Danske Bank

Financial Crime Policy

20 March 2025

1. Objective

The objective of the Financial Crime Policy (the "Policy") is to promote a strong Financial Crime compliance culture within the Danske Bank Group to prevent the misuse of the Group's infrastructure and Products for Financial Crime purposes. In doing so, it protects the Danske Bank Group, our customers and society.

2. Definitions

The definitions for the terms used throughout this Policy are available in Appendix 1.

3. Scope and target group

This Policy establishes the principles for the managing of risks associated with Financial Crime, ensuring compliance with relevant laws, regulations, guidelines and sanctions regimes.

The Policy applies to the entire Danske Bank Group.

4. Policy Content

Principle 1: The Group maintains a robust and efficient Financial Crime Program

Through its Financial Crime Program, the Group is committed to upholding high standards of integrity and compliance to protect the Group, its customers and society from Financial Crime. The Financial Crime Program is designed to enable the Group to safely carry out its business activities while effectively and efficiently managing the Financial Crime Risks it faces.

The Financial Crime Program consists of elements which together form a coherent Financial Crime strategy. The Program is continuously evaluated to allow the Group to proactively anticipate, plan and adapt to emerging risks and changes in relevant laws, regulations, guidelines and sanctions regimes.

The Financial Crime Program includes, but is not limited to:

- a sound Financial Crime compliance culture, strategic prioritisation of Financial Crime compliance and allocation of sufficient funding and resources,
- a three lines of defence model ensuring segregation of duties, independent oversight and consistent enforcement of the Group's governing documents across all lines of defence,
- Financial Crime Risk Tolerances, Key Performance Indicators, Key Risk Indicators and monitoring and reporting capabilities,
- a Financial Crime governance framework,
- frameworks for management of Financial Crime data and technology, including the use of new or innovative technology and maintenance of technical capabilities,
- Financial Crime Risk assessments,
- a Financial Crime Control framework,

- Financial Crime detection capabilities,
- customer and Third-Party due diligence measures,
- unusual and suspicious activity investigation and reporting,
- a Financial Crime training program and
- reporting, escalation and whistleblowing procedures and solutions ensuring prompt response to Financial Crime.

Roles and Responsibilities:

- The Board of Directors and the Executive Leadership team are responsible for setting the tone from the top, ensuring strategic prioritisation of the Group's Financial Crime Program and allocating adequate resourcing, funding and investment.
- 1LoD and 2LoD are responsible for developing, implementing and maintaining the Group's Financial Crime Program in accordance with the respective mandates.
- 1LoD and 2LoD are responsible for operating the Financial Crime Program according to the mandates established in the Group's Enterprise Risk Management Policy and other relevant policies.

Principle 2: The Group maintains a governance framework for effective management of Financial Crime Risks

The Financial Crime Risk governance framework is essential for effectively managing Financial Crime Risks and is established in accordance with the standards of the Group's Enterprise Risk Management Policy. The framework must set clear requirements and be sufficiently operational. This includes:

- defined roles, responsibilities and accountabilities for the management and oversight of Financial Crime Risks within the three lines of defence,
- appointment of Anti-Money Laundering ("AML"), Counter-Terrorist Financing ("CTF") and Sanctions Regulated Person(s) according to the requirements in European Union/European Economic Area and national legislation,
- governance that sets out appropriate compliance requirements, mandates, authorities and oversight standards to manage and mitigate Financial Crime Risks, including requirements for documenting actions, decisions and approvals,
- governing bodies enabling effective oversight of Financial Crime Risks, streamlined decision-making and appropriate and systematic escalation of material risks,
- adequate resources in respect of personnel, including competencies and skills, and technology to facilitate effective execution of the roles expected of these resources,
- management information and reporting requirements and capabilities to facilitate effective management and escalation of material and emerging risks, and
- proactive and transparent cooperation with authorities and participation in relevant industry initiatives.

Roles and Responsibilities:

- The Board of Directors and Senior Management are accountable for ensuring compliance with applicable Financial Crime-related laws, regulations and guidelines, promoting a strong Financial Crime Risk management culture and ensuring that this is reflected in the Group's strategic objectives.
- Regulated Persons are accountable for the proper execution of their regulated tasks.
- Senior Management is responsible for emphasising the importance of Financial Crime compliance and for establishing, implementing and overseeing the adequacy of the Financial Crime compliance governance framework, including allocation of sufficient resources.
- 1LoD is responsible for establishing, implementing and owning the 1LoD Financial Crime governance framework which effectively governs the management of Financial Crime Risks.
- 2LoD is responsible for establishing and implementing the governance framework for 2LoD and overseeing the adequacy of the Financial Crime governance framework of 1LoD.

