responsibility for compliance matters for the Subsidiary. Specific roles and responsibilities between Group Compliance and each Subsidiary may be documented in separate intra group outsourcing/internal service transfer agreements (as detailed in Subprinciple 4.11).

4. Policy Content

Principle 1: Activities in the Group are conducted in a compliant manner

The Board of Directors is ultimately accountable for the Compliance Risks undertaken by the Group, where the Executive Leadership Team retains management responsibility for implementing appropriate systems, processes, and controls to identify and manage Compliance Risks. The Executive Leadership Team is also responsible for following up on the conclusions and recommendations from the Chief Compliance Officer and, where appropriate, implementing corrective measures. The Executive Leadership Team is responsible for implementing and ensuring adherence to this Policy, supported and advised by Group Compliance.

The Group must conduct its activities in adherence with applicable laws, rules, regulations and risk tolerance set by the Board of Directors to manage Compliance Risks. In undertaking its activities, the Group is exposed to Compliance Risk, which is an inherent element of doing business and as such must be considered when developing and/or executing the Group's business strategy. 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 a responsibility for compliance regardless of their position within the Group.

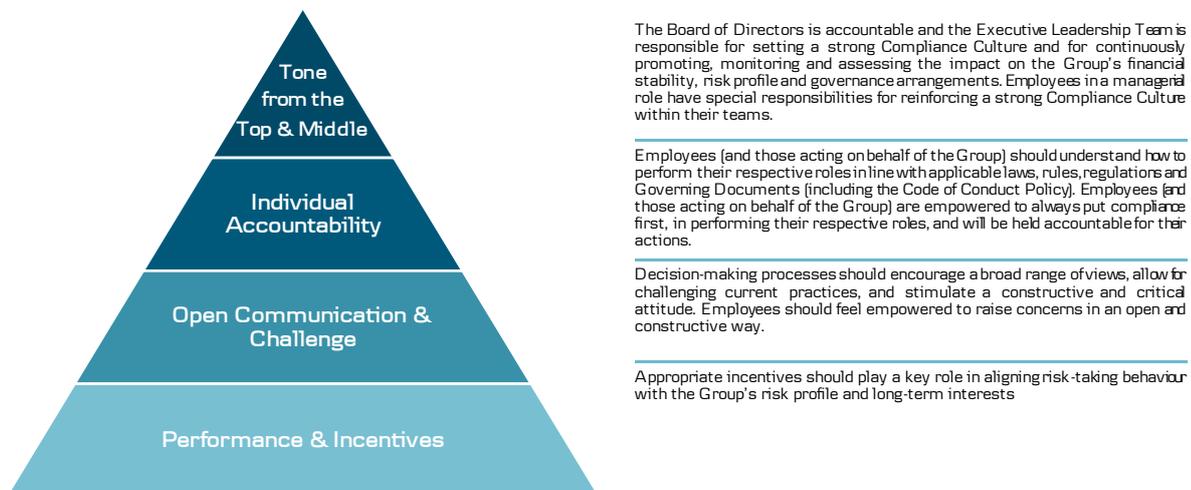
Subprinciple 1.1: All Employees have a responsibility to help maintain a strong Compliance Culture

A strong Compliance Culture means all Employees, and any other natural person or legal entity, acting for or on behalf of the Group, understand the Compliance Risks relevant for their respective roles and are empowered to take active steps to ensure the Group remains compliant with applicable laws, rules, regulations, and Governing Documents. This is a core part of the Group’s overall sound business culture, as outlined in the Code of Conduct Policy.

A strong Compliance Culture begins with the 1st line of defence and is reinforced by a framework of Governing Documents set by the 2nd line of defence³, as well as through role-modelling and incentivising ethical conduct, implementing appropriate governance, including monitoring and reporting mechanisms, relevant policies, instructions and systems, ongoing training and awareness.

Strong leadership from the Board of Directors and Executive Leadership Team is fundamental in promoting awareness and equipping Employees to do their job properly in alignment with sound risk management principles and practices.

