FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Ableitung von Referenzmodellen zur Bekämpfung der Geldwäsche im österreichischen Finanzsektor

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Wirtschaftsinformatik

eingereicht von

Ilian Berov, Bakk.rer.soc.oec.
Matrikelnummer 00451124

an der
Fakultät für Informatik
der Technischen Universität Wien

Betreuung: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Wien, 24 Oktober 2019

Ilian Berov	Markus Haslinger

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Deriving reference models for Anti-Money Laundering in the financial sector in Austria

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Business Informatics

by

Ilian Berov, Bakk.rer.soc.oec.
Registration number 00451124

to the Faculty of Informatics
at the TU Wien

Advisor: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Vienna, 24 October 2019

Ilian Berov

Markus Haslinger

Erklärung zur Verfassung der Arbeit

Ilian Berov, Bakk.rer.soc.oec.
1040 Wien, Kettenbrückegasse 20/27

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 24 Oktober 2019

Ilian Berov

Kurzfassung

Das Finanzsystem in Österreich wird von Banken dominiert, die 75% des gesamten Vermögens des Finanzsektors halten. Ein Finanzsystem solcher Struktur und Größe kann für kriminelle Aktivitäten, wie Geldwäsche, verwendet werden.

Seit Anfang 2017 gibt es ein neues Gesetz in Österreich - das Finanzmarkt-Geldwäschegesetz (FM-GwG). Das Ziel des Gesetzes ist, die entsprechende Rechtsgrundlage in Österreich zu konsolidieren und die EU-Richtlinie 849/2015 umzusetzen.

Banken in Österreich haben ein gutes Verständnis von den Risiken der Geldwäsche und Terrorismusfinanzierung (engl.: ML/TF) und von ihren Verpflichtungen zur Bekämpfung dieser Delikte (engl.: AML/CFT). Zwischen 2014 und 2017 beobachtete man einen Anstieg der Anzahl der Verdachtsmeldungen um ca. 53%, die von den Verpflichteten erstellt wurden.

Trotzdem kann man die Fähigkeit der Finanzinstitute hinterfragen, neue gesetzliche oder regulatorische Anforderungen zu begegnen.

Die Implementierung von rechtskonformen internen Prozessen erfordert die Zusammenarbeit von Compliance-Managern, IT- und Rechtsexperten. Durch die Modellierung dieser Prozesse wird es für die Akteure in ihren Unternehmen leichter sein, entsprechend gegen eventuelle Rechtsverletzungen zu handeln.

In dieser Masterarbeit wird die Aufmerksamkeit auf die AML-Vorschriften in Österreich gelenkt. Zusätzlich werden Referenzmodelle abgeleitet, die spezifische Compliance-Anforderungen erfüllen und interne Prozesse im Kontext von AML unterstützen könnten.

Schlüsselwörter: Geldwäsche, Bekämpfung der Geldwäsche, KYC, CDD, Referenzmodellierung, Compliance Management, Finanzmarkt

Abstract

The financial system in Austria is dominated by banks, which hold 75% of the total assets of the financial sector. A financial system of this structure and size can be used for criminal activities such as money laundering.

Since the beginning of 2017 there is one consolidated money laundering act in Austria - The Financial Market - Money Laundering Act (FM-GwG). The aim of the Act is to consolidate the relevant Anti-Money Laundering legal basis in Austria and to implement EU Directive 849/2015.

Banks in Austria have a good understanding of the risks of money laundering and terrorist financing (ML/TF) and of their obligations to combat these offences (AML/CFT).

Between 2014 and 2017 the number of Suspicious Transaction Reports (STRs), generated by the obliged entities, increased by approximately 53%.

Nevertheless, the ability of financial institutions to meet new legal or regulatory requirements can be questioned.

The implementation of compliant business processes requires the collaboration of compliance managers, IT and legal experts. By modeling these processes, it will be easier for the stakeholders in their organizations to take appropriate actions and act accordingly against potential legal violations.

In this master thesis, the attention is drawn to the AML regulations in Austria. In addition, reference models are derived that meet specific compliance requirements and could support the internal processes in the context of AML.

Keywords: Anti-Money Laundering, KYC, CDD, Reference Modeling, Compliance Management, Financial Sector

Contents

List of figures

List of tables

List of laws

BiBuG	*Bilanzbuchhaltungsgesetz 2014*
BKA-G	*Bundeskriminalamtgesetz 2002*
BörseG	*Börsegesetz 1989*
BWG	*Bankwesengesetz 1993*
Depotgesetz	*Depotgesetz 1969*
Devisengesetz	*Devisengesetz 2004*
E-Geld Gesetz	*E-Geld Gesetz 2010*
EU-PolKG	*EU-Polizeikooperationsgesetz 2009*
FinStrG	*Finanzstrafgesetz 1958*
FKG	*Finanzkonglomerategesetz 2004*
FM-GwG	*Finanzmarkt-Geldwäschegesetz 2016*
GewO	*Gewerbeordnung 1994*
GSpG	*Glücksspielgesetz 1989*
KStG	*Körperschaftsteuergesetz 1988*
NISG	*Netz- und Informationssystemsicherheitsgesetz 2018*
NO	*Notariatsordnung 1871*
PolKG	*Polizeikooperationsgesetz 1997*
RAO	*Rechtsanwaltsordnung 1869*
SanktG	*Sanktionengesetz 2010*
SMG	*Suchtmittelgesetz 1997*
StBG	*Strafgesetzbuch 1993*
StPO	*Strafprozessordnung 1975*
StPÄG 2014	*Strafprozessrechtsänderungsgesetz 2014*

VAG	*Versicherungsaufsichtsgesetz 2016*
WAG	*Wertpapieraufsichtsgesetz 2018*
WTBG	*Wirtschaftstreuhandberufsgesetz 2017*
ZaDiG 2018	*Zahlungsdienstegesetz 2018*
Zollrechts-DG	*Zollrechts-Durchführungsgesetz 1994*

List of abbreviations and acronyms

A-FIU	*Austrian Financial Intelligence Unit*
AML	*Anti-Money Laundering*
AML/CTF	*Anti-Money Laundering/ Counter Terrorist Financing*
AMLC	*Subcommittee on Anti-Money Laundering*
AMLU	*Anti-Money Laundering Unit*
AMLID	*Anti-Money Laundering International Database*
APG	*Asia Pacific Group on Money-Laundering*
BaFin	*Bundesanstalt für Finanzdienstleistungsaufsicht*
BCM	*Business capability models*
BIS	*Bank for International Settlements*
BK	*Bundeskriminalamt*
BMEIA	*Bundesministerium für Europa, Integration und Äußeres*
BMF	*Bundesministerium für Finanzen*
BMVRDJ	*Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz*
BMWFW	*Bundesministerium für Bildung, Wissenschaft, Forschung*
BPCM	*Business process compliance management*
BPMN	*Business process modelling notation*
BVT	*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung*
CBDDQ	*Correspondent Banking Due Diligence Questionnaire*
CDD	*Customer due diligence*

Cf.	from Latin: *confer*, "compare"
CFATF	*Caribbean Financial Action Task Force*
CIP	*Customer Identification Program*
CTF	*Counter Terrorist Financing*
DAP	*Deferred Prosecution Agreement*
DEA	*The U.S. Drug Enforcement Agency*
DNFBPs	*Designated non-financial businesses and professions*
EAG	*Eurasian Group*
EBA	*European Banking Authority*
EC	*European Commission*
ECB	*European Central Bank*
ECJ	*European Court of Justice*
ECOWAS	*Economic Community of West African States*
e.g.	from Latin: *exempli gratia*, “for example”
EGMLTF	*Expert Group on Money Laundering and Terrorist Financing*
EIOPA	*the European Insurance and Occupational Pensions Authority*
ESAs	*The Joint Committee of the three European Supervisory Authorities EBA, EIOPA and ESMA*
ESAAMLG	*Eastern and Southern Africa Anti-Money-Laundering Group*
ESMA	*European Securities and Markets Authority*
et al.	from Latin: *et alia*, “and others”
EUR	*Euro*
FATF	*Financial Action Task Force*
FED	*Federal Reserve System*
FIU	*Financial Intelligence Unit*

FMA	*Finanzmarktaufsicht*
FSAP	*Financial Sector Assessment Program*
FSF	*Financial Stability Forum*
FSRB	*FATF-style regional body*
GAFISUD	*Financial Action Task Force on Money-Laundering in South America*
GDP	*Gross domestic product*
GDPR	*General Data Protection Regulation*
GIABA	*Inter-governmental Action Group Against Money Laundering and Terrorist Financing in West Africa*
GPML	*Global Programme Against Money Laundering*
Ibid.	from Latin: *ibidem*, “in the same place”
ICA	*International Compliance Association*
ICBC	*Commercial Bank of China*
ICPO	*International Criminal Police Organization*
IMF	*International Monetary Fund*
IMoLIN	*The International Money Laundering Information Network*
KYC	*Know your customer*
LEOCMLU	*The Law Enforcement, Organized Crime and Anti-Money-Laundering Unit of the United Nations Office on Drugs and Crime*
MER	*Mutual Evaluation Report*
ML	*Money laundering*
ML/TF	*Money laundering/Terrorist funding*
MONEYVAL	*Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism*
MoU	*Memorandum of understanding*
NCCT	*Non cooperative countries and territories*

NPO	*Non-profit organization*
OAS/CICAD	*Organization of American States*
OCCRP	*The Organized Crime and Corruption Reporting Project*
OECD	*Organisation for Economic Co-operation and Development*
PEP	*Politically Exposed Person*
RTS	*Regulatory Technical Standards*
SAR	*Suspicious Activity report*
SPOC	*Single Point of Contact*
STR	*Suspicious Transaction report*
TF	*Terrorist financing*
UN	*United Nations*
UNODC	*The United Nations Office on Drugs and Crime*
US	*United States of America*
USD	*US dollars*
UTR	*Unusual Transaction Report*
WKStA	*Zentrale Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption*
WB	*World Bank*

chapter 1

Introduction

Money laundering (ML) is a process of legitimizing the profit from criminal activities into legal funds by using undisclosed financial system's shortcomings and thus avoiding existing detection methods. Money laundering is meanwhile a whole industry and the fight against it over the last two decades has also become an increasingly important task. Historically the idea of money laundering has been associated with the 1930s during the prohibition in the United States when Al Capone used the profit from purchased 'Laundromats' to mix it with the profit from illegal activities like bootlegged liquor sales[1]. Later in the mid-1970s during the Watergate case investigation[2] the term acquired a broad public use. Since the 1980s many initiatives have been developed and implemented to combat this criminal activity. The globalization of the world economy in the last 30 years, especially the global financial markets, is one major aspect that must be considered when discussing the problem of money laundering. The liberalization of the markets allows individuals and companies to transfer money and financial assets freely, with insignificant or no barriers, in order to search for the most favorable location and the highest rate of return. This leads to a situation where the increased volumes and high flow of capital is becoming the perfect place to keep money with a criminal origin out of sight. To distinguish between legally derived assets and those acquired by crime activities has become in recent years a complex task[3]. As a result, the financial institutions are facing an increasing number of regulatory obligations.

Relevance for practice and society

The fight against money laundering is as a massive worldwide initiative and not just a local country-specific activity. Almost every country in the world has established Financial Intelligence Units (FIU) or has taken actions to avoid an entry in the list of Non-cooperative countries and territories (NCCT's)[4]. Many governmental bodies, like for example The Bank of International Settlements (BIS)[5], The Organisation for Economic Co-operation and Development (OECD), the G-8, G-20, EU members' finance and justice ministers, several departments in the United Nations, the World Bank, the International Monetary Fund (IMF) and others, are involved in this combat and are all struggling to

[1] *Cf.* Ferguson (n.d.).: Money Laundering, p. 4
[2] *Cf.* Perry (2000): Watergate Case Study
[3] *Cf.* Petrunov (2009): Initiatives to counter money laundering: global, regional, national, p.3
[4] NCCT is issued by the FATF. By May 2018 only one country is part of the list: Democratic People's Republic of Korea
[5] A complete list of all used abbreviations can be found at the beginning of this paper

establish common Anti-Money Laundering (AML) standards to assess and reduce money laundering[6]. With the preparation of the Fifth EU ML directive (AMLD5)[7] even before all 28 EU members states have implemented the Fourth EU ML Directive (AMLD4)[8] the European Union wants to ensure higher transparency of the financial transactions and enhance the access of the FIUs to information including centralized bank account registers.

The Republic of Austria, as one of the most developed countries in the world, is part in the combat against money laundering. With a Gross domestic product (GDP) of approximately 396 billion EUR in 2017[9] it has a highly-developed and robust financial market, with assets totaling around 355% of GDP. 75% of these assets are currently being held by banks that dominate the financial sector[10]. A financial system of such structure and magnitude might be exploited for criminal activities like money laundering. Since the beginning of 2017 there is one consolidated money laundering act in Austria – The Financial Market - Money Laundering Act (FM-GwG)[11]. The goal of the act is to consolidate the AML legal basis (previously implemented in various statutes) and to implement the EU directive 849/2015[12]. FM-GwG applies to all credit and financial institutions in Austria (also called "obliged entities")[13]. **§ 2 FM-GwG** stipulates what a "credit institution" and what a "financial institution" is[14]. For the goals of this master's thesis, the terms "financial institution", "credit institution" and "bank" will be used as synonyms and thus the focus of this master's thesis falls on the "banks" in Austria (and not insurance companies, pension funds, money transfer offices, transmitter companies and others).

In the last couple of years two cases of financial frauds including money laundering have shaken the financial system in Austria. BAWAG (Bank für Arbeit und Wirtschaft, meanwhile known as BAWAG P.S.K.), currently the third largest bank group in Austria, approved in October 2005 a loan of 425 million EUR to Phillip R. Bennett, former CEO of "Refco"[15]. The reason for the loan was an undisclosed loan of 430 million USD of Refco's funds to Bennett. Right after BAWAG released the

---

[6] *Cf.* Unger et al. (2006): The amounts and effects of money laundering, p. 7
[7] *See* The European Parliament and the Council of the European Union (2018): Directive (EU) (Proposal)
[8] *See* The European Parliament and the Council of the European Union (2015): Directive (EU) 2015/849
[9] *Cf.* Wirtschaftskammer Österreich (2018): Economic situation and outlook
[10] *Cf.* FATF (2016): Anti-money laundering and counter-terrorist financing measures in Austria - 2016
[11] *See* FM-GwG (2016): Bundesgesetz zur Verhinderung der Geldwäscherei und Terrorismusfinanzierung im Finanzmarkt (Finanzmarkt-Geldwäschegesetz – FM-GwG), Fassung vom 25.06.2018
[12] *See* The European Parliament and the Council of the European Union (2015): Directive (EU) 2015/849 of the European Parliament and of the Council
[13] **§ 1 FM-GwG**, Fassung vom 25.06.2018: "*Dieses Bundesgesetz ist auf Kredit- und Finanzinstitute (**Verpflichtete**) anzuwenden. Davon ausgenommen sind die in anderen Mitgliedstaaten gelegenen Zweigstellen bzw. Zweigniederlassungen von Kredit- und Finanzinstituten mit Sitz im Inland.*"
[14] **§ 2 FM-GwG**, Fassung vom 25.06.2018: „[…] *Kreditinstitut: ein Kreditinstitut gemäß **§ 1 Abs. 1 BWG** und ein CRR-Kreditinstitut gemäß **§ 9 BWG**, das Tätigkeiten im Inland über eine Zweigstelle erbringt.*
2. Finanzinstitut:
*a) ein Finanzinstitut gemäß **§ 1 Abs. 2 Z 1 bis 6 BWG**;*
b) ein Versicherungsunternehmen gemäß § 1 Abs. 1 Z 1 VAG 2016 und ein kleines Versicherungsunternehmen gemäß § 1 Abs. 1 Z 2 VAG 2016 jeweils im Rahmen des Betriebes der Lebensversicherung (Zweige 19 bis 22 gemäß Anlage A zum VAG 2016);
*c) eine Wertpapierfirma gemäß § 3 Abs. 1 WAG 2018 und ein Wertpapierdienstleistungsunternehmen gemäß **§ 4 Abs. 1 WAG 2018**;*
*d) einen AIFM (Alternative Investmentfonds Manager) gemäß **§ 1 Abs. 5 und § 4 Abs. 1 AIFMG** und einen Nicht-EU-AIFM gemäß **§ 39 Abs. 3 AIFMG**;*
*e) ein E-Geldinstitut gemäß **§ 3 Abs. 2 E-Geldgesetz 2010**;*
*f) ein Zahlungsinstitut gemäß **§ 10 ZaDiG 2018**;*
g) die Post hinsichtlich ihres Geldverkehrs;
*h) Finanzinstitute gemäß Art. 3 Z 2 lit. a bis d der **Richtlinie (EU) 2015/849** mit Sitz in einem anderen Mitgliedstaat mit dem über im Inland gelegene Zweigstellen bzw. Zweigniederlassungen ausgeübten Geschäftsbetrieb sowie im Inland gelegene Zweigstellen bzw. Zweigniederlassungen von solchen Finanzinstituten, die in Drittländern zugelassen sind.*"
[15] "Refco" was a financial service company, specialized in the trading of commodities and futures contracts

loan to Bennett several regulatory investigations were triggered. As a result, in April 2006 the creditors of "Refco" sued BAWAG for over 1.3 billion USD. They claimed, that the bank had known about Bennett's fraud and actively collaborated with him[16]. In 2017 The Organized Crime and Corruption Reporting Project (OCCRP) published the report "The Russian Laundromat". The authors of the report claimed that 4.1 million USD were transferred to 32 bank accounts in Austria as a part of a massive money laundering fraud[17]. According to the last report regarding money laundering published in 2017 by Bundeskriminalamt Österreich[18] (Federal Criminal Police Office, shortly „.BK"), the overall number of Suspicious Activity Reports (SARs; also called "Suspicious Transactions Reports (STRs)"[19])[20] (including reports for suspicious activity in terms of money laundering) has increased since 2014 by approximately 53% (2014: 1637, 2015: 1793, 2016: 2150, 2017: 3541). This number includes all cases of suspicious money laundering, fraud, tax crimes, corruption and others. In 2017 approximately 3000 reports came directly from the credit and financial institutions (around 1000 reports more compared to 2016). Only 21 of them have been submitted to public prosecutor's office and in exactly one case it came to a conviction under the ML regulations. The reason for this is most probably the fact that due to the international interdependence it is difficult to find evidence of money laundering – the authorities can investigate only when there is a "predicate offence" and it must be absolutely clear that the illicit money is associated with a criminal act[21].

The number of STRs correspond to less than approximately 0.1% of total number of STRs Europe-wide[22]. In the Netherlands, for example, the total number of STRs between 2006-2014 is around 2 000 000[23] (for the same period in Austria they are around 14 000; in Germany: around 117 200). Per February 2017 in the Netherlands 354 monetary financial institutions are operating[24] (in Austria: 821; in Germany: 2106). It is important to mention that in the Netherlands the money transfer offices, for example, are obliged to report every transaction over the threshold of EUR 2000[25]. In Austria the regulation is similar[26] (in 2016 around 440 STRs were reported from so called Money-Transmitter-companies, the number for 2017 is unknown). In Austria and in the Netherlands the banks analyze the transactions internally first and then generate a "*suspicious*" (in Austria) or an "*unusual*" (in the Netherlands) transaction report to the domestic Financial Intelligence Unit. Another important aspect is, that the UTRs (in the Netherlands) and the STRs (in Austria) are generally not reported by financial institutions only, but also by other occupations (like lawyers) and sectors (like insurance companies).

---

[16] *Cf.* Unger (2007): The Scale and Impacts of Money Laundering, pp. 4-5 and
See Frey (2008): Nine jailed over Bawag bank fraud, article in Financial Times from July 4, 2008

[17] *See* Eckelsberger/Sim/Florian (2017): Moskau–London–Gänserndorf, article in dossier.at from March 21, 2017

[18] *See* Bundeskriminalamt Österreich (2016): Geldwäsche Jahresbericht and
See Bundeskriminalamt Österreich (2017): Geldwäsche Jahresbericht

[19] There is no single definition of a Suspicious Transaction Report (STR). It is often known as a Suspicious Activity Report (SAR). It is generally understood as a "*report, compiled by the regulated private sector (most commonly banks and financial institutions, but also non-financial designated professions) about financial flows they have detected that could be related to money laundering or terrorist financing.*" (EUROPOL (2017), p.8).
In this thesis STR and SAR will be used as synonyms. More information about the definition of STR, SAR and UAT/UTR ("Unusual activity report" / "Unusual transaction report") can be found in section 3.1.6.

[20] Translated from German: "*Verdachtsmeldung*"

[21] More about the criminal offence "money laundering" can be found in section 3.1.1

[22] *Cf.* EUROPOL (2017): From Suspicion to Action, p. 5

[23] *Cf.* EUROPOL (2017): From Suspicion to Action, p. 10

[24] *Cf.* European Central Bank (2017): List of monetary financial institutions and institutions subject to minimum reserves and list of monetary financial institutions in the acceding countries, p. 11

[25] *Cf.* Financial Intelligence Unit – Nederland (2014): Annual Report 2014, p. 9

[26] *See* section 3.4.1. for more information about the risk assessment on customer level

Since the banks are at the forefront of combating money laundering, they are legally obliged and must establish a robust internal framework for detection and prevention of money laundering by monitoring the cash- and non-cash-based transactions[27]. In case of suspicious activity, the banks must report this to the Financial Intelligence Unit of the Federal Criminal Police Office of Austria[28]. To know who their customers truly are, the banks must check and verify the identity of their customers when, for example, opening an account. This is called the "Know Your Customer" (KYC) principle. It is a fundamental and critical policy for every financial institution. It includes two main tasks: "Customer Identification Program" (CIP) and "Customer Due diligence" (CDD). CIP is a set of tasks regarding the customer identification information: collection, verification, record keeping and screening. The Simplified Due diligence is used to calculate the risk score of the customer and the Enhanced Due diligence is an additional step to collect information for customers with high risk score, in order to understand their financial activities. Both tasks can be executed successfully only when the banks can guarantee an excellent internal processing of the customer data. In order to have compliant internal processes and the observance of different regulations, the banks are supported by different techniques like real-time risk monitoring or methodologies such as business process compliance management (BPCM). According to Merriam-Webster, the term "*compliance*" is "*the ability of an object to yield elastically when a (preferably external) force is applied*"[29]. In the context of AML, the financial institutions must make sure that their internal AML programs and system are up-to-date with each new regulatory change. Moreover, in order to react "*elastically*" to the national regulations and to be able to detect suspicious activities the financial institutions must implement and establish an internal control and monitoring system.

Due to the high number of regulatory changes and short deadlines for their implementation the financial institutions most commonly have an isolated internal approach for implementation. This leads respectively to isolated compliance solutions (which mostly contain from a mixture between organizational structures, internal processes and IT) and solving of the internal compliance challenges and issues on the fly[30]. The CDD process described above is essential for the AML program in every institution and is also affected by regularly changes and modifications. In order to adapt the CDD process the use of a reference model could be helpful. An additional argument for the creation of a reference model is the assumption that currently most of the financial institutions have different approaches in regard to AML. They fulfil their legally stated obligations but, as assumed, internally the organizational structures, processes and IT solutions employed in the daily business differ. This reference model for CDD could be used as bank-independent standard and would also help the supervisory authorities to assess the different implementations more appropriately[31]. However, in

[27] In this master's thesis the terms "wire transfer", "money transfer", "cash transfer", "credit transfer" and similar will be used as synonyms and thus a "transfer" should be understand as:

- a "transfer of funds", that is transferred through a financial institution (a bank), incoming and/or outgoing and
- a "transfer of funds" according to Article 3 (9) of Regulation (EU) 2015/847 (see The European Parliament and the Council of the European Union (2015): Regulation (EU) 2015/847)

[28] Translated from German: "*Geldwäschemeldestelle*": Financial Intelligence Unit of the Federal Criminal Police Office of Austria is the central authority, that receives reports for suspicious financial transactions, according to Austrian jurisdiction. More information can be read in section 3.1.7.

[29] Merriam-Webster (2018): "*compliance*"

[30] *Cf.* Timm/Sandkuhl (2018): Towards a Reference Compliance Organization in the Financial Sector, p. 2

[31] *See* the interview with Dr. Elena Scherschneva-Koller from 04.06.2018, lines 70-79

reality it would be impossible to develop a “one-size” model that is valid for all financial institutions and fits to their needs due to their different size, transaction volumes and customer segments[32]. However, the advantages of the use and application of reference models is already successfully proven in other business fields and industries[33].

Research Design

The first goal of this master’s thesis is to find a relationship between the number of STRs, reported by the financial institutions, and the compliance competencies that are used in the internal AML program. The second goal is to derive a reference model for the CDD process based on the existing internal AML policy. The following main research questions (RQ) were therefore defined:

RQ1: Is there a correlation between a bank’s internal competences (organizational structure, IT, know-how) and the number of Suspicious Transaction reports (STRs) classified as “money laundering” reported by this bank?

RQ2: Is it possible to derive a reference model for the AML Customer due diligence (CDD) from an existing enterprise’s AML context?

In addition, in the course of this master’s thesis I will give answers to following questions, among others:

- What are the main factors for tracking and detection of suspicious transactions by the financial institutions in Austria?
- What are the main challenges for the financial institutions in order to stay compliant with different regulations?
- Is the number of the STRs equally distributed over the banks and branches in Austria?
- What are the reasons for the significant increase of the number of STRs – additional regulations, re-assessment of the risks, re-organization of the enterprise? Is it because the banks’ protective mechanisms are getting better and thus they are able to detect most of the illegal transactions or new forms of money laundering? Some opinions state that an increase of the number of STRs is not a reliable indication of the actual number of money laundering activities in Austria. Experts assume that international pressure - not least from the FATF - has increased attention to the problem and that more suspicious cases are being therefore reported to the authorities[34]. Others highlight the higher responsibility and fulfilment of duties from different designated non-financial businesses and professions (DNFBPs) like lawyers[35]. Of course, the increased number of STRs could also mean that the criminals have increased interest in exploiting and using the Austrian financial system for criminal activities.

It is also interesting to know how far the banks can go with the implementation of the Customer due diligence. Would their customers be happy with and accept a deeper background check? How would this fit with the General Data Protection Regulation (GDPR)[36]?

---

[32] *See* the interview with Dr. Elena Scherschneva-Koller from 22.05.2018, lines 10-16 and *See* the interview with Mag. Oliver Floth from 12.06.2018, lines 139-152
[33] *Cf.* Timm/Sandkuhl (2018): Towards a Reference Compliance Organization in the Financial Sector, p. 2
[34] *Cf.* addendum (2017): Wien als Drehscheibe für Terror-Gelder
[35] *See* the interview with Dr. E. Scherschneva-Koller from 04.06.2018, lines 1-25
[36] *See* The European Parliament and the Council of the European Union (2016): Regulation (EU) 2016/679

The research in this thesis is following a deductive research approach and reasoning (***RQ1***) and is partly based on the design science research methodology (DSRM) proposed by Peffers et al.[37], because it suits well to the scope (***RQ2***) and scale of this master's thesis. The deductive research "*is concerned with developing a hypothesis based on existing theory* [the legal basis und research regarding the combat against ML/TF], *and then designing a research strategy to test the hypothesis* [correlation between the number of STRs and internal competencies]*. In this type of research, theory, and hypotheses built on it, come first and influence the rest of the research process – this type of research is often associated with the quantitative type of research* [questionnaires]"[38]. DSRM, on the other hand, consists of six steps (the last step "*communication*" is not listed below):

1. *Problem identification and motivation*

   In this master's thesis I will do a literature research about the legal aspects in Austria in regard to ML. In addition, I will show the role of the three cores in a successful combat against ML – people, technology, data. The analysis will be further supported by questionnaires filled out by few AML Officers from different financial institutions in Austria and interviews with experts on the AML topic.

2. *Define the objectives for a solution*

   Beside the goals and research questions stated above there are no particular objectives of this master's thesis.

3. *Design and development*

   In order to derive a reference model based on real world policies I should need a full access to the internal process landscape of multiple financial institutions. Due to lack of access to real-world internal processes the CDD reference model can be in the end seen as a proposal or a draft version (otherwise the deriving of a reference model would be in an inductive way). Further, the proposed model could be re-evaluated and modified in the future. But this would be only possible if the financial institutions in Austria or the FMA are part of the process. Therefore, the proposed model cannot be seen as a representation of the "best-practices on the market". The derivation of the reference model will be based on Schütte's work on how reference models are developed and derived[39].

4. *Demonstration and Evaluation*

   Due to the high abstract specification of the proposed CDD reference model and lack of large set of experts it is currently not possible to evaluate its real-world application and impacts. The conclusions made are based also on my own observations, findings and subjective understanding of the problem.

[37] *See* Peffers/Tuunanen/Rothenberge/Chatterjee (2007): A design science research methodology for information systems research
[38] Wilson (2013): Essentials of Business Research: A Guide to Doing Your Research Project, p. 13
[39] *Cf.* Brocke (2015): Referenzmodellierung: Gestaltung und Verteilung von Konstruktionsprozessen, pp. 164-168

Scientific relevance

The topic "Money Laundering" was and still is of great interest for the experts, researchers and law enforcement authorities. The scientific researches on predicate crimes of money laundering or, more generally, on AML legislation have become "*hot*" topics in the last couple of years[40]. The publications from Zünd[41] and Bernasconi[42], for example, were one of the first scientific publications trying to model the process of "Money Laundering". The growing number of detected money laundering cases in the past and the concerns about the problem triggered a massive worldwide flow of documentation, papers and guidelines about the combat against ML. Initiatives all over the world mainly under the jurisdiction of the UN together with experts from the financial institutions and governmental authorities created frameworks like the Forty Recommendations by FATF[43] in order to give the society a tool set to fight against ML. The history of the scientific research regarding money laundering is beyond the scope of this master's thesis. However, in this master's thesis I am using various scientific sources (among others Unger et al. (2006)[44], Bongard (2001)[45], Kirsch (2006)[46]) which might be seen as milestones in the research of money laundering due to their comprehensive and highly detailed analysis of the criminal offence of money laundering, the techniques and methodologies for prevention of ML and the impact of ML on the society. In order to build a reference model in the context of CDD by using the EAM methodology the publications by Schütte (1998)[47], Gajewski (2004)[48], Noran (2006)[49], Kotusev (2017)[50] and Timm/Zasada/Thiede (2016)[51] and Timm/Sandkuhl (2018)[52] were used as a comprehensive source of knowledge.

Outline

This master's thesis is structured as follows: In chapter 2 by doing a literature research I give an explanation what money laundering is, how it works and which are the results from it. Chapter 3 gives an overview over the existing national and international regulations and will focus on the CDD process. In chapter 4 I will summarize known competencies and best-practices for prevention and detection of money laundering by the financial institutions, split by technology, data and people. In chapter 5 I will give a guideline how to build and derive reference models from an existing domain before summarizing the conclusions in chapter 6.

---

[40] *Cf.* Mei/Ye/Gao (2014): Literature Review of International Anti-Money Laundering Research: A Scientometrical Perspective, p. 7 and p. 9
[41] *See* Zünd (1990) in Der Schweizer Treuhänder: Monatsschrift für Wirtschaftsprüfung, Rechnungswesen, Unternehmens- und Steuerberatung: offizielles Organ der Treuhand-Kammer
[42] *See* Bernasconi (1988): Finanzunterwelt. Gegen Wirtschaftskriminalität und organisiertes Verbrechen
[43] *See* FATF (2012): The FATF Recommendations
[44] *See* Unger/Rawlings/Siegel/Ferwerda/de Kruijf/Busuioc/Wokke (2006). The amounts and effects of money laundering
[45] *See* Bongard (2001): Wirtschaftsfaktor Geldwäsche
[46] *See* Kirsch (2006): Systematik der Geldwäschetechniken
[47] *See* Schütte, R. (1998): Referenzmodellierung: Anforderungen der Praxis und methodische Konzepte
[48] *See* Gajewski (2004): Referenzmodell zur Beschreibung der Geschäftsprozesse von After-Sales-Dienstleistungen unter besonderer Berücksichtigung des Mobile Business
[49] *See* Noran (2006): Using Reference Models in Enterprise Architecture: An Example
[50] *See* Kotusev (2017): A Frameworks-Free Look at Enterprise Architecture
[51] *See* Timm/Zasada/Thiede (2016): Building a Reference Model for Anti-Money Laundering in the Financial Sector
[52] *See* Timm/Sandkuhl (2018): Towards a Reference Compliance Organization in the Financial Sector

chapter 2

Money laundering

To understand how financial institutions are managing the problem of money laundering it is needed to answer the question what money laundering actually is. Beside the national regulations, which have been derived from the corresponding EU AML-Directives, there is no other legal basis that can be assumed as relevant for the question. Yet, there are a lot of different interpretations of the term "money laundering". This chapter is structured as follows: Section 2.1. discusses the term "money laundering". Section 2.2. provides an overview over the most common models and processes of money laundering. In sections 2.3. and 2.4. I will show a couple of examples and a short overview over the trends in money laundering found in the literature before summarizing the findings in section 2.5.

2.1. Definition

In 2006 the Utrecht University School of Economics published a report "The amounts and the effects of money laundering"[53]. In this report the authors made a linguistic analysis of 18 different definitions what money laundering is[54]. The key finding from this report is that the act of money laundering could be understood completely differently depending on the point of view or context – economic, social, legal. One main difference in the identified definitions is the understanding of what "money" actually is. It can be understood as "*stock*" or "*flow*", "*income*" or even "*wealth*". Some of the definitions refer to illegal actions that are either criminal or civil offences or both. For example, it is illegal to bet on sport events in an unlicensed betting office but is not a criminal offence to do so. Another identified difference can be found in the goals of money laundering – it is defined as "*trying to hide the source*" of illegal or criminal income or as "*making it appear legal*"[55]. Therefore, with the goal to define one common strategy for the fight against money laundering it is important to find one common definition of money laundering, although there are different penal codes in the different countries. To "*launder*" money means to "*wash*" their criminal origin in order to make them appear legal. Many cases of money laundering from the past show that there are no boundaries, limits or rules how laundering works – it is always about hiding the money from the public and then showing it up "cleaned" and "dried". It can be concluded that the criminals are getting more and more familiar with the national and

[53] *See* Unger et al., (2006): The amounts and effects of money laundering
[54] *See* Ibid., pp. 20-29
[55] *Cf.* Ibid., p. 9

international regulations and that they can avoid them successfully. During the years the term "money laundering" was related to the washing of money from drug dealing and human trafficking. Meanwhile we can see cases of exploiting the digitalization of the society. Currently, the definition given by the FATF includes the financing of terrorism. This development and extension of the definition has the goal of achieving an international standard beside the existing national variations of this definition. It is hard to define, for example, only from a legal point of view what money laundering includes and what it excludes since the cases of money laundering need more broad understanding of the reasons, different typologies, economic and social effects of this criminal activity.

In Austria the following definitions of the term "money laundering" can be found:

§ 43 (2) Bilanzbuchhaltungsgesetz (BiBuG) and **§ 87 Wirtschaftstreuhandberufsgesetz (WTBG)** define "money laundering" as[56]:

"*a) the exchange or transfer of property, knowing that such property originates from criminal activity, for the purpose of concealing or concealing the illegal origin of the property or assisting persons involved in such activity to avoid the legal consequences of their actions, or*

b) concealment or concealment of the true nature, origin, location, disposal or movement of property or of rights or ownership of property, knowing that such property originates from criminal activity or from participation in such activity, or

c) the acquisition, possession or use of property if the person concerned was aware, when taking over such property, that it came from criminal activity or from participation in such activity, or

d) participation in any of the acts listed under a), b) and c), mergers for the performance of such act, attempts at such an act, aiding, abetting or advising for the performance of such an act or facilitating its performance."

In **§ 365n Gewerbeordnung 1994 (GewO)**[57] the term is referencing to the definition of the criminal offence "money laundering", defined in **§ 165** of the Austrian Penal Code[58]:

*""Money laundering" means the criminal offence pursuant to **§ 165 StGB**, [...], including assets arising from a criminal offence committed by the offender himself (self money laundering)*"[59].

---

[56] Bundesgesetz über die Bilanzbuchhaltungsberufe (Bilanzbuchhaltungsgesetz 2014 – BiBuG 2014), **§ 43 (2)**, Fassung vom 25.06.2018 and Bundesgesetz über die Wirtschaftstreuhandberufe (Wirtschaftstreuhandberufsgesetz 2017 – WTBG 2017), **§ 87**, Fassung vom 25.06.2018, translated from German:
„[…] *bedeutet „Geldwäsche" die folgenden Handlungen, wenn sie vorsätzlich begangen werden:*
a) der Umtausch oder Transfer von Vermögensgegenständen in Kenntnis der Tatsache, dass diese Vermögensgegenstände aus einer kriminellen Tätigkeit stammen, zum Zwecke der Verheimlichung oder Verschleierung des illegalen Ursprungs der Vermögensgegenstände oder der Unterstützung von Personen, die an einer solchen Tätigkeit beteiligt sind, damit diese den Rechtsfolgen ihrer Tat entgehen oder
b) die Verheimlichung oder Verschleierung der wahren Natur, Herkunft, Lage, Verfügung oder Bewegung von Vermögensgegenständen oder von Rechten oder Eigentum an Vermögensgegenständen in Kenntnis der Tatsache, dass diese Vermögensgegenstände aus einer kriminellen Tätigkeit oder aus der Teilnahme an einer solchen Tätigkeit stammen oder
c) der Erwerb, der Besitz oder die Verwendung von Vermögensgegenständen, wenn dem Betreffenden bei der Übernahme dieser Vermögensgegenstände bekannt war, dass sie aus einer kriminellen Tätigkeit oder aus der Teilnahme an einer solchen Tätigkeit stammen oder
d) die Beteiligung an einer der unter lit. a, b und c aufgeführten Handlungen, Zusammenschlüsse zur Ausführung einer solchen Handlung, Versuche einer solchen Handlung, Beihilfe, Anstiftung oder Beratung zur Ausführung einer solchen Handlung oder Erleichterung ihrer Ausführung"

[57] **§ 365n GewO (1994)**: Gewerbeordnung 1994 – GewO 1994, Fassung vom 20.06.2018

[58] **§ 165 StGB**: Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB), Fassung vom 20.06.2018, see section 3.1.1. for more information about the criminal offence „money laundering"

2.2. Money laundering models

Money laundering is usually described as a particularly opaque, mysterious or elusive form of crime. The reasons for this can be seen in the fact that the act of money laundering depends largely on the successful concealment of the true origin of funds. A successful money laundering process is that which is unknown to the authorities or financial institutions. All ideas, models and methods on how money laundering works are based on studies of uncovered cases or by expert assessments. Based on such analyses particular patterns and logic can be derived which leads to better understanding of the process and thus to adequate political, legal and economical reactions. Mainly, there are two types of money laundering: chronologically oriented and circular models. The first type represents the process as a linear function of chronologically executed steps where in the end the integration of "washed" funds in the legal financial system takes place. The second type describes the money laundering as a repeating loop of actions with a continuous money flow on the border between the legality and the illegality. Such structure has the aim of keeping the money laundering system alive and therefore stable – criminal offences generate illicit profit following which this profit is laundered and partly re-invested in criminal activities again[60]. In the 1980s and 1990s attempts were made to systemize and to describe various money laundering schemes. The main aspect of this development was the definition and identification of approaches for combating the money laundering[61].

2.2.1. Two-phase model by Bernasconi

Prof. Dr. h.c. Paolo Bernasconi provided one of the simplest models to explain money laundering which distinguishes between the technical, geographical and time aspects of the money laundering. The model also distinguishes first and second-degree money laundering.

Money laundering first- and second-degree

First-degree money laundering involves the laundering of assets - usually cash - that originate directly from a criminal offence. After the first laundering phase the pre-washed funds are still logically related to the main offence and must therefore be completely "*exempted from the smell of illegality*" and reintegrated into the legal economic cycle (so-called "recycling") in the course of second-degree money laundering[62].

Country of trade and Country of money laundering

These two artificial terms denote two categories of countries: in the "country of trade" the production, processing and distribution of illegal proceeds take place, while in the "country of money laundering" the actual act of laundering happens (usually international and offshore financial institution and countries)[63].

Timeframe

---

[59] **§ 365n GewO (1994)**, Fassung vom 20.06.2018, translated from German: *„„Geldwäsche" der Straftatbestand gemäß **§ 165 StGB** […], unter Einbeziehung von Vermögensbestandteilen, die aus einer strafbaren Handlung des Täters selbst herrühren (Eigengeldwäsche);*

[60] *Cf.* Fiedler/Krumma/Zanconato/McCarthy/Reh (2017): Das Geldwäscherisiko verschiedener Glücksspielarten, pp. 7-8

[61] *Cf.* Kirsch (2006): Systematik der Geldwäschetechniken, p.15

[62] Cf. Bongard (2001): Wirtschaftsfaktor Geldwäsche, p. 79

[63] Ibid., p. 79

The money laundering process is characterized by separated coordinated phases. In order to transform the criminal assets quickly and hide their origin, these phases are completed in short chronological order. The recycling phase, on the other hand, has a broader time horizon[64].

2.2.2. The three-layer model

This is one of the most common and well-known models to illustrate how money laundering is conducted and is based on the work of the United States Customs Service[65]. The model breaks down the process of money laundering into three (not always consecutive) phases – placement, layering and integration. The international compliance association (ICA) describes the three-layer model as "*highly simplistic*"[66]:

Placement is the first step of the process when the funds are injected in the legal financial system. This is the step where the money (usually in form of cash or virtual currency[67]) leaves its source. Afterwards comes the placement into circulation through financial institutions like banks, insurance companies, either local or abroad or both. This step corresponds to the first-degree money laundering, described by Bernasconi.

Layering is the most significant step of the processes. It involves numerous money splits and transactions with the goal to isolate and therefore hide the criminal origin of the proceeds. Basically, every transaction corresponds to a new layer. Several transactions lead then to a transactions network that is almost impossible to trace by the authorities. By changing the location (mostly a country with strict banking secrecy laws or an offshore company) but also by changing the type of proceeds a new layer is being added.

