RISK-BASED INDUSTRY BASELINE

Expected Transaction Profile (ETP)

Dutch
Banking Association

CONTEXT

Introduction

The Expected Transaction Profile (hereafter: ETP) is defined as the expected transaction pattern of a client or ETP client group [1] transactions. The ETP can be a useful, and sometimes necessary, tool to detect deviations from expected transaction patterns and unusual transactions. Banks are required to report unusual transactions to the Financial Intelligence Unit. This NVB Industry Baseline describes the risk-based method to use ETP, which Dutch banks can apply to detect deviations from expected transaction patterns and unusual transactions.

The NVB Industry Baseline outlines the following main principles:

- ETP can be used as one of the methods to detect unusual transactions but is not a goal in itself.
- An individual bank determines its risk-based approach to effectively detect deviations from expected transaction patterns and unusual transactions based on its defined risk appetite and AML/CFT control framework.
- The use of specific client groups for rule-based transaction monitoring is not equal to ETP, although overlap may occur.
- A client profile is not the same as an ETP.
- Banks can, but are not obliged to request information from the client to establish the ETP at onboarding.
- The DNB Leidraad [2] is to be used as a good practice and does not represent minimum requirements.

The NVB Industry Baseline describes the risk-based Dutch banking practice regarding the positioning of ETP in the financial crime framework to detect, assess and when needed report unusual transactions. An overview of the ETP scope is provided, which also states processes that are not in scope. This is followed by more detail on risk relevancy, determining ETP, risk response and demonstrating effective implementation of ETP. Use cases are included for various scenarios to illustrate practical implementation of this Industry Baseline with focus on the ETP.

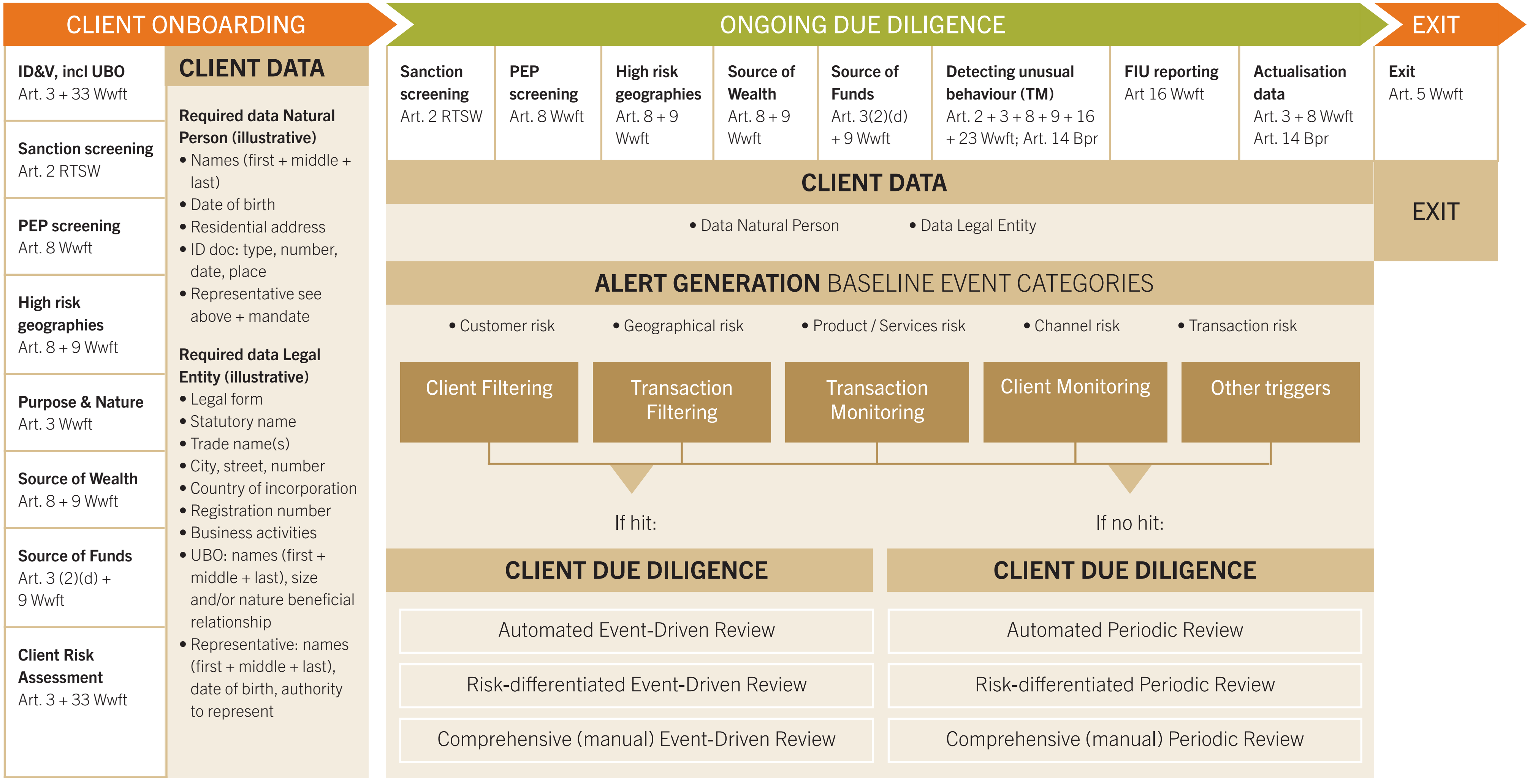
Positioning within Financial Crime Framework

