Integrity Supervision in Focus

2024-2025

DeNederlandscheBank

EUROSYSTEEM

Contents

1 Introduction

Purpose and background of this report

De Nederlandsche Bank (DNB) conducts integrity supervision of, amongst others, banks, payment service providers, crypto service providers, insurers, pension funds, trust offices and financial institutions on the BES islands. Our integrity supervisors monitor compliance by supervised institutions with relevant legislation. The aim of this new report, entitled Integrity Supervision in Focus (ISF), is to share the insights from our integrity supervision more widely.

In doing so, ISF is aligned with previous DNB publications. Supervision in Focus highlights three key pillars that contribute to effective supervision. Our Supervisory Strategy 2021-2024 sets out our risk-based approach and elaborates on the focal points of our supervision. ISF offers additional insights that complement these two publications by addressing relevant developments within the specific domain of integrity supervision, seeking to present an integrated overview of our supervision of different sectors. ISF does not contain new policy.

Following the release of this report, DNB will no longer issue separate sector letters, which we used to share by email with supervised institutions until last year.

The following topics are covered in this publication:

- **Dialogue with the sector**

This chapter describes how, following the publication of the report "From recovery to balance" in September 2022, DNB followed up on its intention to engage in a dialogue with supervised institutions on a more targeted approach to compliance with the Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft).

- **Integrity supervision findings**

Here we provide general feedback on the positive developments and vulnerabilities we have identified in supervised institutions' management of integrity risks. This feedback is primarily based on the results of supervisory examinations conducted between July 2022 and December 2023.

- **Measures taken by DNB**

This overview shows how DNB has used its supervisory instruments to support necessary remediation at supervised institutions.

- **Sectoral integrity risk analyses**

DNB conducts integrity supervision using a risk-based approach. To improve this approach, we map the key integrity risks for each sector on an annual basis. These sectoral analyses set out which integrity risks we deem to be most relevant in different areas of the financial services industry. The overview presented is mainly based on an analysis of external sources and DNB's integrity risk reporting (IRAP).

Dialogue with the sector

Ongoing dialogue with sectors and representative organisations

We have an ongoing dialogue with the institutions we supervise, and we take the input and signals that we receive into account in our supervision. In addition to institutions and representative organisations, we also consult other stakeholders, for example when developing the *Wwft* Q&A and Good Practices. Moreover, we share our knowledge and collaborate in public-private contexts, including through the Financial Expertise Centre (FEC). The signals that we receive from various organisations have led to legislative recommendations, as well as feedback on new legislation.

Roundtables: risk-based approach

In a series of roundtables with the banking sector that began in late 2022, we have been discussing a more focused and risk-based approach to *Wwft* compliance. DNB, the Dutch Banking Association (NVB), individual banks, the Dutch Authority for the Financial Markets (AFM) and the Ministry of Finance have participated in these roundtable discussions. Based on the discussions held so far, the NVB published several industry baselines which incorporate the risk-based approach. Moreover, DNB uses the outcomes of the discussions in revising its Guidance on the *Wwft*, which will take the form of a *Wwft* Q&A and Good Practices.

We are also discussing a more targeted approach to *Wwft* compliance with other sectors, such as the insurance industry.

Roundtables: innovation

One of the main messages of the "From recovery to balance" report is that wider deployment of technologically innovative solutions can make anti-money laundering and anti-terrorist financing activities more targeted. The use of models and algorithms can enhance transaction monitoring, for instance. We are currently discussing these topics with representatives of the banking sector. Talks on the use of electronic identification documents (e-IDs) have started as well.

Roundtables with customer groups

In 2022, DNB and the NVB also started roundtable discussions with customer groups that have difficulty accessing payment services. This may be the result of undesirable side effects of the application of the *Wwft*. As a result of these discussions, the NVB is now working with customer groups to achieve better risk differentiation and to help banks and industry associations communicate more clearly, for instance by setting up an information portal for non-profit organisations. In addition, the NVB has presented so-called sector standards that banks can use to enhance their risk differentiation, including for sex workers and crypto service providers. DNB contributes to these conversations whenever they touch upon areas that are related to our supervision.

The use of cash is also a topic of discussion, for instance when it comes to the bottlenecks experienced by businesses and banks' obligations when handling cash. We are currently considering whether and how to adapt existing publications on these subjects.

2 Integrity supervision findings

Introduction

In this chapter, we discuss the results of our supervisory examinations and the measures we have taken. The examinations specifically focused on:

1. Preventing money laundering and terrorist financing.
2. Compliance with sanctions laws and regulations.
3. Preventing conflicts of interest.

With regard to the *Wwft*, individual examinations have been carried out across all sectors. We have also conducted two thematic examinations on compliance with sanctions regulations. The first of these investigated whether the operational management of institutions in various sectors (banks, payment service providers, insurers, pension funds, trust offices and crypto service providers) complied with the Sanctions Act (*Sanctiewet 1977, Sw*). The second examination tested the effectiveness and efficiency of sanctions screening systems at 31 banks and payment service providers. Conflict of interest examinations were mainly conducted in the insurance sector (including on the BES islands).

