



Transaction monitoring guidelines

for Holland Quaestor members

June 2017

Table of contents

1. Background	2
2. Definitions and preamble	3
3. Flowcharts	5
4. Link between transaction monitoring and SIRA	6
5. Good practice 1: Link to transaction monitoring client risk analysis	10
6. Good practice 2: Transaction profile	12
7. Good practice 3: Transaction monitoring form	15
8. Good practice 4: Online viewing rights	17
9. Good practice 5: Proper reporting	18
10. Good practice 6: Re-assessment of previous and related transactions	19

1 BACKGROUND

On 29 March 2017, De Nederlandsche Bank (hereinafter referred to as ‘DNB’) published the *Good Practices for Transaction Monitoring for Trust Offices*. This prompted Holland Quaestor to elaborate on these guidelines in greater detail. The guideline stands on its own, but at the same time a connection is sought with the DNB publication so that consistency in its application can be enhanced. For this reason, this guideline should be read in conjunction with the DNB’s good practices guidelines.

This guideline is intended to provide trust offices, i.e. members of Holland Quaestor and other interested parties, with practical suggestions for the monitoring of client transactions, principally for the control of their own integrity risks, but also in the implementation of what is expected from trust offices pursuant to laws and regulations.



2 DEFINITIONS AND PREAMBLE

The obligation that trust offices have to monitor transactions stems from the gatekeeper role that the Dutch financial system has. This role is one given to them principally under the Dutch Trust Offices (Supervision) Act [*Wet Toezicht Trustkantoren (Wtt)*], the Dutch Regulations governing Sound Operational Practices under the Trust Offices (Supervision) Act 2014 [*Regeling Integere Bedrijfsvoering Wet Toezicht Trustkantoren 2014 (Rib Wtt)*], and the Money Laundering and Terrorist Financing (Prevention) Act [*Wet ter voorkoming van Witwassen en Financiering van Terrorisme*]. The trust offices' duty to monitor has been set out in Article 13(2)(d) and in Article 19(1)(d) of the Rib Wtt 2014 and in Section 3 of the Dutch Money Laundering and Terrorist Financing (Prevention) Act.

Transaction

In this context, a transaction is defined as an action or set of actions for or on behalf of a client or object company of which a trust office has taken note of for the purposes of its services to the client or object company, i.e. a client transaction.

Transaction monitoring

Transaction monitoring entails the assessment of transactions for legitimacy and integrity risks in order to determine whether or not, to the extent possible, cooperation can be given and whether it should be classified as unusual within the meaning of laws and regulations, and from which a duty to report may ensue.



Client risk analysis

The client risk analysis is the analysis of integrity risks to the extent that this analysis must be conducted for every individual client pursuant to Article 23 of the Rib Wtt.

Client risk profile

The client risk profile is the recording of the client risk analysis that has been conducted for the individual client, and it includes the results of the analysis.

Client monitoring

Client monitoring is the process of fulfilling the ongoing obligation to assess clients for integrity risks, as stated for instance in periodic reviews of client files and parts of these, and the repeating of the client screening process, or part of it, which is required when certain changes are made to the client aspects.



Director's role

Perhaps superfluously, it should be noted that no legal distinction is made between a trust administrator and an operational director. If a trust office is appointed as a director of a company, this role entails all the duties and responsibilities that the law attaches to this position in the context of proper administration, and it includes all the liabilities associated with it. This means that a trust office, especially in terms of its account management task, cannot consider itself to be an extension of the client, but instead it must be mindful of its actual position. In the process, the clients must also acknowledge and appreciate this position as it stands.

Not merely a process

In the context of sound operational practices, transaction monitoring is a process that, together with expertise, common sense and sound business sense, consists of gathering information and identifying, analysing and investigating risks based on a procedure and in such a way that a substantive and substantiated opinion can be given about the integrity risks associated with a transaction. Checklists can contribute significantly to the process of forming the correct opinion. Having said that, checklists are a tool and cannot replace one's own expertise and professional and critical faculties when forming an opinion.