Principle 3: The Group maintains a framework for management of Financial Crime data and technology

The Financial Crime data and technology management framework ensures appropriate governance, quality, efficiency and effectiveness of data and technology in execution of Financial Crime risk management and compliance. This includes, but is not limited to:

- defined roles, responsibilities and accountabilities for the management and oversight of Financial Crime data and technology,
- requirements for the management and oversight of Financial Crime data, solutions, technical features and capabilities and
- management information and reporting requirements to facilitate effective management and escalation of Financial Crime data and technology risks.

Roles and Responsibilities:

- 1LoD and relevant Group Functions are responsible for managing Financial Crime data and technology in accordance with the Group's data and technology management framework.
- 2LoD is responsible for establishing the Group's minimum requirements for Financial Crime-related data, solutions, technical features and capabilities. Additionally, 2LoD is responsible for providing advice and oversight of 1LoD's management and implementation of these requirements.

Principle 4: The Group assesses Financial Crime Risks and applies a risk-based approach

The Group establishes and manages its Financial Crime Risk in line with the Risk Tolerance framework. It identifies and assesses its Financial Crime Risks to enable an effective design and implementation of proportionate Controls to manage and mitigate these risks. This includes, but is not limited to:

- execution of the Group-Wide Risk Assessment for Financial Crime,
- Financial Crime Risk assessment of new and amended Products,
- Financial Crime Risk assessment of new and amended technologies,
- ongoing customer Financial Crime Risk assessment and
- ongoing segmentation of Third Parties.

Roles and Responsibilities:

- the Board of Directors is responsible for setting Financial Crime Risk Tolerances.
- 1LoD is responsible for setting Financial Crime Risk Appetite within the Financial Crime Tolerances.
- 1LoD and 2LoD are responsible for identifying and assessing the Financial Crime Risk associated with the Group's activities.
- 2LoD is responsible for establishing key Financial Crime Risk and performance indicators, developing and maintaining a framework for Financial Crime Risk assessments and maintaining compliance oversight measures linked to Financial Crime Risk Tolerances.

Principle 5: The Group maintains an effective Control framework to manage the inherent Financial Crime Risks

The Group maintains a comprehensive and coherent Financial Crime Control framework to effectively manage and mitigate the inherent Financial Crime Risks to which it is exposed. The framework consists of a broad range of preventive, detective and corrective Controls to enable efficient risk mitigation and facilitate data-driven and evidence-based decision-making. To ensure continuous Financial Crime Risk mitigation and coverage, the Group performs ongoing assurance and testing of its Control framework and has business continuity and contingency plans in place.

Roles and Responsibilities:

- 1LoD is responsible for developing and implementing Controls that appropriately and holistically address the Financial Crime Risk associated with the Group's activities, including ensuring that Controls are regularly tested and improved based on changes in the Group's inherent risk exposure and any identified Control weaknesses.
- 2LoD is responsible for:
    - setting the minimum standards for the Group's Financial Crime Control framework,
    - reviewing the effectiveness of the Control framework and performing assurance, testing and technical validation activities and
    - developing and implementing Controls owned by 2LoD.

Principle 6: The Group applies due diligence measures when establishing and maintaining relationships with customers and Third Parties

Prior to establishing a relationship, the Group ensures that all customer, correspondent, Third Party and relevant non-customer relationships, such as network banks, are subject to appropriate Financial Crime due diligence measures. Risk-based due diligence is performed on an ongoing basis throughout the relationship's duration. The due diligence measures must be completed prior to allowing access to Products or executing any transactions. Third Parties are subject to specific Third-Party Financial Crime due diligence measures and Third Party contracts must include anti-Financial Crime risk provisions.

Roles and Responsibilities:

- 1LoD is responsible for:
    - developing and implementing operational procedures and associated governance that adhere to the Group minimum standards for customer, Third Party and correspondent due diligence, including ensuring that timely and efficient due diligence measures and processes are in place for the duration of the relationship and
    - overseeing Financial Crime-related contractual clauses.
- 2LoD is responsible for setting the Group's minimum due diligence standards for customers, Third Parties, correspondents and relevant non-customers and for ensuring that timely and efficient due diligence measures and processes are in place for the duration of the relationship, where owned by 2LoD. The minimum standards for Third Party Financial Crime due diligence must align with the Group requirements for Third Party Risk Management.

