RISK-BASED INDUSTRY BASELINE

Ongoing Due Diligence

Dutch Banking Association

CONTEXT

Introduction

The Dutch banking sector recognizes the need for a more risk-based way of working in order to effectively prevent financial crime. Therefore, the sector is operationalising the risk-based approach to comply with legal obligations [1] arising from the 'Wet ter voorkoming van witwassen en financieren van terrorisme' (hereafter: Wwft). This risk-based operationalisation is recognised and endorsed by the Dutch AML supervisor, De Nederlandsche Bank (hereafter: DNB). In 2022, DNB published the report 'From recovery to balance' [2] which started off a series of risk-based roundtables with the Dutch banking sector. The intention is to establish effective financial crime control frameworks and adequately assess the relevant Money Laundering (hereafter: ML) and Terrorist Financing (hereafter: TF) risks. Through a risk-based way of working, resources are allocated proportionately towards higher risks. This approach has an impact on the Ongoing Due Diligence (hereafter: ODD) framework of banks [3], where ML/TF risks are being mitigated during the business relationships on an ongoing basis.

This NVB Industry Baseline focuses on:

- the transition towards relying on an (automated) trigger-based ODD framework and relevant Event Driven Reviews (hereafter: EDRs) and, as a result thereof;
- conducting risk-differentiated reviews.

As such, this document does not provide a complete overview of all components of the ODD framework. Rather, the document focuses on applying the risk-based approach and conditions to focus on executing relevant EDRs instead of performing time-driven Periodic Reviews (hereafter: PRs) by default. PRs might add limited relevance from a risk perspective, although in some cases these can still be a valid part of the financial crime control framework.

In line with the aforementioned operationalisation, banks can use a more effective and automated approach for detecting ML/TF by applying continuous monitoring on client behaviour, so-called Client Monitoring (hereafter: CM). CM uses risk triggers on both static and behavioural client data. In general, the quality of the generated alerts and events and the effectiveness of the (automated) detection of risks increases. This is, among others, due to the automation of client data actualisation and improvements in more advanced risk detection mechanisms. Therefore, by adding CM to ML/TF risk detection mechanisms, the added value of spending time and efforts on PRs has diminished. This enables a gradual and diligent operationalisation towards performing relevant EDRs.

This NVB Industry Baseline outlines the following important principles:

- Banks can perform ODD in a risk-based manner (i.e. relying on relevant EDRs instead of PRs as their default CDD method).
- Banks determine themselves which CDD methods they apply to comply with the Wwft.
- The conditions as included in this NVB Industry Baselines must be read as considerations for banks to take into account when applying the risk-based approach. These are not minimal requirements that must be met before banks can start relying on their (automated) trigger-based ODD framework. It is within the banks' discretion to determine whether their implemented Financial Crime Framework is sufficiently effective to transition (partly) away from reliance on PRs.
- It is recognised that banks' risk-based processes and maturity will evolve and improve over time as the bank gains insights from adopting such a framework.

1 The banks' overall objective is to prevent misuse of the financial system for money laundering and terrorist financing.
2 Van herstel naar balans; Een vooruitblik naar een meer risicogebaseerde aanpak van het voorkomen en bestrijden van witwassen en terrorismefinanciering (DNB, 2022).
3 Note that CDD processes (such as transaction filtering) are also used to comply with (parts of) sanction regulations and aim to mitigate certain sanction risks.

The ODD framework comprises three core elements:

- **Client data** refers to the process to keep relevant client data structurally up to date. Many banks are shifting from periodic client outreach processes towards more risk-based and automated methods of actualising client data, for example, using links to external sources (see NVB Industry Baseline 'Client data actualisation', April 2023).
- **Alert and event generation** is the process of applying risk detection mechanisms to continuously screen clients and monitor their behaviour. Hereto, banks take into account risk assessments, including the National Risk Assessment (hereafter: NRA) and risk assessments such as the Systematic Integrity Risk Assessment [4] (hereafter: SIRA) [5], as a starting point, yet these can be supplemented with other internal information (e.g. insights and lessons learned from the alert and event handling feedback loop and external sources such as international reports, papers, leaks, etc.). Many banks are constantly improving their alert and event generating processes by analysing their client data more effectively and efficiently to detect ML/TF risks in a risk-based manner (also see NVB Industry Baselines 'Models in alert and event generation', July 2023, and 'Expected Transaction Profile', April 2023).
- **Alert and event handling** is the risk-based approach to handle (including assessment and review, if applicable) generated alerts, events and clients where potential risks are identified (see section 2.1.3).

Positioning within the Financial Crime Framework

The ODD framework consists of fundamental components required for an effective ongoing due diligence. It contains a set of ongoing screening and monitoring processes and controls to be performed by banks after a client has been onboarded.

