Our redesigned supervison approach

DeNederlandscheBank

EUROSYSTEEM

Contents

1 Introduction

We are introducing a redesigned supervisory approach. Even more than before, we will deploy our available supervisory resources in those areas in which we identify the largest prudential and integrity risks. Our supervision will be more intense as these risks have a bigger impact on trust. The redesigned supervisory approach will be more data-driven than before and should ensure greater consistency in supervision.

In addition, our supervision will be more dynamic, as we seek to respond more rapidly to changes in institutions' risk profiles. Also, this means we keep more options open for making changes to our supervisory activities with respect to an institution over the course of a year, for example if changed risk ratings give us reason to do so.

This brochure describes the main features of our new approach, setting out how it works and how it will contribute to effective supervision. Thus we aim to provide transparency to the institutions we supervise and to other stakeholders.

2 Principles in our supervision

Supervisory resources and expertise are scarce. This means making choices is unavoidable. We do this by deploying our supervisory resources on a risk basis, allocating them to areas in which we identify the greatest prudential and integrity risks. Our supervision will be more intense as these risks have a bigger impact on trust.

In prioritising risks, we use the outside-in principle, so that developments in the outside world are the starting point. To identify priorities, we first identify the risks to which supervised institutions are exposed, also establishing a link with macro-prudential developments and risks that could have an impact on the sector. We refer to this link as the micro-macro link. We then convert these risks bottom-up into supervisory priorities for the period ahead. These priorities also inform our supervisory plans.

We use proportionality as an important principle in the performance of our tasks. We devote our resources to an institution pro rata to its size and complexity and to the risk to which it, or the financial sector as a whole, is exposed. While proportionality can make our supervision of small, less complex institutions more straightforward, it will not necessarily be less stringent.

Where possible, our approach is data-driven and automated to ensure effective and consistent supervision. Applying automated ratings and obliging supervisors to justify any deviations from those ratings promotes consistency and mutual comparability. Furthermore, automation allows us to supervise institutions in the lowest impact class individually without it taking up a disproportionate amount of our resources.

3 Core elements of our supervisory approach

3.1 Our supervisory approach in outline

In outline, our approach is structured around the following three core elements (see also Figure 1):

1. Each year, before we conduct risk analyses, we classify institutions into impact classes. Each impact class has its own intensity of supervision (see Box 1). The impact classes result from the Risk Tolerance in Supervision Statement. This statement centres around the principle that the aim of our supervision is to reduce the likelihood and impact of an institution's failure rather than to prevent such failure at all times.
2. The basic programme reflects the starting level of our supervisory activities and involvement. We always follow this programme for institutions in the 'basic' impact classes (classes I1, I2 and I3). The basic programme's purpose is to identify and establish an institution's risk profile.
3. The risk-based programme includes our supervisory activities that are aimed at drilling down and mitigating. Drilling down means investigating risks identified in the basic programme in further detail, while mitigating aims to ensure that an institution's excessive risk ratings are lowered so they conform to our supervisory risk tolerance.

3.2 Risk Tolerance in Supervision Statement

Our supervisory resources being scarce, we make choices in performing our supervisory tasks. Our guiding principle is that we deploy those resources effectively to address the risks that have an impact on the stability and reliability of individual institutions and the financial system as a whole. In this way, we put our mission of working on trust into practice.[1]

To safeguard the reliability of the financial system, we are committed to sound financial institutions capable of meeting their obligations (prudential supervision) and ethical financial institutions that behave in accordance with laws, regulations and the standards of social propriety (integrity supervision).

It is important that institutions honour commitments to their customers. While our supervision reduces the likelihood of an institution ending up in difficulties, it provides no guarantee. This is reflected in the Risk Tolerance in Supervision Statement (See Box 1). This statement informs all components of the method, including the choices we make in deploying our resources, which in turn form the rationale for the intensity of our supervision.

3.3 Impact classes

Each year, before we conduct risk analyses, we classify institutions into impact classes. The more soundness or integrity issues in a supervised institution impact trust in the financial system, the higher the impact class in which we classify that institution. We do not take account of the *likelihood* of problems occurring in an institution in our impact classification.

1 Viewed from a legal perspective, in tandem with the Dutch Authority for the Financial Markets (AFM), we monitor and enforce compliance with the Financial Supervision Act (*Wet op het financieel toezicht – Wft*), the Pensions Act (*Pensioenwet – Pw*), the Mandatory Occupational Pension Scheme Act (*Wet verplichte beroepspensioenregeling – Wvb*), the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft*), the Act on the Supervision of Trust Offices (*Wet toezicht trustkantoren – Wtt*), the 1977 Sanctions Act (*Sanctiewet 1977 – Sw*) and all ensuing rules and regulations.