The ETP can be part of the ongoing due diligence (hereafter: ODD) and transaction monitoring (hereafter: TM) processes.

[1] In this baseline, the term ‘peer group’ refers to client groups with similar characteristics. ETP client groups and specific client groups are types of peer groups. The term ‘ETP client groups’ refers to homogeneous groups that are set-up to detect unusual transactions by comparing expected transaction behaviour with actual transaction behaviour (i.e. deviations from ETP). The term ‘specific client groups’ refers to other possible peer groups that may be used to detect specific client risks and unusual transactions.

[2] Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act (DNB; December 2020 version), Post-event transaction monitoring process for banks (DNB; 30 August 2017).

FINANCIAL CRIME FRAMEWORK



CLIENT ONBOARDING

ONGOING DUE DILIGENCE

EXIT

ID&V, incl UBO
Art. 3 + 33 Wwft

Sanction screening
Art. 2 RTSW

PEP screening
Art. 8 Wwft

High risk geographies
Art. 8 + 9 Wwft

Purpose & Nature
Art. 3 Wwft

Source of Wealth
Art. 8 + 9 Wwft

Source of Funds
Art. 3 (2)(d) + 9 Wwft

Client Risk Assessment
Art. 3 + 33 Wwft

CLIENT DATA

Required data Natural Person (illustrative)

- Names (first + middle + last)
- Date of birth
- Residential address
- ID doc: type, number, date, place
- Representative see above + mandate

Required data Legal Entity (illustrative)

- Legal form
- Statutory name
- Trade name(s)
- City, street, number
- Country of incorporation
- Registration number
- Business activities
- UBO: names (first + middle + last), size and/or nature beneficial relationship
- Representative: names (first + middle + last), date of birth, authority to represent

Sanction screening
Art. 2 RTSW

PEP screening
Art. 8 Wwft

High risk geographies
Art. 8 + 9 Wwft

Source of Wealth
Art. 8 + 9 Wwft

Source of Funds
Art. 3(2)(d) + 9 Wwft

Detecting unusual behaviour (TM)
Art. 2 + 3 + 8 + 9 + 16 + 23 Wwft; Art. 14 Bpr

FIU reporting
Art 16 Wwft

Actualisation data
Art. 3 + 8 Wwft
Art. 14 Bpr

Exit
Art. 5 Wwft

CLIENT DATA

- Data Natural Person
- Data Legal Entity

EXIT

ALERT GENERATION BASELINE EVENT CATEGORIES

- Customer risk
- Geographical risk
- Product / Services risk
- Channel risk
- Transaction risk