Financial Crime Framework: traditional and risk-based

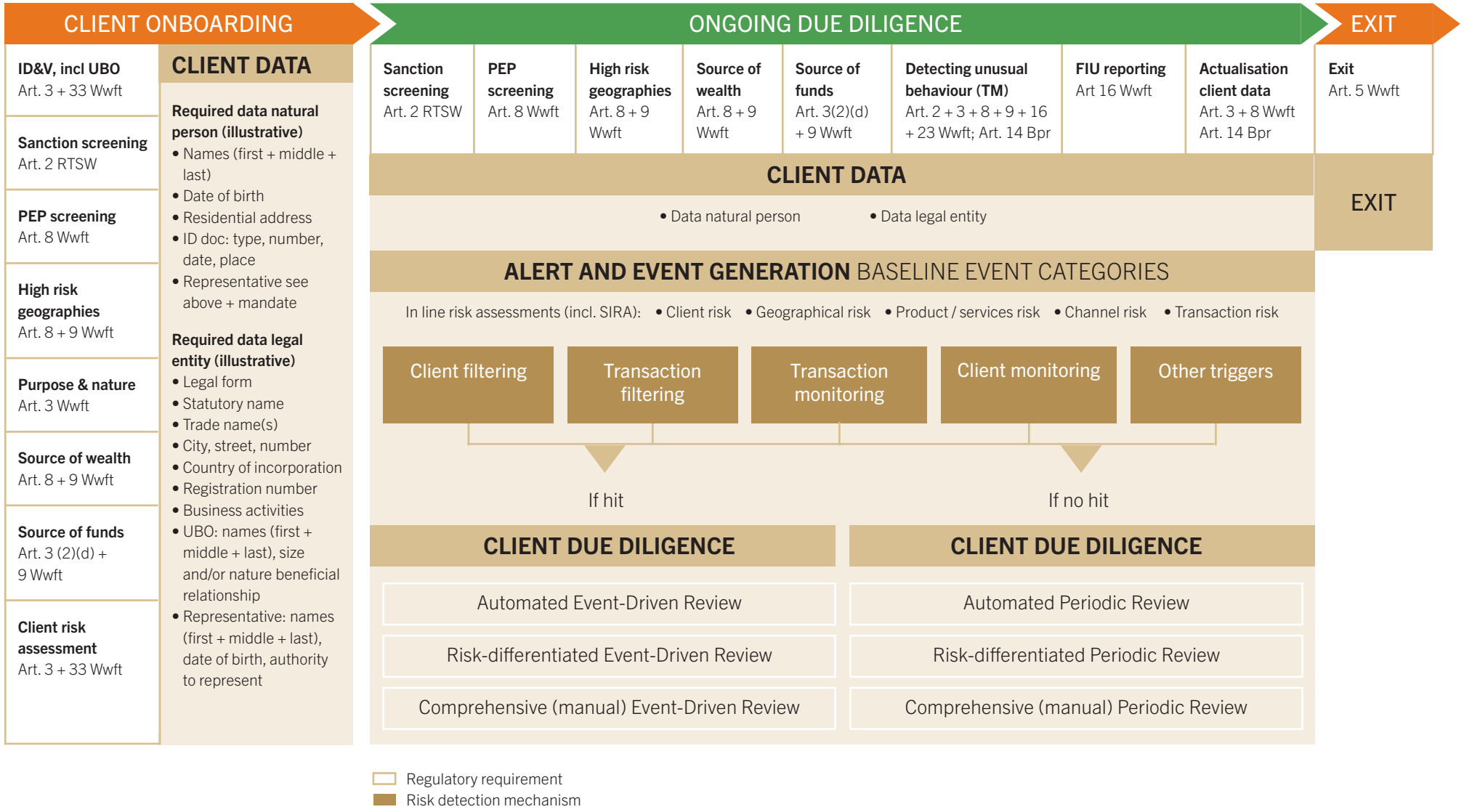
- Page 4 shows the more traditional Financial Crime Framework in which PRs are a significant part of the ODD controls. To apply the risk-based approach, the first banks are applying CM and transition away from conducting PRs by default.
- Page 5 shows the risk-based Financial Crime Framework in which alert and event handling triage is, by default, initiated by trigger-based generated alerts and events. In this framework banks rely, amongst others, on CM in their ML/TF risk detection processes, which enables a gradual and diligent transformation to reliance on effective EDRs.

4 Also known as Enterprise-wide Risk Assessment (EWRA) or Firm-wide Risk Assessment (FWRA)

5 Banks can take into account the relevant EBA Guidelines such as the 'Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions', European Banking Authority, 1 March 2021.