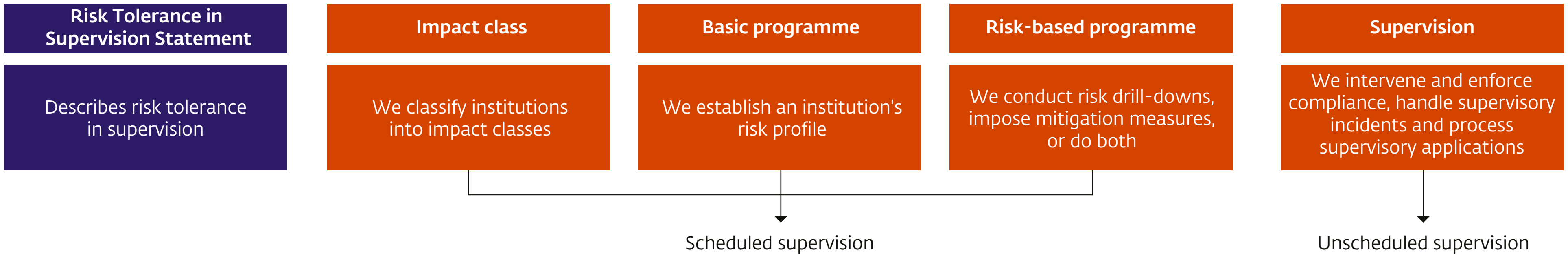
Box 1 Risk Tolerance in Supervision Statement

Through our supervision, we contribute to the public interest by ensuring a stable and reliable financial system, in which sound financial institutions provide their services in an ethical manner. We do so by conducting fit and proper assessments of senior executives, issuing licenses and monitoring that financial institutions prevent involvement in financial crime. We also assess whether institutions are financially sound and whether they can meet their obligations, even when faced with economic downturns. Crucially, we aim to be transparent about the choices we make whenever possible. We aim to be open about our risk tolerance and our approach as a supervisory authority.

A stable and reliable financial system benefits from public trust in financial institutions meeting their obligations and acting with integrity. We deploy our available resources in those areas in which we identify the biggest prudential and integration risks. Our supervision will be more intense as these risks have a bigger impact on trust. This effect is determined by the scale of a financial institution's operations, the extent to which risks spread throughout the financial system, and the institution's function in society. The latter aspect applies even more to financial institutions whose services provide income security, with commitments that must be honoured in the more distant future.

We acknowledge that institutions can fail. But as a supervisory authority, we do not tolerate insufficient management of prudential and integrity risks by financial institutions. As gatekeepers, financial institutions have an obligation towards society to prevent involvement in financial crime. Non-compliance with this statutory task can have consequences under criminal law. However, adequately managing prudential and integrity risks will not guarantee that an institution's failure can be prevented in every single case. Accordingly, we stress that the aim of our supervision is to reduce the likelihood and impact of an institution's failure rather than to prevent such failure at all times. We are well aware that the failure of a financial institution could jeopardise the stability of the financial system as a whole, which in turn could spark concerns over the reliability of the financial system. This is why our risk tolerance of a financial institution failing decreases as its impact on the financial system and society increases. As a resolution authority, we work alongside European peers where needed to prepare resolution plans for financial institutions.

Figure 1



Given the various applicable statutory frameworks, we distinguish between prudential and integrity impact classes. Depending on their size, we classify institutions into impact class I1, I2 or I3. In addition, there are two exceptional impact classes, which are 1X and 3F. We classify institutions and operations into impact class 1X if our supervisory powers are limited.[2]

Classification into a prudential impact class depends for instance on the scope of the institution's operations, its national systemic relevance and the function of its operations in society. Classification into an integrity impact class depends on the importance of the institution's gatekeeper function and the risk of financial loss or damage or reputational damage in the event of integrity failure.

To ensure that institutions are always classified into the appropriate category, we update the classification annually. Also, we always assess whether an institution must be reclassified after it has applied for an amendment to its licence or has undergone any other change, such as strong growth.

Table 1 illustrates how the previously formulated risk tolerance is expressed in impact classes. The higher the impact class and, hence, the greater the impact of potential risks on trust, the further risk tolerance decreases and our supervision becomes more intense. It must be noted, however, that the deployment of our resources in each impact class set out in Table 1 may not exactly reflect the Risk Tolerance in Supervision Statement in every single situation.

