Integrity risk analysis

More where necessary, less where possible

DeNederlandscheBank

EUROSYSTEEM

Integrity risk analysis

More where necessary, less where possible

Good practices document and poster

Summary

This document sets out the steps that financial institutions[1] must take in order to develop an effective integrity risk analysis. Not only is an integrity risk analysis required by law, without it institutions are unable to achieve risk-based compliance with integrity legislation. An integrity risk analysis is also a precondition for the adequate development of ethical and sound business operations. Risk management will not have a clear focus if institutions have insufficient knowledge of possible integrity risks, or make unfounded assumptions about them.

This document explains why your institution should make an integrity risk analysis, how you should do this, and which consequences must be attached to the analysis. The document includes a poster with a summary of the different steps that you should take and the questions that you should ask yourself when making the analysis.

First of all, the areas where your institution may run integrity risks must be identified. You should consider the entire organisation. For each integrity risk, identify the factors playing a role and the likely scenarios, which you then score on likelihood and impact. After determining the nature and size of these gross risks, you must verify whether they are within the boundaries of your risk appetite.

Subsequently, you should assess for each gross risk, which control measures you have in place and whether these measures are effective. Based on the overview of gross risks and the assessment of the control measures in place, a list of net risks must be compiled. Here too, you should verify whether these risks are within the boundaries of your institution's risk appetite and if not, decide how to avoid or mitigate them. If your risk analysis shows that control measures need to be improved, you should also specify this in an overview and include a time schedule for mitigating actions.

The ultimate goal of integrity risk analysis is to serve as a steering document for the management board and to provide a clear overview of risks for the business.

1 By financial institution we mean banks, insurance companies, payment institutions, exchange institutions, trust offices and pension funds.

Contents

Introduction

Do you know where your institution is exposed to integrity risks?

The headlines increasingly reflect the dramatic impact that integrity incidents can have on institutions. Integrity risks are more significant than they used to be. Not only do they have grave consequences for your institution's reputation, but increasingly their financial impact is devastating. You may fall victim to financial-economic crime, or you may be an unwitting partner to criminal actions. This means that you may be called to account by DNB, other supervisory authorities or investigative authorities; executive directors or staff of financial institutions find themselves in the dock more and more often.

Financial institutions and pension funds play an important social role as gatekeepers of an ethical and sound financial sector. They combat criminality by making their systems as inaccessible as possible to criminals and cooperating with the detection authorities.

But how far does your knowledge of integrity risks actually go? Where are integrity risks likely to emerge at your bank, insurance company, payment institution, exchange institution, trust office, or pension fund and how may these risks manifest themselves? And once you know their source, do you also know their nature and size? And have you done enough to control them or (even better) to prevent them? In short, ethical and sound business operations begin by keeping an up-to-date view of the nature and size of the risks that you are exposed to when you engage in or facilitate financial-economic crime, whether you do this knowingly or not. After assessing over 170 integrity risk analyses, DNB found over 80% of these analyses to be deficient. In addition, there are many institutions that do not have an integrity risk analyses at all. DNB finds it very worrying that this crucial part of operational management is deficient at so many institutions and has consequently decided to provide this good practices document.

In order to guarantee that institutions ensure ethical and sound business operations, the legislator has included different requirements in financial legislation that your institution is obliged to comply with. Systematic identification and analysis of integrity risks plays a key role.

Statutory framework

Pursuant to Section 10 of the Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels Wft*) banks, insurance companies, payment institutions, electronic money institutions, exchange institutions or branch offices must ensure systematic analysis of integrity risks. Integrity risks are defined here as the "threat to the reputation of, or the current or future threat to the capital or the results of a financial institution due to insufficient compliance with the rules that are in force under or pursuant to the law."