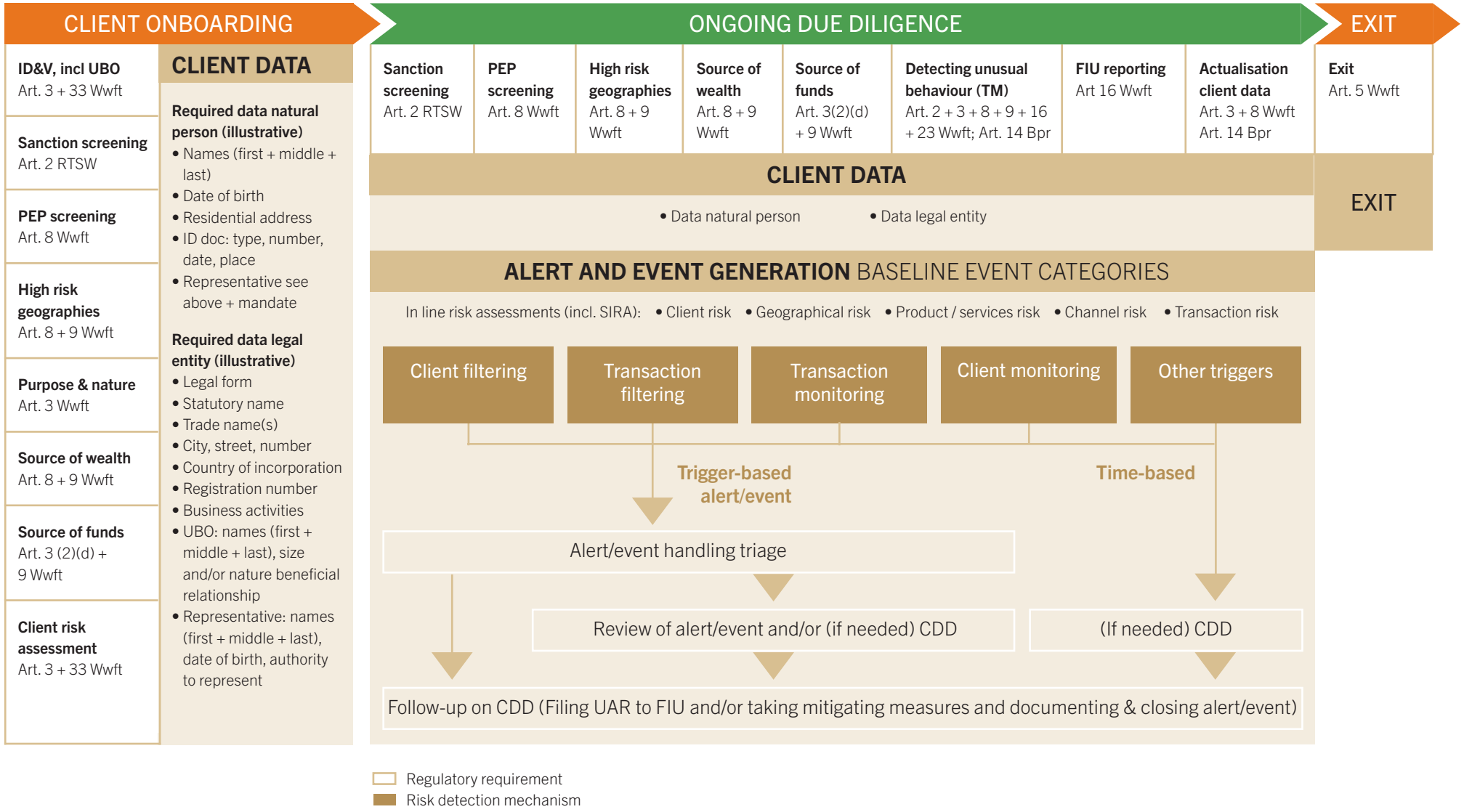
FINANCIAL CRIME FRAMEWORK

TRADITIONAL



FINANCIAL CRIME FRAMEWORK

RISK-BASED



RISK-BASED INDUSTRY BASELINE

1 Industry Baseline

This Industry Baseline describes the operationalisation of the risk-based execution of the ODD framework by the Dutch banking sector. Banks should continuously update their ODD framework to manage and mitigate ML/TF risks in the most effective and proportionate way. Such risks and mitigating measures can, for example, be derived from the risk assessments (e.g. SIRA), based on a proper understanding of the bank's client portfolio, product offering and in line with the bank's risk appetite. These risk insights can be expanded with the NRA, supranational risk assessment and other sources.

To ensure operationalisation of a mature (automated) trigger-based ODD framework in a controlled manner, banks should have auditable processes and control frameworks in place. It is recognized that the processes and their maturity will evolve and improve over time as banks gain insights from adopting such a framework.

1.1 Conditions to operationalise an (automated) [6] trigger-based ODD framework

The ODD framework enables the continuous screening and monitoring of the client, including its transactions and behaviour, with the aim of detecting unusual transactions, keeping the assigned risk classification of the client actual and determining what actions are necessary given the client's risks. Banks are allowed to transition away from predefined PR cycles for their entire client population, relying on client data actualisation and (partially) automated risk assessments.

In order to operationalise an (automated) trigger-based ODD framework, banks should consider the following conditions.

- By means of processes for continuous improvement of data quality, banks strive for their relevant client data to be complete and correct. Quality of relevant client data is to be within risk appetite and subject to regular monitoring and feedback loops. Data is actualised based on rule- and/or model-based alerts and events, or retrieved from external sources, internal analysis or client outreach (see NVB Industry Baseline 'Client data actualisation', April 2023).
- Automated risk detection mechanisms and alert and event generation must be in place (based on transaction patterns, client behaviour and changes in client or transaction data) and have been proven effective. These mechanisms must be properly governed – in case of models according to the model risk management framework.
- Risk triggers should effectively cover the potential risks within the bank's client portfolio and the bank's risk assessments (see section 2.1.2). Banks need to prove that their detection works adequately (based on monitoring, audits and continuous improvement processes). In case of shortcomings, mitigating measures should be taken commensurate to the issue. This could entail for instance reviewing specific client groups.
- Ensure compliance with regulatory requirements (i.e. risk-based approach aligns with relevant regulatory requirements that are applicable). Banks respond to changes in their own risk exposure and regulatory changes.
- Ensure adequate design and implementation of EDR processes and adequate operational effectiveness of those, in accordance with internal policies and procedures outlining the methodology and scope of the approach, as well as the roles and responsibilities [7]. In addition, the design and implementation should adhere to all relevant internal policies of the bank including for example privacy policies.

6 Not all risks can be detected by means of automated risk triggers; for example situations banks become aware of via thematic investigations, portfolio analysis or staff.

7 Art.10 Bpr obliges institutions to comply with their own policies and procedures.

- Ensure adequate oversight on effective EDR processes (on elements such as throughput times, operational insight, priorities and effectiveness) based on adequate management information.
- Alerts or events will be processed within the relevant timeframe in accordance with the risk appetite.

1.2 Conditions for automated risk detection mechanisms

Banks that rely on automated risk detection mechanisms such as transaction filtering, client filtering, transaction monitoring and client monitoring must have sufficient comfort (based on monitoring, audits and continuous improvement processes) that these processes adequately address legal obligations and mitigate the identified potential risks, including inherent risks identified in risk assessments (including SIRA).

