

Good Practices SIRA

1 July 2025

DeNederlandscheBank

EUROSYSTEEM

Contents

1 Introduction

2 Integrity risk
management

3 Risk identification

4 Risk analysis

5 Risk management

6 Risk monitoring
and review

Annex – Main changes compared to
the 2015 SIRA Good Practices

1 Introduction

1.1 DNB's integrity supervision

In addition to solidity, integrity is a prerequisite for a sound and reliable financial system. De Nederlandsche Bank (DNB) conducts integrity supervision of a wide range of financial and other institutions. DNB's integrity supervision is based in particular on the Financial Supervision Act (*Wet op het financieel toezicht – Wft*), the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft*), the Sanctions Act (*Sanctiewet 1977 – Sw*), the Pensions Act (*Pensioenwet – Pw*), the Mandatory Occupational Pension Scheme Act (*Wet verplichte beroepspensioenregeling – Wvb*) and the Act on the Supervision of Trust Offices (*Wet toezicht trustkantoren 2018 – Wtt*) (collectively referred to below as integrity legislation).¹

A sound and ethical financial sector starts with sound and ethical financial institutions. DNB supervises financial institutions to ensure they conduct their business in such a way that sound and ethical business operations are guaranteed. Essentially, ensuring ethical business operations is about managing the integrity risks to which an institution is exposed. Pursuant to the *Wft*, this particularly concerns:

- preventing conflicts of interests
- preventing the financial institution and its employees from committing criminal offences and other breaches of the law which may damage confidence in the financial institution or the financial markets in general
- preventing relationships with customers or consumers that may damage confidence in the financial institution or the financial markets in general, and

- preventing other socially improper acts by the institution or its employees that could seriously damage confidence in the financial institution or in the financial markets.

These aspects of ethical business operations are detailed in general administrative orders, such as the Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels Wft – Bpr*). The relevant legislation (in particular the *Wwft*, the *Wtt* and the *Sw*) provides more details of the obligations related to the prevention of involvement in money laundering, terrorist financing and non-compliance with sanctions regulations.

1.2 The SIRA

To ensure ethical business operations, institutions must conduct a systematic integrity risk analysis (SIRA).² This means the institution must analyse its own organisation on an ongoing basis to identify which business units are exposed to integrity risks. Based on the SIRA, the institution will have to take preventive measures to manage its integrity risks.

This makes the SIRA an important tool for ensuring integrity in business operations. The SIRA can be documented in several ways, for example in a document recording the results and methodology of the different steps. It can also be recorded in multiple documents. The important thing is that the method of documenting fits the institution's operational procedures. The institution's management board can use the SIRA to be informed about the nature and extent of integrity risks, and as a steering instrument to prioritise the controls to be implemented.

¹ DNB also conducts integrity supervision of institutions in the Caribbean Netherlands. This supervision is subject to other laws and regulations.

² Section 10 of the *Bpr*, Section 10 of the Decree on the Supervision of Trust Offices (*Besluit toezicht trustkantoren – Btt 2018*).

Managing integrity risks in day-to-day operations includes raising awareness, and promoting and maintaining integrity within all levels of the institution.³ It is vital that institutions themselves strive to maintain their integrity. Integrity can be understood as: a) the personal integrity of directors and employees; b) the organizational integrity of the institution; c) relational integrity; d) integrity with respect to the market conduct of the institution.⁴

1.3 Link between Wwft risk assessment and SIRA

The Wwft stipulates that an institution must take measures to identify and assess risks of money laundering and terrorist financing (the Wwft risk assessment). These measures must be proportionate to the nature and size of the institution in question. In identifying and assessing Wwft risks, an institution must consider the risk factors relating to its specific types of customers, products, services, transactions and supply channels, as well as to the countries or geographic areas in which it operates. The Wwft also requires institutions to document the results of their Wwft risk assessment. In addition, they must keep their risk assessment up to date and make the results available to the supervisory authority upon request.⁵

The SIRA analyses integrity risks in a broad sense, while the Wwft risk assessment specifically targets the risk of money laundering and terrorist financing – see also DNB's Wwft Q&As and Good Practices.⁶ The SIRA therefore has a broader scope than the Wwft risk assessment. If an institution is also required to prepare a SIRA, it makes sense to include the Wwft risk analysis in the SIRA, but this is not mandatory.⁷

1.4 Rationale, status and structure of this document

1.4.1 Rationale for the review of the SIRA Good Practices

With the SIRA Good Practices, DNB aims to provide guidance to supervised institutions for preparing and using a SIRA.

In 2015, we published our first good practices on preparing a SIRA.⁸ We decided to do so after we found that many institutions lacked such an analysis, and that we assessed over 80% of the SIRAs that we did examine as inadequate.

Almost all institutions have now prepared a SIRA. In recent years, however, we found that in many cases, institutions' SIRAs focus only on the elements described in our good practices, and that their own reflection on the relevant integrity risks remains limited. Because institutions rigidly adhere to the SIRA process as described in the 2015 good practices, they often fail to take more recent insights and opportunities into account in practice. Due to this mechanical approach, there is often insufficient understanding of the specific integrity risks the institution faces. And, as a result, the institution is unable to verifiably and effectively mitigate its integrity risks.

To summarise, although many institutions now have a SIRA, we see that in many cases it is not or insufficiently used as a (dynamic) steering instrument for identifying, analysing and mitigating integrity risks. This prompted us to review our SIRA Good Practices document.

³ Bulletin of Acts, Orders and Decrees 2003, 396, p. 20.

⁴ *Parliamentary Papers II* 2001–2002, 28 373, nr. 3, p. 11.

⁵ Section 2b of the Wwft.

⁶ DNB's Wwft Q&As and Good Practices, par. 2.1.

⁷ *Parliamentary Papers II* 2017–2018, 34 808, no. 3, p. 43

⁸ DNB (2015), The integrity risk analysis. More where necessary, less where possible. These new good practices replace the 2015 document.

1.4.2 SIRA Good Practices status

In supervisory practise, it appears that institutions regard the 2015 Good practices document as a normative framework with little or no room for individual interpretation. To disprove this perception, the reviewed document clearly states that no specific approach is prescribed.

This SIRA Good Practices provides practical examples and highlights points for attention that can be used when preparing the SIRA and the *Wwft* risk assessment.

Good practices set out suggestions or recommendations for supervised institutions. They are examples of possible applications that, in DNB's opinion, provide a good interpretation of the obligations laid down in legislation and regulations. Good practices are indicative and institutions are free to take a different approach, as long as they comply with the laws and regulations.

To read more about the status of our policy statements, go to the [Explanatory guide to DNB's policy statements](#) on Open Book on Supervision.

This SIRA Good Practices document replaces the 2015 Good practices document.⁹ In addition to this document, we have published several other policy statements on integrity legislation. An overview of all our general and sector-specific policy statements on integrity legislation is available on our Open Book on Supervision page.¹⁰

1.4.3 Structure of the SIRA Good Practices

This SIRA Good Practices document is structured as follows: Chapter 1 outlines the context and legal framework. Chapter 2 covers the basics of integrity risk management, including a cycle of process steps generally applied in practice to prepare an adequate and up-to-date SIRA. The chapters that follow describe good practices with regard to the different process steps for preparing and maintaining the SIRA.

1.5 Legal framework

1.5.1 *Wft*, *Pw* and *Wtt*: Systematic integrity risk analysis (SIRA)

Institutions must pursue an adequate policy to ensure ethical business operations.¹¹ They must draft and implement this policy based on a systematic analysis of the integrity risks relevant to them.¹²

Laws and regulations

The following laws and regulations are particularly relevant for a systematic integrity risk analysis (where applicable):

- section 3:10 of the *Wft* in conjunction with Section 10 of the *Bpr*¹³
- section 14 of the *Wtt* in conjunction with Section 10 of the *Btt* 2018¹⁴
- section 143 of the *Pw*, Section 138 of the *Wvb* and Section 19 of the Pension Fund (Financial Assessment Framework) Decree (*Besluit financieel toetsingskader pensioenfondsen – Bftp*)
- section 2b and 2c of the *Wwft*.

⁹ DNB (2015), The integrity risk analysis. More where necessary, less where possible.

¹⁰ <https://www.dnb.nl/en/sector-information/open-book-supervision/open-book-supervision-themes/supervision-of-financial-crime-prevention-integrity-supervision/>

¹¹ Section 3:10 of the *Wft* (payment processing service provider, payment institution, clearing institution, electronic money institution, special purpose reinsurance vehicle, bank, credit union, premium pension institution, insurer, exchange institution or branch as meant in Section 3:10(1), 3:11, 3:12, 3:12a, 3:13 or 3:14 of the *Wft*), Section 14 of the *Wtt* (trust office), Section 143 of the *Pw* (pension fund).