Section 4 of the Regulation on Sound Operational Management relating to the Act on the Supervision of Trust Offices 2014 (*Regeling integere bedrijfsvoering Wet toezicht trustkantoren 2014*) stipulates that trust offices must perform regular analyses of their inherent integrity risks. Sound operational management entails giving guidance to the organisation and developing processes to control integrity risks. Integrity risks embody the risk of insufficient compliance with the law and the risk of involvement of trust offices or their staff in acts that conflict with commonly accepted practices to such an extent that they may cause serious damage to confidence in that trust office or in the financial markets.

Pursuant to Section 19 of the Pension Fund (Financial Assessment Framework) Decree (*Besluit financieel toetsingskader pensioenfondsen*), pension funds must ensure systematic analysis of integrity risks. And pursuant to Section 14 of the Decree on the implementation of the Pensions Act (*Besluit uitvoering Pensioenwet*), pension funds must make systematic analyses of the risks attached to outsourcing of activities at the level of the organisation as a whole, and at the level of its separate business units.

Unwarranted confidence in procedures and measures

Many institutions have manuals as thick as bricks and measures in place to secure ethical conduct by and within their organisations. The law also demands a plethora of procedures and measures, which may create the illusion of control. In fact, procedures only provide you with a semblance of risk management, especially if you do not base them on and direct them at actual risks. You can only use procedures and measures adequately if you truly understand the nature and manifestation of these risks. Without a good grasp of the nature and size of these risks, there is a real danger of a 'tick box attitude' when complying with the procedures.

Compliance without conviction or understanding is a risk in itself. Partly due to this, a large proportion of the regulations is risk-based: the procedures prescribed by law must be complied with, but the manner in which and the intensity with which depend on the size of the risk. So in some cases this offers you the opportunity to limit procedures and achieve cost advantages, but in other cases you will be required to take more stringent measures.

Examples of less where possible and more where necessary

Types of customers and services with potentially lower risks

- Listed companies subject to specific transparency requirements
- Public administrations or enterprises
- Life insurance policies with low premiums
- Pension insurance policies without surrender clauses that cannot be used as collateral
- Financial products or services intended to increase financial inclusion
- Products with low purse limits (e.g. specific types of electronic money)

Types of customers and services with potentially higher risks

- Businesses that are cash intensive
- Legal persons or arrangements that are personal asset-holding vehicles
- Private Banking
- Products or transactions that favour anonymity
- Non-face-to-face business relationships or transactions
- Payments received from unknown or unrelated third parties
- New products and new business practices such as new delivery mechanisms
- The use of new technologies or developing technologies for both new and existing products

What do we mean exactly by systematic identification and analysis?