Figure 2 - Strong Compliance Culture



The Board of Directors and Executive Leadership Team, supported and advised by Group Compliance, must play a key role in developing, embedding and maintaining a strong Compliance Culture across the Group. This is achieved in a number of ways including:

- setting and embedding appropriate Compliance Risk 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”,
- ensuring that there are suitable training and awareness programmes that empower managers and Employees to be, and to help each other to remain compliant,
- maintaining effective incentive and reward practices that reinforce ethical conduct,
- removing barriers to ethical conduct e.g. by maintaining systems, tools and other workplace factors to encourage speaking up,
- setting clear expectations for compliance through comprehensive requirements in Governing Documents,
- 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.

Subprinciple 1.2: The Group conducts its business in line with applicable Compliance Risk tolerances for Regulatory Compliance, Financial Crime, and Conduct Risks.

Each business unit, group function and Subsidiary is expected to consider the impact of their activities on the Compliance Risk profile of the Group and take effective measures to ensure alignment with the Group’s risk tolerance for Regulatory Compliance, Financial Crime and Conduct Risks as defined below.

³ In line with the ERM, risk policies and instructions are defined by the 2nd line of defence. In instances where a 1st Line Specialist Functions set risk standards or methods at the policy or instruction level, the 2nd line is to be engaged to challenge the policy or instruction to ensure its authority and effectiveness for risk management.

Financial Crime Risk

- The Group is committed to act in compliance with applicable laws, rules and regulations in all the jurisdictions where it operates including those relevant to the prevention of financial crimes such as money laundering, terrorist financing and sanctions breaches.
- The Group has implemented and continues to enhance its processes and controls to reduce the impact and likelihood of Financial Crime.
- The Group seeks to limit the potential for exposure to financial crime through having robust systems, processes and controls including but not limited to risk-based customer due diligence, transaction monitoring, sanctions screening and suspicious activity reporting.

Regulatory Compliance Risk

- The Group is committed to act in compliance with applicable laws, rules and regulations in all the jurisdictions where 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 another jurisdiction and conducting permissible cross-border activity.
- The Group 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, processes 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 requires all Employees to always act in accordance with applicable laws, rules and regulations 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 quickly and decisively mitigate any negative customer, regulatory or reputation impacts, if this occurs.

Principle 2: The Board of Directors and Executive Leadership Team take appropriate measures and provide adequate resources to enable Group Compliance to undertake its legal and regulatory responsibilities and maintain its independence

The Board of Directors must appoint a Chief Compliance Officer, who is the Head of Group Compliance. The Chief Compliance Officer is a member of the Executive Leadership Team and is responsible for ensuring adequate governance arrangements are in place within the Group Compliance function to enable the function to undertake the mandate provided by the Board of Directors and applicable regulatory requirements. This also implies solid collaboration with all parts of the Group and the capability to support and challenge business units, group functions and Subsidiaries in the efforts to do the right thing for our customers, colleagues and society.

The Executive Leadership Team must ensure that adequate resources are available to achieve the Board of Directors' objective of managing Compliance Risks effectively, ensuring independence of Group Compliance and meeting relevant regulatory requirements.

Principle 3: The Chief Compliance Officer may delegate specific responsibilities to ensure efficient operation of Group Compliance

The Chief Compliance Officer retains the right to delegate specific elements of the mandate for the role to enable Group Compliance to function efficiently and effectively in providing oversight of the Group's compliance activities.

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

In managing Compliance Risks, the Executive Leadership Team and/or the Chief Compliance Officer, within the limits of each respective mandate, can delegate duties and responsibilities to sub-committees and other relevant fora to provide:

- adequate and coordinated oversight of relevant Compliance Risks overseen by Group Compliance,
- 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 Board of Directors, be undertaken directly. The accountability for performance of activities delegated by the Chief Compliance Officer will ultimately remain with the Chief Compliance Officer.

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

Group Compliance is a permanent and independent function, which forms part of the 2nd line of defence with primary oversight responsibilities for Regulatory Compliance, Financial Crime, Conduct and Sustainability Compliance Risks.

