POLICY FOR THE RIKSBANK'S WORK TO PREVENT MONEY LAUNDERING, TERRORIST FINANCING AND VIOLATIONS OF INTERNATIONAL SANCTIONS

DECISION DATE:	14 December 2023
DECISION BY:	The Executive Board
RESPONSIBLE DEPARTMENT:	Internal Control and Operational Support Department
RESPONSIBLE MANAGER:	Compliance function
DNR:	2023-01190
DOCUMENT CLASSIFICATION:	RB PUBLIC

Policy for the Riksbank's work to prevent money laundering, terrorist financing and violations of international sanctions

Content and purpose

This policy describes how the Riksbank shall work to counteract the risks of the Riksbank being used for money laundering and terrorist financing or violating international sanctions. The purpose of this policy is to guide the Riksbank's employees in this work.

Target group

This policy is addressed to all the Riksbank's employees. The term "employee" refers to all employees and contractors who have access to a Riksbank computer and to the Riksbank's systems and who participate in the Riksbank's day-to-day operations.

Contents

1 Introduction

The Riksbank as a central bank is not subject to the Act on Measures against Money Laundering and Terrorist Financing (2017:630) (the Anti-Money Laundering Act). The Riksbank is therefore not obliged to take the measures provided for in that Act or regulations issued under that Act. On the other hand, the Riksbank's reputation may be seriously damaged, and confidence in the entire financial system may be damaged, if the Riksbank is used for money laundering or terrorist financing. The Riksbank's employees may be subject to criminal law provisions in the Act (2014:307) on penalties for money laundering offences that are generally applicable to individuals and that in criminal matters supplement the Act on Measures against Money Laundering and Terrorist Financing.

To minimise the risk of damage to confidence in the Riksbank and to protect its employees from participating in crimes when carrying out their tasks, the Riksbank uses, in those parts of its operations where there is a risk of money laundering or terrorist financing, the Anti-Money Laundering Act and Finansinspektionen's regulations in this area for guiding purposes. However, it should be clarified that in cases where there is directly applicable legislation for the Riksbank to comply with, which does not correlate with what is stated in the Anti-Money Laundering Act, the binding law must always take precedence.

Unlike the money laundering legislation that the Riksbank applies on a voluntary basis, the Riksbank is directly subject to the provisions of the Act (1996:95) on Certain International Sanctions. According to this Act, under certain circumstances, a penalty may be imposed on a party violating a prohibition in an EU Regulation on economic sanctions or in a supplementary provision adopted by the Government due to a decision on sanctions by the United Nations or the EU. This policy therefore also regulates how the Riksbank works to comply with sanction decisions.

1.1 Underlying regulatory framework

1.1.1 Applicable regulations

The Sveriges Riksbank Act (SFS 2022:1568).

The Rules of Procedure for Sveriges Riksbank

Act (2014:307) on penalties for money laundering offences

Terrorist Offences act (2022:666)

Act on Certain International Sanctions (1996:95)

1.1.2 Regulations that the Riksbank uses for guiding purposes

Act (2017:630) on Measures against Money Laundering and Terrorist Financing

Finansinspektionen's regulations amending the Act on Measures against Money Laundering and Terrorist Financing (2017:11)

1.2 Definitions

Money laundering has the same meaning as in Chapter 1, Section 6 of the Anti-Money Laundering Act. This means actions with respect to money or other property arising from criminal offences or criminal activities that may conceal the property's connection with crime or criminal activity, may promote the possibility of someone acquiring the property or its value, may promote the possibility for someone to evade legal penalties; or means that someone acquires, holds, claims the right to, or uses the property.

Terrorist financing has the same meaning as in Chapter 1, Section 7 of the Act. This means, in short, collecting, receiving or providing money or other property with the intention of the property being used or knowing that it is intended to be used to commit or otherwise contribute to terrorist offences,[1] or attempting, preparing or conspiring to commit terrorist offences; or particularly serious crimes.[2]

International sanctions impose restrictions on the freedom of action of a specific state, group, company or individual. Sweden follows decisions issued by the UN and/or the EU, as well as sanctions imposed by the Swedish Government on the recommendation of the UN or the EU that have been approved by the Riksdag.

Business connection has the same meaning as in Chapter 1, Section 8 of the Anti-Money. A business connection is a business relationship which, when established, is expected to have a certain duration.

General risk assessment has the same meaning as in Chapter 2, Section 1, paragraph 1 of the Anti-Money laundering act: and refers to an assessment of how the products and services provided in the business can be used for money laundering or terrorist financing and the size of the risk of this happening.

Relevant operations refers to an entity, or part of a unit, at the Riksbank whose products or services are in any way deemed to be exposed to the risk of being used for money laundering, terrorist financing or violations of international sanctions.