Information

In the context of forming a critical opinion, it is crucial to assess the information correctly. Information is not the same as documentation. Information may come from a client, a UBO, third parties/business clients, a public source or from one's own organisation. Information may be verbal, a document, in the media, or may arise from one's own actions and/or something that one has generated. Depending on the nature of the information, it must be assessed and valued in terms of its origin, form and contents.

In the context of how information is recorded (understandable, accessible, verifiable), we would like to point out that information can be validated by adding elements such as a date, stamp, initials, signature, notes scribbled in the margin, translations, attached memos, etc.



Systematic integrity risk analysis (SIRA)

SIRA is an activity, not a document, despite the fact that they are generally considered to be one and the same thing. In principle, this activity must be carried out according to a pre-defined procedure and methodology. As a rule, the analysis itself takes place on the basis of a document prepared for this purpose, and aims to provide insight into the organisational risk appetite and the extent to which identified risks are controlled.

The underlying concept is to encourage an organisation, at least the board and other relevant staff members, to consider and think about what steps are being taken in the context of striving to achieve business objectives, and which integrity risks are involved. This is done so that it is then possible to consciously determine which risks are considered acceptable, and how these risks are controlled in the day-to-day business operations.



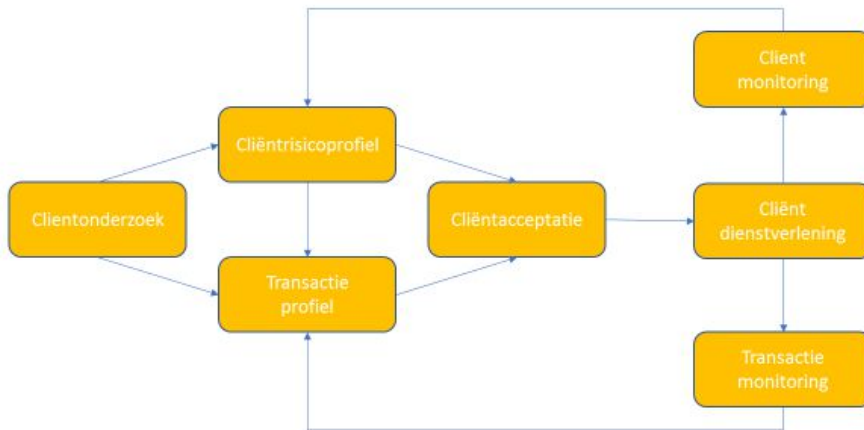
Procedures

Procedures related to sound operational practices are not always practical and, partly because of this, they may not always be congruent with the trust office's actual course of operations. One of the main reasons for this is that procedures are often drawn up in order to comply with laws and regulations related to integrity. In other words, the obligations under the law from a legal perspective are taken and turned into a procedure.

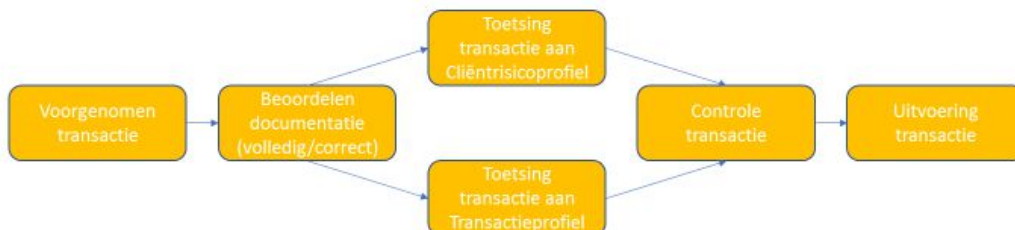
It is possible to create a more practical basis if the processes that are required for this are taken as the starting point when drawing up the procedures. The requirements under the laws and regulations can then supplement the procedure so that all the obligations are met.

3 FLOWCHARTS

Examples of diagrams representing transaction monitoring.
The place of transaction monitoring in the client life cycle.



Implementation of the transaction procedure and transaction monitoring procedure.



4 LINK BETWEEN TRANSACTION MONITORING AND SIRA

SIRA can be seen as a starting point for how sound operational practices should be structured. The DNB has indicated that it expects transaction monitoring to be listed as a mitigating measure when integrity risks are identified in the context of the SIRA. This concerns the risk analysis at organisational level and primarily involves organisational policy and organisational risk appetite, but it also involves the concrete mitigation of accepted risks. By incorporating specific scenarios as they may arise, the measures that are or will be taken can be specifically defined so that the risks are properly controlled. The following components are logically part of this.