Banks can adequately substantiate their automated risk detection mechanisms (and no longer rely upon PRs) by having the following conditions in place.

- Continuously strive for completeness in risk triggers to effectively cover the potential risks within the bank's client portfolio and the bank's risk assessment, and mitigating measures outlined in the bank's risk assessments (including SIRA). The quality of the risk triggers lies within the bank's risk appetite and is subject to regular monitoring and improvement based on feedback loops. It is recognised that 100% risk coverage is not feasible.
- Maintain an adequate level of risk mitigation and ensure continuous improvement cycles of risk detection mechanisms (i.e. feedback loop) are in place and operationally effective.
- Relevant management information (including information on effectiveness) is in place which shows that the results of the automated risk detection mechanism are in accordance with the actual risks in de client portfolio.

1.3 Handling methods

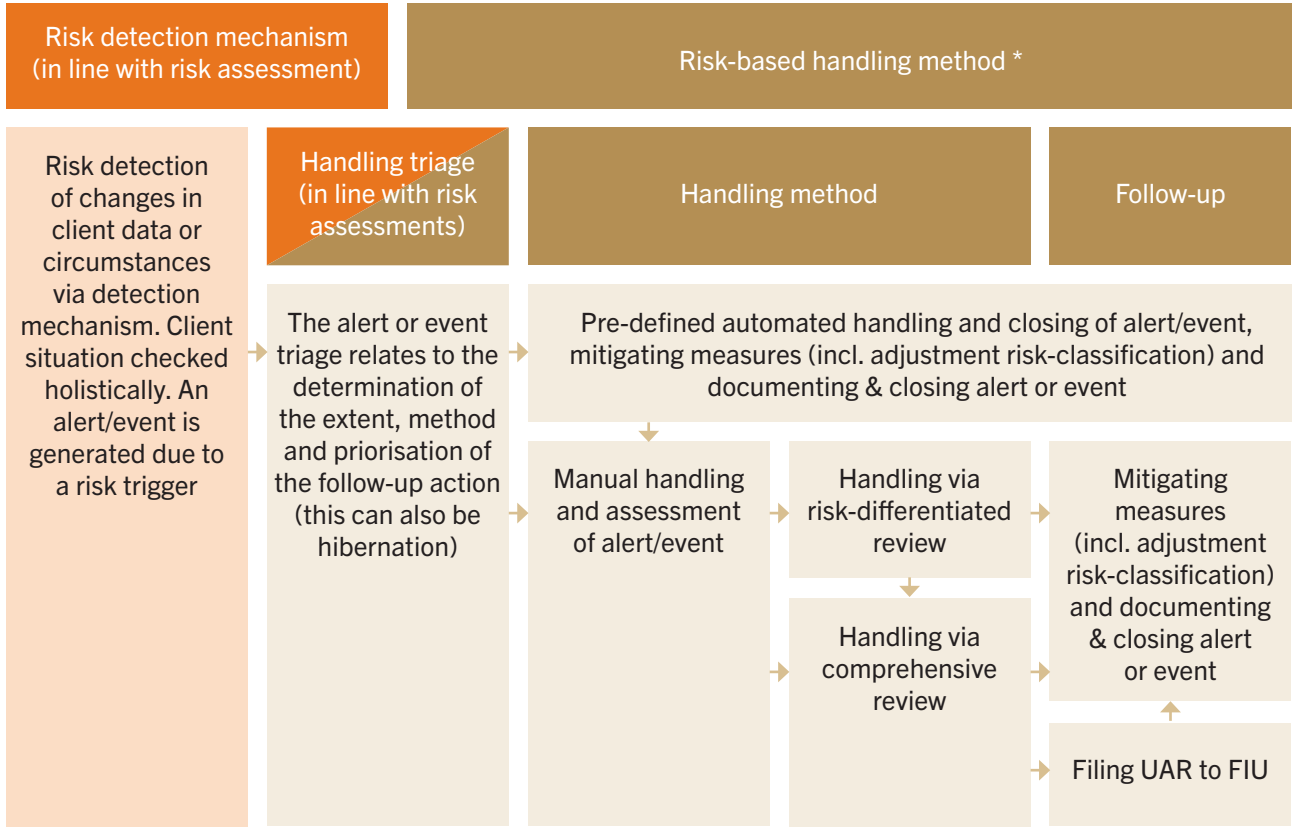
When CM is embedded in ODD processes, banks are able to identify relevant changes in the client situation. In some cases, the change of the client situation triggers an assessment of the identified risk via alert and event handling.

A risk-based approach is applied by banks when setting up the alert and event handling method. The purpose of alert and event handling is to adequately follow-up on the alert and event by validating or adjusting the client's risk profile, applying mitigating measures (if needed) and/or by filing UARs to the FIU.

Banks set-up and document handling processes in accordance with their internal processes and applicable methods of alert and event handling, and take into account the obligations in the law, specific risks, client portfolio, product offering and risk appetite.

Banks are not obliged to periodically conduct comprehensive (manual) reviews (i.e. the traditional PRs) by default for each client when a substantiated and effective trigger-based ODD framework is in place. Banks can apply automated, risk-differentiated and comprehensive methods simultaneously on different sections of their client portfolio in order to assure that resources are allocated in a risk relevant and proportionate manner.

The risk-based approach of alert and event handling can be visualised as follows.



* This flow is a simplified version for illustrative purpose. Please note that for different risk detection processes (TF, TM, CF, CM) different and more specific process flows would apply.