Customer refers to natural persons and legal entities such as central banks, financial institutions and financial bodies with which the Riksbank has a business connection.

[1] Section 6 of the Terrorist Offences act (2022:666)

[2] Section 2 of the Terrorist Offences act (2022:666)

For the purposes of this policy, a legal entity or natural person requesting the redemption of invalid banknotes is also referred to as a customer.

Person in a politically exposed position (PEP) has the same meaning as in Chapter 1, Section 8, paragraph 5, of the Anti-Money Laundering Act, that is a natural person who has or has had an important public function in a state or in an international organisation.[3] A person should still be assessed as PEP for 18 months after they have left their role.

Beneficial owner has the same meaning as in Chapter 1, Section 8, point 6 of the Anti-Money Laundering Act and is deemed to be a natural person who, alone or together with another, ultimately owns or controls a legal entity, or a natural person for whose benefit someone else is acting.[4]

2 Roles and responsibilities

Heads of departments are responsible within their area of responsibility to ensure that:

- the risk of their own department's activities being used for money laundering or terrorist financing is identified
- the activity-specific general risk assessments are carried out
- the person who carries out tasks relevant to preventing the activities concerned from being used for money laundering or terrorist financing has the appropriate knowledge and competence
- the risk of violations of international sanctions in their own department's operations is identified
- the identified risks in the relevant operations of the department are evaluated, managed and reported
- relevant rules and routine descriptions in accordance with this policy are drawn up

Regulatory compliance specialists at the Risk Division are responsible for:

- informing employees of this policy
- coordinating the Riksbank's work to prevent money laundering, terrorist financing and violations of international sanctions

[3] For the definition of an important public function in a state, see Chapter 1, Section 9 of the Anti-Money Laundering Act

[4] See also Chapter 1, Sections 3-7 of the Act (2017:631) on registration of beneficial owners

- informing relevant employees about new trends, patterns and practices, as well as anything relevant to preventing money laundering, terrorist financing and violations of international sanctions
- compiling the general risk assessment that applies to the entire Riksbank
- providing advice and support to business areas in matters related to money laundering and sanctions/ regulations and supporting them by identifying risks of being used for money laundering or terrorist financing
- training employees on an ongoing basis, see section 6
- reporting to the Police Authority, see section 7
- carrying out checks to ensure that the Riksbank and its employees comply with this policy, see section 8

Each individual **employee** shall:

- comply with this policy and associated rules and routine descriptions
- participate in every compulsory course and ensure they increase their own knowledge in the field

For the responsibilities of the **Internal Audit Department** in the area of money laundering, see the Riksbank's Policy for internal auditing.

3 Measures to combat money laundering and the funding of terrorism

3.1 Risk assessment

All heads of department at the Riksbank shall annually evaluate whether there is a risk that their operations may be used for money laundering or terrorist financing. If a head of department assesses that an operation within his department is in any way exposed to this risk, then a general risk assessment specific to that particular operation shall be carried out, an activity-specific general risk assessment. These general risk assessments at operational level shall take into account:

- the types of products and services provided by the operation;
- the customers and distribution channels that it has and
- the geographical risk factors present in the activities concerned and the manner in which they could be used for money laundering or terrorist financing;

The Riksbank uses the classification high, medium-high, medium and low to define the risk. The activity-specific general risk assessment shall then be updated by those areas at least annually, and if necessary (e.g. if the activities change).

The regulatory compliance specialists at the Risk Division are responsible for establishing a comprehensive general risk assessment for the entire Riksbank, based on the operations' general risk assessments. The purpose of this overall general risk assessment is to be able to provide an overall picture of the risk of the Riksbank being used for money laundering or terrorist financing.

3.2 Rules and routines

Where vulnerabilities or risks of potential use of the business for money laundering or terrorist financing are identified in the risk assessment for specific operations, the operations are responsible for drawing up relevant governing documents describing how to manage those risks. Documents shall be adapted to both the specific risks of the operations and the general risk assessment. They shall also be continuously adapted to address new and changing risks of money laundering or terrorist financing.

3.3 Customer due diligence measures

To manage the risks of money laundering or terrorist financing, customer due diligence measures shall be taken in the relevant activities. These measures shall be adapted to the specific operations and take into account whether the respective customer relationship involves a business connection or only covers single transactions.