Integration is the final step from the process when the "laundered" money is introduced to the legal economy. The integration happens through the banking system. Therefore, the money appears as a legal business profit. The integration step is split into a *justification* step and an *investment* step. The goal of justification is to "show" to the world the legal origin of the criminal proceeds and the goal of the investment step is to use the criminal proceeds for personal benefit.

---

[64] Ibid., p. 79

[65] *Cf.* The Secretary of the Treasury, the Board of Governors of the Federal Reserve System, the Securities and Exchange Commission (2002): A report to congress in accordance with § 356(c) of the uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism act of 2001 (USA Patriot Act), pp. 7-10

Please note: The former US Customs Service is since 2003 known as „*Bureau of Customs and Border Protection* and *Immigration and Customs Enforcement*" part of the „*Department of Homeland Security*" and is responsible for customs revenues, protection against smuggling and illegal goods and border controls

[66] International Compliance Association (2018): What is money laundering? and
Cf. OECD (2009): Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors, p. 11

[67] *See* The European Parliament and the Council of the European Union (2018): Directive (EU) 2018/843 of the European Parliament and of the Council, Article 1 (2) d.): virtual currencies are "*digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically*"

2.2.3. Model by Zünd

Swiss-born Andre Zünd describes the money laundering process in ten phases analogous to the natural water cycle. He assigns a money laundering phase to each of the individual stages of the water cycle[68].

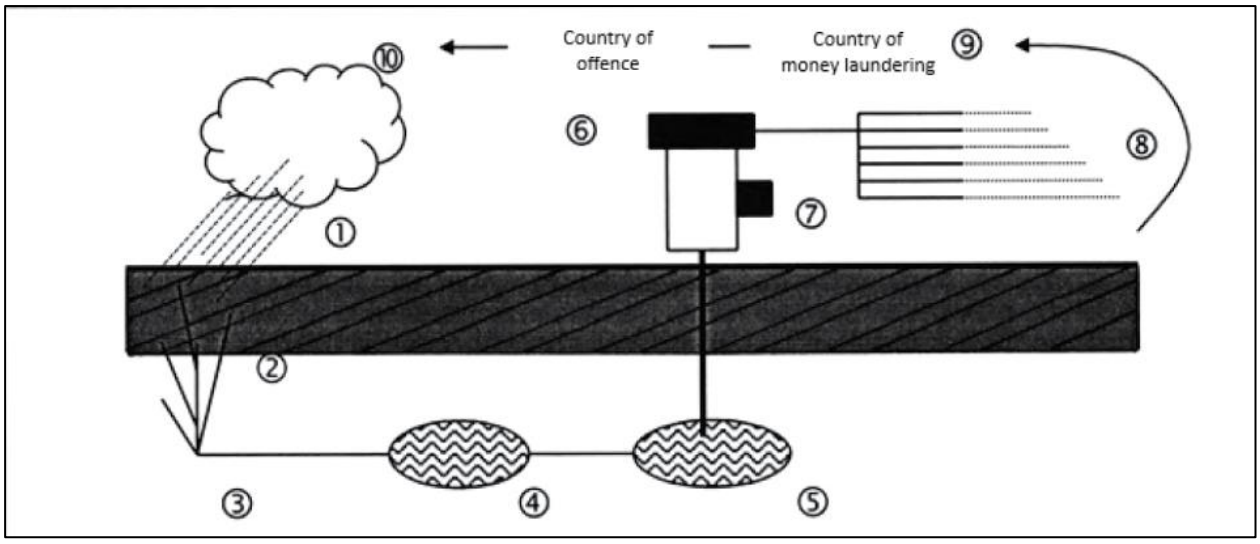

Figure 1 Money laundering process by Zünd (© *Bongard (2001)*)

1.) *"Rainfall in the country of offence":* As a result of a criminal activity, for example drug dealing, small amounts of cash are generated

2.) "Leaching" (first "washing" step): The "dirty" funds are being collected in one central location within the criminal organization. The collected money is then converted to banknotes with higher denomination or other assets.

3.) "Groundwater streams" ("building pools"): The funds from different "streams" are being concentrated further and collected within the organization and converted again into other assets, for example luxury goods or bearer securities.

4.) "Groundwater see" ("First preparation phase"): The collected funds are being handed over to a special money laundering unit within the organization or to an external money launderer. The funds are then ready to be transferred from "country of offence" to "country of money laundering".

5.) "Groundwater see" ("Second preparation phase"): After the transfer in the country of money laundering the funds are being taken over by another money laundering specialist and prepared for legalization.

6.) "Pump station": The funds are being transferred in the legal financial system mostly by opening of multiple bank accounts or by purchasing further assets like shares, gold or diamonds. In countries without identification or verification or reporting obligations this step is relatively easy to implement.

7.) "Filtering" (second "washing" step): If it was not possible to enter the legal financial cycle the funds could be washed again so they can obtain a legal origin. This can be done by the involvement of gatekeepers[69], straw men[70] or the establishment of offshore companies.

[68] *Cf.* Kirsch (2006): Systematik der Geldwäschetechniken, p.19 and
Cf. Bongard (2001): Wirtschaftsfaktor Geldwäsche: Analyse und Bekämpfung, p. 83

8.) “Injection” / “Integration”: In order to hide the criminal origin of the funds deeper the money is being transferred multiple times to numerous accounts. Any short-term investment (e. g. gold) is being replaced by medium-term investment (e. g. shares). This is how the funds are progressively becoming legal. A connection between the assets and the criminal offence(s) from the past is then hard to establish.

9.) “Evaporation”: The funds are now finally washed and can be transferred worldwide completely legal including in the country of offence. The cycle is therefore closed.

10.) “Rainfall in the country of offence”: The laundered and returned funds can be used to finance further illegal activities, invest in the international capital, financial markets and/or in other legal activities.

2.2.4. Four sectors model by Müller

The four-sector model introduced by economist Cristof Müller in the early 1990s is also based on the idea of the closed cycle of money laundering by Zünd. It attempts to describe the entire money laundering process in an abstract manner using a four-field matrix which is formed by two pairs of bi-poles, “Country of trade” / “country of money laundering”, as well as between legality/illegality[71]. This results in four clearly defined sectors:

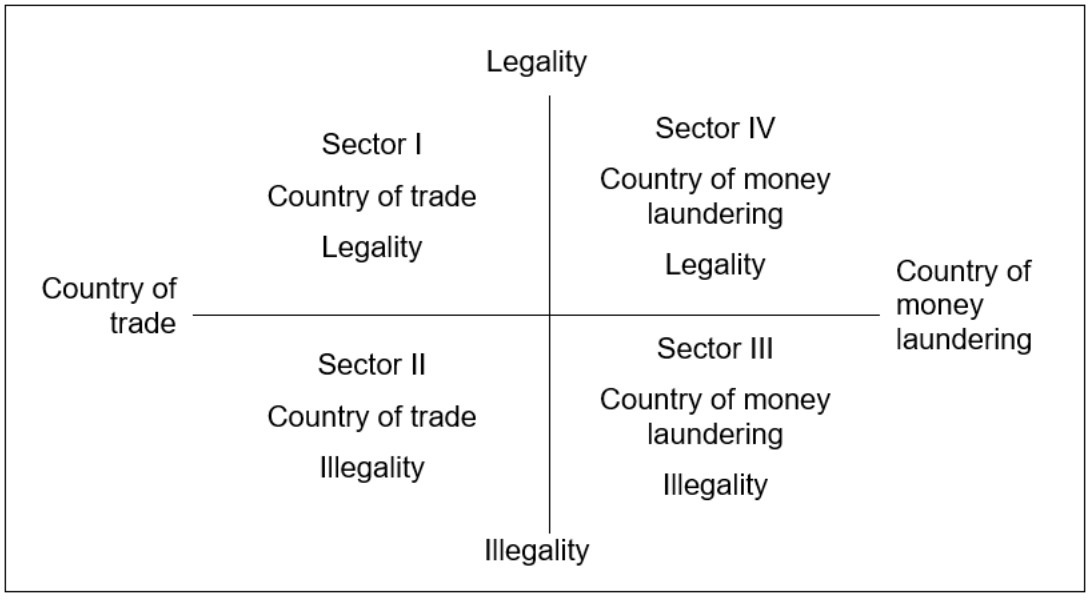

Figure 2 Four sectors model by Müller

The model process begins at the input interface (accumulation of dirty funds, below sector II) and ends with the outflow of the laundered funds at the output interface (above sector I). Each sector contains a specific processing and a refining process. The money laundering process takes place both through

[69] FATF (2010): Global Money Laundering & Terrorist Financing Threat Assessment, p. 44: “*Gatekeepers are, essentially, individuals that “protect the gates to the financial system” through which potential users of the system, including launderers, must pass in order to be successful. As a result of their status they have the ability to furnish access to the various functions that might help criminals to move or conceal their funds.*”

[70] OECD (2009): Money Laundering Awareness: Handbook for Tax Examiners and Tax Auditors, p. 32: *“Straw man/straw men or nominees, perhaps a relative of the criminal or a corporation, often offshore, is used as the registered owner of the real estate property. The criminal is therefore able to remain anonymous.”*

[71] *Cf.* Bongard (2001): Wirtschaftsfaktor Geldwäsche: Analyse und Bekämpfung, p. 85

sectoral "black box" processes and by crossing sector boundaries. Müller distinguishes between 3 different scenarios of money laundering depending on the legal framework (e. g. AML measures, reporting requirements)[72]:

- Scenario 1: *Lack of defence* (no AML policy, no reporting requirements)

In this scenario the illicit money is easily transferred from Sector II ("Country of trade"/ "Illegality") to Sector I ("Country of trade" / "Legality"), then to Sector IV ("Country of money laundering" / "Legality") and finally back completely "washed" to Sector I without any further effort.

- Scenario 2: *Identification and verification policy in the country of trade*

In this case the criminal funds must be smuggled from Sector II to Sector III ("Country of money laundering" / "Illegality"). From there on there are no further barriers to transferring the money back into the legal financial system.

- Scenario 3: *Identification and verification policy in the country of trade and in the country of money laundering*

In such a scenario the criminals must move quickly into another country of money laundering without AML policy in order to avoid any detection.

2.2.5. The cycle model by FED

Another form of a model that underscores the cyclical nature of money laundering treatment is the cycle model developed by the Federal Reserve System (FED) in the USA in 1990[73]: the model represents a combination of the three-phase model and the cycle model by Zünd and considers criminal offences or prohibited activities outside drug trafficking. It also shows that funds of criminal origin do not necessarily have to go through every phase in order to continue to be used. In this way money launderers can use their income from previous offenses directly to finance further illegal activities. It is also possible, however, that there may be no need to blur the paper trail by investing the money immediately in companies. By omitting and skipping individual phases the complexity and flexibility of money laundering treatment become more complex and flexible.

2.2.6. Summary

There is no definite answer which money laundering model, mechanisms or phases are most frequently or most commonly used. The separate phases may overlap over time – for example integration may be just an additional layer in the layering phase. When analyzing a money laundering case, it is important not only to understand the individual steps but also the logic on which the steps are based upon. The process of money laundering can be seen as a function of activities with an input and an output. Therefore, to define a money laundering pattern it makes sense to analyze the different phases, but also, based on further information, to distinguish between and to focus on the particularities and anomalies of these phases. Only then it will be possible to observe and define a money laundering process as such. The separate steps of a money laundering process are in most cases hard to track, difficult to detect and almost impossible to identify as such because in their core

[72] *Cf.* Schneider/Dreer/Riegler (2006): Geldwäsche, p. 36
[73] *Cf.* Kirsch (2006): Systematik der Geldwäschetechniken, p.21

sense and function they are completely legal actions (for example, betting on a football game or donating). Only when the criminal origin of the funds is detected, e.g. there is an interplay between a crime and criminal prosecution, one can speak of intentional money laundering. Even if the conditions change (for example stricter national regulatory or stricter banking policy) it does not mean that the problem is solved, and that money laundering will vanish. It is more likely that new alternative methods of laundering and integration of criminal assets back to the legal financial system will be introduced. Therefore, it makes sense not only to apply the policy "follow-the-money" but to consider the context of specific criminal offences – like the organized crime. In its core the organized crime is a network structure so the fight against money laundering should be one too[74].

2.3. Examples of money laundering

The FATF identified in 2003 and 2004 in its "Report on Money Laundering Typologies"[75] different areas of the financial sector like the gold and diamond markets, credit and debit cards, that are potentially vulnerable to money laundering. Meanwhile the list of problematic areas grows and the number of potential sources of money laundering increases. One thing must be considered – the higher the anonymity of the person or company is, the weaker the money laundering detection implementation is, thereby increasing the risk of money laundering. This is for example the case with the casinos or high-risk investment strategies – both areas are identified with high cash flow volumes and numerous transactions. But both areas are in most of the countries completely legal business models.

In the literature[76] one can find a lot of examples of money laundering in the financial and real sectors. In the last years an enormous number of different techniques for laundering were detected and published in order to warn the authorities and financial institutions. In this section I will give just a small set of examples how money laundering works based on historical events from the last 30 years. At the end I will show the current trends in money laundering, according to the yearly Money laundering reports, published by BK in 2016[77] and 2017[78] and the report "From Suspicion to Action" published in 2017 by Europol[79].

Bank of Credit and Commerce International (1980)

BCCI, founded in 1972, was with its assets in around 20 billion USD the 7th largest private bank in world[80]. It was registered in Luxembourg but operated worldwide. In the mid-80s the bank came into focus of the intelligence services and financial regulators due to suspicious management decisions. It was found out that the bank was part of a massive worldwide money laundering fraud estimated to 24 billion USD and other financial crimes. The investigation showed that BCCI was actively supporting dictatorship regimes, arms smugglers and drug cartels. BCCI used a complex system of shell

[74] *Cf.* Fiedler/Krumma/Zanconato/McCarthy/Reh (2017): Das Geldwäscherisiko verschiedener Glücksspielarten, pp. 12-13
[75] *See* FATF (2003): Report on Money Laundering Typologies 2002-2003
[76] *See* Unger et al., (2006): The amounts and effects of money laundering, pp. 71-85
[77] *Cf.* Bundeskriminalamt Österreich (2016): Geldwäsche Jahresbericht, pp. 22-23
[78] *Cf.* Bundeskriminalamt Österreich (2017): Geldwäsche Jahresbericht, pp. 23-25
[79] *Cf.* EUROPOL (2017): From Suspicion to Action, pp.36-38
[80] *See* Kanas (2005): Pure contagion effects in international banking: The case of BCCI's failure, p. 2

companies and multi-layer organizational structure to hide the criminal activities[81]. The bank has been fined approximately 15 billion USD and was closed by the international regulators in 1991, while still owing around 10 billion USD to its creditors.

Nauru (1998)

Geographically Nauru is a rocky island in the northeast of Australia. But it was also called by the New York Times Magazine "Public Enemy No. 1" [82]. In 1993 Nauru was a tax heaven for money launderers, with its 400 shell companies and "no questions asked" registration policy of companies. It is estimated, that only in 1998 Russian criminals were able to launder through shell banks approximately 72 billion USD. This was the result of a lack of any identification policy as the banks just did not ask who their customers are and where the money comes from[83]. This led to one of harshest sanctions against a country ever. Financial institutions from all over the world just forbid any US dollar transactions from and into Nauru. The situation started slowly improving for Nauru in 2001 when the country made a deal with the Australian government according to which Nauru will be a hosting center for asylum seekers that are trying to enter Australia illegally in exchange for Australia's help in cleaning up its act. After that Nauru closed its 400 shell banks which was followed by lifting of the sanctions and removal from FATF blacklist in 2005[84].

Wachovia (2010)

Before its acquisition by Wells Fargo and Company[85] in 2008 Wachovia was the 4th largest bank holding company in the U.S. It entered in Deferred Prosecution Agreement (DPA)[86] (meanwhile expired) after the biggest ever action taken under the Bank Secrecy Act in the U.S. Everything started with an investigation by the U.S. Drug Enforcement Agency (DEA) when it turned out that the Mexican drug cartels were smuggling US dollars across the U.S.-Mexican border (this being the profit from illegal drug dealing in the United States). The system that was used by the money launderers was based on the weaknesses of the financial system and the AML policies at that point in time and was stunningly simple. The smuggled money (from the U.S. into Mexico) was distributed to money exchangers. The distribution was followed by making deposits in local Mexican bank accounts. The Mexican banks did not check the origin of the money and therefore no further investigation was done. This allowed the placement of "dirty" money in the legal sector in order to "wash" them. Part of the deposits was transferred back to the U.S. to bank accounts in Wachovia bank where, again, no verification of the origin of the money was made. This method allowed the transfer from approximately 400 billion USD between 2004 and 2007 and the re-integration from illegal funds back to country of

[81] *See* Kerry/Brown (1992): A Report to the Committee on Foreign Relations
[82] *See* Hitt (2000): The Billion-Dollar Shack, article in The New York Times Magazine from December 10, 2000
[83] *See* Hilzenrath, D. S. (1999): Tiny Island Shelters Huge Cash Flows, article in Washington Post from October 28, 1999
[84] *Cf.* Wasserman (2002): Dirty money, p. 20
[85] Wells Fargo & Company is an American multinational financial services company
[86] Lewis (2018): Deferred Prosecution Agreements: Key Differences Between the US and UK, p.1: "*A deferred prosecution agreement (DPA) generally is an arrangement reached between a prosecutor and a company to resolve a matter that could otherwise be prosecuted. The agreement allows a prosecution to be suspended for a defined period, provided the organization meets certain specified conditions. A DPA is made with the approval or under the supervision of a judge. DPAs can be used in potential cases of fraud, bribery, and other economic crime.*"

origin. Despite the lack of adequate AML program and transfer monitoring the penalty paid by Wachovia in 2010 was “only” 110 million USD[87].

HSBC (2012)

In 2012 HSBC, a British banking and financial services holding, one of the largest worldwide, had to pay 1.9 billion USD fine for not having a proper and adequate AML due diligence policy, helping drug cartels to launder money, violating sanctions against the Islamic Republic of Iran and other financial crimes. The amount of unmonitored transactions was estimated at around 60 trillion USD. There were approximately 17 000 unchecked reports of suspicious financial activities. In addition, multiple areas of abuse were identified as only some are listed below:

- Servicing high risk affiliates: The US affiliate of HSBC, HBUS, did treat HSBC Bank Mexico as a low risk corresponding bank despite its location in a country dealing with very high drug dealing, money laundering challenges, number of high-risk clients, weak AML jurisdiction (caused by the bank secrecy) and ML prevention and detection policy. It is known that the HSBC Bank Mexico transported physically around 7 billion USD to HBUS between 2007 and 2008.
- Ignoring terrorist financing links: HSBC supplied banks in Saudi Arabia and Bangladesh with US dollars and financial services despite their known connections to terrorist financing.

The amount of money being laundered is being estimated at 7.5 billion USD[88].

Meanwhile, as of 2018 HSBC is working together with crime investigators to develop an artificial intelligence (AI) system to track suspicious financial activities and therefore detect money laundering in real-time[89].

Russian Laundromat (2017)

Between January 2011 and October 2014 around 20.8 billion USD from Russian banks were laundered. The laundering system was exposed by The Organized Crime and Corruption Reporting Project (OCCRP) in 2014 showing a very complex and organized laundering structure and a seven-step process involving shell companies, falsified loans, debts and corruption. The organizers of the laundromat established 21 companies based in the UK, Cyprus and New Zealand. The companies were used to transfer the money out of Russia. Meanwhile in Russia to other Russian companies were preparing to transfer the money outside the country. In order to do this the criminals created a system of fake debts between these shell companies, following which a Moldavian judge ordered one of the Russian companies to pay that debt to accounts controlled by the court in Modindconbank in Moldova. Modindconbank was flooded with cash estimated at 8 billion USD, sent directly from the Russian companies. Soon after that the amount was withdrawn from the accounts and distributed all over the world. Another 13 billion USD were directly transferred to Trasta Komercbanka in Latvia, while the location of the bank in the European Union helped the criminal make the transactions less suspicious

[87] *See* Vulliamy (2011): How a big US bank laundered billions from Mexico's murderous drug gangs, article in The Guardian from April 3, 2011
[88] *See* U.S. Department of Justice (2012): Documents and Resources from the December 11, 2012, HSBC Press Conference
[89] *See* Arnold (2018): HSBC brings in AI to help spot money laundering, article in Financial Times from April 9, 2018

for the national and international authorities and financial institutions. This is how the money appeared as "cleaned" European money that could be legally reused and reintegrated by the criminals[90].

There are many other cases of financial institutions, insurance companies and organizations for which it is known that they were part of money laundering mechanisms[91]. One of the last uncovered cases when an Austrian bank was involved and meanwhile penalized[92] was the "Panama Papers" from the beginning 2017[93].

In all cases so far, the related financial organizations were unintentionally part of a laundering scheme. And almost always it is because there was a massive lack of AML controls and adequate AML mechanisms. Beside the fact that the national and international regulation is getting stricter the criminals are getting smarter, the laundering processes are getting more and more complex and one has the feeling that in the next couple of years we will witness the next big money laundering scandals especially when considering the context of new technologies, like AI, machine learning and (still) unregulated money transfer instruments like the crypto- or virtual currencies[94].

2.4. Current trends in money laundering

The growth of the global markets

One of the major burdens in the combat against ML stated by Europol is the "*the growing demand for online services and related internet payment systems, and the rise in cross-border transactions in volume and frequency*"[95]. It is a burden mainly because the growing numbers of transactions make the tasks of the FIUs challenging: "*The impact of new technologies on the financial system and the development of borderless virtual environments call for reflection on how to adapt policies which are meant to be supervised only at national level, while the underlying business is already transnational and globalised in its own nature: there is an urgent need for a supranational overview.*"[96]. Europol describe the duplication and fragmentation of data because it "*limits the efficiency and effectiveness of reporting entities and FIUs*"[97]. There are known cases when reporting entities (like banks) have detected suspicious patterns and schemes across their networks but due to legal restrictions are unable to forward and share their analysis as a "big-picture" – they are obliged to fragment the information and provide only pieces of the puzzle that is relevant for the FIU in the corresponding country: "*In turn, this requires time and effort from FIUs to recreate the global vision*

[90] *See* OCCRP (2017): The Russian Laundromat Exposed
[91] *Cf.* Office of the Comptroller of the Currency (2002): Money Laundering: A Banker' s Guide to Avoiding Problems, pp. 26-29
[92] *See* Der Standard (2018): Raiffeisen International fasst 2,7 Millionen Euro Strafe aus
[93] *See* Trend (2016)*: Panama Papers: RBI: "Gänzliche Durchleuchtung nicht möglich":* The journalist investigation claims, that Raiffeisen International (RBI) is said to have granted millions in loans to companies in the entourage of the Ukrainian president and "chocolate king" Petro Poroschenko. Experts consider such loans to be an indication of money laundering.
[94] Chohan (2017): Cryptocurrencies: A Brief Thematic Review, p. 2: *"a cryptocurrency can be thought of as a digital asset that is constructed to function as a medium of exchange, premised on the technology of cryptography, to secure the transactional flow, as well as to control the creation of additional units of the currency*"
[95] EUROPOL (2017): From Suspicion to Action, p. 36
[96] Ibid., p. 36
[97] Ibid., p. 36

that the private sector already had. […] *while an isolated transaction at domestic level may appear innocuous, when viewed in its global context, the relevance becomes more apparent*"[98].

The digitalization of the money

One of biggest issues that the money launderers have is how to keep their identity and the origin of the criminal funds hidden from the authorities and financial institutions. In the last few years one can observe the increasing willingness of the society to make the IT communications more secure, encrypted and even anonymous, which resulted in a technological revolution[99]. Terms like "Tor"[100], "onion"[101], "darknet"[102], "deep web", "blockchain"[103] and others have become synonyms to online anonymity and are successfully used by the users nowadays but are also massively exploited by criminals not only as an online market for drug dealing or human trafficking but for money laundering as well. The opportunities which these technologies are offering made the job of the law enforcement agencies still more challenging. Every anonymous money transaction or payment is done without verification of the identification and therefore constitutes a potential step of a money laundering process. Such situation leads to problems for the financial institutions mainly in the area of the customer due diligence – it is getting harder for the financial institution to implement this principle, because of the easy, worldwide access to the financial markets, the speed and volumes of the transactions and in many of the cases – the missing face-to-face contact between the customer and the institution. One of the aims of the Fifth EU AML Directive is to improve the current situation. In 2017, in the yearly report regarding the combat against ML, BK states that "*The use of cryptocurrencies for the acquisition of illegal goods or services is mainly carried out in the darknet. This is called "Criminal-2-Criminal-Payments" (C2C). However, more and more criminals are demanding ransom money in the form of cryptocurrencies from their potential victims, who are, for example, affected by a Ransomware or Distributed Denial of Service (DDoS) attack, for which the term "Victim-2-Criminal" (V2C) is commonly used.*"[104].

Cash will not disappear soon

Despite the digitalization of the financial transactions Europol is confident that cash as a monetary payment method won't disappear soon and even will become more attractive for money launderers and other criminals. Almost 40% of the FIUs Europe-wide reported that the use of cash (deposits, withdrawals and cash transactions) is still the major reason which triggers the generation of STRs[105].

---

[98] Ibid., p. 36
[99] *Cf.* The Home Office of the United Kingdom (2019): Future technology trends in security, p. 14.
[100] Tor is freeware, that enables the anonymous communication online
[101] .onion is domain suffix for anonymous service, reachable via the Tor network
[102] Darknet and Deep Web: Darknet is a subset of the Deep Web; Darknet is not directly accessible from the outside and Deep Web is part of the World Wide Web without being indexed by any search engine
[103] blockchain: is a digitized, decentralized, public ledger of all cryptocurrency transactions
[104] *See* Bundeskriminalamt Österreich (2017): Geldwäsche Jahresbericht, p. 25, translated from German: "*Der Einsatz von Kryptowährungen für den Erwerb von illegalen Gütern oder Dienstleistungen wird vor allem im Darknet vollzogen. Dabei spricht man von „Criminal-2-Criminal-Payments" (C2C). Es ist jedoch auch der Trend sichtbar, dass immer mehr Straftäter von ihren potentiellen Opfern, die z.B. von einer Ransomwareoder Distributed Denial of Service (DDoS)-Attacke betroffen sind, das Lösegeld in Form von Kryptowährungen einfordern, wofür der Begriff „Victim-2-Criminal" (V2C) gebräuchlich ist.*"
[105] *Cf.* EUROPOL (2017): From Suspicion to Action, p. 21

The 2017 Report published by the Europol's Financial Intelligence Group in 2015[106] showed that between 2012 and 2014 the major reason for reporting suspicious transactions to the FIUs Europe-wide was the use of cash. One interesting aspect of the report concerns the use of the EUR 500 banknotes which will not be issued by the European Central Bank (ECB) at the end of 2018 anymore[107]: "[…] *the EUR 500 note alone accounts for around 30% of the value of banknotes in circulation* […] *operational cases evidenced that the EUR 500 banknote is used disproportionally in the various stages of criminal activity and the money laundering process.*"[108]. This, of course, should not stop the work of law enforcement agencies, central banks and reporting entities: "*efforts should be made to address other means of transporting values across borders which will likely attract criminals, for example, other high denominations such as the EUR 200 and CHF 1000 notes, gold, precious metals and stones, high value watches and jewellery*"[109].

The use of social networking

The term "money mules", or money couriers, or "financial agents", is a relatively old phenomenon in the money laundering but it meanwhile has a new updated version which is the result of the massive use of social networks. Basically, it is a recruitment process of people on Facebook or Twitter who either offer the use of their bank account or open a new one so they can be used by criminals for money transfers. The task of the money mule is simple – receive and forward money into and from their account. There are two types of money mules: people who have been offered to work for a subsidiary of an international company as a contact person on-site or even as a manager for the newly opened branch in the country. Then, the person, meanwhile an "employee" of the company, must give her/his permission to her/his account or must open a new account on his/her name. Afterwards, the employee begins to receive orders for money transfers. The other type of a mule are people who were actively recruited by criminals and have been provided with falsified documents to open new accounts in different banks. These accounts are then mostly used for a small number of transactions in order to lower the risk of tracking and detecting.

CEO-Fraud or business engineering fraud

This is a highly profitable method for a financial fraud but also with a high risk of detection. It results in an unauthorized access to corporate accounts. In the moment when the criminals have access to a company's finances the transfer from the accounts is started – the money is transferred to different accounts using money mules. At the same time the banks have the impression that the executed order is completely regular. This false impression is created either by direct hacking into the IT system of the company (and therefore misusing the company's email address) or by falsifying the company invoices and other documents.

[106] *Cf.* Ibid., p. 22
[107] *Cf.* European Central Bank (2016): ECB ends production and issuance of €500 banknote
[108] EUROPOL (2017): From Suspicion to Action, p. 22
[109] Ibid., p. 22

2.5. Summary

In this chapter I described what money laundering is and gave examples from the recent years. Finally, I summarized the current trends in money laundering and the upcoming challenges that the society will have in the fight against money laundering. As one can see money laundering is a multi-layered topic with many obstacles and due to its variety – with no typical or uniform procedures. It is a crime as any other criminal offence and therefore it must be treated as such. The amount of money being laundered has direct negative impacts on the society[110]. Different studies and statistical reports[111] estimate the amount of laundered money globally completely differently and the range between the estimations is huge. The reason for this are basically the different money laundering methodologies and approaches – if it is not impossible at least it will be extremely difficult to estimate the amount globally[112]. In 1998 the Managing Director of the IMF Michel Camdessus stated that the amount of laundered money might be between 2%-5% of the global GDP[113] - this estimation is not based on any documentation or study but on "*experts opinion*". The United Nations Office on Drugs and Crime (UNODC) in 2011 published a study[114] where the estimated amount in 2009 is around 1.6 trillion USD. Europol calculated that around 1% of the annual EU GDP "*is detected as being involved in suspect financial activity*"[115]. The director of Europol Mr. Rob Wainwright described in April 2018 the current situation around the combat against ML as a "black hole": "*We have created a whole ton of regulations* […] *the banks are spending $20 billion a year to run the compliance regime* […] *and we are seizing 1 percent of criminal assets every year in Europe.* […] *Europe is losing the fight against dirty money because it has used national solutions to tackle an international problem. That makes for a system filled with "inflexibilities," which prevents the "free-flowing exchange of information across borders."*"[116].

In the next two chapters I will focus on the legal aspects of the topic and on techniques for prevention and detection of money laundering. Only with a consolidated national jurisdiction (without throwing the financial institutions in an increasing sea of regulations and obligations) and with a proactive international cooperation the fight against money laundering could be more successful.

[110] *Cf.* Pasley/Anderson (2012): Study Guide for the CAMS Certification Examination, pp. 18-25
[111] *Cf.* Lilley (2013): Money Laundering Statistics
[112] *Cf.* Reuter/Truman (2004): Chasing Dirty Money: The Fight Against Money Laundering, p. 9
[113] International Money Fund (1998): Money Laundering: the Importance of International Countermeasures--Address by Michel Camdessus; Michel Camdessus, Managing Director of the International Monetary Fund at the Plenary Meeting of the Financial Action Task Force on Money Laundering, Paris, February 10, 1998*: "While we cannot guarantee the accuracy of our figures - and you have certainly a better evaluation than us - the estimates of the present scale of money laundering transactions are almost beyond imagination - 2 to 5 percent of global GDP would probably be a consensus range."*
[114] *Cf.* United Nations Office on Drugs and Crime (2011): Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes, p. 9
[115] EUROPOL (2017): From Suspicion to Action, p. 5
[116] Politico (2018): Europe is losing the fight against dirty money

chapter 3

Jurisdiction over money laundering

The goal of the most criminal activities is the generation of profit, where money laundering plays an essential role for the criminals. Their goals are to hide the illicit funds from the financial institutions and law enforcement authorities and to avoid any possible association between these funds and the criminal offences preceding the money laundering. The processes and methods of money laundering developed much earlier before their criminalization took place in the law. Until the late 1980s it was not classified as criminal offence. The first official definitions of the term "money laundering" as a crime were made in the United States and in the United Kingdom in 1986, while in 1982 the term was firstly used in an US court case[117]. Germany followed this development with the promulgation of "Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität"[118] in 1992. In Austria money laundering has been firstly mentioned in 1993 in **§165** of the Strafgesetzbuch[119]. In other jurisdictions, however, in the last years money laundering was given less priority as one can see in the list of NCCT published regularly by the FATF[120].

The Republic of Austria was known as an attractive country for the money launderers[121]. The reasons for this were said to lie in the stable currency formerly linked to the Deutsche Mark, the functioning financial system, the liberal foreign exchange policy, strict banking secrecy, the possibility of anonymous investment, a secure economy without significant labour conflicts, the stable political system and its central locations within Europe and thus close to the former Eastern bloc[122]. Nowadays the country has a relative low Basel AML Index[123] of 5.06 which puts the country on the 92nd place (out of 125). This could mean that the financial system is just not interesting for any criminal activities

---

[117] *See* US District Court for the Southern District of Florida (1982)

[118] *See* OrgKG (1992): Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG), Fassung vom 20.06.2018; (in English: Law to combat illegal drug trafficking and other manifestations of organized crime)

[119] *See* Bundesgesetzblatt für die Republik Österreich, ausgegeben am 30. Juli 1993

[120] The first list was published in June 2000, containing fifteen countries. 18 years later the only country left in the list is Democratic People's Republic of Korea (DPRK).

[121] *Cf.* Hufnagel (2004): Der Strafverteidiger unter dem Generalverdacht der Geldwäsche gemäß § 261 StGB, p. 38

[122] *Cf.* Ibid., p. 38

[123] The Basel AML index (https://index.baselgovernance.org/) measures and calculates the risk of money laundering and terrorist financing. The measurement is based only on public available information. To calculate the "risk score" a total of 14 indicators are considered, for example national AML/CFT regulations, corruption, political situation. The risk score represents "*a holistic assessment addressing structural as well as functional elements in the AML/CFT framework and is designed to indicate the risk level, i.e. the vulnerabilities of money laundering and terrorist financing within a country*". Since there is no quantitative data that can be aggregated, the index does not measure the existence of money laundering activity and does not calculate the amount of illicit financial money within a country.

anymore. In contradiction to this assumption two reports from the FATF published in 2016 and 2017 give a better understanding of the situation in Austria. In 2016 the FATF published a Mutual Evaluation Report (MER) giving a compliant rating of all 40 FATF recommendations[124]. The following key findings regarding the combat against money laundering in Austria were derived during the analysis (excerpt)[125]:

- "*Austria has a mixed understanding of its ML/TF risks. The National Risk Analysis (NRA)[126] does not provide a holistic picture of ML/TF risks that are present in the jurisdiction.*"
- "*Each competent authority has its own concept of ML/TF risks based on its practical experience; however, in most cases they do not match with each other and do not provide a complete picture of country's ML/TF risks.*"
- "*Austria did not demonstrate that it had any national anti-money laundering/countering the financing of terrorism (AML/CFT) policies.*"
- "*A-FIU functions well as a predicate offence and associated ML investigation unit, rather than as a financial intelligence unit. The approach of the FIU with regard to STR analysis is primarily investigative (as opposed to intelligence approach).*"
- "*Austria's ML offence is generally comprehensive and in line with the Vienna and Palermo Conventions[127]. But Austria does not pursue ML as a priority and in line with its profile as an international financial centre.*"
- "*Austria has a generally comprehensive framework for police powers and provisional and confiscation measures.*"
- "*The authorities have a good understanding of the terrorist financing (TF) risks, and Austria exhibits many characteristics of an effective system for investigating and prosecuting those involved in terrorist actions. The legal framework for the investigation and prosecution of terrorist and TF is generally sound and there are specialized authorities for investigation, intelligence and prosecution in these fields.*"
- "*Austria has not undertaken a domestic review and comprehensively looked at potential risks within the Non-profit organization (NPO) sector to identify which subset of NPOs that might be of particular risk of being misused for TF. There is insufficient monitoring and supervision of administrative requirements of the large majority of NPOs.*"
- "*Austria demonstrates many characteristics of an effective system for international co - operation.*"

These and other conclusions led to a situation that Austria was put under extended monitoring by the FATF. In 2017 a newer follow-up report[128] by the FATF analyses the progress made by Austria since publishing the MER in 2016. In the report the FATF stated that "*Austria has made good progress in addressing the technical compliance deficiencies identified in its MER*"[129]. However, the major critique was that each relevant authority in Austria has defined its own approach to identify ML/TF risks and its own way to mitigate them which is of course counterproductive. In 2018 in a newer follow-up report by the FATF two of the Recommendations regarding the beneficial ownership of legal

[124] *Cf.* FATF (2012): The FATF Recommendations
[125] FATF (2016): Anti-money laundering and counter-terrorist financing measures in Austria - 2016, pp. 3-4
[126] *See* Bundesministerium für Finanzen in Zusammenarbeit mit den zuständigen Ministerien und Behörden (2015-2016): Nationale Risikoanalyse Österreich
[127] More information about the mentioned conventions can be found in section 3.2.1
[128] *Cf.* FATF (2017): Anti-money laundering and counter-terrorist financing measures in Austria - 2017
[129] FATF (2017): Anti-money laundering and counter-terrorist financing measures in Austria – 2017, p. 13

persons and legal arrangements were positively re-rated from partially compliant to largely compliant[130].

Since the beginning of 2017 there is one consolidated money laundering act in Austria. The goal of the "Finanzmarkt-Geldwäschegesetz" (**FM-GwG**) was to implement the **Fourth Anti-Money Laundering EU Directive** (AMLD4)[131] and to consolidate the AML legal basis (previously implemented in various statutes, for example the Bankwesengesetz (**BWG**)[132], Versicherungsaufsichtsgesetz 2016 (**VAG 2016**)[133] and Wertpapieraufsichtsgesetz 2007 (**WAG 2007**)[134]). This replaces the regulations previously contained in various material laws and creates a uniform, clear legal basis for the supervisory activities of the Finanzmarktaufsichtsbehörde (FMA)[135].

In this chapter I will discuss the national regulations and international collaboration and standards regarding the money laundering with a focus on the newly regulated "Risk assessment on company level" (**§ 4 FM-GwG**), the due diligence (**§§ 5-9 FM GwG**) and reporting obligations (**§§ 16-18 FM-GwG**). Based on this literature research I will provide at the end a simple organigram showing the main communication flows between the obliged entities and the different authorities in Austria.

3.1. Territorial jurisdiction

As a member state of the European Union Austria's national legislation in the fight against money laundering is primarily influenced by the provisions of the EU money laundering directives[136]. In the following section I will show the legal aspects of the term "money laundering" in Austria. I will describe the core of the criminal offence, how it is legally understood[137], the verification (due diligence) and monitoring obligations of the financial institutions and other occupational groups together with the roles of the authorities.

3.1.1. The criminal offence "money laundering"

The money laundering and terrorist financing are subject to the penalty specified in **§§ 165 and 278d** of the **StGB**[138]. In this section only the act of money laundering will be discussed.

---

[130] *See* FATF (2018): Anti-money laundering and counter-terrorist financing measures in Austria - 2018

[131] *See* The European Parliament and the Council of the European Union (2015): Directive (EU) 2015/849

[132] *See* Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG), Fassung vom 31.12.2016, **§§ 40-40d**

[133] *See* Bundesgesetz über den Betrieb und die Beaufsichtigung der Vertragsversicherung (Versicherungsaufsichtsgesetz 2016 – VAG 2016), Fassung vom 31.12.2016, **§§ 128-135**

[134] *See* Bundesgesetz über die Beaufsichtigung von Wertpapierdienstleistungen (Wertpapieraufsichtsgesetz 2007 – WAG 2007), Fassung vom 31.12.2016

[135] Österreichische Finanzmarktaufsichtsbehörde (FMA), in Englisch Austrian Financial Market Authority

[136] More about the relevant EU directives can be found in section 3.2.2.

[137] FMA published in 2017 a translated version of the FM-GwG with following remark: *"All English translation of the authentic German text is unofficial and serves merely information purposes. The official wording in German can be found in the Austrian Federal Law Gazette (Bundesgesetzblatt; BGBl.). All translations have been prepared with great care, but linguistic compromises had to be made. The reader should also bear in mind that some provisions of these laws will remain unclear without certain background knowledge of the Austrian legal and political system. Please note that these laws may be amended in the future and check occasionally for updates.". A*ll translations of the FM-GwG are based on this publication.

[138] **§ 165 StGB (1993)**, Fassung vom 25.06.2018: *„(1) Wer Vermögensbestandteile, die aus einer mit mehr als einjährigen Freiheitsstrafe bedrohten Handlung oder einem Vergehen nach den §§ 223, 229, 289, 293, 295 oder nach den §§ 27 oder 30 Suchtmittelgesetz herrühren, verbirgt oder ihre Herkunft verschleiert, insbesondere, indem er im Rechtsverkehr über den Ursprung oder die wahre Beschaffenheit dieser Vermögensbestandteile, das Eigentum oder sonstige Rechte an ihnen, die Verfügungsbefugnis über sie, ihre Übertragung oder darüber, wo sie sich befinden, falsche Angaben macht, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.*

According to **§ 165 StGB,** money laundering is a follow-up[139] and thus a "*predicate offence-dependent*"[140] criminal act[141]. The ***object***[142] of the crime are ***assets***[143] derived from:

- a crime (according to **§ 17 StGB**)[144],
- an offence threatened with more than one year's imprisonment against third party property,
- an offence in accordance with **§§ 223, 229, 289, 293, 295 StGB**[145],
- an offence in accordance with **§§ 27 or 30 Suchtmittelgesetz (SMG),**
- a commercial offence against intangible property rights regulations,
- assets arising from a criminal financial offence of smuggling or evasion of import or export duties falling within the jurisdiction of the courts (according to **§ 35 Finanzstrafgesetz (FinStrG)**[146]).

The offence of money laundering is committed by anyone who conceals[147] or disguises[148] the origin of assets derived from a predicate offence in particular by providing false information in legal transactions about the origin or true nature, the right of ownership or disposition, other rights or the place of safekeeping, whereby conditional intent must be present with regard to the incriminated origin of the assets and the offence[149].

