White Paper

4th EU Money Laundering Directive:

Applying the intensified risk-based approach when evaluating risks of persons and transactions

A practical guide for Compliance Officers in financial institutions

actico
Smarter Decisions

TABLE OF CONTENT

1. Introduction

This white paper summarizes the key content of the Fourth EU Money Laundering Directive and Funds Transfer Regulation and highlights its impact on companies. The focus is on the risk-based approach with which obligated parties (credit and financial institutions, as well as service providers from the non-financial sector) are required to screen business relationships and financial transactions for money laundering scenarios.

With an eye to practical implementation, the white paper shows how software solutions can be used to implement Anti-Money-Laundering milestones: risk classification, monitoring, clarifying, and auditable documentation. These recommendations primarily illustrate the risk-based approach, which focuses on analyzing cases, drawn from the entire body of data, that pose a genuine risk.

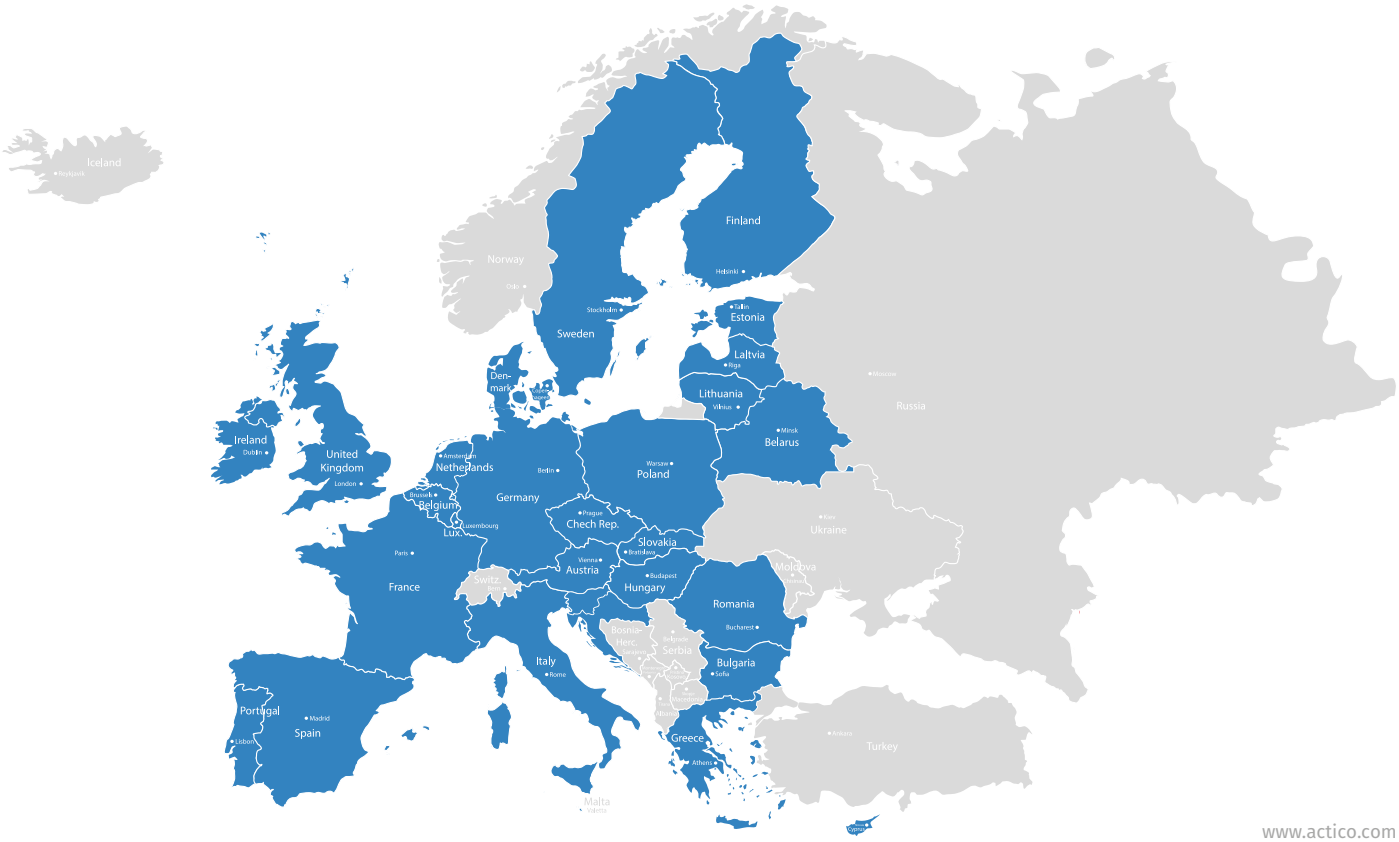
2. New AML Legislation: Challenges for financial institutions

