TEMENOS

Risk-Based Approach in Financial Crime Mitigation

A Cookbook

Introduction

Managing risks is the supreme discipline in banking. Most financial institutions (FIs) are accustomed to manage risks in areas like credit risk or market risk where risks can be rather easily calculated and quantified and where FIs assess these risks prior to accepting them. However, assessing the financial crime[1] risks differs from the "normal" risk assessment, as it is a "consequential" risk. This means that financial crime risks with some customers may only become evident once the customer began transacting through the account. This is the reason why monitoring of customer transactions is a fundamental component of the Risk-Based Approach (RBA).

Hence, financial crime risks reflect an FIs external and internal environment including mitigating controls. Best practices for financial crime risk assessment include quantitative and qualitative methodologies.

FATF, EU anti-money laundering directives, US BSA/AML and many other national legislations put the RBA at the centre of Anti-Money-Laundering (AML) and Combating the Financing of Terrorism (CFT) regimes. As criminals seek to launder proceeds gained from financial crime through the financial system, the focus on the RBA is on money laundering (ML) risks.

ML risks are generally understood to include terrorism financing (TF), bribery & corruption and other serious offences and types of financial crime[2].

1. Financial crime is defined as crime that is specifically committed against property. These crimes are usually committed for the personal benefit of the criminal, and they involve an illegal conversion of ownership of the property that is involved.
2. The 6th Anti-Money Laundering Directive (6AMLD) lists 22 serious offences that fall under ML risks.

Risk Management Process

Strong Governance from a bank's Board and Senior Management sets the tone from the top and resonates in an FIs overall Risk Management Framework. A robust risk awareness ensures allocation of clear responsibilities and driving continual enhancements.

The risk assessment forms the basis for an FI's RBA and reviews robustness of all three lines of defence, embedded good practices, and whether updates to the identified key risks and their red flags are understood.

The Risk Management Process as described in the standard ISO 31000:2018[3] is an integral part of a company's Risk Management Framework, which follows the PDCA cycle (Plan – Do – Check – Act) from W. Edward Deming[4]. The structure of this standard aims to integrate and include actual and future internal and external changes into management decisions in order to optimize and improve strategic and operational process goals. The PDCA cycle is a proven and well-established problem solving principle.

"Do" of the PDCA cycle invokes the risk management process. Once the context is set, i.e. the scope defined, the risk assessment runs through the steps to identify, analyse and evaluate risks. Management of risks includes the decision to treat, tolerate, transfer or terminate a risk. The results of each step in the risk assessment and managing risks provide input to monitoring and review and for the communication to senior management, auditors and regulators.

For each step and decision taken, the FIs need to ensure proper documentation with substantiations and underlying facts and statistics.

This approach to risk management (and risk assessment to set the basis for RBA) is widely used in the financial industry and other industries. FATF[5] , Wolfsberg Group[6], EU AML Directives, U.S BSA/AML Risk Assessment[7], Basel Committee on Banking Supervision (BCBS), Hong Kong Monetary Authority (HKMA) or Monetary Authority of Singapore (MAS), all apply generally the same steps for their risk assessment methodologies in ML/TF.

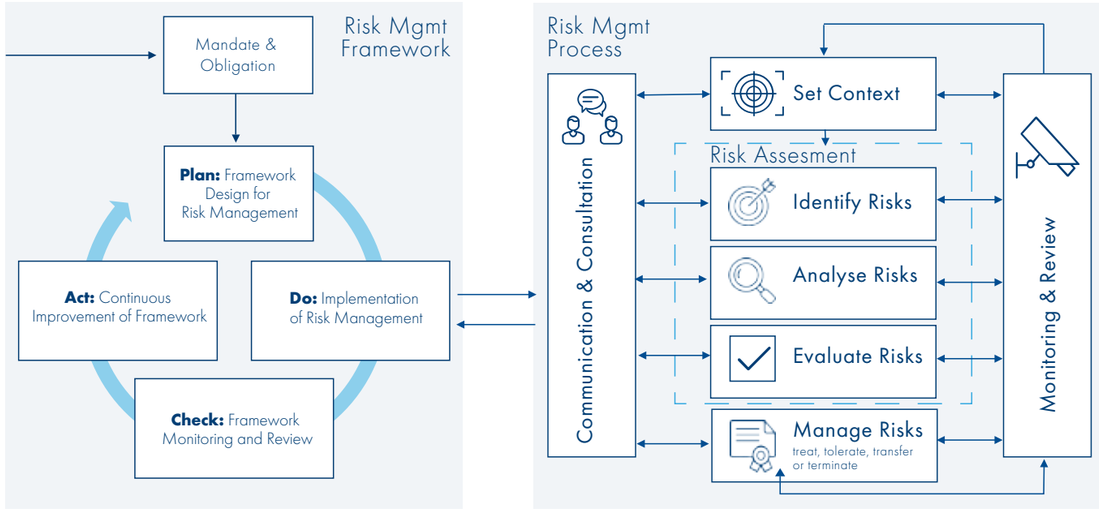


Figure 1: Risk Management Framework and Process – ISO 31000:2018

3. Financial crime is defined as crime that is specifically committed against property. These crimes are usually committed for the personal benefit of the criminal, and they involve an illegal conversion of ownership of the property that is involved.
4. W. Edward Deming developed the PDCA Principle for Quality Management in the late 1940s, which is also frequently used in other areas like strategy implementation on corporate level.
5. http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf
6. https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/15.%20Wolfsberg_RBA_Guidance_%282006%29.pdf
7. https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_005.html