It is not necessary for the forms of committed offences according to **§ 165 (1) StGB** (concealment, disguise origin), that the assets origin from the criminal act of a third party. However, **§ 165 (4) StGB** states, that anyone who commits an offence in respect of a value exceeding EUR 50 000 or as a member of a criminal organization who participated in continuing money laundering is to be punished with a custodial sentence of one to ten years. Also, the money launderer may be the direct perpetrator himself (self-money laundering). **§ 165 (2) StGB** makes the acts of viewing, depositing, managing,

---

(2) Ebenso ist zu bestrafen, wer wissentlich Vermögensbestandteile an sich bringt, verwahrt, anlegt, verwaltet, umwandelt, verwertet oder einem Dritten überträgt, die aus einer in Abs. 1 genannten mit Strafe bedrohten Handlung eines anderen stammen.
(3) Ebenso ist zu bestrafen, wer wissentlich der Verfügungsmacht einer kriminellen Organisation (§ 278a) oder einer terroristischen Vereinigung (§ 278b) unterliegende Vermögensbestandteile in deren Auftrag oder Interesse an sich bringt, verwahrt, anlegt, verwaltet, umwandelt, verwertet oder einem Dritten überträgt.
(4) Wer die Tat in Bezug auf einen 50 000 Euro übersteigenden Wert oder als Mitglied einer kriminellen Vereinigung begeht, die sich zur fortgesetzten Geldwäscherei verbunden hat, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.
(5) Ein Vermögensbestandteil rührt aus einer strafbaren Handlung her, wenn ihn der Täter der strafbaren Handlung durch die Tat erlangt oder für ihre Begehung empfangen hat oder wenn sich in ihm der Wert des ursprünglich erlangten oder empfangenen Vermögenswertes verkörpert."

[139] Translated from German: „*Anschlussdelikt*"
[140] Translated from German: „*vortatabhängiges Delikt*"
[141] *Cf.* Bundeskriminalamt Österreich (2017): Geldwäsche Jahresbericht, p. 8-10
[142] Translated from German: „*Tatobjekt*"
[143] Translated from German: „*Vermögensbestandteile*": according to **§ 43, p. 3 BiBuG** „*Vermögensgegenstand*" means „*assets of all kinds, whether physical or intangible, movable or immovable, tangible or intangible, and legal instruments or documents in any form, including electronic or digital, conferring ownership or rights on such assets, including immaterial speculative objects such as units of virtual currencies and the gains in value attributable to them, but not mere savings such as unrealised losses in value, waivers of claims or savings on expenses or levies*"
(translated from German: "*Vermögenswerte aller Art, ob körperlich oder nichtkörperlich, beweglich oder unbeweglich, materiell oder immateriell, und Rechtstitel oder Urkunden in jeder — einschließlich elektronischer oder digitaler — Form, die das Eigentumsrecht oder Rechte an solchen Vermögenswerten belegen; dazu zählen auch unkörperliche Spekulationsobjekte wie Einheiten virtueller Währungen und die auf diese entfallenden Wertzuwächse, nicht aber bloße Ersparnisse wie etwa nicht eingetretene Wertverluste, Forderungsverzichte oder ersparte Aus- oder Abgaben*")
[144] *See* section 3.1.2. for more information about the predicate offences
[145] *See* section 3.1.2. for more information about the predicate offences
[146] Bundesgesetz vom 26. Juni 1958, betreffend das Finanzstrafrecht und das Finanzstrafverfahrensrecht (Finanzstrafgesetz - FinStrG.), Fassung vom 25.06.2018
[147] Translated from German: „*Verbergen*"
[148] Translated from German: „*Herkunft verschleiern*"
[149] *Cf.* Bundeskriminalamt Österreich (2017): Geldwäsche Jahresbericht, p. 8-10

investing, converting, exploiting or transferring incriminated assets to third parties punishable. Therefore, in order to make a differentiation between legal and illegal forms of assets it is needed to have knowledge about the criminal origin of the property. According to **§ 165 (3) StGB**, it is also punishable to acquire, store, administer, invest, convert, dispose of or transfer to third-party assets that are under the control of a criminal organization or a terrorist group. Here no predicate offence in the sense of **§ 165 (1) StGB** is necessary. In this case both legally and illegally acquired property or assets are considered as objects of crime as far they are in the field of control of the criminal or terrorist organization and are dedicated for their purposes[150].

Financial criminal offences that are punishable with a mandatory prison sentence of more than three years are classified as crimes within the meaning of the Penal Code and thus also constitute a predicate offence suitable for money laundering. These include **§§ 38a and 39 FinStrG** (gang perpetration and tax fraud). For example, the tax evasion according to **§ 33 FinStrG** is not directly associated and understood as a predicate offence to an act of money laundering[151].

3.1.2. Predicate offences

To prove the link to the predicate offence lengthy investigations are necessary in which the payment flows are traced backwards. The central question is whether investigations in this suspicious situation should be permissible at all. The Austrian Penal Code defines precisely which criminal activities are to be understood as predicate offences to money laundering. These include:

- **§ 223 StGB**: Forgery of documents
- **§ 229 StGB**: Suppression of documents
- **§ 293 StGB**: Forgery of evidence
- **§ 295 StGB**: Suppression of evidence
- **§ 27 SMG**: Unauthorized handling of narcotic drugs
- **§ 30 SMG**: Illicit handling of psychotropic substances

It is important to mention, that**:**

- **§ 224 StGB**: Use of falsified documents
- **§ 225 StGB**: Falsification of public certification marks
- **§ 230 StGB**: Shifting of boundary signs
- **§ 269 StGB**: Resistance to the authorities
- **§ 278 StGB**: Criminal organization
- **§ 288 StGB**: Wrong statement of evidence
- **§§ 304-309**: Corruption, giving or accepting of undue advantage, bribe and others

are not explicitly defined as predicate offences anymore[152].

Also, it is interesting that for example the human trafficking is not explicitly defined as a predicate offence (**§ 104a StGB**). According to **§ 17 StGB (1)**, "crime" (translated from German: "*Verbrechen*") is *"[an] intentional act threatened with a life sentence or a prison sentence of more than three years*

[150] *Cf.* Ibid., p. 14
[151] According to **§ 33, 1, (5) FinStrG**, tax fraud could be sentenced with an imprisonment **up to two years** (translated from German: "*Neben der Geldstrafe ist nach Maßgabe des § 15 auf Freiheitsstrafe bis zu zwei Jahren zu erkennen.*")
[152] **§ 165 StGB (1993)**, Fassung vom 31.07.2013 and interview
See the interview with Dr. E. Scherschneva-Koller from 04.06.2018, lines 40-55

and all other criminal acts are "offences" (translated from German: "*Vergehen*")[153]. According to **§ 104a (1) StGB**, "*Anyone who takes advantage of another person's personal or economic predicament or helplessness connected with a stay in a foreign country or who recruits, promotes, transfers, accommodates or takes in another person under the age of twenty-one shall be punished by imprisonment from* ***six months to five years*** […]."[154]

Another important aspect that should be mentioned in the context of predicate offences is the term "initial suspicion"[155]. In 2014 from 1673 STRs there were 46 reports submitted to the public prosecutor's office. 45 of the cases ended with convictions. In 2015 and 2016 despite the higher number of STRs the number of convictions rather variates (2015: 31 reports and 58 convictions; 2016: 46 reports and 36 convictions). The reason may be the fact that not every suspicion leads to an investigation: "*A fact alone does not constitute a justification for an investigation. It must be clarified in advance whether there is a suspicion of a judicially punishable offence, only then can a preliminary investigation be initiated.*"[156] In 2014 in **Strafprozessrechtsänderungsgesetz 2014 (StPÄG 2014)** the term "*initial suspicion*" was introduced[157]. According to **§ 1 (3) Strafprozeßordnung (1975) StPO**, an "*initial suspicion exists if it can be assumed on the basis of certain indications that a crime has been committed*"[158]. In the context of the investigations for ML this decision was criticized[159]. The clarification if an initial suspicion exists can be made based only on facts. This means that as a first step it is being verified if there is a criminal offence or not. This falls under the responsibility of the criminal police or the public prosecutor's office.

According to **§ 1 (2) StPO**, in the case when an identified or identifiable individual is suspected of a criminal offence, the proceedings have to be conducted as investigation proceedings against this individual[160].

§ 91 (2) StPO regulates the execution of inquiries by using generally accessible information or internal sources of information with the aim to clarify the facts of the case[161].

---

[153] **§ 17 StGB (1993)**, Fassung vom 25.06.2018: „*(1) Verbrechen sind vorsätzliche Handlungen, die mit lebenslanger oder mit mehr als dreijähriger Freiheitsstrafe bedroht sind.*
(2) Alle anderen strafbaren Handlungen sind Vergehen."

[154] **§104a StGB (1993)**, Fassung vom 25.06.2018: „*(1) Wer eine volljährige Person mit dem Vorsatz, dass sie ausgebeutet werde (Abs. 3), unter Einsatz unlauterer Mittel (Abs. 2) gegen diese Person anwirbt, beherbergt oder sonst aufnimmt, befördert oder einem anderen anbietet oder weitergibt, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.*"

[155] Translated from German: „*Anfangsverdacht*"

[156] Scherschneva-Koller in Journal für Strafrecht (2015): Geldwäscheermittlungen im Spannungsfeld zum „Anfangsverdacht" nach dem Strafprozessrechtsänderung 2014, p. 532, translated from German: „*Alleine ein zur Kenntnis gelangter Sachverhalt bildet noch keine Rechtfertigung für eine Ermittlung. Vorweg muss geklärt werden, ob der Verdacht einer gerichtlich strafbaren Handlung gegeben ist, erst dann kann ein Ermittlungsverfahren eingeleitet werden.*"

[157] Art. 1, (2) **StPÄG 2014**: „*Das Strafverfahren beginnt, sobald Kriminalpolizei oder Staatsanwaltschaft zur Aufklärung eines Anfangsverdachts gegen eine bekannte oder unbekannte verdächtige Person ermitteln oder Zwang gegen eine beschuldigte Person ausüben*"

[158] **§ 1 (3) Strafprozeßordnung (1975) (StPO)**, Fassung vom 25.06.2018, translated from German: "*Ein Anfangsverdacht liegt vor, wenn auf Grund bestimmter Anhaltspunkte angenommen werden kann, dass eine Straftat begangen worden ist.*"

[159] *Cf.* Scherschneva-Koller in Journal für Strafrecht (2015): Geldwäscheermittlungen im Spannungsfeld zum „Anfangsverdacht" nach dem Strafprozessrechtsänderungsgesetz 2014, pp. 532-533

[160] **§ 1 (2) StPO**, Fassung vom 25.06.2018: „*Das Strafverfahren beginnt, sobald Kriminalpolizei oder Staatsanwaltschaft zur Aufklärung eines Anfangsverdachts (Abs. 3) nach den Bestimmungen des 2. Teils dieses Bundesgesetzes ermitteln; es ist solange als Ermittlungsverfahren gegen unbekannte Täter oder die verdächtige Person zu führen, als nicht eine Person auf Grund bestimmter Tatsachen konkret verdächtig ist, eine strafbare Handlung begangen zu haben (§ 48 Abs. 1 Z 2), danach wird es als Ermittlungsverfahren gegen diese Person als Beschuldigten geführt. Das Strafverfahren endet durch Einstellung oder Rücktritt von der Verfolgung durch die Staatsanwaltschaft oder durch gerichtliche Entscheidung.*"

§ 151 (1) StPO states that "*"enquiry" means the request for information and the receipt of a communication from a person*"[162]. The aim is to investigate a crime and to prepare the collection of evidence. This information is voluntary and may not be enforced unless it is required by law (**§ 152 (2) StPO**)[163]. An enquiry according to **§ 91 (2) StPO** may not be made to bypass enquiry for the purposes specified in **§ 151 (1) StPO** and the mere use of generally accessible information or internal sources of information cannot be described as an "investigation".

According to **§ 100 (3a) StPO**, the criminal investigation department must report to the public prosecutor's office, when:

- from department's point of view, there is no initial suspicion,
- or the department has doubts whether there is an initial suspicion[164].

If the initial suspicion cannot be confirmed (and thus no investigation will be executed) the public prosecutor's office must abstain from initiating investigation proceedings. More about the investigation process of A-FIU can be found in section 3.1.7.

As a helpful resource, The National Risk Analysis[165] provides, as an obligation according to **§ 2 FM-GwG**, a detailed description, categorization and assessment of the risks, which may be a sign for money laundering or other financial frauds.

Europol recognized a clear trend in the suspected predicate offences behind the reported STRs[166]. They (Europol) identified the "fraud" (tax fraud, fraud and swindling) as the dominating criminal offence (69% of all STRs). Despite the growing concern regarding "cybercrime" only 6% of the STRs could be identified as such. The reason for this was the fact that most of the cybercrime activities were reported as a "fraud".

3.1.3. Risk assessment at company level

According to **§4 FM-GwG** the obliged entities (credit and financial institutions) must identify, assess and mitigate the potential risks of ML/TF. This assessment must be done based on collected data and information. The assessment itself must consider all risks that are related to customers, countries or even geographical areas, offered products and services, transactions and distribution channels. In addition, the development of existing technologies or the introduction of new technologies for new or existing products is an important aspect that must not be ignored. The National Risk analysis (**§ 3 FM-**

---

[161] **§ 91 (2) StPO**, Fassung vom 25.06.2018: "*Ermittlung ist jede Tätigkeit der Kriminalpolizei, der Staatsanwaltschaft oder des Gerichts, die der Gewinnung, Sicherstellung, Auswertung oder Verarbeitung einer Information zur Aufklärung des Verdachts einer Straftat dient. Sie ist nach der in diesem Gesetz vorgesehenen Form entweder als Erkundigung oder als Beweisaufnahme durchzuführen. Die bloße Nutzung von allgemein zugänglichen oder behördeninternen Informationsquellen sowie die Durchführung von Erkundigungen zur Klärung, ob ein Anfangsverdacht (§ 1 Abs. 3) vorliegt, stellen keine Ermittlung in diesem Sinn dar.*"

[162] **§ 151 (1) StPO**, Fassung vom 25.06.2018, translated from German: "*„Erkundigung" das Verlangen von Auskunft und das Entgegennehmen einer Mitteilung von einer Person*"

[163] **§ 152 (2) StPO**, Fassung vom 25.06.2018: „*Soweit die Kriminalpolizei nicht verdeckt ermittelt, hat sie bei Erkundigungen auf ihre amtliche Stellung hinzuweisen, wenn diese nicht aus den Umständen offensichtlich ist. Die Auskunft erfolgt freiwillig und darf nicht erzwungen werden, soweit sie nicht auf Grund einer gesetzlichen Verpflichtung zu erteilen ist.*"

[164] **§ 100 (3a) StPO**, Fassung vom 25.06.2018: "*Die Kriminalpolizei hat der Staatsanwaltschaft auch zu berichten, wenn aus ihrer Sicht kein Anfangsverdacht vorliegt, oder sie Zweifel hat, ob ein Anfangsverdacht vorliegt, zu dessen Aufklärung sie berechtigt und verpflichtet wäre, Ermittlungen zu führen*"

[165] *See* Bundesministerium für Finanzen in Zusammenarbeit mit den zuständigen Ministerien und Behörden (2015-2016): Nationale Risikoanalyse Österreich

[166] *Cf.* EUROPOL (2017): From Suspicion to Action, p. 23

GwG) and the report of the European Commission on the risks of money laundering and terrorist financing in the Single market[167] must be taken into account during the assessment. All analyses on new products and/or services, procedures and technologies must be done before their introduction. The different steps and evaluation procedures during the internal risk assessment must be documented and recorded properly, kept up-to-date and made available to the FMA if requested.

In short, the risk analysis at company level should address following questions:

- Which are the relevant risk factors in the context of the business strategy?
- Which risks can be derived from the identified risk factors?
- Which steps should be taken to mitigate the identified risks?

In addition, the risk analysis must encompass in the first place general information about the institution itself: key figures and roles, business strategy (core business activities, target market, business environment (national and regulatory)), organizational structures, distribution channels, outsourcing (IT and/or business), technologies used for customer identification, etc. After the introduction the practical part of the analysis can consist of the following four steps[168]:

1. Definition and an abstract analysis of all relevant risk factors

The first step would be the definition and assessment of all relevant risk factors according to the institution's business strategy and specific environment. **§ 4 (1) FM-GwG** lists 6 risk factors that must be considered in any case:

a. **Customers**: The factor "customers" is the leading one. Customers can be two types: natural or legal persons. They can be represented by third-party representative or even by a beneficial owner, they can also be a private banking customer or a politically exposed person (PEP)[169]. The characteristics of the customer activity are also essential: cash/non-cash intensity, transaction volumes and frequency, international transactions, etc. For example, a complex ownership scheme and/or control structures that may anonymize of the true ownership or the source of funds can be associated with a higher risk customer.

b. **Countries or geographical areas**: Every country must be assessed according to different factors: micro- and macro-economic development, legal system transparency, the political and financial stability, corruption level, crime rate, bank secrecy level and (regulatory) AML policies. Based on this assessment the countries are categorized (for example, non-EU members, offshore countries (the presumption is that offshore countries are always associated/assigned with/to a high risks), low development countries, countries with high risk according to **§ 2 (16) FM-GwG**[170], etc.).

---

[167] *See* The European Commission (2017): EU assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities

[168] *Cf.* Finanzmarktaufsichtbehörde (2018): FMA-Rundschreiben Risikoanalyse zur Prävention von Geldwäscherei und Terrorismusfinanzierung, pp. 15-18

[169] **§ 11 FM-GwG**, Fassung vom 25.06.2018, regulates the due diligence obligations in regard of PEP

[170] **§ 2 (16) FM-GwG**, Fassung vom 25.06.2018, translated from German: "*High risk third countries: Third countries which have strategic shortcomings in their national anti-money laundering and terrorist financing systems that pose significant risks*

c. **Products and services**: Every product or service, offered by a financial institution, has a potential risk of exploitation by money launderers or used for the aim of ML/TF. Following factors must be taken into account when assessing the product and service risk. These and other factors could increase the risk of exploitation or misuse:
    i. the degree of anonymity that the product or service offers (for example, anonymous saving books),
    ii. the liquidity that is needed in order to use the product or service (for example, a constant liquidity),
    iii. the complexity of the products (for example, derivatives, structured or leveraged products, etc.)

d. **Transactions**: Transactions are always associated with a documentation. The higher the level of documentation, the easier it would be to trace a particular transaction. For example, transactions in offshore countries or higher proportion of foreign payment transactions in high-risk countries increase the transaction risk due to the possibility of concealment or anonymity. Any cross-border transactions where the involved institutions do not have a proper due diligence policy increases the transaction risk.

e. **Distribution channels**: The risk regarding the distribution channels depends on the intensity of the customer contact in order to fulfil the due diligence obligations. For example, third-party sales channels and/or outsourced sales channels must be appropriately identified and assessed.

f. **Other new or developing technologies**: The risk related to the use of new or developing technologies depends on two factors according to FATF Recommendation 15[171]:
    i. Risks related to the development of new products and business models
    ii. Risks related to the use of new technologies

    Before the introduction of a new product or service or before the use of new or developing technologies, the financial institution must assess the corresponding risk of misuse.

g. **Others**

    Other factors that must not be ignored when doing the risk assessment are: legal and/or supervisory requirements, findings from suspicious cases from the past, key events worldwide (political, economic, social).

2. Risk assessment of the defined risk factors

The risk assessment at this stage should consider the institution-specific key characteristics (business strategy, target market, etc.). For example, from the evaluation of the risk factors it must be clear how many business relationships with offshore countries exist, while another example is how many PEPs

to the Union's financial system, as identified by the European Commission in a delegated regulation under Article 9 of Directive (EU) 2015/849."

[171] FATF (2012), p. 17: "*Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.*"

have relationships with the institution (it does matter if their percentage is 0.01% or 10%, because this has direct impact on the risk assessment). This evaluation would then allow a comprehensive evaluation of the customer risk (the higher the number of business relationships with PEP, the higher the customer risk will be assessed)[172].

3. Derivation of an overall risk at company level

Based on individual and partial assessment it will be possible to derive the overall risk at company level. For example, if the country risk has been assessed as "low", the product and customer risks as "medium" and the transaction risk as "high", it will be easier to classify the overall risk of the company regarding ML/TF[173].

4. Definition of risk-reducing measures

The last step includes a few sub-steps for definition of measures, internal controls and initiatives at company level in order to mitigate the risks. Some of these sub-steps are[174]:

a. Definition of appropriate strategies and procedures to ensure the compliance with the due diligence obligations. This includes the documentation of written instructions, manuals, handbooks, checklists, customer acceptance processes, etc.
b. Establishing a central AML Office as an integrated part of the organization with access to related and sufficient resources, data and information.
c. Quarterly or yearly risk analysis, re-assessment and definition of an appropriate control plan, including control evaluation and execution.
d. Use of appropriate IT systems (for example, an AML software)
e. Documentation about the taken steps and defined measures

3.1.4. Due diligence and risk assessment at customer level

The first step of the customer due diligence process is to verify the identification of the customer. The verification process itself is based on an authenticity check of, for example, signatures on documents, or other documents identifying the customer. The procedure is executed when a new business relationship between the financial institution and the customer is established or particular circumstances occur, for example, a money transfer above a defined threshold. To ensure an effective CDD following customer's characteristics should be considered: natural or legal person, location or country of origin, businesses (in some cases of a business accounts additional verification checks are needed), business relationships, origin of the funds, number of accounts in other financial institutions, results from third-party verification services and person research, etc. After obtaining and documenting all relevant and needed data and information, the bank should be able to monitor the account's activity

[172] *Cf.* Finanzmarktaufsichtbehörde (2018): FMA-Rundschreiben Risikoanalyse zur Prävention von Geldwäscherei und Terrorismusfinanzierung, p. 17
[173] *Cf.* Ibid., p. 18
[174] *Cf.* Ibid., p. 18

and receive alerts in case of unusual and/or unexpected money transactions[175]. In addition, the collected information and knowledge about a customer during the CDD phase helps the institution to understand the customer and the customer's choices and can be used to model the expected customer activity and transactions behavior. All these steps lead to the creation of a risk profile, whose main task is it to support the institution in its decision if a business relationship should be established, continued or terminated. Of course, in order to perform a proper re-assessment of the customers the risk profiles of the customers should be regularly updated.

The attempts for money laundering can come from different geographical locations, countries, through different products and services offered by the financial institution. In such high-risk cases an Enhanced due diligence should be executed – when opening an account and ongoing[176]. The due diligence obligations for the financial institutions in Austria were regulated until 01.01.2017 in **§ 40 Bankwesengesetz (BWG)**[177] and replaced by **§ 5 FM-GwG**[178]. The obliged entities (credit and financial institutions) have to apply a customer due diligence according to **§ 6 FM-GwG**[179] in any of following cases:

1. **When establishing a business relationship**. Following terms are defined as "business relationship":
    - any business, professional or commercial relationship which relates to the commercial activities of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration.
    - savings deposit transactions according to **§ 31 BWG**[180]
    - transactions according to **§ 12 Depotgesetz (DepotG)**[181]
2. **When executing any transactions which are not conducted within the scope of a business relationship** (occasional transactions),
    a) which involve an amount of at least EUR 15 000 or a euro equivalent value, regardless of whether the transaction is carried out in a single operation or in multiple operations between which there is an obvious connection; or
    b) which involves a transfer of funds as defined in **Article 3 (9) of Regulation (EU) 2015/847**[182] exceeding EUR 1 000;

    if the amount in the cases listed in letter a) is not known prior to the start of the transaction, then the due diligence obligations shall be applied as soon as the amount involved is known and it has been determined that the amount is at least EUR 15 000 in value or euro equivalent value;
3. For each deposit into savings deposits, and for each withdrawal of savings deposits if the amount deposited or withdrawn is at least EUR 15 000 or a euro equivalent value;
4. If the institution suspects or has reasonable grounds to suspect that the customer belongs to a terrorist organization (**§ 278b StGB**) or the customer objectively participates in transactions which

[175] Europol (2017): From Suspicion to Action, p. 41: "*a suspicious transaction is a transaction that causes a reporting entity to have a **feeling** of apprehension or **mistrust** about the transaction considering its unusual nature or circumstances, or the person or group of persons involved in the transaction. Reporting entities assess the suspicion according to a risk-based approach for customer due diligence, real-time payment screening, transaction monitoring and behavioral monitoring, to identify changes in the respondent's transaction risk profile.*"

[176] *Cf.* Office of the Comptroller of the Currency (2002): Money Laundering: A Banker' s Guide to Avoiding Problems, p. 10

[177] *See* **§ 40 BWG**, Fassung vom 31.12.2016

[178] *See* **§ 5 FM-GwG**, Fassung vom 25.06.2018

[179] *See* **§ 6 FM-GwG**, Fassung vom 25.06.2018

[180] *See* **§ 31 BWG**, Fassung vom 25.06.2018

[181] *See* Bundesgesetz vom 22. Oktober 1969 über die Verwahrung und Anschaffung von Wertpapieren (Depotgesetz), Fassung vom 25.06.2018

[182] *See* The European Parliament and the Council of the European Union (2015): Regulation (EU) 2015/847

serve the purpose of money laundering (**§ 165 StGB** – including asset components which stem directly from a criminal act on the part of the perpetrator) or terrorist financing (**§ 278d StGB**);
5. When there are doubts as to the veracity or adequacy of previously obtained customer identification data.

It is expected, but currently unknown[183], that if the number of STRs has increased since 01.01.2017, this is caused by the obligations stated in **§ 5 FM-GwG, p. 2, b.)**.

The scope of the due diligence obligations is described in **§ 6 FM-GwG**. It includes, among others:

1. identifying the customer and verifying the customer's identity,
2. identifying the beneficial owner and taking reasonable measures to verify that person's identity and to understand the ownership and control structure of the customer,
3. assessing and obtaining information on the purpose and intended nature of the business relationship,
4. obtaining and checking of information about the source of the funds used,
5. 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,
6. regular checking of the availability of all required information, data and documents that are required under the federal act and updating of this information, data and documents.

For the first three points the financial institutions can ensure an effective due diligence based only on a "*risk-sensitive basis*"[184]. In order to assess the customer risk of ML/TF the proposals, also called risk variables defined in **Annex I**[185] **FM-GwG,** shall be considered, for example:

Risk variable	Description
Regularity or duration of the business relationship	Long-standing business relationships which regularly lead to customer contact may represent a lower risk regarding money laundering. This assumption can be based on the experience from previous business relationships in the past with the customer (for example, no anomalies in transaction behavior).

[183] *Please note*: per October 6, 2019 there is no yearly report for 2018. The yearly reports, published by BK, do not include detailed information about single cases or investigations, so one can make valid conclusions about the effects from legislative changes during the past few years. It will be also a speculation to make a conclusion about the reasons for the increase or the decrease of the number of STRs, without knowing all facts and details about the processed investigations.

[184] The term "*risk-sensitive basis*" has been introduced in the Third EU AML Directive (Directive 2005/60/EC of the European Parliament and the Council of the European Union). It is not clear what exactly lies behind the "*basis*".

[185] *See* Finanzmarktaufsichtbehörde (2018): FMA-Rundschreiben Risikoanalyse zur Prävention von Geldwäscherei und Terrorismusfinanzierung; *Please note*: FMA published in 2018 a comprehensive guideline for the risk variables from **Annexes I**, **II** and **III FM-GwG** regarding the due diligence obligations. According to FMA, the list of risk variables in **Annexes I**, **II** and **III FM-GwG** is not exhaustive. Depending on the business model/business environment/business strategy, size and complexity of the business activities of the particular financial institution, further institution-specific risk factors must be taken into account.

Based on this assessment every customer shall be assigned to a particular risk class. When the calculated risk for ML/TF score is low, the financial institutions may apply simplified customer due diligence obligations for their customers. Otherwise, when the calculated risk is higher, the risk variables listed in **Annex II FM-GwG** should be considered (**Simplified due diligence** according to **§ 8 FM-GwG**). For example:

Risk variable	Description
Risk factors in geographical terms: EU Member States	Customer from EU Member States are most probably a sign of a potentially low risk in regard to money laundering. Nevertheless, any risk-increasing factors must be taken into account for these countries (for example, the political and economic situation is expected to become unstable)

In any case business relationships and transactions must be appropriately monitored in order to detect unusual or suspicious transactions and account activities. FMA has defined areas with lower ML/TF risk, where the scope of the due diligence in particular cases should be simplified per se. Such areas are (among others):

- Sparvereinverordnung (SpVV) [186]
- Schulsparen-Sorgfaltspflichtenverordnung (Schulspar-SoV)[187]
- Lebensversicherung-Sorgfaltspflichtenverordnung (LV-SoV)[188]
- BVK-Risikoanalyse- und Sorgfaltspflichtenverordnung (BVK-RiSoV)[189]

An analysis of the reasons for these regulations and special exceptions is beyond the scope of this thesis.

In addition to the risk variables defined in **Annexes I** and **II FM-GwG** the variables from **Annex III FM-GwG** offer the possibility for better recognition and confirmation of a customer with possible high-risk score as such. The variables listed there correspond to the process of **Enhanced due diligence** according to **§ 9 FM-GwG**. In case of a high-risk customer the variables listed in **Annex I FM-GwG**

[186] *See* Verordnung der Finanzmarktaufsichtsbehörde (FMA) über die Identifizierung von Sparvereinsmitgliedern (Sparvereinverordnung – SpVV), Fassung vom 25.06.2018, translated from German: "*Regulation on Savings Associations*"; it regulates the identification of members of savings associations

[187] *See* Verordnung der Finanzmarktaufsichtsbehörde (FMA) über die Anwendbarkeit vereinfachter Sorgfaltspflichten im Bereich des Schulsparens (Schulsparen-Sorgfaltspflichtenverordnung – Schulspar-SoV), Fassung vom 25.06.2018, translated from German: "*School Savings Schemes Due Diligence Regulation*"; it regulates applicability of simplified due diligence in relation to school savings schemes

[188] *See* Verordnung der Finanzmarktaufsichtsbehörde (FMA) über die Anwendung vereinfachter Sorgfaltspflichten im Bereich der Lebensversicherung (Lebensversicherung-Sorgfaltspflichtenverordnung – LV-SoV), Fassung vom 25.06.2018, translated from German: "*Life Insurance Due Diligence Regulation*"; it regulates the applicability of simplified due diligence in relation to life insurance

[189] *See* Verordnung der Finanzmarktaufsichtsbehörde (FMA) über die Ausnahme von der Verpflichtung zur Aufzeichnung einer Risikoanalyse und der Anwendbarkeit vereinfachter Sorgfaltspflichten im Bereich des Betrieblichen Vorsorgekassengeschäfts (BVK-Risikoanalyse- und Sorgfaltspflichtenverordnung – BVK-RiSoV), Fassung vom 25.06.2018, translated from German "*Corporate Provision Funds Risk Analysis and Due Diligence Regulation*"; it regulates the exemption from the obligation to record a risk analysis and the applicability of simplified due diligence with regard to the operation of corporate provision funds

are becoming insufficient for the risk assessment and further analysis. In addition, an increased activity monitoring is required. For example:

Risk variable	Description
Risk factors relating to customers: extraordinary circumstances of the business relationship	There are indications that the customer is trying to hide the real reason for the establishment of a business relationship.

The financial institutions can also weigh the risk factors in the customer's risk classification. This means that in particular some risk factors may weigh more than others. For example, a specific risk factor regarding the chosen product by the customer may weigh more than the geographical risk factor of the customer. For example, a customer from an EU Member State (lower risk) opens three accounts as representative for another natural person and three accounts as a representative for a juridical person. Opening six accounts at the same is maybe not unusual and needed for the goals of the business (for example establishing a new company), however, such scenario should be handled properly by the internal AML program. Therefore, the risk weighting will vary depending on the product, customer or customer category and the risk scenarios defined by the financial institution. The weighting itself should be done in a balanced way – one risk factor should not excessively influence another risk factor. Also, the weighting should allow risk classifications of customers and/or transactions as "high risk". This means that the financial institution should consider particular use cases where a "high risk" score can be expected. Any re-assessment or re-calculation of the risk score and risk weights should be reasonable and well documented. A good example for such approach is the risk classification proposed by Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)[190].

To ensure that the risk assessment for all customer is properly done an alternative approach can be suggested. Initially on a daily basis all customers (independent from their type) receive the highest possible risk score – thus, the assumption is that everybody (customers and their transactions) is suspicious. In such a case, the internal CDD processes must be modelled in a such way that for each customer the risk score has to be minimized. Theoretically the results from this assessment should be the same when doing the assessment with an initial low risk score. Major differences may occur in the execution and (manually) processing time due to an eventually high increase of "false positives" ("false negatives" respectively). The risk assessment in both cases also depends on the used data and how the data is structured.

3.1.5. Point of time of application of due diligence obligations

§ 7 FM-GwG regulates the point of time when the due diligence obligations should apply. This must be done before the establishment of a business relationship or before executing an occasional transaction. In cases when the customer is being represented by another natural person, the

[190] Federal Financial Supervisory Authority of the Federal Republic of Germany (homepage: https://www.bafin.de/); *Cf.* FATF (2014): Guidance for a risk-based approach: Banking Sector, p. 28

determination and verification of the identity of the representative is then executed when he/she uses his/her power of representation. There are two exceptions regarding this regulation[191]:

There are also special cases for arrangements for life insurance. The identification of the beneficiary happens before establishing the business relationship and the verification of the identity of the beneficiary happens before payment to the customer.

The ongoing due diligence against existing customers can be automatically executed, for example daily, weekly or quarterly. The verification frequency depends on the risk assessment on enterprise level and on the risk assessment on customer level. External or internal relevant events and circumstances could also be a trigger for subsequent due diligence.

In case that the financial institutions cannot fulfil their due diligence obligation due to missing data or information (exception is **§ 6 (1), p. 6 and 7 FM-GwG**[192]) they should not:

- establish a new business relationship with the customer,
- execute transactions from/to/through the corresponding account

In some special cases (**§ 6 (1), p. 6 FM-GwG**) a transaction can be delayed until all relevant data and information is available, all relevant checks are executed, and the legal environment of the transaction is guaranteed. In such cases the financial institution should internally investigate and analyze the transaction and the customer and shall consider generating a STR to the FIU about the customer in accordance with **§ 16 FM-GwG**.

Similar obligations refer to life insurance companies or pension funds.

3.1.6. Reporting obligations

Every suspicious transaction is analyzed first internally by the financial institution itself and only in case that the internal investigation has led to a suspected case of ML or fraud the institution must report the case to the FIU. According to **§ 41 BWG**:

(1) Credit and financial institutions must report to the FIU as far as this is stipulated in **§ 16 (1) and (3) FM-GwG**

(2) Credit and financial institutions shall provide the FIU with information at its request as far as this is stipulated in **§ 16 (2) FM-GwG**[193].

---

[191] **§ 7 FM-GwG (2)**, Fassung vom 25.06.2018: „*die Verpflichteten* [können] *die Überprüfung der Identität des Kunden, des wirtschaftlichen Eigentümers und des Treugebers* ***erst während der Begründung einer Geschäftsbeziehung*** *abschließen, wenn dies notwendig ist, um den normalen Geschäftsablauf nicht zu unterbrechen und ein geringes Risiko der Geldwäscherei oder Terrorismusfinanzierung besteht. In diesem Fall werden die betreffenden Verfahren so bald wie möglich nach dem ersten Kontakt abgeschlossen.*“ and

§ 7 FM-GwG (2), Fassung vom 25.06.2018: „*Die Eröffnung eines Bankkontos* [ist] *bei einem Verpflichteten zulässig, sofern* ***ausreichend sichergestellt ist****, dass Transaktionen von dem Kunden oder für den Kunden erst vorgenommen werden, wenn die Sorgfaltspflichten gemäß § 6 Abs. 1 Z 1 bis 5 vollständig erfüllt sind.*“

[192] **§ 6 FM-GwG (1), p. 6 and 7**, Fassung vom 25.06.2018: „*Die Sorgfaltspflichten gegenüber Kunden umfassen […]*
6. kontinuierliche Überwachung der Geschäftsbeziehung, einschließlich einer Überprüfung der im Verlauf der Geschäftsbeziehung ausgeführten Transaktionen, um sicherzustellen, dass diese mit den Kenntnissen der Verpflichteten über den Kunden, seine Geschäftstätigkeit und sein Risikoprofil, einschließlich erforderlichenfalls der Herkunft der Mittel, übereinstimmen;
7. regelmäßige Überprüfung des Vorhandenseins sämtlicher aufgrund dieses Bundesgesetzes erforderlichen Informationen, Daten und Dokumente sowie Aktualisierung dieser Informationen, Daten und Dokumente.“

This leads to a situation where the financial institutions are unable to send any information about the customer or report a suspicious activity to the FIU without analyzing it first.

§ 16 FM-GwG regulates the reporting obligations to the Austrian Financial Intelligence Unit[194]. If a financial institution suspects or has a legitimate reason to believe that a transaction or business relationship is misused for the purpose of ML/TF this must be reported to the FIU. In case of an upcoming or delayed transaction the FIU may be asked for an opinion whether there are any objections against the execution of the transaction[195]. If the FIU does not send any feedback to the bank within the bank's working day or within the working day after the report was sent, the transaction can be processed. In such a case the FIU has the complete authority over this particular upcoming transaction. It is important to mention that the more detailed the report is, the higher the possibility is for a decision to be made: "*Please note that a decision on the execution or non-execution of a transaction can only be made by the FIU if a complete report is submitted. This means in particular that the FIU must be informed of all information that was relevant to the suspicion (of the justified reason for its assumption). The transmission of mere parts of the report (e.g. only the report form) results in an inhibition of the decision period stipulated in the relevant material laws.*"[196]

Beside this, the FIU is not responsible for any further business decision (for example, termination of the business relationship) made by the account management or AML Office in the institution and is also not obliged to inform the reporting entities about the status of an investigation. Thus, the financial institution does not receive in most of the cases[197] any feedback if a suspicion was reasonable or not, although **§ 16 (4) FM-GwG** states that FIU "*must also ensure that timely feedback is provided on the effectiveness of suspicious activity reports on money laundering or terrorist financing and* ***the measures taken as a result.***"[198]. Theoretically, a financial institution may analyze the same suspicious behavior or pattern hundred times per year and generate STRs to the FIU on a daily basis without knowing that their internal analyses are likely faulty, or their internal customer risk assessment is maybe much too strict. In addition, proactive collaboration between the financial institution and the FIU could increase the quality of reporting.

---

[193] **§ 16 FM-GwG (2)**, Fassung vom 25.06.2018: "*Die Verpflichteten und gegebenenfalls deren Beschäftigte haben mit der Geldwäschemeldestelle in vollem Umfang zusammenzuarbeiten, indem sie der Geldwäschemeldestelle unabhängig von einer Verdachtsmeldung gemäß Abs. 1, auf Verlangen unmittelbar oder mittelbar alle Auskünfte erteilen, die dieser zur Verhinderung oder zur Verfolgung von Geldwäscherei oder von Terrorismusfinanzierung erforderlich scheinen.*"

[194] More information about the Austrian FIU, its area of activity and international cooperation can be found in section 3.1.8

[195] *Cf.* Bundeskriminalamt Österreich (2017): Geldwäsche Jahresbericht, p. 10, translated from German: „*Steht ein konkreter Geschäftsfall oder eine Transaktion bevor, kann von der Geldwäschemeldestelle eine Entscheidung darüber verlangt werden, ob gegen deren unverzügliche Durchführung Bedenken bestehen. äußert sich die Behörde bis zum der Meldung folgenden Werktag nicht, darf die Abwicklung der Transaktion erfolgen*"

[196] *See* Bundeskriminalamt Österreich (2018): Hinweise zur Einbringung sowie der Bearbeitung durch die Geldwäschemeldestelle: "*Wir* (Geldwäschemeldestelle, remark from author***)*** *weisen darauf hin, dass eine Entscheidung über die Durchführung oder Nichtdurchführung einer Transaktion durch die Geldwäschemeldestelle nur bei Übermittlung einer vollständigen Meldung erfolgen kann. Darunter wird insbesondere verstanden, dass der Geldwäschemeldestelle all jene Informationen zur Kenntnis gebracht werden müssen, die zur Entstehung des Verdachtes (des berechtigten Grundes zur Annahme) maßgeblich waren. Eine Übermittlung bloßer Meldungsteile (etwa nur des Meldeformulars) hat eine Hemmung der in den einschlägigen Materiengesetzen festgelegten Entscheidungsfrist zur Folge."*

[197] *See* the interview with Mag. Oliver Floth from 12.06.2018, lines 85-99 and
See Summary from filled questionnaire by "Bank A" (*see* Table 3, "Number of fraud/ML cases confirmed")

[198] **§ 16 FM-GwG (4)**, Fassung vom 25.06.2018: „*Die Geldwäschemeldestelle […] hat dafür zu sorgen, dass eine zeitgerechte Rückmeldung in Bezug auf die Wirksamkeit von Verdachtsmeldungen bei Geldwäscherei oder Terrorismusfinanzierung und* ***die daraufhin getroffenen Maßnahmen erfolgt.***"

Further legal aspects

The due diligence and reporting obligations of designated non-financial businesses and professions (DNFBPs) in Austria are also regulated in the following administrative provisions:

- **§§ 43-52 BiBuG**: The Balance Sheet Accounting Act regulates the conditions for obtaining the authority of balance sheet accountant, accountant and personnel accountant and at the same time contains provisions on the scope of authorization of the individual professions as well as their rights and obligations in business transactions and vis-à-vis the authorities.
  §§ 43-52 BiBuG define the measures to prevent money laundering and terrorist financing. **§ 43 BiBuG** gives definition to various terms, including "money laundering", **§ 44 BiBuG** describe the mandatory use of a risk-based approach, when executing the professions described in this law. **§§ 45-52 BiBuG** describe the (simplified and enhanced) due diligence obligations, the scope of the due diligence and other regulations, that can be also found in the FM-GwG.
- **§§ 365m-z Gewerbeordnung 1994 (GewO 1994)**: Gewerbeordnung (GewO) is the legal basis for the commercial exercise of activities that are carried out independently, regularly and with the intention of achieving a profit or other economic advantage. Since the 2002 amendment to the Industrial Code, there has been a uniform list of regulated trades - that is, all trades (crafts or other regulated trades) that are subject to a certificate of qualification. All trades that do not appear in this list automatically count as free trades.
  The paragraphs **§§ 365m-z GeWo** contain measures to prevent money laundering and terrorist financing. Explicitly affected by these comprehensive measures are, among others, commercial traders, management consultants and insurance intermediaries.
- **§ 31c Glücksspielgesetz (GSpG)**[199]: The right to conduct gambling in Austria is basically reserved to the federal government (gambling monopoly). Numerous conditions must be met in order to obtain a license. The due diligence and reporting obligations of the concessionaire are regulated in **§ 31c GSpG**.
- **§ 13 Körperschaftsteuergesetz 1988 (KStG)**[200]: The Austrian Corporation Tax Act (KStG) regulates the taxation of the income of legal entities by means of corporation tax. **§ 13 KStG** deals with the special provisions for private foundations and especially point 6 defines the regulations regarding money laundering: "*Private foundations must submit copies of their foundation deed and additional foundation deed in the currently valid version to the responsible tax office. If the founder appears through a hidden trust, this must be disclosed to the responsible tax office. If the private foundation does not meet these obligations despite being requested by the tax office, the responsible tax office must immediately*

[199] *See* Bundesgesetz vom 28. November 1989 zur Regelung des Glücksspielwesens (Glücksspielgesetz – GSpG), über die Änderung des Bundeshaushaltsgesetzes und über die Aufhebung des Bundesgesetzes betreffend Lebensversicherungen mit Auslosung, **§ 31c**, Fassung vom 25.06.2018
[200] *See* Bundesgesetz vom 7. Juli 1988 über die Besteuerung des Einkommens von Körperschaften (Körperschaftsteuergesetz 1988 – KStG 1988), **§ 13**, Fassung vom 25.06.2018

inform the Money Laundering Reporting Office (§ 4 Paragraph 2 of the Federal Criminal Police Office Act, Federal Law Gazette I No. 22/2002).”[201] Currently in Austria there are 3137 (per 12th of June 2018) private foundations[202]. The foundations in Austria are obliged to publish the foundation’s founder but not the beneficiary[203]. Thus, in most cases the authorities might not know who exactly benefits from the funds of the foundation. Therefore, a certain private foundation could be misused for the goals of ML/TF. Private foundations are currently not part of the obliged entities as stated in **§ 1 FM-GwG**. However, private foundations in Austria are obliged to fulfil their customer due diligence obligations in accordance with **§ 3 (1) Wirtschaftliche Eigentümer Registergesetz (WiEReG)**[204].