Client Filtering

Transaction Filtering

Transaction Monitoring

Client Monitoring

Other triggers

If hit:

CLIENT DUE DILIGENCE

Automated Event-Driven Review

Risk-differentiated Event-Driven Review

Comprehensive (manual) Event-Driven Review

If no hit:

CLIENT DUE DILIGENCE

Automated Periodic Review

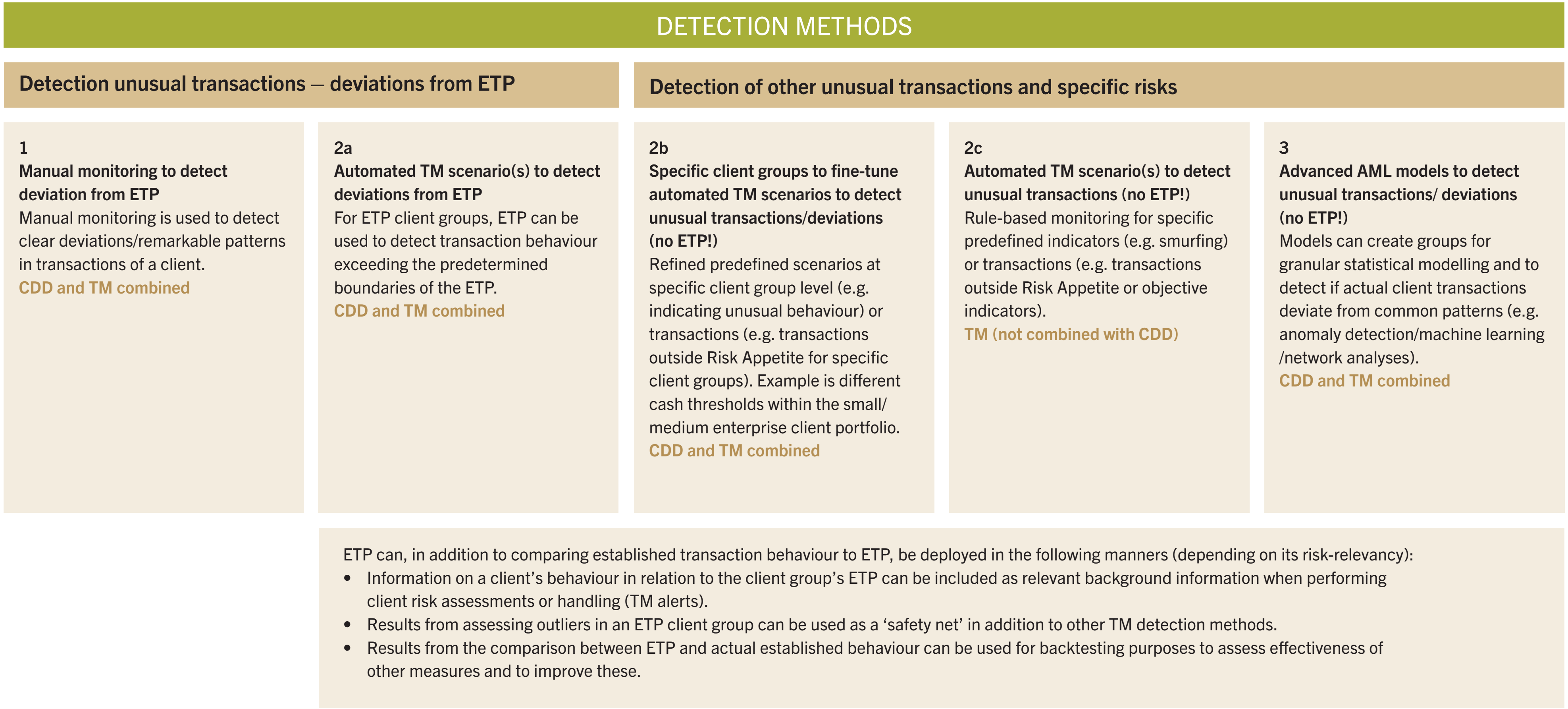
Risk-differentiated Periodic Review

Comprehensive (manual) Periodic Review

□ Regulatory requirement
▨ CDD & TM processes at Bank
■ Risk trigger mechanism /Models at Bank

Figure 1 – **Positioning ETP within Financial Crime Framework**

Based on SIRA, the bank defines mitigating measures, including transaction monitoring measures. ETP can be used to detect unusual transactions, as shown in the visual under 1 and 2a, in addition to rule-based TM and the use of advanced AML models (mentioned in the visual under 2b, 2c and 3).