History of Risk-Based Approach

In the early 1990s, when legislation regarding KYC (Know-Your-Customer) and Anti-Money Laundering (AML) came into force in many countries, there was a mainly a check-box approach to risk assessments, applicable to all banking business models. This had the undesired effect that banks potentially missed real risks, to which they were exposed.

Obviously, this approach was doomed to fail as the risks e.g. in retail banking are substantially different compared to the ones in institutional banking.Hence, banks with their compliance efforts frequently failed to meet regulatory expectations.

In 2007, FATF introduced the first attempt of a RBA with the intention to create processes that are more pragmatic. The result, however, was widespread confusion on how to interpret the guidelines and highly complex processes.

The FATF revision in 2010 brought much clearer definitions of RBA and the concept of "effective risk-based controls", which makes national legislators responsible for defining what is deemed to be effective. Since then, many regulators now use the term "effectiveness" in their guidance and discussions with the FIs. Finally, the FATF revision of the 40 Recommendations in 2012 requires countries to assess and understand their ML- and TF- threat risks.

Risk Assessment

In January. 2014, the Basel Committee on Banking Supervision (BCBS) issued a document about "Sound Management of Risks related to Money Laundering and Financing of Terrorism"[8] which includes the statement on the importance and conduct of a risk-assessment:

> "Sound risk management requires the identification and analysis of ML/FT risks present within the bank and the design and effective implementation of policies and procedures that are commensurate with the identified risks. In conducting a comprehensive risk assessment to evaluate ML/FT risks, a bank should consider all the relevant inherent and residual risk factors at the country, sectoral, bank and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied."[8]

The Wolfsberg Group defines risk assessment as an exercise that is "used to identify key risks faced by the firm and to test the controls that a firm has in place to mitigate these risks. Risks can be both external and internal to the firm. The risk assessment aims to measure the total exposure a firm has to the risks it faces and to plan actions to reduce these risks."[9]

National regulations require FIs to demonstrate strong governance and a robust risk awareness within their organisations, backed and supported with an effective execution. The risk appetite is a key influence upon a firm's strategic goals and drivers, which amount and type of risks the firm is willing and able to accept and which measures are needed to control these risks.

8. https://www.bis.org/bcbs/publ/d405.pdf
9. https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf

Strong Governance
Clear risk appetite and responsibilities, tone from the top, continual enhancements

Risk Awareness
AML/CFT risk awareness and accountability across all three lines of defence

Effective Execution
Good practices embedded, key risk understood and red flags continually updated

Figure 2: Governance, risk awareness and execution

Purpose of Risk Assessment

Improvements in financial crime risk management is the key purpose of a risk assessment through:

1. Identifying general and specific ML risks that an FI faces.
2. Determining how the FI can mitigate these risk with its AML programme controls.
3. Establishing the residual risk that remains.

The results of a risk assessment serve many aspects and include:

- Identification of gaps or opportunities for improvement in AML policies, procedures and processes
- Allocation of resources and technology spend
- Assistance of management to understand how an FI's AML compliance program aligns with its risk profile
- Development of risk mitigating strategies and controls to reduce an FI's residual risk exposure
- Ensurance that both, management and regulators, are aware of key risks, control gaps and remediation efforts

10. http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions/Anti-Money-Laundering-and-Countering-the-Financing-of-Terrorism/Guidance-Papers/2018/Guidance-for-Effective-AML-CFT-Transaction-Monitoring-Controls.aspx

Scope of a Risk Assessment – as Baseline for RBA

Historically, the risk assessment would have covered ML and TF risks and focused on customers, transactions and more traditional forms of ML. Over time, additional types of financial crime became predicate offences, such as fraud of various kinds, insider trading and market manipulation and tax evasion besides ML and international sanctions, TF, bribery and corruption. FATF 2012 names a long list of offences[11], which lead to ML at the end, and which an FI should be able to detect with their AML procedures.

Depending on the specific business model, lines of business and customer base of an FI, the risk assessment may involve some or all of the predicate offences. Whichever scope an FI applies, it must ensure that it is clearly articulated (i.e. assessed factors, criteria used for scoring, applied weightings), approved by management and well documented.

Organisation of a Risk Assessment

Most national legislations require an annual reporting on the status of the ML risk environment of an FI. As undertaking a risk assessment is a rather complex and resource-intense exercise, FIs should at least conduct an annual review of their risk assessment methodology in order to ensure that changes of internal and/or external factors are properly incorporated. This helps to have the most accurate picture of the ML risks.

