

# Financial Crime Policy

1 February 2024

## 1. Objective

The objective of the Financial Crime Policy ("this Policy") is to set out the principles for the management of risk and compliance associated with Money Laundering, Terrorist Financing, Sanctions, Bribery, Corruption, Fraud, Tax Evasion and Facilitation of Tax Evasion in the Group.

This Policy is designed to ensure that the Group adheres to:

- Applicable laws and regulations in relation to Financial Crime compliance for the jurisdictions in which it operates; and
- Relevant Sanctions regimes in all jurisdictions in which it operates. These include European Union ("EU"), United Nations ("UN"), United Kingdom and any other applicable Sanctions as appropriate, as well as United States Sanctions to the extent they have extraterritorial application or risk implications for the Group's business activities.

## 2. Definitions

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

<b>Anything of Value</b>	anything a person might consider valuable, as Bribery occurs not only through the means of cash payments or financial transactions.
<b>Associated Person of the Group</b>	any natural person or legal entity, either incorporated or unincorporated, who performs services for or on behalf of the Group. All Employees are Associated Persons of the Group.
<b>Board of Directors</b>	the Board of Directors of Danske Bank A/S
<b>Branches</b>	foreign establishments through which Danske Bank A/S has a registered physical presence and provides banking or other financial services or support service within a host country (either within the EU/EEA or otherwise within a third country) based on its home country registration with the Danish Financial Supervisory Authority or separate third country license.
<b>Bribery</b>	involves the offer, promise, request, acceptance or transfer of Anything of Value either directly or indirectly to or by an individual, in order to improperly induce, influence, or reward the performance of a function or an activity. An act of Bribery does not have to be successful for it to be considered a bribe. The Group considers Facilitation Payments to be Bribery as well.
<b>Business Unit</b>	<ul style="list-style-type: none"> <li>• Personal Customers,</li> <li>• Business Customers and</li> <li>• Large Corporates &amp; Institutions</li> </ul>
<b>Conflicts of Interest</b>	where, in the course of the Group's business, there are actual or potential Conflicts of Interest between the interests of the Group, its customers, relevant individuals and/or Third Parties and that, as a result, acting in one

	of those interests may be working against (to the detriment of) the interests of another. The more that interests overlap or compete, the greater the risk that a Conflict of Interest may arise.
<b>Corruption</b>	the abuse of entrusted power for private gain.
<b>Employee</b>	covers: <ul style="list-style-type: none"> <li>• an individual who is employed by the Group on a permanent or temporary basis</li> <li>• an individual who is working for but is not directly employed by the Group (including consultants, contractors, agency workers, etc.)</li> </ul>
<b>EU High Risk Third Country List</b>	is published by the European Commission and includes those countries with strategic deficiencies in their national Anti-Money Laundering (“AML”) and Counter-Terrorist Financing (“CTF”) regimes that pose substantial threats to the EU and its financial system.
<b>Executive Leadership Team</b>	the Executive Leadership Team of Danske Bank A/S
<b>External Fraud</b>	wrongful or unlawful deception intended to result in direct or indirect financial gain which is detrimental to the Group and/or its customers, which is committed or supported by external parties, including the Group’s customers.
<b>Facilitation Payments</b>	payments or gifts made to Public Officials to hasten the performance of a routine action that are over and above the normal fee for that service or where a fee would not legally apply.
<b>Facilitation of Tax Evasion</b>	when an Associated Person of the Group deliberately or dishonestly enables Tax Evasion.
<b>Financial Crime</b>	the generic term for Money Laundering, Terrorist Financing, Sanctions, Bribery, Corruption, Fraud, Tax Evasion and Facilitation of Tax Evasion.
<b>Group</b>	Danske Bank A/S, including its Branches and Subsidiaries.
<b>Group Function</b>	refers to and covers areas in the Group such as: <ul style="list-style-type: none"> <li>• CFO area</li> <li>• Group Human Resources (“HR”)</li> <li>• Group Internal Audit</li> <li>• Group Legal</li> <li>• Group Risk Management</li> <li>• Group Compliance</li> <li>• Group Sustainability, Stakeholder Relations, Communications &amp; Marketing</li> <li>• Technology &amp; Services</li> </ul>
<b>Incident of Bribery</b>	any act of Bribery for which the Group bears any level of responsibility. An Incident of Bribery as it relates to the Group can only occur through the actions of an Associated Person of the Group.
<b>Internal Fraud</b>	wrongful or unlawful deception intended to result in direct or indirect financial gain which is detrimental to the Group and/or its customers, which is committed or supported by a party internal to the Group.
<b>Key Function Holders</b>	persons whose position (function) gives them significant influence over the direction of the undertaking, but who are not members of the Executive Leadership Team or relevant Subsidiary executive management cf. applicable regulatory requirements.
<b>Money Laundering</b>	the generic term used to describe the process by which the original ownership and control of the proceeds of criminal conduct is disguised by making such proceeds appear to have derived from a legitimate source.
<b>Products</b>	a collective term covering: <ul style="list-style-type: none"> <li>• Products and services offered by the Group to Customers of the Group or to any other person or legal entity</li> <li>• Products and services that are offered by a Third Party (including partnerships) and distributed by the Group</li> </ul>

