Holland Quaestor

ASSOCIATION OF QUALITY
CORPORATE SERVICES PROVIDERS

Guideline on the integrity risk analysis in practice

of Holland Quaestor members

"The first step in the risk management process is to acknowledge the reality of risk. Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning." (Charles Tremper)

10 June 2019

Integrity • Independence • Reliability • Sustainability • Professionalism

Index

GUIDELINE ON THE INTEGRITY RISK ANALYSIS IN PRACTICE *OF HOLLAND QUAESTOR MEMBERS*

The integrity risk analysis in practice

"What is on paper must also be applied in practice."

(HQ Policy plan 2015-2020)

1. INTRODUCTION

The Wtt 2018 requires trust offices, for the purpose of conducting their business with integrity and in a controlled manner, to periodically carry out an analysis of the risks to sound business operations.[1] The risks identified in that analysis must be incorporated into the procedures, processes and measures to mitigate those risks.

Trust offices have at least an annual process to develop and amend the organisation-wide integrity risk analysis. The results of this organisation-wide analysis are recorded, but that document is often seen as a static document. The objective of the integrity risk analysis is to transpose the analysis into practical procedures and processes, showing why certain measures have to be taken. The intention is also to actively respond to internal and external developments where new risks may arise and to revise that part of the integrity risk analysis. The integrity risk analysis is essentially about the outcome: awareness of risks and taking adequate control measures to manage the risks. It is therefore important that all 1st and 2nd line employees as well as management are involved in the integrity risk analysis process and are informed about the outcomes.

This guideline aims to give trust offices - members of Holland Quaestor and other interested parties - practical tools to align the integrity risk analysis, the risk appetite and the policies and procedures. The guideline must contribute to ensuring that the integrity risk analysis becomes an integral part of the risk management process. By providing some examples, the guideline describes how the outcomes of the integrity risk analysis can be used in the daily business operations. For employees, the integrity risk analysis can help to clarify why some measures have to be implemented. Ultimately, the integrity risk analysis must contribute to enhancing an internalized integrity culture.

2. DNB

DNB has indicated that several supervisory examinations show that the trust sector has made improvements in the design of the integrity risk analysis, but that the operating effectiveness is not yet at the level that DNB expects from the sector, in particular the translation into the individual client files. Trust offices use the good practices of DNB ("The integrity risk analysis – more where necessary, less where possible")[2] in developing the integrity risk analysis, but the use of the results of the integrity risk analysis is insufficient to actually assess and control the integrity risks. In this respect, DNB indicates that the application of the integrity policies of an institution may be compromised and that the institution remains vulnerable to be involved in financial and economic crime. According to DNB, the integrity risk

[1] Article 14 Wtt 2018 and Article 10 Btt 2018

[2] http://www.toezicht.dnb.nl/en/binaries/51-234068.PDF

analysis is often regarded as a static document instead of a dynamic and continuous process for the actual identification, assessment and control of integrity risks.

From the information provided by DNB, the picture emerges that there is a discrepancy between the integrity risk analysis on the one hand and the implementation of sound business operations on the other. The integrity risk analysis must be an integral part of the vision on integrity and the risk appetite of the trust office and the integer and controlled business operations.

3. THE PURPOSE OF THE INTEGRITY RISK ANALYSIS

An integrity risk analysis enables the trust office to comply with (legal) requirements in a risk-based manner. A trust office analyses those risks that may expose the firm to risks such as money laundering, violations of sanctions regulations, and tax evasion.[3] The trust office should also analyse risks that relate to socially accepted standards. This could include, for example, the public opinion regarding tax planning or the culture within the financial sector. By conducting a risk analysis, new risks and changed strategies can be handled in a well-considered way.

A trust office needs to consider the possible inherent risks that may arise and the different ways in which they can arise when it embarks on new services, when the client base changes, or when legal requirements or business strategies change. The trust office must then assess in a fair and clear manner whether the existing controls are sufficient. If these are not (fully) sufficient, amendments must be made to close these gaps in the controls.

The integrity risk analysis is an integral part of the risk management process. This process includes in short

1. identifying and analysing risks;
2. the management of risks through policies, procedures and systems;
3. monitoring and checking that policies and procedures are actually being implemented and systems are working properly
4. assessing whether the risks are adequately and effectively controlled;
5. reviewing policy and procedures where necessary;
6. informing employees about risks and revised policies and procedures.