Group Compliance is responsible for risk-based monitoring and assessing whether the Group's methods and procedures are suitable to identify, manage and reduce the risk of non-compliance. Further, Group Compliance is responsible for testing, using a risk-based approach, whether the Group has sufficient and effective controls in place to identify, manage and reduce the risk of non-compliance with applicable laws, rules and regulations, as well as measures taken to address any deficiencies, are effective.

The Board of Directors and Executive Leadership Team should take reasonable steps to ensure that the independence of Group Compliance is not compromised. In addition:

- The Chief Compliance Officer should be free from any conflicts of interest that may impede the independent and objective performance of the role or which may subject the role holder to undue or inappropriate influence.
- The Chief Compliance Officer must have direct access to the Board of Directors to maintain independence. Additionally, direct reports of the Chief Compliance Officer, (or other roles in Group Compliance where specifically mandated), may approach the Board of Directors 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, Group Data Protection Officer).
- Group Compliance must be provided with the means to recruit and retain 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 4.10 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 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 reporting to the Executive Leadership Team, the Conduct & Compliance Committee and the Board of Directors on matters relating to Regulatory Compliance, Financial Crime, Conduct and Sustainability Compliance Risks (see Subprinciple 4.16 for more details).

Furthermore, Group Compliance is required to develop and implement a structured and well-defined compliance programme setting out its planned activities. The compliance programme should be risk-based, aligned with the Group's strategic business plan 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 the management of Regulatory Compliance, Financial Crime, Conduct and Sustainability Compliance Risks consistent with the ERM⁴

The Group Compliance framework articulates the function's approach to identify, measure, manage, report and escalate Compliance Risks which have a material impact on the Group's Compliance Risk Profile and the delivery of the Group's strategy. Group Compliance's approach is consistent with the ERM Policy which defines how the Group manages all risk types.

The framework includes the Group Compliance strategy, Compliance Risk tolerances (set by the Board of Directors), governance and committee structures, the compliance programme, Governing Documents issued by Group Compliance, including this Policy, and processes and systems supporting the effective management of Compliance Risks (see Figure 3). The Group's Compliance

⁴ The risk management framework for Sustainability is jointly maintained by Group Risk Management and Group Compliance.

framework is underpinned by the capability of its Employees and a strong Compliance Culture. A key component of the framework is clear articulation of the roles and responsibilities for managing Regulatory Compliance, Financial Crime and Conduct Risks.

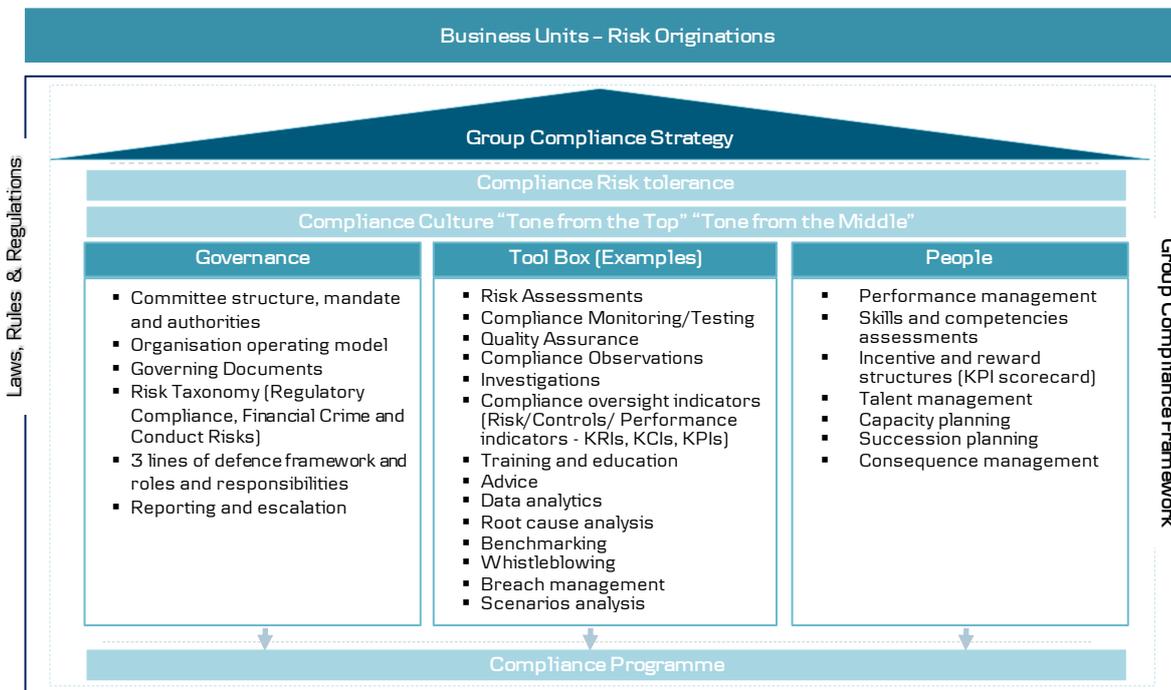
Group Compliance is responsible for overseeing Regulatory Compliance, Financial Crime, Conduct and Sustainability Compliance Risks and for providing advice, guidance and challenge to the 1st line of defence as described in Subprinciple 4.5. This includes providing support and fostering ongoing awareness. 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 Board of Directors has established the Conduct & Compliance Committee, which is responsible for the preparatory work for the Board of Directors with respect to conduct and reputational risk, compliance, financial crime and any other matters, which the Board of Directors may want to have examined by the Committee. The Group has also established the Compliance Risk Committee to discharge the obligations of the Group All Risk Committee for the oversight and challenge of the Group's Compliance Risk profile.