	These include investment Products, non-investment Products and services, but excludes delivery channels
<b>Political Lobbying</b>	The act of lawfully attempting to influence the actions, policies or decisions of politicians or Public Officials. Lobbying also involves advocacy of an interest or interest representation towards relevant stakeholders on the issue.
<b>Politically Exposed Person ("PEP")</b>	a natural person who holds, or has previously held a prominent public function, their family members or individuals known to be close associates.
<b>Public Official</b>	a natural person in any rank or level at the following types of legal entities, organisations, and bodies: <ul style="list-style-type: none"> <li>• national, regional, local or municipal governmental bodies</li> <li>• state-owned or state-controlled legal entities or funds</li> <li>• central banks</li> <li>• sovereign wealth funds</li> <li>• international organisations, development banks and public health agencies, as well as mixed private-public entities</li> <li>• royal families</li> <li>• embassies and embassy diplomats.</li> <li>• political parties, party officials and candidates for any level of a political office.</li> </ul> <p>Local market areas may define Public Official in accordance with local regulation.</p>
<b>Risk Tolerance</b>	the aggregate level of risk the Group is willing to accept in pursuit of its long term objectives while maintaining a stable financial position.
<b>Sanctions</b>	economic sanctions ("Sanctions"). Sanctions are legal measures designed to impose restrictions, prohibitions and require actions in relation to sanctioned countries, parties and activities.
<b>Senior Management</b>	the Executive Leadership Team, Subsidiary executive management and Key Function Holders of the Group.
<b>Subsidiary</b>	any undertaking over which Danske Bank A/S exercises control. For the purpose of this definition "control" means any of the following: <ul style="list-style-type: none"> <li>• direct or indirect ownership of more than fifty per cent (50%) of the share capital or other ownership interest in any other person;</li> <li>• the direct or indirect right to exercise more than fifty per cent (50%) of the votes in any other person;</li> <li>• 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,</li> <li>• 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.</li> </ul>
<b>Tax Evasion</b>	the act whereby liability to tax is deliberately concealed or ignored.
<b>Terrorist Financing</b>	the provision or collection of funds with the intention that these funds can be used to carry out an act of terror, or be used to support any terrorist group, persons or associations in any ways.
<b>Third Party</b>	a legal entity, company, or person(s) that is not Danske Bank A/S or a Group Entity of Danske Bank A/S. Third Parties are not inclusive of Employees or customers, nor the contracts in place with Employees or customers

### 3. Scope

The principles of this Policy set the Group's approach for Financial Crime risk management and compliance with Financial Crime related laws, regulations, regimes and other requirements that are applicable to the Group and its operations.

#### 3.1. Target group

This Policy applies to all Employees in the Group and all Subsidiaries as well as all Associated Persons of the Group. All Third Parties must 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 the 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 this Policy is consulted on any deviation.

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

### 4. Policy Content

***Principle 1: The Group must maintain a governance framework that clearly defines roles, accountabilities, and responsibilities for Financial Crime compliance***

The Group must maintain a governance framework that is promoted across all areas of the Group. The framework must include:

- Clearly allocated accountabilities and responsibilities to manage Financial Crime risk;
- Appointment of AML/CTF regulated persons across the Group;
- An approach from the Board of Directors and Senior Management that actively promotes a strong Financial Crime compliance culture;
- Governance that sets out appropriate mandates, authorities and oversight capabilities to manage and mitigate Financial Crime risk and document actions, decisions and approvals; and
- Adequate resources in respect of personnel, competency and technology.

The governance framework must also include the specific accountabilities held by the relevant bodies and functions within the governance structure, including the Board of Directors, Senior Management, Group Compliance and Business Units.

***Principle 2: The Group must apply the three lines of defence model to ensure effective governance and oversight of Financial Crime risk***

The Group applies the three lines of defence model in accordance with the Group's Enterprise Risk Management Policy. The three lines of defence model is a key element in ensuring effective governance and oversight of Financial Crime risk, including having clearly defined roles and responsibilities in place.