¹² Bulletin of Acts, Orders and Decrees 2006, 519, p. 104 and Bulletin of Acts, Orders and Decrees 2011, 673, p. 19.

¹³ Section 3:10 of the *Wft* and Section 10 of the *Bpr* apply to a payment institution, clearing institution, electronic money institution, special purpose reinsurance vehicle, bank, credit union, premium pension institution, insurer, exchange institution or branch as referred to in Section 3:10(1), 3:11, 3:12, 3:12a, 3:13 or 3:14 of the *Wft*.

¹⁴ Section 14 of the *Wtt* and Section 10 of the *Btt* apply to trust offices.

Integrity risk is defined as follows:

- *For institutions governed by the Wft*: integrity risk is the danger of harming a financial institution's reputation, or an existing or future threat to its assets or financial results ensuing from insufficient compliance with what is prescribed under or pursuant to any legal provision.¹⁵
- *For trust offices*: integrity risk is the risk of insufficient compliance with what is prescribed under or pursuant to any legal provision or involvement by the trust office or its employees in acts or conduct that conflict to such an extent with commonly accepted standards that they may seriously damage confidence in the trust office or in the financial markets.¹⁶

Institutions follow a number of steps to identify and manage circumstances and events that may affect the integrity of the institution's ethical business operations:¹⁷

- a systematic analysis of integrity risks, including periodic review
- developing policies and developing procedures and measures to further specify these policies
- implementing the policies and ensuring systematic assessment of policies, procedures and measures.

Here, it is first of all important that the institution systematically analyses its own integrity risks. This means the institution must analyse its own organisation on an ongoing basis to identify which business units are exposed to integrity risks. Based on this analysis, financial institutions must formulate their policies (procedures and measures), adjusting them where needed to safeguard their ethical business operations on an ongoing basis.¹⁸

'Systematic' implies a cyclical process, i.e. institutions are required to perform identification, analysis and testing of the effectiveness of controls at regular intervals. This is because risks are not static. Risks to which an institution is exposed may change as a result of both internal and external factors. An institution's activities may for instance be expanded or changed, specific trends may emerge in the financial and economic world, or laws and regulations may be amended.¹⁹

1.5.2 Policy statements

With regard to specific integrity risk areas, in particular money laundering, terrorist financing and sanctions, DNB and other supervisory authorities have issued guidelines, including DNB's *Wwft Q&A and Good Practices*.²⁰ Where relevant, the SIRA Good Practices should be read in conjunction with these guidance documents.

The European Banking Authority (EBA) has also issued several relevant guidelines, opinions, reports and other statements relevant to banks and other sectors. Together with the other European authorities represented in the EBA's various bodies, DNB is involved in the development of these policy statements and will take them into account in its supervision. The purpose of the EBA guidelines is to ensure the consistent and uniform application of standards under European legislation in all EU Member States.

The guidelines are addressed to supervisors and, in some cases, also directly to institutions, but do not have the same status as binding European regulations. Guidelines provide guidance on the implementation and application of European regulations, and supervisors and institutions must make every effort to comply with them.²¹ This also means that we will refer

¹⁵ Section 1 of the *Bpr*.

¹⁶ Section 1 of the *Wtt*.

¹⁷ Section 10 of the *Bpr*, Section 10 of the *Btt*, Section 19 of the *Bftp*.

¹⁸ Bulletin of Acts, Orders and Decrees 2006, 519, p. 104.

¹⁹ Bulletin of Acts, Orders and Decrees 2018, 463, p. 28.

²⁰ See DNB's *Wwft Q&As and Good Practices*

²¹ Guidelines are subject to a "comply or explain" requirement, which means that supervisory authorities such as DNB must indicate whether they include them in their supervision. In our periodically updated overview "Application of the Guidelines and Recommendations of the European Supervisory Authorities", available at Open Book on Supervision, we set out which guidelines we take into account in applying the relevant supervisory laws and regulations ([Application of the Guidelines and Recommendations of the European Supervisory Authorities](#)).

to EBA policy statements where relevant. The EBA's policy statements are particularly relevant to the *Wwft* risk assessment, for example the *ML/TF Risk Factors Guidelines* and the *Guidelines on the role and responsibilities of the AML/CFT compliance officer*.

Finally, there are several other international policy statements that may be relevant to the content and application of the SIRA, e.g. from the Financial Action Task Force (FATF) and the Basel Committee on Banking Supervision (BCBS), e.g. the policy statement *Compliance and the compliance function in banks* by the Basel Committee on Banking Supervision (BCBS).

We expect institutions to take these policy statements into account in the design and application of their policies, procedures and measures to ensure effective management of the risks they identify. Where relevant international policy statements exist, we refer to these rather than include information from them in our own guidance. This ensures that institutions can always consult recent sources.

1.6 Risk-based approach

As noted above, ensuring ethical business operations is fundamentally about managing the integrity risks to which the institution is exposed. Ensuring ethical operational management thus assumes a risk-based approach.

A risk-based approach means that the deployment and intensity of procedures and measures depend on the level of risk. More limited scrutiny in the case of low-risk situations will allow for greater capacity and attention to be focused on higher-risk situations. This strategy will make it possible to deploy scarce resources where they will be most effective. To ensure an appropriate, effective and efficient risk-based approach to integrity risks, it is therefore essential that institutions are highly aware of the relevant risks. It is also important in preventing to place an unnecessary burden on customers, unjustified derisking and countering exclusion and (indirect) discrimination.

2 Integrity risk management

2.1 Integrity risk management starts with the SIRA

Integrity risk management is fundamentally about managing the integrity risks to which the institution is exposed. That starts with identifying and analysing the integrity risks at issue: what are the risks, how and where would they arise, and what possible consequences would they have – and that, in a nutshell, is what a SIRA involves. This makes the SIRA an important building block, if not the cornerstone, of integrity risk management. Integrity risks may ensue from activities, relationships and actions of almost all sections of a financial institution.

2.2 Managing integrity risks

In addition to documenting its integrity risks, an institution will also have to manage them adequately. To do so, based on the SIRA, the institution has to put in place policies, procedures and measures. Management focuses on reducing the probability of a risk arising and mitigating negative consequences if a risk materialises. The institution then accepts a risk with due observance of the reasonably taken control measures. The institution may also choose to avoid a risk, for example in the event that adequate control measures would require too much or is not actually possible for the institution.

2.3 Reviewing, updating and adjusting

It is also important that the institution establishes that the controls are adequate. Two main questions are important here:

- Are the controls effective? The institution must determine whether the controls are actually effective in managing the relevant integrity risks adequately. Incident reports or audits, for example, may show that control is too weak or too strong in some areas.

- Are there any risks not yet taken into account? Risks may increase and decrease due to internal and external developments, and new risks may arise. It is important that the institution's controls can effectively respond to them.

In short, the institution must analyse its own organisation on an ongoing basis to identify which business units are exposed to integrity risks, taking into account internal and external developments. Where necessary, the institution must update its SIRA and its controls.

2.4 Ethical operational management: preventing breaches of integrity

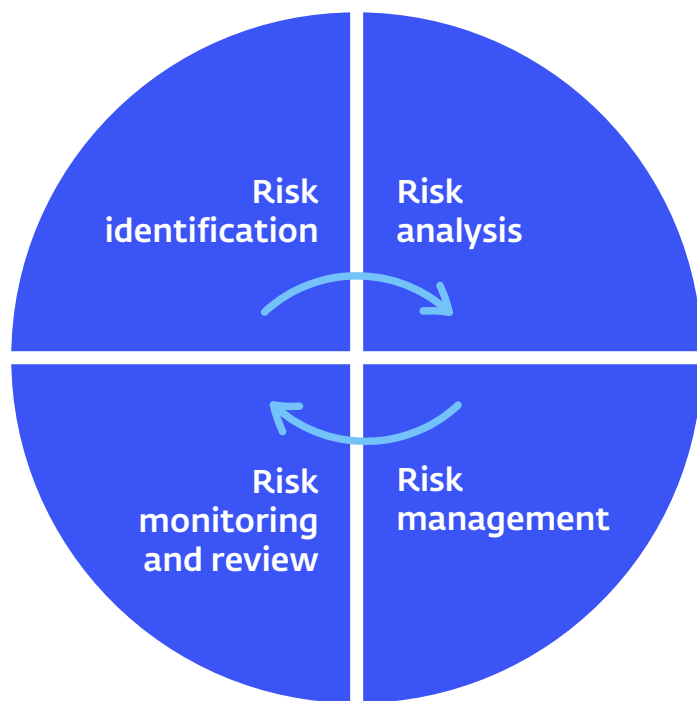
It is worth remembering that integrity risk management is primarily aimed at preventing integrity breaches. This is not to say that such breaches cannot occur. Nor does it mean that an integrity breach is the result of failing operational management, although that may of course be the case. The assessment of an institution's ethical operational management focuses on whether the institution has done what is reasonably possible to prevent breaches of integrity.