- **§§ 36a-37a Notariatsordnung (NO)**[205]: The notarial regulations regulate the notarization of facts and declarations. **§§ 36a-37a NO** are part of the general provisions on the administration of notaries and define the duties and reporting obligations of the notaries in regard of suspicious activities, that may be used for money laundering like for example the purchase or selling of a real estate or a company.
- **§§ 8a-9a Rechtsanwaltsordnung (RAO)**[206]: Like the notarial regulation **§§ 8a-9a RAO** of the Austrian Lawyers' Code deals with the suspicious cases of money laundering and define the duties of the lawyer regarding this.
- **§§ 87-99 WTBG**[207]: The Austrian Public Accounting Professions Act (WTBG) regulates the professional powers of chartered accountants (auditors, tax consultants). Paragraphs **§§ 87-99 WTBG** describe in a similar way like **§§ 43-52 BiBuG** the measures to prevent money laundering and terrorist financing.
- **§ 17c Zollrechts-Durchführungsgesetz (Zollrechts-DG)**[208]: The Austrian Customs Law Implementation Act regulates the trade of goods with other countries. **§17c Zollrechts-DG** defines the obligations of the Austrian Customs Services regarding suspicious activities of money laundering, especially in cases of (undeclared) cash.
- **§ 14 (3) E-Geldgesetz**[209]: The 2010 Electronic Money Act regulates who may issue electronic money and under what conditions
- **§ 20 (3) Zahlungsdienstegesetz 2018 (ZaDiG 2018)**[210]:

The following regulation is not valid anymore or was replaced by paragraphs in the FM-GwG:

---

[201] Translated from German: *“Privatstiftungen haben dem zuständigen Finanzamt Abschriften ihrer Stiftungsurkunde und Stiftungszusatzurkunde in der jeweils geltenden Fassung vorzulegen. Tritt der Stifter über eine verdeckte Treuhandschaft auf, ist diese gegenüber dem zuständigen Finanzamt offenzulegen. Kommt die Privatstiftung diesen Verpflichtungen trotz Aufforderung durch das Finanzamt nicht nach, hat das zuständige Finanzamt hievon unverzüglich die Geldwäschemeldestelle (§ 4 Abs. 2 des Bundeskriminalamt-Gesetzes, BGBl. I Nr. 22/2002) zu informieren.”*

[202] *Cf.* Verband österreichischer Privatstiftungen (2018): Facts & Figures - österreichische Privatstiftungen

[203] *See* Privatstiftungsgesetz (PSG), **§ 9 (1), p. 3.**, Fassung vom 05.08.2018

[204] *See* Wirtschaftliche Eigentümer Registergesetz (WiEReG), **§ 3 (1)**, Fassung vom 05.08.2018

[205] *See* Notariatsordnung (NO), **§§ 36a-37a**, Fassung vom 25.06.2018

[206] *See* Rechtsanwaltsordnung (RAO), **§§ 8a-9a**, Fassung vom 25.06.2018

[207] *See* WTBG (2017), **§§ 87-99**, Fassung vom 25.06.2018

[208] *See* Bundesgesetz betreffend ergänzende Regelungen zur Durchführung des Zollrechts der Europäischen Gemeinschaften (Zollrechts-Durchführungsgesetz - ZollR-DG), **§ 17c**, Fassung vom 25.06.2018

[209] *See* Bundesgesetz über die Ausgabe von E-Geld und die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten (E-Geldgesetz 2010), **§ 14**, Fassung vom 25.06.2018

[210] *See* Bundesgesetz über die Erbringung von Zahlungsdiensten 2018 (Zahlungsdienstegesetz 2018 – ZaDiG 2018), **§ 20 (3)**, Fassung vom 06.10.2019

- **§ 25 Börsegesetz 1989 (BörseG)**[211]: The Austrian Stock Exchange Act 2018 (BGBl. No. 107/2017) as amended regulates the Austrian stock exchange system.

3.1.7. The role of the authorities

One can distinguish between money laundering, terrorism and organized crime. This separation and the investigative activities of the financial institutions and relevant authorities may lead, as expected, to different investigative situations. One of the main objectives for the financial institutions is to prevent the misuse of the Austrian financial system for the goals of ML/TF. Therefore, for the banks it is essential to know the customers and to be able to trace the cash flows. If criminal activities are suspected, it is necessary to submit reports of suspected money laundering activities. The task of the investigating authorities is focused on the criminal aspect. In case of a conflict between different authorities, different authorities assume different roles and functions.

Various authorities and institutions are involved in the fight against money laundering and terrorist financing in Austria. After defining the role of the financial institutions in the previous sections this one will focus on the roles which the FIU and the Supervisory Authorities like FMA have.

The role of the Financial Intelligence Unit

In Europe one can distinguish between four types of Financial Intelligence Units. They differ in their structures and working processes[212]:

- **Administrative type**: FIUs from this type are an integrated part of a governmental structure (often this is the Ministry of Finance). They are separated from the law enforcement or even from the judicial authorities[213]. FIUs from this type are used as a buffer between the reporting entities (incl. financial institutions) and the prosecution and have the goal to validate the suspicion before the case is being forwarded to authorities responsible for further criminal investigations. Currently, 12 FIUs Europe-wide can be classified as "administrative"[214].
- **Judicial**: In this case the FIU is part of the judiciary (mostly under the prosecutor's jurisdiction). FIUs from this type are typical for countries with strict bank secrecy laws. This allows the execution of relevant measures, like account freezing, to be executed quickly. In Europe only one FIU is from type "Judicial" – the FIU in Luxembourg.
- **Law enforcement**: FIUs from type "law enforcement" are part of the corresponding law enforcement agency. This organizational structure leads to fewer access restrictions to law enforcement operative data and information and therefore – to beneficial operational cooperation on national and international levels. The A-FIU is from type "law enforcement"[215].

---

[211] *Cf.* Bundesgesetzblatt für die Republik Österreich, Teil I vom 26.07.2017, **§ 182**: „*Das Börsegesetz 1989 – BörseG 1989, BGBl. Nr. 555/1989, tritt mit Ablauf des 2. Jänner 2018 außer Kraft.*"

[212] *Cf.* EUROPOL (2017): From Suspicion to Action, p. 28

[213] Business Dictionary (2018): "*judicial power*" is "*the constitutional authority vested in courts and judges to hear and decide justiciable cases, and to interpret, and enforce or void, statutes when disputes arise over their scope or constitutionality.*"; translated from German: *Justizbehörden*

[214] Such are the FIUs in Belgium, Bulgaria, Croatia, Czech Republic, France, Italy, Latvia, Malta, Poland, Romania, Slovenia, Spain

[215] Beside the A-FIU, in following countries, the FIU is from type "law enforcement": Estonia, Finland, Germany, Great Britain, Lithuania, Republic of Ireland, Portugal, Sweden and Slovakia

- **Hybrid**: As its name says the FIUs from type "Hybrid" may have characteristics from the other FIU types. For example, a FIU can be legally defined as an administrative body but its employees may have law enforcement and/or investigative responsibilities and powers[216].

Because of this classification each FIU has its own character, working practices and models, which is very important for the effectiveness of STR reporting and further case analysis. Therefore, it is not possible to make a direct comparison regarding the processing of the STRs which one is better or worse. Even the understanding what a "STR" is may be a burden for future evaluations. Some of the FIUs are receiving STRs, while some of them UTRs[217]. Other FIUs must deal with SARs (in such cases the behavior of the customer like the account activity as a whole or inconsistency between the customer and his/her businesses may be the trigger; a single suspicious transaction is not necessary, therefore the scope of the SARs is broader), while others with a mixture of STRs, UTRs and SARs. This differentiation is a major problem and a challenge for an eventual statistical analysis of the reports. For example, a particular FIU records the UTRs separated from the STRs, another one stores all reports regarding a couple of transactions to the same target account as one single report. According to FATF's Recommendation 20, "*if a financial institution **suspects** or **has reasonable grounds to suspect** that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report **suspicions** promptly to the financial intelligence unit (FIU)".*

In the context of recently disclosed ML cases and investigations the role of the STRs is becoming much more important than its exact denomination:

- In November 2014 the former Prime Minister of Portugal Jose Socrates was arrested. The reason was an investigation about tax fraud, corruption and money laundering conducted by Autoridade Tributária e Aduaneira[218]. The amount of money involved in this case was calculated to be approximately 20 million EUR. The investigation was started because of a set of suspicious reports issued by the financial institutions and the triggering event was an indirect deposit of 600 000 EUR into the bank account of the former PM[219].
- In 2015 an international investigation against Chinese organized crime culminated in an operation (known as "Operation Snake") by the Spanish Guardia Civil[220]. The estimated amount of laundered money is 300 million EUR for the period of two years. Also, in this case the role of the STRs was essential: the financial institutions reported that for at least 3 months around 25 persons with Chinese nationality and 17 companies made numerous cash deposits

[216] In Cyprus, Greece, Denmark, Hungary and in the Netherlands the FIU is from "hybrid" type
[217] *Cf.* Bundesministerium für Finanzen (2016): Veröffentlichung von Statistiken gemäß Artikel 44 Abs. 3 der 4. Geldwäsche-Richtlinie: In Austria, STRs, UTRs and SARs are defined as follows:
- **STR** is a disclosure made to an FIU by a party having an obligation to disclose based on **any type of suspicion of ML/TF** which are required by regulations which may include **unusual behaviour**.
- **SAR** is a disclosure made to an FIU by a professional having an obligation to disclose based **on any suspicious activity of ML/TF**.
- **UTR** is a disclosure made to an FIU by a professional with an obligation to disclose, based **on unusual behaviour** in a client's profile.
- The main distinction between an **STR** and **UTR** is the higher standards and quality expected of STRs.

[218] Tax and Customs Authority of Portuguese Republic (homepage: https://www.portaldasfinancas.gov.pt/)
[219] *See* Reuters (2014): Portuguese ex-PM Socrates arrested in corruption probe
[220] Guardia Civil is the law enforcement agency in Spain

followed by money transfers to China[221]. In 2016 "Snake" was followed by "Shadow". "Operation Shadow" was an operation targeting the governing structures of Commercial Bank of China (ICBC) in Spain "*due to suspicions of large scale money laundering services offered to clients*"[222] for the period of 3 years during which ICBC didn't fill out at least one STR or fulfill its due diligence duties[223].

As shown above, the important role of the STRs is without doubt. The increasing use of cash by the criminals or their re-orientation to more unregulated financial systems is a sign of success of the STR policy in Europe. However, the STRs alone are not the only factor for a successful AML investigation. Europol points out the major role of the financial intelligence during every financial investigation and the role of the STRs as part of this intelligence: „*Financial intelligence is a core component of financial investigations, providing indications not only on origin, transfers, destination, beneficiaries, storage and usage of funds, but also to reconstruct geographical movements of criminals, to discover the current location of persons of interest, and to retrieve all types of data around suspects (contained in customer due diligence). More importantly, it allows for the identification of participants in a criminal network – the highest levels included - and provides the basis for seizure/confiscation opportunities. Financial intelligence is a precious resource not only in money laundering cases, but can also be fruitfully used for tackling a number of offences such as terrorist financing or tax offences, and accordingly, many countries now provide access to STR data to revenue authorities and terrorist financing units. STRs are also a key source of financial intelligence, providing early warnings on emerging threats that can be used as tactical intelligence for investigations or for strategic purposes in order to inform and support policy decisions.*"[224]

In Austria, the FIU (A-FIU) is part of the Federal Criminal Police Office (Bundeskriminalamt[225]) of the Federal Ministry of the Interior (Bundesministerium für Inneres). This is legally defined and based on **§ 4 Bundeskriminalamtgesetz (BKA-G)**[226]. The main tasks and responsibilities of the FIU are:

- conducting independent money laundering investigations based on reports of suspected money laundering,
- coordinating national and international money laundering investigations,
- aiding other departments and organizational units

[221] *See* Europol (2015): Large Chinese Money Laundering Network Dismantled
[222] Europol (2017): From Suspicion to Action, p. 32
[223] *See* Europol (2016): Directors of Chinese bank arrested in Spain in money laundering probe
[224] Europol (2017): From Suspicion to Action, p. 32
[225] Bundeskriminalamt Österreich is the federal police force in the Republic of Austria. Its role is to fight against crime nationwide and serve as a centre for cooperation with international police functions. It has been established in 2002. It is a subordinate to the "Generaldirektion für die öffentliche Sicherheit" in the Federal ministry of the Interior.
.BK supports as the central office in Austria all state criminal police offices and subordinate police departments through assistance services, support services and controlling.
[226] *See* Bundesgesetz über die Einrichtung und Organisation des Bundeskriminalamtes (Bundeskriminalamt-Gesetz – BKA-G), **§ 4**, Fassung vom 25.06.2018

- coordinating relevant information on suspicious transactions between financial institutions and other authorities (receiving, analyzing, forwarding)
- organization of awareness-raising events for professional groups subject to reporting requirements
- international correspondence and cooperation (single-point-of-contact ("SPOC") in Austria,)
- on specific occasions: Investigations into the financing of terrorism are carried out jointly with the "Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT)"[227]

The analysis procedure of the FIU is initialized after a report regarding unusual or suspicious account activity or transaction is received. The received information is ***checked*** regarding its relevance under the criminal law. The reason for this is that it is assumed that the reporting is based on "*suspicion*" or "*justifiable reason for accepting*"[228] and this has nothing to do in the first place with any findings from criminal investigations.

The second step of the analysis is the ***enrichment*** of the report with additional data: findings from criminal investigation, the customer data and information are verified, an economic plausibility check is processed. Thus, the FIU is authorized to collect, process and exchange with other international partners any relevant data regarding natural and legal persons or entities, including personal data about the customer. If the suspicion can be confirmed during the analysis an investigation according **§ 20a (8) StPO**[229] is started. In case that the FIU does not process the further analysis the STR can be forwarded to another responsible department. For example, in case of suspected terrorist financing the case is forwarded directly to BVT and in case of suspected predicate offence according to FinStrG the report is forwarded to the "Bundesministerium für Finanzen" (BMF)[230].

The exchange of data between the A-FIU and international FIUs is legally regulated for example in **§ 8 Polizeikooperationsgesetz (PolKG)**[231] or **§ 6 EU–Polizeikooperationsgesetz (EU-PolKG)**[232]:

§ 6 (1) EU-PolKG[233]

> *Security authorities shall be authorized to use data transmitted by or through Europol for the purposes of preventing and combating organized crime, terrorism and other forms of serious crime and related offences.*

---

[227] Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) (homepage: http://www.bmi.gv.at/205/)

[228] Translated from German: "*berechtigter Grund zur Annahme*"

[229] **§ 20 StPO (1975),** Fassung vom 25.06.2018: „*Der Zentrale Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption (WKStA) obliegt für das gesamte Bundesgebiet die Leitung des Ermittlungsverfahrens […] sowie die Einbringung der Anklage und deren Vertretung im Hauptverfahren und im Verfahren vor dem Oberlandesgericht wegen folgender Vergehen oder Verbrechen: […] Geldwäscherei (**§ 165 StGB**), soweit die Vermögensbestandteile aus einer in den vorstehenden Ziffern genannten Straftat herrühren.*"

[230] Bundesministerium für Finanzen (BMF) (homepage: https://www.bmf.gv.at/)

[231] *See* Bundesgesetz über die internationale polizeiliche Kooperation (Polizeikooperationsgesetz – PolKG), **§ 8**, Fassung vom 25.06.2018

[232] *See* Bundesgesetz über die polizeiliche Kooperation mit den Mitgliedstaaten der Europäischen Union und der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol), (EU – Polizeikooperationsgesetz, EU-PolKG), Fassung vom 25.06.2018

[233] **§ 6 (1) EU-PolKG**: "*Die Sicherheitsbehörden sind ermächtigt, Daten, die von Europol oder im Wege von Europol übermittelt wurden, für Zwecke der Vorbeugung und Bekämpfung von Straftaten im Bereich organisierter Kriminalität, Terrorismus sowie anderen Formen schwerer Kriminalität sowie damit im Zusammenhang stehender Straftaten zu verwenden.*"

In addition, A-FIU has direct access to the "Egmont Channel" (Egmont Secure Web (ESW))[234] for exchange of information. Since 2012 A-FIU is a member of the international association of the FIUs Europe-wide called FIU.NET[235].

One of challenges for the financial institutions is to distinguish between "unusual" and "suspicious" cases in the context of the customer's behavior. For the A-FIU it is relevant and important that when a particular bank generates STRs it has a reasonable reason to classify a transaction as suspicious. There are different cases in the course of the daily business when a suspicious activity or transaction can be easily explained and classified as part of a legal transactions, although it looks unusual at first sight. Few examples[236]:

- The owner of a small IT company is afraid of a personal pressure to sell the company to a larger competitor. Thus, the owner decides to hide his/her true identity by establishing a complex ownership structure.
- The political and economic situation in a particular country becomes unstable. Due to the increasing inflation this leads to a massive cash flow out of the country with the aim not to lose the real value of the assets.

To deal with such cases more quickly the financial institutions have to carefully study their customers and when possible – to predict what could happen in the future. That is why it is important that the internal analysis is done appropriately and in case of a STR - to communicate all relevant information about the customer regardless of the reason for the STR.

Another challenge for the law enforcement authorities (including A-FIU) is to distinguish between the above mentioned "*initial suspicion*" and "*justified suspicion*"[237] in order to proceed with an investigation. A *justified suspicion* for a certain transaction that could be linked to money laundering depends on the existence of an evidence to conclude the high probability of money laundering. This is mostly the case when a certain transaction can be hardly explained or it is not understandable.
The *justifiable reason for accepting* must also be based on enough and objective facts for *suspicion*.
The assessment of *suspicion* made by the reporting entity is based on enough trainings and experience but in most cases not on criminal law studies. Therefore, when the STR is received, it can be assumed that an "*initial suspicion*" has been already identified, based on an internal analysis by the reporting entity. In practice, the reasons for an STR relate more to circumstances surrounding the transaction rather than to facts and relations to a certain criminal (predicate) offence. The STRs are based on the risk-assessment made by the reporting entity, by classifying risk-relevant types of money laundering (for example, offshore companies). That is why it is unclear, "*when is the suspicion of a crime to be assumed to be sufficiently substantiated to justify further investigations by the criminal*

[234] More information about Egmont Group can be found in section 3.2.4
[235] Financial Intelligence Units – FIU.NET (homepage: https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net/)
[236] Examples are based on the article from Die Presse (2016): Was Banken (nicht) gegen Geldwäsche tun
[237] *Cf.* Scherschneva-Koller in Journal für Strafrecht (2015): Geldwäscheermittlungen im Spannungsfeld zum "Anfangsverdacht" nach dem Strafprozessrechtsänderungsgesetz 2014, pp. 534-535

police or the public prosecutor's office?"[238] The majority of STRs require immediate reporting to public prosecutor's office (according to **§ 100 (2) 1 StPO**, this is the case of a suspicion in respect of a serious crime or another crime of public interest). However, many investigations for suspicion of ML have been closed immediately after they have been reported. The reason is that there is no offence in the context of money laundering due to the lack of (investigated) predicate offence.

Therefore, the question that arises is: to what exactly the *initial suspicion* for money laundering is associated with: does the connection to a predicate offence need to be already established at the beginning of an investigation or "*should not the very aim of the investigation procedure be to prove this connection and whether the existence of concealment mechanisms already points to a possible money laundering*"[239]?

The role of the Financial Market Authority (FMA)

Finanzmarktaufsichtsbehörde (FMA)[240] was established in 2002 as a supervision authority responsible for the supervision of credit and financial institutions, insurance companies, pension funds and other service providers. In the context of ML/TF the main task of the FMA is to check the compliance of the above entities with the legal obligation including the due diligence duties. In case when this and other related obligations are not fulfilled the FMA can take appropriate measures and necessary steps, including on-site inspections and evaluation of the existing (ML/TF) control and preventive mechanisms. The goal is to ensure the "*restoration of legal compliance or to address the shortcomings*"[241].

In addition, **§ 18 FM-GwG** regulates the reporting obligations in case, when the FMA suspects that a particular transaction is misused for ML/TF:

§ 18 FM-GwG[242]:

> *If the FMA or the Oesterreichische Nationalbank, when exercising its supervisory activities, suspects that a transaction serves money laundering or terrorist financing, they must immediately inform the Money Laundering Reporting Office. This also applies mutatis mutandis to the federal tax authorities in the performance of their duties.*

[238] Ibid., p. 534, translated from German: „*Ab wann ist ein Tatverdacht als ausreichend konkretisiert anzunehmen, um auch weitere Ermittlungen durch Kriminalpolizei oder Staatsanwaltschaft zu rechtfertigen?*"

[239] Ibid., pp. 534—535, translated from German: „*In diesem Zusammenhang stellt sich die Frage, woran der „Anfangsverdacht" bei der Geldwäscherei zu knüpfen ist. Also ob die Verbindung zur Vortat tatsächlich bereits zu Ermittlungsbeginn feststehen muss, oder ob es nicht gerade Ziel des Ermittlungsverfahrens sein sollte, diese Verbindung nachzuweisen und bereits das Vorhandensein von Verschleierungsmechanismen auf eine mögliche Geldwäscherei hindeutet. Um diese Frage beantworten zu können, ist ein näherer Blick auf das Wesen der Geldwäscherei und die Methoden der Geldwäscher erforderlich.*"

[240] Finanzmarktaufsichtsbehörde (FMA) (homepage: https://www.fma.gv.at/)

[241] Finanzmarktaufsichtsbehörde (FMA) (2018): The role of the various authorities and institutions in Austria / The Role of the Financial Market Authority (FMA)

[242] **§ 18 FM-GwG**, Fassung vom 25.06.2018, translated from German: „*Ergibt sich der FMA oder der Oesterreichischen Nationalbank bei Ausübung ihrer Aufsichtstätigkeit der Verdacht, dass eine Transaktion der Geldwäscherei oder der Terrorismusfinanzierung dient, so haben sie die Geldwäschemeldestelle hiervon unverzüglich in Kenntnis zu setzen. Dies gilt sinngemäß auch für die Abgabenbehörden des Bundes bei Wahrnehmung ihrer Aufgaben.*"

The role of the Federal Ministry for Constitution, Reforms, Deregulation and Justice (BMVRDJ)

BMVRDJ[243] is responsible for the further development of criminal law in the field of ML/TF and for the regulation concerning lawyers and notaries. Criminal prosecution is a responsibility of the courts and public prosecutors.

The role of the Federal Ministry of Finance (BMF)

The role of BMF is to adapt the relevant laws for the financial sector (BWG, VAG 2016, WAG 2007, etc.), in order to align them according to the latest international standards in field of ML/TF. BMF heads also the Austrian delegation to the Financial Action Task Force (FATF)[244].

The role of the Austrian National Bank (OeNB)

The Oesterreichische Nationalbank[245] is responsible for enforcing restrictions on international payment transactions according to **Devisengesetz 2004** and **Sanktionengesetz 2010 (SanktG)**[246]. Like FMA, OeNB is obliged to report any suspicious transactions while executing its supervisory activities.

The role of various Ministries and Chambers

The Federal Ministry of Science, Research and Economics (BMWFW)[247], the Federal Ministry for Europe, Integration and Foreign Affairs (BMEIA)[248], the chambers of attorneys, notaries and Professional Accountants and Tax Advisors have their roles in the fight against money laundering and terrorist financing in Austria.

The following figure represents an abstract picture of some communication and collaboration channels, supervision activities between the obliged entities (financial institutions, insurance companies, etc.), the supervisory authorities (FMA, OeNB and all responsible chambers) and law enforcement authorities in Austria, including the partnership collaboration between A-FIU and EUROPOL. For example, the FMA supervises the financial institutions. The financial institutions and pension funds are reporting any suspicious activity in accordance with their legal obligations. A-FIU can forward the case to the public prosecutor's office or contact EUROPOL in order to receive more information regarding a certain case or investigation.

[243] Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz (BMVRDJ) (homepage: https://www.justiz.gv.at/)
[244] *See* Kurier (2016): Aktion scharf gegen Geldwäsche in Österreich
[245] The Oesterreichische Nationalbank is the central bank of Austria) (homepage: https://www.oenb.at/)
[246] *See* Devisengesetz 2004, Fassung vom 25.06.2018 and
Bundesgesetz über die Durchführung internationaler Sanktionsmaßnahmen (Sanktionengesetz 2010 – SanktG), Fassung vom 25.06.2018
[247] Bundesministerium für Bildung, Wissenschaft, Forschung (BMWFW) (homepage: https://bmbwf.gv.at/)
[248] Bundesministerium für Europa, Integration und Äußeres (BMEIA) (homepage: https://www.bmeia.gv.at/)

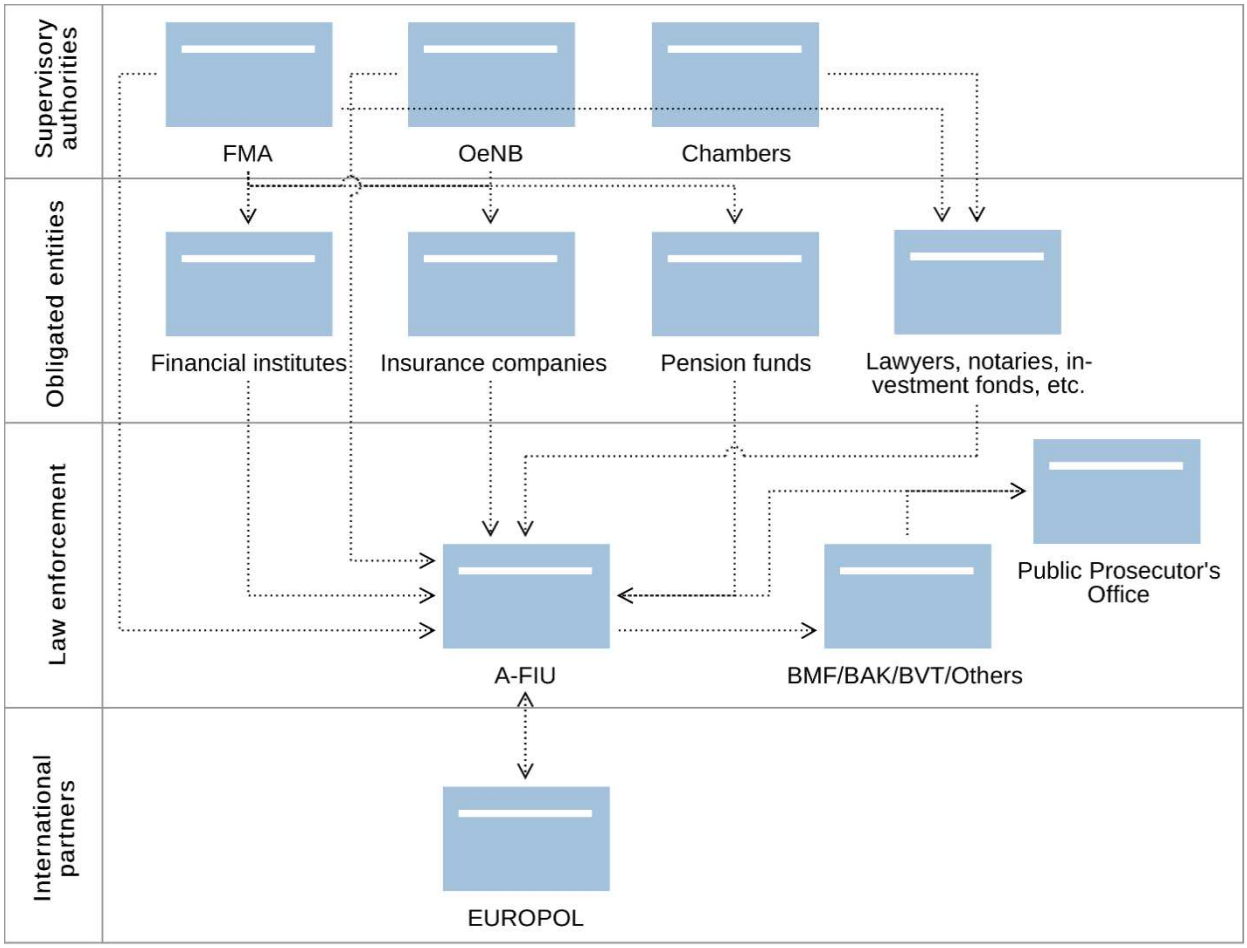

Figure 3 Communication and collaboration flows

3.2. International collaboration

In 1999 the G8 stated that money laundering was one of the "*dark sides of globalisation*"[249]. Different studies have proven the association between the country-specific AML jurisdiction and the globalization of the financial markets: "*Money laundering is the first serious crime whose existence can be directly related to global economic concerns, rather than those of individual jurisdictions. That, more than any other reason, is why its emergence has coincided with globalization.*"[250]

The lack of international cooperation and communication in the field of criminal prosecution may be exploited by the criminals for successful layering. There are very few money-laundering cases where all three phases have taken place in only one country[251].

Therefore, a successful combat against the money laundering can only be based on internationally agreed standards that are implemented by all countries. If this cannot be done the AML strategies and therefore the fight against ML will be like "*squeezing a balloon - you simply displace the activity to*

[249] Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime (1999): Communique, p. 1
[250] Alldridge (2013): Forfeiture, Confiscation, Civil Recovery, Criminal Laundering and Taxation of the Proceeds of Crime, p. 31
[251] *Cf.* Fiedler/Krumma/Zanconato/McCarthy/Reh (2017): Das Geldwäscherisiko verschiedener Glücksspielarten, pp. 30-31

wherever there is the least resistance"[252]. The Forty Recommendations by the FATF[253] are mostly based on the factor of information sharing. In the last few years the result of many international operations and projects against ML show that through joint efforts the combat can be successful[254]. The advantage and importance of the sharing of information stand in opposition to the privacy laws. FATF's Recommendation 9 states, that "*Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.*"[255] Therefore, it can be expected that in the next few years a major development in this direction will be made.

In this section I will provide an overview over the worldwide initiatives in the last decade in the combat of money laundering.

3.2.1. The United Nations

The United Nations (UN)[256] is an international organization, founded in October 1954. With its 193 member states[257] it has the broadest membership and therefore it is the largest international organization.

GPML

The UN operates the Global Programme Against Money Laundering (GPML), which is part of the United Nations Office on Drugs and Crime (UNODC)[258]. The Programme was developed and established as a research project in 1997 in a response to the mandate provided by the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 (*The Vienna Convention*)[259]. The main tasks of GPML is to "*to strengthen the ability of Member States to implement measures against money-laundering and the financing of terrorism and to assist them in detecting, seizing and confiscating illicit proceeds, as required pursuant to United Nations instruments and other globally accepted standards, by providing relevant and appropriate technical assistance upon request*"[260].

The Vienna Convention came into force on November 11, 1990 and is limited to drug trafficking offences as predicate offences and defines the concept of money laundering without mentioning the term itself or addressing the preventive aspects of it and calls upon countries to criminalize this activity[261]. In 2000, the UN adopted The International Convention Against Transnational Organized

---

[252] Shelton (2003): Commitment and Compliance, p. 247
[253] More about the FATF can be read in section 3.2.3.
[254] *Cf.* Maxwell/Artingstall (2017): The Role of Financial Information-Sharing Partnerships in the Disruption of Crime, pp. 13-18: some examples for such initiatives are "Project Protect" in Canada, "The Fintel Alliance" in Australia and "Joint Money Laundering Intelligence Task Force" in the United Kingdom
[255] FATF (2012): The FATF Recommendations, p. 12
[256] The United Nations (homepage: https://www.un.org/)
[257] In addition, there are two non-member observer states of the United Nations General Assembly: The Holy See (which holds sovereignty over Vatican City, in Italian: *Santa Sede*) and the State of Palestine
[258] The United Nations Office on Drugs and Crime (homepage: https://www.unodc.org/)
[259] *See* United Nations Convention (1988): United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances
[260] United Nations Office on Drugs and Crime (2011): UNODC on money-laundering and countering the financing of terrorism
[261] *Cf.* United Nations Convention (1988): United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Article 3 (b) and (c) (i)

Crime (*Palermo Convention*)[262] as a result of the expansion of the combat against international organized crime. The Convention came into force on September 29, 2003 and contains a comprehensive range of provisions to fight organized crime. These provisions adopt the same approach previously adopted by the FATF in its Forty Recommendations on Money Laundering[263]. In addition, the Convention obliges every ratifying country to:

- "*Criminalize money laundering and include all serious crimes as predicate offenses of money laundering, whether committed in or outside of the country, and permit the required criminal knowledge or intent to be inferred from objective facts;*
- *Establish regulatory regimes to deter and detect all forms of money laundering, including customer identification, record-keeping and reporting of suspicious transactions;*
- *Authorize the cooperation and exchange of information among administrative, regulatory, law enforcement and other authorities, both domestically and internationally, and consider the establishment of a financial intelligence unit to collect, analyse and disseminate information*"[264]

IMoLIN / AMLID

The International Money-Laundering Information Network (IMoLIN)[265] is an international network established in 1998 by the UN in partnership with various international organizations involved in the AML/CTF. The network is administrated and maintained by The Law Enforcement, Organized Crime and Anti-Money-Laundering Unit (LEOCMLU) of the UNODC. The network includes a comprehensive secured database, called AMLID, which among other features offers a collection of legislations and regulations from all over the world.

3.2.2. The European Union

"*The European Union Anti-Money Laundering and Financing of Terrorism Directives*[266] *are designed to protect the financial system and other vulnerable professions, such as lawyers, from being misused for money laundering and financing of terrorism purposes."*[267]

EU Directives

First AML Directive

The aim of the First AML Directive[268] was to answer the growing concerns that the financial systems could and would be used for money laundering activities. The Directive provided a framework for the

[262] *See* United Nations Convention (2000): United Nations Convention against Transnational Organized Crime
[263] More information about the FATF's Recommendations can be found in section 3.2.4.
[264] Schott, (2006): Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, III-3-4
[265] The International Money Laundering Information Network (IMoLIN) (homepage: https://www.imolin.org/)
[266] A "*directive*" is a legislative act that sets out a goal that all EU countries must achieve. Therefore, it cannot be applied directly and it is up to the individual countries to devise their own laws on how to reach these goals. A "*regulation*" is a binding legislative act. It must be applied in its entirety across the EU.
[267] Anti-Money Laundering Forum (2009): History of the European Union Anti-Money Laundering and Financing of Terrorism Directives

subsequent Directives regarding ML. The Directive introduced important measures on customer identification and methods for reporting of a suspicious transactions. To protect the EU Single Market, the universal approach in the combat against ML developed in the Directive was adopted by all Member States. Some of the main requirements of the Directive stated that:

- All credit and financial institutions must fulfil their due diligence duties before establishing any business relationship or before conducting any transaction over a certain amount,
- All credit and financial institutions must keep all collected information as part of the due diligence check for at least five years,
- The reveal of a suspicious money laundering activities should dominate the confidentiality rules regarding the collected customer information.

Second AML Directive

The Second AML Directive[269] updated and amended the First AML Directive by refining the arrangements stated there. In addition, the 40 Recommendation by the FATF were used to fill the gaps in the legislation. The European Council thought at that time that the First AML Directive was not able to propose an adequate definition which authorities should receive information about suspicious transactions since the financial institutions had branches in various countries and therefore various jurisdictions. The main aspects of the Second AML Directive were:

- Broader definition of the term “money laundering”,
- Extension of the scope of the Directive to companies like currency exchange offices or investment companies,
- Extension of the powers of the authorities to identify, trace, freeze, seize and confiscate any property and proceeds associated to criminal activities.

One major aspect of the Second AML Directive is that certain occupations like lawyers are not part of the obliged entities for reporting. The fact that lawyers also participate in financial transactions meant that the Directive have been applicable for them too. However, this Directive was not extended in a such way as to cover professions like lawyers. The major argument was that including lawyers in the Directive as an obliged entity could have direct impact on the confidentiality rules.

Third AML Directive

The Third Directive[270] from 2005 was built up on the revised AML/CTD standards by the FATF from 2003. Two years after 9/11[271] and one year after the Madrid bombing[272] it was finally decided and realized that the Non-Financial Businesses and Professions like lawyers could also (un-) intentionally

---

[268] *See* The Council of the European Communities (1991): Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering

[269] *See* The European Parliament and the Council of the European Union (2001): Directive 2001/97/EC The European Parliament and the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering

[270] *See* The European Parliament and the Council of the European Union (2005): Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

[271] “9/11” is the acronym for the terrorist attacks against the United States of America, which took place on September 11, 2011

[272] On March 11, 2004, the train system of Madrid was attacked by coordinated bombings

participate in ML schemes. The result from the Directive's implementation was a tighter EU AML regime and policy – occupations like lawyers, notaries, real estate agents and businesses like casinos were included within the scope of the Directive. The Third Directive was also the first which included measures against the financing of terrorism. In addition, the Third Directive includes the following key implementation objectives in regard to due diligence:

- Enhanced due diligence for PEP
- Simplified due diligence procedures, transparency and monitoring for low-risk transactions (as assessed by the Member States), which involve public authorities or public bodies

The Third Directive was transposed in Austria in 2007 by amendments of Bankwesengesetz (BWG), Versicherungsaufsichtsgesetz (VAG) and Wertpapieraufsichtsgesetz (WAG).

Fourth AML Directive[273]

On 26 June 2015 the Fourth Directive on Money Laundering as well as the new Regulation (EU) 2015/847 on information accompanying transfers of funds entered into force. This new AML package by the EU includes the adoption and implementation of the 40 recommendations amended in 2012 by the Financial Action Task Force (FATF). The aim of the Money Laundering Directive is to strengthen the financial system of the EU in order to protect it against misuse for the purposes of ML/TF.

Following key aspects were introduced (among others):

- Extension of the risk-based approach,
- Establishment of a register of beneficial owners,
- Extension of the list with predicate offences,
- Regulations for identifications of PEP.

With regard to the Austrian financial sector the implementation was completed with the introduction of the new FM-GwG.

Fifth AML Directive[274]

In June 2016 the European Commission published the proposal to amend the fourth Anti-Money Laundering Directive. On May 14th, 2018 the European Council adopted the Directive.

The Directive aims to strengthen further the financial system as a result of recent terrorist attacks by increasing the transparency:

- in order to prevent large-scale concealment of funds and
- in order to provide easier ownership identification of companies and trusts.

In addition, the risks referring to the use of prepaid cards and crypto- and virtual currencies are also addressed. The Directive has entered into force on July 9th, 2018 following which the EU Member States will have 18 months to implement it in national legislation.

[273] *See* The European Parliament and the Council of the European Union (2015): Directive (EU) 2015/849 of the European Parliament and of the Council

[274] *See* European Commission (2018): Directive (EU) (Proposal) of the European Parliament and of the Council laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences and repealing Council Decision 2000/642/JHA

EU Regulations

Regulation (EC) No 1889/2005 on controls of cash entering or leaving the Community[275]

The regulation was an implementation of FATF Special Recommendation 9. The aim of the regulation was to "*detect the physical cross-border transportation of currency and bearer negotiable instruments*"[276]. This means that travelers carrying EUR 10 000 or more in cash must report this to the customs authorities.

Regulation (EU) No 2015/847 on information accompanying transfers of funds[277]

The Regulation entered in force on 26th of June 2017. It repeals Regulation 1781/2006[278] and requires that every transfer of funds has to include information on payer and payee. The aim of the Regulation was to enable the tracking of transfers.

Regulation (EU) 2016/1675[279] supplements the Fourth EU AML Directive.

There are many other EU Directives and Regulations which are not directly associated with the combat against ML/TF but still are important for the integrity of the financial markets and therefore important to mention here (among others):

- Directive 2014/57/EU on criminal sanctions for market abuse (market abuse directive),[280]
- Regulation (EU) No 596/2014 on market abuse (market abuse regulation),[281]
- Regulation (EC) No 924/2009 on cross-border payments[282].