The Group's frontline units and their direct support functions within the Business Units constitute the **first line of defence** and are accountable for identifying, mitigating, managing and taking ownership of the Financial Crime risks associated with (but not limited to) customers, Third Parties, Associated Persons of the Group, Products, and services. This includes designing, implementing and executing processes and controls to identify and manage Financial Crime risks within their business and operations, and performing ongoing oversight on the effectiveness of these processes and controls.

Group Compliance constitutes part of the **second line of defence**. Group Compliance is responsible for ensuring the Group has adequate and robust policies and instructions addressing Financial Crime risk, while also monitoring, testing, supporting, advising and challenging first line of defence risk management and compliance practices. As described in the Group's enterprise risk management framework, for each level 1 risk type, there is a second line of defence risk type responsible function which sets the overall framework and performs Group-wide oversight of the specific risk types. For Financial Crime risks, this function is Group Compliance.

Group Compliance is also responsible for updating the Group-wide risk assessment that identifies and measures the inherent risk of Financial Crime and evaluates the design and effectiveness of controls to determine the Group's residual risk.

Group Internal Audit constitutes the **third line of defence**. The scope of Internal Audit's mandate is unrestricted and includes oversight of the activities conducted by both the first and second lines of defence and of Third Parties where facilitated by contractual provision.

***Principle 3: Employees and other Associated Persons of the Group must not participate in misusing the Group's infrastructure, Products and services for Financial Crime purposes***

All Employees and other Associated Persons of the Group are prohibited from, directly or indirectly, actively or passively advising on, facilitating, engaging or participating in activities or behaviour that misuse the Group's infrastructure, Products and/or services for Financial Crime purposes or otherwise circumvent requirements imposed by this Policy and its underlying instructions.

In addition, the Group must set out the responsibilities that all Employees and other Associated Persons of the Group have in the management of Financial Crime risk.

**Subprinciple 3.1: Employees and other Associated Persons of The Group must not make Facilitation Payments as it relates to responsibilities associated with the Group**

Employees and other Associated Persons of the Group must not make Facilitation Payments as it relates to responsibilities associated with the Group, except in instances where the person being asked to make the payment believes that refusal would endanger their personal or another person's safety. Any payments made under such coercive circumstances must be reported to Group Compliance. Even if a Facilitation Payment is requested in a jurisdiction where it is culturally expected and not prohibited by law, the Group defines these payments as Bribery.

**Subprinciple 3.2: The Group must ensure that gifts, hospitality and entertainment are not used to engage in an Incident of Financial Crime**

The Group must ensure that all Employees and other Associated Persons of the Group adhere to the Group requirements, thresholds and approvals for gifts and hospitalities before giving or receiving Anything of Value. This is regardless of whether it takes place during participation in external events or marketing events, roadshows or conferences held or sponsored by the Group which are attended by customers.

All gifts, hospitality and entertainment provided to, or from, customers or Third Parties must be in accordance with the Group's relevant instructions. Additionally, any Conflicts of Interest arising from the use of gifts, hospitality and entertainment must be reported in accordance with the Conflicts of Interest Policy.

**Subprinciple 3.3: The Group must maintain controls to manage the Financial Crime risk associated with its Employees and potential Employees**

The Group must ensure appropriate controls, where relevant and legally possible, are put in place to identify, investigate and, if deemed appropriate, apply disciplinary actions to Employees engaging or participating in activities or behaviour that misuse the Group's infrastructure, Products for Financial Crime purposes, or that are grossly negligent in complying with this Policy.

In addition, the Group must ensure that offers of employment are not used to engage in an incident of Financial Crime and where legally possible, that all potential Employees are screened in relation to Financial Crime risks (for example criminal records screening, Sanctions screening, PEP screening and, where legally possible, adverse media screening, as necessary). All paid and unpaid (for example internships) employment must be agreed to and contracted through established standardised HR processes.

**Subprinciple 3.4: The Group must maintain controls to manage the Financial Crime risk associated with Employee incentives**

The Group must ensure that any incentives provided to Employees are not used to encourage an incident of Financial Crime.

All incentives must be agreed to and contracted through established standardised HR processes.

***Principle 4: The Group must have sufficient management information and reporting to monitor and oversee the management of Financial Crime risk***

The Group must develop and produce management information ("MI"), including both qualitative and quantitative indicators to maintain effective oversight of the Group's management of risk and compliance associated with Financial Crime and to inform Senior Management and other key stakeholders.