2.1 Banks

Between July 2022 and December 2023, DNB conducted 26 examinations of banks' compliance with the *Wwft* and *Sw*. Overall, we found that integrity risk management at banks has reached a higher level, as more and more banks have completed their recovery phase or are getting closer to doing so. These institutions can further develop their risk management maturity in this area in a business-as-usual setting.

At the same time, recovery programmes are still regularly delayed because of the intractable issues underlying them. There are also banks that still have a lot of work to do, as well as banks that have taken a turn for the worse after a period of business as usual, ending up in a situation where recovery is needed once again. Cases such as these highlight the importance of continued vigilance on this issue, which must remain a priority. The following sections set out DNB's main findings in this area.

2.1.1 Money laundering risk management

The picture that emerges from our examinations is that the maturity of quality management frameworks varies considerably between banks. In these frameworks, institutions describe how their system for assessing the quality of customer and alert handling files is set up, and how their feedback loop is designed to achieve necessary improvements.

SIRA

We found room for improvement at several banks with regard to their systematic integrity risk analysis (SIRA). What stands out in particular is the lack of sufficient in-depth data analysis for risk factors related to customer type, product, service, transaction, delivery channel and countries or geographical areas. We note that the controls in place at some institutions are not sufficiently specific, and therefore may not be effective in managing these risks. We also found that institutions that prioritise integrity risks based on the actual risk level are generally more aware of their biggest risks and are often better able to justify the use of available resources.

Transaction monitoring

The examinations show that most banks have not yet sufficiently aligned their transaction monitoring systems with their risk analysis. We regularly come across poorly substantiated alert definitions and threshold values. Meanwhile, more sophisticated models are becoming increasingly popular, even though they are not widely used yet. For these models too, the substantiation and demonstration of effectiveness – for example by back testing – can often be improved. We therefore encourage banks to pay extra attention to this in the coming year.

Reporting obligation
There is considerable variation among institutions when it comes to reporting behaviour. Different institutions may have very different thresholds for reporting, and the nature and quality of reports varies widely. We also found that several institutions do not meet their reporting obligations to the FIU, for instance by failing to structurally report transactions that could be linked to predicate money laundering offences, such as external payment fraud. In addition, not all reports are filed without delay yet. Not only is this against the rules, but it also hinders investigations carried out by the police and the Fiscal Intelligence and Investigation Service (FIOD).

Customer due diligence
Overall, we find that banks have made great strides in terms of customer due diligence compared to a few years ago. However, many of our examinations do point to the recording of customer due diligence as an area of concern. Enquiries show that, although financial institutions often have the necessary customer information, they do not always record such information in the customer file, or do so inadequately.

In addition, we still regularly observe backlogs in periodic and event-driven reviews of customer files. The reasons for these backlogs range from capacity shortages to poor-quality management information that is either outdated or incomplete.

Finally, we observe that customers in the process of being offboarded are not always adequately monitored, which sometimes leads to delays. This deficiency can create serious risks, for instance by inadvertently facilitating financial crime or violating legal requirements.

2.1.2 Sanctions screening
In May 2023, DNB shared the findings from its Sanctions Act examinations. The picture that emerges from these examinations is that banks generally have adequate sanctions screening systems in place. However, we do want to underline the importance of screening against Dutch sanctions lists, in addition to screening against international sanctions lists. This is sometimes overlooked by institutions. Furthermore, some institutions are not yet making use of fuzzy matching. We also note that the detection of so-called dual-use goods, which can be used for both civilian and military purposes, remains a challenge for banks. We refer to this DNB news release for more information on our Sanctions Act examinations.

2.2 Insurers
Between July 2022 and December 2023, DNB conducted 27 examinations of insurers, focusing on the management of risks related to conflicts of interest and money laundering, and compliance with the *Sw*. The key findings are summarised below.

2.2.1 Money laundering risk management
In general, Dutch insurers have a low risk profile with regard to money laundering. Nevertheless, a basic level of risk analysis, customer due diligence, transaction monitoring and compliance monitoring remains essential. Our examinations show that remedial measures are needed in some cases to achieve this basic level of control.

While term life insurance policies without value accumulation, funeral insurance policies that pay out in kind and pension insurance are low risk, some life insurance policies with value accumulation, such as savings insurance policies with extensive surrender options, pose a considerable risk of money laundering. The higher the risk, the more measures are needed to control it. For low-risk policies, life insurers may carry out simplified customer due diligence. In fact, life insurers do not have to take more measures than strictly necessary with regard to low-risk products.

2.2.2 Sanctions screening
We found that several insurers had not conducted proper Ultimate Beneficial Owner (UBO) screening: they had neither identified UBOs nor screened against sanctions lists. Moreover, we noted that some institutions had only discovered that one of their customers was on a sanctions list after a considerable time, posing a serious risk to *Sw* compliance.

2.2.3 Preventing conflicts of interest

In our examinations of conflicts of interest management, we looked at risks of conflicts of interest in activities related to the purchase and sale of real estate, in sponsorships and donations, and in lending. Although most insurers have policies and procedures in place to manage these risks, we find that these are often too general. We note that insurers' controls are insufficiently focused on specific risks of conflicts of interest that may arise in the above-mentioned activities. For example, many insurers have no controls in place to identify and mitigate potential conflicts of interest in decision-making processes for sponsorships. As a result, there is a risk that parties with ties to a director with signing authority could benefit from funds which have been made available by the insurer.