A trust office will often already consider the possible risks concerning risk factors such as clients, third parties, employees, delivery channels, countries or services. However, by doing this in a structured way and by making this a continuous process and recording the results, the firm will ensure that reflecting on the risks is 'ingrained' in everyday processes and done intrinsically. This means, for example, that if 1st line employees point out that the transaction behaviour of a few clients has changed, this will not only be assessed for those clients, but that a broader analysis is made if a new risk occurs structurally. And by involving all relevant employees in assessing risks, an internalized, integer culture can be implemented within the trust office. This means that from the 1st line all employees who have client contact or handle and assess client documents and transactions, such as employees of the Finance, Legal, Tax, and office support departments who are aware of all activities and risks, are actively involved. But management, Compliance and Risk Management also have an essential role. Ultimately, the integrity risk analysis serves as a steering document for management, on the basis of which management must decide on the actions to be taken.

Risks consist of threats and vulnerabilities. The purpose of the integrity risk analysis is to identify all possible threats and vulnerabilities that could damage the operations and reputation of the trust office and to assess them in a realistic manner. By means of a critical assessment of the risks, a trust office is

[3] In DNB's guidance the following examples of integrity risks are provided: money laundering, terrorist financing, circumvention of sanctions legislation, corruption (bribery), conflicts of interests, fraud within or outside the organization, evasion or avoidance of tax regulations, market manipulation, cybercrime, socially unacceptable behaviour.

well able to manage risks that may occur concerning clients, other business relationships and services in an appropriate way. By understanding the risks, the trust office can tailor its policies and procedures.

'Risk' can be considered as a factor of threats, vulnerabilities and impact.

Risk is the likelihood of an event and the consequences of this event. The likelihood of an event is the combination of threats and vulnerabilities. A risk can occur when a threat exploits a vulnerability.

Threats arise from persons, groups of persons, or activities that can cause damage to, for example, a country, society, a financial undertaking and the economy. Threats are posed by criminals, terrorist groups, their facilitators, their funds and the activities that they undertake.

Vulnerabilities make the realization of threats possible. Examples are weaknesses in the anti-money laundering and terrorist financing system, such as inadequate controls, or specific characteristics of a financial undertaking or sector, services or products.

Impact relates to the damage that can occur as a result of financial and economic crime. This could include the long or short-term effects of the criminal activities on the financial system, financial undertakings, the economy and society.

4. THE INTEGRITY RISK ANALYSIS PROCESS

DNB's guidance on the integrity risk analysis provides an overview of the steps that can be taken to develop an integrity risk analysis. These steps are briefly summarized here.[4]

The essence of an integrity risk analysis is to map the threats and vulnerabilities with regard to each integrity risk, and to assess, by way of risk scenarios, the likelihood that a scenario will occur and what the consequences may be. A risk scenario is a description how a risk can materialise, or in other words how the trust office can be used for financial-economic crime or other integrity violations. With an integrity risk analysis, the trust office can make informed decisions about the risks that a trust office is willing to take and the control measures that have to be taken.

Preparation and identification: To make an integrity risk analysis, a number of steps have to be taken. An important step is drawing up an organization overview: a 'photo' of the institution. This means that over a period of, for example, one or more years, the number and types of clients are analysed and how often certain services have been provided. It also identifies with which countries the clients and the trust office do business and which roles certain employees or third parties have. The more clients of a certain type are there or the more certain services are provided, the greater the likelihood that a risk manifests itself. But unexpected risks can also arise with services that are not core business of the trust office. It is important that the office collects quantitative data about or has a very good knowledge of the entire client base and its services. Subsequently, the trust office determines which risk scenarios can occur. This includes - combinations of - risk factors such as clients, third parties, employees, delivery channels, countries or services.

Examples of risk scenarios where a trust office may be confronted with financial and economic crime

Money Laundering	
Factors	
clients	Client with corporate structures that include non-transparent entities.