DETECTION METHODS

Detection unusual transactions – deviations from ETP

1
Manual monitoring to detect deviation from ETP
Manual monitoring is used to detect clear deviations/remarkable patterns in transactions of a client.
CDD and TM combined

2a
Automated TM scenario(s) to detect deviations from ETP
For ETP client groups, ETP can be used to detect transaction behaviour exceeding the predetermined boundaries of the ETP.
CDD and TM combined

Detection of other unusual transactions and specific risks

2b
Specific client groups to fine-tune automated TM scenarios to detect unusual transactions/deviations (no ETP!)
Refined predefined scenarios at specific client group level (e.g. indicating unusual behaviour) or transactions (e.g. transactions outside Risk Appetite for specific client groups). Example is different cash thresholds within the small/ medium enterprise client portfolio.
CDD and TM combined

2c
Automated TM scenario(s) to detect unusual transactions (no ETP!)
Rule-based monitoring for specific predefined indicators (e.g. smurfing) or transactions (e.g. transactions outside Risk Appetite or objective indicators).
TM (not combined with CDD)

3
Advanced AML models to detect unusual transactions/ deviations (no ETP!)
Models can create groups for granular statistical modelling and to detect if actual client transactions deviate from common patterns (e.g. anomaly detection/machine learning /network analyses).
CDD and TM combined

ETP can, in addition to comparing established transaction behaviour to ETP, be deployed in the following manners (depending on its risk-relevancy):

- Information on a client's behaviour in relation to the client group's ETP can be included as relevant background information when performing client risk assessments or handling (TM alerts).
- Results from assessing outliers in an ETP client group can be used as a 'safety net' in addition to other TM detection methods.
- Results from the comparison between ETP and actual established behaviour can be used for backtesting purposes to assess effectiveness of other measures and to improve these.

1 Industry Baseline

This Industry Baseline describes the use of ETP as a method to detect deviations from expected transaction patterns and unusual transactions. It provides details on:

- purpose and scope of ETP as part of the alert generation framework;
- risk relevant use of ETP;
- determining ETP;
- criteria to demonstrate effective implementation;
- response to transaction behaviour diverting from the ETP in a risk-based manner.

1.1 Purpose and scope of ETP

The purpose of using ETP is to detect deviations or remarkable patterns when comparing expected transaction behaviour with actual transaction behaviour. A deviation from ETP could indicate a potential unusual transaction.

Only methods that explicitly detect deviations from the predetermined ETP by comparing expected transaction behaviour with actual transaction behaviour (which could indicate an unusual transaction), are considered as ETP. To enable this comparison, banks establish an ETP based on expected transaction behaviour for (groups of) clients, usually combining client characteristics with transaction data. Banks assess when a deviation exceeds the predetermined boundaries of the ETP, i.e. if the event constitutes a possible ML/TF risk where further investigation is needed.

Besides comparing with the ETP, banks also have other methods to detect specific unusual transactions or patterns or specific risks. These methods are designed for specific unusual transactions or specific risks and can also make use of peer groups. These methods are not referred to as ETP but might also use client characteristics, specific client groups, or even ETP client groups. Examples are:

- Use of specific client groups to tune automated TM scenarios to detect unusual transactions.
- Rule-based transaction monitoring for specific risk indicators (e.g. smurfing) or transactions (e.g. transactions outside risk appetite or objective indicators).
- Advanced AML/CFT models can create groups for granular statistical modelling and to detect if actual client transactions deviate from common patterns (e.g. anomaly detection, machine learning, network analyses).