Depending on who owns and manages the risk assessment, the context and how the risk assessment is conducted (by business line, country or enterprise-wide) may differ substantially.

11. Such as organised criminal group, human trafficking, sexual exploitation, drugs/weapons/stolen goods trafficking, extortion.

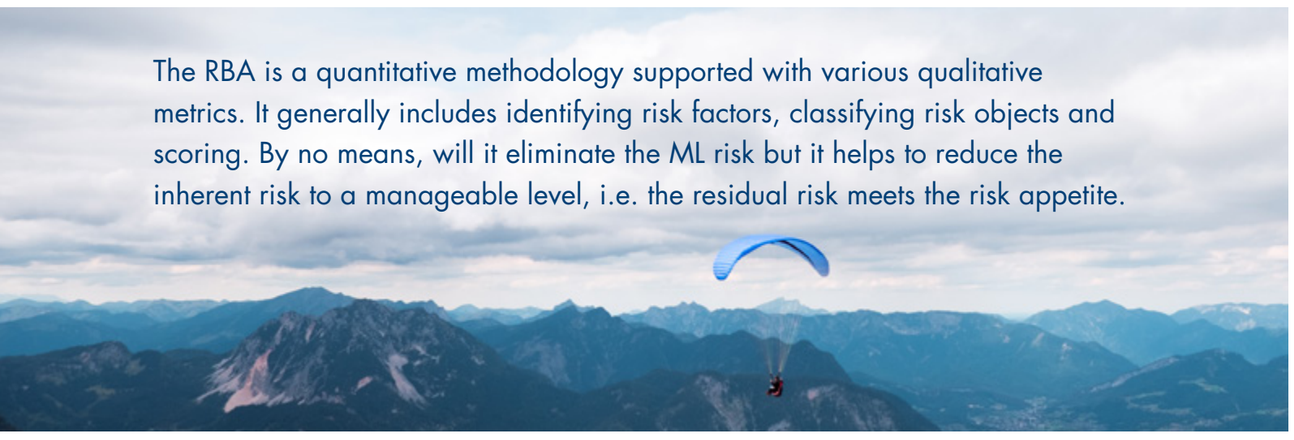
Risk–Based Approach (RBA)

"Means an approach whereby competent authorities and obliged entities identify, assess and understand the Money Laundering (ML) and Terrorist Financing (TF) risks to which subjects of assessment are exposed and take Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) measures that are proportionate to those risks."

EBA – European Banking Authority

The Wolfsberg Statement (2006, FAQs 2015) regarding the risk-based approach for money laundering risks states: "A reasonably designed risk-based approach will provide a framework for identifying the degree of potential money laundering risks associated with customers and transactions and allow for an institution to focus on those customers and transactions that potentially pose the greatest risk for money laundering."

The RBA is a quantitative methodology supported with various qualitative metrics. It generally includes identifying risk factors, classifying risk objects and scoring. By no means, will it eliminate the ML risk but it helps to reduce the inherent risk to a manageable level, i.e. the residual risk meets the risk appetite.



Important to know

Regulators imposed heavy fines in the last couple of years for AML failures and increased personal liability of senior management. As a result, C-Suite and compliance professionals drive to keep the FI (and themselves) safe. This led to the tendency to overly complicate the risk assessment processes and the RBA, with the result that the implemented controls are not always commensurate with the actual risks.

Instead of implementing a very detailed, complicated and complex RBA, it is more beneficial for an FI to have a leaner RBA, which is well documented, understood by all employees and implanted in an FI's compliance culture and DNA. Briefly: Less is more.

RBA not only applies to KYC/CDD and customer risk scoring but also transaction and customer screening against watch lists, PEPs lists and sanctions lists as well as transaction monitoring for suspicious activities in ML and fraud. In these disciplines, the chosen RBA influences the specific configuration and parametrisation, e.g. in watch list screening the level of fuzziness or in transaction monitoring the ML and fraud scenarios. Analytics and statistics from these financial crime mitigation systems may feedback to risk factors.

FIs should document and periodically review their risk assessment approach.

Risk Categories

The last two FATF revisions in 2010 and 2012 provided guidelines that are more "workable" to FIs and additionally build the basis for national legislations. As a result, the RBA consists of two distinct pillars:

1

The **country pillar**, where each individual government needs to understand its specific vulnerability to ML through a national risk assessment, an important pillar for an FIs robust AML strategy.

2

The **"own-internal-risk-assessment"** pillar, where each individual FI needs to assess own ML/TF-threat risks in context with the national risk.

Derived from the two pillars, the risks an FI is facing can be grouped in four clusters:

Vulnerability to serious and predicate offences of a specific business line. FATF 2012 names a long list of predicate offences, which impose greater obligations on banks to implement monitoring systems that detect proceeds possibly linked to these offences. Therefore, the questions to answer are: "Are we vulnerable to any of these offences? If yes, what is the magnitude of the vulnerability?"