***Principle 5: The Group must apply a risk-based approach to ensure that risk mitigation measures are proportionate to the level of associated Financial Crime risk***

The Group must apply a holistic, risk-based approach to ensure that effective and appropriate controls are in place that are proportionate to the identified Financial Crime risk. The Group must identify and assess its Financial Crime risk to enable the effective design and implementation of adequate controls to manage and mitigate these risks in accordance with the Risk Tolerances set by the Group.

In addition, applying a risk-based approach informed by a robust understanding of risk enables the Group to allocate and target its efforts and resources in the most efficient manner, with enhanced measures taken in instances that present an increased risk of Financial Crime.

***Subprinciple 5.1: The Group must update the Group-wide risk assessment to identify and measure the inherent risk of Financial Crime and evaluate the design and effectiveness of controls to determine the Group's residual risk***

The Group must update the Group-wide risk assessment, at least annually, to identify and measure the Group's inherent Financial Crime risk and evaluate the design and effectiveness of controls to determine the Group's residual Financial Crime risk.

In addition, where significant changes are made, for example to the Group's operations, or new or revised supranational or national risk assessments have been issued, these must be reviewed to determine whether they affect the Group-wide risk assessment in such a way that updates are deemed necessary.

The Group-wide risk assessment must adequately account for the potential Financial Crime risk arising from all relevant factors, including (but not limited to) the Group's customers, Products, services, delivery channels, Third Parties, Associated Persons of the Group, transactions, technology and geographic locations. The Group-wide risk assessment must also be proportionate to the size and complexity of the Group and its operations.

The Group-wide risk assessment results must be used by the Group to inform the design, development, maintenance and implementation of the Group's Financial Crime framework and other mitigation activities.

***Subprinciple 5.2: The Group must establish and manage its Financial Crime risk in line with the enterprise risk management framework***

The Group must establish Risk Tolerances through the enterprise risk management framework including any relevant governing documents, in order to manage its Financial Crime risk exposure in an effective and efficient way.

In addition, the Group must ensure adherence with the established tolerance levels and that relevant statements and metrics as set out by the tolerance statement are adequately monitored over time.

***Principle 6: The Group must maintain a control framework that enables effective and efficient mitigation of Financial Crime risk***

The Group's internal control framework must enable the Group to adequately identify, manage and mitigate Financial Crime risk. The framework must set clear expectations that include:

- Identifying, documenting, monitoring and preventing Financial Crime risk;
- Investigating and reporting potential Financial Crime incidents and violations;
- Defining, documenting and maintaining risk-based control procedures and processes pertaining to Financial Crime compliance;

- Defining, documenting and maintaining procedures and processes to cease identified Financial Crime activities; and
- Regular testing of the controls to ensure effective operation as well as ensuring the controls are appropriate and proportionate to the associated Financial Crime risk.

The framework includes screening, monitoring and due diligence controls that take into account relevant risk factors associated with customers, industries, geographies, typologies, Products and service channels, Third Parties or a combination of these.

**Subprinciple 6.1: The Group must maintain controls to identify and manage the Financial Crime risk associated with its corporate development and strategic decisions**

The Group must ensure that any merger, acquisition, joint venture, principal finance investment or strategic decision to enter a new market, jurisdiction, Product category or customer segment made by the Group considers Financial Crime risk as part of the due diligence, risk assessment, contracting, management and monitoring processes.

In addition, the Group must ensure that this is done in accordance with the Group's Non-Financial Risk policies and underlying instructions.

**Subprinciple 6.2: The Group must maintain controls to manage the Bribery and Corruption risk associated with Political Lobbying**

The Group must ensure that Political Lobbying is not used to engage in an Incident of Bribery. All Employees must adhere to the requirements set out in the Group's Stakeholder Policy when lobbying politically. In addition, all Employees must give consideration to the Bribery and Corruption risks that the potential engagement with this population could present to the Group and adhere to the requirements set out in relevant instructions.

**Subprinciple 6.3: The Group must maintain controls to manage the Financial Crime risk associated with sponsorships and donations**

The Group must ensure that payments for sponsorships and donations are not used to engage in an incident of Financial Crime.

In accordance with the Third Party Risk Management Policy and underlying instructions, the Group must perform due diligence on sponsorship recipients, taking into account the potential affiliation with Public Officials. The purpose and selection criteria of a sponsorship or donation must be documented and approved before any payment is made.

In addition, adequate controls must be put in place to ensure that the authorised recipient is the natural person or legal entity being paid and that there are no pending business decisions with the recipient of the sponsorship or donation payment.