Depending on the type of relationship the Riksbank has with the customer, customer due diligence measures may include:

- customer identification, which includes verification of the identity of a natural person, for example by electronic identification, by obtaining information on the person's name, address, personal identity number or equivalent or by a certified copy of an identity document;
- investigation of whether a legal entity that is a customer of the Riksbank has a beneficial owner and, if so, verification of the identity of the beneficial owner;
- an investigation of whether the customer can be identified as a PEP or as a family member or known colleague of a PEP;[5]
- an investigation into whether establishment in a high-risk third country exists;

[5] For the definition of a family member and known colleague, see Section 10 of the Anti-Money Laundering Act

- an investigation of the purpose and nature of the business connection (this need not be verified in the case of individual transactions).

3.3.1 Risk assessment of customers

Information collected in connection with the customer due diligence measures and the activity-specific general risk assessment shall form the basis for the risk assessment of the individual customer, i.e. the customer's risk profile, that each area of operations must make. One way to determine the customer's risk profile is to consider the circumstances that according to Chapter 2, Sections 4-5 of the Anti-Money Laundering Act may indicate a low, or medium/high risk of being used for money laundering or terrorist financing in the relationship with a customer. If the risk associated with the business connection is considered low, simplified customer due diligence measures can be taken. If the risk is considered to be medium/high, stricter customer due diligence measures must be taken. Stricter customer due diligence measures may involve gathering more information about the origin of the customer's financial resources, conducting more extensive investigations or following up the business connection more frequently.

3.3.2 Follow-up of business connections

The operations that have customer relationships in the form of ongoing business connections shall follow up on them to ensure that their knowledge of the customer is up-to-date and sufficient to address a risk of money laundering or terrorist financing. The follow-up of business connections shall take into account, among other things, the results of transaction checks carried out on an ongoing basis to detect any discrepancies. The frequency of follow-up of a business connection shall be determined on the basis of the customer's risk profile and other risk indicators.

3.3.3 Suspicion of money laundering or terrorist financing

If suspicious activities or transactions are brought to the attention of the public, enhanced customer due diligence or other necessary measures shall be taken to assess whether there are reasonable grounds to suspect money laundering or terrorist financing. See also Section 7 on reporting to the Swedish Police Authority in case of suspected crime.

4 Sanctions

All heads of department at the Riksbank shall annually evaluate and document which of the Riksbank's operations need to take sanctions legislation into account. For the Riksbank, sanctions legislation may include, for example, a ban on carrying out transactions for natural persons or legal entities that are included in a sanction list or a ban on entering into agreements and other connections with such a natural person or legal entity.

The operations within the Riksbank that need to take into account the sanctions legislation must ensure that relevant international sanctions decisions are complied

with, to prevent the Riksbank from violating them. The respective operations shall also have rules, routine descriptions or both as to how the operations are to prevent violations of international sanctions. These must state how a hit against a sanction list is handled.

5 Preservation of documents and data

The operations concerned by the risk of being exploited for money laundering and terrorist financing shall develop and regularly update activity-specific regulations and routine descriptions for the preservation of documents and data (including the processing of personal data).

These regulations and routine descriptions shall be drawn up in accordance with the Archives Act (1990:782), the Public Access to Information and Secrecy Act (2009:400) and the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and the provisions thereof applicable at the time.

6 Training

The regulatory compliance specialists at the Risk Division are responsible for ensuring that all employees receive continuous training in the work against money laundering and terrorist financing and on the relevant regulations and in the area of sanctions, to ensure a continuous update of knowledge. The compliance specialists are also responsible for introducing new employees to the topic.

Targeted training and information for new employees takes place at operational level. This training should be tailored to the specific risks of being exploited for money laundering or terrorist financing purposes.

7 Reporting

The regulatory compliance specialists at the Risk Division are ultimately responsible for reporting to the Police Authority (Financial Intelligence Unit) when it comes to suspicion that a customer is trying to use the Riksbank for money laundering or terrorist financing. The regulatory compliance specialists may appoint someone within the operations in their place to prepare these reports.

According to the Sveriges Riksbank Act[6], the Riksbank is obliged to inform the Police Authority if information arises in parts of its operations that gives reason to assume that a crime has been committed, such as suspicion of money laundering offences. In cases other than those referred to above, the Security Division (SÄK) is responsible for reporting to the Swedish Police Authority.

[6] Chapter 7, Section 23 of the Sveriges Riksbank Act (2022:1568)

8 Compliance

Regulatory compliance specialists at the Risk Division are responsible for monitoring and continuously verifying compliance with this policy. Regulatory compliance specialists shall report regularly, at least once a year, the results of the overall general risk assessment and the risks identified to the Executive Board via the interim report.

9 Entry into force

This Policy enters into force on 1 January 2024. This policy repeals the previous Policy on the Riksbank's work against money laundering and terrorist financing and work to prevent violations of international sanctions (DNR 2022-00634), which was decided on 8 November 2022.