Firm's inadvertent ML risk to create an environment that allows or promote money laundering, and includes the potential lack of a sound culture of compliance within an FI. The questions to answer are: "Are there any gaps in our controls that can be exploited by criminals? Do our controls promote an environment where money laundering can slip through?"

ML/TF risks inside the FIs sub-divided into customer, country, products & services, industries and channels risks

Regulatory risk to not adequately measure up to expectations. The fear of regulatory failures can lead to a disproportionate interpretation of the requirements and at the end increase the regulatory risk.

The risk clusters Vulnerability, Inadvertent ML risk and Regulatory risks are externally driven risks, which FIs need to take into consideration when creating their own RBA with risk factors, criteria for scoring, weightings and scoring methodology. The sum of the risks within the four clusters equals to the inherent risk of an FI before risk mitigation measures and control effectiveness are applied. The remaining residual risk, which FIs manage with a set of strategic and tactical measures, mirrors the FIs risk appetite.

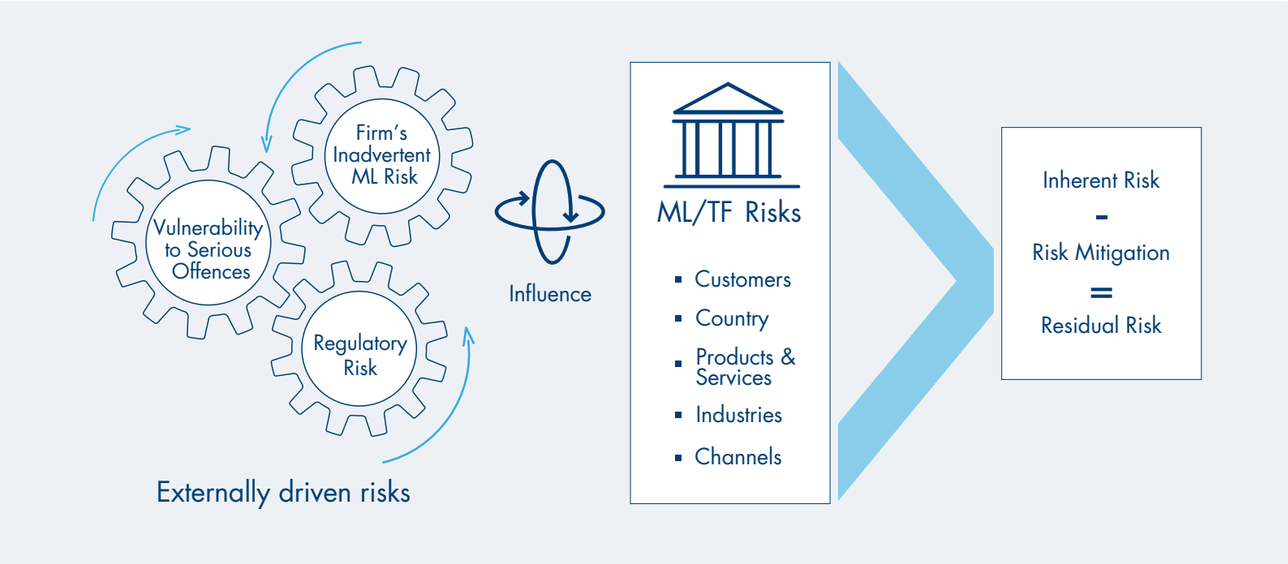


Figure 3: External driven risks influence inherent risk

Conventional/ Standard ML Risk Assessment Methodology

Generally, there is not a "One-size-fits-all" RBA for all FIs, as business models and associated ML/TF risks greatly vary. However, from the many ways to assess risks the conventional or standard ML risk assessment is the most commonly used approach.

It highlights the variety of recommended controls to mitigate risks in order to reduce the residual risk until it matches the FIs risk appetite. Defining an FIs RBA can be a challenging undertaking. Hence, thinking in risk scenarios, can help to identify the ML and TF risks of business lines, customers, products, services, industries and occupations or distribution channels.

Inherent Risk

The inherent risk represents the exposure of an FI to ML, sanctions, bribery & corruption risk before risk mitigating controls and measures are applied. Each of the inherent risk categories include sub-categories with inherent risk factors derived from regulatory guidance, expectations and leading industry best practices. These inherent risk factors can be a combination of qualitative and quantitative criteria (e.g. customer is a PEP, or no. of SARs filed). With the use of parameters and thresholds as well as statistical data, an FI can define and calibrate the risk factors and assign a weighting to each risk factor.