Principle 7: The Group detects indications of Financial Crime

The Group develops and implements capabilities to detect indications of Financial Crime by continuously evaluating, adjusting and enhancing monitoring, screening, intelligence and analytics-based Controls. Financial Crime Risks and activities relevant to the Group must be considered, including trends and emerging Financial Crime Risks.

Where legally permissible, detection Controls must include:

- transaction and activity monitoring for money laundering ("ML")/terrorist financing ("TF") risks,
- screening for ML/TF risks,
- sanctions screening,
- fraud monitoring and detection.
- adverse media searches or screening,
- observation lists screening and trigger events and incidents monitoring,
- export control compliance monitoring and
- thematic reviews and investigative deep dives.

Roles and Responsibilities:

- 1LoD and 2LoD are responsible for developing and implementing operational procedures, processes and associated governance that adhere to the Group minimum standards for Financial Crime detection, including efficient escalation processes to ensure timely reporting of identified suspicion.
- 1LoD owns the Group's detection solutions and is responsible for ensuring that indications of Financial Crime are identified and acted upon in a timely manner by implementing effective and efficient detection solutions covering the Group's business activities and Products and for maintaining the efficiency of the solutions through ongoing tuning, calibration and testing.
- 2LoD is responsible for setting the minimum standards for, and monitoring, as well as overseeing the Financial Crime detection solutions applied, including testing the effectiveness and efficiency of the detection Controls and identifying, analysing and communicating trends and Financial Crime Risks related to the 1LoD-owned detection framework.

Principle 8: The Group prohibits engagement in Products or relationships that are illegal or out of tolerance

The Group does not offer Products or engage in relationships that are prohibited by law and generally does not offer Products or engage in relationships that are out of its Financial Crime Risk Tolerance. Additionally, the Group does not engage in business activities with customers, Associated Persons, Third Parties or counterparties operating in or with links to jurisdictions that are comprehensively restricted by law. Where a Product, relationship or business activity is out of Financial Crime Risk Tolerance, the legal obligation to provide such must be considered independently.

Roles and Responsibilities:

- 1LoD is responsible for identifying such Products, relationships and jurisdictions and setting the 1LoD Risk Appetite within the Group's Financial Crime Risk Tolerance and the Group's Financial Crime Risk Position[1].
- 2LoD is responsible for overseeing compliance with international and national legal and regulatory regimes, the Group's Financial Crime Risk Tolerance and the Group's Financial Crime Risk Position.

Principle 9: The Group investigates and reports on suspicious activities, incidents of Financial Crime and potential Financial Crime violations

The Group maintains effective processes and Controls to ensure that suspicious activities, incidents of Financial Crime or potential Financial Crime violations are reported to the relevant competent authorities and followed up internally without undue delay.

Roles and Responsibilities:

- Employees are responsible for reporting potential Financial Crime incidents, violations and unusual activities and escalating those to 2LoD in a timely manner in accordance with the Group's governing documents to enable prompt reporting to the relevant competent authorities.
- 1LoD is responsible for managing risks following the identification of unusual and suspicious activity and must have procedures and processes to ensure risks are managed and escalated in a timely manner.
- 2LoD is responsible for having procedures and processes for investigating and reporting potential Financial Crime incidents, violations and suspicious activities to the Financial Intelligence Unit or other competent authorities and must inform the 1LoD risk owner when Financial Crime Risk has been identified.

[1] See Appendix 3 for 2LoD Financial Crime Risk Position Statement.

Principle 10: The Group ensures that its infrastructure and Products are not misused by Employees for Financial Crime purposes

Employees are prohibited from advising, facilitating, engaging or participating in activities that misuse the Group's infrastructure or Products for Financial Crime purposes or otherwise circumvent requirements imposed by this Policy and its underlying governing documents. The Group achieves this through:

- appropriate pre- and in-employment screening and monitoring of Employees for indications of Financial Crime Risks, where legally permissible,
- implementation of Controls to identify, investigate and apply appropriate disciplinary actions to Employees engaging in activities or behavior that leads to the misuse or potential misuse of the Group's infrastructure or Products for Financial Crime purposes, or who are grossly negligent in complying with this Policy,
- setting requirements, thresholds and Controls on the giving and receipt of gifts and hospitalities and
- adherence to the Group requirements on reporting actual or perceived Conflicts of Interest in accordance with the Conflicts of Interest Policy, as far as they apply to the identification and management of Financial Crime Risks.