Consequences of non-implementation

Each Member State is responsible for the implementation of European Community Law within its own legal system and the role of the European Commission is to ensure this by using various mechanisms– from sending a formal letter of notice to the Member State which is still non-compliant to referring the case to the European Court of Justice (ECJ)[283].

In addition, following groups and supervisory authorities exist:

---

[275] *See* The European Parliament and the Council of the European Union (2005): Regulation (EC) No 1889/2005 of the European Parliament and the Council of the European Union of 26 October 2005 on controls of cash entering or leaving the Community

[276] FATF (2001): FATF IX Special Recommendations, p. 3

[277] *See* The European Parliament and the Council of the European Union (2015): 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

[278] *See* The European Parliament and the Council of the European Union (2006): Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds

[279] *See* The European Parliament and the Council of the European Union (2016): Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies

[280] *See* The European Parliament and the Council of the European Union (2014): Directive 2014/57/EU of the European Parliament and the Council of 16 April 2014 on criminal sanctions for market abuse (market abuse directive)

[281] *See* The European Parliament and the Council of the European Union (2014): Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directives 2003/6/EC, 2003/124/EC, 2003/125/EC, 2004/72/EC

[282] *See* The European Parliament and the Council of the European Union (2009): Regulation (EC) No 924/2009 of the European Parliament and of the Council of 16 September 2009 on cross-border payments in the Community and repealing Regulation (EC) No 2560/2001

[283] *Cf.* European Commission (2016): Monitoring implementation of EU directives

- Expert Group on Money Laundering and Terrorist Financing (EGMLTF): the main tasks are to coordinate the Member States and to provide expertise and advise the European Commission. FMA is part of the Expert Group.
- The European Banking Authority (EBA), the European Securities and Markets Authority (ESMA), the European Insurance and Occupational Pensions Authority (EIOPA) and the Subcommittee on Anti Money Laundering (AMLC): they all coordinate the work performed by the national supervisory authorities in the field of ML/TF prevention. FMA, as supervisory authority, is represented in AMLC.

MONEYVAL

Moneyval[284] is the Council of Europe's expert committee for the evaluation of measures against money laundering and terrorist financing. Moneyval was established in 1997 to monitor and facilitate the implementation of the 1990 Convention[285] against Money Laundering and Terrorist Financing. Moneyval uses the FATF standards and reports its findings to the FATF. The aim of the work is to enforce the standards in countries that are members of the Council of Europe but not members of the FATF. Austria is a member of the FATF but not of Moneyval.

3.2.3. Financial Action Task Force (FATF)

The Financial Action Task Force (FATF)[286] was established as an inter-governmental organization in 1989 on the G7 Summit in Paris[287]. The organization has currently 37 members. The main goal of the FATF is "*to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.*"[288]. The role of the FATF is essential because of its Forty Recommendations. This list of recommendations, meanwhile international recognized standards, "*set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing*"[289] and has the aim to support the governments and financial institutions in the combat against MF/TF. The first issue dates back from 1990 and the last, fourth update was in 2012. In 2001 and 2004 9 additional special recommendations concerning the combat against the financing of terrorism were adopted. One of the major tasks of the FATF is the monitoring of the progress of the countries – FATF measures and evaluates the implementation of the recommendations on country level and reviews the current AML policy of the countries in order to protect the international financial system from misuse.

[284] Moneyval (homepage: https://www.coe.int/en/web/moneyval/)
[285] *See* Council of Europe (1990): Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime
[286] The Financial Action Task Force (FATF) (homepage: http://www.fatf-gafi.org/)
[287] *See* G7 Paris Summit (1990): Economic Declaration
[288] FATF (2018): Who we are?
[289] FATF (2018): The FATF Recommendations

UN Resolution 1617 (2005)[290] and Annexed Plan of Action of Resolution 60/288 of the UN General Assembly (20 Sept 2006)[291] highlight the importance of the implementation of the 49 Recommendations by the countries.

3.2.4. Others

Interpol

Interpol[292] is the abbreviation for International Criminal Police Organization (ICPO). It was founded in Vienna in 1923 and is today a worldwide criminal police organization with 192 member states with a headquarter in Lyon, France. The task of the organization is to provide a range of policing expertise and capabilities in the following three main criminal areas: Counter-terrorism, Cybercrime, and Organized and emerging crime. Interpol defines money laundering as "*any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources*"[293].

Interpol supports the combat against ML through exchange of data and as a coordination unit between experts in the field and between national and international organizations.

Europol

The European Union Agency for Law Enforcement Cooperation[294] supports the 28 EU Member States, many non-EU partner states and international organizations in their combat against terrorism, cybercrime and other serious and organized forms of crime including money laundering.

International Money Fund

The role of the International Money Fund (IMF)[295] in the context of AML/CTF is, among others, to provide financial integrity advices to countries and to evaluate their compliance regarding international AML/CTF standards and guidelines.

Eurasian Group

The Eurasian Group (EAG)[296] was established on 6 October 2004 as an initiative of the Russian Federation supported by the FATF, IMF, World Bank and several other countries. The Group is an FATF-style regional body (FSRB) and became an Associate Member of the FATF in June 2010. The goals of the organization it to support the combat against terrorism and increase the transparency and security of the financial systems of the region.

The Egmont Group

The Egmont Group[297] is a "*united body*"[298] of 164 Financial Intelligence Units. The main tasks of this international cooperation are:

[290] *See* The United Nations (2005): Resolution 1617 (2005)
[291] *See* The United Nations (2006): Resolution adopted by the General Assembly on 8 September 2006
[292] Interpol (homepage: https://www.interpol.int/)
[293] Interpol (2018): Money Laundering
[294] Europol (homepage: https://www.europol.europa.eu/)
[295] International Money Fund (IMF) (homepage: https://www.imf.org/)
[296] The Eurasian Group (EAG) (homepage: https://www.eurasiangroup.org/)
[297] The Egmont Group (homepage: https://www.egmontgroup.org/)
[298] The Egmont Group (2018): About Egmont Group

- *"to provide a platform for the secure exchange of expertise and financial intelligence to combat ML/TF*
- *to support the efforts of its international partners and other stakeholders to give effect to the resolutions and statements by the UN Security Council, the G-20 Finance Ministers, and the FATF*
- *to add value to the work of member FIUs by improving the understanding of ML/TF risks"* [299]

The FIUs worldwide are obliged by international AML/CTF standards and bilateral agreements to exchange information with international partners and thus to be part of a worldwide collaboration in the combat against ML/TF. The operative role of the Egmont Group is to facilitate and support this collaboration.

The Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision (Basel Committee)[300] was established by the central bank governors of the Group of Ten countries in 1974. The Committee "*was established to enhance financial stability by improving the quality of banking supervision worldwide, and to serve as a forum for regular cooperation between its member countries on banking supervisory matters.*"
In its core function the Committee formulates supervisory standards, guidelines and recommendations for bank supervisory issues, including money laundering.

The Wolfsberg Group

The Wolfsberg Group[301] is an organization of thirteen of the largest banks worldwide founded in 2000. The main goal of the Group, similar to the goals of the FATF, is to develop standards for the financial sector especially in the fields of AML, KYC and Counter Terrorist Financing (CTF). The group has published 16 documents which are called the Wolfsberg Standards. In 2018 the Group published an updated Correspondent Banking Due Diligence Questionnaire (CBDDQ). "*The CBDDQ aims to set an enhanced and reasonable standard for cross-border and/or other higher risk Correspondent Banking Due Diligence, reducing to a minimum any additional data requirement, as per the Wolfsberg definition and current FATF Guidance.*"[302]

[299] The Egmont Group (2018): About Egmont Group
[300] The Basel Committee on Banking Supervision (Basel Committee) (homepage: https://www.bis.org/bcbs/)
[301] The Wolfsberg Group (homepage: https://www.wolfsberg-principles.com/)
[302] The Wolfsberg Group (2018): Wolfsberg CBDDQ

3.3. Other aspects related to the combat against money laundering

The costs of compliance

The total costs of compliance in 5 European countries (Germany, Italy, France, Switzerland and The Netherlands) was estimated at approximately 83 billion USD in 2017[303]. This is an increase from almost 40% since 2015. The major reason for this increase is the implementation of the Fourth EU AMLD which has been transposed in 2017 in most of the EU Member States. According to a market survey[304], most of the compliance costs (around 75%) are caused by laboring and staffing of professionals. The remaining 25% are for investments in new AML technologies or update of the existing solutions. Therefore, the financial institutions are struggling to optimize their risk management systems by introducing intelligent solutions which may optimize the processing time for tasks performed manually by the employees. Currently, the banks are hit by the "80/20" Pareto principle rule. In the context of AML 80% of the overall AML costs are caused by 20% of the customers. Approximately the due diligence could take up to 30 hours for foreign corporate clients, while only approximately 10 new accounts are opened monthly. Therefore, the financial institutions are confident that an optimization of the internal AML compliance procedure could lead to better customer relationship management and risk assessment[305]. It is also important to mention that the costs of compliance are not lower for smaller banks with less customers (compared to financial institutions which are, for example, internationally represented). In order to fulfil their legislative obligations smaller financial institutions, which are in most cases cost-sensitive, sometimes decide to outsource certain activities (like screening or online-identification) to third-party service providers (e.g. FinTechs)[306].

The risk of fines is still (not) ok

Only between March and June 2017 11 different banks and companies were fined with around 500 million USD for violating AML laws in different countries[307]. In only few of these cases as per June 2018 it came to imprisonment of the corresponding responsible individuals from these companies. In case of non-compliance the most common penalty is a monetary fine and it is not relatively rare, at least in the U.S., when a particular bank employee gets imprisoned[308]. However, no matter how big the fine is (few examples: approx. 2 billion USD for HSBC and 320 million USD for Standard Chartered in 2012, 8.9 billion USD for BNP Paribas in 2014) and how high the risk for reputation loss is, it seems that the penalized banks are dealing well with such fines and one should ask: do penalties have real pedagogical impact on the financial institutions? It is believed that for example the US Department of Justice "*has chosen not to prosecute bank officers for fear of threats to the stability of the financial*

[303] *Cf.* PR Newswire (2017): European Financial Services Providers face overall Anti-Money Laundering Compliance costs of $83.5 billion a year
[304] *Cf.* Ibid.
[305] *Cf.* Ibid.
[306] *See* the interview with Mag. Oliver Floth from 12.06.2018, lines 70-84
[307] RiskScreen (2017): Infographic showing significant AML fines between March & June 2017
[308] *See* IRS (2018): Statistical Data - Money Laundering & Bank Secrecy Act (BSA); *Please note*: in this master thesis the term "imprisonment" includes confinement to prison, halfway house, home detention, or some combination thereof

system as a whole."[309]. Similar is the case in Austria. FMA may publish the name of the natural person or legal entity in case of a violation of different duties, according to **§ 34 FM-GwG**[310], in case that such publication does not seriously endanger the stability of the financial markets. However, the fear of fines should not be the main motivation for implementing an adequate AML program. "*Rather, financial institutions need to be increasingly vigilant as regulators continue to raise the standard for corporate integrity and as consumers and clients increasingly expect demonstrated moral behavior from their banks.*"[311]. Penalties and fines for faulty AML should be adequate, of course and the authorities should be able to distinguish between systematic non-fulfillment of the AML obligations and unintended circumstances, for example, the case that the ID of a particular customer is expired[312].

De-risking vs. risk-based approach

When there is no risk for ML/TF there is no need to measure the risk factors, do risk profiling, define controls for risk mitigations, etc. And when there are no undetected cases for ML/TF there are no penalties for banks. One of the objectives of the Fourth EU AML Directive is to strengthen the European financial system by increasing transparency and strengthen the customer checks. Thus, "low risk" customers or a customer that was considered as "low risk" are potentially re-assessed as "high risk" customers. In addition, the nature of the bank and customer business relationships previously seen as opportunities are classified now as risky (for example, the sanctions against the Islamic Republic of Iran led to a situation of unwillingness for the banks to establish business relationships there)[313]. The term "de-risking" means basically to cut off the access to financial instruments or services for banks and customers from particular regions under particular conditions due to their high-risk assessment. The main reason for the "de-risking" is the reputation risk for the financial institutions. When a financial institution decides not to establish business relationship with, for example, customers who have accounts in an offshore country (even though the establishment of such a business relationship is not illegal), the bank decides to act with caution and thus to mitigate the reputation risk[314]. As a side effect of the "de-risking" approach the access to the financial markets and banking services from legitimate businesses from particular business fields (like Bitcoin exchangers or third-party payment services) is denied. This can force businesses and customers to use alternative and maybe less regulated or even illegal transaction channels. The FATF is trying to discourage the application of this approach by the financial institutions and proposes a (risk-based) assessment on case-level and extension of the CDD process by expanding the verification process and using reliable and independent information sources[315]. This means that every case could be analyzed more carefully to understand the customer better and do the risk assessment more

[309] Trulioo (2015): What happens when businesses don't comply with AML/KYC regulations?
[310] **§ 34 FM-GwG**, Fassung vom 25.06.2018, regulates the penalties and fines in case of a violation of different duties stipulated in the FM-GwG
[311] Trulioo (2015): What happens when businesses don't comply with AML/KYC regulations?
[312] *See* the interview with Mag. Oliver Floth from 12.06.2018, lines 120-131
[313] *Cf.* Correia (2015): False positives: a growing headache
[314] *See* the interview with Mag. Oliver Floth from 12.06.2018, lines 100-119
[315] *Cf.* FATF (2013): Revised Guidance on AML/CFT and Financial Inclusion, p. 6 and FATF (2017): FATF Guidance on AML/CFT measures and financial inclusion, with a supplement on customer due diligence, p. 10;
Please note: Directive (EU) 2015/849 and Regulation (EU) 2015/847 do not specify what "*reliable and independent sources*" are

accurately. Despite its overall short- and mid-term negative effects[316], de-risking is currently still preferable by the financial institutions than the risk-based approach presented in section 3.1.3. due to the high efforts and operative challenges while managing the financial transactions and due to the reputation loss for the banks in case of disclosed money laundering cases reported in the last years. Therefore, the de-risking is an understandable reaction of the financial institutions, but it is the wrong approach because in effect it leads to increase of the overall ML-risk[317].

Different AML legislatives

Unger et al.[318] highlighted in 2006 one major problem regarding the internationality of the combat against ML: "*the problem is that, despite harmonizing efforts at both European and international level, national legislations criminalizing money laundering continue to differ. Most countries have criminalized serious offences but have nevertheless, adopted different approaches to what constitutes a serious crime for the purpose of. Thus, the predicate offences that generate proceeds vary from one country to another.*" In the same publication, the authors proposed two alternative solutions to this problem: either "*to extend the scope of predicate offences to cover all crimes*"[319] or "*to adopt a more restrictive approach to predicate offences so as to cover only crimes generating substantial proceeds*"[320]. However, in practice, it is not the differences in criminal law that play a major role but the different priorities of the national authorities[321].

GDPR

GDPR (General Data Protection Regulation)[322] came into effect on 25th of May 2018 with around 200 pages of regulations regarding the privacy of data. The Regulation affected how the companies manage, process, store and delete data. This includes the financial institutions – due to their due diligence obligations they have to store and process personal data about their customers and how they do this has to be transparent. Thus, GDPR has a direct impact on how the financial institutions act in regard of their AML programs[323]:

- GDPR requires increased security standards for all data, collected during the KYC process
- Increased use of automation (incl. automatic onboarding for new customer, automatic monitoring and data enrichment process)

However, the new Regulations are seen as "*an additional hurdle on the cross-border transfer of data to a country outside of the EU, if that country to which the data is being transferred has been deemed to have inadequate data protection laws. A country is only considered to provide an*

[316] *Cf.* The World Bank (2016): De-risking in the Financial Sector and
Cf. ACAMS Today (2017): De-Risking and Financial Inclusion
[317] *See* the interview with D. Thelesklaf, lines 16-19
[318] Unger et al. (2006): The amounts and effects of money laundering, p. 25
[319] Ibid., p. 27
[320] Ibid., p. 27
[321] *See* the interview with D. Thelesklaf, lines 20-22
[322] *See* The European Parliament and the Council of the European Union (2016): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
[323] *Cf.* Security Watchdog (2017): The impact of GDPR on KYC

adequate level of protection if they provide protections of essential equivalence to those protections in the EU."[324].

Barriers in the international cooperation

The main objective of the STR is to prevent and detect the misuse of the financial system for the goals of ML/TF. Most of the FIUs in the European Union are from an administrative type. Thus, they are playing an essential role in the transmission and coordination of STR and are not responsible for investigative tasks. In their role they must exchange financial data and financial intelligence on a domestic and international level independent of their type and authority powers. The international cooperation is, as described before, supported by different forums like the Egmont Group (preferred for information exchange with non-EU Member States) or FIU.net (preferred for information exchange with EU Member States). A major problem in this context is the missing ability of the FIU to cooperate with non-FIU counterparts. Due to the nature of ML/TF the international cooperation between EU and for example, U.S. law enforcement authorities, is crucial. For example, a STR generated in an EU-Member State may lead to investigation in the U.S. and culminate with a law enforcement operation in Asia. Currently, however, such scenarios are hardly possible, due to the simple fact that a FIU from an administrative type is prevented to share or even to forward STRs cross-border.
However, the ability to perform this role is limited by the classification of many FIUs as administrative, preventing the sharing of cross-border STRs diagonally with law enforcement[325].

3.4. Summary

The Austrian jurisdiction is a good example for a basically successful AML policy but there is room for improvements. For example, a consolidation of all legislative texts regarding the definition and combat against ML/TF would be the first step[326]. The Austrian government and experts struggled in the last few years to increase the country's ratings after the recommendations made by the FATF by developing the National Risk analysis and implementing the AMLD4. This was a huge step in the right direction. With the upcoming AMLD5 two major changes on national levels are expected:

- The identification and verification of producers, exchange platforms, wallet providers and customers that are issuing and using virtual/crypto-currencies (such as Bitcoin)
- The easier and centralized access of the FIUs to payment account registers or data retrieval systems

It is just a matter of time to see if the number of STRs in next years will further increase or stay steady even if it is not a real AML performance indicator or sign of success[327]. Nevertheless, a reversal in the way of investigations can be suggested to make the investigative process and prosecution more efficient. For example, without the need for proving the existence of a predicate offence one (a suspected individual or a suspicious group) would have to prove the legal origin of his/her/their funds. With the implementation of AMLD5 it is also expected that the real estate agents and real estate

[324] Hughes (2017): The Importance of Incorporating Data Privacy into Anti-Money Laundering and Anti-Corruption Compliance Programs, p.4
[325] *Cf.* EUROPOL (2017): From Suspicion to Action, p. 34
[326] *See* the interview with Dr. E. Scherschneva-Koller from 04.06.2018, lines 66-69
[327] *See* the interview with D. Thelesklaf, lines 5-6

companies will be excluded from the list of the obliged entities, despite critique from experts and despite the fact the real estate market is one of the channels through which illicit money may be successfully laundered[328].

Another problematic aspect that must be taken into account is the balance between transparency and (personal) data protection. For example, a European-wide register of all beneficiaries of companies could ease the investigative processes. However, currently it is hard to predict, what the impacts and effects from the establishment of such or similar register for the financial system and/or for the society as a whole would be.

In the last decades many initiatives with the goal of combat ML were introduced on international level. At the beginning these initiatives "*led to a huge amount of conflicting agreements, various standards and recommendations, that does not help the FIUs, but make their main task more difficult, because this has contributed to jurisdictional arbitrage whereby money launderers can take advantage of*"[329]. Meanwhile a progress has been made. For example, The Forty Recommendations by the FATF or The Wolfsberg Standards are recognized worldwide and established as standards and they are used for effective combat against the money laundering. One small part of the puzzle is missing – the easier communication and collaboration between the national FIUs. When this happens in reality then the combat will become more successful than ever.

[328] *See* BMDW (Bundesministerium für Digitalisierung und Wirtschaftsstandort) (2018): (Begutachtungsentwurf) Risikobewertungsausnahmeverordnung - RAV, Fassung vom 26.06.2018 and
See Profil (2018): Regierung nimmt Immobilienmakler von neuen Anti-Geldwäsche-Regeln aus and
Cf. FATF (2007): Money laundering and terrorist financing through the real estate sector, p. 4 and
Cf. OECD (2007): Report on tax fraud and money laundering vulnerabilities involving the real estate sector, pp. 2-3

[329] Unger et al. (2006): The amounts and effects of money laundering, p. 2

chapter 4

Detection and prevention of money laundering

One can ask provokingly "*Why fighting money laundering? Why don't we leave the things as they are?*".

In 2001 Dr. Richard W. Rahn[330] stated: "*We are told we must stop money laundering in order to combat terrorism, drug dealing, assorted criminality, and tax evasion. However, if you look at the results of this so-called war on money laundering, you find that it has failed to produce the advertised results and, in fact, has not been cost effective, has resulted in wholesale violations of individual civil liberties (including privacy rights), has violated the rights of sovereign governments and peoples, has created new opportunities for criminal activity, and has actually lessened our ability to reduce crime."*[331] In the next 16 years Dr. Rahn did not change his opinion: *"The current effort to stop money laundering has turned into a disaster for the global poor, who can no longer get bank accounts or easily and legally transfer money (remittances) to their relatives in poor countries. The anti-money laundering laws and regulations have made international trade and investment more expensive, thus perpetuating poverty. They have destroyed much legitimate financial privacy, and they have undermined the rule of law by destroying due process. Serious drug dealers, criminals, tax evaders and terrorists can find plenty of legal and illegal ways to launder money."*[332]

Of course, the opinion of Dr. Rahn is just one side of the coin. FATF claims that "*the economic and political influence of criminal organisations can weaken the social fabric, collective ethical standards, and ultimately the democratic institutions of society. In countries transitioning to democratic systems, this criminal influence can undermine the transition. Most fundamentally,*

[330] Richard W. Rahn is an American economist, specialized in the fields of supply-side economics, was the Vice President and Chief Economist of the United States Chamber of Commerce during the Administration of Ronald Reagan (1981-1989)
[331] Competitive Enterprise Institute (2001): Why the war on Money Laundering should be aborted
[332] The Washington Times (2017): Useless anti-money laundering laws

money laundering is inextricably linked to the underlying criminal activity that generated it. Laundering enables criminal activity to continue."[333]

In addition, the Basel Committee states that "*public confidence in banks, and hence their stability, can be undermined by adverse publicity as a result of inadvertent association by banks with criminals. In addition, banks may lay themselves open to direct losses from fraud, either through negligence in screening undesirable customers or where the integrity of their own officers has been undermined through association with criminals. For these reasons the members of the Basle Committee consider that banking supervisors have a general role to encourage ethical standards of professional conduct among banks and other financial institutions.*"[334]

In my opinion, the most important reason for the combat against ML was clearly formulated by the OECD in 2009: "*Money laundering allows the criminal to start, continue and expand activities in legitimate sectors of the economy. It may create a perception that crime pays and may also have a stimulating effect on our youth starting a criminal career.*"[335] That is why money laundering cannot just be ignored. However, the moral aspects and the specific purpose of the combat against ML and the discussion about "privacy against bank secrecy" are beyond the scope of this master's thesis. In 2006 Unger et al. made a comprehensive analysis of the effects of ML[336]. This chapter will focus more on the current state of the technologies used to support this combat, on the know-how and experience which the compliance officers should have and on the mountain of information they should climb every day in order to manage the ML cases.

I distinguish the combat against ML in two parts: detection and prevention and these parts can be seen from three different points of view: technology, data, people. According to Merriam-Webster, "*detecting*" means "*to discover or determine the existence, presence, or fact of*"[337] and "*preventing*" means "*to keep from happening or existing*"[338]. In the context of ML both terms are most commonly associated with the techniques and methodologies based on previous experience. The software vendors would not be able to implement software solutions based on mere assumptions how the money laundering process could look like. The financial institutions would not be able to prevent the misuse of their infrastructure for the goals of ML without knowing how theirs or another infrastructure were exploited in the past. In both cases, the term "experience" plays a major role. It is interesting to know how the financial institutions use their resources, how they re-organise themselves, how the external factors have influence on their internal decisions and processes. The mere definition or implementation of an internal AML programme without its successful use could be seen as a waste of money, time and expertise. The financial institutions are those who define what "success" in the context of AML actually means and what factors are involved in achieving of this goal. For example, the number of alarms, the processing and analysis time of these, the number of reported STRs are

[333] FATF (2018): Money Laundering
[334] The Basel Committee on Banking Supervision (BCBS) (1988): Prevention of criminal use of the banking system for the purpose of money-laundering, pp. 1-2
[335] OECD (2009): Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors, p. 11
[336] *Cf.* Unger et al. (2006): The amounts and effects of money laundering, p. 14 and pp. 115-153
[337] Merriam-Webster (2018): "*detecting*"
[338] Merriam-Webster (2018): "*preventing*"

good performance indicators, which can be further to use to optimize the internal processing and to calibrate the IT systems[339]. The research made in this chapter answers the first research question:

RQ1: Is there a correlation between a bank's internal competences (organizational structure, IT, know-how) and the number of Suspicious Transaction reports (STRs), classified as "money laundering", reported by this bank?

In this chapter I will show how a good AML programme could look like, representing the three main aspects of it – technology, data, people. The recommendations made below are based entirely on literature research and expert interviews.

4.1. Technology

The combat against ML has become a high strategic priority for most of the financial institutions worldwide. With the aim to develop effective AML and overall complaint programs, the banks are facing challenges on almost every level of their internal organisations – from hiring the right employees up to the choice of the appropriate AML software solution that can successfully support them. The role of the data processing is getting even more essential. It does not matter anymore if the collected customer data is highly detailed and up-to-date – it is important to know how to use and process it successfully. In its core the detection of ML is pure analysis of data or alerts, based on specific internal processes. In the past the early IT-solutions were not able to process the amount of information effectively and many analytical steps were or are still done manually by the corresponding employees and this can be resource-intensive and -consuming. The answer of the banks to such situation is hiring more employees and extend the AML and compliance teams. However, the supply of skilled workers could not fulfil the demand leading to an increase of the salaries of AML professionals which led further to an increase of the overall costs for compliance. The internal AML system, deployed in a bank, is most probably one of the oldest in a bank's application portfolio. This means that they are or should be those applications that are mostly being kept up-to-date or at least being updated regularly, so the banks can benefit from the new capabilities that the installed or renewed solutions provide. Meanwhile, there is a trend that the financial institutions are investing in new AML solutions or replacing their existing AML solutions that support and have the capability to automatically process the previously manually done analytical steps[340]: "*Investing in AML software can reduce manual review requirements, minimize the occurrence of false positives*[341]*, and streamline the regulatory reporting process.*"[342]

But one thing must not be ignored: the "installation risk". The deployment of an AML software is associated with following key risk drivers (among others)[343]:

- "*risk of inaccurate or time-consuming compliance with regulatory requirements*"
- "*vulnerability of the system to security threats*"

[339] *See* the interview with Mag. Oliver Floth from 12.06.2018, lines 52-69
[340] *Cf.* CEB (2016): Combatting Rising Threats with Aging Infrastructure, pp. 5-9
[341] Merriam-Webster (2018): "*false positive*"; Also called in the literature „*false positive error*". According to Merriam-Webster, false positive means "*a result that shows something is present when it really is not*"
[342] CEB (2016): Combatting Rising Threats with Aging Infrastructure, p.6
[343] Ibid., p.7

- "*ability of the system to meet current and projected transaction volume*"

In order to detect suspicious movements of money all transfers must be monitored by the financial institutions. The monitoring itself may be seen as a combination between computer technologies, organisational structures, like compliance offices and reporting requirements. Because of the amount of money which is transferred daily the computer technologies are the foundation for such monitoring.

Transaction monitoring systems (TMSs) represent the core of the suspicious activity reporting. The monitoring system in every financial institution is based on the risk assessment made by this institution. It allows the banks to monitor the transactions for risks in real-time or on a daily basis.

The major critique on the current TMSs is that the costs for the current solutions keep increasing, while the satisfaction from them declines[344]. From a functionality point of view, TMSs are working on rule-based principle[345] which may be very resource- and cost-intensive[346]. When a particular rule is fulfilled, or a particular condition is met, the system triggers a predefined action. Meanwhile, the development of such system goes in direction of the machine learning, AI and advanced analytics[347].

In the literature and in the WWW one can easily find an enormous amount of information about the technology used to support the fight against ML[348]. Therefore, with all my respect, I will spare the reader the information and details, that has been already published multiple times by multiple channels and by multiple authors[349]. In this chapter I will focus more on the current state of technologies by providing an overview over few solutions on the AML software market (section 4.4.) and over the tasks those solutions currently can fulfil and the capabilities they provide. The reason for this is the rapid development of the artificial intelligence (AI) and machine learning in the last years and its direct impact on the software development and solutions including the software used to support the employees and financial institutions in the combat against ML[350].

According to a report published in 2017 the global AML software market is about to grow further and is expected to reach 1.4 billion USD by 2023[351]. But what does "information technology" actually mean in the context of AML? Is it a software solution or is it a mix of internal and external (and therefore outsourced) software and hardware solutions? Does the use of a particular software improve the detection rate and therefore minimize the risk of money laundering? What is needed to integrate such software and at what costs? What will the used software actually do and which capabilities it has in order to support the AML policy of the financial institution? What is the best IT solution against ML?

---

[344] *Cf.* KPMG (2014): Global Anti-Money Laundering Survey, p. 21
[345] *Cf.* Financial Service Authority (2016): Automated Anti-Money Laundering Transaction Monitoring Systems, p. 1
[346] *Cf.* Accenture (2017): Leveraging machine learning within anti-money laundering transaction monitoring, p. 3
[347] *Cf.* Kumar (2017): To truly transform KYC and AML operations adopt AI and ML and
Cf. McKinsey & Company (2017): The new frontier in anti–money laundering and
Cf. McKinsey & Company (2017): Risk analytics enters its prime
[348] A search online for „technologies for detecting money laundering" returned on 20.05 2018:
- around 680 000 matches via google.com,
- around 3 million matches via bing.com,
- around 61 million matches via yandex.ru (translated term in Russian: "технологии обнаружения отмывания денег")
- around 1000 matches via baidu.com (translated term into traditional Chinese: "檢測洗錢的技術")

[349] One very detailed publication is the report "Information Technologies for the Control of Money Laundering" by the U.S. Congress, published in 1995. Beside this, the digital library of the IEEE (Institute of Electrical and Electronics Engineers, https://ieeexplore.ieee.org) offers an access to many publications and research papers on the topic "Detection of money laundering"
[350] *Cf.* Celent (2016): Artificial Intelligence in KYC-AML: Enabling the Next Level of Operational Efficiency and
Cf. Raj (2018): How Financial Institutions Can Use AI to Enhance Due Diligence
[351] *Cf.* BIS Research (2017): Global Anti Money Laundering (AML) Software Market - Analysis and Forecast (2017-2023)

In my opinion, it is hard to give a universal answer to all of the above. The use of a particular software depends on the size and the risk assessment of the financial institutions. The numerous features that the software products currently offer must be used appropriately so there can be an impact. Therefore, it is more accurate to ask following: "*What must the bankers do in order to avoid problems?*" and "*What should a software product for a successful AML policy look like?*".

In this section I will address the research on only one aspect of the above questions: Which tasks must the software solutions provide for successful AML strategy?

From the legal point of view, FMA states that the technologies used to support the financial sector (FinTechs[352]) "*are also expected to comply with the due diligence obligations for the combatting of money laundering and terrorist financing, if they provide activities that require a licence and are therefore subject to supervision by the FMA*"[353]. Until 2018, the use of IT-Systems was not legally regulated in Austria; thus, the IT compliance of the financial institutions was not regulated by any law in Austria and it was up to the banks to decide how they must manage and use different software and hardware solutions. There are official guidelines and collections of best practises how the banks can build and manage their own IT landscape[354] and meanwhile, in 2018 the EU Directive 2016/1148[355] concerning the security of network and information systems was incorporated into national law. This topic is however beyond the scope of this thesis.

In addition, the term "RegTech" is getting more and more broader understanding. These are solutions that help and support highly regulated industries like financial sector in their compliance challenges[356].

In Germany, for example, the IT-Sicherheitsgesetz[357] (among others) regulates data protection and information security in terms of availability, confidentiality, integrity and authenticity.

Every financial institution in Austria must at least do the following in order to detect and prevent ML[358]:

1. Establish a FM-GwG compliance program

Banks must have a Finanzmarkt-Geldwäschegesetz (FM-GwG) and Bankwesengesetz (BWG) compliance program. Banks, as outlined in **§ 42 BWG,** must assure the compliance regarding FM-

---

[352] Dorfleitner et al. (2017): FinTech in Germany, p. 5: "*The term "FinTech," which is the short form of the phrase financial technology, denotes companies or representatives of companies that combine financial services with modern, innovative technologies*"

[353] Finanzmarktaufsichtsbehörde (FMA) (2018): FinTech Navigator, translated from German: "*FinTechs haben die Sorgfaltspflichten zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung jedenfalls dann einzuhalten, wenn sie konzessionspflichtige Tätigkeiten erbringen und daher der Aufsicht der FMA unterliegen*"

[354] *See* WKO (2018): IT-Sicherheit, Datensicherheit and
Finanzmarktaufsichtsbehörde (FMA) (2018): FMA Guide on ICT Security in Credit Institutions

[355] *See* The European Parliament and the Council of the European Union (2016): Directive (EU) 2016/1148 and
See Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), Fassung vom 23.09.2019

[356] *Cf.* PwC (2017): Get ready for RegTech

[357] *See* Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Fassung vom 26.06.2018

[358] In alignment with **FM-GwG**, Fassung vom 25.06.2018, and
Office of the Comptroller of the Currency - U.S. Department of Treasury (2002): Money Laundering: A Banker' s Guide to Avoiding Problems, pp. 9-17 and
Finanzmarktaufsichtsbehörde (FMA) (2011-2012): FMA Circulars on prevention of Money Laundering & Terrorism Funding and
The Basel Committee on Banking Supervision (BCBS) (1988): Prevention of criminal use of the banking system for the purpose of money-laundering and
The Wolfsberg Group (2006): Guidance on a Risk Based Approach for Managing Money Laundering Risks

GwG[359]. According to **§ 23 FM-GwG**, the banks must develop "*policies, controls and procedures to reduce and manage effectively the risks of money laundering and terrorist financing identified at […] national and company level […]*"[360] In addition, the bank must be compliant in regard of the record keeping and reporting requirements (**§ 16 FM-GwG**).

The developed policies, controls and procedures must be written, approved by the management board, updated, when necessary and should contain the following:

1. a risk assessment at customer level (**§ 6 FM-GwG**)
2. a risk assessment regarding PEP (**§ 11 FM-GwG**)
3. an appropriate due diligence according to **§§ 7-9 FM-GwG**
4. a fully developed reporting mechanism (**§ 16 and § 22 FM-GwG**)
5. an adequate record keeping procedure (**§ 21 FM-GwG**)

In addition, the banks must establish a compliance officer in order to ensure the compliance with the provisions of the legal act. The officer is responsible only to the management board and must report directly and without an intermediate level.

One interesting aspect is missing: the (independent) tests of the developed compliance strategy. The banks are legally not obliged to test their own environment in regard of CDD. Moreover, they must ensure the existence of adequate AML policies which are later checked by the FMA. FMA in this case is the authority which supervises the fulfilment of the regulations (**§ 25 FM-GwG**):

"*The FMA must monitor compliance by […] with the provisions of this Federal Act and Regulation (EU) 2015/847 with the aim of preventing the use of the financial system for the purpose of money laundering and terrorist financing.*"[361]

This approach is similar to **§ 11a Finanzkonglomerategesetz (FKG)**[362].

The Basel Committee[363] states in this context, that the "b*anks' management should ensure that business is conducted in conformity with high ethical standards and that laws and regulations pertaining to financial transactions are adhered to. As regards transactions executed on behalf of customers, it is accepted that banks may have no means of knowing whether the transaction stems from or forms part of criminal activity. Similarly, in an international context it may be difficult to ensure that cross-border transactions on behalf of customers are in compliance with the regulations of another country. Nevertheless, banks should not set out to offer services or provide*

---

[359] **§ 42 BWG**, Fassung vom 25.06.2018, translated from German: „*Kreditinstitute und Finanzinstitute haben eine interne Revision einzurichten, die unmittelbar den Geschäftsleitern untersteht und ausschließlich der laufenden und umfassenden Prüfung der Gesetzmäßigkeit, Ordnungsmäßigkeit und Zweckmäßigkeit des gesamten Unternehmens dient.*"
(4) Die interne Revision hat auch zu prüfen:
3. die Einhaltung des § 41 und der Bestimmungen des FM-GwG;

[360] **§ 23 FM-GwG**, Fassung vom 25.06.2018, translated from German: „*Die Verpflichteten haben Strategien, Kontrollen und Verfahren zur wirksamen Minderung und Steuerung der […] auf nationaler Ebene und auf Unternehmensebene ermittelten Risiken von Geldwäscherei und Terrorismusfinanzierung einzurichten […].*"

[361] **§ 25 FM-GwG**, Fassung vom 25.06.2018: „*Die FMA hat die Einhaltung der Vorschriften dieses Bundesgesetzes und der Verordnung (EU) 2015/847 durch […] mit dem Ziel zu überwachen, die Nutzung des Finanzsystems zum Zwecke der Geldwäscherei und der Terrorismusfinanzierung zu verhindern.*"

[362] Bundesgesetz über die zusätzliche Beaufsichtigung der Kreditinstitute, Versicherungsunternehmen und Wertpapierfirmen eines Finanzkonglomerats (Finanzkonglomerategesetz - FKG), Fassung vom 26.06.2018, **§ 11a FKG**: „*Die FMA hat als die für die zusätzliche Beaufsichtigung zuständige Behörde angemessene und regelmäßige Stresstests bei Finanzkonglomeraten durchzuführen.*"

[363] *See* section 3.2.4. for more information about the international cooperation in regard of the combat against ML/TF

active assistance in transactions which they have good reason to suppose are associated with money-laundering activities."[364]

2. Establish an effective CDD system and monitoring programs

Customer due diligence, as described in chapter 3.1.4, is the only way the banks can defend themselves against ML/TF or against being unintentionally exploited for such goals. Thus, to detect ML means to know the customers. This includes not only the verification of the identification of the customer, but also to understand his/her transactions, businesses and/or business relationships. An appropriate CDD framework is in the core of the compliance in regard of different reporting provisions.

The Basel Committee's proposal in this case is that the "*banks should make reasonable efforts to determine the true identity of all customers requesting the institution's services. […] It should be an explicit policy that significant business transactions will not be conducted with customers who fail to provide evidence of their identity.*"[365]

One big challenge in this context and in regard to the monitoring that the banks always have to keep in mind is the problem with high "false positives" and/or "false negatives" rates. Two examples: due to their enhanced due diligence obligations the financial institutions are not allowed to establish business relationships with groups like Hezbollah[366] and due to the high reputation risk the banks mostly avoid business contacts with companies for which it is reported that they employ child labour. The list of exclusions could be very long and to mitigate such risks the banks monitor their customers and transactions on a daily basis. The process of monitoring could be very complex and mostly caused by the different national- and international jurisdictional requirements (for example, a branch of an U.S. bank in Europe has to fulfil both jurisdictions – U.S. and that of the territory it is operating in). The result of such monitoring is a high number of "false positives". Shortly, "false positives" are false alarms that something suspicious is happening and it needs further analysis (which generates further costs), but at end it turns out that everything was alright. It is believed that around 80% of the alerts reported on daily basis are "false positives". "False negatives" are just the opposite. A non-suspicious customer behaviour turns out to be a tax fraud or a scam scheme (without further investigation from the financial institution and without any financial loss for the bank). When a bank has to screen millions of customers the costs could increase tremendously. There is a direct connection between the increasing rate of "false positives" and the growing number of obligations to fulfil (for example, the sanctions against Russian citizens and companies after Russia's intrusion in the Crimea in 2014 or the Fourth EU AML Directive which included requirements for real estate companies)[367]. A typical example for a cost- and resource-intensive analysis of a single "false positive" is following scenario:

---

[364] The Basel Committee on Banking Supervision (BCBS) (1988): Prevention of criminal use of the banking system for the purpose of money-laundering, p. 3

[365] The Basel Committee on Banking Supervision (BCBS) (1988): Prevention of criminal use of the banking system for the purpose of money-laundering, p. 3

[366] Encyclopaedia Britannica (2018): *„Hezbollah is a militia group and political party that first emerged as a faction in Lebanon following the Israeli invasion of that country in 1982."*

[367] *Cf.* Correia (2015): False positives: a growing headache

A customer withdraws cash in such a pattern that the activity is recognised as possible structuring and thus as a suspicious for ML[368]. The structuring pattern is the following: cash withdrawals at either the same of different bank branches, on the same or following days. This activity would generate then an internal STR due to the high risk of the activity and/or the customer. The generated STR would mean that the customer activity and behaviour will become subject to a detailed analysis. If the suspicious behaviour can be proven this would be reported to the corresponding law enforcement authority. The law enforcement authority will then invest time and resources in analysing the behaviour by generating documentation, questionnaires and records about the case. The investigation would include also branch managers and bank employees. In the course of the investigation it may turn out that the reasons for the "suspicious" activity have "logical" explanation: the bank had set a cash withdrawal limit for several nearby branches below the expected by the customer (for example EUR 400). Therefore, the customer had to visit several branches to receive the needed cash. This simple situation could trigger high investments during the investigative process.

There will be always "false positives" and "false negatives" that will be undetected by the corresponding monitoring programs. Relying purely on the algorithm implemented in the program can cause high financial costs. An error in the software is manageable but the mitigation of the risks must have a higher priority[369].

3. Establish an effective screening program

§ 11 FM-GwG regulates the business relationships with politically exposed persons (PEP). PEP is defined, according to **§ 2 (6) FM-GwG** as "*a natural person who holds or has held important public offices*"[370], such as ministers, parliament members, members of supreme courts, ambassadors, etc. The regulation refers also to the family members of the PEP or persons who are known to be close to PEP. In such cases the enhanced due diligence obligations stated in **§ 9 FM-GwG** must apply. One of the goals of such screening is the mitigating of the sanctions and financial crime risks.