Access to transaction information

In this connection, the primary issue is how a trust office finds out about an proposed transaction or one that has already taken place. During the SIRA, the focus is on the services that the trust office provides, and on the conditions under which these services are offered.

Examples of relevant aspects/considerations in this respect would include:

- Contact with the client (direct or indirect)
- A new or existing structure (establishment through the trust office, transaction history)
- Authority to represent (non-executive director, power of representation)
- Receiving post at the trust office address
- Access to bank accounts
- Authority with respect to the bank account
- Provision of service including the administration
- Experience with the client

In other words, if the trust office confines itself from a policy perspective to clients with whom it has direct contact, for whom a new structure is established and from the outset it is solely and independently authorised to represent the object company, whose mail is received at the trust office and the trust office manages the bank accounts, the situation is different to when an existing structure is accepted as a client with external independent directors and co-directors and/or the trust office has no access to or insight into the object company's bank account(s).

In the former case, the company cannot be de facto bound by rights and obligations, and no banking transactions can take place without the knowledge and cooperation of the trust office. In the latter case, there may be fund flows that the trust office has no insight into. Every restriction to full insight into and/or control of matters requires control measures.

The policy decisions that are made in this case may affect the transaction monitoring since they help to determine the trust office's information position.

An important aspect of this is that the information position is a contributing factor to the question of whether the trust office is in a position to intervene in a *timely* manner if an unusual transaction takes place or may take place.

- ❖ **The SIRA can include those information positions that are acceptable to the trust office and how they ensure that all the information reaches it in good time. The way in which this is provided for determines the risks and the appropriate measures.**

Nature of the client

The presence of integrity risks is also related to the nature of clients. This is determined by various factors that may to a greater or lesser degree involve specific integrity risks.

Examples of relevant risk indicators and considerations:

Client/UBO

- Private individual or corporate entity
- External audit mandatory or otherwise
- The presence of a UBO
- Involvement of PEP
- Introduction via or involvement of an intermediary (particularly if based in a tax haven)
- No personal meetings
- Limited or no direct contact
- Based in or originating from a country against which international sanctions have been imposed
- Based in or originating from a country with an emerging market
- Risk of money laundering (FATF)
- Risk of terrorist financing
- Risk of fraud (including tax fraud)
- Risk of corruption (including conflicts of interest) (CPI)
- Conviction for a criminal or financial offence
- Involvement in a lawsuit involving integrity issues
- Negative media coverage

Object company and structure

- Non-executive director authorised to act independently
- External person authorised to act independently with respect to bank accounts
- Operational activities
- Production
- Trade (import/export)
- Activities related to the arms industry, animal industry, art trade, adult entertainment, gambling operations, virtual currency and cash-intensive industries
- Property (development, commercial operation, trading in)
- Consultancy
- Business clients/activities involving organisations in countries with a certain (x) CPI score
- Business clients/activities involving organisations in countries against which international sanctions apply
- Foreign object company
- Hybrid entities in the structure
- Nominee shareholder involved
- Trust or private foundation is part of the structure
- Staff working for the object company
- Presence in the sector
- Head entity based in a tax haven
- Several national and international trust service providers involved

- Illogical use of legal entities
- Repeated changing of trust office

Including the relevant risk indicators in the SIRA reveals the policies and risk appetite related to the type of clients as well as the conditions under which certain risks are accepted. It is especially this part of the SIRA that affects the client risk analysis under Article 23 Rib Wtt 2014. The client risk analysis as performed in the context of client acceptance must provide a (clear) evaluation of policy and risk appetite.

- ❖ **Information about the client portfolio must be available so that the nature of the client portfolio can be determined when conducting the SIRA. Compiling a list of the organisation's own client portfolio vis-à-vis the relevant client aspects (risk indicators) prior to conducting the SIRA may also benefit its effectiveness and scope (compare with ISI reporting).**

Objective of the service provision

A trust office is obliged to ascertain the purpose of the service. This obligation does not involve examining the service itself, such as having a local director, but rather the objective that the client intends to achieve through the services provided by the trust office, such as tax planning, having a European branch, local expertise and so forth.