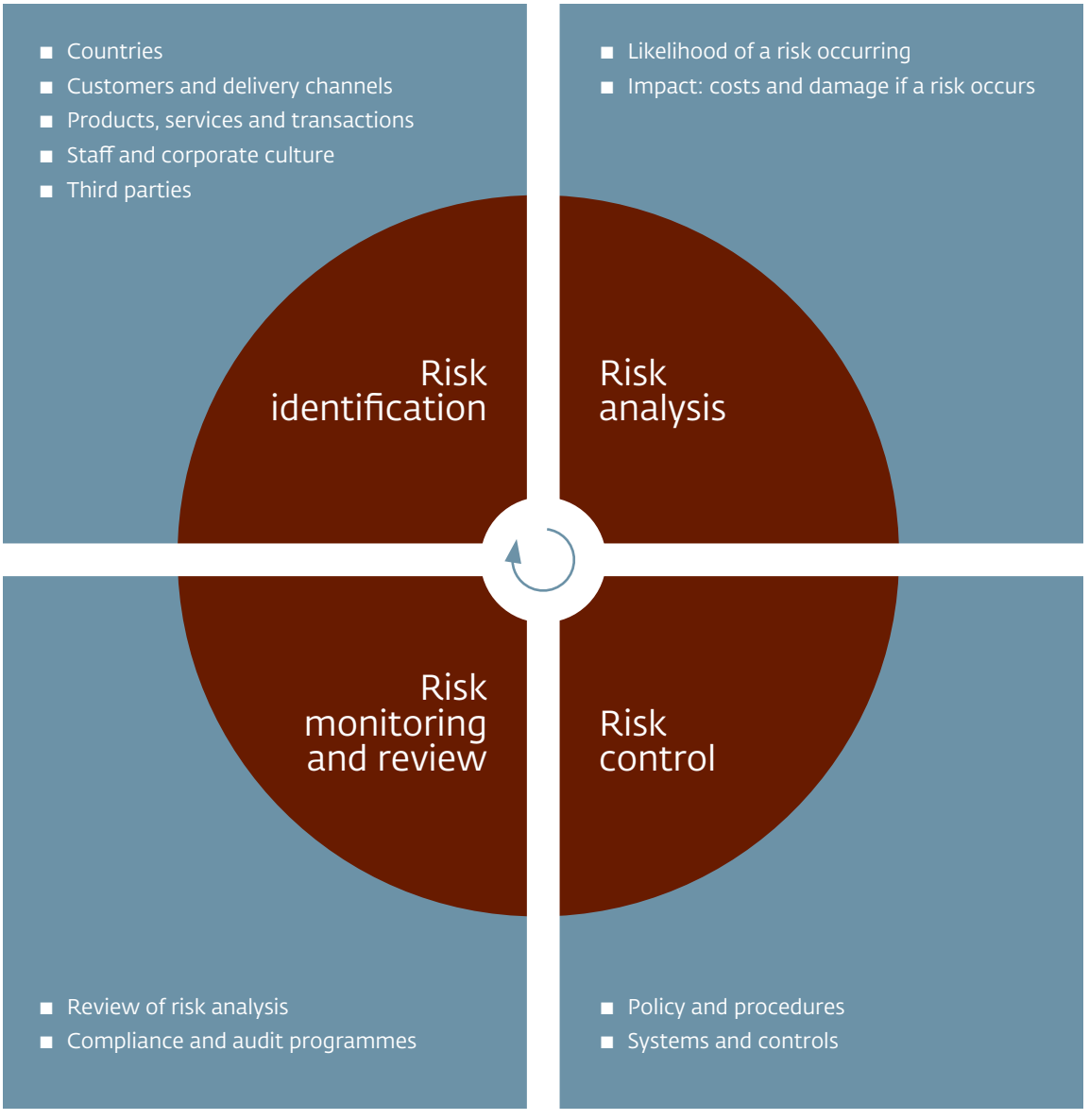
'Look before you leap' is the golden rule here. Before implementing or revamping procedures and measures, you must first thoroughly examine the nature (manifestations, scenarios of financial-economic crime) and size of the associated risks. This is done in two phases.

1. Identify possible risks.
2. Analyse and determine the nature and size of these risks.

Then follows the tailoring of the control framework: fleshing out policies, measures and procedures.

The law and the supervisory authorities demand a systematic approach to risk management. Systematic also means that this is a cyclical process, which means that you are required to perform the whole cycle of identification, analysis and testing of the effectiveness of controls at regular intervals. This is because risks are not static. Risks to institutions may change as a result of both internal and external factors. Your 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. This document provides you with instruments for the risk identification and the risk analysis phase, ranging from making preparations to deciding on the measures to be taken.

Identification and analysis are systematic as you perform them periodically (and in case of trigger events) and because this is a cyclical process of identification followed by analysis and control. The outcome of this process is the net risk; the size of risk that remains after all procedures and measures have done their work. The question then is to what extent the remaining net risk is acceptable to you and is within your risk appetite.


Countries
Customers and delivery channels
Products, services and transactions
Staff and corporate culture
Third parties
Risk identification
Likelihood of a risk occurring
Impact: costs and damage if a risk occurs
Risk analysis
Risk monitoring and review
Review of risk analysis
Compliance and audit programmes
Risk control
Policy and procedures
Systems and controls

Integrity risk analysis: mandatory, but essential above all

Systematic risk analysis will provide you with essential information about the activities of the different departments in your organisation. These reports will form the basis for your integrity policies that must be reviewed at regular intervals. Most of all, the outcome of the risk analysis serves as a steering document for management. It sets the organisation into action and prompts it to take adequate measures to actually control the risks. The results of the risk analysis also play an important role for Compliance and Audit. They use the results for their gap analyses and in developing annual plans and performing audits. Compliance and other second-line functions also play an important advisory role in the development of integrity policies. As communication and training are key processes in risk control, the responsible departments will at least also have to take note of the outcome of the risk analyses. After all, these reports are of such essential importance that the institution's supervisory bodies (supervisory board, supervisory committee) must be informed about them.

