Danske Bank

Group Compliance Policy

23 June 2021

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

The Policy is designed to meet applicable laws, rules and regulations for the compliance function and the management of Compliance Risks. Key regulations include: Executive Order on Management and Control of Banks No. 1706, 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, EBA Guidelines on Internal Governance EBA/GL/2017/11, Basel Committee on Banking Supervision guidance for Compliance and the Compliance Function in Banks, ESMA35-36-1952 Guidelines on certain aspects of the MiFID compliance function requirements.

Failure to comply with the Policy is a serious violation and may lead to action being taken in accordance with applicable employment legislation, including but not limited to warning, redundancy, suspension or dismissal.

2. Definitions

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

BoD	The Board of Directors of Danske Bank A/S. When the Policy is adopted by a Subsidiary, references to the BoD may be understood to mean the respective roles and responsibilities of the board of directors[1] for that Subsidiary.
Compliance Culture	A culture where all Employees, managers and members of the BoD feel empowered to take active steps to ensure the Group remains compliant with applicable laws, rules and regulations. A strong Compliance Culture is reinforced through role-modelling and rewarding positive behaviours; implementing appropriate governance and reporting mechanisms; relevant policies, instructions and systems; as well as, ongoing training and awareness.
Compliance Oversight Assessments	Specific reviews undertaken by Group Compliance to assess the frameworks put in place by Group Risk Management and 1st Line Specialist Functions to manage Compliance Risks.

[1] Responsible for setting the strategy, objectives and overall direction of the Subsidiary.

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, regulations and Governing Information applicable to the Group's activities.
Conduct Risk	The risk that the Group's behaviour, in supplying financial services, causes customer detriment or damages the integrity of financial markets.[2]
ELT	The Executive Leadership Team of Danske Bank A/S. When the Policy is adopted by a Subsidiary, references to the ELT may be understood to mean the respective roles and responsibilities of the board of management[3] or such person as appointed to undertake the responsibility for that Subsidiary.
Employee	For the purpose of the Policy, an Employee is considered to be: • A permanent or temporary Employee of the Group • A contingent worker, individuals who are working for the Group but are 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 established 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.[4]
Group	Danske Bank A/S including all Subsidiaries.
Group Compliance	A permanent and independent function within the Group, which forms part of 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 information that guides Employees across the Group in performing their daily tasks, i.e. policies, instructions and business procedures.
Regulator	All supervisory and regulatory authorities that oversee the Group's activities and that have the authority to initiate regulatory issues. These include but are not limited to financial supervisory authorities, competition authorities and data protection authorities[5].
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 breach of licensing, accreditation and registration requirements.[6]
1st Line Specialist Functions	Functions in the 1st line of defence (e.g. Group HR, Group Legal, CFO Area and Technology & Services) that are responsible for designing and maintaining effective risk management frameworks within their respective areas of responsibility.
Subsidiary	Any undertaking over which Danske Bank A/S exercises control[7].
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).

[2] As defined by the ERM.
[3] Responsible for executing the strategy, objectives and overall direction of the Subsidiary set by the supervisory body.
[4] As defined by the ERM.
[5] As defined by the Regulatory Engagement Policy.
[6] As defined by the ERM.
[7] 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

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. Group Compliance is responsible for the oversight of the following Level 1 risk types, as defined by the Enterprise Risk Management document (the "ERM"): 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 has specific responsibilities for the oversight of additional risk areas. The scope of Group Compliance's oversight is illustrated in Figure 1.

Figure 1 – Scope of Group Compliance

<table>
<tr><th colspan="2">Conduct Risk</th></tr>
<tr><th>Financial Crime Risk</th><th>Regulatory Compliance Risk</th></tr>
<tr><td>• Money Laundering
• Terrorist Financing
• Economic Sanctions
• Client Tax Evasion
• External Fraud
• Internal Fraud
• Bribery & Corruption</td><td>• Treating Customer Fairly
• Data Protection & Confidentiality
• Market Integrity
• Licensing, Accreditation & Registration</td></tr>
<tr><th colspan="2">Additional Risk Oversight Areas</th></tr>
<tr><td colspan="2">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 Information. Group Compliance undertakes specific Compliance Oversight Assessments to evaluate the adequacy and effectiveness of these frameworks (as outlined in Principle 5).

Additionally, Group Compliance performs oversight, including advice and challenge on the application of IT Regulation, where Group Non-Financial Risk is the primary 2nd line oversight function.</td></tr>
</table>

3.1. Target Group

The Policy is established by the BoD 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 the Policy when acting on behalf of the Group.