The screening or matching process can be done based on several lists (like Sanctions or Embargo's List, published by the UN[371], EU[372] and other national[373] or international organisation), information provided by the customer and/or simply by doing a research in the news. The screening can be "*reverse*" or "*forward*" (a comparison of the client's data with the World Check database[374]) or event-triggered, can be done manually for particular customers or automatically (and therefore, periodically) for all new or existing customers[375].

One major problem may occur when using a faulty screening software. This may lead to higher "false positives" or "false negatives", as described above.

---

[368] See section 2.1.1. The three-layer model; "*structuring*" is part of the layering phase
[369] *Cf.* ACAMS Today (2017): Artificial Intelligence: The Implications of False Positives and Negatives
[370] **§ 2 (6) FM-GwG**, Fassung vom 25.06.2018, translated from German: „*eine natürliche Person, die wichtige öffentliche Ämter ausübt oder ausgeübt hat*"
[371] *See* UN (2018): Consolidated United Nations Security Council Sanctions List
[372] *See* European Union External Action (2018): Consolidated list of sanctions
[373] *See* Wirtschaftskammer Österreich (2017): Länder- oder personenbezogene Embargos und Sanktionen and U.S. Department of the Treasury (2018): Consolidated Sanctions List Data Files
[374] *See* Thomson Reuters (2018): About World-Check
[375] *Cf.* Sanctions Alert (2016): Faulty sanctions screening software can lead to fine, underscoring need to have appropriate tools in place

4. Establish an effective reporting process

Banks must report every suspicious transaction or activity of their customers[376]. This does not mean that the banks must know or understand the origin of the (eventually) illicit money. Their only task is to report this accordingly. The decision if there is a reason for further investigation or not is in the responsibility scope of the law enforcement authorities. As a further confirmation, the Basel Committee states that "*Banks should cooperate fully with national law enforcement authorities to the extent permitted by specific local regulations relating to customer confidentiality. […] Where banks become aware of facts which lead to the reasonable presumption that money held on deposit derives from criminal activity or that transactions entered into are themselves criminal in purpose, appropriate measures, consistent with the law, should be taken, for example, to deny assistance, sever relations with the customer and close or freeze accounts.*"[377]

Europol criticized the current reporting mechanisms and regulations and gave recommendations what could be technologically done to be able to provide adequate reporting procedures: „*Often, when a bank officially reports an offence to their FIU, by the time it is addressed or reaches investigative services, the data provided is old and little can be done to identify the offenders or recover funds.*"[378]

This could be improved by the use of appropriate software solutions: *"*[…] *technology could help in building targeted intelligence-led monitoring to leverage the quality of STRs through collaborative secure channels of communication. This would also enable financial institutions to cooperate on key investigations and speed up law enforcement access to relevant data. Big data analysis with artificial intelligence could enable the detection of sophisticated and cross-financial institution patterns that might be underreported, as they were not properly understood.*"[379]

FATF's recommendations 10-20 and 26[380] encompass the customer due diligence, outsourcing (and therefore reliance on third parties) and reporting of suspicious activities. These recommendations can be successfully integrated or just used as an additional source of know-how and what an internal AML strategy should have and should be able to provide.

All legal provisions and obligations (from the customer due diligence up to the reporting procedures) have to be supported by IT solutions. Otherwise, it would be impossible to detect suspicious financial activities that might be a sign for ML/TF. The reason for this are the amount of transactions and the volumes of the funds transferred yearly in Austria[381]. Therefore, the financial institutions must consider and choose a software solution according to their size and internal risk assessments. This can be done by developing an own custom solution or relying on a third-party software framework or both. There are many aspects that must be considered when choosing the software solutions – functionality of the tool(s), cloud support for storing the data, vendor stability, etc. The discussion which solution is better is out of the scope of this master's thesis. In any case the financial institutions must invest time

[376] *See* section 3.1.6. for more information about the reporting obligations
[377] *Cf.* The Basel Committee on Banking Supervision (BCBS) (1988): Prevention of criminal use of the banking system for the purpose of money-laundering, p. 4
[378] EUROPOL (2017): From Suspicion to Action, p. 24
[379] Ibid., p. 37
[380] *See* FATF (2012): The FATF Recommendations, pp.12-17
[381] *Cf.* Statista (2018): Statistiken zu bargeldlosen Zahlungen in Österreich

and personnel in order to find the best suitable solutions. In recent years, the financial institutions are trying to improve the internal processes by standardizing them internally, expanding their automatic execution and increasing the performance[382]. Since the criminals are improving their knowledge, well-known solutions, like for example the rule-based monitoring systems, are becoming less effective. Some financial institutions are using behaviour-based AML solutions in order to predict suspicious activities and react accordingly[383]. This leads to situations where the banks must use more internal systems, but the bigger the number of the systems, the harder it is to manage and synchronize them[384].

One important aspect in the context of CDD is the customer satisfaction. How far can a particular bank go in order to process the CDD? It is important to find a balance between these two topics which are completely different but at the same time depending on each other. The prevention of money laundering is in its core a process that includes a proper reaction to a so called "Red Flags"[385]. Shortly, "Red Flags" are alarms that ring when specific predefined conditions are met – for example, a money transfer above specific threshold or a money transfer from specific geographical region and so on. In most of the cases the banks are those who decide which actions trigger an alarm, what should happen, which actions should be taken, and when this alarm rings. The problematic aspect in such situation is that the higher the number of red flags, the bigger problems are caused for the customer. This leads to an over-restrictive AML bank strategy which can lead to decreasing number of customers. For example, if a bank decides to define a red flag for every transaction between 1000 EUR and 2000 EUR and the corresponding reaction to such transaction is "block transaction", this may lead to a very high number of unhappy clients. This case is just an example for a simple red flag. In reality the red flags are much more complex and mostly based on customer's behaviour and other factors. In all cases the bank must find the perfect balance and carefully decide which risk is more critical for the institution – the risk of losing clients or the risk of unintentionally ignoring transactions which in reality are part of a ML scheme and which may lead to worse consequences like reputation loss. FATF also sees this as a problem: "*applying an overly cautious approach to AML/CFT safeguards can have the unintended consequence of excluding legitimate businesses and consumers from the formal financial system.*"[386]

In addition to the above four factors or key requirements that every bank at least must assure in order to have a proper AML programme, the factor "AML software" must be also considered. According to The Corporate Executive Board Company (CEB), every AML software solution can be split in four different categories of attributes and features[387]:

[382] *Cf.* Harris (2017): Implementing an effective Anti-Money Laundering System, p. 3
[383] *Cf.* Ibid., p. 4
[384] *See* the interview with Mag. Oliver Floth from 12.06.2018, lines 81-84
[385] S*ee* section 4.3. for more information about the "Red Flags"
[386] FATF (2013): Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion, p. 5
[387] *Cf.* CEB (2013): Anti-Money Laundering: Technology Abstract

1. Detection capabilities

This category includes all features and functionality that support the financial institutions in the identification process and in the prevention of transactions and activities that are designated and assessed with higher risk score. This includes following features:

a. An extendable list of ML types[388]: The software can identify and store the type of ML cases in order to increase its detection and prevention potential of similar cases (self-learning). The list should not be a "black box". Moreover, it should be configurable and extendable by the end-user.
b. Detection of anomalies: The software should be able to distinguish between transactions according to some behavioural indicators. The software should be able to identify and store any suspicious transactions and define patterns based on the findings.
c. Predictive approach: Especially in the case of a new customer the system should be able to predict the behaviour of the customer and detect any suspicious activities. All expectations are based the risk assessment made by the financial institutions.
d. "Cross-Channel"[389]: All features of the application should be applied in the same way when a particular transaction was made via cash, cash-less or via Internet, should make no difference for the software.
e. Transaction details recognition: the application should be able to detect suspicious activities also in multi-language and international financial environment. This means that the software should be able the distinguish between different currencies and different geographical areas.
f. Link Analysis: The application can detect and analyse all relationships between different entities (customers).
g. Risk assessment: the application can provide run-time risk assessment for all transactions and customers based on the provided customer and/or transactional information, predefined risks and processing/business rules. The user should be then able to understand the derived score and how it was derived by the system.

2. Enterprise operation

This category includes features that should support a standardized AML approach across the organisation:

a. Automatic handling of "false alarms": "False alarms" are caused mostly during the screening phase – when the customer is checked, for example, against a sanctions list by the UN or EU. The reason in most cases is insufficient information about the customer and customer's behaviour. Proper automatic handling of "false positives" and "false negatives" could reduce the overall compliance costs.

---

[388] Also called in the literature „*AML Typologies*"; According to the IMF (2011): Anti-Money Laundering/Combating the Financing of Terrorism - Topics: „*In the AML/CFT context, the term "typologies" refers to the various techniques used to launder money or finance terrorism*."

[389] The term "*cross-channels*" comes from the field of marketing and is "*is a practise that integrates the use of all available channels and devices to connect and engage with customers*" (MDirector (2017): What is Cross-Channel Marketing?)

b. Customization: the application can be configured individually for a particular user or group of users in order to provide only the relevant information and functionality
c. Authentication mechanisms: the software can assure high security standards and grant permission and access to functionality and/or data according to the needs of the organisation
d. Interfaces to third-party solutions: the software can be easily integrated in an existing IT landscape with no or at low costs and with no or little configuration effort
e. Workflows functionality: the application provides a subset of features and functionalities, that can be integrated to additional data sources or AML applications. Such features can be (among others) the versioning of documents about cases or standard procedures in case of an alarms or in cases which should be reviewed by the management.

3. User experience

Following features should support a higher user productivity by improving the quality of the used data:

a. Management “Alarms”: The application provides manageable alarms in case of detected ML activity
b. Management “Cases”: The application provides functionality for proper and easy management of cases, documentation and communication about them
c. Management “Reporting”: The application provides broad reporting functionality and support the export of data or the report generation in different export types
d. Management “Transactions”: Any suspicious transaction is automatically prioritized and queued to the proper workflow, according calculated risk score, used service, geographical location, etc.
e. Ease of use: the application is intuitive for the end-user and supports various additional features for better user experience like, for example, reporting dashboard.

4. Vendors’ properties

These are some of the capabilities and properties that every vendor should have. The choice of the vendor and respectively the software solution might have an excellent impact on the financial institution or lead to some worst-case scenario (for example, not properly working AML software solution).

a. Compliance alignment: the vendor is aware of all relevant, new and upcoming regulatory requirements, successfully implements them in its solutions, if needed, and supports the financial institution during external reviews (supervisory audits).
b. Pricing: the vendor provides different pricing models according to the software modules and functionality
c. Deployment: the vendor supports different technical environments and deployment strategies
d. Innovation: the vendor invests actively resources in research and development and align the technological innovations with its product roadmap

e. Stability: the vendor is an established part of the industry and can provide long term partnership to the financial institutions

In 2013 and 2016 CEB highlighted the following software capabilities (among others) that could increase or already support the AML efficiency of the financial institutions[390]:

Technology capability	Technology State (2013) according to CEB	Technology State (2016) according to CEB	ROI Potential (2013) according to CEB
Analytics-Based Detection: technologies based on statistical analysis of the transactions	Partial Adoption	Already broadly used	High
Next Generation Link Analysis: technologies that provide dynamic analytics and network linking	Market-Ready	Market-Ready	Medium/High
Complex Events Processing and Data Lakes: technologies that enable the centralisation of large volumes of data and it's processing ("Big Data")	In Development	Partial Adoption	High
Real-Time Processing: technologies that provide the capability to real-time analysis of transaction and relevant AML activity	In Development	Market-Ready	Medium/High
Anti-Stripping Technology: technologies that detect transfer stripping or manipulations	Partial Adoption	Outdated	Medium/High
Cloud deployment: availability of hosted systems that can help firms optimize current monitoring and alerting systems.	unknown	Partial Adoption	unknown
Real-Time Transaction Monitoring: real-time processing, for both transactional data and payments, rather than scheduled monitoring	unknown	Partial Adoption	unknown

Table 1: AML software capabilities (excerpt)

In a report from 2017 the Financial Conduct Authority in Great Britain highlights the use of new technologies like data analytics and machine learning for the aims of efficient processing of AML activities. However, the authors state that the legislation and regulation are still unable to keep pace

[390] *Cf.* CEB (2013): Anti-Money Laundering: Technology Abstract, p.16

with development and use of these new technologies[391]. In section 4.4. I will present a few AML solutions including their key features.

Based on the research above the following conclusions regarding the used technologies for detection and prevention of ML can be drawn:

- To meet the obligations and duties stated in **§§ 5-6 FM-GwG**, the financial institutions have to ensure a stable IT environment, training sessions for the responsible employees and identify the risks accordingly.
- The banks must carefully define and prioritize the functionality they are expecting from an AML software because not all the vendors offer the same set of features[392].
- Most of the financial institutions "*want to be able to manage everything with one solution*"[393]. Therefore, any dependency on a third-party software vendor should be restricted to a minimum and any incompatibility between different tools should be avoided.
- The employees who will work with the AML application(s) must be able to use it/them easily in order to derive proper analyses and conclusions.
- Cloud based solutions must be considered with the utmost care. The cloud-based solution providers claim that the process of storing and processing data in the cloud can lead to a restructuring in the organisation and the operations. Nevertheless, most of the financial institutions are sceptical about the security features of an AML cloud-based software. The risk of data leaks will always exist if the data is not adequately protected. On the other hand, as mentioned at the beginning of this section the market for AML solutions will keep growing. Many vendors are actively using cloud-based solutions or extending the functionality of their software with cloud-based features. Therefore, the use of cloud-based AML solutions has its advantages and disadvantages that must not be ignored[394].

4.2. Data

In section 4.1. I showed the most properties every AML software solution must have. As every other software solution, it must have some proper input in order to produce adequate and expected or readable output. In section 3.1.4. I described the basic framework of the internal CDD process and in the following section I will show the important role of the above-mentioned input – the data that will be used for processing and analysis. Only to have numerous databases with customer data would not be enough. The data must be prepared well and processed intelligently. Otherwise, undetected suspicious activities may lead to harsh penalties[395]. In the last couple of years, the banks are challenged with an increasing number of regulations and new or updated obligations in the fields of KYC. A study from 2013 by the OECD showed that around 56% of the OECD countries were AML non-compliant in regard to PEP and around 50% were non-compliant regarding the corresponding

[391] *Cf.* Financial Conduct Authority (2017): New technologies and anti-money laundering, p. 11
[392] *Cf.* CEB (2013): Anti-Money Laundering: Technology Abstract, p. 26 and
Cf. CEB (2016): Combatting Rising Threats with Aging Infrastructure, p. 10
[393] CaseWare Analytics (2017): Trying to find the right AML software? Here's what you should consider
[394] *Cf.* Harris (2016): Implementing an effective Anti-Money Laundering System, p. 10
[395] *See* section 2.3. for examples about money laundering and the followed penalties

banking business relationships[396]. The financial institutions are therefore under huge pressure from three different sides – regulatory, moral and internal. The risk of unwished financial consequences because of noncompliance is one of the major reasons for the institutions to apply and use proper AML solutions[397]. Even if a financial institution has met all regulatory obligations, there are still problems using the applied solutions[398]:

1. **Scattered IT infrastructure** may lead to distorted internal communication, incomplete documentation and incorrect risk assessment due to distributed und not centralized monitoring and screening systems and/or
2. **Scattered data**: when an employee wants to analyse a particular customer in more detail (activities, transactions, background, etc.), he/she has to have access and permission to use all relevant data which in many cases is distributed across the organisation. If this is not the case, the result of the analysis would be incomplete and may lead to high "false positives" rates.

When it comes to data management the best-case scenario would be: all data resides in one centralized database, it is highly structured, without duplicates, gathered from different sources, always up-to-date, well secured and with clear identification of the data ownership[399]. In reality it is assumed that some of these data properties are not always fulfilled. Yet, in order to meet the regulatory requirements, the financial institutions have to try to reach high data standards[400]. The process of due diligence is the only way how the banks can have a complete and clear understanding of their customers, their businesses and plans. In order to be able to detect suspicious account activities, the banks must ensure that there will be continuous updates of their customer data. This would allow them to implement behavioural patterns, predict the usage of their services and act accordingly in case of unusual activities. The definition and management of the risks and controls in a bank could be used in the same way to assess, predict and understand the customer needs. Observation of the behaviour would lead to more appropriate behavioural patterns and thus to higher predictability. Peer group analysis or link analysis could not only enhance the profile of a particular customer but also identify and understand his/her needs more properly. The risk assessment on a customer level[401] can be additionally supported by transactions monitoring tools or predictive modelling tools. Thus, the banks would be able to classify their customers or group of customers and decide if a particular business relationship should be continued or not. Yet, all mentioned tasks cannot be successfully done when the used data is either incomplete and/or outdated.

Each transaction is categorized by:

1. Information about the originator (who sends the money?): name, address, account number, bank
2. Information about the beneficiary (who receives the money?): name, account number

---

[396] *Cf.* OECD (2014), Illicit Financial Flows from Developing Countries, p. 33
[397] *Cf.* CEB (2013): Anti-Money Laundering: Technology Abstract, p. 9
[398] *Cf.* Ibid., p. 12
[399] *Cf.* Intra-governmental Group on Geographic Information (IGGI) (2005): The Principles of Good Data Management, pp. 12-14
[400] For example, ISO/TS 8000-1:2011: "*ISO 8000 is the international standard that defines the requirements for quality data, understanding this important standard and how it can be used to measure data quality is an important first step in developing any information quality strategy*" (Benson (2009): Meeting the requirements of ISO 8000, p. 1)
[401] *See* section 3.4.1. for more information about the risk assessment on customer level

3. Information about the transfer (what is sent?): amount, date, additional information (not mandatory)

The analysis of this data can lead to unexpected problems, for example incomplete or faulty data or huge number of transactions. In the following paragraphs I will list some key factors, challenges and recommendations in the context of data management and data processing that are sufficient in order to execute proper and adequate CDD process[402].

1. Enrich the data

The financial institutions are using one or more databases for screening against different sanctions lists (UN sanctions list[403]) or other higher-risk lists (PEP and terrorists lists[404]) provided and kept up-to-date by various vendors. The institutions, however, must implement and develop their own customer lists which include:

1. Database with all STRs ever reported by the bank (internally and externally) in order to eventually make an automatic association with other databases (for example with the PEP list)
2. An interface to other public records, for example police records or court records
3. An interface to real-time market data (in case of legal entity)
4. Database with lost or stolen identification documents of the customers
5. An interface to third-party sources (other financial institutions, insurance companies, lawyers, etc.)

It is important to note that the more data is collected, the easier and more correct the risk assessment is.

2. Higher quality of the data

The quality of the customer data must be also defined as a risk for the enterprise that should be mitigated. Higher quality of data means that the information stored for a particular customer is up-to-date and the customer profile does not need further details in order to assess customer risk correctly. Any missing part of the puzzle could only lead to demotivation for further and deeper case analysis because the employee won't be able to do what he/she is supposed to do. Storing the data in various formats can just decrease the productivity. There should be clear document standards and guideline on how a document from a particular type should look like and what it should contain. Thus, it will be easier and faster to find a particular information rather than lose time and resources dealing with a document mess. The following tasks can help achieving a higher level of data quality:

- A knowledge centre and sharing policy: all relevant data should be accessible and readable for most of the responsible employees. The data responsibility should be transparent.

[402] *Cf.* Bedi (2010): The Future of AML/CFT – Technology, Data, People, pp. 17-18 and
Cf. U.S. Congress, Office of Technology Assessment (1995): Information Technologies for the Control of Money Laundering, pp. 63-69 and
Cf. NICE Actimize (2017): Customer Due Diligence (CDD) Market Survey, pp. 12-14

[403] *See* UN (2018): Consolidated United Nations Security Council Sanctions List

[404] *See* Thomson Reuters (2018): About World-Check

- An organisation specific data model could support the mapping between transactions, accounts, customers and businesses. Permission policy and predefined access rights would increase the security around the data
- Dynamic checks for already existing data will decrease the duplicates in the system
- Appropriate escalation process in case of missing or faulty data
- Supporting and understanding various data types, for example geographical coordinates
- Establish an internal translation and verification process in case of non-translated documents in foreign language documents

3. Intelligent use of intelligence (Big Data)

It can be assumed that every financial institution has access to huge amounts of data. On the one hand, this may seem to be helpful with the potential investigation. On the other hand, it makes the intelligent use of this data really challenging. "Big Data" is a term or field mostly related to large and complex amounts of data. It can be a logistical nightmare to manipulate or manage it properly. In in the context of AML, especially CDD, a single transaction is meaningless. The analysis of such transaction requires additional data from numerous data sources ("*contextualization*"[405]). A million transactions lead to a mountain of information that must be analyzed in order to identify trends, patterns and associations. Therefore, the computational analysis of such amount of data is essential for the successful ML analysis process. Europol states that "*the traditional model for detecting suspect financial flows is based on screening for pre-defined risk scenarios could lead to the problem that 'we don't know what we don't know', and more so that we don't know what risk scenarios look like for emerging products and services.*"[406]

Also: "*Proponents of new analytical approaches believe that data-driven big data analytics hold the key to shifting towards a more effective intelligence-driven approach towards anti-money laundering and counter terrorist financing.*"[407]

4. Incomplete or faulty data

Every bank transfer contains few mandatory fields and several non-mandatory fields that can be left blank. If every field is being filled out, the transaction will be more detailed and thus more understandable for the banks. There are cases, for example an anonymous donation, when the identification of the originator is unknown. And there are cases when the individual clients or organisation is giving false or misleading information. Another typical example is the ordering of a transfer full of mistakes or typographic errors. In such a case the transfer cannot be executed and is returned to the originator. This can lead to complicated internal procedure and "*wrong analysis schemes that assume each transfer of funds is only associated with a single wire transfer record*"[408].

---

[405] Merriam-Webster (2018): "*contextualization*"
[406] EUROPOL (2017): From Suspicion to Action, p. 37
[407] Ibid., p. 37
[408] U.S. Congress, Office of Technology Assessment (1995): Information Technologies for the Control of Money Laundering, p. 79

Another problem may occur with the different variations of individuals or company names or addresses. For example, the company "A.B.C." GmbH is an abbreviation for "Accounting, Business and Consulting" GmbH. But so could be ABC GmbH or "Firma ABC GmbH", etc. –the same company is meant in both cases, but it is just written differently. To make the situation more complex: the company has five branches on five different addresses (worldwide). The company operates four accounts in three different banks. This could lead to wrong associations "transfer → company" and make the identification of transfers more difficult.

5. Labelling problem

The time frame between a reported suspicious activity and the final conclusion made during an investigation and leading to particular suspects may take years. It is equally difficult only by looking at a transfer's details to conclude that the funds are with a licit or illicit origin or to label the transfer as suspicious. "*Even if criminal prosecution records were carefully matched with wire transfers, it is unlikely that concluded cases would identify all, or even most, of the records that were actually involved with money laundering.*"[409] The law enforcement authorities may obviously detect and catch only those money launderers that are "*incompetent*"[410]. The "self-revealing" characteristic is something unusual for money launderers. The investigators can make conclusions based on previous experience from ML schemes which are already known. Therefore, many ML techniques and schemes could stay undetected for years.

The following case is a good example of the labelling problem that decreases the potential success of the data analysis for developing ML profiles:

"*Suppose a set of data is labelled so that each known case of money laundering is used as a positive example and all the remaining cases are used as negative examples. The negative examples almost certainly contain undetected cases of money laundering, perhaps representing as many (or more) cases than are being used as positive examples. If these data are used to derive profiles of money laundering, the profiles will be "trained" to ignore negative examples - even though they may, in truth, involve money laundering. The resulting profiles will faithfully profile known money laundering schemes, rather than detect new ones."*[411]

6. Third-party data

Third-party data is sometimes the missing part of the puzzle called "customer profile". In the last few years the social networks became a massive part of our lives and also are an enormous source of personal information. The information most of the people are sharing, sometimes unintentionally, can only enrich the information about particular customer and help understand his/her needs more accurately.

Large bank holdings with millions of customers and thousands of branches worldwide have of course big challenges in the context of data collection and processing and it does matter which AML software

[409] Ibid., p. 68
[410] Ibid., p. 68
[411] Ibid., p. 68

is used in the organisation. Nevertheless, the application may be a leader on the market but when the input is faulty one cannot expect that the output will be satisfactory. The last major aspect in the combat against ML is the human factor that will be presented in the next section.

4.3. People

In Austria the analysis of suspicious activity happens internally in the financial institutions itself. If the financial institution concludes that there might be a case of a fraud or money laundering, they contact the corresponding authorities. Therefore, the internal analysis must be done in time and in quality. This means that every unusual transaction should be detected automatically for example by an AML software or by an employee directly and then reported to the responsible person from the AML internal office. The time frame between the detection and internal reporting should be minimal. In most of the cases the analyst does not know anything about the type of the criminal activity that led to the suspicious transaction of the customer – this should not be the case[412]. Therefore, the subsequent analysis must be done according to the internal bank's procedures and standards, communicated and documented properly. Only then the suspicious activity report can gain quality and could help the law enforcement authorities to speed up the further analysis. In such constellation the first stage of investigation (in-house) must be properly done, so that the second stage (FIU) can be proceed well. The combat against ML can be then seen as a relay that requires more than teamwork. In this section I will focus on the role of the AML Officer (according to **§ 23 FM-GwG**) and the challenges that AML employees could face. In addition, I will give few recommendations (split in four categories) that may be helpful to improve the internal processing of unusual account activities. It is important to mention that the following categorisation is based on literature research and assumptions only and they were not officially confirmed, corrected or commented by any AML/Compliance officer with the appropriate experience.

1. The role of the AML Officer

"An adequate AML program costs money, which management may be reluctant to spend. The AML officer's challenge is to convince management that, while an AML program may cost money, it is an indispensable expense to protect the institution and to avert legal problems and reputational harm for the institution."[413]

In Austria the role of the AML Officer is regulated in **§ 23 FM-GwG**. The financial institutions are obliged to appoint an officer whose main task is to ensure the compliance with the due diligence provisions of the FM-GwG. The Officer is an integral part of the organisation and directly responsible to the management board (or managing directors, in short management). The reporting to the management must happen directly and without intermediate levels. The financial institutions must ensure that the duties and responsibilities of the Officer can be fulfilled at any time. The Officer should have full access to all kinds of information, data, records and systems, related to a (A)ML activity.

[412] *Cf.* Fiedler/Krumma/Zanconato/McCarthy/Reh (2017): Das Geldwäscherisiko verschiedener Glücksspielarten, p. 13
[413] Association of Certified Anti-Money Laundering Specialists (ACAMS) (2012): Study Guide for the CAMS Certification Examination, p. 207

The following list represents some of the core functions of the AML Officer[414]:

- Perform verification tasks
- Block transactions or accounts
- Terminate existing business relationships or reject new business relationships
- Define initiatives and review them regularly (strategies, processes, IT systems) in order to guarantee that the due diligence (simplified and enhanced) and reporting obligations are met
- Provide documentation, instructions, manual on how to detect and prevent ML activities
- Analyse and follow-up of unusual behaviour resulting from ongoing monitoring of the business relationships
- Report suspicious transactions according to **§ 16 FM-GwG**
- Be the internal and external "Single-point-of-contact" for questions related to the combat against ML
- Establish an internal reporting procedure in order to report regularly or ad-hoc to the management board
- Organise trainings for existing employees

2. Everyday activities

a. "Follow the white rabbit"[415]

Every financial transaction is potentially a case of money laundering. Yet, nobody can definitively classify it as such without knowing its history, context and purpose. The result of the everyday work of the bankers who are responsible for the monitoring and observing of the transactions could be described as unpredictable because of the analysis results of the AML software, following which the employee must react accordingly. Basically, the bankers must look for "red flags". "Red flags" is a non-all-inclusive list of suspicious activities that may help employees recognize ML schemes. Since the financial institutions in Austria should analyse all suspicious behaviour by themselves and in case of confirmation report it the FIU, the employee must be experienced and has to follow the internal procedures strictly. The "Red Flags" could be categorized as follows:

- Unusual transactions
  - Large cash transactions or transactions which are in incompatible with the customer's financial standing
- Irregular account movement
- Suspicious behaviour/habits
- Dealing with high risk jurisdictions
- Suspicious behaviour of employees of the financial institution

In the last few years the FATF, the OECD and the UNODC published comprehensive lists with various red flags, case studies and best practices in this context[416].

---

[414] *Cf.* Finanzmarktaufsichtsbehörde (FMA) (2012): FMA Circular on the Anti-Money Laundering Officer, pp. 6-8

[415] The White Rabbit is a fictional character in Lewis Carroll's book Alice's Adventures in Wonderland. The phrase "Follow the white rabbit" means to follow an idea or a concept which may lead to an unknown place, to be curious, to want to discovery the unknown

[416] *See* FATF (2013): Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, pp. 77-82 and *See* OECD (2009): Money Laundering Awareness: Handbook for Tax Examiners and Tax Auditors, pp. 31-48 and

b. Research

Every person, including criminals, who is interested, has access to information about ML including regulations, methodologies, techniques, history, cases, detection and prevention software, etc. The question would therefore be who has the advantage of this amount of information – the money launderers, the employees who are in the forefront of the combat against ML, the FIUs? In order to be one step ahead and to at least try to predict ML through his/her organisation the employee has the responsibility and maybe the obligation to inform him-/herself about forthcoming legislative changes (for example the implementation of an EU directive) or about new technological developments, etc. By doing this it will be easier to predict future changes in the internal structure and processes and understand the capabilities of the technologies, like for example AI-based ML detection.

c. Gain know-how from the "bad guys"

In the context of ML, usually the financial institutions are defending themselves against the money launderers. It is the banks that must adapt and consider what ML techniques, methodologies and technologies the criminals use. This kind of "re-action" to the events (instead of "pro-action") may be a good (or the only) defensive tactic against ML. But knowledge can be gathered before it's too late. If a financial institution hires professionals who have been previously involved in illegal activities, including ML, this could help the bank build up stronger defence, to fill the eventual gaps in their strategies and counter-measures. Such approach could be helpful for the bank, at least in the short-term.

d. Skills

A single employee cannot combine all relevant skills to become a mastermind in the field of AML. Yet, the financial crime experts must be tech-savvy and business-oriented in order to execute his/her tasks efficiently. For example, they need to understand the various types of transaction monitoring system, know what they are capable of, and what their advantages and disadvantages are. Thus, they would be able to explain and analyse particular behaviour or activity patterns or they must be otherwise experts in the field of international sanctions and/or embargoes. A particular employee can focus only on the governance function in order to establish an institution-wide A ML standard and policy, while another one on the internal organisation and trainings[417]. The following list summarizes a few key abilities of an AML expert that could be crucial for the internal AML processing. An AML specialist:

- should have appropriate analytical skills in order to manage and analyse several data sources
- should be able to develop and understand statistical analysis
- should have comprehensive knowledge about the internal processes, risk and controls, in order to be able to assess them and propose risk mitigation strategies
- should have knowledge about the used software in order to assess its advantages and disadvantages

See UNODC (2010): Risk of Money Laundering through Financial Instruments

[417] *See* the interview with Mag. Oliver Floth from 12.06.2018, lines 32-51

3. Internal organisation

a. Avoid communication or activity loops

Avoiding loops is a goal in every organisation not only in the financial institutions. The more steps are included in an internal process, the higher the risks of misunderstanding in the communication are, such as repetitive execution of the same activity, when it is unnecessary, loss of time and money, both valuable resources. All internal processes should be reviewed regularly not only following a regulatory change but also in order to avoid the above constellations.

b. Establish an escalation path

Time is critical for every execution of an internal process. This means that unnecessary loss of time should be avoided. In case of suspicious account activity, the financial institution must ensure proper escalation plans in order to start the internal analysis as soon as possible. Some unplanned circumstances (sickness, holidays, weekends) cannot be avoided but the proper reaction to them must be defined (like delegation of responsibilities, cases, customers or definition of deputies).

c. Switching responsibilities

Another important aspect is the concentration of particular responsibilities on one employee. For example, a particular employee is responsible for high risk customer monitoring only, while another one is responsible for customers from the U.S. Switching the responsibilities between the employees could lead to increasing the quality of the analyses because over time the attention and motivation of the employee may decrease.

d. Trainings

According to **§ 23 FM-GwG** the financial institutions are obliged to train their employees. In a market survey from 2015 44% percent of respondents chose the training programs for existing employees as a top goal among the operational priorities: "*Investment in training staff on existing programs can help institutions ensure that they are maintaining and encouraging a culture of compliance throughout the institution, preventing regulatory fines and sanctions.*"[418]

With the latest regulation changes and the increased focus in the AML/CTF activities the skill set which is required by the financial institutions is transforming. Mostly, the expectation of the financial institutions is that the compliance employees are multi-skilled, including having a technological background. However, it is believed that the balance between a highly skilled risk manager and an IT specialist is not found. The reason for this is the significant effort that must be invested by the employees in order to stay up-to-date with the new technological developments. That is why it is important to support the employees in their further technological development with a focus on problems that may occur when using a particular technology[419].

[418] NICE Actimize (2017): Customer Due Diligence (CDD) Market Survey, p. 10
[419] *Cf.* Bedi (2010): The Future of AML/CFT – Technology, Data, People, p. 4

4.4. AML solutions landscape

Since 9/11 the focus on compliance has increased. Thus, the financial institutions are investing resources more than ever in order to implement and manage new regulatory obligations. For example, between 2007 and 2013 the compliance costs of the six largest US banks doubled (from USD 34.7 billion to USD 70.1 billion). At the same time the non-compliance of several banks led to huge financial penalties. Only in 2013 and 2014 the banks paid approximately USD 15 billion USD penalties due to violations of the AML policy[420].

The process of AML compliance is complex and is triggered at the time of customer onboarding. It monitors the ongoing customer activity (cash and non-cash transactions) and supports the reporting of suspicious transaction to the domestic FIU. The following figure shows an abstract view over the typical AML components and functions, some of them already discussed in chapter 3, and how they are or could be triggered (for example, the establishment of a new business relationship triggers a customer risk assessment procedure).

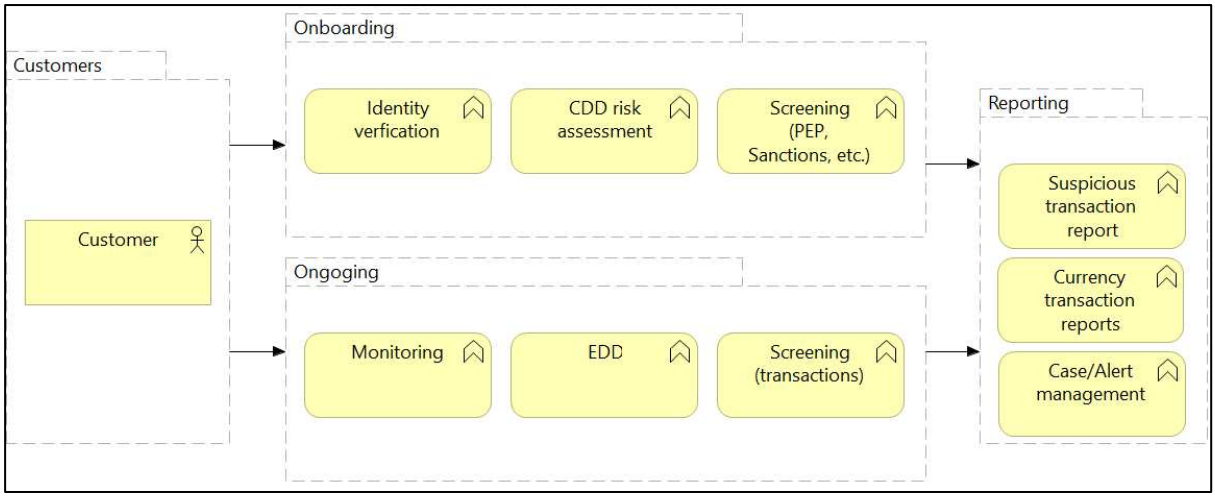

Figure 4 AML core components

The AML solutions and implementations are complex. They provide various features and functionality in the field of ML detection. Beside the standard features that almost all software solutions have different vendors are offering additional features in order to differentiate from their competitors[421].

The following table represents some of the software solutions on the current market. This overview has not the aim to evaluate the advantages or disadvantages of a particular solution but to show what he current trends in the AML software development are. I selected the software vendors based on market surveys by KPMG[422], CEB[423] and Aite Group[424]. As discussed in section 4.1., in order to detect, prevent and handle the cases of ML the financial institutions have to be able to automatically monitor the transactions, screen their customers (against sanctions and other lists), do a comprehensive risk assessment, etc. Most of the current solutions on the market provide such and other capabilities. The biggest challenges are the automation of the internal processes, the use of AI

[420] CEB (2016)
[421] Cf. Aite Group (2015): Global AML Vendor Evaluation: Managing Rapidly Escalating Risk, pp. 21-22
[422] *See* KPMG (2014): Global Anti-Money Laundering Survey
[423] *See* CEB (2013): Anti-Money Laundering: Technology Abstract
[424] *See* Aite Group (2015): Global AML Vendor Evaluation: Managing Rapidly Escalating Risk

and machine learning for deeper and detailed analysis of the customer data, the proper and useful mining of the collected data and not in the last place – the fulfilment of the legal obligations and ensuring compliant internal processes.

ESAs (The Joint Committee of the three European Supervisory Authorities EBA, EIOPA and ESMA) states that "*innovations and technological developments in financial services can potentially improve the efficiency and robustness of these services while also presenting many other benefits to firms and their customers.*"[425], however "*the firms and competent authorities need to be aware not only of the benefits but also of the risks and challenges presented by these innovative solutions. It is important that firms can demonstrate to their competent authorities that they have identified, assessed and mitigated all relevant risks before introducing the innovative solution in their CDD process*"[426].

This means that no matter how good a solution from a particular vendor is on the market it won't be integrated by the financial institutions if they are unable to prove that through this particular software they still can fulfil their legal obligations (e.g. to mitigate the identified risks). Such process could cost a lot of time and resources.

Company	Features of the AML software (among others)
Oracle	• Watch list screening • Currency transaction reporting • AML and fraud analytics • Enterprise case management • Regulatory reporting • KYC/AML module
SAS	• Predictive alert analytics • Peer-group analysis • Sanctions monitoring • AML transaction monitoring
NICE Actimize	• Suspicious activity monitoring (SAM) • Watch list filtering (WLF) • CDD • Currency transaction reporting
BAE Systems	• KYC/CDD module • Sanctions/PEP screening • Transaction filtering and monitoring • Correspondent banking module

[425] The Joint Committee of the three European Supervisory Authorities (EBA, EIOPA and ESMA) (ESAs) (2018): Opinion on the use of innovative solutions in the customer due diligence process, p. 18
[426] Ibid., p. 18

	• STR module
Tonbeller	• AML/KYC • Fraud prevention and detection • Prevention of market abuse • Business-partner due diligence
Verafin	• Behavioural analytics • Ongoing customer risk rating • Predictive analytics

Table 2: Features of selected AML software solutions (excerpt)

Which software product to use depends mostly on the size of the financial institutions, its risk assessment, business strategy, the number of customers and the number of transactions.

Here it is important to mention the software product called goAML[427]. It is developed by the UNODC to help the FIUs in their analysis. Some of the features provided by goAML are (among others): statistical reports, intelligence report writer, rule-based analysis and document management.

As one can see, all solutions listed above offer a numerous set of features and innovative solutions. However, the banks must consider the use of an external software solution very carefully, as discussed in section 4.1.

4.5. Summary

The financial institutions rely on IT in order to ensure the integrity and stability of their systems. Research shows that in the context of AML a consolidated control framework is needed like COSO and/or COBIT and/or combination of both. COSO is seen as a highly abstract framework and focuses mainly on the financial reporting task, while COBIT concerns the management and control of IT-related systems. By mapping the corresponding COBIT process to the COSO framework it could be possible to establish a framework for goals of AML in the financial institutions[428].

At the beginning of this master's thesis I presented the first research question:

RQ1: Is there a correlation between a bank's internal competences (organizational structure, IT, know-how) and the number of Suspicious Transaction reports (STRs) classified as "money laundering" reported by this bank?

The answer is "**most probably no**". Every financial institution in Austria fulfils its regulatory obligations according to the corresponding legislative basis. From that moment on every bank monitors and analyses the transactions and customers in its own way. Almost every bank has a different business strategy, different number of customers and customer types and segments. Therefore, it may be impossible to find a direct correlation between particular internal factors and the number of reported STRs. For example, the use of a certain AML software products or solutions cannot be identified as the key factor for the increase of detection rate of suspicious activities. A new IT System may and has the goal to decrease the number of "false positives" but in most of the cases the number of STRs

[427] goAML - a UNODC software (homepage: https://http://goaml.unodc.org/)
[428] Pramod/Li/Gao (2012): A framework for preventing money laundering in banks, p. 1

reported to the FIUs stays relatively the same[429]. The other identified factors such as internal processing and organizational structure are also essential for the proper analysis of suspicious activities. Yet, due to the fact that organizational structures and internal processes are adapted when needed, it can be only assumed and cannot be concluded how particular organizational structure or particular internal processes have a direct impact on the number of STRs. To find a correlation one may simplify the question, for example, if there is a connection between the reported STR concerning particular customer types (e.g. offshore-customers) and the risk-assessment for this customer type, or if there is a relation between the STRs concerning international customers only and the knowledge and expertise provided by the AML experts or the account managers responsible for these customers. Thus, the generalization "internal factors" is in this case not appropriate.