**Subprinciple 6.4: The Group must maintain controls to identify, assess and manage the Financial Crime risk associated with Products and services**

The Group must ensure that the Product approval process set out within the Group identifies and assesses the potential exposure to Financial Crime risk of the Group, when Business Units are considering customising or altering the features and terms of a Product or service for a specific customer or group of customers. This must take place prior to approving such customisation or alteration.

Before approving a new Product or service, and before customising or altering the features and terms of a Product or service, Business Units must ensure that Financial Crime subject matter experts are engaged for advice on the risk associated with said Product and/or service.

In addition, the Group must ensure that this is done in accordance with the Group's Non-Financial Risk policies and underlying instructions.

**Subprinciple 6.5: The Group must maintain controls to identify, assess and manage the Financial Crime risk associated with geography and industry**

The Group must establish a list management framework and governance that identify, assess and manage the Financial Crime risk exposure associated with geography and industries for customers and Third Parties. This

includes the development of appropriate list management controls to ensure that all lists used are accurate and up-to-date.

**Subprinciple 6.6: The Group must maintain controls to detect and prevent customer impersonation attempts for Financial Crime purposes and to ensure that customers are who they are purporting to be**

The Group must establish an authentication framework that ensures that all customer interactions have the necessary verifications in order to provide a high level of confidence that the customers with whom the Group interacts and to whom the Group offers Products and services, are who they are purporting to be.

The framework must take into account customer interactions throughout the end-to-end lifecycle of a customer's relationship with the Group, irrespective of the Products and services offered and used. The authentication methods utilised must be regularly reviewed to ensure they at all times provide the required level of protection and customer usability.

***Principle 7: The Group must perform due diligence measures when establishing and maintaining relationships with customers and Third Parties***

The Group's due diligence framework must ensure that all customers and Third Parties are subject to due diligence measures prior to establishing a relationship and throughout the duration of the relationship. The due diligence measures must be completed prior to carrying out any transactions on behalf of the customer and before a Third Party relationship is entered into.

**Subprinciple 7.1: The Group must not establish or maintain relationships where it cannot obtain sufficient information, or mitigate the Financial Crime risks associated with the customer or relevant parties**

The Group must ensure that all customers and Third Parties are subject to an appropriate level of due diligence at the time of on-boarding or entering into a contract and during the duration of the relationship, in accordance with the identified level of risk informed by a Financial Crime risk assessment and the Group's policies, instructions and procedures. Third Party contracts must include anti-Financial Crime risk provisions.

The Group must not establish a relationship with customers or relevant parties where it has not obtained all necessary information as required by the due diligence requirements or maintain relationships where it has been unable to complete the due diligence processes.

Where the Group is unable to mitigate the Financial Crime risk associated with maintaining a relationship or where there is a suspicion of Financial Crime, adequate procedures must be in place to determine the appropriate course of action.

Further, the Group must not maintain or enter into prohibited relationships such as relationships with shell banks. Please refer to the underlying instructions to this Policy for further details on prohibited relationships.

**Subprinciple 7.2: The Group must develop and maintain procedures and processes for information sharing within the Group**

The Group must develop and maintain procedures and processes for sharing of information within the Group with the purpose of preventing Financial Crime.

Any sharing of information must be done in accordance with applicable regulation and the Group's Personal Data Protection Policy [internal document], Security Policy [internal document], and Information Classification Taxonomy.

**Subprinciple 7.3: The Group must identify and assess the Financial Crime risk associated with its customers, Third Parties and Associated Persons of the Group**

When a relationship is established or is intended to be established, the Group must ensure that the Financial Crime risk associated with the individual customer, Third Party and Associated Person of the Group is identified and assessed to determine the appropriate level of due diligence measures the customer, Third Party or Associated Person of the Group must be subject to.

**Subprinciple 7.4: The Group must perform enhanced due diligence measures where the relationship with the customer or Third Party is assessed to pose an increased risk of Financial Crime**

The Group must apply enhanced due diligence measures on customer or Third Party relationships that expose the Group to a higher Financial Crime risk. This requires Business Units to collect and assess additional information/documentation in relation to the customer or Third Party to ensure the application of appropriate controls and to ensure that the relationship is within the Group's Financial Crime Risk Tolerance.