● Risk detection mechanism ● Risk-based handling method

To ensure banks' resources are most effectively allocated, banks use a risk-based approach, which allows for:

- alert and event handling triage (i.e. determination of handling method);
- automated handling and closing of alerts and events;
- handling of the alert and event by an analyst via:
  - risk-differentiated review (i.e. reviewing only the identified risk), and/or
  - comprehensive review (i.e. reviewing the full scope).

The following considerations must be taken into account in order to determine the handling method banks need to perform.

- The maturity of the identification and coverage of ML/TF risks in the bank's risk detection processes. Banks must be sufficiently comfortable with their overall ODD processes in order to apply risk-differentiated EDRs (see conditions under 'Handling via risk-differentiated review'). The level of comfort is, amongst others, based on testing, monitoring results and audits.
- The banks' risks as identified in their risk assessments. Handling methods must be in line with the bank's SIRA outcomes and risk appetite. More specifically, in line with the risks related to the bank's client portfolio and product offering (e.g. handling method could differ between specific clients or client groups) and in line with the risks related to the generated alert and event. Complexity of the client or the client's risk profile might be relevant; highly complex clients might

require extensive expertise of staff and can therefore be handled comprehensively. Examples of complex clients differ per bank. Less complex clients are more suited for risk-differentiated reviews or automated closing of alerts and events.
- Through continuous improvement of data quality, banks strive for their relevant client data to be complete and correct; the data quality of relevant client data is to be within risk appetite and subject to regular monitoring and feedback loops. Data is actualised based on rule- and/or model-based alerts and events, or retrieved from external sources, internal analysis or client outreach (see NVB Industry Baseline 'Client data actualisation', April 2023).

Alert and event handling triage

Banks' detection mechanisms generate alerts and events. The alert and event triage relates to the determination of the depth, method, and prioritisation of the follow-up action (this can also be hibernation; the situation where an alert or event becomes relevant only in combination with other triggered client behaviour, and will be handled in the context of the triggered client behaviour rather than in isolation). It must be assessed whether the generated alert and event relates to an actual identified ML/TF risk which needs to be handled by an analyst.

Banks determine themselves where the deployment of their staff has the most added-value. Possible handling methods are:
- *Automated handling and closing of alerts and events that are within risk appetite.* The handling of the alert and event is finalised when the conclusion is drawn that there is no risk identified and manual handling is not necessary.
- *Handling via risk-differentiated review.* If a risk is identified and follow-up is necessary, the next step is initiating a risk-differentiated review.
- *Handling via comprehensive review*. Outcome of triage could directly initiate a comprehensive review of the alert and event.

Automation of handling process

Alerts and events can automatically be handled by means of a predefined risk response. The automation of handling processes functions within the banks' Financial Crime Framework. An example is the (rule-based) automated handling and closing of alerts and events. It can be considered a risk-based decision not to act further on specific risk triggers. As such, automated handling and closing of alerts or events should be regarded as a risk assessment in its own right. This response is within the bank's risk appetite and compliant with the legal obligations arising from the Wwft. Banks should keep record of:
- the considerations;
- evidence potential impact of the closures on the risks identified in the risk assessments;
- the explicit relation to the bank's integrity risk appetite;
- the files that are in scope.

Autoclosure should lead to refinement of the alert and event generation rules and is not a long-term structural solution.

Mass closing refers to the practice of closing or terminating a large number of alerts and events. This can occur when deciding (after thorough testing) to (gradually) de-activate specific risk triggers. For example, as a consequence of a change in risk appetite, or when alerts or events are incorrectly generated. In these cases, the identified risk is assessed and substantiated with evidence as being within the bank's risk appetite. Such a mass closing should be seen as a risk assessment in its own right. In the risk-based approach, the larger the number of mass closings, the more in-depth the evidence for showing its impact on the relevant risk, risk appetite, and legal obligations needs to be.

Conditions for applying predefined risks responses.
- *Client data*
  Banks strive to have the relevant client data required for risk assessment available and accessible in a structured and retrievable format to be able to use it in an automated manner. Furthermore, they implement data quality controls to monitor and demonstrate the correctness, completeness, and integrity of the relevant client data in a risk-based manner.
- *Effectiveness testing documentation*
  Documentation regarding internal testing of the design, existence and operating effectiveness of key controls.

Handling via risk-differentiated review

Handling via risk-differentiated review focuses on the ML/TF risks related to the alert and event. The analyst assesses the alert and event in relation to the specific client situation. Upon finalisation of the handling, a conclusion is documented including a substantiation on the applied way of the handling of the alert and event and the related impact the alert or event has on the required risk mitigating measures (including confirming or changing the risk classification of the client). If the analyst thinks the risk-differentiated review is not sufficient to ensure an appropriate risk response, the analyst initiates comprehensive review and provides feedback to the automated risk detection mechanisms.

Conditions for applying handling via risk-differentiating review.

- Substantiation is required of the conditions under which the bank wants to apply the risk-differentiated reviews (e.g. number of risk triggers applicable to a client, specific risks as identified in the bank's risk assessment, specific client groups).
- Periodically, ex-post checks are conducted and documented to assess whether the conditions have been met in practice. Analysts are trained to focus on the relevant risks related to the alert and event of the risk trigger in relation to the client situation and know when to finalise the handling (i.e. know when to stop) [8]. Analysts are also trained to recognise situations that require a comprehensive review [9].
- Banks have documented procedures and working instructions in place on risk-differentiated reviews of alerts and events. Performing processes in a risk-based manner also means balancing time and depth of assessments and reviews. Regardless of the controls and measures banks apply in their ODD processes, there is always a need for staff to perform AML/CFT controls with a risk management mindset.
- Internal (e.g. 1st, 2nd and 3rd line) and/or external parties verify the effectiveness of the applied approach and demonstrate effectiveness evidence based (among others through quality assurance, sample checks, back-testing and portfolio analysis).
- Banks strive for their relevant client data to be complete and correct. Furthermore, there is a risk-based process to actualise relevant data. Data quality is within the bank's risk appetite and subject to regular monitoring and feedback loops. Data is actualised based on rule- and/or model-based alerts or events, or retrieved from external sources, internal analysis or client outreach. Internal (e.g. 1st, 2nd and 3rd line) and/or external parties verify the effectiveness of the applied approach and demonstrate effectiveness evidence-based.