[4] See the "Integrity risk analysis Poster" in DNB's guidance. This poster provides an overview of the steps an institution must take in drawing up an integrity risk analysis.

clients & countries	UBOs from high risk countries who acquired EU citizenship in exchange of, for instance, investments in an EU member state (golden visas).
transactions & third parties	Unclear payments of fees and commissions from / to third parties.
Corruption	
Factors	
clients	Customers whose UBO is a PEP with an unexplained wealth.
countries & transactions	Cash flows from sovereign wealth funds from high risk countries.
Evasion or avoidance of tax regulations	
Factors	
clients	Clients whose ultimate beneficial ownership or control is disguised by the use of nominee shareholders.
clients & countries	Clients with corporate structures that include many entities in offshore jurisdictions.
Terrorism financing	
Factors	
clients	UBOs from existing customers are placed on a terrorism sanction list.
clients & transactions	Clients pay funds to organizations affiliated with terrorism.
Sanctions evasion	
Factors	
clients & countries	Clients trade, via non-transparent structures, with sanctioned countries.
clients	Clients trade in embargo goods.
Socially improper behavior	
Factors	
clients	Clients are active in sectors that do not comply with CSR / ESR standards (such as pharmaceutical industry, arms trade, extraction of raw materials, deforestation).
Conflict of interests	
Factors	
employees & third parties	Employees and introducers have personal relationships.
Internal and external fraud	
Factors	
clients	Clients use false or falsified invoices for payments.
employees	Employees forge clients' invoices.
Market abuse	
Factor	
employees	Employees spread misleading information about a client's stock price.
Cybercrime	
Factors	
third parties	The computer systems of the trust office have been hacked.

The analysis: The organization overview and the risk scenarios lead to the inherent risks. This is done by determining the likelihood that a risk scenario will occur or can occur and its impact. The likelihood is, for example, the number of times per year that something occurs or could occur. When determining the likelihood, the information from the organization overview is used. The impact relates to the financial damage or costs and the reputational damage that can occur if a risk materializes. The latter will usually be an estimate because it is not easy to 'calculate' the impact.

The effectiveness of the controls per inherent risk scenario also has to be assessed. For this, among others, audit reports, information from the compliance monitoring, incident reports and, if available, reports from DNB can be used. It is important that a realistic assessment is made whether the existing measures are being effectively applied and implemented.

Assessment and measures required: Finally, the net risks and gaps in the existing control measures are determined. On the basis of this, it must be assessed which additional measures have to be taken. An integrity risk analysis provides insight into whether a risk can actually occur and must be further reduced to an acceptable level. The trust office also considers whether the (gross and net) risks fall within the risk appetite. The risk analysis provides the trust office and its management with clear insight into the risks that need to be controlled and which measures need to be taken.

Trust offices have different risk profiles depending on the type and number of clients that an office focuses on or the quantity and type of services that are provided. An office with a high risk profile, for example because it mainly focuses on clients with a high inherent risk, will also have to devote extra attention to this in the integrity risk analysis, for example by developing more risk scenarios, being even more critical about the effectiveness of the control measures, and also to think 'out of the box' about possible scenarios.

5. RELATIONSHIP BETWEEN RISK APPETITE AND RISK ANALYSIS

When developing a risk analysis, the trust office examines which risks can be accepted, which must be avoided or can be reduced by taking (additional) control measures. It is also necessary to formulate an "integrity risk appetite".[5] The risk appetite is the set of policies, procedures, limits, controls, and systems that define and indicate how much risk the trust office is willing to take on. The formulation of the risk appetite and the development of the risk analysis are linked, but the processes can be separate. If a trust office is prepared to accept certain risks as part of its business strategy, it will be apparent from the risk appetite. Through the risk analysis process, the trust office can then examine the extent of the measures needed to mitigate those risks to a level within the risk appetite.

The trust office formulates a risk appetite for each integrity risk. By testing the outcomes of the integrity risk analysis against the integrity risk appetite, the firm decides whether to accept, limit or avoid the identified risks. The integrity risk appetite will usually be a qualitative statement, for example that

- the trust office wants to avoid measures by the regulator,
- clients from certain sanctioned countries are not to be accepted,
- tax risks can be accepted with certain clients, but must be properly managed,
- there is no appetite for transactions where aggressive tax planning is the main driver,
- if after applying control measures to PEPs from high-risk countries there remains an unacceptable residual risk, these clients must be avoided,
- the trust office must have sufficient insight into the flow of funds and the activities of clients with operational branches,
- in-house companies can only be used for services that are actually provided,
- there is no appetite for clients that deal in weapons, products that are made with child labour, or with CSR unacceptable activities,
- there is no tolerance for the loss of, or unauthorised or accidental disclosure of, customer information.

Risk appetite needs to be sufficiently measurable. Otherwise there is a risk that statements become void.

In the risk appetite, risk limits can also be set, for example that

- no more than 20% of the customer base can consist of UBOs from high-risk countries,
- there is a maximum to the number of introducers from a certain country,
- domicile-only services are only provided to clients from certain EU countries,
- there should be no more than 2 days backlog with regard to handling transaction monitoring alerts.

