

# International Sanctions Policy - Overview

## Introduction

Sanctions are laws, regulations or orders enacted by governing authorities to support foreign policy and national security objectives. They prohibit certain activities involving foreign states or jurisdictions, organizations, or individuals considered a threat to international peace and security and form an essential instrument of the international community.

Sanctions may take the form of financial restrictions, travel bans, arms and related material embargoes, export/import limitations, and suspensions of technical or financial assistance. Depending on the objective, these measures may target specific economic sectors or apply broadly to a designated person or a sanctioned jurisdiction.

## Sanctions Program

National Bank of Canada and its subsidiaries (« the Bank ») comply with sanctions in force in each of the jurisdictions in which they operate. To do so, the Bank has implemented an enterprise-wide Sanctions Program grounded in a rigorous International Sanctions Policy (« the Policy ») that applies to all Business Units, subsidiaries, and foreign centres (« Business Units »), regardless of location.

The Policy sets out compliance requirements, the oversight and operational framework, and the escalation processes necessary to identify and address sanctions related issues in a timely manner. It is read in conjunction with the other Bank and Compliance policies, notably the AML/ATF Program, screening standards, and Know Your Client identification and documentation standards. This document is a summary of the Policy.

## Key Elements of the Policy

### Risk Assessment

The effectiveness of the Program relies on control measures that reflect inherent risks associated with the Bank's business relationships, countries of operation, distribution networks, and products and services offered. Sanctions exposure for Business Units forms part of the enterprise AML/ATF Program risk assessment. This risk-based approach enables controls to be tailored to the most sensitive geographies, transaction types and sectors.

### Compliance Requirements and Screening

The Bank complies with sanctions regimes applicable in the jurisdictions where it operates. Compliance may restrict or prohibit the provision of financial services where an activity involves prohibited conduct or designated persons/entities. Any attempt to evade sanctions or related controls is strictly prohibited.

To ensure compliance, the Bank conducts screening of accounts, products, transactions and third parties against consolidated official sanctions lists that are updated daily and include designated persons and



entities under applicable sanctions. Screening also extends to non-clients, such as suppliers, partners, originators, and beneficiaries of international payments.

Where screening identifies a potential match, the Bank performs analysis and applies prescribed measures, such as freezing property, rejecting transactions, or declining services. The Bank also complies with regulatory reporting obligations to competent authorities.

A transaction involving a sanctioned jurisdiction may be prohibited under the Bank's internal policy, even if not directly prohibited under applicable sanctions.

## **Violations and Penalties**

In the event of violation of sanctions, the Bank may be exposed to civil and criminal fines and penalties, including imprisonment. The Bank may also be prohibited from establishing, continuing or expanding business operations in a given jurisdiction following a sanctions breach.

Any Bank employee who contravenes sanctions or this Policy is subject to corrective and disciplinary measures in accordance with applicable internal policies.

## **Exceptions, Licences and Certificates**

Regulatory authorities may provide exceptions or issue licences or certificates authorizing activities otherwise prohibited by sanctions. The Bank does not generally take charge of client applications for permits or exceptions. However, where an exception is confirmed and consistent with internal policy, the Bank may decide to participate in the relevant activity.

## **Training**

Training is a core component of the Sanctions Program. It is overseen by the Chief Anti-Money Laundering Officer (« CAMLO ») and deployed enterprise-wide. An annual general module is mandatory for all employees, with specialized training provided to units with higher exposure to sanctions risk.

## **Specific Standards**

Certain Business Units, due to their exposure, may be required to establish sector-specific standards and procedures in collaboration with Compliance. These controls address transactions, sectors or jurisdictions that present heightened sanctions risk.

## **Effectiveness of Controls**

The effectiveness of controls is verified through an annual self-assessment under the AML/ATF Program, with results communicated to the CAMLO and the Board. In addition, Internal Audit conducts an independent examination at least every two years to assess the robustness of controls and Program compliance.

## **Roles and Responsibilities**

- **Board of Directors and GRC:** ultimate oversight of the Program and approval of the Policy.



- **CAMLO:** appointed by the Board; provides independent oversight; ensures regulatory compliance, risk management, control supervision, periodic program evaluation, and reporting of conclusions to the Board.
- **Compliance:** responsible for developing and maintaining the program; analyzing applicable laws and regulations; issuing standards and tools for Business Units; managing sanctions lists and exception requests; and liaising with regulatory authorities.
- **Compliance Officers:** responsible for operational implementation of the Program and managing relationships with local regulators.
- **Business Units:** responsible for integrating controls, identifying gaps, and implementing corrective action plans where necessary.

## Policy Review and Approval

The Policy will be reviewed at least annually by the CAMLO in order to keep its content current and effective and will be submitted every three years to the GRC for approval. The Policy may also be revised and updated as needed in response to material changes in the regulatory environment or other significant developments that justify Policy revision.