Additionally, the Chief Compliance Officer (or delegate cf. Principle 3 above) should be a permanent member of all Executive Leadership Team committees mandated to address matters relevant to Regulatory Compliance, Financial Crime, Sustainability Compliance or Conduct Risks. Group Compliance may also participate in other committees, where there are specific agenda items discussed related to Regulatory Compliance, Financial Crime, Conduct or Sustainability Compliance Risks.

Group Compliance assesses, in a risk-based manner, the possible impact of legal & regulatory changes on the Group's Financial Crime, Regulatory Compliance, Conduct and Sustainability Compliance Risk framework and risk profile and advises on implementation of related requirements.

Figure 3 - Group Compliance framework



The Group operates within an internal control environment underpinned by a “three lines of defence model” as described by the ERM. In this model, Group Compliance as a 2nd line of defence function (i) sets the framework for managing Regulatory Compliance, Financial Crime, Conduct and Sustainability Compliance 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 Executive Leadership Team and to the Board of Directors.

The 1st line of defence owns the management of Compliance Risks and is responsible for identifying, assessing, managing and reporting Compliance Risks and issues in accordance with the Group Compliance framework (including reporting on Compliance Risk management activities and control effectiveness).

Subprinciple 4.2: Group Compliance establishes and maintains Governing Documents for the management of Regulatory Compliance, Financial Crime, Conduct and Sustainability Compliance Risks

Group Compliance is responsible for establishing and maintaining Governing Documents in line with applicable laws, rules and regulations within the jurisdictions in which the Group operates. This includes advice and guidance to the Executive Leadership Team and Board of Directors on specific Compliance Risks requiring a policy response. The establishment and maintenance of Governing Documents may extend to Subsidiaries and Branches, where it is appropriate to do so and whilst maintaining the legal entity integrity of Subsidiaries.

Group Compliance supports the Group to implement Governing Documents issued by Group Compliance. Implementation involves communicating requirements, providing training, as well as advising, guiding and challenging the suitability and effectiveness of controls, tools and systems to meet Governing Documents requirements.

Group Compliance is also mandated by regulation to participate in the establishment and review of relevant Governing Documents maintained by other areas in the Group (specifically for the ones related to Remuneration and Product Governance) to ensure compliance with applicable laws, rules, regulations, and alignment with existing Governing Documents maintained by Group Compliance.

Subprinciple 4.3: Group Compliance undertakes Compliance Risk assessments for Regulatory Compliance, Financial Crime and Conduct Risks

Group Compliance designs and maintains a compliance risk assessment methodology and appropriate tools, which allows effective assessment of inherent and residual risks which are overseen by Group Compliance. Group Compliance executes independent compliance risk assessments using this methodology⁵ and tools.