Roles and Responsibilities:

- The Group is responsible for implementing and maintaining processes and Controls to manage the Financial Crime Risks associated with its Employees.
- Employees are responsible for adhering to the Group's Financial Crime compliance requirements and for escalating Financial Crime concerns or violations in accordance with the Group's governing documents.
- Human Resources is responsible for ensuring that Financial Crime Risks are considered in recruitment and talent acquisition processes and throughout the employment lifecycle.

Principle 11: The Group encourages and facilitates prompt reporting and escalation of Financial Crime-related concerns

The Group establishes a framework and multi-channel approach for prompt reporting and escalation of Financial Crime related concerns, ensuring multiple avenues for safe and effective communication. Employees, Third Parties and external parties are encouraged to escalate their concerns through line management chains or dedicated reporting channels for Unusual Activity Reporting. However, there may be instances where this is not possible or where a reporter may require protection or anonymity. In such cases, the whistleblowing scheme must enable prompt reporting and escalation of Financial Crime-related concerns, always protecting the identity and rights of the whistleblower. The requirements, roles and responsibilities related to the operation of the Group's Whistleblowing channels are detailed in the Group Whistleblowing Policy.

Roles and Responsibilities:

- The Group is responsible for developing and maintaining a robust escalation framework to manage and respond to Financial Crime-related concerns effectively. This includes ensuring that Employees are provided anonymity and protection in accordance with applicable regulatory and internal whistleblowing requirements and that easily accessible reporting channels are available.
- Employees are responsible for being aware of and escalating Financial Crime concerns through the designated reporting channels and must escalate potential breaches, Financial Crime concerns, non-compliance with applicable legislation and any warnings on Financial Crime incidents identified during their employment to the AML Responsible Person or AML Responsible Compliance Officer without undue delay

5. Breaches and escalation

5.1 Breaches

If an Employee identifies a breach (defined as an instance of non-compliance with applicable laws, rules, regulations and/or requirements in this Policy that is not already subject to a deviation or exemption), it must be reported to FinancialCrimeBreaches@danskebank.dk in accordance with the Financial Crime Compliance Breach Business Procedure. If the breach is also defined as an operational risk event, it must be registered and categorised immediately in ORIS according to the Non-Financial Risk Event Escalation Instruction.

5.2 Escalation

The Administrator of this Policy must escalate significant breaches of this Policy, including significant Financial Crime Risk events about which they are notified to the Board of Directors in accordance with the Non-Financial Risk Event Escalation Instruction. Significant breaches include, but are not limited to:

- non-compliance with applicable Financial Crime legislation and regulation,
- failure to implement the Group's risk taxonomy or inaccurate reporting of material risks as defined by the taxonomy, Financial Crime Policy and related instructions,
- excessive risk-acceptance culture or behaviour conflicting with the Group's strategy, culture or non-financial Risk Tolerance framework,
- inadequate Controls and processes to identify, manage and mitigate Financial Crime Risks,
- advising, facilitating, engaging or participating in activities or behaviour misusing the Group's infrastructure or Products for Financial Crime purposes and
- actions or behaviour to circumvent Financial Crime requirements imposed by the Group's Financial Crime Policy and related instructions.

When there is doubt about whether an event or violation is of a significant or material character, the relevant Financial Crime Compliance Advisory & Assurance Team[2] must be consulted for further guidance.

6. Implementation

The requirements outlined in this Policy must be operationally implemented as soon as possible, and no later than 90 days following their publication. Subsidiaries must implement them no later than 90 days following an adoption decision. After the 90-day implementation period, a status update on whether the Policy is implemented, implemented with exemptions or not implemented must be submitted to Financial Crime Compliance Policies & Governance[3]. In cases where the Policy has not been fully implemented, the report must outline the remaining gaps and include a detailed timeline for their remediation.

7. Exemptions

If the requirements of this Policy cannot be met, an exemption request must be raised:

- within 90 days of publication for any requirements that cannot be implemented within 90 days, and/or
- as soon as the need is identified for reasons other than implementation timelines.

Exemptions should be raised in accordance with the Financial Crime Compliance Exemption Handling Business Procedure.