While writing this master's thesis I sent questionnaires regarding the internal AML policy covering the period 2015-2017 to eight AML- and Compliance-Officers from different Austrian banks. The aim of the questionnaire was to find out if there is any objective reason for a possible increase or decrease of the number of STRs. Only three of the respondents filled out the questionnaire. The following tables summarize the results from the filled questionnaires. One can see that due to the low number of filled questionnaires and missing information it is hardly possible to conclude objectively any general relation between the mentioned factors and the number of STRs and therefore, any generalization or even a statistical analysis is impossible without cooperation of the financial institutions. Thus, it is hard to conclude what the banks are doing well and what not. **Bank A and Bank C** replaced in 2017 the internal core AML software solution and thus the number of alarms increased (from approximately 2400 in 2016 to 7240 in 2017 for **Bank A** and from 1267 in 2016 to 2982 in 2017 for **Bank C**). Since the number of STRs in 2017 compared to 2016 increased by 2 (**Bank A**) and by 1 (**Bank C**) ("Number of forwarded cases"), a (still) not well calibrated transaction and customer monitoring could be the reason for the higher number of alarms ("Detected suspicious/unusual activity ") and thus higher number of "false positives" ("false negatives" respectively). **Bank B** has less transactions (on a yearly basis) ("Number of transactions yearly") but more employees responsible for the internal AML policy than **Bank A** ("Number of employees Compliance/KYC/AML"). On the other hand, **Bank C** has the highest number of transactions and the highest number of AML employees. For **Bank B** it is unknown how many alarms or STRs were generated in the period 2015-2017, therefore it is impossible to make any assumptions. One can see that the employee training efforts of **Bank B** and **Bank C** are high (in 2017 there were on an average 16 internal AML/CTF trainings at both banks). It is interesting to mention that **Bank A** and **Bank B** (but not Bank C) rely on third-party software, companies, solutions or experts in order to carry out some of their AML functions ("The institution employs third parties to carry out some of the AML functions")**.** The outsourcing of functions itself is not surprising but is currently unknown what exactly is being outsourced and if this outsourcing affects the internal analysis of suspicious activities and thus the number of generated STRs. It is also interesting that **Bank A** did not know by the time the questionnaire was filled what the current status of the sent STRs is. **Bank B**, however, knows exactly that in none of the STR cases a ML case has been confirmed by A-FIU ("Number of fraud/ML cases confirmed").

[429] *See* the interview with Mag. Oliver Floth from 12.06.2018, lines 1-9

Bank A

Year	2015	2016	2017	2018
Number of employees Compliance/KYC/AML	2,5	2,5	2,5	-
Number of transactions yearly	n.a.	> 35 m	> 36 m	-
Number of used AML software solutions or solutions supporting the AML process	3	3	3	-
Detected suspicious/unusual activity	1962	2431	7240	-
Number of forwarded cases	28	16	18	-
Screening of the customer database	-	-	-	daily
Business relationships with offshore banks, internet banking-based institutions or banks located in high risk areas as highlighted by the FATF	-	-	-	no
The institution employs third parties to carry out some of the AML functions	-	-	-	yes
Number of fraud/ML cases confirmed	n.a.	n.a.	-	-
Number of trainings	1	1	-	-
Key changes or events in the internal AML policy	no changes	no changes	Replacement of the used AML core system	-

Table 3: Summary from filled questionnaire "Bank A"

Bank B

Year	2015	2016	2017	2018
Number of employees Compliance/KYC/AML	4	5	5	-
Number of transactions yearly	approx. 24 m	approx. 25 m	approx. 23 m	-
Number of used AML software solutions or solutions supporting the AML process	6	6	6	-
Detected suspicious/unusual activity	n.a.	n.a.	n.a.	-
Number of forwarded cases	n.a.	n.a.	n.a.	-
Screening of the customer database	-	-	-	daily
Business relationships with offshore banks, internet banking-based institutions or banks located in high risk areas as highlighted by the FATF	-	-	-	no
The institution employs third parties to carry out some of the AML functions	-	-	-	yes
Number of fraud/ML cases confirmed	0	0	0	-
Number of trainings	9	5	15	-
Key changes or events in the internal AML policy	no changes	no changes	New set-up of the risk-model and risk analysis	-

Table 4: Summary from filled questionnaire "Bank B"

Bank C

Year	2015	2016	2017	2018
Number of employees Compliance/KYC/AML	21	24	24	-
Number of transactions yearly	approx. 50 m	approx. 51 m	approx. 59 m	-
Number of used AML software solutions or solutions supporting the AML process	8	8	8	-
Detected suspicious/unusual activity	1163	1267	2982	-
Number of forwarded cases	17	5	6	-
Screening of the customer database	-	-	-	daily
Business relationships with offshore banks, internet banking-based institutions or banks located in high risk areas as highlighted by the FATF	-	-	-	no
The institution employs third parties to carry out some of the AML functions	-	-	-	no
Number of fraud/ML cases confirmed	n.a.	n.a.	n.a.	-
Number of trainings	9	12	17	-
Key changes or events in the internal AML policy	among others: • Definition of new internal processes for customer identification • Reduced due diligence in particular cases	among others: • Outsourcing of AML activities • Implementation of the new rules regarding foreign and domestic PEP • Integration of CRS (Common Reporting Standard)	among others: • Change of the used AML tool • Increased focus on defence against terrorist financing	-

Table 5: Summary from filled questionnaire "Bank C"

chapter 5

CDD reference model

As shown previously the KYC-process is essential for every financial institution. As an integrated part of it the CIP-program represents the very first step of the process when the bank collects and documents the customer's basic information (name, address, date of birth). Right after that the CDD-program is initialised. CDD helps the institution in the verification and risk assessment of the customer. In case of a customer with higher risk score, an EDD is enabled. Every bank defines the CDD and EDD steps on their own and depends on the risk assessment on the company level made by the bank itself. A small branch in a small village in Lower Austria has with high probability a lower risk profile than a bank operating in Vienna. To fulfil their CDD (and eventually the EDD) obligations and deliver appropriate customer analysis the banks have to have access to reliable, up-to-date information about the customer, his/her account behaviour (withdrawals, cash and non-cash transactions, geographical aspects, etc.). With the collected information the bank can classify their customers into categories, distinguish them by customer type, business type, transaction volumes, operating countries etc. This process creates the customer profile. The activity of the customer (and its profile) is being constantly measured – mostly automatically by an appropriate AML software, using different techniques, from statistics up to AI. It may sound like an easy process but the steps in every CDD (and eventually EDD) process are resource-intensive and must be executed properly. Otherwise, a missed detail can lead to an unreported activity and in a worst-case scenario to an (internally) undetected ML scheme and penalties for the financial institution.

In this chapter I will show some best-practices in the context of CDD found during the literature research. In addition, I will show a short overview over the AML software market. Finally, after a short introduction in the fields of "*reference modelling*" and "*Enterprise architecture*" I will summarise the findings concerning the CDD/EDD-process made in chapters 3. and 4 and together with the expert interviews made I will give a proposal for a CDD reference model. Thus, I will give an answer to the second research question introduced at the beginning of this thesis.

5.1. CDD practices

As stated in section 4.1. a good AML programme depends on previous experience. Even if the financial institutions implement their programmes appropriately, haven't been sanctioned, have an excellent risk assessment process and fulfil their AML obligation, they could still be misused for the

goals of money laundering. Most of the disclosed ML cases from last few years show that organised crime is still able to exploit successfully the products and services – even if a particular bank has an excellent AML reputation and/or AML policy. In some of the cases the financial institutions did know about the misuse of their services and actively collaborated with the FIU, while others, with the aid from their employees, actively participated in the ML schemes[430]. In both cases at the end the financial institutions are those which are sanctioned by the authorities and those who have to re-act accordingly, so the risk of future ML cases can be mitigated. That is why it is easy just to list a couple of recommendations and guidelines based on previous experience. Under the assumption that most of the financial institutions Austrian-wide have never ever be sanctioned because of a weak or faulty AML policy, the challenge is to give recommendations for an AML policy even better than the current one.

In this section I will give a list of several key categories of "good" and "poor" practices that might increase or decrease respectively the quality of the internal AML policy. In the first place, the financial institutions are those which must implement an adequate ML defence strategy. That is why it is up to the bank to prioritise and conduct this task accordingly.

Risk assessment	
Good practice	Poor practice

• The risk assessment made by the financial institution:
  ○ is comprehensively documented and regularly reviewed (internally and externally)
  ○ weights the identified risk factors in accordance with the business strategy, size, customers, products and services of the financial institution
• The assessment and decision for each transaction is historically available and can be easily linked to a customer profile and other relevant transactions
• The responsible persons for the risk evaluation are known, experienced and trained employees
	• The customer risks assessment is not kept under regular review
	• Emerging risks concerning money laundering are not considered
	• The focus of the customer risk assessment falls on the reputational risk only without considering the financial crime risk
	• The customers' use of the financial products and services is not considered during the risk assessment of a customer

Governance	
Good practice	Poor practice
• The organisational structure, responsible roles and responsibilities itself in the financial institution are documented, regularly reviewed and transparent	• There is a lack of internal communication, reviews and audits regarding the internal risk assessment strategy • The organizational structure and culture make the internal sharing of relevant information and knowledge complicated

[430] see the examples provided in section 3.1.7, "The role of the Financial Intelligence Unit"

AML/Due diligence	
Good practice	Poor practice
• The employees are required to consider ML risks related to the business strategy, customers and products of the financial institution • The internal operative procedures and guidelines regarding CDD are documented, regularly reviewed and transparent • The internal operative procedures and guidelines regarding high risk customers are documented, regularly reviewed and transparent • Escalation paths in order to trigger an internal investigation and internal/external reporting process are available, regularly reviewed and transparent • There exists a collaboration between different organisational structures in regard to the customer risk assessment and CDD • The generated customer profiles are regularly updated and reviewed by the responsible account managers • Data sources (internal white, internal black lists) are regularly reviewed and if needed renewed • Reliable third-party data sources are used, if and when possible • The list with "Red Flags" is regularly reviewed and updated, when needed • The handling of the alerts and hits by the transaction activity monitoring and other alert systems is predefined and the processing of the alerts is prioritised • Regular review of activities made in the past: customer/transaction risk assessments, escalations, internal investigations, generated STRs • Regular external review of the internal current AML policy, independent from the supervisory authorities	• Missing documentation regarding the internal risk assessment procedures regarding customers and/or transactions • Misunderstanding of the potential ML risks in regard of customers, products, services • Unable to assess the risk of ML of the transactions • Missing documentation and information about the decision for a certain "false positive" or screening match • Customer due diligence processes and procedures are the only possibility to assess and mitigate the risk of ML of certain transaction • Missing documentation regarding internal escalation procedures for potentially suspicious transactions • Internal trainings are the only source of knowledge regarding the escalation of certain transactions without the establishment of additional internal processes or controls • Unable to investigate suspicious customer behaviour and/or transactions due to lack of expertise, time or pressure from the management • Sanctions and embargoes lists are the only sources for screening of the customers • Collected knowledge concerning suspicious ML cases from the past cannot be shared or used for transactions monitoring or internal investigations
Knowledge/Trainings	
Good practice	Poor practice
• Expert training especially developed for the particular needs of the different employees depending on their field of activity (processing and analysis of alerts, sanctions and embargoes, etc.) • Regular internal meetings and workshops regarding current situation and future	• Generic trainings for all AML employees without taking into account new emerging ML risks, new technologies or legislative changes • Internal organization is unbalanced, e.g. inexperienced or not qualified staff is not actively supported by experienced colleagues

expectations in the context of new emerging ML risks and/or legislative changes • The review of the internal processes and staff assessment is done by employees with the appropriate knowledge • The AML employees have the possibility to attend international conferences, workshops and external trainings in order to gain more knowledge, depending on their field of activity	• Inability to ensure a common understanding of the ML risks • Mere definition of "Red Flags" without regular review and/or update • Inability to encourage the AML employees to communicate, share and store information regarding suspicious transactions, emerging ML risks, new technologies or legislative changes

Table 6: Examples for "good" and "poor" AML policy practices

5.2. Reference models: definition, methodologies and purpose

The term "*reference model*" does not have one strict, general or enveloped definition. In its semantics the term can be split in two parts: it can be derived from the definition for a "*model*" and then – it can address the characteristics of what is being referenced. Thus, a "*reference model*" has to address on the one hand a framework (for example, ISO/OSI reference model[431]) and on the other hand the role of reference model in an enterprise modelling (for example, SAP R/3[432]). A "*reference model*" can be seen "*as a starting point for the development of a concrete model*"[433] or as "*model that provides a recognized good solution to a common problem. The reference model serves as a point of reference for possible further developments of a concrete model that maps similar problem areas.*"[434]. Schütte concretizes the term "*reference model*" in the context of enterprise modelling: "*In practice, reference information models, abbreviated as reference models, play an important role. They represent universally valid representations of knowledge. After the adaptation of the reference model, their purpose is to be used in an individual context*"[435] and Schmalzl provides a general definition of the term in the context of a modelling framework and application for enterprise modelling: "*Using*

[431] "ISO/OSI reference model" is a seven-layer networking model developed by the "International Standards Organization" (ISO, https://www.iso.org/). It was introduced in 1978 as the "ISO Open Systems Interconnection (OSI) Reference model", it describes networking as "*a series of protocol layers with a specific set of functions allocated to each layer. Each layer offers specific services to higher layers while shielding these layers from the details of how the services are implemented. A well-defined interface between each pair of adjacent layers defines the services offered by the lower layer to the higher one and how those services are accessed*." (Microsoft (2017): Windows Network Architecture and the OSI Model)

[432] "SAP R/3" is the former name of the enterprise resource planning software produced by the German corporation SAP SE (https://www.sap.com). It is an enterprise-wide information system designed to coordinate all the resources, information, and activities needed to complete business processes such as order fulfillment, billing, human resource management, and production planning. The "R" stays for "Real-time data processing" and "3" stays for "3-tier": 1) database, 2) application server, and 3) client (GUI)

[433] Scheer (1999): ARIS – House of Business Engineering: Konzept zur Beschreibung und Ausführung von Referenzmodellen, p. 6, translated from German: "*Ausgangspunkt für die Entwicklung konkreter Modelle [...]*"

[434] Hansen/Mendling/Neumann (2015): Wirtschaftsinformatik, p. 92, translated from German: „*Ein Referenzmodell ist ein Modell, das eine anerkannte gute Lösung für ein häufig ausgetretenes Problem bietet. Das Referenzmodell dient als Bezugspunkt für mögliche Weiterentwicklungen eines konkreten Modells, das ähnliche Problembereiche abbildet.*"

[435] Schütte (1998): Referenzmodellierung: Anforderungen der Praxis und methodische Konzepte, p. 64, translated from German: "*In der betrieblichen Praxis nehmen Referenzinformationsmodelle, die verkürzt als Referenzmodelle bezeichnet werden, einen hohen Stellenwert ein. Sie stellen allgemeingültige Repräsentationen von Wissen dar. Sie verfolgen den Zweck, nach der Adaption des Referenzmodells in einem individuellen Kontext eingesetzt werden zu können.*"

characteristic properties, a situation and its valid forms are generally described in a reference model. Reference models obtain their special value when, with knowledge of the influencing parameters and general conditions, not only concrete characteristics are derived from them, but the reference model can also serve as a comparative value for the different end products"[436].

Reference models can be classified into two types[437]: industry-specific and class-specific. The first type includes for example procedure reference models or software-specific reference models. Procedure reference models, also called phase models, can be seen as a pattern or guideline for describing a development-process including key indicators for the objectives and their fulfilment. Procedure reference models can be found mostly in the fields of software engineering[438] and business process reengineering[439]. An example for such a model is the Waterfall model[440]. Software-specific reference models, also called reference application system models, represent all operational processes in an enterprise which are supported by the use of integrated software systems. SAP R/3 and Oracle Utility Reference Model [441] can be seen as software-specific reference models.

The definition of a reference model according to Schütte considers the task of a reference information model and sums up the company and project aspects in order to develop recommendations based on these aspects:

"*A reference information model is the result […] of a modeler, who declares information for application system and organizational designers about generally valid elements of a system to be modeled at a time as recommendations with a language, […] so that design problems can be solved and efficiency increases can be achieved.*"[442]

Reference models do not serve to prove the truthfulness in relation to the verification or validation of statements or the recognition and explanation of facts. Their aim is to construct a larger range of possible (decision) situations and thus serve as ready-made solution schemes for certain classes of (decision) problems in order to solve practical problems. However, for them to be reused, the

---

[436] Schmalzl (1995): Architekturmodelle zur Planung der Informationsverarbeitung von Kreditinstituten, p. 206, translated from German: „*Anhand charakteristischer Eigenschaften wird ein Sachverhalt mit seinen gültigen Ausprägungsformen in einem Referenzmodell allgemein beschrieben. Ihren besonderen Wert erhalten Referenzmodelle, wenn daraus bei Kenntnis der Einflußparameter und Rahmenbedingungen nicht nur konkrete Ausprägungen abgeleitet werden, sondern das Referenzmodell auch als Vergleichsgröße der unterschiedlichen Endprodukte dienen kann*"

[437] *Cf.* Gajewski (2004): Referenzmodell zur Beschreibung der Geschäftsprozesse von After-Sales-Dienstleistungen unter besonderer Berücksichtigung des Mobile Business, pp.11-16

[438] In this thesis Software Engineering is understand according to the definition provided by Mills (1980): The management of software engineering, Part I: Principles of software engineering, p. 1: "*Software engineering may be defined as the systematic design and development of software products and the management of the software process.*"

[439] In this thesis BPR is understand according to the definition provided by Hammer/Champy (1994): Business Reengineering – Die Radikalkur für das Unternehmen, p. 48: "[Business Process*] Reengineering is defined as the fundamental rethink and radical redesign of business processes to generate dramatic improvements in critical performance measures -- such as cost, quality, service and speed.*"

[440] Gessler (2014): Entwicklung Eingebetteter Systeme, p. 88, translated from German: "*The Waterfall model is one of the classic and fundamental models of software engineering.*"

[441] Oracle Inc. (2006): Utilities Customer Care and Billing 2.3.1 Utility Reference Models: "*The Utility Reference Models (URMs) are a set of business process models that show how Oracle Utilities Customer Care and Billing supports a utility's standard business processes*"

[442] Gajewski (2004): Referenzmodell zur Beschreibung der Geschäftsprozesse von After-Sales-Dienstleistungen unter besonderer Berücksichtigung des Mobile Business, p. 34, translated from German: „*Ein Referenz-Informationsmodell ist das Ergebnis* […] *eines Modellierers, der für Anwendungssystem- und Organisationsgestalter Informationen über allgemeingültig zu modellierende Elemente eines Systems zu einer Zeit als Empfehlungen mit einer Sprache deklariert,* […] *so dass Gestaltungsprobleme gelöst werden können und Effizienzsteigerungen erzielt werden*."

reference models must have a certain general validity, but not be syntactically complete and consistent.

The various definitions of “reference models” result in various requirements, application areas and goals for the use of such models. It can be distinguished between the modellers and users of reference models. The modellers are in most cases researchers trying to give a shape of the reality using models. The users of reference models are looking for cost reduction, revenue improvement and risk mitigation. Therefore, the use and application of reference models could help to achieve these goals by supporting the users, for example, in the selection of software solution, the process and/or software development. The cost reduction can be achieved due to the collaboration between practical experience and comprehensive theoretical knowledge. This collaboration results in a simplified, uniform, enterprise-wide framework of processes and procedures. This leads further to mitigation of the risks of using faulty, incorrect and inappropriate models. However, the costs for development of the reference models must be considered. To reduce these costs, the reference models can be reused. When a reference model is reused certain additional steps are needed like adaptation or adjustment which are also the main criticized aspects of the use of reference models. In addition, the lack of sufficient modelling knowledge and acceptance of the models in practice by the users are also known problems[443].

Schütte provided a five-steps process model for the development and application of reference models, independent of the application area. The process model is a comprehensive, yet understandable, approach for the development and reuse of reference models that could make the handling of reference models easier for the modelers. The main task of this process was to enable a uniform modelling procedure[444]. For the aim of deriving a proposal for a CDD reference model only steps from 1 to 4 will take place[445].

1. Problem definition: The first step of the process is the development of the problem definition and types (e.g. modelling objectives). In this case the modelling objectives represent the need for a consolidated CDD framework considering the organizational structures and internal processes.
2. Development and construction of a reference model frame: In this step the “WHAT” of the reference model is designed. For this goal Schütte introduces the term “master reference models”. These are models that contain model building blocks that can be used in the construction of reference models independently of any company classification and are therefore superior to reference models. They describe standard structures that consist of (information) objects, tasks and the (application) context and are independent of aspects of specific organization, (information) technology, execution sequences and task carriers. For this goal, the principles of the Enterprise Architecture (EA) will be used. It is more appropriate to use such methodology in addition to pure Business process modelling notation (BPMN) because it can describe

[443] *Cf.* Ibid., pp. 34-37
[444] *Cf.* Ibid., pp. 73-75
[445] *Cf.* Brocke (2015): Referenzmodellierung: Gestaltung und Verteilung von Konstruktionsprozessen, pp. 134-138

a single domain from different point of views and/or layers (business, data, organization, technology, etc.)[446].

3. Development and construction of a reference model structure: The reference model structure is designed to define the "HOW" of the reference model and for which purpose the models declared in the reference model framework must be represented using a language. The process and data models relevant to process objects must be constructed and linked to one another. In this step the previously developed frame is given a concrete structure.
4. Finalization: The fourth phase completes the reference model, creates cross connections within the reference model and to other reference models. In this step the model is being enriched with data and evaluated (for example, by conducting expert interviews with AML officers).
5. Application: The last phase of the process model concerns the application of reference models.

Another alternative approach is the use of a process defined by Rosemann and Schütte and already successfully applied by Timm et al.[447]. However, for the scope of this master's thesis the initial model by Schütte is sufficient[448].

5.3. Enterprise Architecture modelling

EA is a methodology to manage the enterprise design, planning and implementation in order to achieve the strategy goals of the enterprise. By developing an enterprise-wide architecture framework or programme it is possible to get a clear overview over the organisation, understand how business and IT are working and collaborating and how the visions and the strategy of the enterprise can be achieved. EA allows the alignment between organisational structures, processes and IT, in order to speed up the delivery of higher quality business services with less costs. Yet, EA is subject to criticism caused by its "*lack of realism*"[449]: "*EA is a very important instrument for modern organizations critically dependent on IT in their daily activities. However, EA is also an extremely complex and multifaceted instrument which is still poorly understood. The idea of EA is typically explained*

[446] *Cf.* Timm/Zasada/Thiede (2016): Building a Reference Model for Anti-Money Laundering in the Financial Sector, p. 7
[447] *Cf.* Ibid., p. 8
[448] Despite the fact that Rosemann and Schütte proposed a multi-perspective reference modeling in order to avoid quality defects of models used for different goals („*Einsatzzwecke von Referenzmodellen*") for the aim of this master's thesis the multi-perspectivity property of the referenced model will be compromised and thus waived (*See* Rosemann/Schütte (1999): Multiperspektivische Referenzmodellierung: "*Üblicherweise wird bei der Erstellung von Referenzmodellen nur eine Perspektive fokussiert, die integrative Gestaltung mehrerer Verwendungszwecke eines Informationsmodelles wird hingegen nicht betrachtet. Wird die Qualität eines Informationsmodells an der Bewertung des Nutzers ausgerichtet, so sollte diesem Umstand insbesondere durch den frühen Einbezug repräsentativer Modellanwender Rechnung getragen werden.*", p. 1 and „*Wird die Verwendungseignung eines Modells für die mit diesem Modell verfolgten Zwecke als wesentliches Merkmal der Modellqualität verstanden, und wird der beschriebene Zweckpluralismus zugrundegelegt, so wird deutlich, daß ein (Referenz-)Modell für unterschiedliche Zwecke unterschiedliche Qualitäten besitzen kann. Da sich die genannten Zwecke offensichtlich nicht gleichermaßen durch ein Modell unterstützen lassen, bedarf es zur Vermeidung von Qualitätsmängeln, einer am Verwendungszweck orientierten Modellkonstruktion.*", p.4)
[449] Kotusev (2017): Enterprise Architecture on a Single Page, p. 2

through popular EA frameworks, but their prescriptions hardly correlate with successful EA practices in real organizations [...]."[450]

Despite the critics, currently one major alternative to describe the enterprise's architecture would be to use business capability models (BCM)[451]. In this section I will try to answer shortly what an EA reference model is and will propose a CDD reference model modelled with the EAM framework TOGAF®[452] by using ArchiMate®[453]. TOGAF® is a recognized framework, broadly used in the practice and research for the purposes of Enterprise Modeling[454]. It distinguishes between four different enterprise architecture domains: business, data, application and technology, and provides an Architecture Development Model (ADM) which is an iterative process for continuous architecture definition and realization[455]. On the other hand, ArchiMate® is a language for EAM modelling specially developed for TOGAF®. Thus, the ArchiMate® language completes the TOGAF® framework. In addition, ArchiMate® consolidates the data and application domain into one[456]. By complementing TOGAF®, ArchiMate® provides techniques and instruments for description, analysis and visualization of the relationships between the enterprise's domains.

Reference models (RMs) in the context of EA can have different forms and functions[457]. The main goal of the RMs is to speed up the modelling process by using templates and patterns to avoid duplicates, loops and "reinvents the wheel" multiple times. RMs have different "*degree of specialisation*"[458]. This means that more generic RMs have to be adapted in order to fulfil the EA tasks, for which they will be used for: "*RMs are developed to encapsulate reusable knowledge about various domains of the modelled enterprise; thus, RMs are typically focused on specific aspects (e.g. function, information, decision, etc.) or on a combination thereof."*[459].

In March 2018 Felix Timm and Prof. Kurt Sandkuhl from University of Rostock published a research paper[460] originating from a project sponsored by 9 member organizations of BITKOM[461], the German digital industry association. The authors of the research are proposing a model for a Referenced Compliance Organisation (RC-O).

The result of that research and the referenced models proposed in this master's thesis are similar and at the same time different. In this master's thesis I put the focus on the customer due diligence aspects and this results in a proposal for a CDD reference model, while Timm/Sandkuhl distinguish between three different regulatory domains: AML, KYC and Fraud prevention. Another differentiation between these two works is the fact that Timm/Sandkuhl used inductive and deductive strategies for

---

[450] Kotusev (2017): A Frameworks-Free Look at Enterprise Architecture, p. 19
[451] *Cf.* Kotusev (2018): Fake and Real Tools for Enterprise Architecture, p. 4. A remark: Kotusev criticizes mainly the Zachman Framework which can be seen as the foundation for all modern EA frameworks. Meanwhile, BCM can be seen as an integrated part of most of the EA frameworks. However, a comparison analysis between framework-dependent EA and the role of BCM in EA is beyond the scope of this thesis.
[452] *See* The Open Group (2018): The TOGAF® Standard (homepage: ww.opengroup.org/subjectareas/enterprise/togaf/)
[453] *See* The Open Group (2018): The ArchiMate® Enterprise Architecture Modeling Language (homepage: www.opengroup.org/subjectareas/enterprise/archimate-overview/)
[454] *See* The Open Group (2018): TOGAF® 8.1.1: Case Studies
[455] *Cf.* The Open Group (2018): TOGAF® 9.2: Core Concepts
[456] *Please note*: The complete ArchiMate® architecture model consists of six layers
[457] *Cf.* Noran (2006): Using Reference Models in Enterprise Architecture: An Example, p. 4
[458] Ibid., p. 4
[459] Ibid., p. 5
[460] *See* Timm/Sandkuhl (2018): Towards a Reference Compliance Organization in the Financial Sector
[461] BITKOM (homepage: https://www.bitkom.org/)

the construction of the proposed RCO, while this master's thesis is based on a deductive approach and reasoning as described above.

5.4. CDD reference model

The second research question of this master's thesis is:

RQ2: Is it possible to derive a reference model for the AML Customer due diligence (CDD) from an existing enterprise's AML context?

In this case the answer is "**maybe**". I did receive access to the internal processes from only one financial institution (out of eight). Therefore, the developed reference model which will be presented below is based mainly on literature research. In addition, the needs and methodology for such a model were discussed during two interviews with a compliance officer from one of the financial institutions and an EA expert. The model itself was then methodologically validated by EAM experts. Therefore, the results from the literature research made in chapter 3, 4 and 5 provide partly a basis for the creation of a simple CDD reference model. The proposed model could be extended and modified after additional feedback from experts and an analysis of the internal bank's processes. Based on ArchiMate® modelling concepts the CDD reference model has the following structure: The ArchiMate® layers are the frame or structure of the model, while ArchiMate® views represent the relevant CDD perspectives (organisation, business, application). In other words, a viewpoint represents a particular pool of models and/or classes of objects. For example, the view "Application landscape" consists of relevant applications needed for an operative CDD process, the view "Risk assessment" includes all relevant processes and risk categories needed for the risk assessment on customer level, etc. Following the ArchiMate® architecture I represent the CDD reference model on three different levels.

The first productive steps of the construction of the reference model are the definition of the model frame and model. The modelling framework is defined as an ArchiMate® viewpoint on Level 1 of the model. Level 1 represents an abstract picture of the core components of a CDD model, following the three-layer structure by ArchiMate® aspects. Each layer consists of different ArchiMate® views. Due to the assumption that most of the financial institutions are using different technologies and for the goals of definition of a reference model and despite that there are known technologies that are common for all (for example, an E-Mail Client), the proposed reference model does not contain a technology layer. The proposed referenced model below is structured as follows (corresponds to steps 2 and 3 from Schütte's process, "Development and construction of a reference model structure"). The model is represented on three levels with three different degrees of detail.

CDD reference model: Level 1

Level 1 represents an abstract picture of the core components of a CDD model following the three-layer architecture of ArchiMate® (business, application and technology). Each layer consists of different views describing the core elements of the CDD.

Business layer

On business layer "CDD organization" is the view showing the organizational structure and organizational entities involved in the CDD process. It corresponds to the ArchiMate® organizational view: "*The organization viewpoint focuses on the (internal) organization of a company, department, network of companies, or of another organizational entity.*"[462].

The view "Risk assessment" references the risk factors needed for the objectives of the risk assessment, while "Customer Due Diligence" represents the ArchiMate® view over the corresponding business processes and procedures. The business layer is represented on two additional degrees of detail (Levels 2 and 3).

Application layer

On the application layer only one view is defined: the "Application and data landscape (internal & external)". According to the ArchiMate® specification, the application layer is used to model the enterprise's information system (IS), including the structure and interaction of the applications. The application layer is represented on only one additional degree of detail (Levels 2).

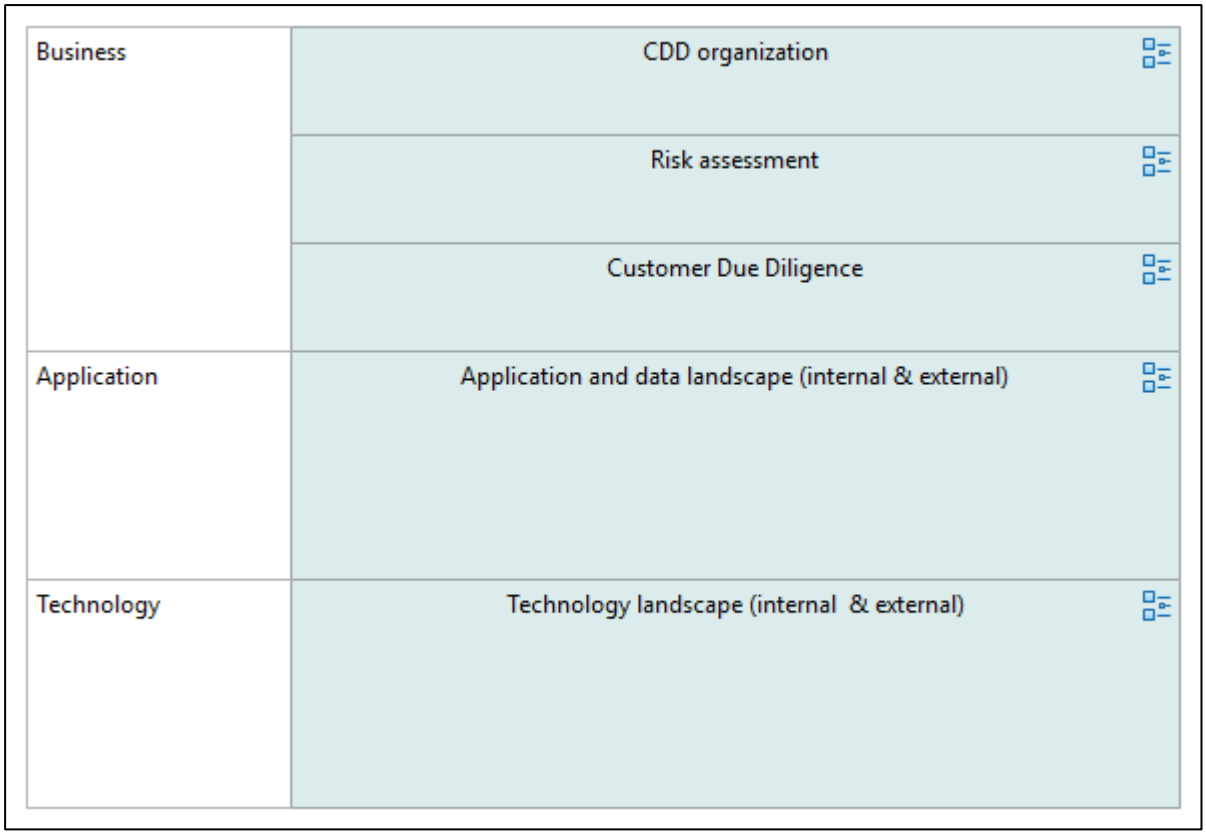

Figure 5 CDD reference model (Level 1)

Technology layer

The Technology layer is used to model the technology architecture of the enterprise. This corresponds to the structure of and interaction between different services, logical and physical technology

[462] The Open Group (2018): ArchiMate® 3.0.1 Specification, "*Organization Viewpoint*"

components. As mentioned above, due to lack of detailed information regarding the core systems in the financial institutions and due to the assumption that every financial institution has its own technology landscape and architecture, it is not reasonable or useful to develop a reference technological architecture with the idea of re-usability.

CDD reference model: Level 2

Business layer: view "CDD organization" (Organization viewpoint)

The proposed organizational structure shown in figure 6 consists of few business roles and one business actor - the customer. Business roles, according to the ArchiMate® specification, are responsible for performing of a certain behavior against a certain object. A particular (business) actor can be assigned to one or more roles but it is not necessary in this case. On the top of the organization is the business role "Management board". Due to the responsibilities and decision powers that the management board in a financial institution has, one needs to specify the communication channels to other organizational entities. The roles "Compliance/AML-Office", "Process management", "Risk and control management" and "IT" represent the core roles involved in the CDD process. In parallel, the "Account management" is an essential part of the organization due to its role as "first line of defence" and single point of contact to the customers.

Between the management board and the other roles there is, as assumed, a constant information exchange. Further, between the "Account management" and the roles responsible for the proper functioning of the internal CDD there should be also exchange of information and data. At the end, between the different CDD roles several communication channels are established. For example, a change of the internal control and risk assessment proposed by the management board or by the Compliance department would trigger changes in the internal risk and control documentation and in the way how this processing is done ("Process management"). Another example is when a request in the context of an IT change request triggers communication and information flow from and to the internal "IT" department. One can model additional roles in the context of CDD (e.g. sub-roles of "Compliance" for "Sanctions" or "Alerts management") but this would go out of scope of the reference model due to the fact that different financial institutions have different organizational structures. Therefore, the proposed organizational structure can be seen as an abstract interpretation of the regulatory obligations regarding the prevention and detection of money laundering stated in FM-GwG.

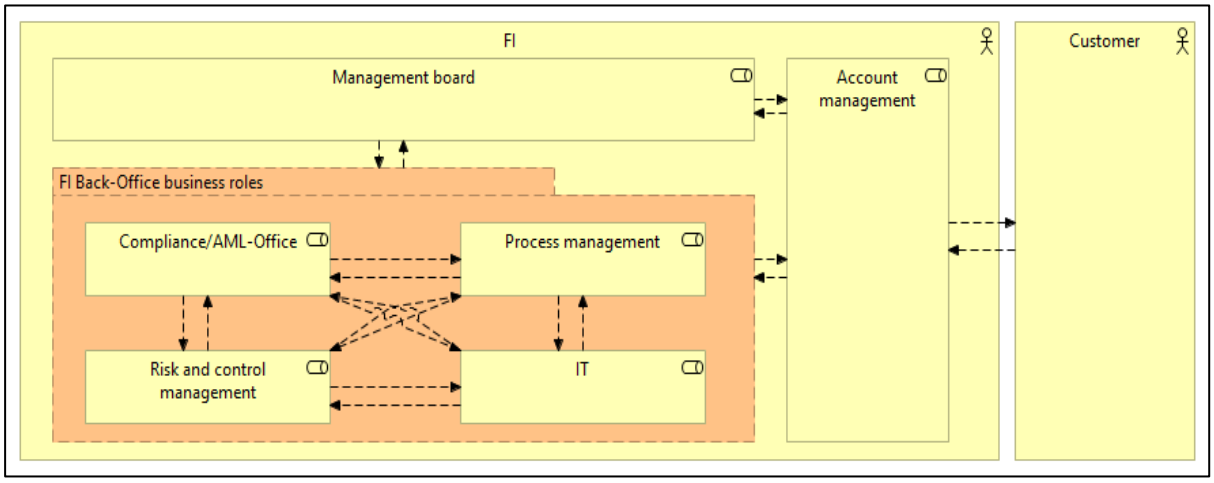

Figure 6 CDD reference model (Level 2: View "CDD organization")

Business layer: view "Risk assessment"

The current version of ArchiMate® does not provide a direct possibility to model classes of risks and/or controls or to define a risk management viewpoint. However, there are research approaches in this direction with the definition (or mapping) of the "risks" and "controls" as "specializations" (ArchiMate®) and definition of "control objectives" as "goals" (ArchiMate®)[463]. For the purpose of this master's thesis I modelled the risk factors as modelling classes which can be then instantiated further as objects on deeper levels or which can be used in order to classify the risks in a more detailed way. Due to lack of further specific and detailed information, the model (or the view) includes only those risk factors which are specified in **Annexes I**, **II** and **III FM-GwG**. The risk variables are groups as follows: "General risk factors", "Risk factors in geographical terms", "Risk factors relating to customers" and "Risk factors relating to products, services, transactions or distribution channels". Each risk factor is comprehensively commented and described in the previously mentioned publication by FMA[464]. Few important aspects are missing from this model - the definition of corresponding controls and definition of responsible business roles. According to the nature of risk factors, some of them may be relevant for or may concern only the account management ("Purpose of the account or business relationship") department or only for the compliance unit ("Anonymous use of products, services or transactions") or for both ("Receipt of payments from unknown third parties"). What is also missing due to lack of real-world information about different scenarios is the probability and impact these risk factors could have, in case they have any. Of course, the proposed catalogue of risk factors can be extended with the additional risk factors listed in the Austrian National Risk analysis[465].

[463] *See* Koning (2007): Risk Management in TOGAF & Risk Modeling in ArchiMate
[464] *See* Finanzmarktaufsichtbehörde (2018): FMA-Rundschreiben Risikoanalyse zur Prävention von Geldwäscherei und Terrorismusfinanzierung
[465] *See* Bundesministerium für Finanzen in Zusammenarbeit mit den zuständigen Ministerien und Behörden (2015-2016): Nationale Risikoanalyse Österreich

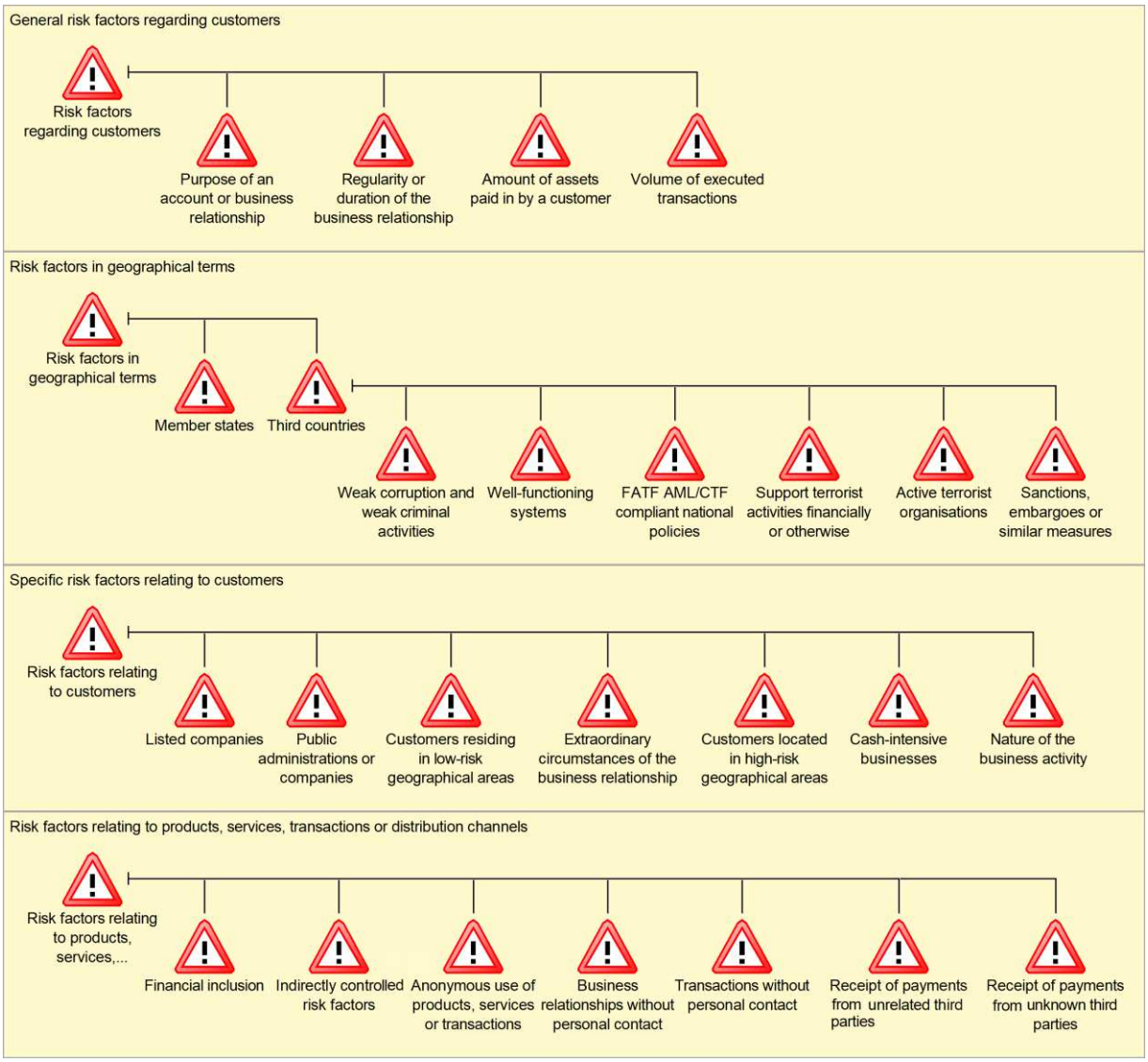

Figure 7 CDD reference model (Level 2: General risk factors)

Business layer: view "Customer due diligence"

On Level 2 the reference CDD model contains a simple process landscape similar to the typical AML compliance program in figure 1 but focused on the Reporting and CDD processes. In the "CDD" model there is no explicit differentiation between natural or legal persons. Both process landscapes consist of several business processes and business functions. According to ArchiMate® specification, a "business process" "*represents a workflow or value stream consisting of smaller processes/functions, with one or more clear starting points and leading to some result.*"[466] A "business function" is "*a collection of business behavior based on a chosen set of criteria (typically required business resources and/or competencies), closely aligned to an organization, but not necessarily explicitly governed by the organization*"[467]. The business processes are grouped in an "Onboarding" business function (processes corresponding to the verification process while establishing a new business relationship with a customer, e.g. CIP), "Ongoing" business function

[466] The Open Group (2018): ArchiMate® 3.0.1 Specification, "*business process*"
[467] Ibid., "*business function*"

(business processes corresponding to the daily customer due diligence activities of the financial institution) and "Reporting" business functions (consists of functions corresponding to the reporting obligations and activities [in this case it is not distinguished between the internal and the external reporting procedures]). There are no specific business events defined because the due diligence obligations are applied before the establishment of a business relationship or when executing an occasional transaction as stated in **§ 7 FM-GwG**[468]. In the current view there is only one business actor, the "Customer", who is just a readable representation of the entity responsible for the customers and two business roles: "Account management" and "Compliance/AML-Office" (both in a constant interconnection and information exchange). The business role "Account management" is triggering, at least, the "Onboarding"-functions and the role "Compliance/AML-Office" can trigger and is associated to all relevant AML functions. The business object "Risk assessment score" represents the assessment score for a particular customer. The object can be modified as a result from a particular action or function and accessed by all business roles.