2.5 The SIRA as an anchor

The SIRA is an important anchor in this regard. Indeed, without a systematic analysis of an institution's integrity risks, it is impossible to determine whether its policies, procedures and measures are adequately aligned with these risks. The institution then runs the risk of insufficiently preventing its involvement in criminal offences, breaches of the law or socially inappropriate acts that could damage confidence in the institution or in the financial markets.

2.6 Integrity risk management cycle

DNB has reviewed and assessed many SIRAs and their underlying design and review processes in recent years. Based on this and taking into account the legal framework, we have identified a good practice involving a cycle of four process steps. These steps cover the entire integrity risk management process and are applied in practice to develop an adequate SIRA and keep it up to date. This cycle is shown in the figure below and provides a logical sequence of steps to be taken.



Practice shows that the integrity management process is also dynamic. For example, risks not previously identified in the 'risk identification' stage may still be identified in the 'risk analysis' stage or in the 'risk management' stage. The cycle can also be run for emerging or new risks.

The exact sequence of process steps is not key here. What matters is that the institution has a SIRA, and corresponding and appropriate risk management that ensures ethical business operations.

3 Risk identification

3.1 Rationale

The SIRA is an institution-specific analysis of the integrity risks relevant to the institution, so having a good understanding of the institution's organisation and business should be the starting point. Conducting the SIRA therefore starts with drawing up the organisational risk profile.

An organisational risk profile identifies the integrity risks as they occur at different levels within the institution, including the elements that may contribute to the extent to which these risks occur.

The organisational risk profile contains a quantitative and qualitative description of these risk factors. In identifying the risk factors, the institution will consider at least the risks that are of such importance that the law requires that they be addressed, including the risk of:

- involvement in money laundering
- involvement in conflicts of interest and corruption
- investment in socially unacceptable activities.

Examples of risk factors include the type of services provided, the customer portfolio and its related transactions, delivery channels, geographical areas, signatories, outsourcing relationships, etc.

Risk identification, including drawing up an organisational risk profile, is a knowledge-intensive step – it requires knowledge and expertise. This involves knowledge of the organisation on the one hand, and knowledge of integrity risks and the way in which they could materialise on the other. Based on the organisational risk profile, the institution has a good idea of the integrity risks that may occur within its various units and the factors that may expose it to these risks. It can then further analyse the identified integrity risks – this is discussed in Chapter 4.

3.2 Good practices

Good practice – Preparation for the SIRA

An institution starts its periodic SIRA process. Before starting the process and to gain an understanding of the potential integrity risks, the designated officer first prepares the process and undertakes several actions, including the following:

- The designated officer engages (external) expertise to provide support in determining what integrity risks may be involved for this institution.
- Through targeted communication and by obtaining commitment in the organisation, the officer ensures involvement, support and organisational input needed in the process.
- In consultation with the (external) expert, the designated officer identifies relevant and authoritative sources that can be helpful in the process. The officer shares an overview of key resources in the organisation, with a brief summary of the content. This includes in this example:
 - relevant passages from the explanatory memoranda to the *Wft*, *Bpr*, *Wwft* and *Sw*
 - DNB's SIRA Good Practices
 - the EBA's ML/TF Risk Factors Guidelines
 - DNB's *Wwft* Q&A and Good Practices
 - DNB's Guideline on the Sanctions Act
 - the National Risk Assessment (NRA) for Money Laundering
 - the DNB report Integrity Supervision in Focus
 - other relevant sector-wide risk assessments available
 - DNB's Good practices fighting corruption.

- The officer also scrutinises incidents that have occurred at the institution as well as internal reports, audits, complaints and notifications that can provide insight into where integrity risks may be at play.
- Together with the (external) expert, the designated officer draws up a plan of action. The plan includes an internal communication plan, and also provides for management of the SIRA, including through periodic updates.

- the mandatory risks to be addressed, in particular risks of involvement in money laundering, terrorist financing, (national, European or other international) sanctions, conflicts of interest and socially improper conduct
 - the risks associated with the integrity of policymakers and employees
 - the risks indicated by past events and incidents.
- In its identification, the institution also considers any applicable factors that may affect these risks.

Good practice – Steps to draw up an organisational risk profile

An institution takes the following steps to draw up its organisational risk profile:

- inventory of organisational units
- for each organisational unit, an inventory of:
 - the portfolio of products/services
 - the number of FTEs
 - integrity-sensitive positions
 - the customer portfolio
 - the number, size and geographical distribution of transactions
 - the number of incidents, including an overview of internal and external complaints
 - measures imposed by supervisory authorities
 - media coverage which points at potential integrity risks of at factors that could influence these risks.
- inventory of key outsourcing partners and suppliers
- identification of potential integrity risks, both by organisational units and for the institution as a whole:

Good practice – Life insurer organisational risk profile, money laundering risk

A life insurer's compliance officer draws up an organisational risk profile. With regard to money laundering risk, the following risk factors were identified:

- With regard to products, the following factors are explicitly reflected in the organisational risk profile:
 - number of life insurance policies, without capital accumulation
 - number of policies with capital accumulation
 - number of policies with premiums of more than €2,500 per year.
- Regarding delivery channels, the compliance officer notes that the institution only works via direct sales, and not via intermediaries.
- With regard to customers, the following factors are taken into account, while it is already established in advance that the institution does not serve corporate customers. These factors are specifically reflected in the organisational risk profile:
 - number of private customers from the Netherlands
 - number of private customers from other EU countries
 - number of private customers outside the EU.

Good practice – Organisational risk profile, sanctions risk

A bank's management board requests an update of the organisational risk profile with regard to sanctions risk. The officer in charge within the first line prepares the update together with a sanctions expert. For the 'trade finance' organisational component, an expert from that department is engaged. Together, they identify the following risk factors:

- Number of 'Trade Finance' customers.
- Number of customers with import or export relations with Russia. *The same analysis is made for other sanctioned areas such as North Korea, Iran and Myanmar.*
- For sanctions evasion purposes: number of customers with import or export relations with areas with areas prone to sanction evasion regarding Russia, for instance areas bordering Russia. *The same analysis is made for other sanctioned areas such as North Korea, Iran and Myanmar.*
- Number of customers supplying strategic goods and/or dual-use goods.
- Transaction volume to Russia in the last quarter. *The same analysis is made for other sanctioned areas such as North Korea, Iran and Myanmar.*
- In view of sanctions evasion: transaction volume in the last quarter to areas prone to sanction evasion regarding Russia, for instance areas bordering Russia. *The same analysis is made for other sanctioned areas such as North Korea, Iran and Myanmar.*

Good practice – Involving knowledge and expertise

When preparing the organisational risk profile, the officer responsible for the SIRA takes the initiative to involve the various business units and lines of defence. This provides a comprehensive picture of the organisation, including a good understanding of its governance, products on offer, customers, transactions and geographic area of operation. In addition, compliance and integrity expertise is involved to help identify integrity risks and interpret relevant risk factors.

Good practice – Risk factors and data analysis

As part of its money laundering risk analysis, an institution makes a breakdown of its customer portfolio. This provides more insight into the risk factors present in the portfolio. Risk factors include certain legal forms, high-risk countries, high-risk sectors, high-risk products, high-risk channels and cash payments. This breakdown includes the following components:

Customers

- Number of customers by Dutch legal form, such as foundations and sole proprietorships.
- Number of customers by foreign legal form, such as Ltds, S.A.s, LPs and LLPs.
- Number of customers by customer segment, such as private, small and medium-sized enterprises (SMEs) and large corporations.
- Number of customers by some specific customer groups, such as minors, students, elderly persons and persons under guardianship.
- Number of customers by high-risk sector, such as the online gambling and adult entertainment industries.
- Number of customers operating in cash-intensive sectors.

- Number of customers in sectors in which investigative and government agencies have identified malpractice.
- Number of customers maintaining partnership structures with other institutions, such as sub-merchants.