The EU Anti-Money Laundering Directive

The EU Anti-Money Laundering Directive also states that risk analysis is essential. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, stipulates the use of a comprehensive and risk-based approach. This is because the risk of money laundering and terrorist financing is not the same in every case. This risk-based approach is not an unduly permissive option, but it involves the use of evidence-based decision-making. This provides for a more efficient approach to target the risks of money laundering and terrorist financing that face financial institutions.

Article 8 of the Directive stipulates that institutions must take appropriate steps to identify and assess the risks of money laundering and terrorist financing. They are required to take into account risk factors relating to their customers, countries or geographical areas, products, services, transactions, and delivery channels. These steps are proportionate to the nature and size of the institution. The risk assessments are documented, kept up-to-date, and made available to the supervisory authorities.

The annexes to the Directive include lists of factors and types of evidence of potentially higher and lower risk.

Pointers for integrity risk analysis

Who performs the integrity risk analyses?

Systematic risk analysis is often incorrectly viewed as an issue mainly for Compliance. Management, Compliance, Risk Management and the business should work together on performing the integrity risk analyses. Primarily, responsibility for the quality and execution of the integrity risk analyses lies with the first line. This is the business, as risks manifest themselves first there. The role of Compliance is process monitoring, facilitating and testing. Other departments such as Security and Audit can also provide the necessary input. The ultimate responsibility for the integrity risk analysis lies with the management board.

Many institutions use the support of external experts in the fields of integrity, fraud, financial-economic crime or risk management. In the end, the ownership of risk identification and analysis, including the decision-making, lies with the first responsible person or department.
This responsibility is mostly assigned to the business or to risk management. Pension funds often have their risk analyses performed by their business operations office, or even by pension administrators. As said, the responsibility lies with the management board, which must consequently play an active and initiating role. This is only logical, as the majority of procedures and measures must be implemented by the first line.

Good practices

An institution forms dedicated working groups for each business unit. These working groups discuss the likelihood of integrity risks occurring, for instance with respect to money laundering or corruption. They assess among others the likelihood of customers using the institution for money laundering by means of specific money laundering scenarios, the likelihood of conflicts of interests arising between staff and customers, or the use of specific products or activities in specific countries in order to circumvent international sanctions. These sessions are supported by Compliance.

Using a predetermined scoring model, Compliance then evaluates together with Risk Management how the institution would be impacted if a certain scenario materialises. After these sessions, a matrix of likelihood and impact of gross risks is produced, and Compliance and Audit subsequently determine the level of controls for the different scenarios. The matrix of gross risks and control measures provides the institution with a list of net risks and deficiencies in controls.

This is then discussed in detail with the management board, which verifies whether the gross and net risks identified are within the boundaries of the institution's risk appetite. The management board then decides whether these risks should be reduced or prevented and which additional measures are necessary.

Which integrity risks are at stake?

Integrity risks are defined as non-ethical behaviour of staff and executive directors of institutions and non-ethical behaviour of third parties (customers, suppliers, advisers) that can be attributed to the institution, or in which the institution plays a punishable role. The most noticeable non-ethical behaviour is characterised by acts qualifying as criminal offences under the Criminal Code or economic regulations: money laundering is one of the better known integrity risks. Less well-known are varieties of money laundering such as laundering due to negligence, insider trading, financing of terrorism, circumvention of economic and financial sanctions, fraud, embezzlement, forgery, bribery, and the appearance of conflicting interest. These are only a couple of examples. Integrity risks may also include breach of or acting in conflict with the organisation's internal rules.