Compliance risk assessments are used to prioritise the focus of monitoring, testing, training, management of governing documents and advisory activities performed by Group Compliance.

Compliance risk assessment results should also be used by the Group to inform the design, development, maintenance and implementation of the Group's controls framework to mitigate Regulatory Compliance, Financial Crime and Conduct Risks.

Ad hoc compliance 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 4.4: Group Compliance performs monitoring and testing activities for Regulatory Compliance, Financial Crime, Conduct and Sustainability Compliance Risks

Group Compliance is responsible for monitoring and assessing whether the Group's methods and procedures are suitable to identify, manage and reduce the risk of non-compliance with applicable laws, rules and regulations.

Group Compliance is also responsible for testing whether the Group has sufficient and effective controls in place, and that measures taken to address deficiencies are effective.

A risk-based approach is used to prioritise monitoring and testing activities based on regulatory expectations, outcomes of risk assessments and other relevant information. This monitoring and testing is in a 2LoD capacity and does not substitute the 1LoD's responsibility to ensure they appropriately manage the risks owned by them.

Subprinciple 4.5: Group Compliance provides independent advice and assistance to the Board of Directors, Executive Leadership Team and 1st line of defence

Group Compliance advises the Board of Directors and the Executive Leadership Team (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 Documents. Furthermore, Group Compliance provides independent advice to the 1st line of defence on whether the day-to-day business activities and/or controls are compliant and in line with Governing Documents, 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 Documents and/or compliant with applicable laws, rules and regulations. Group Compliance Employees may escalate to the Chief Compliance Officer, decisions, actions or activities undertaken by the Group which poses a risk of non-compliance.

Subprinciple 4.6: Group Compliance provides relevant training on Regulatory Compliance, Financial Crime, Conduct and Sustainability Compliance Risks

⁵ Group Compliance's Group-wide Risk Assessment is an independent methodology, but it is aligned to the ERM and its taxonomy.

Group Compliance provides regular mandatory compliance training to all relevant Employees across the Group based on an assessment of training needs. Such training enables Employees to fulfil their responsibilities in respect to adherence with laws, rules, regulations and requirements set in Governing Documents. Training is provided on an on-going basis so that it takes into account relevant changes.

Group Compliance is also responsible for providing specific training on sound practice for the management of risks overseen by Group Compliance to the Executive Leadership Team, as well as offering and, upon request, facilitating appropriate training to the Board of Directors.

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

Separately, Group Compliance provides oversight and challenge to ensure specific training needs within the 1st line of defence are identified and subsequent training is designed by 1st line of defence to meet relevant regulatory requirements.

Subprinciple 4.7: Group Compliance is responsible for coordinating and supporting all material regulatory engagements across the Group.

Group Compliance provides the Regulatory Affairs function, the central unit that supports and coordinates all material regulatory engagements across the Group and administers the Regulatory Engagement Policy. The ownership and delivery of regulatory engagements is the responsibility of the business units, group functions and Subsidiaries involved. Regulatory Affairs is involved in all material regulatory engagements. Regulatory Affairs sets out the processes and requirements to be followed in the management and registering of regulatory engagements.

Subprinciple 4.8: Group Compliance provides the data protection compliance function, including the role of Group Data Protection Officer

The Group Data Protection Officer, supported by Data Protection Compliance, oversees compliance with the General Data Protection Regulation, European ePrivacy law and applicable national data protection laws.

Subprinciple 4.9: 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, product launches and major transactions (together "Major Decisions"⁶). In keeping with Subprinciple 4.5, 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 Board of Directors for consideration where there is an actual or potential material risk of non-compliance, or the decision is inconsistent with the risk tolerance 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 Board of Directors.

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. This includes known forthcoming changes and obligations on identifying and assessing Financial Crime Risk associated with the new or amended product/service or business practice (Financial Crime Product Risk Assessment). 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 process⁷. 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

⁶ While *Major Decision* is not a specifically defined term in the Policy, Group Compliance would expect reasonable judgement to be applied to any decision, change project, strategic initiative, product launch or transaction. Where there is uncertainty about interpretation, advice should be sought from Group Compliance.