Handling via comprehensive review

During the handling via comprehensive review, an analyst manually and comprehensively assesses the complete client situation. This can be approached as an EDR or PR. During this review the relevant new risks are assessed to determine if the risk classification and the potentially relevant mitigating measures still fit the client profile. In addition, this can provide clear input on the effectiveness of the risk detection mechanism – are all relevant risks detected by the system?

Comprehensive reviews are applied in the following cases.

- If the automated risk detection mechanisms do not sufficiently cover the risks as identified in the bank's risk assessment (including SIRA) for specific clients or events; or
- New risks are detected during the risk-differentiated review, or risks appear to be too complex for a risk-differentiated review, which triggers a comprehensive review; or
- The client and/or transaction is deemed too complex for automated or risk-differentiated review; or
- In case a comprehensive review is required by law.

1.4 Risk-relevancy

The ODD framework as laid out in this NVB Industry Baseline contributes to operationalising the risk-based approach and meet Wwft obligations. Clients, their transactions and behaviour identified by banks' risk detection mechanisms as a potential higher risk are prioritised in order to mitigate those risks.

8 The Wwft requires banks to educate and train all employees involved in the AML/CTF domain, to ensure they have the skills and knowledge to perform their job.

9 This is in addition to the training on performing comprehensive reviews.

Operationalising an (automated) trigger-based ODD framework increases the relevancy of the handling process, as resources are allocated proportionately towards higher risks and priorities, as identified by the risk detection mechanisms. This means that banks must take steps to determine appropriate controls and measures (including risk triggers, thresholds, etc.) to comply with the Wwft and in relation to their exposure to ML/TF risks and their risk appetite.

It should be noted that with any risk-based way of working, risks will be missed. No framework is flawless, and the risk-based approach is not a 'zero failure' approach as is also the case when doing manual handling and PRs. Feedback loops, process monitoring, internal control testing and audits should be in place for continuous improvement purposes and to enhance the framework where required. Regardless of the controls and measures banks apply in their ODD processes, there is always a need for staff to perform AML/CFT controls with a risk management mindset.

1.5 Client types

Banks can apply the risk-based approach for all clients and client types. Depending on the bank's risk appetite, they can differentiate the handling method for different client groups considering the size, complexity, specific risks, client portfolio and product offering.

1.6 Criteria to demonstrate effective implementation

Whilst the design and implementation of an ODD framework may be bank specific, banks must ensure that they continue to improve their frameworks for the purpose of increasing effectiveness and to continue to address risks they may encounter. This continuous improvement cycle is essential to ensure an adequate and timely response to new and emerging risks. Furthermore, continuous monitoring of the existing processes and performance testing are essential criteria for effective implementation. The effective implementation of the (automated) trigger-based ODD framework and of the handling methods must be demonstrable.

Demonstrating an effective (automated) trigger-based ODD framework

Banks demonstrate the effective implementation of the conditions required to operationalise a trigger-based ODD framework by substantiating how they establish and maintain a proportionate risk-based set of controls to mitigate ML/TF risks. Furthermore, the relation to other existing processes or controls should be defined (i.e. data actualisation processes, threshold setting, risk responses, etc.).

This is bank specific as the design and implementation of the ODD framework is based on, and matched with, the risk appetite and corresponding AML/CFT policy. In addition, the maturity will develop over time with insights gained in adopting an automated trigger-based ODD framework.

Banks should have the following documentation in place to demonstrate effective implementation of the risk-based approach within their respective ODD processes.

I Risk & control documentation

- Mapping of key risks and controls to clearly demonstrate the relation between the bank's ML/TF risks (for example as documented in the bank's risk assessment including SIRA), its risk detection mechanisms and processes to mitigate the risks.
- Risk & control documentation demonstrating the quality of the detection mechanisms, in relation to risks as identified in the bank's risk assessment and portfolio management results.
- Management information and reports to demonstrate the effective implementation of the risk detection mechanisms the bank has in place.
- Banks have a process demonstrating continuous improvement of risk detection mechanisms (i.e. feedback loop)
  - Improving detection of known risks, for example by following-up on outcomes of control assessment and testing;
  - Improving by identifying new risks for example based on back-testing activities or external situations that exposes the bank to new risks.
- Settings of the risk detection mechanisms, such as setting of thresholds based on data analysis (including documentation of threshold rationales). Settings are sufficiently substantiated and show an overview of current settings, the involved risks, and a clear link to the risk appetite.

II Effectiveness testing documentation

Effectiveness is strongly related to the extent to which banks have internal control testing in place to test the design and operating effectiveness of key controls. Banks should determine how, and to what extent and frequency, testing the effectiveness of controls should be performed. Effectiveness is assessed based on the intended objective or desired outcome of a particular mitigating control measure.