The risk appetite will have to be reviewed regularly. It is a logical part of the business strategy and business operations. For example, if a trust office is planning to provide a new type of service, the office will automatically consider, when developing that service, which risks can be accepted or which risks

[5] See also DNB's Good practice document on Integrity Risk Appetite (http://www.toezicht.dnb.nl/en/binaries/51-236451.PDF)

cannot. Considering the risks, the risk limits, the risk scenarios and how the risks have to be managed is a continuous process where the risk appetite and the risk analysis meet.

It helps to develop the integrity risk analysis, if the trust office clearly knows the risks that can be accepted, the risks that need to be additionally controlled or should be avoided. The integrity risk analysis looks at the risks that can actually occur and how these risks are managed. If the risk appetite already determines what can be accepted, it will be clear during the risk analysis process whether a risk falls within the boundaries of the risk appetite.

6. TRANSLATING THE RESULTS OF THE INTEGRITY RISK ANALYSIS INTO POLICIES, MEASURES AND AWARENESS

With its integrity risk analysis, the trust office assesses whether there are gaps in the controls. If, against expectation, a risk has a higher likelihood of materializing, this must also be reflected in (amendments of) the policies and the processes and the knowledge and awareness of employees. The identified risks will have to be incorporated in various processes of the trust office, such as the customer acceptance, transaction monitoring, reporting of unusual transactions or incidents. If the risk analysis shows that there is a (too) high net risk for clients who have operational branches abroad, then the client acceptance process, the review process as well as the transaction monitoring on these clients will have to be enhanced.

A trust office will usually be operational for some years and have policies and procedures in place, which will also have been periodically amended. In drafting these policies and procedures, risks have often been implicitly considered. This will however not always be clear to employees. By carrying out the risk analysis process by including the entire business and by sharing the results of the integrity risk analysis with and explaining them to employees, further risk awareness can be achieved. During the risk analysis process, on the basis of the organization overview, 1st line employees, together with Compliance, will examine whether risks have changed. If, for example, it appears there are more clients with CV structures or clients from high-risk countries and that the client risk analysis does not sufficiently considers the risks of those types of customers, the client acceptance policy and processes relating to client risk analysis will have to be amended in order to strengthen controls. In that part of the policy and processes, it must therefore be explained what the outcome of the risk analysis was and why the policy and processes were amended in a certain way. By also paying attention in the policies and procedures to the results of the risk analysis and thus the background of the control measures to be taken, a link can be established between the integrity risk analysis and the integrity policy.

Legal requirements and social norms are constantly changing. Examples include corporate social responsibility, (aggressive) tax planning, privacy regulation and client integrity. It is therefore also a continuous process to reflect on risks and control measures. Adequate controls do not always lie in procedures or codes of conduct, but also in the behaviour of employees. The results of the integrity risk analysis, the identified gaps and additional measures must therefore be communicated concretely and clearly. This can be done, for example, in meetings with employees or by providing specific explanations during training and in the procedures. This means that in addition to changes to the policy and processes, for example on the intranet, in newsletters or in other ways, the changes and underlying reasons must be communicated. In this way, the integrity risk analysis can be fostered and the usefulness and necessity can be demonstrated.

The amendments to the policies and procedures can also have consequences for the client acceptance, the client risk analysis and the transaction monitoring. If the client acceptance process is amended as a result of the (revised) integrity risk analysis, this will also have to be reflected in the client files, the client risk profiles or the transaction profiles. Again, making an explicit link with the integrity risk analysis is important, for instance by explaining clearly to those who have to do these client files or risk profile reviews what the identified risks are.

As stated in the HQ Policy Plan, "what is on paper must also be applied in practice." This also applies to the integrity risk analysis. If this analysis is only done annually for the regulator or because it has to be done by law, the analysis quickly turns into a paper tiger. By also amending parts of the analysis when there is reason for it and actively involving several employees, it can become clear that the integrity risk analysis is not about the process and the final document, but about the outcome that risks are identified and controlled.