The management body of any Subsidiary may approve the Policy with deviations to ensure the policy is fit for purpose for the Subsidiary. 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 owner and ultimately to the ELT. The ELT shall report all material deviations from Group Policies to the BoD.

When the Policy is adopted by a Subsidiary, references to the BoD and ELT 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 BoD is ultimately accountable for the Compliance Risks undertaken by the Group, where the ELT retains management responsibility for implementing appropriate systems and controls to identify and manage Compliance Risks. The ELT is responsible for implementing and ensuring adherence to the 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 BoD 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.[8] 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.

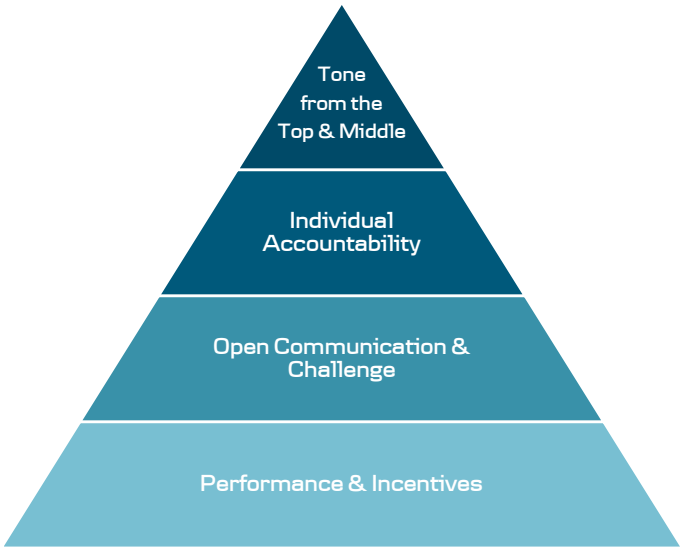
Subprinciple 1.1: All Employees are responsible for maintaining a strong Compliance Culture

A strong compliance culture 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 Information. 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 Information set by the 2nd line of defence.[9]

Strong leadership from the BoD and ELT 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 BoD is accountable and the ELT is responsible for setting a strong Compliance Culture and for continuously promoting, monitoring and assessing the impact on the Group's financial stability, risk profile and governance arrangements. Employees in a managerial role have special responsibilities for reinforcing this strong Compliance Culture within their teams.

Employees (and those acting on behalf of the Group) should understand how to perform their respective roles in line with applicable laws, rules, regulations and Governing Information (including the Code of Conduct Policy). Employees (and those acting on behalf of the Group) are empowered to always put compliance first, in performing their respective roles, and will be held accountable for their actions.

Decision-making processes should encourage a broad range of views, allow for challenging current practices, and stimulate a constructive and critical attitude. Employees should feel empowered to raise concerns in an open and constructive way.

Appropriate incentives should play a key role in aligning risk-taking behavior with the Group's risk profile and long-term interests.

[8] 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).
[9] 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.

The BoD and ELT, supported and advised by Group Compliance, must play a key role in developing and embedding a strong Compliance Culture across the Group. 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",
- Ensuring that there is suitable training and awareness programmes that empower managers and Employees to remain, and help each other to remain compliant,
- 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 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.

Subprinciple 1.2: The Group conducts its business in line with a sound risk taking approach 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 risk profile of the Group and take effective measures to ensure alignment with the Group's risk taking approach for Regulatory Compliance, Financial Crime and Conduct Risks as defined below.

Financial Crime Risk

- By providing products and services to customers there is an inherent risk that the Group may be used to commit financial crime activities.
- The Group does not tolerate financial crime or any other criminal activity and has implemented, and continues to invest in 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 expose the Group to Financial Crime Risk that cannot be adequately managed. 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 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 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 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 takes appropriate measures and provides adequate resources to enable Group Compliance to undertake its legal and regulatory responsibilities and maintain its independence

The BoD appoints a Chief Compliance Officer, who is a member of the ELT and Head of Group Compliance. The Chief Compliance Officer ensures adequate governance arrangements are in place within the Group Compliance function to enable the function to undertake the mandate provided by the BoD 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 ELT must ensure that adequate resources are available to achieve the BoD's 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 day-to-day business operations.

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 ELT 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 BoD, 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 and Conduct 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 Risk, Financial Crime Risk and Conduct Risk.