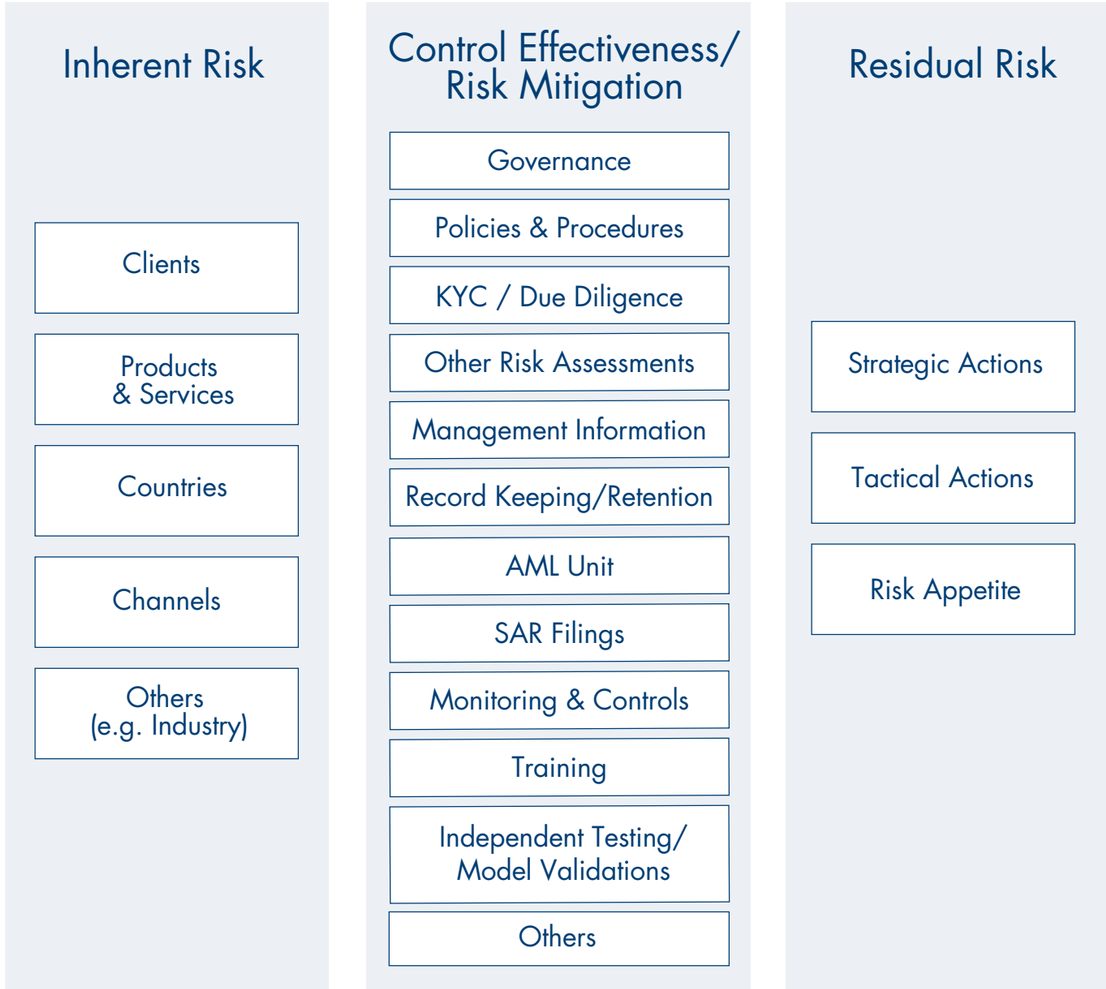


Figure 4: Conventional / Standard ML Risk Assessment Methodology – Source: Wolfsberg Group

Clients

This risk category is composed of several sub-categories such as industry, beneficial ownership, activity, profession, business, occupation, country of residence, nationality, duration of banking relationship, product usage and other factors that the FI deems useful and helpful to determine the ML risk.

In addition, circumstances or factors add to the inherent risk, like purpose of the account (e.g. savings, foreign deposits, payable through account), actual or anticipated activity in the account, nature of the customer's business or occupation (e.g. does the occupation justify level of wealth deposited), customer's location or which types of products and services does customer use.

Products, Services, Transactions

The risk category includes products, account types and services offered to the client or customer and transactions executed for and on behalf of customers. Some of the products and Services offered may have a higher risk assigned, depending on the nature of the product and service, e.g. because they may facilitate anonymity or handling with high volumes of currency

Countries

The country or geography risk is influenced by mainly three financial crime relevant risk parameters:

Criminal
indicators such as corruption indices, political risk maps, countries considered as tax havens, countries susceptible to terrorism etc.

Political
factors such as political stability, rule of law, civil liberties etc.

Regulatory
expectations and requirements: expectations of home or host regulator how to categorise countries from a ML risk perspective or FATF Mutual Evaluation Reports

However, the Basel AML Index 2015 states: "Ranking countries according to their risk of money laundering and terrorist financing presents several methodological challenges. To date there has been no universally agreed definition or methodological approach that prescribes whether a particular country represents a high risk." Therefore, an FI may use different data sources with country risk ratings and calculate a weighted average score.

Or, if available an FI may need to adhere to local regulatory guidance.