The European Parliament and the council passed the Fourth Anti-Money-Laundering Directive (EU) 2015/849[1] on May 20, 2015. It was aimed at preventing the use of the financial system for the purposes of money laundering or terrorist financing.

Following the revelations of the Panama Papers, policy makers now want to go a step further and strengthen anti-money-laundering legislation. Germany's Federal Ministry of Finance presented a 10-point action plan for a fair international tax system and more effective international action against money laundering. At its heart, the plan seeks to improve tax transparency through automatic information exchange among nearly 100 states, make changes to corporate law, identify business advantages, and create a global network of national money laundering registers as specified in the Fourth EU Anti-Money-Laundering Directive.

In November 2016, the German Ministry of Finance published the draft of a new law (known as Panama law) against tax evasion. The Panama law will be used to put the 10-point-action plan into effect.

Credit and financial institutions, as well as the non-financial sector find themselves confronted with a raft of new requirements. The task now is to plan for the changes in the process landscape, and not only meet statutory requirements, but also protect their reputations and those of their customers.



3. Monitoring business relationships and transactions[2]

The risk-based approach requires obligated entities to rate the money laundering risk of each individual business relationship and transaction. Circumstances that the Third Money Laundering Directive automatically categorized as low risk – such as when a customer was another institution, a listed company or a national authority – will in future simply be considered single "risk factors". Only a comprehensive evaluation of all relevant risk factors can serve as the basis for a final rating determining whether an individual situation must be considered a high or low risk. An obligated entity is a person or company subject to the Fourth Anti-Money-Laundering Directive. In addition to credit and financial institutions, this includes specific service providers in the non-financial sector, such as notaries, lawyers, and gambling service providers.

The goal is to prevent automatisms when conducting risk analysis. However, this approach is overridden when specific high-risk situations are evaluated. Politically exposed persons (PEPs), correspondent relationships, and customers from specific high-risk countries will automatically be categorized as high-risk situations. The EU Commission will publish a negative list of "high-risk third countries". The existing approach of keeping a positive list with equivalent third countries will be discontinued.

The Directive also contains new requirements for complying with the risk-based approach at the state level. In future, every Member State must compile and maintain a national risk analysis. Furthermore, the ESAs will draft a joint opinion on the money laundering and terrorist financing risks for the financial sector of the European Union. The opinion will be incorporated into a supranational risk report to be drafted by the EU Commission. The Directive also explicitly calls on national supervisory authorities to begin exercising a risk-based supervisory approach.

3.1 Customer due diligence

There are various due diligence obligations with regard to business partners.

- Simplified or enhanced customer due diligence
- Customer due diligence for life or investment-related insurance
- Due diligence for cross-border correspondent relationships
- Due diligence for politically exposed persons

The target is to know business partners as well as possible. One of the requirements of Article 13 is identifying the customer and verifying the customer's identity on the basis of documents, data, or information obtained from a reliable and independent source. This also applies to legal persons, trusts, companies, foundations and similar legal arrangements. The aim is to obtain information on the purpose and intended nature of the business relationship.