**Subprinciple 7.5: The Group must perform ongoing due diligence on all customers and Third Parties to ensure that information is accurate and up-to-date**

The Group must perform ongoing due diligence ("ODD") on all customers and Third Parties consisting of periodic reviews and ongoing monitoring of their profile, activity and behaviour. This enables the Group to assess whether the activities correlate with the information provided at on-boarding or when entering into the contract or when an ODD review was last performed, and to detect any suspicious activity and behaviour. Performing ODD also enables the Group to ensure that the controls and due diligence measures applied on the relationship continue to be adequate.

The frequency for ODD is determined by the risk rating or where circumstances or events associated with the customer or Third Party trigger a review.

**Subprinciple 7.6: The Group must identify and manage risks associated with customers and relevant parties that are considered PEPs**

The Group must develop, implement and maintain effective measures and processes to identify and mitigate the risks associated with PEPs, their known close associates and family members.

Further, the Group must maintain an appropriate definition of a PEP (as well as of known close associates and family members) that meets the applicable regulatory standards within the jurisdictions in which the Group operates, as well as establish PEP-specific due diligence measures and controls.

**Subprinciple 7.7: The Group must identify and manage risks associated with Public Officials**

The Group must develop, implement and maintain effective measures and processes to identify and mitigate the Bribery and Corruption risks associated with Public Officials. This includes maintaining specific due diligence measures and enhanced controls for customers, Third Parties or Associated Persons of the Group that are identified as Public Officials to address the risks identified.

The Group considers all Facilitation Payments to Public Officials in any geographic location to be an Incident of Bribery.

**Subprinciple 7.8: The Group must have controls to manage Financial Crime risks associated with correspondent relationships**

The Group must develop and maintain specific due diligence measures and controls relating to correspondent relationships, enabling an effective and consistent risk-based approach across the Group.

**Subprinciple 7.9: The Group must have controls to manage Financial Crime risks associated with higher risk countries, such as those on the EU High Risk Third Country List and, where relevant, equivalent local lists**

The Group must conduct enhanced due diligence on customers or Third Parties carrying out transactions involving or maintaining a registered office address in/residing in countries on the EU High Risk Third Country List and, where relevant, equivalent local lists.

**Subprinciple 7.10: The Group must develop and maintain procedures to manage relationships with Third Parties or Associated Persons of the Group that carry out aspects of the Financial Crime compliance framework on its behalf**

The Group must develop and implement appropriate standards and procedures when relying on or outsourcing Financial Crime risk management to Third Parties or Associated Persons of the Group including ensuring that Third Parties and Associated Persons are subject to an appropriate risk-based due diligence at the time of the establishment and throughout the duration of the relationship. The due diligence must be completed before a Third Party or Associated Person of the Group carries out any activity related to the Financial Crime compliance framework

on the Group's behalf. Financial Crime compliance responsibilities can be performed by Third Parties or Associated Persons of the Group on its behalf, however, the Group remains ultimately accountable for their activities.

Third Parties working or performing services for, or on behalf of the Group, to perform elements of the Group's Customer Due Diligence or who carry out aspects of the Group's Financial Crime Framework on its behalf must be considered as higher risk and thus subject to enhanced due diligence.

***Principle 8: The Group must conduct risk-based monitoring and screening to identify Financial Crime risk***

The Group must develop and implement risk-based transaction monitoring and screening controls to identify its Financial Crime risk exposure, potential suspicious or inconsistent activity, PEP relationships and, where legally possible, potential adverse media. Such monitoring and screening must comply with any relevant data protection laws and regulation.

**Subprinciple 8.1: The Group must conduct risk-based transaction monitoring to identify Financial Crime**

The Group must monitor all customer relationships on an ongoing basis. Transactions carried out as part of the customer relationship must be monitored to identify whether they are consistent with the Group's knowledge of the customer and the customer's business and risk profile, and to enable the detection of unusual or suspicious transactions.

The Group must develop risk-based scenarios, typologies, rules and thresholds to identify such activity.

**Subprinciple 8.2: The Group must apply risk-based Sanctions screening against relevant Sanctions lists**

The Group must screen all relevant information related to customers, potential customers, Third Parties, relevant associated parties, transactions and business activities against relevant Sanctions lists to ensure compliance with Sanctions. A risk-based approach may be applied where legally possible. Relevant associated parties to Third Parties (including beneficial owners ("BO") and key controllers) are subject to screening where higher risk is identified or a Third Party holds a critical relationship with the Group as defined in the Third Party Risk Management Policy.

The Group must ensure that the screening controls are applied prospectively and prior to engaging in a relationship or a transaction and that any potential Sanctions-related alerts and concerns identified through application of those controls are resolved prior to completing the engagement or transaction.

