Good practice document on integrity risk appetite

DeNederlandscheBank

EUROSYSTEEM

Contents

Introduction

Over the past years, we have explicitly drawn attention to the need for high-quality systematic integrity risk analyses (SIRAs) as the groundwork for robust risk management. It is a vital element of the risk management cycle that financial institutions make deliberate choices on an ongoing basis about integrity risks such as money laundering, terrorist financing and corruption, asking themselves which risks they are prepared to accept, and which must be avoided or mitigated by implementing controls. Your institution will be best equipped to make such choices if you have formulated an unambiguous integrity risk appetite. By calling on institutions to devote attention to this, we are acting in line with the FSB report 'Principles for An Effective Risk Appetite Framework' of 18 November 2013. Earlier, we drew attention to the financial risk appetite, in connection with our examination into the effectiveness of risk management at banks[1].

In this document, we provide more details about the integrity risk appetite, further to our findings from the exploratory examination into its practical application, which dates from 2016. Our aim was to establish the degree with which financial institutions had explicitly documented their risk appetite in the area of integrity risks and whether they actually made deliberate choices about dealing with the various integrity risks inherent in their business model and the conduct of their business operations. As announced in June 2016 and subsequent newsletters, our examination focused particularly on whether the SIRA's outcomes were assessed against the integrity risk appetite and on the involvement and roles of staff members and departments in drawing up that appetite.

It became apparent that many financial institutions were unable to describe how they explicitly document their integrity risk appetite or which role it could play in their organisations. This leaflet is meant to assist you in designing and putting into practice a robust integrity risk appetite. Also, we will address the topic of de-risking, which is one way in which a financial institution could deal with integrity risks. The Financial Action Task Force (FATF) defines de-risking as terminating or restricting business relationships with specific categories of customers due to unacceptable integrity risks, without performing individual risk assessments.

1 Read more about the examination in our Banking Supervision Newsletter.

1 SIRA as a basis for risk management

This section deals with role of a systematic integrity risk analysis (SIRA) in a financial institution's risk management process.

Sound and ethical operational management

Every financial institution must safeguard sound and ethical operational management, pursuant to the laws and regulations listed in section 4. For your operational management to be ethical, you must take measures aimed at preventing your institution or your staff from becoming involved in money laundering, terrorist financing, corruption and conflicts of interest, breaches of the law or other acts that are so contrary to generally accepted standards that they may harm confidence in your institution or the financial markets as a whole. Your institution's operational management must also be sound, meaning that it must be commensurate with the nature, size, risks and complexity of your institution's activities. Lastly, sound and ethical operational management requires that your financial institution uses the SIRA to identify risks and subsequently take appropriate measures to control them.

Without a SIRA, your institution is unable to safeguard adequate risk-based compliance with integrity legislation. Therefore, you must have sufficient knowledge of the inherent integrity risks to inform the assumptions you make to ensure adequate risk control. In August 2015, we issued our good practices brochure 'Integrity risk analysis – More where necessary, less where possible'. This provides financial institutions with guidance for setting up a SIRA step by step. The brochure also introduces the term 'integrity risk appetite'. It describes the SIRA as an assessment of inherent risks that is as objective as possible and that is decisive for risk control. The integrity risk appetite describes the integrity risks a financial institution is prepared to accept.

Ideally, you draw up your integrity risk appetite before performing the SIRA, determining in advance which risks you find acceptable after applying possible risk controls, as well as risks you do not wish to accept in the first place. In practice, formulating your integrity risk appetite will often be an iterative process, as you will make adjustments to your integrity risk appetite on an ongoing basis, for example due to changes in the relationships with customers or your institution's objectives, the availability of new risk controls, changed expectations on the part of external stakeholders or geopolitical developments. By reviewing the outcome of the SIRA against your integrity risk appetite, you continually determine whether your institution wishes to accept, limit or avoid the risks that emerge from the SIRA, subject to the statutory minimum requirements. Subsequently, you implement the required risk controls, based on the choice of risks you find acceptable. In addition, your institution may decide to discontinue specific activities because you do not wish to accept the relevant residual risks, meaning you choose to apply de-risking.