Continuous monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship must ensure that the transactions being conducted are consistent with the obligated entity's knowledge of the customer, and the business and risk profile, including, where necessary, the source of funds.

3.2 Beneficial ownership information

Article 30 requires Member States to ensure that companies registered in their territory and other legal persons collect and store appropriate, precise, and current information about their owners, including provision of accurate information about business interests. Each Member State will maintain this information in a central register.

3.3 Policies, procedures, and supervision

Article 45 requires obligated entities which are part of a group to implement group-wide policies and procedures, including data protection policies and procedures for sharing information within the group for AML/CFT purposes. Member States shall require obligated entities operating establishments in another Member State to ensure that those establishments respect the national provisions of the other Member State implementing this Directive.

3.4 Sanctions

According to Article 58, Member States shall ensure that obligated entities can be held liable for breaches of national provisions transposing the Directive in accordance with Articles 59 to 61. Any resulting sanction or measure shall be effective, proportionate, and dissuasive. For credit or financial institutions, the following sanctions can be applied in the case of a legal person: at least EUR 5 Million or 10% of the total annual turnover.

Member States shall ensure the publication of their decision to impose an administrative sanction or measure for breach of the national provisions transposing the Directive against which there is no appeal.

4. Regulation of information accompanying transfers of funds

Directive 2015/847[3] of the European Parliament and the Council of May 2015 replaces Directive 1781/2006. This new directive is not part of the Fourth Anti-Money-Laundering Directive but is important for financial institutions with regard to transaction control.

According to Article 9, the full traceability of transfers of funds can be a particularly important and valuable tool in the prevention, detection, and investigation of money laundering and terrorist financing, as well as in the implementation of restrictive measures. It is therefore appropriate, in order to ensure the transmission of information throughout the payment chain, to provide for a system imposing the obligation on payment service providers to accompany transfers of funds with information on the payer and the payee.

Article 16 states that in order to avoid impairing the efficiency of payment systems, the obligation to check whether information on the payer or the payee is accurate should be imposed only for individual transfers of funds that exceed EUR 1,000, unless the transfer appears to be linked to other transfers of funds which together would exceed EUR 1,000, the funds have been received or paid out in cash or in anonymous electronic money, or there are reasonable grounds for suspecting money laundering or terrorist financing.

5. Increasing technical requirements in Compliance

Money-laundering prevention, identifying persons on sanctions lists, and monitoring financial transactions place high demands on the performance of IT systems in financial institutions. This is partly due to the intensification of screening scenarios, but also to the steady increase in data volume. The number of at-risk persons and PEPs in sanctions lists rises daily and they must be checked against customer data regularly.

But persons and companies are not all that need to be screened for sanctions violations; even financial transactions have to be scrutinized. If monetary transactions with high-risk countries, banks, or persons are suspicious, execution of the transaction must be halted. Depending on the size of a financial institution, an IT system must be capable of analyzing up to 2 million transactions per hour and delivering the results within a few seconds.

6. Implementation of the risk-based approach

In order to detect suspicious business transactions as accurately as possible, it is important to differentiate between persons and transactions in analysis. Private or retail banking, retail or corporate business, institutional investors or brokerages have business relationships that each demonstrates a different business behavior. While high volumes of money flow in and out of corporate accounts on a near daily basis, this is unusual in the accounts of private customers. So if an unusually large transaction occurs in the account of a private customer, a compliance officer should look into the matter.

Institutions that assign risk classes to all of their customers and business relationships that regulate evaluation of potential risks obtain the best analytical results. For example, the analysis of a high risk could mean that crediting a payment could be delayed until the case is resolved. It is also important to assign a separate risk class for politically exposed persons because, from a compliance perspective, they require special attention and are considered “high-risk situations” in the new money laundering directive.