- Documentation showing a test plan outlining the objective, scope and methodologies for conducting the effectiveness testing. This also includes test scripts describing detailed instructions or steps that outline how the system will be tested. They specify the actions to be performed, inputs to be provided, and expected outputs or results.
- Documentation showing the (operational) effectiveness of the output of risk detection mechanisms in relation to the assessed ML/TF (top) risks (e.g. via back-testing activities, based on the relevant management information). It demonstrates how and to what degree of effectiveness banks' detection mechanisms are detecting the risks.
- In addition, banks should follow-up on these results, for example by tuning and documenting the actions taken. Where a control requires significant time and/or resources for minimal risk mitigation, banks should consider changing or eliminating the control and allocating those resources to controls with more effective outcomes. With this regular practice banks decommission ineffective and inefficient controls. The opportunity cost of failing to change or eliminate an ineffective or inefficient control should be a part of banks' overall assessment of its risk-based controls.

III Process validation documentation

- Outcomes of 1st, 2nd and 3rd line (or external) control testing and (external) quality assurance processes.
- Documentation of the follow-up actions on these results, for example, demonstrate adjustments and/or improvements in the ODD processes.

IV Documentation of relevant decision making

- Documented rationale and substantiation for decisions regarding for example prioritisation of improvements, and threshold settings (rule, model, transaction, event level), mass/auto-closing also related to the risk appetite.
- Documented and clear governance in place that allows the bank to steer and make decisions, amongst others, impacting the execution of processes in the ODD framework.

V Client data documentation

- Documented required financial crime data including data governance.
- Description of the bank's data quality processes and procedures (e.g. related to data actualisation).
- Sufficient substantiation of the relevant data quality components (such as data integrity).

Demonstrating the effective implementation of the alert and event handling methods

- Banks have a clear governance in place that allows the bank to steer and make decisions that, amongst others, impact which handling methods are applied in specific situations.
- Banks substantiate which handling method is to be applied in specific situations (criteria, decision and analysis thereof, i.e. regarding type of clients, risks and effectiveness of risk detection mechanisms). With an audit trail of the applied handling methods over time.
- Banks record and document in the client file the handling of all generated alerts or events for an individual client (which process has been applied and the conclusion thereof, including impact on the risk classification) in a retrievable manner.
- Banks conduct periodic effectiveness tests of the handling methods and act on the results.
- Process in place to monitor and improve the quality of alert and event handling methods.
- Banks have sufficient management information available to demonstrate the effective implementation of any automated or manual alert or event handling solution, the bank applies.

Note that in practice, the banks' risk-based implementation of handling methods will focus on the highest risks, accompanied by more intensive quality processes.

2 Impact

This NVB Industry Baseline provides guidance to the Dutch banking sector on how to transition from conduction PRs by default towards relying on an (automated) trigger-based ODD framework and conducting more event-driven and risk-differentiated reviews.

Operationalising a continuous screening and monitoring framework is crucial to enable a risk-based approach and avoid time consuming PRs. The ODD framework contributes to the risk-based approach by applying a trigger-based way of assessing alerts and events that enables banks to effectively deploy resources in a risk relevant way. The risk-based approach of ODD will enable banks to execute more effective AML/CFT controls by increasing focus on higher risks and apply mitigating measures where they are most effective. This is essential to avoid overcompliance with PRs providing limited added value to mitigate ML/TF risks, compared potentially more effective mitigating measures. In addition, not applying ODD in a risk relevant way, could lead to burdensome requests and disproportional measures towards clients.

The way risk-based ODD will be conducted has an impact on banks' internal monitoring and audit processes. In addition, it impacts the discussions regarding the quality of banks' internal control processes within the 1st and 2nd line and with internal (supervisory board) and external supervisors.

By improving effectiveness and efficiency of AML/CFT controls, society as a whole benefits from a safe and trustworthy financial system while limiting the unnecessary burden for law-abiding citizens.

3 Use cases

ODD FRAMEWORK: NO RISK TRIGGER

Example

A client has a regular pattern of in- and outgoing transactions which are in line with their ETP. The client does not purchase complex products. The client has been living in the Netherlands, at the same address for over 10 years.

Industry Baseline

- Bank mitigates the risk related to the client by applying CM and transaction monitoring processes and controls.
- No alert will be generated for this client, since the static and baviour data of the client give no reason to indicate a change in the risk classification of the client.
- As long as client's situation stays the same, meaning transactions stay within the ETP, and no changes occur in the behavioural or static data which may affect the risk classification of the client, there will be no need to review the client.
- The above is based on a situation where ETP, CM and TM are working effectively, SIRA risks are covered, and no major gaps are detected.

ODD FRAMEWORK: RISK TRIGGER

Example

A client has a regular pattern of in- and outgoing transactions and acts in line with the ETP. The client does not purchase complex products. Client has been living in the Netherlands, at the same address for over 10 years. Transaction data might indicate a change in the country of residence, since the client has inbound and outbound transactions from and to Spain several consecutive months. The event 'potential change in country of residence' will be triggered. Internal analysis might indicate the need for data actualisation.

Industry Baseline

Transaction data indicates a potential change in the country of residence. Since the situation of the client might be different (see NVB Industry Baseline 'Client data actualisation'), there is reason to perform an alert and event assessment, potentially automated when related risks falls within the bank's risk appetite.

HANDLING METHOD: RISK-DIFFERENTIATED EDR

Example

Client

A client is a legal entity located in the Netherlands. The parent company is registered in a higher risk jurisdiction that requires increased monitoring due to strategic deficiencies in their AML legislation according to the FATF. Furthermore, the client's core business activity is to import traditional food from the higher risk jurisdiction for sale in the Netherlands. This is considered a cash-intensive industry, and therefore a higher risk business activity.