Breach of international rules and regulations is also considered to be an integrity risk. Take for instance the extra-territorial operation of the US sanctions and anti-corruption laws and the British anti-corruption laws.

Examples of integrity risks

- Money laundering
- Terrorist financing
- Circumvention of sanctions legislation
- Corruption (bribery)
- Conflicts of interests
- Fraud within or outside the organisation
- Evasion or avoidance of tax regulations
- Market manipulation
- Cybercrime
- Socially unacceptable behaviour

Integrity risk analysis Poster

This poster provides an overview of the steps an institution must take in drawing up an integrity risk analysis. It shows you how to chart the gross risks and analyse these for likelihood and impact, assess the effectiveness of the controls, determine the net risks and identify any gaps in the control measures. It contains helpful questions you can ask yourself in the process of making the analysis.
Please note that this poster is meant as a overview document and not as a standard form.

Integrity risk analysis

Step 1:
preparation and identification

- Business inventory: make an inventory for each business unit/branch office/subsidiary of the organisation with respect to products, customers, countries, staff, third parties, et cetera.
- Scenarios: assess which integrity risks may occur and the form that they may take.
- Scoring system: determine how to assess likelihood and impact

Step 2:
analysis

- Gross risks: for each scenario, determine the likelihood of the scenario occurring and the resulting impact.
- Risk appetite: assess the gross risk and verify whether this is within the boundaries of your risk appetite.
- Controls: list and assess the control measures in place for each scenario.

Identificatie			Analyse			
Risk	Factor	Scenario	Likelihood	Impact	Gross Risk	Risk appe
(Which integrity risks is the institution likely to face?)	(Which factors play a role for each risk?)	(How is the risk likely to manifest itself?)	(What is the likelihood of a particular scenario occurring?)	(What will be the impact on the institution if the scenario materialises?)	(Determine the inherent risk by assessing its likelihood and impact)	(Is the in risk with boundari risk appe
Money laundering						
Corruption (bribery)						
Tax fraud						
Circumvention of sanctions						
Terrorist financing						
Conflicts of interests						
Internal fraud						
External fraud						
Market manipulation						
Cybercrime						
Socially unacceptable behaviour						

Step 3:
assessment and measures required

- Nett risks: determine the net risk for each scenario by comparing gross risk and level of control.
- Risk Appetitie: determine whether net risk is within the boundaries of your risk appetite.
- Measures: determine the type of action to be taken, increase control or reduce risk.

			Beoordeling			
etite	Control measures	Assessment of control	Net risk	Risk appetite	Gap	Measures required
herent in the ies of the etite?)	(Which control measures are in place for each risk scenario?)	(How effective are these control measures?)	(Determine net risk by assessing gross risk and the relevant control measures in place)	(Is the net risk within the boundaries of the risk appetite?)	(Are there any deficiencies where measures are concerned?)	(Which measures are required in order to control or avoid this particular risk?)

What does an effective risk analysis look like?

Step 1: preparation and risk identification

Before embarking on the integrity risk analysis itself, a couple of preparatory steps must be taken. You need to draw up an overview of the organisation, make a list of possible scenarios for each integrity risk and determine how to assess likelihood and impact. The examples given here are general examples, which you will have to translate to the context of you own organisation.

Organisation overview – mapping

In order to perform an integrity analysis, you need an accurate picture of your organisation. This means that you will have to map out the different areas of your institution where integrity risks may occur. This entails making an up-to-date description of the nature and size of the company and the markets in which it operates. Larger institutions should also analyse their units and business lines. Subsidiaries and branch offices should also map out their own activities.

Different factors are important for each integrity risk. For the risk of money laundering the number and type of customers, the products provided to these customers, countries where these customers do business, receive transactions from and make payments to should be analysed. A risk analysis with respect to non-compliance with sanctions requires, in addition to the analysis of customers and countries, good knowledge of the type of goods traded by customers. In order to adequately analyse risks like corruption or conflicts of interests, you will for instance have to have knowledge of the number of staff members involved in insourcing of third parties, and the number and type of sponsoring contracts in place.