6.1 Risk classification in the Know Your Customer (KYC) profile

KYC identity checks are necessary not only for new customers, but for existing customers as well. At a minimum, institutions are required to identify the contractual partner, determine beneficial ownership, and evaluate economic background. Every business relationship is subject to different logic. Here are some examples:

- Is the customer in private or retail banking or involved in the commercial banking business?
- Is it an institutional investor or broker?
- What kind of business does the bank expect to conduct with the customer (credit, deposits, transactions with foreign business partners)?

For the various banking activities, there are different business behaviors. For instance, corporate accounts have high inflows and outflows of money. For a private account, this transaction pattern would be more unusual and would be considered a potential risk. Further analyses by client type might include country risk, transaction behavior, legal status, financial circumstances, industry, politically exposed persons or professions.

6.2 Checking customer data against sanctions list entries

Screening of customer data against national and international sanctions lists is one of the risk management tasks expected of financial institutions. A large selection of public and commercial sanctions lists is available on the market. Many institutions have even started using several lists concurrently. Automatic checks usually include names, aliases, alternative name spellings, dates of birth, nationality, and domicile. Institutions regularly screen all of their customers and business relationships – usually once a day. To avoid runaway screening costs, it is good practice to fine-tune results so that institutions end up with a list of only the truly relevant suspicious cases.

6.3 Know Your Transaction (KYT): Monitoring transactions

Monitoring payment transactions is part of the KYT principle. To find out whether a transaction poses a risk, an analysis must be performed to determine whether the initiator or recipient is on either an internal or external blacklist, whether limits are complied with, which countries are involved, the reason for payment, and the customer's history.

It is also a good idea to analyze transaction patterns. This means that the analysis takes not only individual transactions into account, but also the connection between a number of payments. Inflows and outflows occurring within a brief period can be an indication of money laundering. Smurfing is another technique in which large transactions are broken down into smaller tranches. In practice, numbers of financial transactions are subject to seasonal fluctuation. Banks have to be capable of reliably analyzing the transaction spikes that occur on weekends, before holidays, and at the end of the month or year, which are generally higher than volumes on other days.

Throughout the duration of the customer relationship, it makes sense to collect baseline data for risk classification from transaction behavior. For example:

- Assets and number of transactions
- Overall cash turnover within a defined period
- Total turnover in relation to assets
- Cash turnover in relation to assets
- Transactions and the amount of turnover with high-risk countries within a specified period

In the final determination of risk, it is important to place the numbers in context. For instance, it makes sense to differentiate between threshold values for retail, corporate, and private banking clients. This makes it possible to classify transactions from corporate customers with high-risk countries as less critical than transactions with high-risk countries initiated by private persons.