Products and services

- Number of customers purchasing/using high-risk products, such as cash deposits, trade finance, anonymous payment methods and prepaid debit cards.
- Number of customers using high-risk services, such as crypto services.
- Number of customers who applied for a large number of debit or credit cards.
- Number of (foreign) customers using Dutch IBANs from an electronic money institution.

Geography

- Number of customers operating in high-risk countries.
- Number of customers based within the Netherlands and outside the Netherlands.
- Number of customers based in offshore jurisdictions or high-risk countries.

Supply channels

- Number of customers using specific (high-risk) delivery channels such as brokers, independent asset managers or point of sale terminals.
- Number of branches.

Transactions

- Number and total volume of cash transactions (broken down by customer group).
- Number and total volume of inbound and outbound international transactions to and from high-risk countries or high-risk banks.

- The top 10 high-risk countries and/or banks based on transaction volume are identified and further study is carried out to see if this matches the customer portfolio.
- Significant deviations of transaction flows to specific high-risk countries or sectors compared to the previous year are highlighted and the explanations for these differences are examined.

Good practice – Risk factors and data analysis at trust offices

As part of its money laundering risk analysis, a trust office makes a breakdown of its customer portfolio. This provides more insight into the risk factors present in the portfolio. Risk factors include certain legal forms, high-risk countries, high-risk sectors, high-risk products and high-risk channels. This breakdown includes the following components:

Business relationship/customers

- Number of target companies (TCs) by high-risk sector.
- Number of TCs involving a complex structure (>5 layers).
- Number of TCs with a trust in the structure.
- Number of TCs involving a politically exposed person (PEP).
- Number of customers/TCs with a tax benefit due to establishment in the Netherlands.
- Number of TCs where a report under the 6th Directive of Administrative Cooperation (DAC6 report) has been made with regard to the structure.
- Number of TCs involving a structure with elements that promote anonymity (nominee, trust office foundation (STAK) etc.).
- Number of TCs qualifying as foundation.
- Number of TCs with independently authorised external directors.

- Number of TCs without authorisation to make payments/right to monitor the account.
- Number of TCs involving circular elements in terms of entities/ownership.

Geography

- Number of TCs operating in/with holdings in high-risk countries.
- Number of TCs operating in offshore jurisdictions.
- Number of TCs operating in multiple offshore jurisdictions.
- Number of TCs involving circular elements in terms of structure and countries.
- Number of UBOs from high-risk countries.

Supply channels

- Number of customers introduced by an intermediary.
- Number of customers introduced by a tax consultant.

Combination of risks

- Number of TCs operating in/with holdings in high-risk countries and high-risk sectors.
- Number of TCs with an independently authorised external director and no payment authority on the account/right to inspect the account.
- Number of TCs with a legal form in the structure that provides anonymity and parts of the structure that are established in offshore jurisdictions.

Sanctions

- Number of TCs operating in sanctioned countries.
- Number of customers/UBOs/TCs involving sanctioned entities/persons.
- Number of TCs involving strategic and/or dual-use goods.

Transactions

- Number of TCs involving transactions as meant in Section 35 of the Wtt.
- Number of TCs involving 0-1 million, 1-10 million, 10-100 million, 100-500 million, >500 million transactions.
- Number of TCs involving transactions reported to FIU-NL.
- Transactions involving a known loss.

Board/staff

- Number of trust office UBOs residing in a high-risk country.
- Relevant ancillary positions of board members.

Good practice – Identification of risk of conflict of interests

With regard to the risk of conflict of interests, a number of risk factors emerge in the organisational risk profile, including the following:

- At the board level, directors can independently bind the institution up to €25 million.
- In addition, the institution finds that the directors have various ancillary positions that may bring other interests into the decision-making process. For example, one director holds several ancillary positions with parties with which the institution has commercial relationships. This includes a party to which the institution makes significant donations in the form of sponsorships.

Good practice – Identification of risk of (indirect) discrimination

A bank finds that there may be unintended side effects in implementing its policies relating to the *Wwft* and the *Sw*, such as exclusion and discrimination of customers. The bank has taken note of a number of relevant studies (a Ministry of Finance study and a DNB study).²² The bank has also listed complaints filed by customers experiencing discrimination in the bank's application of measures relating to the prevention of money laundering and compliance with sanctions regulations.

Based on this information, the bank identifies the risk that customers are unintentionally indirectly discriminated against in the customer due diligence (CDD) process. The bank decides to conduct a more comprehensive risk analysis to identify the steps and elements in the CDD, transaction monitoring (TM) and Sanctions process where the bank is at increased risk of customers being unintentionally discriminated against or experiencing discrimination. Based on this analysis, the bank will take appropriate measures to mitigate the risk of actual or perceived discrimination.

Good practice – Identification of risks and risk factors at a trust office

A trust office analyses its portfolio and identifies several relevant risks and risk factors:

1. The trust office is vulnerable to money laundering through real estate. It has a number of target companies with an independent external director combined with activities in high-risk real estate. The trust office finds that half of these target companies have a structure involving multiple companies, with the UBO being involved in all of them. This indicates an increased risk of money laundering with real estate through ABC transactions, for example.
2. The trust office has a number of target companies with operational activities in countries that are geographically close to sanctioned countries and have close political ties with these sanctioned countries. This indicates possible exposure to evasion of sanctions regulations.
3. The trust office also identifies potential involvement in corruption and the receipt of funds derived from corruption. The trust office has a number of target companies with operations in countries with a poor Corruption Perceptions Index (CPI) score, combined with operations in an industry prone to corruption. In this case, it concerns a state-owned company and a mining company. The trust office also finds that a PEP is involved.

²² See: www.rijksoverheid.nl/documenten/publicaties/2024/04/19/rapport-kmpg-en-i-o-research-naar-ervaren-discriminatie (in Dutch).
See also: www.dnb.nl/media/ozsdxz4/78730-2400217-dnb-brochure-tegengaan-van-discriminatie_tg-pdf.pdf.

Good practice – Identification of risks and risk factors at a payment service provider

A payment service provider (PSP) analyses its portfolio and identifies several relevant risks and risk factors:

1. The institution finds that it could potentially be involved in circumvention of sanctions regulations. It has carried out an analysis of the risk factors in its SME portfolio related to transaction flows. In doing so, the institution has provided insight into the total number and volume of inbound and outbound international transactions to high-risk countries, and how this compares with figures from previous years. The analysis shows that the transaction volume to a particular high-risk country has risen sharply since sanctions were imposed on a neighbouring country.
2. Based on an analysis of its customer portfolio, the PSP identifies specific factors related to money laundering risks. In its customer portfolio, the institution notes a sharp increase in customers active in crypto trading through unregistered foreign platforms – there is a group of customers with large transaction volumes flowing towards these platforms. The institution also identifies a number of customers active in the gambling industry with strongly rising transaction volumes.
3. To gain further insight into potential exposure to money laundering risk due to the cash risk factor, the institution analyses its retail customers' cash usage. The institution analyses which customers deposit more than a certain amount of cash per year. It does so for a number of different thresholds (€20,000, €50,000 and €100,000). In particular, the institution is mindful of those cases where the use of cash does not fit within the expected pattern and business model of the client. The institution identifies a number of customers for which the amount of cash deposited is many times higher than that customer's annual income.

Good practice – Developing new activity

An institution actively seeks opportunities for growth, and for strengthening and deepening its customer relationships. The institution is considering entering into a new activity. As part of the decision-making process, the institution commissions an integrity risk analysis. This 'SIRA for the new activity' provides insight into the integrity risks involved in operationalising, implementing and running the potentially new activity. The decision of whether to enter into the new activity and under what conditions is based in part on this integrity risk analysis.

Good practice – Geopolitical developments

To prevent its investments from not being in line with what is considered socially acceptable, a pension fund pursues a socially responsible investment policy.

The pension fund notes that social acceptance of investments in the defense industry has increased as a result of recent developments in the security situation in Europe and the Netherlands. The pension fund decides to conduct a further analysis on this, on the basis of which the investment policy could be reconsidered.

4 Risk analysis

4.1 Rationale

After drafting the organisational risk profile, as described in the previous chapter, the institution has an overview of the integrity risks that are relevant to it. In order to develop, implement and prioritise appropriate controls, it is important for the institution to conduct a risk analysis. The institution analyses the identified risk factors and integrity risks and estimates the materiality and frequency at which these risks may actually occur.