1.2 Risk relevant use of ETP

Banks determine how and for which risks ETP is applied. ETP will be applied in scenarios where this method has relevancy to detect certain risk(s) and can be used in different ways. Depending on the risk there are multiple possibilities to use ETP.

1 To assess significant deviations of client behaviour in comparison with the client group's ETP. The comparison can be performed manually or automated (e.g. rule-based calculations on deviations from the client group's ETP in TM scenarios).

2 Information on a client's behaviour in relation to the client group's ETP can be included as relevant background information when performing client risk assessments or handling (TM) alerts. Example: a client periodically performs transactions ranging from e.g. €50-500 per transaction to an EC high risk third country to support family and behaves in line with the client group's ETP. When within ETP there is no need to perform EDD measures for this specific situation.

3 Results from assessing outliers in an ETP client group (specific types of transactions, amounts, number of transactions, etc.) can be used as a 'safety net', in addition to other TM detection methods, to detect deviations or potential unusual transactions that could otherwise go unnoticed and can indicate emerging risks. Banks should make thresholds used in outlier detection explicit and document the substantiation thereof. Risk relevancy is leading to determine thresholds.

4 Results from the comparison between ETP and actual transaction behaviour can be used for backtesting purposes to assess effectiveness of other measures and to improve these. For example, in case the comparison indicates a specific risk in a sector which has not been identified through

other scenario's, this could lead to improvement of scenarios.

The way an individual bank uses ETP should be defined and documented in their policies and procedures. With regard to the use of ETP banks can take additional measures to the ones described in this Industry Baseline but are not required to do so.

1.3 Determining ETP

There are different techniques to determine and maintain ETP. Banks decide on how they determine the ETP and document the process (incl. risk tolerance level, risk acceptance level, early warning level, etc.) ETP can be based on information provided by the client and/or be derived from client data and/or client behaviour after onboarding (e.g. by modelling). It is not required to define a unique ETP tailored to each individual client. Nor is it required to request information at client onboarding on their expected transaction behaviour. Client outreach in relation to ETP will be conducted when appropriate and in a proportionate way. It is not required to document the ETP in individual client files. The ETP's can be stored in a separate ETP database.

For example, an ETP can be established by using segmentation via peer grouping (groups of clients with common characteristics). Note that a change in client characteristics (e.g. a minor turning 18 or organization changing legal form) are indications that the ETP of the client changes, but should not in itself be considered as an alert or risk.

Examples of possible grouping characteristics

Natural persons
- Age group
- Residency
- Client size (assets under management)
- Client relationship type
- Type of products
- Length of client relationship

Legal entities
- Industry
- Residency
- Company size
- Legal form
- Type of products
- Length of client relationship

Examples of components of ETP

Activity
- volume of total transactions (incoming and outgoing)
- volume of non-domestic transactions (incoming and outgoing)
- volume of non-domestic with high-risk jurisdictions (incoming and outgoing)
- frequency of transactions (incoming and outgoing)

Type of transactions
- cash
- non-cash
- crypto

1.4 Risk response

Based on the risk relevant use of ETP (see 1.2), banks decide on the appropriate and proportionate risk response to client behaviour that deviates from ETP (e.g. based on frequencies and thresholds). The risk response needs to be sufficiently substantiated, documented and readily available for risk mitigation, internal controls and supervision. A risk response can be that a bank assesses transactions and reviews the risk classification of a client. In case a bank detects unusual transactions, they will report these to the Financial Intelligence Unit.

Note that an ETP related alert could also indicate atypical transaction behaviour which might be caused by outdated or incorrect information on the client, which results in an incorrect assigned ETP. Hence, this can be a reason to review the client and/or actualise the client data. Upon actualisation of the data, the client will (automatically) be placed in the correct ETP client group.

1.5 Client types

The method of implementing automated TM scenarios to detect deviations from ETP determined by the ETP client group is most effective when the bank can make homogenous groups. As a result of this condition of homogeneity, it might not be feasible to determine a meaningful ETP client group (e.g. rare client types; partnership set-up for a one-off transaction at an unknown point in time or a client with extreme fluctuating business activities). Banks can decide to establish an individual expected transaction profile or determine that an expected transaction profile is not feasible, with substantiation of the rationale.