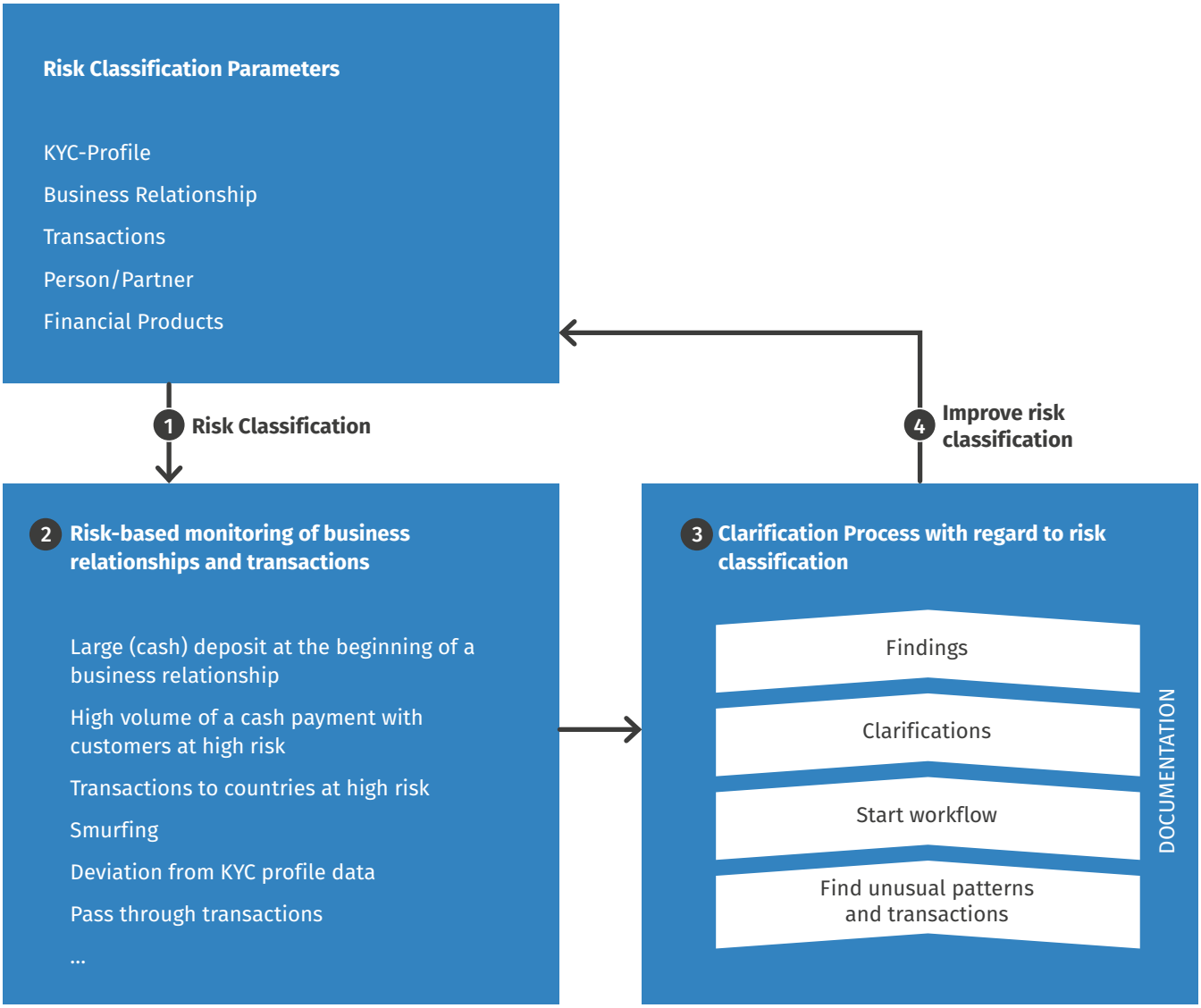
6.4 Monitoring rules for persons and transactions

All monitoring scenarios, regardless of whether the analysis is of personal or transaction-related data, are defined by rules. Below are some examples:

- What is the maximum transaction amount for private clients?
- How high is the limit for financial transactions for corporate clients?
- What is the customer's risk class?
- How is a particular risk customer classified (PEP, crime, terrorist)?
- What is the nature of payment transactions between two business partners internally in the bank or with external payees?
- Which countries are on a sanctions list?

6.5 Milestones in automated money-laundering prevention

For reasons of time and cost, and also due to steadily increasing data volumes, money-laundering prevention must be automated and to the greatest extent possible generate only truly relevant results. If a risk is identified, it must be checked by a compliance officer. The most important milestones for effective anti-money-laundering measures are: risk classification, monitoring, clarification, and auditable documentation.