This organisation overview will provide you with an accurate picture of all factors exposing your organisation to risks.

Good practices

An institution makes a quantitative analysis per business unit of customers, products and supply channels for the purpose of a money laundering risk analysis.

- Customer analysis includes the maturity of the customer base, the complexity of customer structures, the number of politically-exposed persons (PEPs), a list of assets and the breakdown of customers across the different risk categories.
- With respect to different countries, the institution determines the number of transactions to and from high-risk countries, the number of customers operating in high-risk countries, and the countries where customers are active.
- Where products and transactions are concerned, the institution maps out the product groups and types of product for each department, and records whether products carry low, medium or high-risk. The number of customers involved in high-risk products and the number of cash transactions are also identified.
- For delivery channels, the number and percentages of customers served via direct channels, via account managers, and doing primarily online business with the institution are outlined.

Scenarios – types of risk

Every institution needs to know how integrity risks can manifest themselves. In other words, the different forms that financial-economic crime can take. You will have to stay informed of new forms of money laundering, ways of circumventing sanctions, new forms of fraud, and leeway for corruption.

These are forms of inherent or gross risks – the risks that exist if there are no control measures in place to mitigate them. It is an inventory of the threats that the organisation is exposed to.

It is important for institutions to keep abreast of the publications of the Financial Action Task Force, the European Union, the International Monetary Fund, the World Bank, Transparency International, national and international supervisory authorities, the Financial Intelligence Unit, and consultancy agencies.

Good practices

The institution works out several relevant scenarios for each integrity risk, describing how risks may manifest themselves through factors including customers, staff, third parties, products, services or countries.

Tax risks	■ Customers use complex and opaque structures ■ Staff members provide advice on opportunities for tax evasion ■ Customers have their registered offices in non-transparent jurisdictions
Money laundering	■ The origin of assets is unclear ■ Customers operate in a cash-intensive sector ■ Prepaid cards can be topped up with large amounts ■ The remuneration policy induces unwanted customer acceptance ■ Money flows from/to a politically-exposed person (PEP) in a high-risk country ■ Pay-outs made upon surrender of insurance policies go to others than the insured parties ■ Pay-outs on insurance policies are made to countries under sanctions or high-risk countries
Corruption/ conflicts of interest	■ Personal relationships between staff members and customers/third parties/ insourced staff ■ A small group of staff members working in a specialist field ■ The institution's internal corporate culture does not allow people holding each other to account ■ The culture prevailing in branch offices abroad fosters scope for conflicts of interests ■ Customers are active in real estate/ infrastructure/raw materials/energy sectors ■ Customers or institutions are active in politically unstable areas
Circumvention of sanctions	■ Customers do a lot of business with countries under sanctions ■ Customers trade goods that are subject to embargoes ■ The institution facilitates trade financing with parties in sanctioned countries ■ The institution itself is active in sanctioned countries
Internal fraud	■ There is no periodical internal screening ■ The institution does not use the four-eyes principle ■ Procedures are unclear

Scoring systems

The scenarios that you specified for each integrity risk must be scored on likelihood and impact. Likelihood and impact is best quantified as a value, e.g. a number. You should assess the likelihood of a specific scenario occurring at your organisation and describe the consequences that this would have. Quantification or qualification of risks also allows for risk comparison, and can be used to plot increasing or decreasing risk through time.

When scoring likelihood, you should think of the number of times per year that something occurs, i.e. frequency. In order to assess the likelihood of a certain risk occurring, you should look at whether it occurred before and whether relevant incidents have occurred. Or you can estimate how often a certain scenario may occur.