2 This impact class also includes single-person pension funds, savings funds and pension funds that are in liquidation and have reported a group transfer of accrued benefits.

Table 1 Relation between Risk Tolerance in Supervision Statement and impact classes

	Impact on trust	Risk tolerance of failure[3]	Supervision effort
Impact class 1	Low	We accept the likelihood of failure	**Adaptive supervision** ■ We recognise that this approach allows risks to go unnoticed. ■ We only get in touch with an institution if we have reason to do so. ■ Mitigation measures in the event of heightened risk are more limited in duration and scope compared with institutions in impact classes I2 and I3.
Impact class 2	Medium	We accept the likelihood of failure to a small extent	**Active supervision** ■ To a small extent, we accept the likelihood of risks going unnoticed, because they do not appear from the available data. ■ We get in touch with an institution on a regular basis to identify risks, even if its reports give us no reason to do so. ■ The duration and scope of drill-down examinations and mitigation measures in the event of heightened risk is more extensive than for institutions in impact class I1.
Impact class 3	High	We accept the likelihood of failure to a very small extent	**Proactive supervision** ■ To a very small extent, we accept the likelihood of not noticing risks. ■ We supervise the institution intensely to identify less obvious risks. ■ We take immediate action if risks are heightened using potentially labour-intensive instruments.

3 Our tolerance of failure may differ if there is a systemic risk whereby several institutions are simultaneously at risk of failure.

Table 1 illustrates how the impact classes generally affects the deployment of our supervisory resources. This method acknowledges that some institutions require a great deal of prudential supervision effort while we have assigned them a lower priority in terms of integrity supervision. The reverse is also true when we assign them a higher priority in terms of integrity supervision, while they require less of a prudential supervision effort. Naturally, there are also institutions that require an equal effort from both perspectives.

The intensity of our supervision also increases, in addition to the mechanism shown in Table 1, if an institution's risk profile so warrants. In that case, our supervisory intensity will be related to the institution's risk profile, and to a lesser extent to its impact class. This situation is described in section 3.5 below.

3.4 Basic programme

Each impact class has its own basic programme in terms of supervisory activities and involvement. The basic programme's purpose is to identify and establish an institution's risk profile. It uses the same method for all supervised institutions to promote consistency and mutual comparability.

A basic level of supervision applies to all institutions, which is, however, not identical for each impact class. Supervision must be tailored to a financial institution's size and complexity and, most of all, the risks to which it is exposed (proportional supervision). Accordingly, the basic programme has a smaller scope for an institution in a lower impact class. We will increase the intensity of our supervision whenever the institution appears to be exposed to risks outside the risk tolerance of our supervision. We will then perform additional supervisory activities under the risk-based programme (see section 3.5 below).

3.4.1 Risk taxonomy

The risk taxonomy is the basis for establishing an institution's risk profile. We have identified five risk areas and broken these down into 17 risk components (see Figure 2).[4] We aim to use this as a basis for clear and logical communications with an institution about its risk profile. Where possible, we translate macro-risks, sector risks and new risks into risk ratings for the risk components they impact.

Our supervision method distinguishes between risk level and risk management.

a. Risk levels refer to the magnitude of risk to which an institution is exposed with a view to the internal and external environments in which it operates and the mitigation measures it has taken.
b. Risk management refers to the measures an institution has taken to manage its risks. Our assessment of an institution's risk management is initially aimed at verifying whether the design, existence and effective operation of its risk controls meet the prevailing supervisory standards. In addition, we verify whether its risk management framework matches the risk level and complexity.

For each risk component we compute both an automatic risk level rating and an automatic risk management rating, with the following two exceptions. We only compute automatic risk level ratings for the two risk components in the "business model and strategy" risk area. We only compute an automatic risk management

4 A supervisor may choose not to rate and establish a specific risk component, subject to adequate justification, if that component is not or only to a very limited extent relevant to an institution.

Figure 2 Risk taxonomy under the basic programme

	Overall rating				
Risk areas	**Business model and strategy**	**Governance, behaviour and culture, and risk management**	**Integrity**	**Prudential risks**	**Capital**
Risk components	1. Viability of business model 2. Viability of strategy	1. Internal governance 2. Behaviour and culture 3. Risk management	1. Money laundering 2. Terrorist financing 3. Sanctions regulations 4. Corruption 5. Socially unacceptable behaviour	1. Credit risk 2. Market risk 3. Interest rate risk 4. Operational risk 5. Liquidity risk 6. Underwriting risk	1. Capital position

rating for the "risk management"[5] component in the "governance, behaviour and culture, and risk management" risk area.