7. ACTICO Money Laundering Detection System (MLDS)

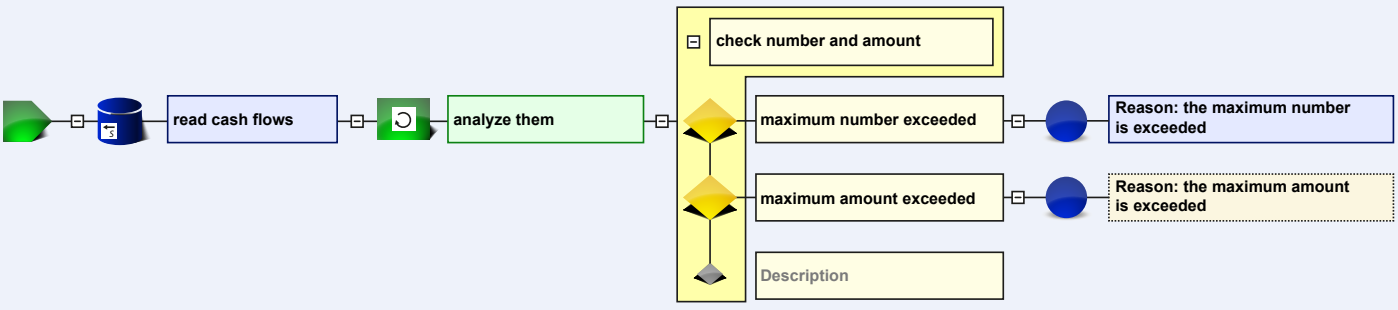
The ACTICO Money-Laundering Detection System (MLDS) helps banks and financial institutions make operational decisions. It is a technical analysis that offers insights into whether persons and financial transactions represent a money-laundering scenario.

7.1 Automated analysis with Business Rules Management

Rules prescribed by lawmakers for identifying customer, product, and transaction risks can be loaded into MLDS. Internal institution rules can also be included.
Rules are modeled on a graphical interface. The ACTICO Compliance Agility Package, which is integrated into MLDS, forms the basis. It enables even personnel who are not experts in IT – compliance staff, for instance – to model and tune money laundering rules. The complete body of rules comprises the business logic.

To screen business relationships and transactions, data are checked against defined sets of rules and yield so called “alerts”.

Three steps to detect and classify risk transactions



1 *Read cash flows in MLDS*

2 *Make automated decisions: Analyze cash flows (maximum number and amount)*

3 *Display reasons for classifying cash flows as risky transactions*

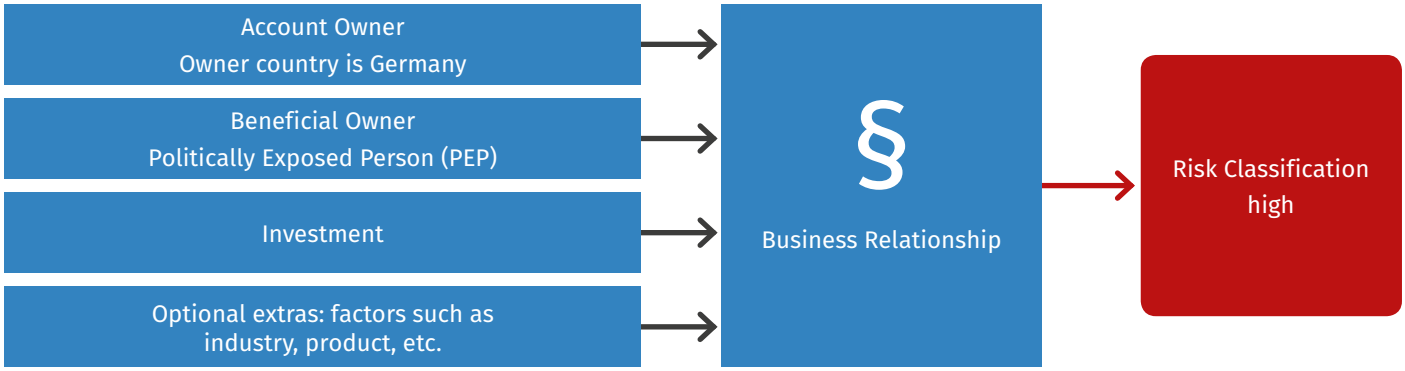
Business rules in MLDS to determine the size and number of cash flows. In addition to the analysis, the system substantiates the reason for the report of a high-risk transaction.