2.3 Pension funds

Between July 2022 and December 2023, DNB conducted two examinations of pension funds, focusing on *Sw* compliance. The key findings are summarised below.

2.3.1 Sanctions screening

Among the pension funds we examined, we identified shortcomings with regard to the policies in place as well as the procedures and controls regarding compliance with the *Sw*. More specifically, we found that implementation was fully outsourced while no concrete controls were in place to ensure effective compliance with the *Sw*. In addition, risks related to circumvention of the *Sw* had not been sufficiently identified. This lack of control can lead to situations where the *Sw* actually is circumvented.

2.3.2 Preventing conflicts of interest

There have been several incidents involving conflicts of interest. These incidents could occur because the risk of conflicts of interest was not identified in time, or because there were no or insufficient controls in place. Examples of inadequately controlled conflicts of interest that we encountered in our supervision included incompatible secondary positions, unfair selection procedures and the purchase of services from a subsidiary.

2.4 Payment institutions and electronic money institutions

Between July 2022 and December 2023, DNB carried out 12 examinations of payment institutions and electronic money institutions' compliance with the *Wwft* and *Sw*. We note that there is a growing awareness of integrity risks among payment institutions and electronic money institutions, as evidenced by, among other things, the tone at the top. Furthermore, an increasing number of institutions is including risks in the SIRA that are appropriate in the context of the services that these institutions provide, making it easier for them to develop concrete mitigation measures. With regard to customer due diligence, we find that institutions are making progress in documenting and tracking the outcomes of their screening processes. As a result, institutions are better able to establish risk and transaction profiles, which contribute to better ongoing monitoring of business relationships.

Besides these positive developments, our examinations also identified areas of concern. These are described below.

2.4.1 Money laundering risk management

SIRA

Our examinations reveal that risk analyses often fail to provide sufficient insight into the risks associated with sub-merchants. Because of this, it remains unclear to supervised institutions how these risks may materialise and how they can be mitigated. As a result, the policies and procedures in place are not adequately geared towards the management of these risks.

Customer due diligence

In many of our examinations, we found that the risk profile assessment lacked sufficient depth. Customer files often lacked substantiation regarding how the supervised institution arrived at a customer's risk profile, and many do not specify what factors were considered in the assessment.

Results of thematic examination

In a thematic examination of fast-growing institutions, DNB found that these organisations do not always take sufficient measures

to effectively manage integrity risks. When onboarding new customers, for example, some institutions do not pay sufficient attention to integrity risks of these potential customers. In other instances, there were shortcomings with regard to the ongoing monitoring of customers and the transactions that were processed on their behalf.

2.4.2 Sanctions screening

We shared the conclusions from our Sanctions Act examinations with the public in May 2023. For more information, please refer to our news release.

2.5 Trust offices

The number of trust service licences in the Netherlands continues to decrease. DNB observes that trust offices often do not carry out the necessary customer due diligence when acquiring customer portfolios (which include high-risk customers) from other trust offices. Moreover, we finds that some customers of legal trust offices end up with illegal parties.

We also see that some trust service providers are segmenting their trust services to avoid having to comply with the requirements of the *Wtt* and the *Wwft*. This is done by artificially dividing one service into smaller segments so that no individual segment exceeds the legal threshold requirements. Breaking up trust services can lead to high money laundering risks. In addition, the services offered are still subject to a licence requirement in some cases. In these cases, DNB takes enforcement action.

Between July 2022 and December 2023, DNB carried out 25 examinations at trust offices to assess compliance with the Act on the Supervision of Trust Offices (*Wet toezicht trustkantoren – Wtt*), *Wwft* and the *Sw*. The key conclusions from these examinations are described below.

2.5.1 Money laundering risk management

Customer due diligence

Since the *Wtt* entered into force, DNB has observed an overall improvement in trust offices' customer due diligence processes. However, our examinations and enforcement processes have also revealed that various shortcomings persist at both larger and smaller trust offices, particularly with regard to ongoing monitoring and establishing the source of object companies' assets. If a trust office has insufficient knowledge in these areas, it is unable to properly exercise its role as gatekeeper.

2.5.2 Sanctions screening

We published the results of our Sanctions Act examinations of trust offices and other financial institutions in May 2023 (see also our news release).

2.6 BES institutions

Between July 2022 and December 2023, DNB conducted 10 examinations at institutions on the BES islands. These examinations focused on managing money laundering risks, *Sw* compliance and preventing conflicts of interest. The key findings are summarised below.

2.6.1 Money laundering risk management

The management of money laundering risks by the various institutions on the BES islands has clearly improved in recent years, and the completeness of customer files is generally of a good standard. At the same time, DNB observes that institutions are struggling to identify and effectively manage higher risks, including those related to the structure or activities of their customers.

2.6.2 Sanctions screening

One of the key findings from our *Sw* compliance examinations is that several institutions do not have effective sanctions screening practices in place. While institutions do screen against sanctions lists, our examination revealed a minimum match rate of 100% in multiple instances. This means that sanctioned entities are detected only if there is a 100% match between the name on the sanctions list and the name in the institution's records. Immediate measures were necessary to remedy these deficiencies, as well as follow-up checks.