1.6 Criteria to demonstrate effective implementation

Banks are required to demonstrate the effectiveness of their AML/CFT controls, which is bank specific as it is based on its risk appetite and corresponding AML/CFT approach.

Criteria for demonstrating effective AML/CFT controls include:

- Banks substantiate the use of controls – and thus the possible use of ETP – in their (SIRA) risk response and risk & control documentation. This shows how the bank builds and maintains a proportionate risk-based set of controls to mitigate ML/TF risks. Expected transaction behaviour of ETP client groups is translated into parameters as used in the bank's TM processes.
- Periodically, the method's effectiveness of capturing risks identified in the SIRA is evaluated, backtested and tuned.
- In order to measure effectiveness, a bank also exhibits the time and resources devoted to the risk-based controls aimed at detecting unusual transactions relative to the results of these controls [3].
- Banks present method(s) and evaluation results of effectiveness testing.
- Where a control, e.g. the use of ETP, 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 a bank's overall assessment of its risk-based controls [4].
- Sufficient substantiation of data integrity.
- Performing quality assurance by the 1st, 2nd and 3rd line of defence.
- When applying ETP client groups:
  - substantiation of the ETP client groups and/or specific client groups both encompassing statistical relevancy and client portfolio analysis (based on SIRA) to achieve homogeneity in ETP client groups.
  - document methodology (e.g. through scenarios, model features, threshold setting, outlier detection, etc.)
  - evaluate results of effectiveness testing related to capturing risks and correctness of ETP and specific client groups through data-driven insights.
  - improve ETP client groups (i.e. structural periodic controls on whether clients are allocated to the correct ETP client group). In case ETP client groups are ineffective due size, a decision should be made to adjust.

2 Impact

A risk-based design and use of ETP is crucial to avoid (frequent) outreach to clients to provide sensitive information on their transactions if there is no risk-relevancy for it, if this can also be determined through internal analysis or retrieved through open sources. In addition, not applying ETP in a risk relevant way, could lead to burdensome requests and disproportional measures towards clients.

The risk-based design and use of ETP will enable banks to execute more effective AML/CFT controls focusing on relevant risks and apply mitigating measures effectively. This is essential to avoid overcompliance where ETP has limited added value to mitigate AML/CFT risks, next to potentially more effective mitigating measures.

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

3 Use cases

Please note that the use cases below are examples to illustrate a practical application of this Industry Baseline and not intended to be exhaustive.

[3] Demonstrating Effectiveness (The Wolfsberg Group, 2021)
[4] Demonstrating Effectiveness (The Wolfsberg Group, 2021)

MINORS

2a – Automated TM scenarios to detect deviations from ETP

Example

A client is assigned to the ETP client group 'minors' through the common characteristics age group and product type ('minors' account). The client's ETP is determined based on statistics of the specific client group the client is part of (averages, standard deviations, etc.).

Industry Baseline

- An alert is generated when non-domestic transactions are detected which exceed the predefined expectations of the ETP client group.
- The alert must be assessed to determine the appropriate follow-up. Such a follow-up could require a change in risk classification of the client and/or additional mitigating measures.
- Periodically, the method's effectiveness of capturing risks as identified in the SIRA, and the client group's ETP ('underaged children') correctness is being evaluated, backtested and tuned.

PRIVATE LIMITED COMPANY

2b – Specific client groups to tune automated TM scenarios to detect unusual transactions or deviations

Example

A client is a private limited company (B.V.), which is a supermarket. The client is assigned to a specific client group through the common characteristics cash intensive industry, geography, size and legal form. The client's ETP was determined as part of the client group 'mid-sized supermarkets'.