7.2 Substantiation of risk

MLDS always provides a detailed justification for the risk classification. This makes it possible to provide evidence directly from the system indicating why a customer or business relationship was classified as high-risk.

This example explains the risk classification of a business relationship. It consists of an account owner, a beneficial owner, and a financial investment. In MLDS, the politically exposed person leads to the risk classification “high” resulting in enhanced customer due diligence.

The risk factors and their weighting having an impact on the rating rules can be derived from the financial institute’s risk analysis. They are represented in ACTICO Rules. Any additional data, such as industry, product, etc., can also be taken into account to classify the risk.

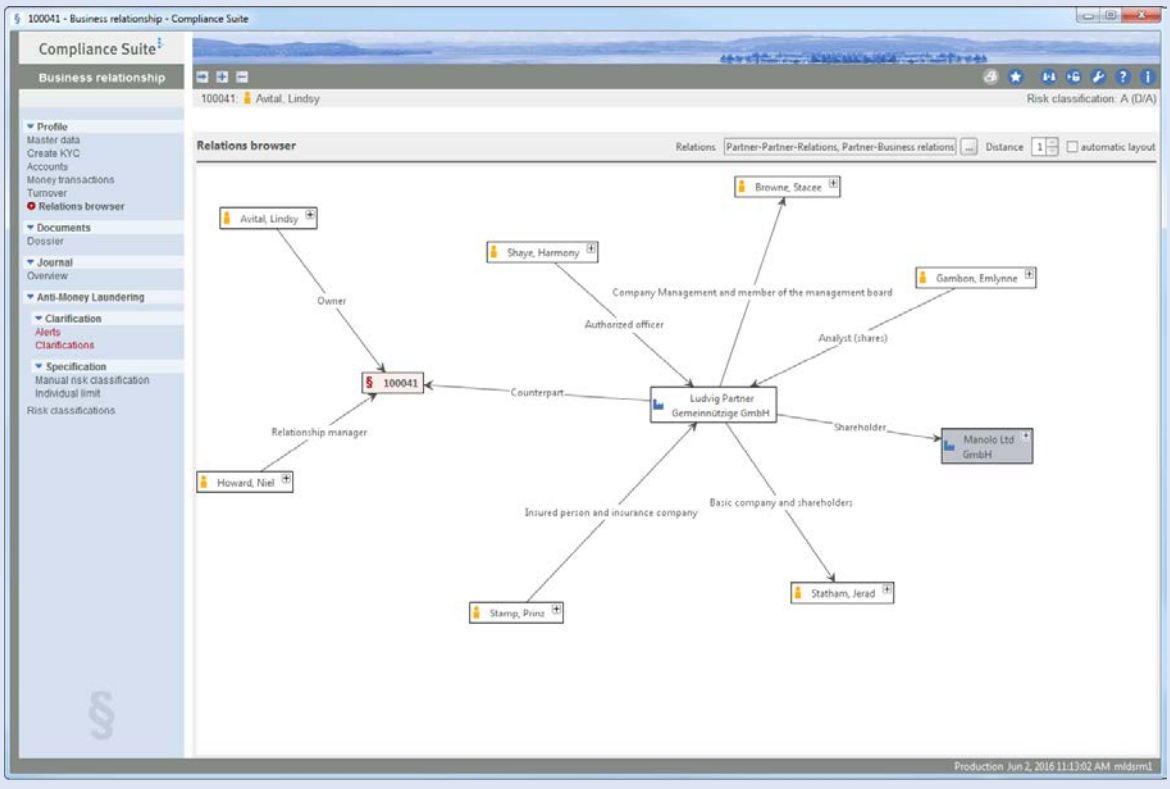


7.3 Automated documentation and historization

All data updates that are relevant to due diligence must be documented to prove why and when each risk assessment was made, and what clarification processes were performed. When assessing the risk of a business event, the automated documentation stores all customer information the risk of a business event, including the transaction history and all transaction details, in the form of a compliance journal. The journal cannot be deleted and is therefore the auditable documentation of due-diligence efforts.