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. Further, Group Compliance is responsible for testing 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 BoD and ELT 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 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, 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, 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 reporting to the ELT, the Conduct & Compliance Committee and the BoD on matters relating to Regulatory Compliance, Financial Crime and Conduct 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 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 the management of Regulatory Compliance, Financial Crime and Conduct Risks consistent with the ERM

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

The framework includes the strategy, governance and committee structures, the compliance programme, an approach to sound risk taking, Governing Information owned by Group Compliance, including the Policy, a toolkit and processes and systems aimed at managing Compliance Risks (see Figure 3). The 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 and Conduct 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 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 Committee. The Group has also established the Conduct & Reputational Committee to support the ELT in reviewing Conduct and Reputational risks.

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

Group Compliance assesses the possible impact of any applicable changes in the legal or regulatory environment on the Group's activities and on the Group Compliance framework, and advises and supports the 1st line of defence on implementation as required.

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 the 2nd line of defence (i) sets the framework for managing Regulatory Compliance, Financial Crime 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.

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 Information for the management of Regulatory Compliance, Financial Crime and Conduct Risks

Group Compliance is responsible for establishing and maintaining Governing Information in line with applicable laws, rules and regulations in the jurisdictions within which the Group operates. This includes advice and guidance to the ELT and BoD on specific Compliance Risks requiring a policy response. The establishment and maintenance of Governing Information 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 Information issued by Group Compliance. Implementation involves (but is not limited to) communicating requirements, providing training, as well as advising, guiding and challenging the suitability and effectiveness of controls, tools and systems to meet Governing Information requirements.

Group Compliance is also mandated by regulation to participate in the establishment of other relevant Governing Information (specifically the Group's Remuneration and Product Governance Policies).

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 methodology[10] and tools.

Compliance risk assessments are used to prioritise the focus of monitoring, testing, training, advisory and assistance 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 and Conduct 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 any 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.

Subprinciple 4.5: Group Compliance provides independent advice and assistance to the BoD, 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 the day-to-day business activities and/or controls are compliant and in line with 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 4.9 for details of the Chief Compliance Officer's right to access the BoD).

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

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

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

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

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 Information. Training is provided on an on-going basis so that it takes into account all relevant changes.

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

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 engages, cooperates and communicates with Regulators openly, forthcoming and transparently

The Group, as a provider of a wide range of financial services and products, operates in a highly regulated environment and is required to liaise with different Regulators. The Group has an open, forthcoming and transparent relationship with Regulators. 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 (see the Regulatory Engagement Policy for details).

Subprinciple 4.8: 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, European ePrivacy law 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 4.9: 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 (altogether "*Major Decisions*"[11]). 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 BoD for consideration where there is an actual or potential material 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.

[11] 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.

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 and obligations on identifying and assessing Financial Crime Risk associated with the new or amended product/service or business practice. 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[12]. 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 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 BoD and ELT. This includes access to all relevant databases, records and information on customer complaints.

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 with existing legal limitations.

Subprinciple 4.11: The ELT and BoD 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

ELT & BoD 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 service intra group outsourcing/internal service transfer agreements with Group Compliance to detail the services received.

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

The scope of Group Compliance activities require 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

[12] See Product Governance Policy for NAPA for details of the Group's process.

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 ERM (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 4.13: 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 Governing Information. The Group maintains a Conflicts of Interest Register for documenting live conflicts and 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 ELT and the BoD 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 the 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, and 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 for possible illicit activity or of criminality, must be referred to Group Compliance for investigation. Where allegations relate to Group Compliance, these should be directed to Group Internal Audit.

Subprinciple 4.16: 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, Conduct & Compliance Committee and BoD. Group Compliance may also provide additional reporting.

Group Compliance reports are expected to provide a clear picture of the Group's 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 Information set by Group Compliance,
- Key changes and developments in applicable laws, rules and regulations,
- A summary of the Group Compliance structure and resources,
- A summary of findings and recommendations from Group Compliance, including breaches and deficiencies in the Group's organisation and 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,
- Deviations by the 1st line of defence from important recommendations or assessments issued by Group Compliance,
- Overview of material engagements with and orders from Regulators,
- 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 BoD or committed to a specific Regulator (e.g. the Rules of Procedure or guidelines from the BoD).

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 ELT, Conduct & Compliance Committee and BoD to ask questions and discuss relevant issues.

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 Information) 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 Risk,
- 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 the Policy

Where a breach or potential breach of the Policy has been identified, an Employee should notify an immediate manager, main contact in the Business Risk & Control function and/or designated compliance officer. Such events must be registered and categorised immediately in ORIS according to the Non-Financial Risk 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, 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 BoD or the Chairman of the BoD. 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

The Policy is reviewed and updated at least annually. The changes must be endorsed by the ELT and the Conduct & Compliance Committee, and approved by the BoD.