Suggested country risk data sources:

FATF High risk and non-cooperative countries
http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)
FATF Mutual Evaluation Reports
http://www.fatf-gafi.org/publications_mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate)
Transparency International – Corruption Perception Index CPI
https://www.transparency.org/cpi2018
UN Sanctions
https://www.cedb.gov.hk/citb/txt_en/Policy_Responsibilities/united_nations_sanctions.html

12. https://index.baselgovernance.org/sites/index/documents/Basel_AML_Index_Report_2015.pdf, p.5

Basel AML Index
https://index.baselgovernance.org/
OFAC
https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx
EU Sanctions
https://sanctionsmap.eu/#/main map
UK HM Treasury and Office of Financial Sanctions Implementation
https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases

Channels

Depending on how well an FI know their customers, some delivery channels and servicing methods can increase the ML risk, e.g. customer A is well-known and his identity is verfied by the FI compared to customer B who was introduced through an intermediary, and both customers use only non-face-to-face channels.

Additional examples are account origination, whether solicited or unsolicited, account servicing, whether face-to-face or non-face-to-face via intermediary or online account opening facilities, whether for existing verifed customers or new customer relationships.

Control Effectiveness/ Risk Mitigation

After the FI defined the inherent risk categories and assessed the inherent risk factors, it must evaluate how controls and risk mitigation measure effectively reduce or offset overall risks. Controls are composed of programmes, policies or activities, which the FI puts in place to protect against ML risks to materialise. Controls should also ensure that potential risks are quickly identified. Rating these controls have a qualitative component, where an FI needs to apply a weight to each control or risk mitigation measure and define how effective or strong these are in order to calculate the residual risk.

Risk mitigation measure may also include the parametrisation and configuration of watch list screening and ML monitoring solutions with the level of fuzziness and ML search patterns.

Higher Risk Activities – some Examples

The following examples provide an overview of some higher risk activities, although this list does not claim to be exhaustive.

Customers

- High proportion of foreign deposits compared to overall deposits at an FI
- High proportion of high risk customers compared to overall customer base
- Companies incorporated in offshore countries or tax havens
- Customers involved in Trade Finance transactions for no apparent reason
- Customers conducting business with commodity traders or arms manufacturers
- Domestic or international Politically Exposed Person (PEP)
- Charity located close to or operating in a sanctioned country
- Company in sensitive industry operates in perceived tax havens, free trade zones or sanctioned countries

Products, Services, Transactions

- Physical cash transactions
- E-Banking (electronic funds transfers)
- International funds transfers
- Payable Through Accounts
- Correspondent accounts for foreign banks
- Wire transfers in USD with high risk countries involved
- Unusual high values in payments exceeding a given limit
- FI offers anonymus or number accounts to foreign customers

Industry

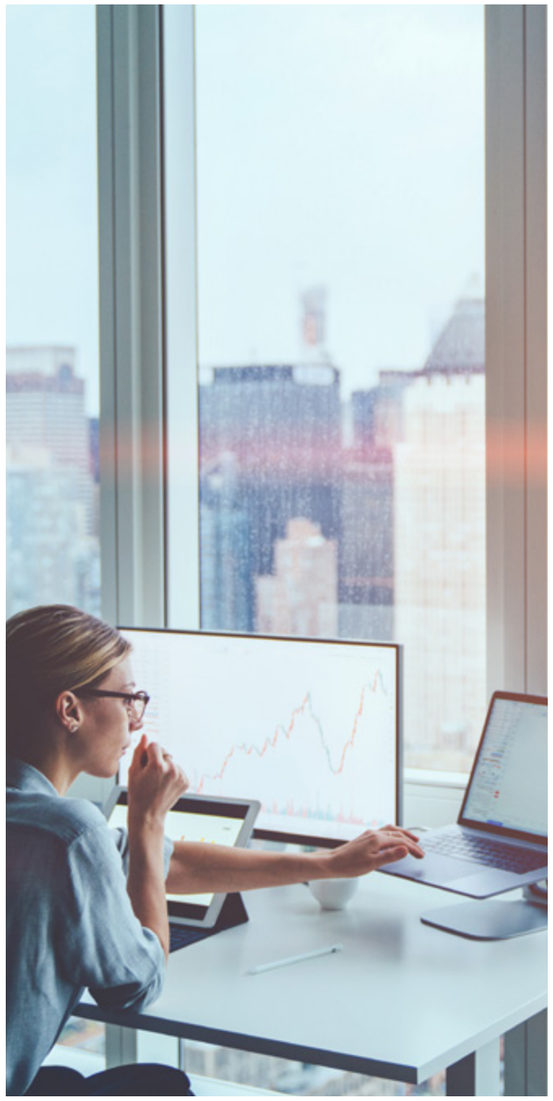
- Commodities
- Military equipment Manufacturer
- Private Military Firms
- Arms Dealers
- Casinos and Internet Gambling
- Gatekeepers
- High Value Goods Dealers

Channels

- Non face-to-face communication
- Via intermediary or professional service providers

Countries

- Country is a perceived tax haven
- Country has a high risk rating for bribery & corruption
- Country is sanctioned or subject to extended measures
- Country has a high risk rating for AML deficiencies



RBA in Temenos Financial Crime Mitigation (FCM) Product Famly

Use data from Screen, Profile and SAP to increase or reduce risk scoring.