**Subprinciple 8.3: The Group must conduct screening to identify which customers and relevant parties should be classified as PEPs**

The Group must ensure that all customers and relevant parties are screened against PEPs lists to determine whether there are any PEPs or known close associates and family members of PEPs within the Group. If hits are identified, these should be investigated to determine whether they are genuine and if so, appropriate due diligence should be applied. Third Parties and their relevant associated parties (including BOs and key controllers) are subject to screening where higher Financial Crime risk is identified.

**Subprinciple 8.4: The Group must conduct risk-based searches to help identify potential adverse media associated with its customers, potential customers, Third Parties and where relevant Associated Persons of the Group**

The Group must apply, where legally possible, risk-based media searches to help identify whether any customers, potential customers, relevant associated parties, Third Parties and Associated Persons of the Group are subjects of Financial Crime related adverse media.

The Group must, where legally possible, conduct media searches of Third Parties, conducted in languages relevant to the Third Party and their business operations, with the Third Parties' associated parties (including relevant BOs and key controllers) subject to screening where higher risk is identified or a Third Party holds a critical relationship with the Bank.

Relevant hits and potential red flags must be investigated, and documented, to determine whether they are true and if so, their materiality in respect of the relationship with the Group should be assessed.

**Subprinciple 8.5: The Group must maintain a list management framework to ensure up-to-date and accurate screening for Sanctions and PEPs**

The Group must establish a list management framework and governance that defines the relevant internal and/or external Sanctions and PEP lists to be applied in screening. This includes the development of appropriate list management processes to ensure that all lists used for screening are accurate and up-to-date.

**Subprinciple 8.6: The Group must conduct risk-based ongoing monitoring and oversight of all relationships with Third Parties and Associated Persons of the Group (where relevant) to identify Financial Crime risks**

The Group must implement and maintain effective processes and controls to ensure all relationships with Third Parties and where relevant, Associated Persons of the Group are subject to ongoing monitoring and oversight of their performance and compliance with the requirements of the agreement to identify Financial Crime risk.

**Subprinciple 8.7: The Group must undertake profiling and monitoring of customer, Employee and Third Party activity to assess Fraud risk**

The Group must, where legally possible, profile and monitor all activity of customers, Employees and Third Parties it engages with to identify suspicious behaviour that could indicate that Internal or External Fraud is being committed. Due to the significant volume of transactions processed, the Group must develop risk-based scenarios, typologies, rules and thresholds to identify such behaviour.

***Principle 9: The Group must ensure that suspicious activity, incidents of Financial Crime or potential Financial Crime violations are investigated and reported to the competent authorities***

The Group must ensure that it implements and maintains effective processes and controls to ensure that suspicious activity, incidents of Financial Crime or potential Financial Crime violations are reported to the competent authorities in a timely manner.

**Subprinciple 9.1: The Group must investigate and report knowledge or information of transactions, assets or activities that are deemed to be suspicious**

The Group must ensure that if there is any concern relating to transactions, assets or activity that may be connected to Money Laundering, Terrorist Financing or any other type of Financial Crime, this must be investigated and reported to the Suspicious Activity Reporting Office ("SARO") or, local Money Laundering Reporting Officer ("MLRO") as an Unusual Activity Report ("UAR"). The investigation process must include controls to prevent the customer being tipped off.

Where the unusual activity is determined to be suspicious, the relevant SARO or, local MLRO must report the activity to the local Financial Intelligence Unit ("FIU") or equivalent competent authority.

**Subprinciple 9.2: The Group must investigate potential Sanctions breaches to determine appropriate action and, when necessary, report those to the relevant authorities**

The Group must ensure that potential Sanctions breaches or material Sanctions concerns are reviewed by Group Compliance to determine whether they require further action. Any action taken will depend on the applicable Sanctions implicated by the concerns. These may include, among others, freezing of funds, rejecting a transaction or declining a relationship and reporting to the competent authorities.

Where a transaction, relationship or other activity is determined to be subject to applicable Sanctions, Group Compliance must, when necessary, report it to the competent authorities.

**Subprinciple 9.3: The Group must investigate incidents of Fraud (Internal and External) or potential Fraud (Internal and External) violations to determine appropriate action, and when necessary, report those to the relevant authorities**

The Group must ensure that incidents of Fraud (Internal and External) or potential Fraud violations (Internal and External) are reviewed, escalated and investigated in accordance with the Group's policies and underlying instructions in order to determine whether it requires further action. Where deemed necessary, reporting must be done to the competent authorities in a timely manner.