2.6.3 Preventing conflicts of interest

Preventing conflicts of interest remains an important theme for BES institutions, even though the level of control at the institutions we examined was found to be good. As BES

institutions remain relatively vulnerable in this respect, DNB will continue to monitor this issue over the coming year.

2.7 Crypto service providers

In 2023, the crypto service provider sector began to consolidate. Several providers partnered with other providers (registered in the Netherlands or abroad), resulting in shareholder changes and customer portfolio migrations. DNB sees a risk that unregistered parties may still offer crypto services through registered parties. Moreover, when migrating large numbers of customers in a short period of time, it is important that customer due diligence is carried out carefully and completely before service provision starts.

Between July 2022 and December 2023, DNB conducted *Sw* compliance examinations of nine crypto service providers. The key findings are described below.

2.7.1 Sanctions screening

All the institutions that were examined by DNB conducted sanctions screening and had implemented the basic requirements, such as mandatory reporting and customer screening. However, we did find that sanctions risks were not thoroughly analysed, and that the institutions did not have adequate frameworks for policies, procedures and measures to ensure compliance with sanctions regulations. In this way, the frameworks that crypto companies have set up for *Sw* compliance are lagging behind those which have been set up for *Wwft* compliance. To ensure adequate screening, it is essential that policies and procedures offer comprehensive and consistent guidelines on who should be screened and when.

We note that many institutions consider that the measures they take to comply with the *Wwft* also reduce the risk of sanctions violations. However, specific aspects of service provision and customer information (such as nationality, residential address or metadata, such as IP addresses) may have a different impact on the assessment of sanctions risks.

Almost all institutions have started implementing the *Sw* Q&A in their wallet partner verification. The good practices we have identified in this area will be shared with the sector later, where possible.

2.8 Measures taken by DNB

Between 1 July 2022 and 31 December 2023, DNB took several informal and formal measures in response to non-compliance with integrity regulations by supervised institutions. These are listed below.

Measures imposed on supervised institutions 1 July 2022 – 31 December 2023

Formal measures	**16**
Formal instruction	4
Order subject to penalty	0
Revocation of licence	2
Administrative fine	10
Informal measures	**22**
Compliance briefing	6
Written warning	16
Total	**38**

Between 1 July 2022 and 31 December 2023, DNB imposed 16 formal measures and 22 informal measures on supervised institutions for integrity-related violations. Some of the informal measures were imposed on groups comprising several entities, each with their own separate licence. The remedial measures were aimed at correcting significant shortcomings in institutions' SIRAs and their implementation, customer due diligence, the failure to report incidents or changes in structure to DNB, and the screening of customers against sanctions lists.

2.9 Enforcement to end illegal service provision

DNB is committed to effectively ending illegal service provision, and we have various instruments at our disposal to do so. In most cases, a warning letter is sufficient to end non-compliance. If necessary, DNB can also use formal instruments to stop the provision of illegal services, such as an order subject to penalty. Depending on the severity and culpability of the non-compliance, an administrative fine may also be imposed. Recently, for instance, we have imposed several fines on companies that offered crypto services in the Netherlands without having registered with DNB.

We received more reports of illegal service providers in 2023 than in 2022. Most of these reports were related to the provision of trust services without a licence or the provision of crypto services without the required registration.

DNB has a team that is specifically dedicated to tackling illegal service providers. This team's work is report-driven, and reports can be filed by private individuals, fellow supervisory authorities and investigative agencies. We also regularly receive reports from supervised institutions. Reported can be submitted to handhaving@dnb.nl.

3 Sectoral integrity risk analyses

As part of a risk-based approach, DNB maps the main integrity risks for each sector. In these sectoral analyses, the risks mentioned in the National Risk Assessment (NRA), other national and international sources, and information from supply chain partners are assessed per (sub)sector of the financial industry. We assess supervised institutions' vulnerability to integrity risks for each sector using the supervisory information that is available to us, including information from our integrity risk survey (IRAP). It is therefore vital that supervised institutions enter the correct data when they submit the IRAP to DNB. We use this information to determine sectoral risk levels, and to calculate a risk score for each institution, both of which play an important role in setting our supervisory agenda.

At present, there are still white spots for some sectoral risks, which means that too little information is available to effectively determine the vulnerability at sectoral and institutional level. We will address this in the next IRAP survey, for instance by adding new questions or adapting existing ones. As BES institutions are excluded from the IRAP, they are not included in the sectoral analyses.

Besides information from the IRAP, DNB also considers institutions' SIRAs in the sectoral analyses. We have found that some institutions are already using data to analyse the risks they are exposed to in their SIRA. At the same time, we see significant room for improvement in the SIRAs in terms of providing concrete analyses of the risks identified in the NRA and other national and international sources. We intend to pay more attention to these topics in our supervision.

3.1 Cross-sectoral risks

The sector analyses have highlighted risks that are relevant to several sectors. Such cross-sectoral integrity risks in the financial sector are often linked to current issues in politics and the media or which have been identified by public or private institutions with which DNB cooperates in the Financial Expertise Centre. Examples of such risks include international drug trafficking, terrorist financing and sanctions circumvention. We expect supervised institutions to always be aware of any weaknesses in their operational management regarding the placement of criminal money (e.g. cash transactions), the concealment of criminal money (e.g. through opaque structures) or the spending of criminal money (e.g. on real estate or high-value products).