Bank

Automated risk detection mechanisms of the bank sufficiently cover the relevant ML/TF risks of the bank (based on SIRA).

Risk trigger

The client's transaction data indicate that the business activities, next to the Netherlands, also take place in Belgium (neutral ML/TF risk country). Besides that, the detection mechanisms do not detect any other changes in the client situation.

Industry Baseline

Since the geography and cash related risks have been previously assessed, the analyst is instructed to focus on the assessment of the risks related to the business activities conducted in Belgium, whilst also considering the other risk triggers (import from high-risk jurisdiction and cash-intensive industry). The analyst concludes the change in the client situation fits the client profile and identifies no risks. There is no need for a comprehensive handling [10].

Notes

1 This example might trigger the actualisation of certain client data in order to meet the bank's reporting obligations (e.g. CRS).
2 This assessment could also be automated by a predefined risk response of the bank.

10 In case the analyst concludes the change in the client situation does not fit the client profile or in case new risks are identified, the analyst could trigger a comprehensive review.

HANDLING METHOD: COMPREHENSIVE PR

Example

Client

A client is a legal entity located in the Netherlands. In addition, the client has a complex ownership structure (multiple layers between client and UBOs) and adverse media screening has previously detected negative press on the parent company of the client. The client's business activities have recently expanded from a retail clothing shop that only accepts card transactions to also include hospitality, which is considered a cash-intensive industry and therefore a higher risk business activity.

Bank

Risk detection mechanisms of the bank sufficiently cover the relevant ML/TF risks of the bank (based on SIRA).

Risk trigger

The rule-based detection mechanism of the bank detects a change in business activity. An alert is generated.

Industry Baseline

The analyst manually performs a comprehensive risk review because of complex risk situation (complex ownership structure) and a change in business activities is detected.

CONTEXT

Regulatory framework

The regulatory context for this topic is described in relevant parts of applicable laws, regulations and guidelines from various authorities. Relevant legal provisions are part of Wwft, Besluit prudentiële regels Wet financieel toezicht (hereafter: Bpr Wft) and Regeling toezicht Sanctiewet 1977 (hereafter: RtSw).

Banks are not obliged to periodically perform a review of individual clients. The Wwft does not define when or with what frequency CDD needs to be performed. It does specify that the intensity of CDD should be tailored to the risk sensitivity of the client. Nevertheless, the Wwft does state that the bank's client and the business relationship must be continuously monitored.

There are no specific legal requirements on alert and event handling methods. However, banks are obliged to file Unusual Activity Reports (hereafter: UAR) to the Financial Intelligence Unit (hereafter: FIU), as soon as the unusual nature of the transaction or proposed transaction becomes apparent.

- **Article 2a(1) Wwft**

"In order to prevent money laundering and terrorist financing, an institution shall perform CDD and report unusual transactions in accordance with the rules laid down by or pursuant to Chapters 2 and 3. In doing so, an institution pays particular attention to unusual transaction patterns and to transactions that, by their nature, entail a higher risk of money laundering or terrorist financing."

- **Article 3(2)d Wwft**

"CDD enables the institution to (. . .):
d. conduct ongoing monitoring of the business relationship and the transactions carried out during that business relationship to ensure that these are consistent with the institution's knowledge of the client and its risk profile, and where necessary an investigation into the source of funds used in the business relationship or transaction."

- **Article 3(8) Wwft**

"An institution demonstrably tailors CDD to the risk sensitivity for money laundering or terrorism financing of the type of client, business relationship, product or transaction."

- **Article 3(9) Wwft**

"When determining the risk sensitivity, as referred to in paragraph eight, the institution takes into account at least the risk indicators listed in Annex I to the 4th Anti-Money Laundering Directive."

- **Article 3(11) Wwft**

"An institution shall take reasonable measures to ensure that the data collected pursuant to paragraphs 2 to 4 concerning persons referred to therein are kept up to date."

- **Article 16(1) Wwft**

"An institution shall report an executed or intended unusual transaction to the Financial Intelligence Unit promptly after the unusual nature of the transaction has become known."

- **Article 14(4) Bpr Wft**

"The financial institution, referred to in paragraph 2, or branch respectively, has established procedures and measures regarding the analysis of client information, including in relation to the products and services purchased by the client, and with regard to the detection of deviating transaction patterns. Based on the aforementioned procedures and measures, the financial institution also determines the risks of specific clients, products or services for the sound pursuit of its business."

- **Article 2 RtSw**

"1. The institution shall ensure that, in the areas of administrative organisation and internal control, it has taken measures to comply with the Sanctions regulations.
2. The measures as referred to in subsection (1) shall at least provide for an adequate check of the records kept by the institution in order to establish any match between the identity of a relation and that of a natural or legal person or entity referred to in the Sanctions regulations, in order to permit that the relation's assets to be frozen or to prevent financial resources from being made available, or services from being rendered, to that relation.

- **Article 3 RtSw**

"If the institution ascertains that the identity of a relation matches that of a natural or legal person or entity as referred to in the Sanctions regulations, it

shall notify this to the supervisory authority immediately. When making the notification, the institution shall also submit the data on the identity of the relation to the supervisory authority."

Relationship 'DNB Good Practices' and 'NVB Industry Baseline'

DNB aims to illustrate its supervisory practices to the benefit of supervised entities by, for example, providing an interpretation on regulatory requirements (Q&As) and examples on how regulatory requirements can be met (Good Practices). It is important to note that neither the DNB Q&As nor Good Practices are legally binding.

The NVB Industry Baseline describes the application and execution of the ODD framework in more detail and how this contributes to a more risk-based approach.

• • •