How the risk analysis is carried out depends on the institution and the risks. In some cases, the emphasis will be on quantitative in-depth data analysis and in other cases and/or for other risks, analysing the key manifestations, e.g. through scenario analysis, will provide the most insight. A combination of methods often proves to add value in practice. In any case, the risk analysis should make clear to the institution which risks need most attention, with what (type of) controls they can be mitigated and on which moment.

4.2 Good practices

Good practice – Use of external sources

In drafting its risk analysis, a bank uses insights from the National Risk Analysis (NRA), Financial Action Task Force (FATF) publications, the Anti Money Laundering Centre (AMLC) and other relevant external sources (such as risk assessments from industry associations) that provide insight into typologies and indicators related to integrity risks.

The various organisational units use the same approach. For example, the compliance officer for the 'Correspondent Banking' department uses the FATF guidance on correspondent banking in their analysis. This FATF guidance refers to *"The risk factors included in the Annex II of the BCBS Guidelines on Sound management of risks related to money laundering and financing of terrorism"*.²³

Based on the information from these sources, the bank considers the following factors in its risk analysis:

- the inherent risk arising from the nature of the services provided
- the characteristics of (and information about) the respondent bank
- the environment/jurisdiction in which the respondent bank operates.

In addition, the bank also pays particular attention to 'nested correspondent banking' in its risk analysis.²⁴

²³ FATF (2016), *Guidance on correspondent banking services* (Guidance on Correspondent Banking (fatf-gafi.org)), p. 10. See also BCBS (2020), *Guidelines on Sound management of risks related to money laundering and financing of terrorism* (Sound management of risks related to money laundering and financing of terrorism (bis.org)).

²⁴ BCBS (2020), *Guidelines on Sound management of risks related to money laundering and financing of terrorism*, p. 27; www.austrac.gov.au/correspondent-banking-relationships.
Nested correspondent banking: a bank's correspondent relationship is used by a number of indirect respondent banks ('nested banks') through their relationships with the bank's direct respondent bank to conduct transactions and obtain access to other financial services.

Good practice – Use of money laundering indicators at a money transaction office

The organisational risk profile of an MTO states that branches in tourist areas handle comparatively more different currencies. In that context, there are also some offices in the Netherlands where many customers with a French residential address have transactions carried out once or several times a month.

The AMLC's Overview of Money Laundering Indicators used in the risk analysis mentions "that various forms of crime involve large amounts of cash in various currencies."²⁵ Based on this, the MTO concludes that the money laundering risks associated with cash deposits are higher for transactions involving large amounts of cash in various currencies, and that this particular risk manifests itself particularly in branches in the identified tourist areas.

The MTO also considers the EBA's ML/TF Risk Factors Guidelines in its analysis. One of the factors that may contribute to higher risk is: "The customer's needs may be better served elsewhere, for example because the money remitter is not local to the customer or the customer's business." On this basis, the MTO finds that the service provided by the Dutch branches to customers with a French residential address poses an increased risk of money laundering.

Good practice – Use of money laundering indicators at a life insurer

In terms of products, the organisational risk profile of a life insurer shows that the institution only offers term life insurance. Premiums are collected from a fixed contra account. Premiums average around €1,000 a year and do not exceed €5,000 a year.

In its risk analysis, the institution considers the EBA's ML/TF Risk Factors Guidelines. Based on Guideline 14.7, the institution finds that its term life insurance is a low money laundering risk. The institution's own insights support this conclusion, also because it appeared during the SIRA session that no realistic scenarios could be devised for money laundering through term life insurance.

Good practice – Partial analysis of the risk of conflict of interests

An insurer analyses the risk of conflict of interests at board level, and takes as a starting point the question of how directors may favour themselves and/or parties related to them using their decision-making power – the institution sees this as a major risk factor. The director responsible for 'Compliance' read in a DNB publication how DNB points out the risk of directors with significant powers of procurement for independently making commitments and/or payments. Assigning significant powers of procurement to a director entails an increased risk of conflict of interests.²⁶

²⁵ Anti Money Laundering Centre, *Overview of Money Laundering Indicators*, p. 4. At the time of preparing this Good Practice, the February 2024 version was the current version (in Dutch): [Overzicht-witwasindicatoren-februari-2024.pdf \(amlc.nl\)](#).

²⁶ DNB (2024), *Integrity Supervision in Focus 2024-2025*, p. 15.

The institution analyses various possible manifestations to specify this risk, such as:

- making private purchases or sales from or to the institution (e.g. real estate or business assets)
- hiring a personally related company for assignments
- approving business declarations for private expenses
- acquiring business assets for private purposes, such as a car or a holiday home
- approving services with conditions that are exceptionally favourable to the service provider
- getting themselves invited to trips and seminars, and then approving them
- influencing decisions favourable to an organisation where the director holds an ancillary position (e.g. sponsorship of a related party).

Because of the director's position in decision-making, the institution further finds that directors hold confidential information, which may give rise to the following manifestations of integrity risks:

- passing on confidential information to an organisation where the director holds an ancillary position
- using prior knowledge for the purpose of self-enrichment.

The institution translates these types of manifestations into detailed scenarios to estimate how a risk may manifest itself and what the impact, if any, would then be. The institution also uses the scenarios to develop mitigation measures.

Good practice – Use of scenarios – Criteria for describing scenarios

An institution uses scenarios for its risk analysis, among other things. Within this framework, it has drawn up criteria that a scenario has to meet, such that it supports the institution, on the one hand, in detecting the occurrence of the risk in practice and, on the other hand, in defining concrete control measures.

The criteria established by the institution for the description of a scenario are:

- A scenario is concrete and describes a series of actions, decisions and/or events. These are formulated in such a way that they are observable (a "payment" is observable, but that it is "payment of a bribe" is not readily observable).
- A scenario is institution-specific, i.e., a link to the characteristics and services of the institution in question is important.
- A scenario relates to the actual manifestation of the integrity risks and not to process-related shortcomings (such as, for example, the late reporting of a transaction to the FIU or the failure to carry out client screening adequately or on time).

Good practice – Use of scenarios – Conflict of interests when a director hires their own company

To specify how integrity risks may manifest themselves, an institution draws up scenarios and describes them as a series of detailed actions.

The institution has created a scenario regarding the institution's hiring of a director's own company. The scenario describes detailed steps and actions:

1. The institution formulates an assignment on the basis of which an external party can be engaged.
2. One of the commercial directors says she knows a suitable party, and would like to sound them out. The director is a co-shareholder of the party in question. However, she does not report this interest.
3. The director in question then reports positively on the party, indicating that they made a knowledgeable and professional impression, and that a quotation for the work will follow shortly.
4. Upon receipt of the quotation, this director approves it.
5. The director also approves the invoices for the assignment.

Using this scenario, the institution finds that prior to decision-making, it is important to know about the interests, if any, that the persons involved may have, and that these must be explicitly addressed when making decisions. The institution also defines mitigating measures, in particular that decisions about hiring third parties cannot be made by one person.

Good practice – Use of scenarios – Money laundering via loanback

In its organisational risk profile, an institution noted that a relatively large percentage of smaller companies in its customer base receive loans from foreign parties. The institution identifies a risk of involvement in money laundering through customer-applied loanback structures, and elaborates on this in a scenario:

With a loanback construction, a person or entity makes it appear as if it has legally obtained money at its disposal through a loan from another party. However, in fact, they are 'lending' money (not legally obtained) to themselves through an affiliated entity. The related entity may have partly the same directors or UBOs, for example. The loan adds an apparent legal touch to what is actually the disposal of funds obtained through crime. The scenario addresses the following series of actions:

- *Company A is a customer.*
- *A foreign company B provides a loan to company A. There is a flow of funds from company B to company A. This flow of funds is supported by a loan agreement.*
- *The loan features have unusual aspects, such as higher or lower than usual interest rates, no collateral, no repayment terms or annual deferral of repayment.*
- *Although the loan agreement suggests that company A will repay the borrowed amount to company B, this does not happen in practice. The money remains with Company A and is used for other purposes.*

Using this scenario, the institution finds that in this situation, it is important to conduct in-depth research into possible relationships between company A and company B, and, in particular, to check carefully who the UBOs and directors are. It is also important to have sufficient insight into the source of the cash flow associated with the loan and to check the commercial rationale for the loan and the loan conditions. All the above also applies to similar scenarios, where, for example, money is borrowed from a private individual.

