Results of DNB's examinations on compliance with sanctions regulations

DeNederlandscheBank

EUROSYSTEEM

Table of contents

Introduction 3

Risk analysis 4

Circumvention of sanctions 5

Dual-use goods screening 6

Sanctions screening system 7

The relationship concept and minority shareholders 8

Introduction

In this document, DNB offers feedback on a number of themes and findings from the cross-sectoral thematic examination on compliance with sanctions regulations and the examination of the effectiveness and efficiency of sanction screening systems.

Sanctions regulations have tightened considerably since the beginning of the war in Ukraine, and further changes are expected to follow. The implementation of the new sanctions packages requires significant commitment and flexibility from financial institutions. Given the challenges that are emerging in today's rapidly changing sanctions landscape, it is important to reflect thoroughly on this period of crisis in order to be better prepared for such situations in the future.

Risk analysis

In our assessment of institutions' administrative organisation and internal control structure (AO/IC), we look at the sanctions risks institutions face and how these are analysed and recorded in their systematic integrity risk analysis (SIRA). We find that institutions that have already identified and analysed sanctions risks in their SIRA based on the available data are well positioned to adequately handle potential threats. Systems appear to work better when explicit attention has been paid to the circumvention of sanctions and the detection or screening of dual-use goods.

However, real-world sanctions scenarios may differ from the risks already identified in an institution's SIRA. That is why many institutions have conducted ad hoc risk analyses to assess portfolio risks related to new sanctions packages, allowing them to take additional mitigation measures.

In practice, we see significant differences in the extent and depth to which institutions have analysed their customer portfolios, for instance with regard to exposure to countries with an increased sanctions risk. Institutions that had carried out such analyses were able to respond more quickly to events following Russia's invasion of Ukraine and also needed less time to get a clear picture of the impact the new sanctions packages would have on their operations.
We also see differences in terms of the depth and granularity of the scenarios used in institutions' SIRAs to identify potential vulnerabilities.
We encourage institutions to draw lessons from their experiences and the challenges they faced over the past year. Institutions can examine how they can tighten up their portfolio analysis and the analysis of various sanctions scenarios relating to, for example, the circumvention of sanctions and dual-use goods. Doing so will help them optimise their preparedness for future sanctions.

Circumvention of sanctions

As described in DNB's integrity risk analysis good practice document (*Good Practice Integriteitrisicoanalsye*), one of the risks that can be included in a SIRA is that of sanctions circumvention.

The extensive sanctions packages that have been imposed against Russia and Belarus include a comprehensive set of import and export restrictions. These sanctions can be circumvented, for example by exporting goods via non-sanctioned countries. We have found that there are still a number of institutions that do not pay sufficient attention to this risk. Meanwhile, there are also institutions that conduct data-driven research to detect increasing flows of money and goods to countries in the vicinity of sanctioned countries, or to countries that are known to cooperate with sanctioned countries.

Customers whose UBOs have been placed on sanctions lists can also circumvent sanctions by changing their ownership and control structure. This circumvention strategy has been used in particular in response to Russian oligarchs being placed on sanctions lists, which had consequences for the financial institutions involved. The chances of detecting circumvention are improved by being alert to structural changes and, in particular, situations where shares are placed in a separate entity or transferred to other non-sanctioned UBOs.

Dual-use goods screening

Several sanctions packages include prohibitions or restrictions on the provision of financial services for goods.[1] These include military goods, dual-use goods, strategic services (such as software and technology) and goods that can be used for internal repression and torture.

The first sanctions packages against Russia led to a significant expansion of the ban on the trade in dual-use goods (goods that could strengthen Russia's military and technological capabilities). As a result, transaction screening for dual-use goods and other means of detection have become increasingly important in ensuring effective compliance with sanctions regulations.

Products that are prohibited from being imported or exported are listed in various annexes to EU regulations. We are aware that screening for or detecting dual-use goods requires a different approach than that used for screening individuals and entities, and that many institutions will need time to make the necessary adjustments. Nevertheless, there are also institutions that not only recognise the importance of screening for dual-use goods, but that have also implemented automated detection measures. Overall, we believe that further improvements in this area are possible as the sector gains more experience.

One possible detection measure could be to include descriptions of dual-use goods in automated transaction filtering systems to ensure that illegal transactions are detected and investigated before they are executed. This may not be feasible for all transactions, but based on their risk appetite institutions may choose to screen specific kinds of transactions, such as payments to Russia, Belarus and Ukraine, or to other countries with an increased sanctions risk.