⁷ See Product Governance Policy for NAPA for details of the Group's process.

requirements. To the extent required by applicable laws, rules and regulations, Subsidiaries must allocate necessary resources to monitor relevant product governance arrangements.

Subprinciple 4.10: 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 from across the Group to carry out its duties and to enable the function to provide independent information to the Board of Directors and Executive Leadership Team. This includes, but is not limited to, access to all relevant databases, records and information on customer complaints. The Executive Leadership Team is responsible for disclosing information to the Chief Compliance Officer assessed as significant to the role of the Chief Compliance Officer and/or to the proper operation of the function.

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

This applies to all business units, group functions and Subsidiaries.

Subprinciple 4.11: The Executive Leadership Team and Board of Directors must have appropriate reporting structures to enable aggregation and presentation of Regulatory Compliance, Financial Crime and Conduct Risks relevant to the Group as a single consolidated entity

Executive Leadership Team and Board of Directors must maintain a functional reporting structure to allow timely reporting and escalation of Regulatory Compliance, Financial Crime and Conduct Risks across the Group.

All agreed reporting structures must be in accordance with relevant laws, rules and regulations applicable to the Branch or Subsidiary. Any such structure should enable Group Compliance to understand, aggregate and present relevant risks, which might impact the Regulatory Compliance, Financial Crime or Conduct Risk profile of the consolidated Group.

Where appropriate and consistent with local legislation, Branches of the Group, Subsidiaries, or connected parties may enter into formal intra group outsourcing/internal service transfer agreements with Group Compliance.

Subprinciple 4.12: Group Compliance cooperates with Group Legal, Group HR, Group Risk Management and Group Internal Audit

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

In particular, Group Compliance and Group Risk Management cooperates and exchanges 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 (1) the development, maintenance and enhancement of the ERM (to the extent it impacts the effective management of Compliance Risks) in order to effectively identify, assess, manage and report relevant risks, and (2) other policies, regulatory controls and frameworks (such as Remuneration Policy, reputational risk) which Group Compliance is reliant on to discharge its responsibilities.

Subprinciple 4.13: Group Compliance is responsible for the conflicts of interest framework

The Board of Directors is 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 Governing Documents. The Group maintains a Conflicts of Interest Register for documenting live conflicts and a Conflicts of Interest Catalogue for recording inherent conflicts. The designated Group Conflicts Officer is responsible for providing a report on conflicts of interest to the Executive Leadership Team and the Board of Directors at least annually.

Subprinciple 4.14: Group Compliance is responsible for overseeing and ensuring the integrity, independence and effectiveness of the whistleblowing procedures

The Whistleblowing Policy is administered by Group Compliance and sets out the principles and standards for the management of whistleblowing reports regarding breaches and identifies related roles and responsibilities. The whistleblowing scheme is managed by Whistleblowing Operations 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 laws, rules and regulations.

Subprinciple 4.15: Group Compliance is responsible for conducting referred investigations across the Group

Group Compliance is responsible for investigating allegations that indicate customer wrongdoing and/or Employee misconduct and/or other threats to the integrity of the Group that might expose the Group to material financial or reputational risk, regulatory scrutiny or enforcement action. Instances where Employees are suspected of colluding with a customer in possible illicit or criminal activity, must be referred to Group Compliance who determines whether to conduct an investigation. Where allegations relate to Group Compliance, these should be directed to Group Internal Audit, to avoid any conflict of interests. Group Internal Audit will investigate or will task Compliance Investigations to investigate if Group Internal Audit considers appropriate and secure to do so; in the latter case Group Internal Audit will exercise oversight over the investigation.

Subprinciple 4.16: Group Compliance is responsible for independent reporting on matters relating to Regulatory Compliance, Financial Crime, Conduct and Sustainability Compliance 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 direct access to the Board of Directors for matters requiring escalation. The Chief Compliance Officer provides quarterly written compliance reports to the Executive Leadership Team, Conduct & Compliance Committee and Board of Directors. Group Compliance may also provide additional reporting where the Chief Compliance Officer deems appropriate.