***Principle 10: The Group must ensure that its Employees have adequate competence and awareness about Financial Crime compliance requirements and controls by providing regular training and communication***

The Group must provide Employees with training on the regulatory requirements the Group must adhere to and the Financial Crime risks to which the Group is exposed. This includes specific, tailored training for Employees that fulfil roles with higher Financial Crime risk exposure.

Training is an integral part of the Group's Financial Crime risk management. Completion of training must be documented and monitored through appropriate MI metrics, and non-completion of training must be taken seriously through appropriate consequence management.

***Principle 11: The Group must ensure that records relevant for Financial Crime compliance are retained to ensure auditability and investigation***

The Group must retain accurate electronic records concerning customers and Third Party information, risk assessments, transactions, reviewing and investigation of alerts and other relevant information. Decisions, approvals and exceptions related to the management of Financial Crime risk must be documented and display professional judgement and objectivity. Employees must not engage in fraudulent record keeping activities, including but not limited to theft, Fraud, forgery and fabrication of false evidence records, defacement or destruction of any record belonging to the Group, the Group's customers, Employees or other Associated Persons of the Group when acting on behalf of the Group.

All records must comply with relevant data retention, data privacy and data protection laws and regulations. All records must be retained in accordance with retention periods specified by the Group and any retention requirements specified in applicable legislation.

***Principle 12: The Group must assess and monitor the effectiveness of its Financial Crime compliance framework through regular assurance and control testing including audits***

The Group must regularly conduct risk-based assurance and control testing of its Financial Crime compliance framework. The methodologies and frequency of testing should be appropriate to the level and sophistication of the risks. In addition, and on a risk-based approach, Group Internal Audit, or a representative of Danske Bank should exercise the right to audit Third Party Financial Crime controls and processes.

The Group must ensure that the functions performing assurance and control activities have sufficient skills, expertise, resources and authority within the organisation to effectively identify weaknesses and deficiencies, identify enhancement opportunities as well as enrich management reporting on the Financial Crime risk profile of the Group.

***Principle 13: The Group must ensure that all Financial Crime compliance controls and processes are adequately managed through business continuity management arrangements***

Financial Crime compliance controls and processes are interlinked with the ability to process transactions, deliver Products and services, and on-board and maintain customers and other relationships. Any disruption in such processes and controls may potentially have a significant impact on the Group's compliance with its Financial Crime obligations and its ability to service customers and society on a continuous basis.

As it is critical to ensure compliance while also ensuring that the Group continues to provide and deliver services, the Group must ensure that all critical Financial Crime related processes and controls have appropriate contingency plans and associated measures implemented to ensure compliance and avoid disruptions.

***Principle 14: The Group must engage, cooperate and communicate with supervisors, competent authorities and law enforcement agencies***

The Group must ensure that any interaction or engagement with supervisors, competent authorities and law enforcement agencies is carried out in accordance with the Group's policies and underlying instructions.

Group Compliance must immediately be informed of any Financial Crime related request received from supervisors, competent authorities or law enforcement agencies. Group Compliance must ensure that all information requests are promptly responded to and managed in accordance with relevant data protection and bank secrecy requirements, as necessary.

## 5. Escalation

In accordance with the Group's risk event escalation framework the administrator of this Policy must, when notified, escalate to the owner of this Policy without undue delay:

- any significant breaches of this Policy, and
- any material violations of applicable Financial Crime laws and regulations and relevant regimes

For the avoidance of doubt, the requirements as set out by the risk event escalation framework must always be considered in relation to violating the Group's regulatory obligation to prevent and mitigate Financial Crime.

### 5.1. Breaches

A breach, in the context of this Policy, is defined as non-compliance with any requirement in this Policy or the underlying instructions. All breaches, regardless of the breach being defined as significant, must be reported to the administrator of this Policy without undue delay. In addition, recording must also be made in line with any other departmental or Group-wide escalation procedures such as disclosure through the operational risk information system ("ORIS").

Lack of adherence to this Policy and its underlying instructions may have severe consequences to the Group and its Employees including:

- violating Financial Crime laws, regulations and regimes
- receiving monetary fines, criminal penalties, and/or regulatory enforcement orders
- exposing the Group to financial, customer, operational, legal and reputational risk

In addition, it may also lead to disciplinary action up to and including potential dismissal, contract termination, criminal indictment or claim of damages.

## 6. Review

The administrator must review and update this Policy at least annually or more frequently if required. Events which may cause a need for a review by the administrator include changes to relevant applicable regulation and legislation.

In the circumstance where the maintenance of this Policy cannot be completed in accordance with the Group's Internal Governance Policy, the administrator of this Policy must escalate this to the owner of this Policy