2 Designing the integrity risk appetite

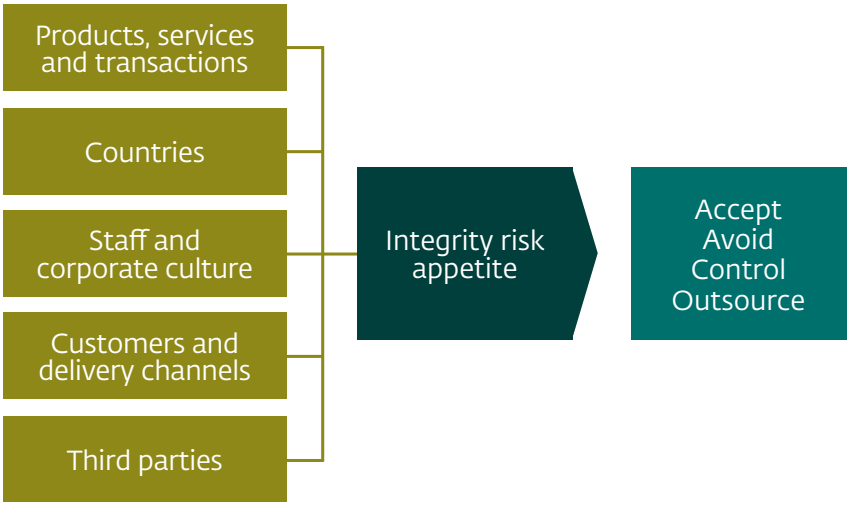
We believe it is important that you consider three aspects when you design your integrity risk appetite:

- the scope of the integrity risk appetite
- the responsibility of senior management for establishing, communicating and monitoring the integrity risk appetite
- embedding the integrity risk appetite into your institution's operations, and the allocation of roles between its lines of defence.

We will discuss these aspects in more detail below.

Scope of the integrity risk appetite

The integrity risk appetite preferably states, for each activity or product category, the relevant risk type and the corresponding risk appetite. These must be considered for a range of scenarios. Accordingly, all relevant disciplines in your institution's organisation must be involved. This diagram illustrates the use of an integrity risk appetite:



As noted earlier, adopting and updating the integrity risk appetite is an iterative process, meaning that it must be repeated at regular intervals and also whenever there is reason to do so.

Responsibilities of senior management

Your institution's senior management (specifically the members of its management board) bears final responsibility for the institution's risk profile. This means that it chooses to either accept, avoid, control or outsource specific risks. The Financial Stability Board has described the role and responsibilities of senior management, whose responsibilities include:

- ensuring that the integrity risk appetite is aligned with the financial institution's short-term and medium-term strategic objectives
- reviewing the integrity risk appetite against the financial institution's risk profile and arranging for independent audits of those reviews

- ensuring that the effectiveness of risk controls is tested and monitored, and taking measures in the event of activities outside the integrity risk appetite
- safeguarding the robust implementation of the integrity risk appetite throughout the organisation, and facilitating clear internal and external communications about the integrity risk appetite.

The latter aspect is a vital responsibility. Formulating the integrity risk appetite in the most concrete terms possible and raising sufficient awareness internally and externally helps you make the first step towards compliance.

Operational embedding

A financial institutions' integrity risk appetite has a bearing on all of its operational aspects, both in primary processes, such as lending and insurance, and in secondary processes, such as procurement and HR. Accordingly, when drafting process descriptions or procedures, your institution should consider whether there are risks of operating outside its integrity risk appetite. Below are several examples of how a financial institution's integrity risk appetite impacts its operations:

- A payment institution decided to implement additional risk controls for services to specific sectors which involved heightened integrity risks, prompted for example by our report on risks of money laundering in sports
- A pension fund chose to maintain investments in a specific high-risk country. To that end, it instructed the asset management firm to closely monitor specific risks associated with the high-risk country.
- A bank that would soon undergo major restructuring decided to implement additional risk controls relating to its corporate culture to prevent integrity breaches that might result from potentially reduced staff motivation or loyalty
- An insurer decided to cease offering insurance through specific agents, which helped control the risk of non-compliance with sanctions regulations
- A trust office decided that it would no longer accept involvement of third parties in facilitating specific transactions. It believed third-party involvement carried an unacceptably high risk of conflicts of interests

A further notable example is one we encountered during our examinations. A bank had identified heightened integrity risks in the areas of acceptance and monitoring involving a specific group of customers. The group was relatively limited in number, generating a small proportion of the bank's revenues and profits only. This made it unprofitable for the bank to design and implement risk controls specifically tailored to this group and perform individual risk assessments and mitigation to reduce the integrity risks to acceptable levels. At the same time, the bank felt it would be incorrect to terminate its relationship with this group.

It therefore decided to transfer its service provision for this group to a specialised team. This team used pre-existing processes and procedures of other departments which better safeguarded adequate monitoring of integrity risks. By serving a specific group of high-risk customers through a specialised team, the bank could continue providing its services within the limits of its integrity risk appetite.