3.1.1 High-risk countries

Banks, payment service providers and trust offices deal with many high-risk countries as part of their operational management. A UBO or company may be based in a high-risk country, for example, or they may process transactions to and from high-risk countries. Some banks, PSPs and trust offices may also have customers whose corporate structures or complex international financing structures are linked to high-risk countries. When doing business with complex structures and foreign financing, it is particularly relevant that financial institutions include the involvement of high-risk countries in their assessments.

It is important for banks and PSPs (including electronic money institutions and money transfer organisations) to determine whether the volume of their transactions to and from these high-risk countries is appropriate for the customers involved and the markets in which they operate. Large discrepancies between customers' actual operational activities and the countries through which their transactions flow may indicate an increased risk of money laundering or sanctions violations. The possibility of a customer moving its operations or funds to another country as a result of sanctions therefore warrants additional attention.

In the trust sector, the top five high-risk countries where object companies operate are Israel, Switzerland, Singapore, China and Turkey. In previous communications to the trust sector, we have highlighted the risks associated with politically exposed persons (PEPs) in high-risk countries and high-risk sectors. There may also be an increased country risk if the structure of the object company includes a registered office in a high-risk country. It is important

that trust offices have insight into transactions to and from high-risk countries within the structure. This helps trust offices avoid becoming involved in money laundering, corruption and sanctions circumvention.

Finally, we note that pension funds invest in high-risk countries. However, they are not subject to the provisions of the Wwft.5

3.1.2 Increasing opacity in the payment chain

Increasing opacity in the so-called payment chain, which includes all parties that are involved in the processing and execution of a payment transaction, is a cross-sectoral trend. As the payment chain becomes more complex, it is increasingly difficult for financial institutions to have a clear and complete view of all the transaction flows which they facilitate. This is the case, for example, when a transaction involves multiple countries, sectors (correspondent banks, payment service providers, crypto providers) or payment methods.

Criminals may try to make use of such complex transactions to conceal illicit funds. They may also use intermediaries, third party payment structures and transactions (including currency transactions) between different countries, or they may convert funds into different cryptocurrencies. Of course, not all transactions that go through PSPs or crypto service providers involve high risks. For banks, it is important to look closely at transactions that also involve other high-risk factors, such as transaction flows to and from high-risk countries or transaction flows that show a sharp and difficult-to-explain increase in volume.

Among payment service providers, we observe increasing fragmentation of the payment service chain across different payment service providers, as well as increasing segmentation of transactions in the payment chain. This involves different PSPs, intermediaries and payment methods, thereby limiting transparency. At the customer level, transactions are segmented using sub-merchants. In addition, by making licenses and payment services that are subject to a licence requirement available to third parties, electronic money institutions (e.g. white labelling and virtual IBANs), payment service providers including money transfer organisations contribute to opacity in the payment chain. Mapping the above risks will help institutions to complement their SIRA. In this context, it is also important for supervised institutions to pay explicit attention to compliance with the Wire Transfer Regulation 2 (WTR 2).

3.1.3 Sanctions

International sanctions affect all supervised sectors. Sanctions evasion is an important issue when it comes to the sanctions that have been imposed on Russia since the spring of 2022. The extensive sanctions packages that have been imposed on Russia and Belarus include a comprehensive set of import and export restrictions. These sanctions can be circumvented, however, for example by exporting goods via non-sanctioned countries. Customers whose UBOs have been placed on sanctions lists can also circumvent sanctions by changing their ownership and control structures. The chances of detecting sanction circumvention are improved by being alert to structural changes and situations where shares are placed in a separate entity or transferred to other non-sanctioned UBOs.

There is also a risk that sanctioned UBOs' international property holdings are obtained through money laundering or corruption. Such properties may also be directly or indirectly held by straw men, for example, or by a Dutch legal entity, such as a foundation or company.

For payment service providers and banks, increased opacity also increases the risk of processing transactions for sanctioned parties.

In the trust sector, the risk of sanctions circumvention is high due to the large number of customers operating in the oil, gas and energy sectors. In our sector letter to the trust sector, we also noted that trust offices' exposure to Russia required special attention, and we expressed the expectation that institutions reduce this exposure. The screening of goods and services at the start of and during a business relationship, as well as the identification and assessment of the dual use nature of goods and services, is particularly relevant in this context.

Regarding the pension and insurance sector, DNB sometimes receives reports suggesting flaws regarding insurers' compliance with sanctions regulations. We also note that there are

discrepancies between the number of hits reported by institutions in the IRAP and the number of sanction reports submitted to DNB. It is important that pension funds and insurers report all their sanction hits to DNB.

In the pension and insurance sector, sanctions screening is often outsourced to a third party. We have received reports indicating that not all outsourcing parties, which handle sanctions screening for multiple institutions, are providing services of sufficient quality. This puts institutions at risk of not complying with sanctions regulations and providing services to a sanctioned entity.

Investment data shows that the pension sector invested €5 billion in high-risk countries in Q4 2022. Sanctions risks are relatively high for insurers that are active in international shipping (insuring ships or cargoes) and the energy sector, where inherent sanctions risks are higher.