The intended objective must be substantiated. In other words, based on information it must be possible to determine the reasons for the business relationship, for the services of the trust office and for the structure. By extension, a trust office forms an opinion of how realistic and feasible the objective is. Finally, it must be determined periodically whether and to what extent the objective is met.

As an example: a tax objective may be substantiated by tax advice from an (independent) expert. The substantiation includes the entire structure and the structure is also in line with the advice given. Anomalies in the structure are explained and substantiated. The advice in question is assessed periodically to check whether it is still valid and to ascertain whether the structure still corresponds and functions as intended. In this respect, it generally does not suffice to say that a structure has been set up to take advantage of the favourable tax regime in the Netherlands, whether or not with reference to a regulation or treaty, and then to periodically discover that the structure has not yet been used for the intended objective.

It may be relevant to investigate unintended consequences. For instance, a certain fiscal position or anonymity may not be intended, and yet they may be the result because of the structure.

- ❖ **Information about the client portfolio must be available to be able to effectively take into consideration the objective of the business relationship, service and structure when conducting the SIRA. Compiling a list of the client portfolio vis-à-vis the intended objectives may improve the effectiveness and scope of the SIRA.**

Nature of the transaction

Although there is overlap with the considerations related to the nature of the client, it is also important to distinguish between the nature of transactions. To be able to monitor efficiently and effectively but also thoroughly, management measures should also cater for this.

Examples of relevant risk indicators and considerations:

- Cash/banking transaction
- Non-cash transaction
- Size
- Parties involved
- Government related (collaboration, concession)
- Verifiable performance fee (consultancy)
- Verifiable valuation (property)
- Risk of money laundering
- Risk of terrorist financing
- Risk of fraud (including tax fraud)
- Risk of corruption (including conflicts of interest)

These risk indicators and considerations must be worked out in detail in concrete and realistic risk scenarios so that practical control measures can be taken and assessed. If, for example, a trust office serves clients who carry out operational activities, a relevant question would be whether specific (operational) expertise is required to be able to assess transactions in terms of their legitimacy and integrity risks.

❖ **Information about the client portfolio must be available in order to be able to determine the nature of the transactions when conducting the SIRA. Compiling a list of the client portfolio vis-à-vis the nature of the client transactions that are being carried out may benefit the effectiveness as well as the scope of the SIRA.**

5 GOOD PRACTICE 1: LINK TO TRANSACTION MONITORING CLIENT RISK ANALYSIS

This good practice concerns linking transaction monitoring to the risk analysis of the client.

The policy and risk appetite take shape by conducting the SIRA, and this is reflected in the client risk analysis as it should be performed for each individual client (under Article 23 of the Rib Wtt).

- ❖ A separate client risk analysis must be carried out for every client/object company and recorded in the client risk profile. For efficiency considerations, one may opt in certain cases to have a combined client risk profile, for instance, the company with the trust office foundation.

The client risk analysis must be designed in such a way that it is possible to demonstrate that the client, including its objective and activities, falls within the policies and risk appetite. Relevant client risks, like those mentioned in Section 4 above, may be part of the client risk analysis in the context of client acceptance as well as subsequently when providing client services, i.e. client monitoring/transaction monitoring.

- ❖ If certain client risks are beyond the scope of the trust office's risk appetite, they will form part of the client acceptance process and, depending on the set up, the client acceptance process may be part of the client risk analysis but in principle not part of the client risk profile. For instance, if clients trading in arms are categorically rejected, then this does not need to be mentioned in the client risk profile.



Link to transaction monitoring

The client risk profile should then be a factor in the design and execution of transaction monitoring for the individual client. In other words, the way in which transaction monitoring is conducted with an individual client is based in part on the client risk profile.

On the one hand, this can be reflected in the transaction monitoring procedure (in the procedures manual) by providing specific measures for the various situations (as also included in the SIRA). On the other hand, these measures for individual clients can be recorded in their client dossiers. These measures must be properly aligned to ensure that the process is effective.