[2] fcadvisory@danskebank.dk

[3] financialcrimepolicy@danskebank.dk

Appendix 1 – Definitions

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

Associated Person	any natural person or legal entity, either incorporated or unincorporated, who performs services for or on behalf of the Group.
Board of Directors	the Board of Directors of Danske Bank A/S.
Control	any action or activity designed to manage risks that might otherwise impact the achievement of the objectives of the process, Product, system or regulation.
Employee	covers: • an individual who is employed by the Group on a permanent or temporary basis • an individual who is working for but is not directly employed by the Group (including consultants, contractors, agency workers, etc.)
Financial Crime	the generic term for money laundering, terrorist financing, sanctions, bribery, corruption, fraud, tax evasion and facilitation of tax evasion as defined in the Group's Enterprise Risk Management framework.
Financial Crime Risk	the risk of internal or external parties using the Group's infrastructure and Products to move and conceal proceeds of criminal conduct, defraud, manipulate or circumvent applicable rules, laws and regulations in the areas of Financial Crime.
Group	Danske Bank A/S including its Branches and Subsidiaries.
Group Functions	refers to and covers areas in the Group such as: • CFO area • Group Human Resources ("HR") • Group Internal Audit • Group Legal • Group Risk Management • Group Compliance • Group Sustainability, Stakeholder Relations, Communications & Marketing • Technology & Services
Product	a collective term covering: • products and services offered by the Group to Customers of the Group or to any other person or legal entity • products and services that are offered by a Third Party (including partnerships) and distributed by the Group
Regulated Person	person holding a Financial Crime related role which is required under applicable Financial Crime law or regulation, including Money Laundering Reporting Officers and AML Responsible Persons or equivalent
Risk Appetite	business'/1 LoD articulation of the level of risk it is willing to take in pursuit of its commercial strategy/plans while staying within the outer boundaries (Risk Tolerance) defined by the Board.
Risk Tolerance	the aggregate level of risk the Group is willing to accept in pursuit of its long term objectives while maintaining a stable financial position.

Senior Management	the Executive Leadership Team, Subsidiary executive management and key function holders of the Group.
Subsidiary	any undertaking over which Danske Bank A/S exercises control. For the purpose of this definition "control" means any of the following: • direct or indirect ownership of more than fifty per cent (50%) of the share capital or other ownership interest in any other person • the direct or indirect right to exercise more than fifty per cent (50%) of the votes in any other person • 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 • 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.
Third Party	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[4].

Appendix 2 – Author and input providers

Information regarding the author and input providers in Appendix 2 is intended for internal use only and has been excluded from the external version of the Policy. This ensures that sensitive internal details are safeguarded while maintaining transparency in publicly shared documents.

Appendix 3 – 2LoD Financial Crime Risk Position Statement for Comprehensively Restricted Territories

When evaluating the overall Financial Crime Risks from specific geographical areas and regions, the Group has determined it necessary to generally avoid any direct or indirect activities involving the following jurisdictions, unless explicitly permitted and approved in accordance with requirements set out in the Group's governing documents:

- Iran
- North Korea
- Syria
- Belarus
- Non-government controlled Ukrainian areas
- Cuba
- Russia

These countries and regions are comprehensively restricted due to a combination of significant risk factors, including:

- sanctions risks,
- bribery and corruption risks,
- tax evasion risks,
- fraud risks,
- terrorist financing risks,
- money laundering risks,
- involvement in cyber-attacks,
- involvement in the proliferation of weapons of mass destruction and
- involvement in cryptocurrency mining.

Some activities, such as educational activities, activity relating to humanitarian assistance and disaster relief, non-commercial personal remittances, diplomatic missions, intellectual property or government repatriation payments facilitated through Danske Bank Products, may be carried out if strict criteria are fulfilled. For further detail, please refer to underlying instructions as well as jurisdiction-specific Financial Sanctions guidance.

Exceptions

Activity outside the Group's 2LoD Financial Crime Risk Position Statement for Comprehensively Restricted Territories may be carried out only in exceptional circumstances, subject to Financial Crime Compliance review and approval in accordance with the Group's sanctions exception process and any other relevant governance processes.

Breaches and Escalation Requirements

Potential or actual breaches of the Group's 2LoD Financial Crime Risk Position Statement for Comprehensively Restricted Territories must be reported in accordance with the Group's sanctions risk event process and any other relevant governance processes.