The documentation helps meet the information requirements of authorities with regard to assessing client risk in the context of the risk analysis.

7.4 Display of transactions of a customer and his relationship network and relationship network



MLDS spotlights not only individual persons, but also their relationship networks. This includes KYC items and threshold values and countries on the negative list.

8. Conclusion

The Fourth EU Anti-Money-Laundering Directive requires obligated institutions (credit and financial institutions, as well as service providers from the non-financial sector) to intensify their risk-oriented efforts. Each individual business relationship and transaction must be screened for money laundering risk. Obligated organizations must also be capable of monitoring information and data streams to ensure reliable detection of risks arising from business relationships and transactions. Due to the growing data volume in the digital world, software has to decide automatically which risks are truly relevant, and then initiate measures resulting either in additional clarification, for instance, or a halt to the financial transaction.

In practical implementation, risk screening through the use of business rules in a business rules management system such as MLDS has proven effective. Within seconds, countries on the negative list or threshold values for money flows can be migrated to existing data. New, legally-mandated checks of PEPs, corresponding bank relationships, and limit values for electronic transfers or linked transactions not permitted to exceed EUR 1,000 can all be represented transparently with rule sets. Last but not least, high transparency offers synergies in terms of legal security for the company and operations department. Understanding customers and their business behavior helps companies identify sales potential.

9. Outlook: Fifth EU Money Laundering Directive[4]

In July 2016, the European Commission adopted a proposal to further reinforce EU regulations on anti-money laundering to counter terrorist financing and increase transparency about who really owns companies and trusts.

This proposal, amending the Fourth Anti-Money Laundering Directive, is intended to complement the existing preventive legal framework in place in the Union by setting out additional measures to better counter the financing of terrorism and to ensure increased transparency of financial transactions and legal entities.

Sources:

1 *Fourth Anti-Money-Laundering Directive (EU) 2015/849, http://eur-lex.europa.eu*

2 *Hans Martin Lang, Jan Noll, 2015, Adoption of the Fourth European Money Laundering Directive and New Funds Transfers Regulation, www.bafin.de*

3 *REGULATION (EU) 2015/847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, http://eur-lex.europa.eu*

4 *European Commission – Press Release dated 5 July 2016, http://europa.eu*

ACTICO

EMEA

ACTICO GmbH
Ziegelei 5
88090 Immenstaad
Germany

info@actico.com
www.actico.de

Americas

ACTICO Corp.
200 S. Wacker Dr.
Suite 3100
Chicago, IL 60606/USA

info@actico.com
www.actico.com

Asia & Pacific

ACTICO Pte. Ltd.
11 Bishan Street 21
Singapore 573943

info@actico.com
www.actico.sg

ACTICO is a leading international provider of software solutions and technologies for decision management.

In a digital world, it is necessary to process large volumes of data and make real-time, consistent and auditable decisions. ACTICO software allows companies to implement highly flexible applications to optimize their daily decision-making on a continuous basis. This enables them to accelerate growth, innovate effectively, stay compliant and as a result, increase profits.

ACTICO offers solutions in these areas:

- Credit Risk Management: Monitor, assess and manage credit risk
- Loan Origination: Automate credit decisions
- Compliance: Enable transparency, avoid fraud and comply with regulations
- Client Management: Process sensitive customer data securely – from onboarding to reporting
- Underwriting & Claims: Make claim settlement processes quicker, consistent and cost-effective

Since 1997, ACTICO has delivered software and services to our customers' benefits. Headquartered in Germany with offices in USA and Singapore.

More information at **www.actico.com**

01/2017 FE