Good practice – Use of scenarios – Trade-based money laundering

In its organisational risk profile, a bank has found that there is a risk of involvement in money laundering through trade-based money laundering, where customers use trade structures to give obtained money through crime an apparently legitimate origin. The bank lists possible manifestations of trade-based money laundering:

- Company A receives a consignment of goods from Company B (from abroad). The goods are priced (much) too high or too low.
- Company A receives from company B (abroad) a consignment of goods with invoices and bills of lading that show inconsistencies.
 - For example, the price or weight on the documents does not match.
 - With multiple invoices for the same consecutive flows of goods, inconsistencies in invoice numbers, container numbers or VAT numbers may also stand out.
- Company A receives from Company B a consignment of goods imported via an airport, while it makes no sense to transport this type of goods by aircraft.
- Company A receives from a foreign company B a consignment of goods that logically cannot originate from that country or for which there are sufficient low-priced goods in Company A's country.

The institution translates these types of manifestations into detailed scenarios to estimate how a risk may manifest itself and what the impact, if any, would then be. The institution also uses the scenarios to develop mitigation measures.

Good practice – Data analysis and reference groups

When analysing the customer portfolio, an institution uses reference groups: groups of customers with similar characteristics. The aim of the analysis is to detect anomalous and conspicuous behaviour (outliers) that could indicate money laundering. The institution therefore ensures that the group of customers in a reference group is sufficiently homogeneous, and has defined, for example, the following reference groups:

- persons using a student payment account
- minors using a child account
- customers under guardianship
- customers with dormant accounts
- business customers operating in a specific sector, such as hairdressers and taxi companies.

Based on the defined reference groups and using e.g. the AMLC's money laundering indicators, the institution identifies anomalous and conspicuous behaviour (outliers). Behaviours that could indicate involvement in money laundering flows may include the following:

- customers withdrawing and/or depositing noticeably more cash, which cannot be explained on the basis of their customer profile
- customers with (relatively) much higher or lower turnover than their peers
- customers with larger inbound and outbound cash flows to high-risk countries than their peers
- customers who apply for many payment cards relative to their peers
- customers who receive or pay relatively more payment requests than their peers.

The institution finds that these specific money laundering indicators can actually be observed in its customer portfolio. The institution therefore specifically takes these indicators into account when setting up its transaction monitoring system.

Good practice – In-depth data analysis and key risk indicators at a bank

A bank conducts in-depth quantitative analysis to examine the identified integrity risks in more detail and properly assess the actual extent and impact of these risks.

First, the bank identifies specific topics where high integrity risks have been identified and where deeper analysis is required, such as:

- transactions with high-risk countries
- transactions with high-risk sectors or institutions
- international transactions that are not logical based on the purpose and nature of the business relationship
- customers with many debit cards or credit cards
- many customers registered at the same address, without any immediate rational explanation for it
- accounts of minors with large transaction volumes
- customers whose cash use is conspicuously high, which cannot be explained on the basis of their customer profile.

In the in-depth analysis of conspicuous cash use, the institution looks at both the likelihood and impact of the occurrence of this risk and includes the following factors:

- Cash deposits
 1. How many natural and legal persons deposit more than a certain amount of cash and what are the possible outliers on this?
 2. How many transactions are involved? What is the total transaction volume? Does it concern a specific group of natural or legal persons?
 3. What is the geographical profile of these cash deposits?
 4. How do the cash deposits compare with those of the peers of specific customer groups?
- Cash withdrawals
 5. How many natural and legal persons withdraw more than a certain amount of cash and what are the possible outliers on this?

6. How many transactions are involved? What is the total transaction volume? Does it concern a specific group of natural or legal persons?
7. What is the geographical profile of these cash withdrawals?
8. How do the cash withdrawals compare with those of the peers of specific customer groups?

In the in-depth analysis with regard to high-risk countries, the institution looks at both the probability and the impact of the risk and includes the following factors:

- Number of customers and volume of both inbound and outbound transactions at branches in offshore jurisdictions and/or high-risk countries.
- Changes over time in the number of customers and volume of both inbound and outbound transactions at branches in offshore jurisdictions and/or high-risk countries.

Based on the results of these analyses, the institution can determine where the probability and the impact of the risks are significant. The institution then defines key risk indicators. These are indicators that provide early indication that a potential risk may manifest itself so that risks are identified in a timely manner.

Good practice – In-depth data analysis and key risk indicators at payment institutions and electronic money institutions

A payment institution conducts an in-depth quantitative analysis to further examine the risks identified and to properly assess the actual size and impact of integrity risks.

First, the institution identifies specific topics where high integrity risks have been identified and where more in-depth analysis is required, such as:

- the use of anonymous payment methods that can be topped up with cash
- offering digital wallets that can be topped up with cash or crypto.
- issuing IBANs to foreign customers
- customers who want cashback transactions deposited back into other accounts
- transactions with high-risk sectors or institutions such as online gaming and gambling
- transactions on behalf of partner structures
- transactions with high-risk countries.

In the in-depth analysis on the use of anonymous payment methods, the institution looks at the probability and impact of the risk, and includes the following factors:

- How many transactions are conducted via anonymous payment methods (per customer and in total)?
- How many customers purchase more than a certain number of different anonymous payment methods to offer to its end users?
- What is the volume flowing through these anonymous payment methods (per customer and in total)?
- Does it concern a specific group of customers that purchase a large number of anonymous payment methods to offer to their end users?
- What is the geographical profile of customers offering these anonymous payment methods to their end users?

Based on the results of this analysis, the institution determines the following key risk indicators:

- The number of different payment methods used by a customer.
- The number of different payment methods used by a customer in a high-risk country.
- The number of transactions conducted through anonymous payment methods (per customer and in total).
- The volume flowing through these anonymous payment methods (per customer and in total).

Good practice – In-depth data analysis with risk factors and scenarios at trust offices

A trust office conducts an in-depth quantitative analysis to further examine the identified money laundering risks and properly assess the actual size and impact of this integrity risk.

The trust office has several target companies in high-risk countries and high-risk sectors. The trust office analyses the transactions of all these target companies using the following risk factors, which are relevant according to the external sources consulted by the trust office:

- transactions involving a PEP
- transactions involving state-owned enterprises
- transactions for which insufficient substantiating documentation has been provided to indicate the origin/legitimacy
- transactions involving circular elements (such as circular transactions within the same group or transactions from country A, through country B, back to country A)
- transactions involving affiliates (another company with the same UBO, same management, or of family members)
- loan agreements with unusual characteristics.

The trust office translates these risk factors into detailed scenarios to estimate how and where a risk may manifest itself and what the impact, if any, would then be. The institution also uses the scenarios to develop mitigation measures, on a target company-specific basis where necessary.

5 Risk management

5.1 Rationale

The risk analysis described in the previous chapter provides important insights for various departments within the organisation. These insights provide guidance for management and lay the foundation for the institution's integrity policy, based on which the institution intends to manage its integrity risks. The integrity policy is reviewed on a regular basis. Based on the risk analysis, the institution puts in place policies, procedures and measures to manage its integrity risks.²⁷

And this reflects the purpose of risk management: by deploying controls, the institution mitigates the integrity risks revealed in its SIRA process. It also assesses whether the risks can be adequately mitigated. On this basis, the institution can then decide to accept the residual risk, reduce it further by deploying additional controls, or avoid it altogether.

Risk management is about the institution applying controls that are appropriate to the risks identified. In this context, it is not only important for institutions to take more measures in the case of higher risks, but it is also appropriate for institutions to use the scope available to apply more limited measures in the case of lower risks. It also implies that a risk assessment, however judicious, may nevertheless potentially result in a decision that, in hindsight, was poor. This does not necessarily indicate a management failure. In other words, good risk management does not mean that undesirable events will no longer occur. What it does mean is that the institution has done what is reasonably possible, and commensurate to the risks, to prevent the occurrence of such events and can adequately mitigate any negative consequences should they occur.

²⁷ The set of policies, procedures and measures is also referred to as 'controls'.

5.2 Good practices

Good practice – Establishing controls based on the scenario of 'a director hiring their own company'

An insurer's risk analysis includes a scenario on a conflict of interests arising from a director hiring their own company. The analysis reveals it is a material risk.

The scenario allows the insurer to determine appropriate measures to manage this risk. It then deploys the following controls:

- The institution has a code of conduct that requires policymakers to report actual or perceived conflicts of interests.
- The institution keeps a register of interests and ancillary activities.
- The institution uses criteria for the selection of external parties, and has a procedure for awarding contracts.
- If a director introduces a party, that director is asked about the source of the positive recommendations of the party they introduced and their relationship, if any, with that party. The institution consults the register of interests and ancillary activities, and in the case of larger assignments it conducts additional open-source research.
- Before entering into discussions with an external party, it is first checked whether the party in question meets the criteria and whether and how an initial interview would fit within existing procedures.