We rate and assess the 17 risk components according to a fixed pattern. The process consists of four distinct phases. They are illustrated in Figure 3, and we will describe them in detail below.

1. The first phase consists of collecting the information we need to compute automatic risk ratings. This information comprises the data which institutions provide periodically and in a standardised manner – such as regular financial reports – and questionnaires which institutions or supervisors have completed, and external data sources. In addition, the supervisor can use sector-wide analyses in the basic programme. The depth and amount of information obtained may vary according to impact class, but there is always a minimum amount of information we collect, taking account of the sector in which an institution operates.

5 Risk management assessment involves a general assessment of the institution's operational and organisational structure, overall risk management framework and technical architecture supporting the risk management framework and practice. We assess the following three principal aspects of risk management: (i) the institution's internal governance framework, (ii) its risk management framework and risk culture, and (iii) its risk infrastructure, internal data and reports. Risk management provides a broad perspective for assessing an institution's overall organisational competence and capacity. This does not include the detailed assessment of the risk controls related to the specific risk components in the integrity, prudential risks and capital risk areas. We assess risk management for each of these risk components separately. This definition of risk management assessment is in line with that used by the Single Supervisory Mechanism (SSM).

Figure 3 Four phases for rating and assessing the risk components

2. We generate the automatic risk level ratings from the current values of the predefined quantitative indicators for each risk component. We then compare the indicators with the prescribed limits and criteria, aggregating them to produce a risk level rating. This promotes consistency and comparability in risk level rating. We use different rating methods to compute the automatic risk control ratings, such as rating models based on quantitative indicators and compliance checks based on a questionnaire.
   After we have computed automatic risk level and risk control ratings for each risk component, a supervisor assesses these ratings on a regular basis. The supervisor has the option of modifying the risk picture that emerges from automatic ratings. The assessment takes place in two consecutive steps.
3. To assess automatic risk level and risk management ratings, the supervisor relies on the available information, such as periodic reports, audit reports and the information from our drill-down risk analyses under the current year's or previous years' risk-based programmes. We can also obtain additional information from policy reports and internal reports drawn up by supervised institutions. In some cases, we may need to speak with the institution's management. The depth and frequency of our information collection efforts will increase as the impact class is higher. In the case of institutions in the lowest impact class, we will rely more heavily on the automated ratings than for those in the highest impact class.
4. Based on the previous step, the supervisor assesses the ratings. To ensure consistent supervision, it is important that deviations from the automatic rating are possible only when properly justified.

We arrive at a rating for each risk component by combining their risk level and risk management ratings using a fixed formula.

3.4.2 Establishing a risk profile

In addition to assessing the automatic ratings for each risk component from time to time, we also establish the risk profile periodically. Such an overall rating encompasses all the risks to which an institution is exposed, and its purpose is to determine the intensity of our supervisory activities. This is important because most of the risks interact, while the different types of supervisory measures are also interrelated. This is important to realise in relation to larger and more complex institutions, as the holistic picture of the risk profile may be different from the sum of the different risk components. We establish overall ratings separately for integrity and prudential supervision purposes.
We incorporate the outcomes of the basic programme into the supervision plan, supplemented by any follow-up actions under the risk-based programme (see section 3.5 below). In addition, we discuss the outcomes and the supervision calendar

with institutions in impact classes I2 and I3. We inform institutions in impact class I1 of the outcomes, but do not generally schedule a meeting.

3.5 Risk-based programme

The risk-based programme includes our supervisory activities that are aimed at drilling down and mitigating. Drilling down means investigating risks identified in the basic programme in further detail, while mitigating aims to ensure that an institution's excessive risk ratings are lowered so they conform to our supervisory risk tolerance. Depending on the nature and scope of the risk, non-compliant behaviour[6], or both, we may decide to intervene and enforce compliance as part of the mitigation process.

We may have various reasons to launch a risk-based programme. Firstly, the risk component ratings under the basic programme may give us reason to do so. Secondly, unexpected developments, supervisory incidents, or both, which we had not yet factored into the risk component ratings, may trigger the programme's launch. Lastly, sector-wide or system-wide macro developments which we had not yet factored into the risk component ratings, may warrant activation of the programme.