- ❖ What it may boil down to in practice, for instance, is that if a trust office accepts clients with a PEP, this must be included in the SIRA. For this, measures must be devised that can be expected to control the associated risks. The transaction monitoring procedure provides for the measures that are taken when applicable. This client aspect must also be included in the client risk analysis, whereby the measures are assessed against this client's context. The control measures must be applied during the transaction monitoring process, for instance, by including them in the transaction profile or ensuring that a transaction is evaluated based on the client risk profile.

In this regard, the compliance function is expected to play a part in formulating the procedure, right down to the forms and checklists used. It must also verify whether the procedure is followed and it must be adjusted if necessary. Furthermore, the compliance function can be expected to play a role



when drawing up and/or changing a client risk profile if there is an increased risk. Finally, the compliance function should be included when assessing potentially unusual transactions.

The audit function is expected to form an opinion about the design of the procedure, including the forms and checklists used. It must also assess the procedure's existence by establishing that it is actually being followed, and also whether it has the intended effect by carrying out spot checks to assess transactions on their own merits.

6 GOOD PRACTICE 2: TRANSACTION PROFILE

This good practice involves using transaction profiles when assessing individual transactions and transaction patterns.

It is generally accepted that using a transaction profile is indispensable when visibly and systematically assessing transactions for integrity risks. According to the DNB good practices, a transaction profile must be:

1. Current
2. Complete
3. Specific
4. Clear
5. Substantiated
6. Documented

Re 1

To keep a transaction profile up-to-date, the monitoring procedure must provide for amendments if and when they are warranted. The first transaction profile is drawn up in the context of client screening and client acceptance. No transactions have yet been executed at that point. When transactions are executed, they should be assessed against the existing transaction profile, in combination with the client risk profile if applicable. If the transaction differs from the transaction profile, it should be determined whether there is 1) a new standard transaction and the transaction profile has to be adjusted as a consequence; 2) a one-off, unusual transaction resulting in a specific investigation and recording; or 3) a potentially unusual transaction with appropriate follow-up action (prompting a procedure for 'internal alert' or 'unusual transaction').

The transaction profile does not necessarily have to be changed due to a one-off unusual transaction, as long as a clear and full integrity risk analysis is conducted, based in part on the client risk profile.

- ❖ The initial preparation and changes to a transaction profile, as well as one-off (unusual) transactions, must be handled taking into account the four eyes principle. The basic assumption underlying the four eyes principle is that it is secured in the first line. Depending on the nature and organisation of the trust office, the compliance officer can handle it.

It is also advisable to review the transaction profile comprehensively and periodically. In the process, the extent to which the expected transactions have not taken place, and which conclusions should be drawn from this, can also be assessed. A logical time to review the transaction profile would be when the financial statements are being prepared.

- ❖ It is advisable to screen all business clients regarding their transaction profiles (automatically) against the sanctions lists and negative news (on the internet/Google alerts).

Re 2 and Re 3

A transaction profile is complete and specific if it is possible to determine with certainty that an individual transaction is covered by the transaction profile when compared to the definition of a standard transaction. Needless to say, this depends on the circumstances, but very general characteristics will not suffice.

- ❖ All rights and obligations must be included in the transaction profile. Rights and obligations may, for instance, consist of:
 - Property
 - Investments
 - Agreements with service providers, employees, purchasers or suppliers
 - Loans
 - Guarantees and securities
 - Licences
 - Options

- ❖ The definition is expected to include the following components:
 - The other party
 - Type of transaction, for instance:
 - Acquisition or disposal of shares in a subsidiary or participation
 - Receipt of dividends from a subsidiary or participation
 - Repayment or receipt of a loan
 - Repayment or receipt of interest payments for a loan
 - Paying instalments on a loan
 - Purchase or sale of fixed assets or inventory
 - Paying dividends
 - Payments related to current account ratios within a group
 - Receipt or payment of royalties
 - Payments to/from trade creditors/debtors
 - Amounts and/or ranges
 - Frequency
 - Description/explanation
 - Currency
 - Bank account for receipts
 - Bank account for payments

A risk analysis is then carried out on the transaction, clearly based on risk indicators and taking into account the client, the other party or parties and the transaction. The more detail there is about the standard transaction in question in the profile, the easier it will be to include it later during the execution.