- The initial interview is conducted by at least two representatives of the institution (four-eyes principle). The director who introduced the party does not participate in the interview if they have a relationship with the party concerned.
- During the interview, the selection procedure is explained. A report of the initial interview is produced. The report specifies the reason for the interview as well as the involvement and/or relationship of the institution's representatives with the relevant business unit and party.
- The selection procedure involves soliciting multiple bids, assessing parties against the selection criteria, talking to multiple parties where possible, and applying the four-eyes principle.
- Persons on the selection committee indicate in writing their relationship(s), if any, with the interested parties. The register of interests and ancillary activities is also consulted. In case of an actual or perceived conflict of interests, the person concerned will be excluded from the selection committee.
- The directors and owners of the interested parties are identified.
- The power of representation for approval is clearly defined and delineated.
- Regarding the billing process:
 - the execution of the work is reviewed
 - the four-eyes principle is applied for the approval and payment of invoices
 - the power of procurement is defined and delineated.

The insurer also actively works to promote an integrity-aware corporate culture, which includes exemplary behavior, open communication and dialogue, holding each other accountable and safely reporting possible incidents.

Good practice – Establishing controls based on a loanback scenario at a bank or trust office

An institution's risk analysis reveals that involvement in a loanback scenario is a material risk.²⁸ The institution uses its loanback scenario to establish controls to manage this risk.

Transaction monitoring

The institution takes measures to detect suspicious transactions that may indicate a loanback scenario.

A bank establishes business rules to identify suspicious transactions within the transaction monitoring system that may indicate a loanback scheme.²⁹ These business rules include:

- Detection of consecutive transactions between the same parties that exceed normal business activities.
- Detection of large transfers to a customer with the description 'loan' or equivalent descriptions – while these transfers do not originate from a regular lender.

Thresholds and/or bandwidths are set for transactions that deviate from expected behaviour/the transaction profile, allowing further investigation of suspicious activities.

Enhanced Customer Due Diligence (EDD)

In response to transaction monitoring alerts, the institution conducts in-depth background checks of customers involved in transactions involving loan agreements with transfers from foreign entities. In particular, the institution examines:

- Unusual business structures, such as customers with dormant businesses or businesses with little activity. The rationale for using these structures should be clear and rational.

²⁸ See Good practice – Use of scenarios – Money laundering via loanback in Chapter 4.

²⁹ For an explanation of the use of business rules in transaction monitoring, see DNB's *Wwft* Q&As and Good Practices, par. 4.1

- The source of funds that are transferred to the customer as a 'loan'. The institution also analyses the loan documentation, possibly using special analysis and tools (see below).
- Where loans are involved, it is verified that there are also periodic payments of interest and repayments of the principal.

Automated analysis of loan agreements

The institution uses analytics software to scan customer loan agreements for suspicious patterns or inconsistent information. The institution:

- Checks whether there are any loan agreements where the terms and amounts appear unrealistic in relation to the normal business activities of the parties involved.
- Checks for potentially fraudulent loan documentation, such as documents with a layout indicating copied elements or inconsistent signatures – these factors can indicate fraudulent loan agreements.
- Checks the repayment schedule in loan agreements and verifies that there is no continuous suspension of repayment instalments.

Good practice – Establishing controls based on data analysis of transactions to high-risk countries

A bank has found that exposure to high-risk countries is a material risk. It carried out an in-depth analysis of transaction flows in its portfolio to high-risk countries.

- Based on this analysis, the bank has identified a group of customers who classify as an outlier group compared to their peers. These customers are then subjected to an Event Driven Review (EDR).
- The bank also assesses whether the customers' transaction behaviour fits within the institution's risk appetite, and if not, what mitigating measures are needed in this context.
- The bank also uses the insights from the analysis to improve its mitigating controls. Business rules and transaction monitoring models are refined where necessary.

Good practice - Limited control measures at low risk

The risk analysis of a life insurer shows that the institution has a very low money laundering risk (see the earlier good practice 'Life insurer organisational risk profile, money laundering risk').

The insurer decides to apply simplified customer due diligence measures with regard to term life insurance.

Good practice – Cash transactions and low risk

A bank conducts an analysis of its retail customer portfolio and cash usage. The bank sets a threshold amount on the basis of this. A cash transaction that remains below that threshold amount is – without the presence of other risk indicators – no reason for further investigation.

Good practice – Unmanageable risk

An institution operating in the EU is exploring opportunities to expand its activities. One of these opportunities involves offering products and services through local agents in South American countries. While carrying out the SIRA, the institution finds that the corruption risk with regard to the target countries is such that it is not sufficiently manageable with the existing measures.

The institution does not want to get involved in corruption. Managing this risk in this case would require more intensive measures and a high degree of professionalism. The institution does not have the required capacity and expertise. It therefore decides to avoid the risk and forgo this opportunity.

Good practice – Monitoring payment requests

In its risk analysis, an institution finds that a large volume of payment requests received and sent from or to one customer could be an indicator of fraud or money laundering. Based on the analysis and its risk tolerance, the institution has established Key Risk Indicators (KRIs) by peer group for the number of payment requests received and sent and the size of the amounts involved. If the thresholds specified in these KRIs are exceeded, an Event Driven Review (EDR) is initiated.

Good practice – Payment authorisation procedure

A director of an institution has independent authority to bind the institution for up to €10 million. To prevent directors from taking advantage of this authority, the institution has procedures in place that ensure the four-eyes principle is applied when deciding on commitments and also that at least two people must approve payments. The latter is enforced by the institution's payment system.

Good practice – Loans to directors

An institution provides loans to its directors. The risk analysis shows that the risk of conflict of interests is material. To manage this risk, the institution has policies and procedures in place to ensure such loans are granted only in the context of the institution's regular business operations and are concluded only after approval by the supervisory board. An opinion of the compliance officer is attached to the proposal to the supervisory board.

Good practice – Data analysis for cash use: KRIs and transaction monitoring

Based on a data analysis of its customers' cash use, an institution has gained insight into the average cash use and outliers of its retail customers and the different reference groups within this population. Based on these insights, the institution draws up KRIs and transaction monitoring rules for each reference group. If customers deviate from the KRIs, the institution determines whether an EDR is needed. The customer is questioned only if their cash use is conspicuous and possibly illegitimate.

Good practice – Country risk and risk management

Based on various external sources, an institution has identified a number of countries it considers high risk. In the context of its control framework, the institution has determined that the capacity to mitigate these risks is insufficient to operate in some of these countries. For other countries, it has set limits for the number of (business) customers it is willing to accept from these countries. At the same time, the institution has defined KRIs for the transaction flows to and from these countries and converted them into specific business rules for the transaction monitoring system. As a result, the institution is able to adequately monitor the money flows to and from these countries.

Good practice – Risk assessment of payment service providers with sub-merchants

A payment institution has established that payment services are provided to customers with sub-merchants. To properly focus the controls, the payment institution decides to take the risks of the underlying sub-merchants into account when establishing a risk profile for the customers with sub-merchants. After all, the risks of the sub-merchants could also affect the customer's risk profile – for example, in a situation where the customer would be assigned a 'low risk' rating on a stand-alone basis, while the customer's sub-merchants engage in 'high risk' activities such as gambling.

Good practice – A trust office decides to part ways with customers following its risk assessment

A trust office has identified target companies in its customer portfolio that have an independently authorised external director as well as no right for the trust office to inspect the target company's bank account.

The trust office finds that adequate transaction monitoring is not possible as a result and there is an increased risk of various integrity risks such as money laundering, sanctions evasion and tax evasion – which cannot be further analysed and therefore cannot be managed. The trust office decides to part ways with these customers if the right to inspect the account is not obtained within a month – the risks cannot be adequately managed and therefore fall outside the scope of its risk tolerance.

Good practice – Deciding not to hire a candidate

An institution has a vacancy for a compliance officer. One of the applicants meets the criteria according to their CV and is invited for an interview. The interview goes well and the institution wants to hire this person.

The institution regards the position of compliance officer as an integrity-sensitive position. The institution has set up a procedure for such positions, which involves screening and an assessment of the candidate's propriety in advance. Part of the screening is a diploma check.

The diploma check reveals that the applicant does not have the degree indicated on their CV. When confronted, the candidate admits they do not have it. The institution decides not to proceed with the candidate.