The supervisor's judgement is leading in selecting drill-down and mitigation activities that must be undertaken. To promote the effective and efficient deployment or our scarce supervision resources, the risk-based programme indicates which drill-down or mitigation activity we must initially undertake for a certain impact class or risk rating. The guiding principle is that we only use a heavier instrument if we have established that a lighter instrument is insufficiently effective. In a low impact class, in line with the risk tolerance in supervision, our drill-down and mitigation activities are more limited in terms of their scope and duration.

Annex 1 lists various instruments that can be used in the risk-based programme. As a rule, if institutions have the same risk component ratings, we use our supervisory drill-down instruments more intensely if they are in a higher impact class. By contrast, we can use any mitigating supervisory instrument in the highest risk component rating, irrespective of the impact class.

6 Non-complaint behaviour, such as inadequate risk management, increases risks, potentially threatening an institution's solidity, integrity, or both. To mitigate the risks, we may decide to intervene and enforce compliance as part of the mitigation process.

Annex 1 Examples of supervisory instruments in our regular and non-regular supervision

Basic programme	
Supervision plan	Establishing and communicating a supervision plan for a supervised institution. This includes, where relevant, communication with the institution about the supervision plan.
Data requests	Requesting regular and other supervisory data from institutions, and improving data quality. This does not include assessing these data to verify an individual institution's compliance with requirements and agreements.
Risk profile	Preparing and challenging manual and automatic risk ratings, where necessary reviewing them based on the supervisor's judgement.
Regular supervisory meetings	Holding regular meetings with institutions, regardless of risks identified. They do not include meetings held in the context of other activities, such as supervisory planning.
Qualitative reports assessment	Assessing qualitative reports submitted by individual institutions, including risk management reports, compliance reports, internal audit reports, ORSA/ERB/ICAAP/ILAAP and minutes of management and supervisory board meetings.
Quantitative report assessment	Assessing quantitative reporting submitted by individual institutions, including quarterly financial reports.
Recovery and resolution plan assessment	Assessing recovery and resolution plans submitting by individual institutions.
Capital or liquidity decision	Adopting a capital or liquidity decision following the assessment of qualitative or quantitative reports, for example as part of the Supervisory Review and Evaluation Process.
Internal/external coordination of our supervisory approach	Coordinating the supervisory approach for specific institutions, including within DNB's Prudential Supervision Council, the European Central Bank's Supervisory Board, colleges or crisis management groups. This includes preparatory work, briefings and coordination directly related to these fora.
Sector-wide analysis	Preparing and assessing analyses on a specific subject or risk area that cover multiple supervised institutions.

Risk identification drill-downs under the risk-based programme	
Risk-identification meetings	Holding exploratory meetings with an institution, in addition to regular meetings under the basic programme, aimed at obtaining a clearer picture of one or more specific risks. They may include meetings with the institution's external auditor or consultants, or both.
Deep dives	Conducting an in-depth desktop examination into a specific institution to analyse a particular risk in more detail.
Thematic examinations/sector-wide analyses	Conducting an examination at multiple institutions, focusing on a specific theme in response to a change in their external environment or the need to analyse a specific risk in more detail.
On-site inspections	Performing supervisory drill-down inspections at one or more institutions, focusing on specific topics or themes.
Stress test	Conducting scenario analyses to test an individual institution's robustness in certain respects in stress situations.
Sharing sector-specific expertise	Providing information to and training staff of DNB or peer supervisory authorities on specific risks or areas of risk.

Mitigation under the risk-based programme	
Mitigation meetings and letters	Holding meetings or sending letters to an individual institution with the aim of mitigating one or more of the identified risks.
Seminars and roundtables	Interacting with one or more specific institutions on the basis of identified areas of concern or risks, with the aim of achieving behavioural change by talking to them about the supervisory approach related to those risks or areas of concern.
Risk mitigation plans	Drawing up a plan to mitigate one or more of the identified risks at a specific institution – with the aim of achieving a measurable outcome – and implementing the planned activities and monitoring progress. If the risk to be mitigated is material and there is a reasonable likelihood of an enforcement measure being called for, we may consider intervention or enforcement.

Intervention and enforcement	
Intervention strategy	Defining, preparing and implementing the intervention strategy, including the deployment of enforcement measures, to address and mitigate the specific worrisome situation or non-compliant behaviour
Formal enforcement measures	■ Issuing an instruction prescribing a specific course of action ■ Appointing a caretaker or special administrator ■ Issuing an order subject to penalty ■ Imposing a fine ■ Reassessing a managing or supervisory board member or other policymaker or officer ■ Revoking a licence
Informal enforcement measures	■ Holding a compliance briefing ■ Issuing a written warning