Impact is about negative influences on the continuity of the company, and about size if the risk occurred before. Impact may be described in terms of 'loss of confidence', 'loss of sales', and 'reputational damage'. 'Loss of confidence' should also be seen in a broader perspective of 'loss of confidence in the financial system', 'the reputation of the Netherlands', 'the international reputation', and 'damage to the business climate'. Your institution will have to quantify these kinds of factors. When quantifying impact you should also think of quantifying reputational damage, or the costs that the institution will incur as a result of measures taken by the supervisory authority.

Some examples of assessing likelihood and impact

Likelihood	Unlikely: the scenario occurs less than once a year Possible: the scenario may occur once a year Likely: the scenario is likely to occur several times a year	1 the scenario occurs once every five years 2 the scenario occurs once a year 3 the scenario occurs two to three times a year 4 the scenario occurs more than four times a year	Low: the scenario is unlikely to occur Medium: there is a small likelihood of the scenario occurring High: there is a reasonable likelihood of the scenario occurring

Impact	Low: negligible financial or reputational damage, no measures from supervisory authority Medium: limited financial or reputational damage; simple measure from supervisory authority High: severe financial or reputational damage; heavy or several measures from supervisory authority	Financial losses (fines, court cases, etc.) and indirect losses (costs, etc.) 1 < EUR 9,999 2 Between EUR 10,000 and EUR 100,000 3 Between EUR 100,000 and EUR 1,000,000 4 Above EUR 1,000,000	Reputational damage 1 negligible loss of confidence, no impact on operational management 2 oss of confidence, or complaints from customers, short-term impact on operational management 3 medium-term impact on customers and operational management 4 long-term impact on customers and operational management

Step 2: risk analysis

In the analysis phase, you now assess the gross risks and the control measures that are taken to mitigate these gross risks. The result should be a list of net risks: the remaining or residual risks.

Analysis of gross risks by scenario

After your institution has outlined the possible scenarios and has determined how to assess likelihood and impact, you must now actually analyse the scenarios. This may be done by having the first line score the different scenarios through self-assessments by assessing the level of likelihood of the described scenario actually occurring. You can also do this by means of interviewing staff or by way of working groups within the organisation or its different departments.

Accurate analysis prompts staff to think about other possible scenarios, or different situations that occurred in the past. Compliance has the task of challenging first-line staff, and assessing the impact of the different scenarios.

Likelihood and impact together constitute gross risk. You should assess for each scenario whether these gross risks are within the boundaries of your institution's risk appetite. Risk appetite is a framework developed by senior management and the board prescribing the type and level of risk that the institution is prepared to accept. Risk appetite specifies the boundaries that staff have to respect when pursuing the institution's strategy. The risk appetite should for instance specify the shortcomings and violations that the institution does not want to be involved in.

If gross risks fall outside your institution's risk appetite, you should consider not providing the services concerned, or no longer serving a particular type of customer.


Likelihood
X
impact
=
Gross risk

Examples of likelihood and impact analyses

Gross risks		Impact			
		4	3	2	1
Likelihood	4	Extreme	Extreme	High	High
	3	Extreme	High	High	Moderate
	2	Extreme	High	Moderate	Low
	1	Extreme	Moderate	Low	Low

Gross risk	Description	Actions/risk appetite
Low	Unlikely to happen, low impact	Acceptable risk
Moderate	May be prevented, slight impact	Risk is acceptable with some monitoring
High	Highly likely to occur with large impact	Risk must be controlled
Extreme	Risk is certain to occur with dramatic impact	Risk must not be taken

Good practice of gross risks analysis

Scenario	Likelihood	Impact	Gross risk	Action/risk appetite
Customers use complex and opaque structures	4	4	Extreme	unacceptable, avoid
Staff member provides advice on how to avoid tax regulations	1	3	High	acceptable, monitor
Customers are located in off-shore locations	3	3	High	acceptable, monitor
Staff member is privately involved with customer	2	2	Moderate	acceptable, some monitoring

Note: This part of the analysis is **not** concerned with assessing risks associated with individual customers.

Analysis of control

You should analyse the control measures necessary for each scenario/gross risk. This means for example that you should specify all work instructions and evaluate them on effectiveness.