6 Risk monitoring and review

6.1 Rationale

By monitoring risks and the effectiveness of controls, an institution determines whether its control framework is still adequate. There are several reasons for an institution to review its organisation on an ongoing basis to identify business units at risk of integrity risks, and to adjust its SIRA and its controls where necessary:

- An institution and its environment continue to evolve. For example, incidents that occur, geopolitical developments, the introduction of a new product or an acquisition may prompt a review of the integrity risk analysis. This may obviously also have implications for the controls.
- Some of the implemented controls may turn out to be inadequate. For example, incident reports, complaints or audits may show that risk management is too weak in some areas, or that certain low risks are being managed with more resources than necessary. It may also turn out that some of the risks for which controls are in operation are no longer current – the institution may then consider removing these controls.

The institution uses risk monitoring and review to ensure its SIRA is up-to-date and well-focused and its controls are appropriate. In doing so, the institution safeguards the integrity of its operations and thus makes every reasonable effort to avoid becoming involved in events, activities or parties that could affect the integrity of the institution and/or its staff.

6.2 Good practices

Good practice – Using feedback loops

An institution has implemented feedback loops as part of its risk monitoring. The institution uses these feedback loops to monitor whether integrity risks change or whether there are new integrity risks or manifestations of integrity risks.

The institution includes insights from the following sources:

- reports from relevant authorities and organisations such as DNB, FATF, AMLC, OECD, etc.
- supervisory examinations
- event-driven and periodic reviews
- reports to and feedback from FIU-NL
- results of sector analyses by industry associations
- outcomes of compliance monitoring and audits performed
- lessons learned from complaints and incidents.

The institution conducts an analysis based on questions such as: Does this involve a new or changed risk? How could this have happened? Why were the controls ineffective? How do we prevent failure in the future? In this way, the institution increases its understanding of how risks may materialise and the effectiveness of its controls.

Good practice – Feedback loop based on outcome of periodic review

During the periodic review of a target company, an account manager of a trust office observes that the turnover from operational activities of a target company's holding has increased sharply. The holding is based in a country bordering a sanctioned country.

The account manager requests documentation from the target company to investigate the matter further. Based on the outcome of this investigation, a re-acceptance procedure is initiated. The account manager also notifies the compliance officer.

The compliance officer performs a broader analysis on the portfolio to check whether this scenario also occurs in other target companies in the portfolio. The scenario is included in the SIRA.

Good practice – Feedback loop based on an analysis of recent exits

A payment institution regularly conducts an in-depth analysis of recent exits, analysing and evaluating the underlying reasons for exiting these customers. This allows the payment institution to identify trends and patterns regarding high-risk customers and activities.

Based on these insights, the institution adjusts its risk analysis by adding new risk factors, reviews existing risk models and makes improvements to its customer monitoring and due diligence procedures.

By drawing lessons from recent Wwft-related exits, the payment institution can strengthen its risk management processes and proactively identify and manage risks.

Good practice – Feedback loop following a data breach or scandal

An institution continuously monitors external news sources and media releases for information that may be relevant to its risk analysis. When a new major data breach or financial scandal comes to light, the institution immediately analyses the available data and identifies potential risks and exposures within its customer base and transaction flows. These findings are then used to refine and adjust existing risk models, strengthening the institution's financial crime prevention and detection capabilities. This approach enables the institution to respond proactively to new information and continuously improve its risk management process.

Good practice – Monitoring geopolitical developments

An internationally operating insurer keeps a close eye on geopolitical developments and international conflicts that may affect its business activities. When an international conflict escalates and leads to the imposition of sanctions, the insurer immediately conducts a risk analysis to evaluate the potential impact on its business. This includes a thorough assessment of its exposure to risks arising from the sanctions, such as doing business (or facilitating business) with sanctioned persons or entities, and damage to its reputation.

Based on this analysis, the insurer develops an updated risk management plan aimed at identifying, assessing and controlling new and emerging risks arising from the conflict and subsequent sanctions.

Good practice – Using reports to and feedback from FIU-NL

A bank uses its reports to FIU-NL and the feedback on these reports from FIU-NL as input for its risk analysis process. It analyses this information to identify trends, patterns and risky behaviours that its own monitoring processes may not have detected before.

Based on this analysis, the bank adjusts its risk models and transaction monitoring rules to improve its ability to detect and report unusual and potentially suspicious activity to FIU-NL. In addition, the bank uses the feedback received to train its staff and make them aware of the latest developments and trends in financial crime.

Good practice – Analysis of transactions to high-risk countries

A bank notes a significant increase in transactions from a country bordering a sanctioned country. The bank conducts a more in-depth analysis into the transactions, involving indicators such as:

- frequency, size and destination of transactions
- relationship between payor and payee
- nature of the transactions
- regular activities of the parties involved in relation to the transactions observed.

The bank notes a significantly increased likelihood of involvement in circumvention of sanctions regulations. This is far beyond the bank's risk tolerance, and it is therefore implementing additional, tightened controls.

Good practice – Assessment of design and effectiveness of control measures

To ensure the effectiveness of the entire SIRA process and its consistency with procedures and measures, an institution's compliance and audit functions periodically assess the design and operation of the control framework with respect to integrity risks. This is done in collaboration with the Risk Management department. This is reported to the executive board. Based on this, the institution adjusts, where necessary, the control measures required on the basis of the SIRA.

Good practice – Management Board & Supervisory Board involvement

An institution regularly discusses the results of the recent SIRA in meetings of its Management Board (MB) and Supervisory Board (SB). The key risks are discussed and evaluated, including their potential impact on the organisation. Based on this analysis, the SB and MB set risk management priorities and determine which areas need special attention.

The MB then takes the lead in tightening mitigating measures to effectively address the identified risks. This may include allocating additional resources to high-risk areas, implementing new checks and procedures, updating existing guidelines and policies, or removing certain controls because the risk in question no longer occurs.

The MB ensures that measures taken are followed up regularly to evaluate whether they have been effective in mitigating the risks. If necessary, adjustments are made to improve their effectiveness.

The MB reports on this to the SB on a regular basis. In that context, the role of the MB and the development of an integrity-aware corporate culture are also being discussed.



Annex – Main changes compared to the 2015 SIRA Good Practices

The main changes compared to the 2015 SIRA Good Practices are the following.

Topic	Change	Topic	Change
Risk management cycle representation	The integrity risk management cycle is shown in less detail by limiting it to the four main steps. This was prompted by the desire for less prescriptive wording.	Risk identification and risk analysis	The 'risk identification' step involved developing an organisation outline, defining scenarios and the scoring system for probability and impact.
Rationale	The rationale for taking the relevant step is indicated for each part of the integrity risk management cycle. At the same time, this makes it clear that it is not primarily about performing certain steps in a certain order, but much more about the outcome of the process: a good SIRA as the basis for implementing appropriate controls.		In this new Good Practice document, the risk identification step emphasises the organisational risk profile and identification of factors that may be relevant in the context of integrity risks.
Examples of integrity risks	The list of examples of integrity risks is no longer included. It was intended to provide examples that could help institutions identify risks that may be relevant to them. In practice, we found that institutions used the list as a prescriptive element. In many SIRAs, the list of examples is then taken as the starting point for the analysis.		The risk analysis step focuses on working out the risks in more detail. We refined the approach from the 2015 SIRA Good Practice, in which determining probability and impact for scenarios was important, because we found that institutions viewed determining probability and impact as a mandatory step, applying a mathematical precision that is less well suited to the qualitative nature of many integrity risks. Thinking about probability and impact can be helpful in the analysis stage, but there are several other ways that can also support the analysis.
Integrity risk analysis poster	We have removed the poster. In practice, many institutions considered it as the method of analysis prescribed by DNB. However, it was only intended as an overview, to provide guidance.		It is good to realise that while risk identification and risk analysis can be distinguished, they cannot (always) be properly separated. The stages can be completed sequentially but often also simultaneously. For example, an institution may take the view that working out the risks should be done in the risk identification stage rather than in the risk analysis stage. We believe the specific stage in which this is done is of minor importance.
		Using scenarios	With regard to using scenarios, more emphasis is now placed on the need to develop detailed scenarios that are tailored to the institution. This puts the institution in a better position to define and set effective controls.
		Using data analysis	The new SIRA Good Practices document puts more emphasis on the fact that data analysis can, dependent on the products and services provided, be of added value when preparing a SIRA.

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+31 (0) 20 524 91 11
dnb.nl/en

Follow us on:

 Instagram
 LinkedIn
 X

DeNederlandscheBank

EUROSYSTEM