We have requested crypto service providers to improve their policies, procedures and measures regarding sanctions. A proper analysis of the risks of violation or circumvention of sanctions is necessary to implement appropriate controls. These risks will vary depending on the provider's business model, customer base and transaction capabilities. In addition, it is vital to ensure a clear division of responsibilities when it comes to the screening process, alert handling, freezing assets and reporting hits.

3.1.4 Tax abuse

Tax abuse is another cross-sectoral trend receiving increasing international attention. In practice, it is often difficult for institutions to determine where tax optimisation in fact becomes tax evasion. In addition to determining their risk appetite for tax optimisation, DNB expects institutions to be alert to the risk of tax evasion when dealing with customers or investments with tax-driven structures, particularly where these structures involve entities in high-risk countries. We will pay more attention to this in the upcoming IRAP.

3.2 Key integrity risks by sector

The information on sector-specific risks presented in this chapter has been compiled using quantitative and qualitative supervisory data. The aim here is to provide an overview of the most salient risks for each sector. These key sectoral risks exist alongside the cross-sectoral risks described above. It is important to note here that there are also niche players for which these risks do not apply, or only to a lesser extent, and for which other risks are more relevant.

3.2.1 Banks

The Dutch banking sector consists of a few major banks and a highly diverse group of medium-sized and small banks. This means that the key risks listed below (cash, correspondent banking and real estate) are not equally relevant for all banks. It is important that banks always include cross-sectoral risks when assessing key risks in their own operational management, as a combination of these risks requires significantly more attention.

Money laundering using cash

Cash is legal tender and fulfils an important function in society. As a central bank, DNB is part of the Eurosystem, and our mandate includes ensuring the smooth operation of payment systems and facilitating the efficient circulation of euro banknotes. At the same time, the use of cash by consumers and retailers can also be an indicator of money laundering or terrorist financing. Given the difficulty of tracing cash flows, the use of cash carries an inherent risk of money laundering and underlying predicate offences, such as corruption, fraud and terrorist financing, and may therefore warrant tighter monitoring by banks.

Striking the right balance between mitigating risk and not impeding legitimate use of cash is key. Knowledge about individual customers and their transaction profiles is an important starting point in this context. There has been a decline in the volume of cash deposits and withdrawals over the last few years. The use of cash remains something banks need to monitor closely to identify unusual individual patterns.

Figure 1 Number of deposits/withdrawals > 5000

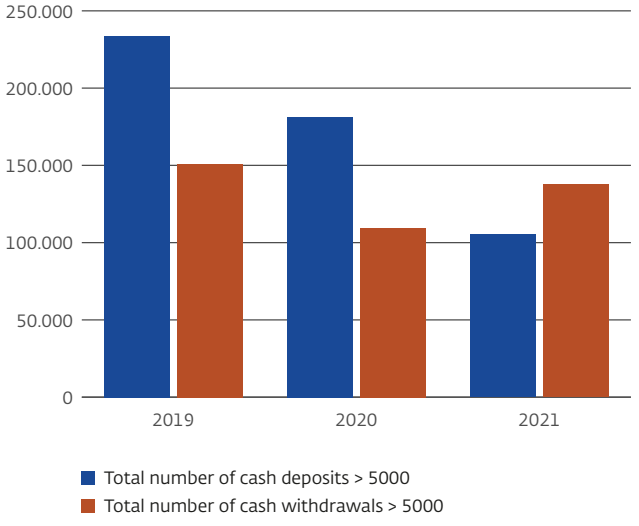
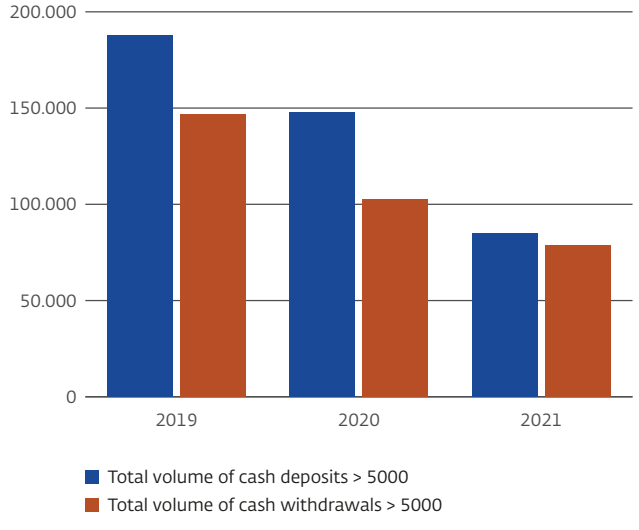


Figure 2 Volume of deposits / withdrawals > 5000

Amounts x 10.000



Money laundering through correspondent banking

Correspondent banking (COBA) relationships are essential in the global payment system and vital to international trade and the world economy, including emerging markets and developing economies. However, correspondent banks have limited information about respondent banks' customers and the nature or purpose of the underlying transactions. These risks of opacity may become more complex in arrangements where a correspondent bank offers access and additional flexibility to respondent banks and their customers, for instance in the case of nesting/ downstreaming services or payable-through accounts.

Money laundering through real estate

This includes the use of properties for criminal activities and the investment of funds obtained through criminal activities in real estate in the Netherlands and abroad. In this context, we recommend paying particular attention to property investments from high-risk countries. Given the increasing complexity of real estate structures, it is important for credit providers to look closely at the nature of each real estate transaction that they facilitate.