Industry Baseline

- Unusual behaviour/transactions of the client are being detected through refined, predefined and automated TM scenarios. An alert is generated for this client when the total amount of cash transactions of the past month is outside the predefined threshold.
- It is assessed whether the deviation requires a change in the risk classification of the client and/or whether additional mitigating measures must be taken. Information on the client's behaviour in relation to the client group's ETP is used as relevant background information when assessing the alert.
- Periodically, the TM scenarios' effectiveness of capturing specific client risks as identified in the SIRA, and the specific client group's ETP correctness are evaluated, backtested and tuned.
- ETP can be used for backtesting purposes. Results from the comparison between ETP and actual established behaviour can be used for backtesting purposes to assess effectiveness of automated and refined TM scenarios, and to improve or refine the existing business rules and thresholds.

PEPS

2c – Automated TM scenario(s) to detect unusual transactions

Example

- A client who is a parent of a PEP (parent) whose transactions show a pattern of smurfing. The bank has a mature and sophisticated rule-based TM in place for specific predefined indicators and transactions.
- The client is also part of a specific client group 'retirees with average assets' through the common characteristics age group, income and assets. The alerted smurfing behaviour is not related to the ETP behaviour.

Industry Baseline

- An alert is generated for the client (parent of a PEP) whose transactions show a pattern of smurfing. It is assessed whether the deviation requires a change in risk classification of the client and/or whether additional mitigating measures must be taken.
- Periodically, the automated TM scenarios are evaluated, backtested and tuned.
- As a method to detect deviations or emerging risks that otherwise remain unnoticed, ETP could be combined with automated TM scenarios as a 'safety net'. Periodically, the top outliers within the ETP client group are assessed. This assessment could result in improvement of TM scenarios.

CORPORATE CLIENT GROUP

3 — Advanced AML models to detect unusual transactions/deviations

Example

The client is a corporate client group with accounts that are linked through a cash pool. Due to the different activities within the group, the amount and volume of the transactions in the cash pool are unpredictable and depend on many factors.

Industry Baseline

- This client does not fit in an ETP client group nor is it feasible to establish an individual ETP.
- Substantiation on why ETP methodology is not feasable for specific client groups is documented in risk and control documentation.
- Unusual transactions can be detected by other methods such as (specific) TM scenarios and advanced AML models.
- The model generates alerts which must be assessed whether the deviation requires a change in risk classification of the client and/or whether additional mitigating measures must be taken.
- Periodically, the AML models' effectiveness of capturing the specific client risks as identified in the SIRA are evaluated, backtested and tuned.

CONTEXT

Regulatory framework

The regulatory context on this topic is described in relevant parts of applicable laws, regulations and guidelines from various authorities, such as: EU, EBA, Ministry of Finance and DNB. Below an overview of the current regulatory framework with reference to ETP.

- **AMLD5 Article 13 (1, c-d)**
  "Customer due diligence measures shall comprise:…
  c assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
  d conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date."
- **EBA Guidelines on ML and TF Risk Factors, section 4.64**
  "EDD measures firms should apply may include:…
  Examples include:…
  Information about the intended nature of the business relationship to ascertain that the nature and purpose of the business relationship is legitimate and to help firms obtain a more complete customer risk profile. This may include obtaining information on:
  a) the number, size and frequency of transactions that are likely to pass through the account, to enable the firm to spot deviations that might give rise to suspicion (in some cases, requesting evidence may be appropriate);
  b) why the customer is looking for a specific product or service, where it is unclear why the customer's needs cannot be met better in another way, or in a different jurisdiction;
  c) the destination of funds;
  d) the nature of the customer's or beneficial owner's business, to enable the firm to better understand the likely nature of the business relationship."
- **Wwft Article 3 (2, c-d)**
  "Customer due diligence enables the institution to:
  c establish the purpose and intended nature of the business relationship;
  d conduct ongoing monitoring of the business relationship and the transactions carried out during that relationship to ensure that these are consistent with the institution's knowledge of the customer and its risk profile, and where necessary an investigation into the source of funds used in the business relationship or transaction."
- **Bpr Wft Article 14(4)**
  "The financial undertaking, or branch respectively, has established procedures and measures regarding to the analysis of customer information, including in relation to the products and services purchased by the customer, and with regard to the detection of deviating transaction patterns."

Relationship between '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 of 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 risk-based approach in more detail. Additionally it provides more practical examples on the use of ETP in different scenarios.