Re 4

Where appropriate, an overview of the structure can be added that clearly shows the fund flows; this will enhance the transparency.

Re 5

Every standard transaction that is included in the transaction profile must be substantiated in such a way that the underpinning can be aligned with the nature of the transaction.

- ❖ **If it is clearly laid down in policies, then in principle transactions like those with the trust office, the Dutch tax authorities, Dutch civil-law notaries or the Chamber of Commerce do not require a substantiation, or a limited substantiation will suffice.**

Transactions can be substantiated, for instance, by adding the relevant legal and other documentation and/or information, for instance, an invoice, contract, agreement, decision, Chamber of Commerce extract, printout of the website and so on. For efficiency reasons, a reference to the source of this documentation can be included in another file. This reference must be sufficiently specific and the person who signs the transaction profile must guarantee its correctness.

- ❖ **The reliability of the procedure determines, up to a point, the extent to which a reference can be relied on. In other words, if the procedure excludes the possibility of an incorrect reference, for instance to a non-existent document or to one that does not meet the requirements, the substantiation may be more effective in certain cases. For instance, a procedure may prescribe that a control document detailing the existence of certain documents must be signed for approval.**

Re 6

The assessment of a transaction is adequately recorded if someone else can ascertain afterwards that the procedure has been followed, and it is clear which members of staff have carried out the assessment (and the check) and which considerations have underpinned the opinion. Depending on the circumstances of the case, it may be useful to have a stamp for this that can be used on bank statements or the transaction monitoring form (see Good Practice 3), and to add documentation or a reference to the source.

7 GOOD PRACTICE 3: TRANSACTION MONITORING FORM

This good practice concerns the monitoring of the rights and obligations that an object company undertakes using a form specifically designed for this purpose.

The DNB good practices rely on the trust office's common sense, whereby it is ensured that the trust office has the appropriate expertise and involvement in the object company's operations. In this regard, it is particularly important that a trust office is aware of its administrative and other responsibilities, given that no distinction is made between the responsibilities of a trust administrator and those of a full executive director. A trustee is expected to ensure that all the requirements that apply to proper administration of a company are met, as these are laid down in Book 2 of the Dutch Civil Code.

A form that has been specifically designed for that purpose can be used to support the staff members who assess and/or execute transactions. The form can include among other things whether and, if so, which standard transaction in the transaction profile is linked to it. The form may also include a checklist that makes it easier to ensure that all the requirements for the execution have been met, for the integrity risks as well as for the administrative and/or financial requirements.

- ❖ **The transaction monitoring form for the transaction should at any rate include the following components:**
 - **Client's name**
 - **Transaction date**
 - **Standard transaction**
 - **Yes, related to transaction # [] in the transaction profile**
 - **No, type of transaction:**
 - **Description/explanation**
 - **Payment or performance**
 - **Bank account for payments or receipts**
 - **The other party**
 - **Payment or performance**
 - **Bank account for payments or receipts**

- ❖ **The following questions may also be included on the transaction monitoring form:**
 - **Is there an adequate overview of all the object company's rights and obligations, and have these been recorded in the client dossier?**
 - **Have all the obligations under company law regarding the recording of decision-making process been met?**
 - **Have all the administrative obligations been met?**
 - **Have all the tax obligations been met?**
 - **Does the transaction serve the interests of the company?**
 - **Is the object company in a position to execute the transaction from a financial/economic perspective? (Also bear in mind future liquidity events, such as loan repayments and guarantees that may be invoked)**

- ❖ The transaction monitoring procedure and the transaction profile may provide for the possibility of performing certain (low-risk) transactions without using a transaction form. It is worth noting that transactions that fall within the transaction profile may also be considered unusual. See, for instance, Good Practice 6 for retrospective assessments.
- ❖ As a means of ensuring that the transaction profile is up to date, the transaction monitoring form could include the question of whether the assessment/ analysis in that particular situation requires an adjustment to the transaction profile or even the client risk profile.

8 GOOD PRACTICE 4: ONLINE VIEWING RIGHTS

This good practice concerns insight into bank transactions using online viewing rights.