During the review of the integrity risk analysis with regard to the "money laundering" component, a trust office has followed the following steps:

1. During a working group session of 1st and 2nd line employees, it was determined on the basis of a risk scenario that there is a high inherent risk of money laundering through clients with structures that include a trust.
2. When assessing the effectiveness of the measures (e.g. audit reports and compliance monitoring), the firm concluded that the structure overviews in several client files are not always complete and substantiated.
3. The control measures are therefore not fully effective, resulting in an excessively high net risk.
4. The trust office will now have to take additional measures to reduce the net risk.
5. To this end, the management decides, on the recommendation of Compliance, to take certain measures that must be carried out within set timelines.
6. In this way, the client acceptance and review procedures will have to be amended and, for example, clearer guidance for employees will have to be provided on how verify structures and additional attention will have to be given to this in training.
7. Now that the procedures are being amended, this must also be reflected in the client files and risk profiles by paying extra attention to the changes and substantiation of the structure overviews and the risk analysis of relevant clients.
8. During the next cycle of this part of the risk analysis, the trust office will assess whether the amended measures have had an effect and the net risk is at an acceptable level.

7. TRIGGERS TO REVISE THE INTEGRITY RISK ANALYSIS

Part of the risk management process and thereby the integrity risk analysis is to properly monitor if new risks can arise. Sources for this include the media, DNB newsletters, FATF reports, and national and international legislation, but also a changed client base, internal incidents or reports to the FIU.

Some time ago, DNB pointed out the risks associated with the sports and entertainment industry, and specifically football. Examinations by DNB showed that a number of institutions had insufficiently included this risk in their risk analysis and that, despite indications, they had not designated football as a specific risk. When such reports are published, the trust office should assess whether the specific risks can occur and whether there are sufficient control measures. But also the Panama Papers, Paradise Papers, Russia Sanctions, the parliamentary questioning committee on tax constructions should have been reasons to revise parts of the integrity risk analysis.

With new signals, information and risks, the trust office should not wait for the annual cycle to amend the whole integrity risk analysis, but updates of the relevant parts of the analysis must be made immediately. Only in this way can the trust office proactively respond to signals and changes.

New legislation is a reason to carry out a risk analysis. In July 2018, with the revision of the Wwft, a new objective indicator came into effect. Based on this indicator, transactions of or for the benefit of a natural or legal person who is domiciled or established or who has his or her registered office in a state designated by the European Commission, must be reported to the FIU.

A trust office can choose to add this indicator directly in the procedures and to only inform the person responsible for the transaction monitoring. However, since such an amendment of the legislation can have major effects on business operations, it is better to go through the risk analysis process. For this, the trust office determines how many of the current clients have carried out transactions with these countries in the past year and how many clients are resident or established in those countries. On the basis of that data, the trust office can assess the likelihood that the trust office will have to deal with this objective indicator because of its clients and transactions. Depending on the result of the analysis, it will then be examined whether additional measures are required. In addition to the mandatory reporting, this can also be a reason to review certain client files. Several employees will also need to be informed and trained, for example to recognize attempted transactions or other unusual situations.

In view of various international cases and developments, a trust office has decided to make a risk analysis with regard to sovereign wealth funds. The organization overview has shown that the client base includes more sovereign wealth funds than expected, and the various risk scenarios relating to this type of client show that there is a high inherent risk.

An analysis of the policy shows that there is no requirement for enhanced customer due diligence on these clients. Net risk is therefore also high due to the lack of enhanced customer due diligence in all cases. In consultation with Compliance, management then immediately decides to amend the policy and procedures. Because the policies and procedures have been amended, the relevant client files must also be reviewed and the integrity risk profiles amended. The employees who will do these reviews will receive additional guidance from Compliance and an explanation why these reviews are being done.

Internal factors can also be a reason to carry out a review of (part of) the integrity risk analysis. For example, the compliance monitoring shows that there are many signs or alerts of potentially unusual transactions, but that an unusual transaction has never been reported to FIU. During the risk analysis process is a session is also held with management. During this session it becomes clear that management must make the final decision to report but is very cautious to do this. A process change is therefore proposed in which Compliance will be ultimately responsible for reporting to the FIU. This process change is also communicated to all employees.

A review of the integrity risk analysis, or part of it, will first of all have as a consequence that a policy or procedure will be amended. Such an amendment shows how the identified risks and gaps in the controls are resolved.

If such an amendment is made ‘silently’, but when it has many consequences for the execution of the internal processes, there may be some resistance. To show the added value of the integrity risk analysis process to the employees, attention can be drawn to the new risks more actively when policies and procedures change. Especially if the changes to the procedures are significant and several client files have to be reviewed, it is advisable to explain the background to the employees and to connect this to the relevant part of the integrity risk analysis. In this way, the trust office can promote that the integrity risk analysis is no longer a static document, but it can easily show the usefulness and necessity.