3.2.2 Insurers

The insurance sector faces a number of specific risks that are not highlighted in the NRA. It is also important to note that only life insurers are subject to the provisions of the *Wwft*. The greatest risk in the insurance sector is posed by actual or perceived conflicts of interest.

Risk of actual or perceived conflicts of interest

In recent years, there have been several incidents at insurers involving actual or perceived conflicts of interest, some of which involved serious and structural shortcomings.

Insurers reported a total of 905 secondary positions held by employees in the 2022 IRAP. These secondary positions were spread across different types of organisations, increasing the risk of actual or perceived conflicts of interest. Moreover, it appears that there is relatively little monitoring in this area, and awareness of this risk is low. Some insurers (17%) do not review the completeness of the information employees submit about their secondary positions. If a review is conducted, it is often sufficient for employees to sign a declaration of compliance with the employer's codes of conduct. Moreover, many insurers offer sponsorships or make donations, which sometimes involves large sums of money. Our thematic examination shows that little attention is paid to the risk of actual or perceived conflicts of interest regarding these activities.

DNB has also highlighted the risk of senior executives with significant powers of procuration making commitments or payments independently. A recent survey of insurers shows that 25 of the 118 respondents have senior executives with independent powers of procuration exceeding €10 million. These kinds of powers pose an obstacle to evaluation and accountability, leading to an increased risk of conflicts of interest.

Real estate risk

Several insurers invest directly in real estate and manage these investments in-house. Real estate is a high-risk sector, for instance regarding criminal money laundering and sanctions circumvention, but insurers must also consider the risk of conflicts of interest. It is important that insurers pay attention to the risk of actual or perceived conflicts of interest when investing in real estate.

3.2.3 Pension institutions

Like the insurance sector, the pension sector faces specific risks that are not highlighted in the NRA. Moreover, pension institutions are not subject to the provisions of the *Wwft* in this regard. The most significant risk for pension institutions is that of actual or perceived conflicts of interest.

Inherent risk of conflicts of interest

The governance models of pension funds are designed to ensure that employer and employee members of the participating companies are well represented in the board and/or other bodies, creating an inherent risk of conflicts of interest. At most pension funds, the bulk of the work is outsourced to external parties, and the number of people directly employed by the pension fund is relatively limited. Nevertheless, the number of secondary positions in this sector is high: the total number of declared secondary positions held by persons affiliated with pension institutions was 5,200 last year. This does not include other positions with the same employer.

Increased risks of conflicts of interest

There are several specific combinations of roles that increase the risk of actual or perceived conflicts of interest. For instance, almost half (75 out of 158) of all pension institutions use a fiduciary manager for asset management who is also employed by the party to which the pension fund has outsourced its asset management. The fiduciary manager advises on strategic investment policy and may have an incentive to recommend asset classes that are highly lucrative for the outsourcing party.

In addition, some investment advisory committees at pension institutions include external members employed by the external party conducting the ALM study on which the fund's investment policy is based. Some investment advisory committees are even chaired by an external member. These increased risks of conflicts of interest are compounded by the fact that a quarter (41 out of 158) of pension institutions report spending less than 50 hours on compliance each year.

We expect pension institutions to assess these increased risks of conflicts of interest in their operational management and, where necessary, to take appropriate measures to ensure compliance.

Investments in high-risk sectors

Of all investments made by pension institutions in Q4 of 2022, €237 billion (16%) were in high-risk sectors. High-risk sectors are those that are generally known to be more vulnerable to integrity risks, such as real estate, construction, gambling, tobacco and mining.

3.2.4 Payment service providers, such as electronic money institutions, money transfer organisations and exchange institutions

The payment services industry is characterised by a wide variety of payment service providers (and intermediaries), customer bases and payment products. In addition, many PSPs in the Netherlands also operate on a cross-border basis, for example using payment service agents. By their nature, the services provided by money transfer organisations and exchange institutions are very different from those provided by other payment institutions and electronic money institutions. In the payment services sector, it is vital that PSPs assess cross-sectoral risks, including payment chain opacity, in combination with sector-specific key risks.

Money laundering through high-value product traders

DNB observes that companies trading in high-value products (including jewellery, art, luxury goods, vehicles and electronics)

are increasingly accepting electronic payment methods and hybrid payment methods, such as foreign payment methods or prepaid cards linked to an e-wallet containing crypto credit, or cash transfers via chargebacks. Acquiring payment service providers need to have a clear picture of which of their customers offer high-value products and which carry increased risk due to the use of certain payment methods (including foreign payment methods) that provide limited visibility of the origin of the funds.

Money laundering through cash and cash conversion
It remains as important as ever that money transfer organisations (and their Dutch agents) carefully check the origin of cash funds, especially if these funds are being transferred to a high-risk country. There is also a risk of electronic money institutions accepting cash in exchange for electronic money through distributors or other PSPs. Electronic money institutions should manage the specific risks of money laundering and may implement additional controls if they outsource the acceptance of cash payments to third parties.

3.2.5 Trust offices

Tax-driven corporate structures with a relatively high number of object companies with operations in high-risk countries and high-risk sectors are common in the trust sector. DNB is aware that this group of object companies is not homogeneous regarding the ultimate risk of financial crime.