Allocation of roles among the three lines of defence

Identifying risks and developing appropriate risk controls requires that you collect input from a range of organisational units, such as compliance, risk, audit, product development, policy and sales. You need the involvement of these entities to embed the policy adopted and ensure the procedures are actually put into practice. This is in line with Section 10(3) and (4) of the Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels Wft*) which requires financial institutions to inform all relevant organisational units of its policy and procedures and see to their implementation. In doing so, each line of defence has its own responsibility with respect to the integrity risk appetite.

The first line must formulate the integrity risk appetite specifically for its own organisational unit, while ensuring that it is in line with the integrity risk appetite of the financial institution overall. It provides sufficient substantiation, such as scenarios and data analysis. It also monitors whether the formulated integrity risk appetite is applied correctly. The second line, besides being involved in formulating the integrity risk appetite, is responsible for reviewing it against applicable laws and regulations, as well as for monitoring application of the integrity risk appetite in day-to-day operations, independently from the first line. The third line performs independent audits to provide assurance to senior management that all organisational units operate in accordance with the formulated integrity risk appetite.

3 De-risking

In conclusion, we will discuss de-risking. As noted earlier, this is a specific way of applying the integrity risk appetite which we also looked at during our examination into integrity risk appetite. In essence, de-risking is the result of a strictly applied integrity risk appetite. It means that a financial institution avoids risks by excluding or terminating relationships with entire groups of customers for integrity reasons, without performing individual risks assessments. The FATF likewise defines de-risking as 'terminating or restricting business relationships with categories of customers'.

We have examined the extent of de-risking in the Netherlands, for the following reasons. De-risking carries the risk of customers being unjustly excluded from financial service provision, while it also results in certain activities moving under the financial system's radar and being conducted through unregulated channels.

In our research, we have concluded that the exclusion of categories of customers for integrity reasons is not a large-scale phenomenon in the Netherlands. Where institutions deny a customer their services, freeze their service provision or terminate a customer relationship, they mostly do so based on an individual customer assessment. Although payment institutions, trust offices and, to a lesser extent, banks and money transaction offices use lists of unacceptable customers and activities, these are largely prompted by regulatory and legislative requirements, contractual obligations and reasons other than integrity risks alone. We continue to keep a close watch on developments in de-risking, both in the Dutch financial sector and internationally.

Our examination has revealed that the concept of a risk-based approach as referred to in laws and regulations is sometimes misunderstood. As explained in section 3.4 of the DNB Guidance on the Wwft and SW, if a heightened risk is inherent in a specific category of customers, your institution does not necessarily need to deny its services to the entire category of customers. You must assess on a case-by-case basis whether the integrity risks related to high-risk customers or activities can be mitigated. Termination or denial of service is only appropriate if a prospective or existing customer or activity is considered to be too risky.

Various financial institutions have commented that customers or prospective customers can help ensure that they are not rejected. For example, by being open and transparent in the course of the customer acceptance process, providing accurate and adequate information about activities pursued, and providing information about how they themselves (if applicable) perform customer due diligence, current and prospective customers allow institutions to better analyse the integrity and other risks associated with them.

4 Status of this document

Good practice document of De Nederlandsche Bank N.V., dated 28 September 2017, with guidelines for the integrity risk appetite (official title: 'Good practice document on integrity risk appetite')

Disclaimer

This good practice document provides non-binding recommendations for the application of rules regarding sound and ethical operational management, notably banks, pension funds, insurers, payment institutions and trust offices, referred to below as 'financial institutions'.

It sets out our expectations regarding observed or envisaged behaviour in policy practice that reflects an appropriate application of the rules to which this good practice document pertains.

We encourage financial institutions to take our expectations into account in their considerations and decision-making, without them being obliged to do so, while also taking into consideration their specific circumstances. The good practice document is only indicative in nature and therefore does not alter the fact that some financial institutions should apply the underlying regulations differently, and possibly more strictly. It is your institution's responsibility to take this into account.

Related legislation and regulations

This good practice document pertains to the following statutory provisions:

- Sections 3:10 and 3:17 of the Financial Supervision Act (*Wet op het financieel toezicht – Wft*), read in conjunction with Section 10 of the Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels Wft – Bpr*)
- Section 19 of the Pension Fund (Financial Assessment Framework) Decree (*Besluit financieel toetsingskader pensioenfondsen – Bftk*), read in conjunction with Section 14 of the Decree implementing the Pensions Act (*Besluit uitvoering Pensioenwet – BuP*)
- Section 10 of the Act on the Supervision of Trust Offices (*Wet toezicht trustkantoren – Wtt*), read in conjunction with Section 4 of the Regulation on sound operational management (*Regeling integere bedrijfsvoering Wtt – RIB Wtt*)

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
P.O. Box 98, 1000 AB Amsterdam
The Netherlands
+31(0)20 524 91 11
dnb.nl