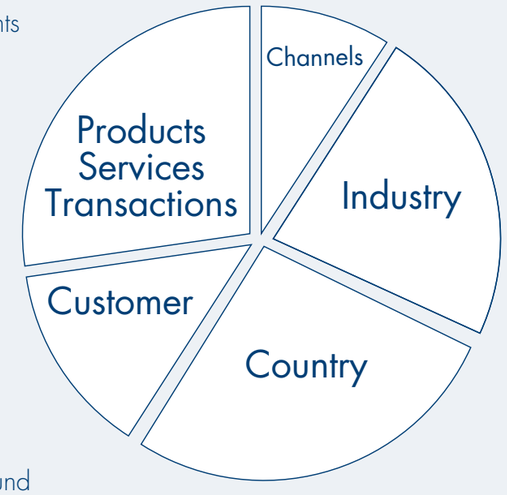
The RBA in FCM has strong similiarities with regulatory guidelines on sound risk assessment and RBA as well as best practices in the financial industry. Derived from these best practices and guidelines, Temenos defined its own RBA with Elements in FCM KC+ for KYC/CDD/EDD, FCM Screen for watch lists and PEPs screening, FCM Profile for AML monitoring and FCM Suspicious Activity Prevention for fraud detection[13]. The below picture shows the risk categories and risk factors, used in KC+ to score customer and transaction risk. In FCM KC+, risk categories are called Risk Definitions which contain one to many risk attributes, i.e. risk factors. The model is highly flexible to support any RBA that FIs define.

Products, Services, Transactions:

- Type of account and/or facility
- Previous banking relationship
- Private banking
- Account currency
- Monetary instruments
- …

Channels:

- Non face to face
- Face to face
- E-verification
- …



Industry

- Nature of business activities
- Related activities
- …

Customer

- AML system check
- Customer background
- Political affiliations if (PEPs)
- Cash-intensive businesses
- Foreign corporations
- …

Country

- Country of residence
- Country of incorporation
- Fiscal country
- Sanctioned country
- …

Figure 5: RBA with Risk Definitions and Risk Attributes

13. Check out for more information about Temenos FCM here: https://www.temenos.com/en/solutions/financial-crime/

Risk Assessment Process with Temenos's RBA

An FI's sound and robust RBA requires input from various systems and applications to assess the inherent ML risks. Temenos's Financial Crime Mitigation product family is designed as a complete offering to protect an FI against ML risks:

- Screen for transaction and customer screening against sanctions, PEPs and watch lists
- Suspicious Activity Prevention S.A.P. to detect suspicious behaviour and fraudulent transactions
- Profile for transaction monitoring against a variety of ML scenarios and patterns

The following example of a high level risk assessment process illustrates the steps to identify risks, score them, apply weightings, rate risk mitigating measures to arrive the residual risk.

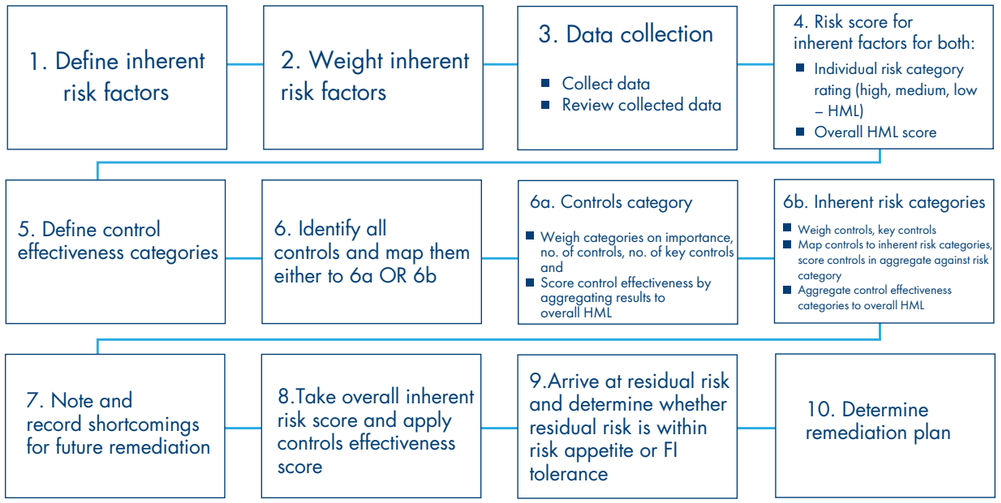


Figure 6: Risk Assessment Process – Source: Wolfsberg Group

The benefits of an integrated FCM solution allows an FI to define an overall consistent RBA, which includes inherent risks apparent in watch lists and PEPs screening as well as ML transaction monitoring.