High-risk sectors
The main risk sectors are: i) commercial real estate, ii) oil, gas and energy, iii) commodities, minerals and mining.

For activities associated with commercial and other real estate, the origin and destination of funds are particularly relevant when it comes to the risk of money laundering. The comparatively high number of customers within the trust sector operating in the oil, gas and energy sectors creates an increased risk of sanctions circumvention and corruption, in addition to money laundering. The same applies to the commodities, minerals and mining sector. We will pay attention to this in our supervision this year.

Cumulative risks
Regarding activities in the high-risk sectors mentioned above, elements that limit the transparency of corporate structures (including international corporate structures) also play an important role. For example, a customer's corporate structure may be made up of more than five tiers of cross-border entities, or it may include a nominee shareholder, an Anglo-Saxon trust or any other element limiting its transparency. To properly perform their gatekeeper role, it is important that trust offices have an overview of the relevant parts of the structure and their associated relationships.

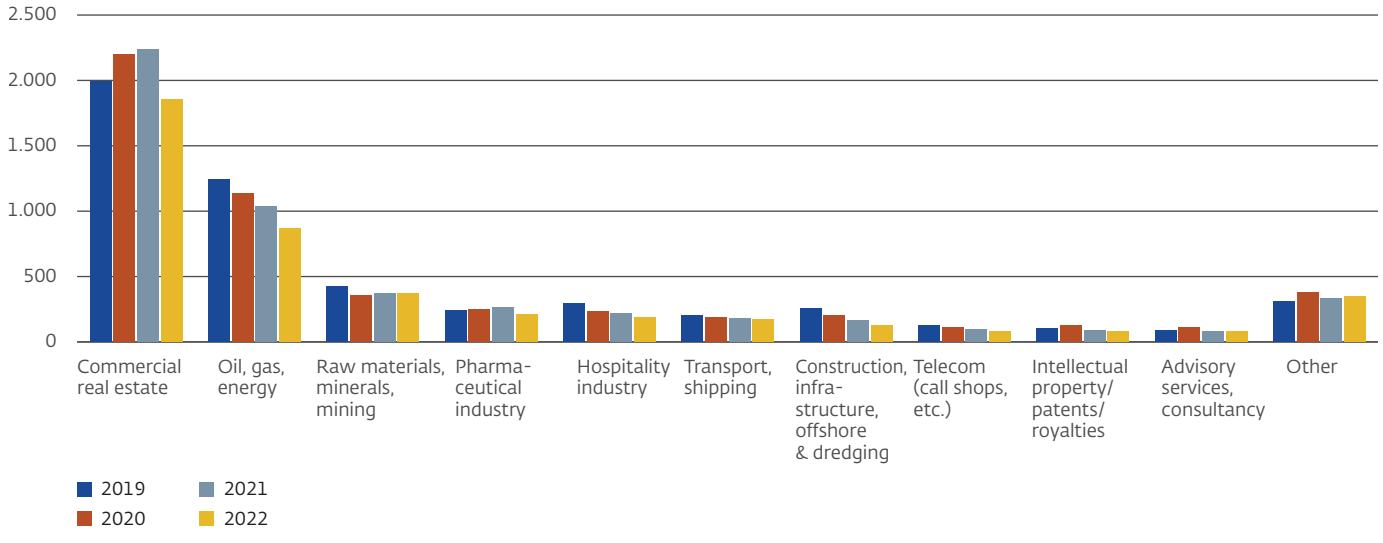
We want to draw particular attention to the way in which trust offices address the cumulative risks of high-risk countries, high-risk sectors and opaque structures in their SIRA.

3.2.6 Crypto service providers

IRAP results: room for improvement in specific areas
Based on the results of the IRAP 2023, DNB concludes that most crypto service providers update their integrity risk analysis at least annually. However, we also observe that in some instances updates have not taken place for some time. Regarding the process of drafting or updating, discussing and conducting the integrity risk analysis, we consider it a good practice to involve the relevant employees, such as the management board and the compliance function. According to the IRAP results, this is not the case at all institutions.

The results further suggests that crypto service providers (at least at the time of submission) do not seem to comply with all *Wwft* requirements regarding transaction monitoring. For example, a number of crypto service providers indicate that they do not establish a transaction profile for each customer at the start of service provision. This makes it impossible to check whether an (intended) transaction deviates from the knowledge the institution has of the customer and its risk profile. Also, monitoring

Figure 3 Number of object companies with activities in high-risk sectors



of intended transactions and/or investigation of whether there is a connection between two or more transactions (monitoring of compound transactions) does not (always) take place at some crypto service providers.

Sanctions screening

Regarding sanctions screening, some crypto service providers indicated that they screen only periodically (not upon changes to customer data, sanction lists or transactions), or that they only screen upon changes (not periodically), do not screen transactions or do not screen the UBOs of customers periodically or upon changes. Where institutions only screen periodically, there is a risk that transactions for or with sanctioned persons are still possible in the interval between a change in the sanctions list or customer data and a periodic screening. Some institutions limit their screening to transactions following customer onboarding. With a large interval between transactions, this gives rise to the risk that it may take a long time for sanctioned persons to be detected and reported.

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+(31) 20 524 91 11
dnb.nl/en

Follow us on:

DeNederlandscheBank
EUROSYSTEEM