This is an obvious task for Compliance, Audit, and various other departments where control measures are performed. Compliance has a monitoring role and will therefore be aware of the level of risk control in the institution. Using the knowledge and insight from the business is, however, essential for this part of the analysis.

When assessing the control measures for the integrity risks, it is very important to also include the extent to which the organisational culture promotes ethical conduct, or detracts from it. Remuneration, outsourcing, and having activities in various countries are factors that play a role in the effectiveness of control.

It is very important that you assess the level of control realistically. If you want to create an accurate picture of possible large risks that are only partially controlled, it is no use making an overoptimistic assessment of control. There is also not much point in summing up the procedures in place or the fact that audits are performed. It is primarily about establishing that control measures are in place and actually implemented. Your institution should also systematically analyse the level of control. This may be either a qualitative or a quantitative analysis.

In addition to an inventory and valuation of control measures, institutions should provide a list of incidents that occurred or deficiencies that came to light in the past year.

If new risks occur that do not yet have dedicated control measures in place, the institution must decide whether it wants to accept, mitigate, or avoid these particular risks. Depending on the decision, appropriate control measures must be put in place.

Examples of assessment of the effectiveness of control measures

Assessment criteria for the existing level of control (design and implementation)	1 fully operational and fully effective 2 could be improved in certain parts, but works adequately and is effective 3 substantial improvement necessary, but has some effect 4 no control, or control has no effect.	Strong: there are several measures in place to control risk Effective: risk is managed adequately Ineffective: risk is not managed adequately

What is not considered good practice?

On the whole, institutions are strongly committed to compliance with regulations and requirements. This means that most attention is usually paid to residual risks after measures have been taken (net risk). In integrity risk analysis it is especially relevant not to take the level of control as a starting point and subsequently examine whether there are any net risks remaining. Without prior analysis of gross risks, institutions will never be able to assess adequately where integrity risks are likely to emerge.

Step 3: determine net risks and decide on control measures to be taken

Net risk is determined by 'subtracting' the level of control from gross risk. Net risk is the residual risk remaining of the gross risk with fully effective control measures in place.

After determining net risk, you should verify whether this is within the boundaries of your institution's risk appetite. In other words, you should determine the level to which your institution is prepared to accept, mitigate, or avoid the remaining net risk. If this residual risk is not within the boundaries of your institution's risk appetite, you should take additional control measures, or reduce the risk in question. If reduction is impossible due to the nature of the risk (e.g. countries that customers receive payments from), you must of course make sure that additional control measures are taken. It will be impossible to reduce all risks to 'zero', residual risk may remain after additional measures have been put in place. You must always remain aware of this.

This part of the analysis, where deficiencies are found in the control of risks that fall outside the risk appetite is particularly important for management to be aware of. Management will then have to act on the deficiencies identified in the analysis, as it will use the integrity risk analysis as a guiding instrument. This is because the integrity risk analysis highlights the risks that need more control and those that may be mitigated by means of less strict control.

It is also important to provide all staff members with a copy of the integrity risk analysis, including explanatory notes. This may for instance take the form of a chart showing where the biggest risks are likely to occur and how they should be mitigated. This ensures that staff members are fully aware of the main risks that the institution is exposed to, and it enables them to exercise risk-based compliance.

Examples of assessment of net risks and follow-up actions

Net risk	Description	Actions that the management may decide on
	Low risk: the risk is unlikely to cause damage Medium risk: there is a slight likelihood of this risk causing damage High risk: there is a considerable likelihood of this risk causing damage	Accept: net risk is low and mitigating measures are working well Reduce: reduce risk or improve control Transfer: possible risk insurance (no outsourcing) Avoid: end the activities

Good practice

An institution provides its management with a clear overview of identified deficiencies in gross and net risks that fall outside the boundaries of the institution's risk appetite. This includes proposed mitigating measures and a time schedule, and it shows the priorities. In addition, more general points for improvement that came up during the analysis are listed.

DeNederlandscheBank

EUROSYSTEEM

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