As noted previously, the trust office's information position is crucial to transaction monitoring. In principle, the basic assumption is that no transactions can take place without the trust office's cooperation, but this principle may be departed from under certain conditions. DNB good practices are clear about this: any concession to that basic assumption must be substantiated so that it is clear why the concession in question is being made and how the risks arising from it are being controlled.

In this, the nature of the client (risk profile), the nature of the service and the client's activities are an indispensable part of the assessment. For example, the transaction may entail a 'domicilie plus' situation whereby the client performs certain transactions for which monitoring is done retrospectively, such as on expenses incurred, while other transactions are presented to the trust office in advance, for example, a transfer of shares as a result of which an unknown person qualifies as the UBO.

The most noteworthy elements are therefore the importance of client management in the sense that the timely and accurate communication about transactions with the client has to be guaranteed, and the time allowed between the transaction and transaction monitoring assessment is limited. The length of time set aside for this depends on the risk analysis, but one year seems to be the maximum if the risk is extremely low. See also 'Access to transaction information'

9 GOOD PRACTICE 5: PROPER REPORTING

This good practice concerns the proper reporting of monitoring activities and the associated considerations.

For this component, the DNB specifies their expectations with respect to the recording of monitoring. As a general rule, additional recording leads to additional administrative duties and responsibilities that are often regarded as bureaucratic, particularly if it involves broad knowledge and expertise. Having said that, a professional organisation ought to operate transparently and in a verifiable manner, and create an audit trail when conducting operations and implementing procedures. This is a condition for existence for a licensed trust office.

The balance to be found to meet all the obligations and/or expectations in a workable manner depends on the circumstances. In some cases, a tick on the checklist may suffice; in other cases, this tick needs to be substantiated. Many transactions do not require substantiation or only up to a point, such as those for the Dutch tax authorities, civil-law notaries, Chamber of Commerce and so on. Some transactions require an initial assessment that can be referred to subsequently for repeat transactions, with or without periodic retrospective assessments. And there are transactions that require very thorough underpinning.

In addition to those aspects that have already been discussed in this respect, the DNB emphasises that the compliance officer's involvement must be recorded, regardless of whether it is a supervisory role.

How effectively this recording has been provided for depends on the compliance officer's role that has been assigned in the transaction monitoring procedure. What is important at any rate is that the compliance officer's involvement, insofar as it is not otherwise clear, must be guaranteed by his or her own position. The involvement of the compliance officer in the context of the procedure for 'unusual' transactions and 'internal alerts' (incidents procedure) may be deemed to provide for the compliance officer's monitoring of the procedure.

- ❖ **Make sure that the compliance framework records the compliance activities as referred to above correctly and comprehensively. For instance, the compliance officer must keep records of a work programme and relevant issues must be reflected in compliance reports.**
- ❖ **Client dossiers considered to be the property of the company, such as banking files, are handed back to the client when the client leaves. If the recording of transaction monitoring is kept in these files, this may in certain cases be in conflict with the obligation to keep certain data for at least five years.**

10 GOOD PRACTICE 6: RE-ASSESSMENT OF PREVIOUS AND RELATED TRANSACTIONS

This good practice concerns the re-assessment of previous and related transactions after an unusual transaction has been detected.

By assessing transactions retrospectively based on the most up-to-date knowledge and interdependence, transactions may be put into a different light. The DNB expects trust offices to cater for this procedurally, particularly when it concerns the discovery of an unusual transaction. The practical implementation of this must be reasonably in line with the client's risk profile, as well as the extent to which there is or may be a change to the circumstances or perspective.

Here we have in mind the following measures.

- Periodic retrospective monitoring as standard practice, for instance, in line with the periodic review of the transaction profile mentioned previously, possibly when the financial statements are being prepared. It may be necessary to do so more often than once a year if the transaction profile or the client risk analysis warrants it.
- Any indication that it may involve an unusual transaction constitutes a reason to assess or review the preceding transactions, and to include them in the decision, before a final opinion can be formed about the unusual nature of the transaction. The period that needs to be reviewed will depend on the circumstances, but it should be a conscious and substantiated decision.

-O-O-O-