Group Compliance reports should provide a clear picture of the Group's material Compliance Risks and include insights on the potential strategic business risks (as related to the areas overseen by Group Compliance). Group Compliance reports should also describe the implementation and effectiveness of the overall control environment and provide a summary of identified risks and measures required to reduce or mitigate these risks.

Specific areas of coverage for Group Compliance reporting include, but are not limited to:

- the adequacy and effectiveness of the Governing Documents set by Group Compliance,
- key changes and developments in applicable laws, rules and regulations within Group Compliance's primary oversight mandate,
- a summary of the Group Compliance structure and resources,
- a summary of material findings and recommendations from Group Compliance, including on Compliance Breaches, deficiencies in the Group's organisation and/or compliance process,
- a summary of actions taken to address any significant risk of failure to comply with the obligations under the applicable laws, rules and regulations,
- material deviations by the 1st line of defence from important recommendations or assessments issued by Group Compliance,
- material regulatory engagements and regulatory issues relevant to Group Compliance,
- information in relation to product governance as required by applicable regulations,
- a summary of complaints, resolutions and any key trends,
- any additional reporting requirements as defined by the Board of Directors or committed to a specific Regulator (e.g., the Rules of Procedure or guidelines from the Board of Directors).

In addition to written reports, sound practice dictates that the Chief Compliance Officer (or delegate) also provides an oral presentation of quarterly reports (and other reports where necessary) to allow the Executive Leadership Team, Conduct & Compliance Committee and Board of Directors to ask questions and discuss relevant issues.

Subprinciple 4.17: Group Compliance maintains an effective service delivery framework in line with relevant outsourcing requirements

Business units, group functions, Subsidiaries and Branches are accountable for managing their Compliance Risks. The responsibility for specific 2nd line compliance activities may be outsourced or transferred internally to Group Compliance. In those instances, Group Compliance may appoint local compliance officers to provide specific compliance services in agreement with the management of relevant business units, group functions, Subsidiaries and Branches.

Group Compliance maintains an appropriate framework to manage and report on the delivery of compliance services to the Group's subsidiaries and Branches who are responsible for participating in the production, implementation and maintenance of relevant service delivery documentation and for providing prompt and appropriate access to information and personnel as necessary to execute such services.

To maintain Group-wide continuity and independence, appointed local compliance officers and Subsidiary Compliance must have a mechanism for reporting material issues to senior staff in Group Compliance and thereby ultimately through to the Chief Compliance Officer.

Principle 5: Group Risk Management and 1st Line Specialist Functions are responsible for managing specific Compliance Risks. Group Compliance is responsible for performing Compliance Oversight Assessments on these areas.

Group Risk Management and 1st Line Specialist Functions are responsible for designing and maintaining effective risk management frameworks (i.e., processes and control requirements, as well as Governing Documents) to manage Compliance Risks within their respective areas of responsibilities. Group Risk Management and 1st Line Specialist Functions also assess, control, and monitor adherence to these frameworks under their ownership.

Group Compliance supports the Group to remain compliant with applicable laws, rules and regulations by conducting Compliance Oversight Assessments, in line with the expectations of local Regulators, to:

- evaluate the suitability and effectiveness of the frameworks put in place by Group Risk Management and 1st Line Specialist Functions to identify and reduce Compliance Risks,
- assess and challenge whether the measures taken to address any identified deficiencies are effective.

Group Compliance undertakes Compliance Oversight Assessments on a two-year cycle.

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

Where a breach or potential breach of this Policy has been identified, an Employee should notify an immediate manager, main contact in the relevant 1st line of defence business control functions and/or designated compliance officer. Where the breach is also defined as an event, this must be registered and categorised immediately in ORIS according to the Non-Financial Risk Event Escalation Instruction.

Group Compliance retains the right to undertake an investigation, or require the relevant department 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 Board of Directors or the Chairman of the Board of Directors. Where required, the report may be provided to Regulators 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.

6. Review

This Policy is reviewed and updated at least annually. The changes must be endorsed by the Executive Leadership Team and the Conduct & Compliance Committee and approved by the Board of Directors.