In addition to transaction screening, institutions can also analyse or investigate sanction risks with regard to import and export restrictions and dual-use goods screening in thematic investigations by the institutions, for example to determine whether customers that operate in a particular sector comply with import and export restrictions and sanctions on dual-use goods. Should such an analysis reveal customer risks that lie outside the institution's risk appetite, it can conduct an event-driven review and, where necessary, report any unusual transactions.

Yet another way to manage this risk is by setting up mitigation procedures, such as a pre-transaction approval procedure for transactions to and from sanctioned countries. This requires customers to submit a request, including an explanation of the purpose of their transaction and relevant documentation, which is then assessed by the institution before it decides whether or not to execute the transaction. Pre-transaction approval can also be used for transactions related to trade finance activities. Ultimately, the risk appetite and business model of the institution in question determines which measures are appropriate.

1 Guideline on the Wwft and the Sw, December 2020 version

Sanctions screening system

Our examination of sanctions screening systems used test data to assess the effectiveness and efficiency of the systems in place at a number of institutions. Overall, institutions' sanctions screening systems were found to be highly effective. This means that most of the sanctioned persons and entities included in the test produced a hit against the relevant sanctions lists. While institutions generally achieved high scores on their effectiveness at screening against EU and UN sanctions lists, there is still room for improvement when it comes to screening against the Dutch sanctions list. This National sanctionlist terrorism (*Nationale sanctielijst terrorisme*) was not always included in the relevant screening systems.[2]

We also note that many institutions trust that their (external) screening systems function adequately, and that they do not carry out their own periodic assessments, such as spot checks.

Institutions can set their screening systems to produce hits for names that are similar to names on relevant sanctions lists ("fuzzy matching"). The examination revealed that several institutions still struggle to screen for and detect manipulated sanctions data based on fuzzy matching. Institutions that failed to adequately detect manipulated data were asked to take remediation measures. Continuous testing and sufficient knowledge and expertise in this field therefore remain necessary. In addition, some of the institutions that were included in our examination did not know the fuzzy matching percentage of their system or were not aware that this percentage can be adjusted by the screening system provider at their request.

There are also institutions that do conduct periodic assessments, and that are in discussions with the providers of their sanctions screening systems to become more conversant in the operation of the software. These institutions are better equipped to know which sanctions lists should be screened against and whether the way their systems are configured is appropriate for their products, services and activities (for instance in relation to where the institution is based or the countries with which it does business). Further areas of concern in the various screening systems that were examined were the detection of dual-use goods as well as (to a lesser extent) the detection of sanctioned bank identifier codes (BICs).

2 National sanctionlist terrorism is a freezing instrument and derives from the international obligation set out in United Nations (UN) Security Council Resolution 1373 (2001). Official announcements related to the National sanctionlist terrorism are published on overheid.nl. The search term "Terrorisme 2007-II" can be used to find relevant publications in the Government Gazette. It is also possible to sign up for email notifications regarding official changes to the list.

The relationship concept and minority shareholders

The examinations revealed that some institutions do not apply sanction screening to their customer's minority shareholders. Given the broad definition of the relationship concept (*relatiebegrip*) in the Regulation on Supervision pursuant to the Sanctions Act 1977 (*Regeling toezicht Sanctiewet 1977 - RtSw*), we interpret the statutory requirement such as to require institutions to screen all shareholders, including their customers' minority shareholders, as well as all directors of these shareholders, against the sanctions lists. If the UBO limit of 25% is used as a minimum threshold, potentially sanctioned shareholders with lower ownership percentages may go unidentified, creating a risk of (indirectly) making financial resources available to such minority shareholders. This also creates the risk of a customer incorrectly being qualified as non-sanctioned. This could be the case, for example, if five sanctioned shareholders each have 11% ownership in and/or control over the customer.[3]

However, we understand from the sector that screening minority customer shareholders is not a market practice and that sanctions regulations on this subject are interpreted differently across Europe. In response to these signals, we have submitted this issue to the European Commission.

Pending the European Commission's response, we will give low priority to enforcement in this area. As soon as the European Commission has made its position clear, we will communicate accordingly with the sector.

3 See European Commission Consolidated FAQs on the implementation of Council Regulation No 833/2014 and Council Regulation No 269/2014 – Question 8.

P.O. Box 98, 1000 AB Amsterdam
+31 (0)20 524 91 11
dnb.nl

Follow us on:

DeNederlandscheBank

EUROSYSTEEM