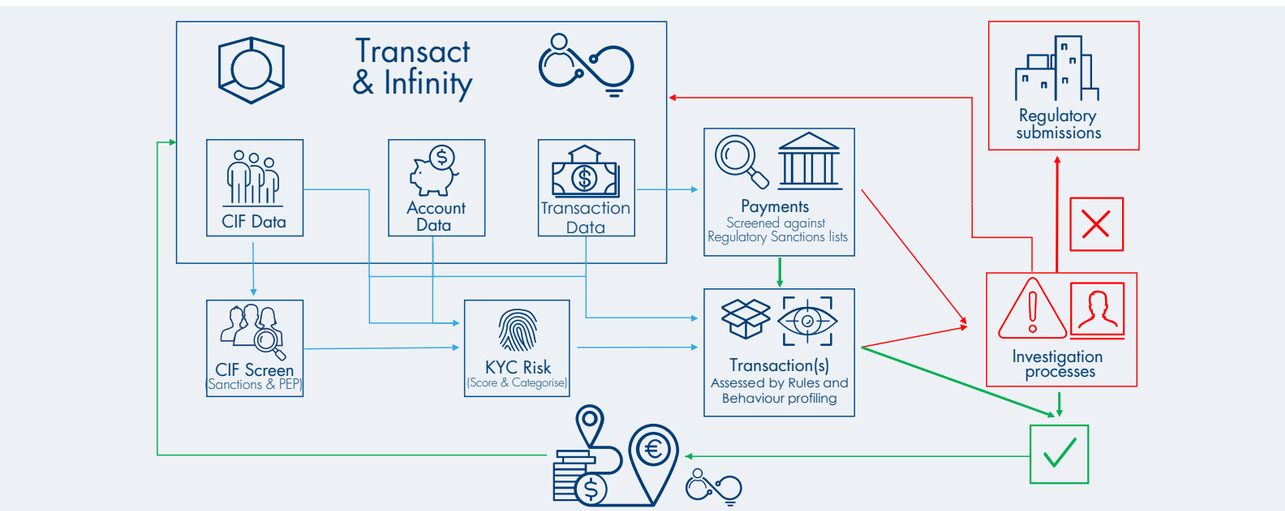


Figure 7: FCM Integrated Risk-Based Approach

Glossary

AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFT	Combating Financing of Terrorism
EDD	Enhanced Due Diligence for higher risk customers
Financial Crime Risk	Financial crime is defined as crime that is specifically committed against property. These crimes are usually committed for the personal benefit of the criminal, and they involve an illegal conversion of ownership of the property that is involved.
Inherent Risk Categories	Inherent risks grouped in categories such as client, products & services, country/geography, industry and channels
Inherent Risk Factors	Sub-categories of Inherent Risk Categories having a weighting associated to
Inherent Risk	Represents the exposure to money laundering, sanctions or bribery & corruption risk in the absence of any control environment being applied.
Internal Controls	Policies, procedures, systems and personnel in place within an FI, designed to protect against the materialisation of a ML risk, or to ensure that risk factors are promptly identified.
KYC	Know Your Customer
RBA	Risk-Based Approach
Residual Risk	The risk that remains after controls are applied to the inherent risk. It is determined by balancing the level of inherent risk with the overall strength of risk management activities and controls.
Risk Appetite	The amount and type of risk that an organisation is willing to take in order to meet their strategic objectives. Organisations will have different risk appetites depending on their sector, culture and objectives. A range of appetites exists for different risks and these may change over time.

Sources and References

The Wolfsberg Group - https://www.wolfsberg-principles.com/publications/wolfsberg-standards
The Wolfsberg Group Guidance on a Risk Based Approach for Managing Money Laundering Risk
The Wolfsberg Group FAQ's on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption
The Wolfsberg Group Country Risk FAQs
Basel Committee on Banking Supervision - https://www.bis.org/bcbs/publications.htm?m=3%7C14%7C566
Basel AML Index - https://www.bis.org/bispapers/index.htm?m=5%7C27
Financial Action Task Force FATF - http://www.fatf-gafi.org/home/
FATF 40 Recommendations
FATF Guidance for RBA for Banking Sector - http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf
Ministry of Authority MAS, Singapore - http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions/Anti-Money-Laundering-and-Countering-the-Financing-of-Terrorism/Guidance-Papers/2018/Guidance-for-Effective-AML-CFT-Transaction-Monitoring-Controls.aspx
U.S. Federal Financial Institutions Examination Council FFIEC https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_005.htm

About Temenos

Temenos AG (SIX: TEMN) is the world's leader in banking software. Over 3,000 banks across the globe, including 41 of the top 50 banks, rely on Temenos to process both the daily transactions and client interactions of more than 500 million banking customers. Temenos offers cloud-native, cloud-agnostic and AI-driven front office, core banking, payments and fund administration software enabling banks to deliver frictionless, omnichannel customer experiences and gain operational excellence.

Temenos software is proven to enable its top-performing clients to achieve cost-income ratios of 26.8% half the industry average and returns on equity of 29%, three times the industry average. These clients also invest 51% of their IT budget on growth and innovation versus maintenance, which is double the industry average, proving the banks' IT investment is adding tangible value to their business.

For more information please visit www.temenos.com.

TEMENOS

THE BANKING SOFTWARE COMPANY