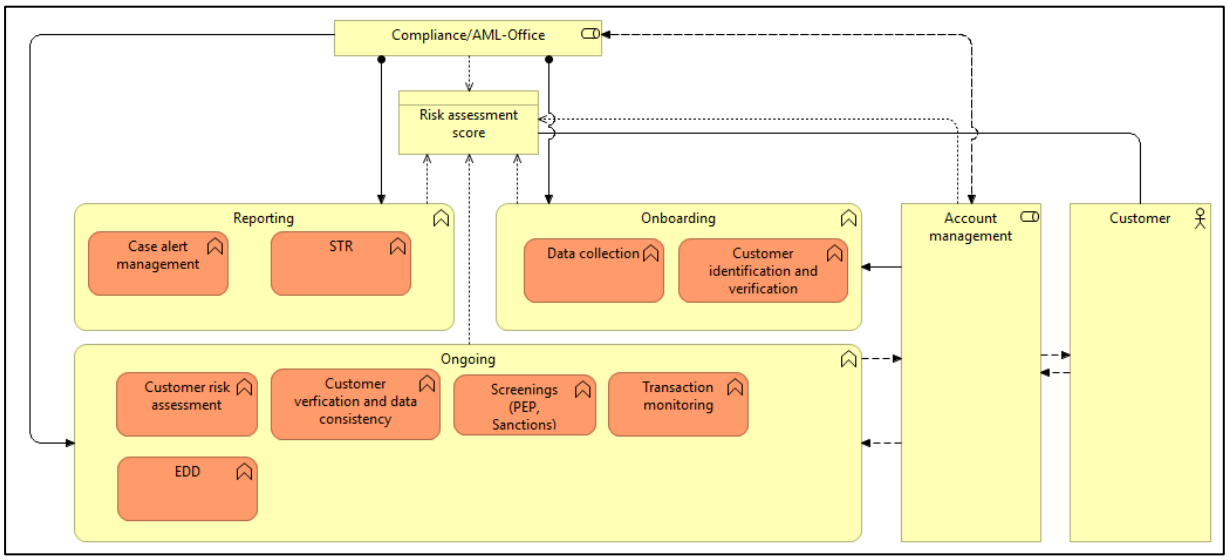

Figure 8 CDD reference model (Level 2: Business functions)

Application layer

On the second level of the "Application layer" the reference model consists of an abstract representation of the applications and data entities in the context of CDD. The representation can be divided into three main elements:

1. Internal document management system (Application collaboration[469])

   The main purpose of this system is to store, not necessary centrally, all relevant customer data like the customer profiles. The profiles themselves consists of different data objects like "Personal data", "Statistics" (about customer's transactions and activities) and up-to-date "Risk score". In the customer profile additional, third-party data may be included or at least referenced. The document system contains also the data objects "Sanctions" and "Red flags".
2. Application functions

[468] *See* section 3.1.5 for more information about the point of time of application of the due diligence obligations
[469] The Open Group (2018): ArchiMate® 3.0.1 Specification: "*application collaboration*": "*An application collaboration is defined as an aggregate of two or more application components that work together to perform collective behavior.*"

Both data objects, mentioned above, are used from the application functions “Ongoing CDD” and “Risk assessment” (according to ArchiMate® specification an application function “*describes the internal behavior of an application component. If this behavior is exposed externally, this is done through one or more services. An application function abstracts from the way it is implemented.* “[470].

3. Application services

   The application function “Ongoing CDD” consists of four business services which support the (automatically) execution of the function (“*An application service is defined as a service that exposes automated behavior.*”[471]).

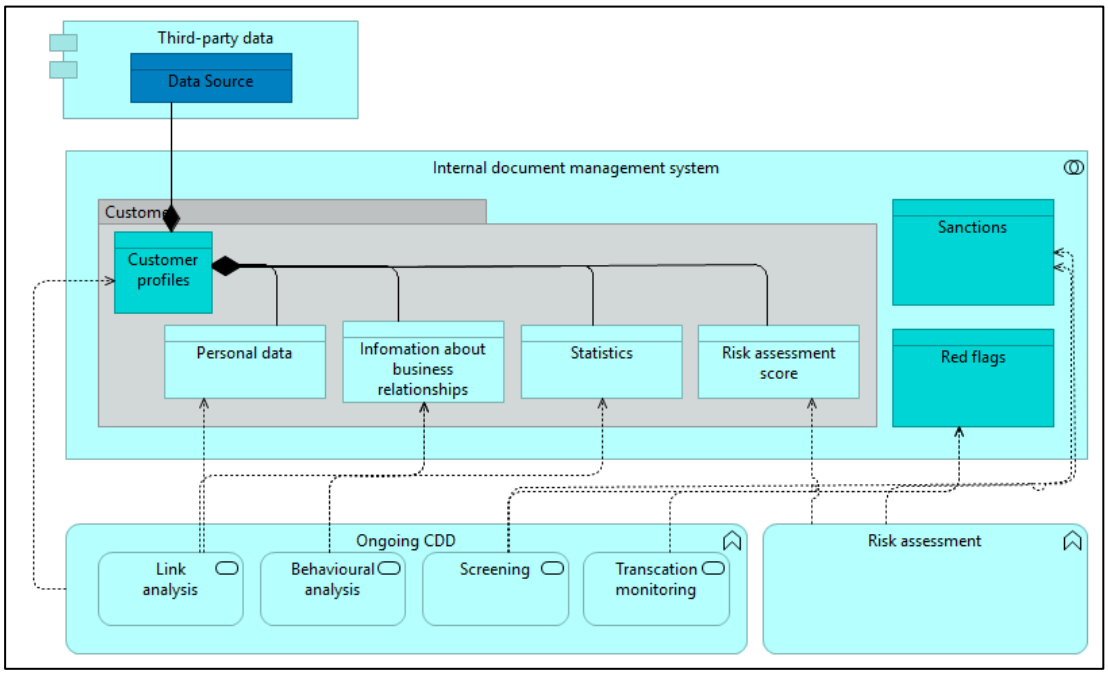

Figure 9 CDD reference model (Level 2: Data and Application landscape)

CDD reference model: Level 3

Business layer

On Level 3 I propose, as stated in section 5.1., a definition of the core CDD processes modelled in BPM notation (this step corresponds to step 4 “Finalization” from Schütte’s process for deriving a reference model). In its core the CDD for *new customers* consists of two steps:

1. Check and verify customer identification
2. Calculate risk score
   - If the risk score is lower or equal than the expected one: a new business relationship can be established and/or a transaction can be executed
   - else: execute EDD

[470] The Open Group (2018): ArchiMate® 3.0.1 Specification, “*application function*”
[471] Ibid., “*application component*”

What is interesting is the CDD for *existing customers* when the customers and their transactions are screened. This means customers for which the risk score has been already calculated and who already have an established business relationship. In this case all checks could be triggered manually or automatically. The re-calculation of the risk score could be seen as an iterative loop. The CDD processes, for new or existing customers, are visually represented most commonly as a set of steps that must be conducted manually and/or as on event-triggered occasion. The following figure represents the CDD process divided into “Risk identification”, “Risk assessment” and “CDD/EDD” sub-processes (for better graphical representation all three sub-processes are represented on the same layer in figure 12). I distinguish between two lanes of responsibility - the “Account management” and the “Compliance/AML-Office”. The “Account Management” is responsible for all actions regarding the establishment and management of business relationships with the customers. In case of a new customer the Customer Identification program is executed, when the customer identification is verified. This step is followed by calling the “Risk assessment” sub-process, which falls in the responsibility field of the Compliance unit. Depending on the calculated risk score, a Simplified (or Enhanced, respectively) due diligence is triggered. The next steps are the storing or updating of all collected relevant information about the customer. In case of suspicion, an (internal) STR process is executed. At the end, further steps regarding the customer are executed (establishment or termination of the business relationship).

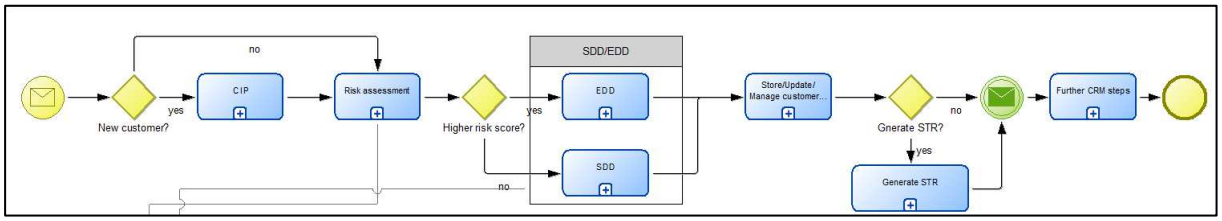

Figure 10 CDD reference model (Level 3: Business processes): Account management perspective

The compliance unit is responsible for the risk assessment and for the procedures supporting the SDD and EDD processes. The risk assessment is based on the risk factors defined by the financial institution. On a process level, this is supported by some additional steps (like “Transaction monitoring” or “Link analysis”), executed manually or automatically. As a result of these steps, the risk profile of the customer is generated (or modified). The step “Verification of the identification” could be, of course, also part of the sub-process “Customer identification program”.

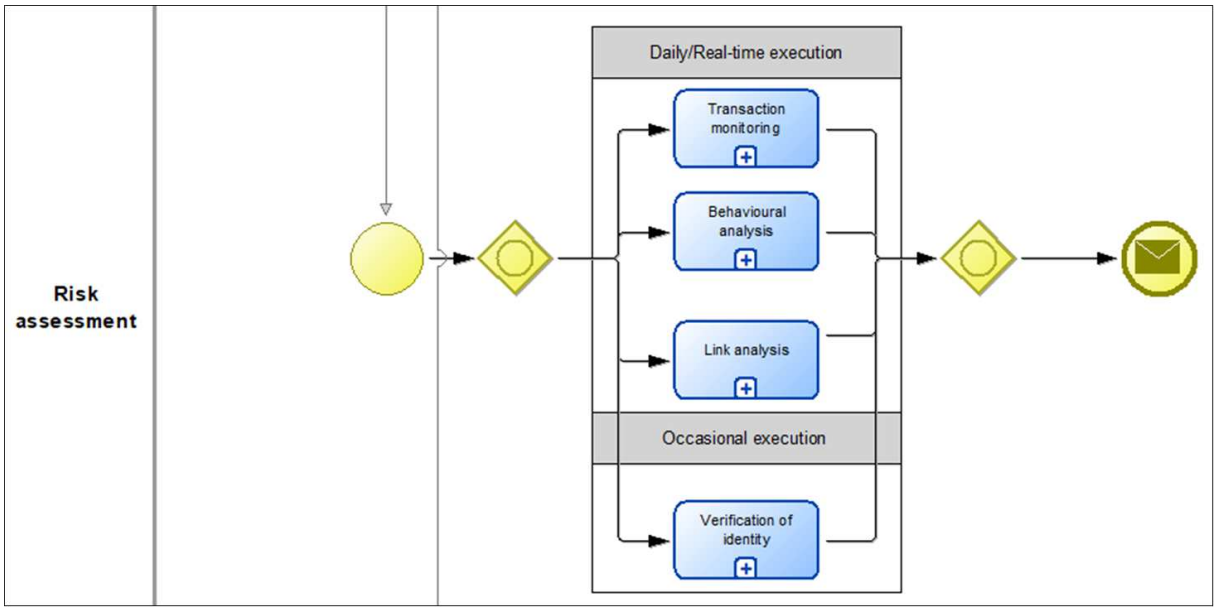

Figure 11 CDD reference model (Level 3: Business processes): Risk assessment from Compliance perspective

Based on the calculated risk score the CDD process is executed. The checks during the process can be “simplified” or “enhanced”, while it is again supported by additional sub-steps or by parts of them (for example “Beneficial ownership” or “Third-party research” are executed only when this makes sense and depending on the customer and his/her business(es)).

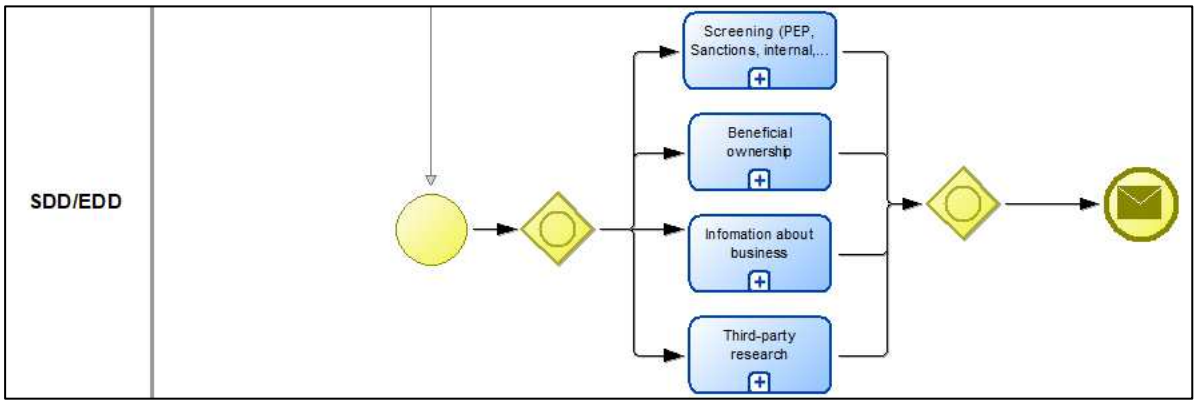

Figure 12 CDD reference model (Level 3: Business processes): Due diligence procedures from Compliance perspective

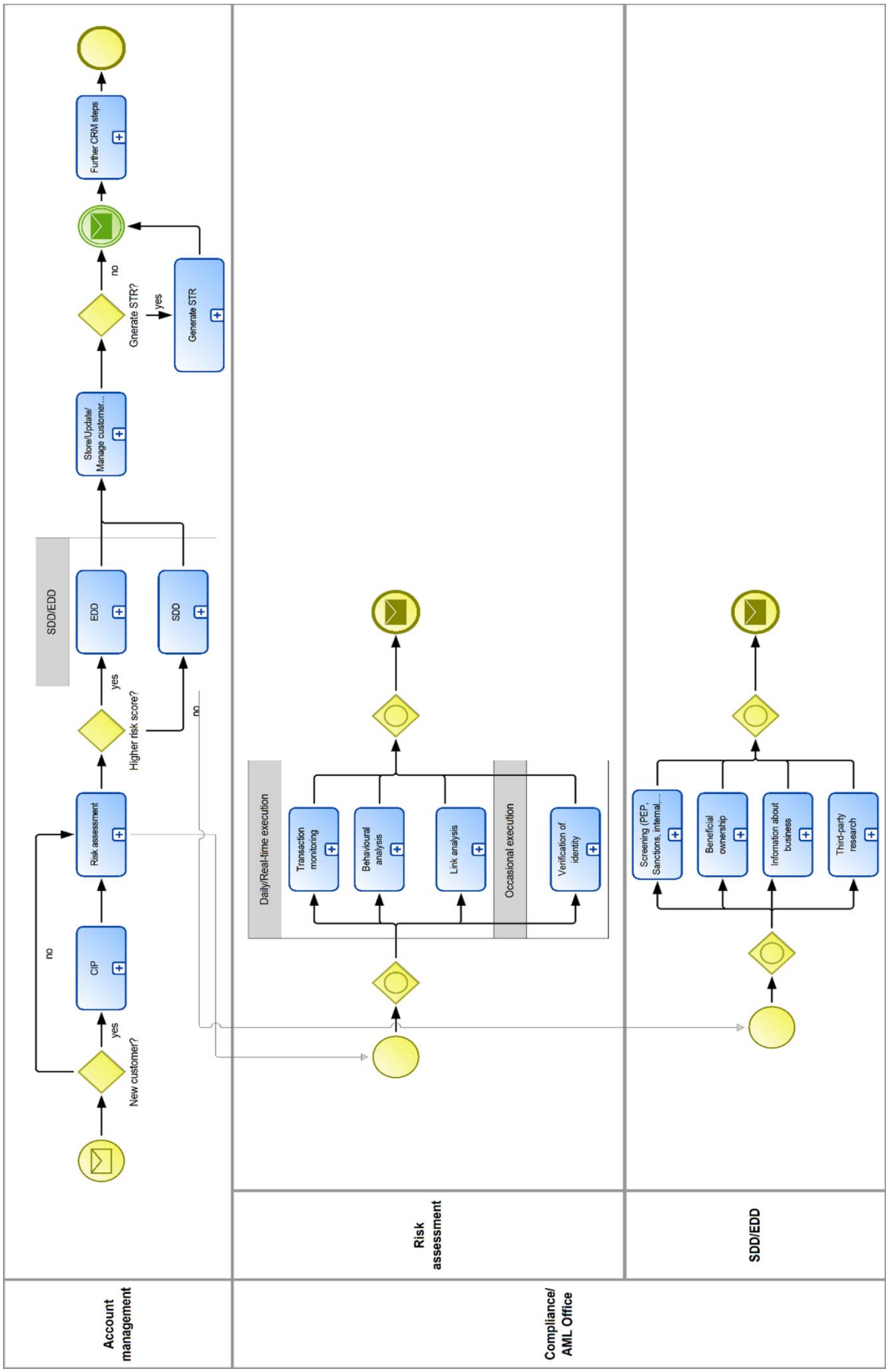

Figure 13 CDD reference model (Level 3: Business processes)

5.5. Summary

In this chapter I was able, in a deductive way, to derive a proposal for CDD reference models. The methodology proposed by Schütte for developing reference models was successfully applied. In addition, during the definition of the reference models I considered some properties of the models. Despite the fact that they can be seen as a proposal and not as an illustration or extraction of the real-world practices, it might be helpful to build or derive more appropriate models considering in addition some of the following two properties.

Consistency

The model needs to support a **consistent** information for all customers at the same time. This means that at any given point of time the customer data should be up-to-date and include possible relationships to other customers of the same bank and up-to-date information about the business relationship. This could be done by extending the application layer with relevant application components and services and connecting them with the corresponding business processes on the business layer. This would result in a collaboration between these two aspects in order to provide the scenario needed to keep up-to-date customer data.

Control

Currently, the model could be extended in a such way that it should be easy to freely **control** the executed checks, align them with the specifics of the customer and modify them when needed. Therefore, the models must be dynamic and act accordingly. This could be done by adding business processes (now business functions) and business events on the business layer. Thus, the information and data flow could be regulated.

On ***organisational*** level the ***consistency*** aspect requires the availability a proper customer documentation from the key account managers, transparency regarding the customer management and internal organisational management. It must be easy to ***control*** the flow of customer data and/or customer requests and manage it appropriately. The organisational structure must be, of course, ***compliant*** to the provisions, defined in the corresponding laws (for example BWG or FM-GwG).

The ***business*** domain includes all business processes for a successful CDD internal procedure. The defined internal processes must be valid and ***compliant*** at any point in time. A regular internal revision must check the state and their ***consistency*** of the processes and give appropriate recommendations, if needed. The process responsible employees must be able to ***control*** the process execution and to manage them accordingly on demand (updates and/or modifications). In addition, the process owners are responsible for the validity of the models.

Behind ***application*** (or ***technology)*** all relevant IT key factors are included. Every bank must establish an adequate IT landscape in order to detect and prevent money laundering. Otherwise, the risk of a money laundering breach increases. Therefore, the technology must be in a ***consistent*** state (for example, the used software must be up-to-date, the internal security standards must be documented accordingly, etc.). Moreover, the IT must be operated and managed easily (***control***). For example, the creation of an account for a new compliance officer must not be a burden for him/her to properly fulfil his/her duties on time. A ***compliant*** IT means that the IT landscape or used IT systems,

or more precisely - the business processes supported by this IT landscape, must fulfil particular requirements, regulations and/or laws (for example GDPR, FATCA or SOX[472]).

In this master's thesis I am proposing reference models which might be the basis for future developments and researches. The topic requires additional validation and evaluation by AML experts and it has room for improvements in regard to the EAM. Due to lack of application tests it is questionable if the proposed model(s) can fulfil any particular goal or be successfully used in the practice.

[472] *See* The European Parliament and the Council of the European Union (2016): Regulation (EU) 2016/679 (GDPR)
See IRS (2018): The Foreign Account Tax Compliance Act (FATCA): "[FATCA] *generally requires that foreign financial Institutions and certain other non-financial foreign entities report on the foreign assets held by their U.S. account holders or be subject to withholding on withholdable payments*"
See U.S. Securities and Exchange Commission (2018): Sarbanes-Oxley Act of 2002 (SOX): "[SOX] *mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud*"

Conclusion

Since (organized) crime is in the main reason for money laundering it would be wrong to say that the end of money laundering is near. Austria has an adequate legislative basis to combat ML/TF but as mentioned already there is room for improvement of the legislative landscape. The financial institutions are already working proactively to establish and develop a proper internal ML defence strategy and policy. Other obliged entities like insurance companies, investment funds, money transmitter companies and non-financial businesses and professions (DNFBPs) like lawyers or notaries should follow their example. Beside this, the financial institutions should keep and further improve their strong collaboration with the A-FIU and when possible – establish new collaborations with other banks. The A-FIU must be more open for domestic partnerships with the financial institutions in Austria. The current communication could be improved in a way that the STR process consumes less time and efforts (from both sides). Both A-FIU and banks need to be more transparent when it comes to topics like ML/TF. Any improvements in the internal processing regarding STRs could lead to improvements in the legislative basis. In addition, the fact that in 2018 no annual report regarding the ML has been published is, to say the least, surprising and unexplainable. In this master's thesis I tried to find any correlation between the internal competencies in a bank and the number of STRs generated by the bank. Despite the fact that the eventual correlation should be defined more appropriately (for example, STRs generated in the context of offshore-customers), it should be easier to find out what happens behind the mere numbers published by the Bundeskriminalamt yearly.

The role of the FMA is not only as a supervisory authority and shall not be underestimated. The FMA has a clear leading role in the combat against ML/TF which must be strengthened further. The FATF and other international organizations could be an excellent partner of the financial institutions when it comes to knowledge sharing and knowledge acquisition.

The proposed CDD model can be used as a good starting point for future researches and studies. For example, a topic for a future development could be the development, and in the best-case, the establishment of an Austrian-wide CDD framework which can be easily adapted in accordance with new and upcoming (regulatory) challenges together with one consolidated legal basis. Another possible research topic could be a research project directly in A-FIU which could, in an anonymous way, analyze the processing and give improvement proposals – either for legislative changes or process optimization or both.

One of the most important reasons why money laundering should be tackled is the dependence in organized crime on the ability to transfer and (thus) invest large amounts of illicit funds back to the legal economy[473]. Essentially that is why according to Bernasconi the money laundering can be seen as the Achilles heel of criminal activity[474] as it forces criminals to use the legal financial systems and services. Successful AML counter-measures reduce incentives for criminals. That is why the combat

[473] *Cf.* Fiedler/Krumma/Zanconato/McCarthy/Reh (2017): Das Geldwäscherisiko verschiedener Glücksspielarten, p. 15
[474] *Cf.* Stessens (2000): Money Laundering: A New International Law Enforcement Model, pp. 12-13

against ML/TF has meanwhile developed into the most important and control-intensive component in the fight against organized crime. Successful AML counter-measures would increase the costs of money laundering. This would lead to an increase of the costs of the crime itself which makes them less profitable and thus leads to a reduction in crime levels[475]. However, it will not be possible to stop or at least to minimize money laundering without full global cooperation.

[475] *Cf.* Fiedler/Krumma/Zanconato/McCarthy/Reh (2017): Das Geldwäscherisiko verschiedener Glücksspielarten, p. 16

Appendix

Appendix I: Expert Interviews

During the writing of this master's thesis following interviews were conducted. The interviews were structured as an open discussion and most of them were audio recorded. In addition, during the discussions notes were taken. Afterwards the recorded audio was transcribed into text and together with the taken notes summarized in sentences. The answers to the questions represent in most of the cases the exact wording given by the experts. However, in some cases the answers are content-wise correct but do not represent the exact wording.

Dr. Elena Scherschneva-Koller

Interview Partner	Dr. Elena Scherschneva-Koller Self-employed lecturer, trainer and expert in the field of combating money laundering and terrorist financing
Date	22.05.2018
Time	14:15 – 14:45
Language	German
Communication	Phone
Remark	The conversation was not recorded

Anzahl STRs: Vergleich zwischen Österreich und den Niederlanden

Wenn man sich die Statistiken in den Geldwäscheberichten schaut, sollte man alle Fälle berücksichtigen, und nicht nur jene, die schließlich als „Geldwäscherei" klassifiziert wurden. Diese Klassifizierung ist eher subjektiv. Die hohe Anzahl von UTRs in den Niederlanden kann mit verschiedene Vorgehensweise bei der Berichtserstattung und mit den unterschiedlichen Typen von den jeweiligen FIUs (in Österreich und in den Niederlanden) begründet werden. In Österreich darf man nicht einfach alles, was verdächtig ausschaut, weiterleiten, da das Bankgeheimnis (§ 38 BGW) gilt. Die Analyse von verdächtigen Fällen passiert in Österreich vorerst innerhalb den Banken; erst danach wird ein STR an A-FIU erstellt. In den Niederlanden ist die Vorgehensweise komplett andere.

Einheitliche KYC/CDD Modell möglich

Es ist, meiner Meinung nach, nicht möglich ein „one-size" Modell zu entwickeln, da sich die Banken hinsichtlich ihren Größen, Transaktionsvolumen, Typen von Kunden unterscheiden. Der risiko-basierter Ansatz (Die Klassifizierung von Kunden anhand des Gesamtbankrisiko (d. h. Risikobeurteilung auf Unternehmenseben) und schließlich Risikobeurteilung auf Kundenebene) finde ich momentan sehr gut. Deswegen sind (unter anderem) der risiko-basierter Ansatz, der menschliche Aspekt (interne Organisation) und die verfügbare/vorhandene Informationen („je mehr, desto besser") die wichtigsten Komponenten eines AML Programms.

Die Situation in Österreich im Kontext von Geldwäschebekämpfung

Österreich als „ein attraktives Land für Geldwäsche" zu bezeichnen ist eher übertrieben. Ja, Österreich ist ein „Finanzplatz" und das GW-Risiko besteht immer, das System (inkl. Banken) an

19 sich ist jedoch gut ausgeprägt und dafür vorbereitet.

Dr. Elena Scherschneva-Koller

Interview Partner	Dr. Elena Scherschneva-Koller Self-employed lecturer, trainer and expert in the field of combating money laundering and terrorist financing
Date	04.06.2018
Time	09:30 – 10:30
Language	German
Communication	In person

STRs: Gründe für den Anstieg zwischen 2014 und 2016

1 Einer der Gründe für den Anstieg ist, dass alle meldungspflichten Gruppen einfach sensibler
2 geworden sind. Die Annahme, dass der Anstieg auch wegen internationalem Druck (bspw. seitens
3 FATF) ist, kann man auch nicht ausschließen, das ist aber nicht der einzige Grund. Einerseits wird
4 von den Meldepflichtigen mehr (an A-FIU) gemeldet, andererseits ist der Druck auf den Banken
5 seitens der Aufsichtsbehörden gestiegen. D. h. es wird seitens der Banken im Zweifelsfall eine
6 Meldung (STR) generiert – das ist mittlerweile ein Standard. Außerdem, andere Berufsgruppen,
7 die bisher vielleicht zurückhaltender waren (z. B. Rechtsanwälte und Notare), werden immer
8 aktiver, da es eben rechtliche Konsequenzen bei einer „nicht-Meldung“. Früher gab diese
9 Konsequenzen auch, dafür aber waren die Aufsichtsbehörden nicht so ganz aktiv.
10 Die Qualität von STRs ist von Bank zu Bank unterschiedlich. Der Grund dafür ist der Grad der
11 Schulung („Schulungslevel“) der Mitarbeiter, die die Meldungen erstellen. Wichtig ist erwähnen,
12 dass man heutzutage komplett andere Sachverhalte meldet wie vor 10 Jahren, da sich die
13 Typologien (GW-Typologien) verändern, die Vorgehensweisen der Täter verändern und etwas,
14 was vor 10 Jahren verdächtigt war, ist heute nicht mehr verdächtigt und umgekehrt. Deswegen
15 kann man einen Qualitätsvergleich von den Meldungen in den letzten Jahren nicht machen.
16 Wenn z.B. eine Bank einen Kunden hat, der etwas macht, was für einen anderen Kunden völlig
17 normal wäre, aber für diesen aktuellen Kunden komplett „aus der Reihe tanzt“, wäre das auf jeden
18 Fall „unusual“, also ungewöhnlich. In diesem Fall müsste die Bank schon näher hinterfragt.
19 Ein konkretes Beispiel: Ein Einzelhändler, der Schuhe verkauft, bekommt plötzlich eine
20 Überweisung in der Höhe von EUR 500.000, mit dem Verwendungszweck „Loan agreement“. Das
21 wäre seltsam, da wie kommt er zu diesem agreement. Wenn man einen Kunden hat, der
22 permanent solche „Loan agreements“ abwickelt, ist das zwar ein Fall mit hohem Risiko, jedoch
23 nicht ungewöhnlich für den Kunden. Wenn der Kunde in beiden Fällen die Gründe für die
24 Überweisungen nachweisen kann, dann kann es sein, dass der Kunde unter einem verstärkten
25 Monitoring ist, aber eigentlich vom Risiko her eher niedriger eingestuft wird.

De-Risking vs. Risiko-Basierter Ansatz

26 Für die Banken ist das de-risking sicher eine gute Strategie, das GW-Risiko zu minimieren oder
27 nicht zu haben. Aber, die Kunden würden das verwenden, was am leichtesten zugänglich für die
28 Zwecken ist. Und wenn das für die Behörden noch leicht verfolgbar ist, dann ist es prinzipiell gut
29 für die Behörden. Aus der Sicht der Behörden ist es vielleicht besser zu wissen, wo die Leute
30 ihres Geldes und Finanzbewegungen haben, als es nicht zu wissen. Je mehr die Kunden auf
31 alternativen Zahlungsmitteln umsteigen, weiß man schließlich weniger.

Zusammenhangs zwischen Vortat und Geldwäsche und Alternative Vorgehensweise (Der Verdächtige soll die Herkunft des Geldes beweisen)

Momentan ist es relativ schwierig ein Verfahren (gegen GW) zu eröffnen. Der Ansatz „Jeder Verdächtige soll beweisen, woher das Geld kommt“ würde natürlich die Sachen leichter machen. Die Länder, die diesen Ansatz haben (vor allem Spanien, Italien), haben damit sehr gute Erfahrungen gemacht. Die Frage ist, ob das nicht überschießend wäre, wenn man in jedem Fall so vorgehen würde, wobei faktisch ist es so, dass der Kunde schon sehr viel nachweisen muss. Deswegen glaube ich nicht, ob der Alternativansatz sehr großer Unterschied in der Praxis machen würde. Die Mittelherkunftsregel hat man im Compliance-Bereich jetzt schon. Von der strafrechtlichen Seite aber ist es ein interessantes Thema.

Änderungen von § 165 (Katalog von Vortaten)

Der „Katalog“ schaut wenig aus, wurde aber tatsächlich erweitert. Vorher hatte man grundsätzlich nur Verbrechen als GW-Vortat (§ 17 StGB), die über 3-jährige Freiheitsstrafe bedroht sind und Vergehen, die über 1-jähriger Freiheitsstrafe, und zwar nur bei Vermögensdelikten bedroht sind. Das ist jetzt geändert worden. Jetzt ist alles, was mit über 1-jährige Freiheitsstrafe bedroht, ein „Geldwäsche-Vortat“. Dadurch ist der „Katalog“ naturgemäß kleiner geworden. Bisher war im Katalog alles drin, was trotzdem GW-relevant sein soll, obwohl es noch kein Verbrechen und kein Vermögensdelikt ist. Jetzt ist es sozusagen alles, was mit zwischen 1- und 3-jährige Freiheitsstrafe bedroht ist, auch drin. Im Bereich der GW bewegt sich alles in Richtung „all crime approach“, d. h. jede strafbare Handlung soll *vortattauglich* sein. Jetzt regelt FM-GwG alle kriminellen Handlungen, die mit GW in Zusammenhang stehen könnten.
Ein größeres Problem ist die aktuelle Situation „Ohne Vortat gibt es keine Ermittlung“ – das ist aber bedenklich, da bei der GW es genau darum geht – man hat die Verbindung zur Vortat nicht und wenn man nur die zwei Voraussetzungen dafür (Ermittlung) hat: 1. Aus einem Vortat stammendes Vermögen und 2. Verschleiern oder Verbergen der Herkunft. Alternative wäre, dass wenn man die Herkunft verbirgt oder die Herkunft verschleiert, dann muss das auch eine Ermittlungstätigkeit ermöglichen.

Übersiedeln von A-FIU ins BMF

Da GW ein strafrechtliches Delikt ist, gehört es dort behandelt, wo die Behörden angesiedelt sind. Dasselbe gilt für den Bereich des Terrorismus bzw. Terrorismusbekämpfung. Zuständig für die Bekämpfung von GW ist BMI.

Rolle der Kryptowährungen

Ich würde die Kryptowährungen eher als eine Möglichkeit Geld zu veranlagen und zu überweisen sehen und nicht als separate Typologie. Aber, die Tatsache, dass die Währung per se schon anonym ist, ist das Verschleierungsrisiko naturgemäß hoch. Aber ich würde die Kryptowährungen eher nicht als „Geldwäschewährung“ oder Ähnliches zu bezeichnen.

Die Situation in Österreich im Kontext von Geldwäschebekämpfung

Die Systeme sind an sich schon sehr stark. Das GW-Risiko ist weitläufig bewusst, es gibt jedoch meldepflichtige Berufsgruppen, die nachrüsten dürfen. Aber, die Zusammenarbeit zwischen den Behörden ist gut und läuft gut.

Rechtslage in Österreich im Kontext von Geldwäschebekämpfung

Die Rechtslage in Österreich im Kontext von Geldwäschebekämpfung kann man als „adäquat, mit Luft nach oben“ beschreiben, da sie sehr zerstreut ist. Es wäre gut, wenn man ein Gesetz hätte, in dem man zwischen den einzelnen Berufsgruppen differenziert und in dem man eine einheitliche Formulierung hat.

Referenzmodell: Meinung

Ein Modell wäre vielleicht nicht schlecht, wenn man in ganz groben Grundzügen ein

Minimalstandard geben würde. Das Modell könnte man auf Basis der externen Vorgaben entwickeln, da die internen Prozesse bei den einzelnen Finanzinstituten sind sozusagen das Ergebnis der Umsetzungen ihrer (den Finanzinstituten) Pflichten. So ein „Mindest-Modell“ wäre gut, weil dadurch die Sicherheit bei den Prüfungen durch die Aufsichtsbehörden geben würde und dadurch die Prüfung viel einheitlicher ausfallen würde. Deswegen würde es Sinn machen, so ein Modell in enger Zusammenarbeit mit der FMA zu entwickeln, damit es (das Modell) für die Beaufsichtigten auch wirklich sinnvoll ist. Gäbe es ein Modell, das je nach Risiko noch erweitert oder verengert werden kann, wäre das gut. Man kann das Ganze mit einem Rezept vergleichen. Man nennt die einzelnen Zutaten, die Köche (die Finanzinstitute) kochen dann das Gericht.

Univ.-Prof. Mag. Dr. Michael Getzner

Interview Partner	Univ.-Prof. Mag. Dr. Michael Getzner University professor at TU Wien, Head of the Department of Spatial Planning
Date	30.05.2018
Time	10:30 – 11:30am
Language	German
Communication	In person

Gemeinsames Forschungsprojekt mit Universität Utrecht

Seit ungefähr ein Jahr läuft ein gemeinsames Forschungsprojekt mit der Universität Utrecht. Die zuständige Person für die Forschungsgruppe dort ist Prof. Brigitte Unger. Im Laufe des Forschungsprojekts werden Daten analysiert, die die Geld- und Zahlungsströme in den Niederlanden umfassen. In den Niederlanden werden in einem „Datenpool" jegliche relevanten Daten zentralisiert abgelegt. Diese Datenbank ermöglicht das Verfolgen von Geldströmen aus dem Ausland in die Niederlande und umgekehrt und innerhalb der Niederlande. D. h. es werden auch potenzielle kriminelle Gelder oder Geld mit einer kriminellen Herkunft auch davon befasst. Es wird dabei versucht, sozusagen ein „Gravitätsmodell" zu entwickeln. Das bedeutet, man möchte auf Basis bestimmter Kerngrößen oder Kennzahlen (wie z. B. Raumüberwindungs-, Kommunikations- und Transaktionskosten, Größe des Herkunftslandes, Korruptionsindex des Herkunftslandes, etc.) die Bestimmungsgründe für einen Geldstrom herausfinden, sodass man diese Ströme von Land A (Ausland) nach Land B (Inland) und dann wieder ins Ausland leichter verfolgen könnte.
Auf Basis der Daten und den Beträgen kann man schließen, dass:

- in größeren Volkswirtschaften kriminelle Zahlungen häufiger auftreten, als in Kleineren und
- die einzelnen Geldströme nicht immer voneinander unabhängig sind (auch wenn es wirklich von außen so aussieht). Zum Beispiel: ein Geldtransfer von den USA nach China und schließlich nach Österreich könnte aus weiteren Zwischenverkettungen an Zahlungen bestehen – diese Annahme muss man auch berücksichtigen.

Verfügbarkeit von und Zugriff auf Zahlungsdaten in den Niederladen

In den Niederlanden ist man wesentlich weiter als in Österreich, was die Datenverfügbarkeit betrifft. Dort (in den Niederlanden) sind die Daten über jeden einzelnen Bürger und Bürgerin so verknüpft, dass man sehr leicht herausfinden und nachvollziehen kann, wo wer welches Geld auf dem Konto hat (inkl. Kontotransaktionen), ob mit dem Geld Liegenschaften, Autos oder Sonstiges gekauft wurde. Schließlich kann man anonym auf anonymisierten Daten und nach gerichtlichem Beschluss auf allen Geldströmen mithilfe von diversen Abfragen zurückgreifen und analysieren, wie sich das Geld innerhalb des Systems bewegt. Somit, was die Frage die Daten und Datenpooling aus verschiedenen Quellen betrifft, hat die Niederlande einen riesen Vorteil.

Verfügbarkeit von und Zugriff auf Zahlungsdaten in Österreich

Auch in Österreich gibt es Bestrebungen in dieser Richtung (Registerdaten, die sich aktuell in diversen Datenpools befinden für die Forschung zugänglich zu machen). Vor einigen Jahren gab es die Initiative, personenbezogenen Daten mit Steuer- und Einkommensdaten zu verknüpfen. Man muss jedoch vorsichtig sein – jegliche Verknüpfung von Daten muss mit der entsprechenden Datensicherung „ausgestattet" sein. Als Wissenschaftler interessiert man sich nicht über einzelnen Personendaten. In allen Fällen muss der Zugriff aber anonymisiert sein.

Anzahl von STRs

Es wird mich nicht wundern, wenn die Anzahl von Verdachtsmeldungen zwischen den Banken sehr unterschiedlich ist, da die Banken ja unterschiedliche Geschäftsbeziehungen, mit unterschiedlichen Ländern haben. Die Herkunft von kriminellen Geldern hängt unter anderen von der Größe der Volkswirtschaft (des Herkunftslandes), von dem Korruptionsniveau (des Herkunftslandes), vom Governance und von den institutionellen Rahmenbedingungen (des Herkunftslandes) ab. Wenn die Banken unterschiedliche Geschäftsbeziehungen in unterschiedlichen geografischen Räumen haben, die Wahrscheinlichkeit, dass sie (die Banken) unterschiedliche Anzahl von Verdachtsmeldungen melden, ist hoch. Ein wichtiger Aspekt ist natürlich die Kapazitäten der Banken: wann, was, wie gemeldet ist.

Die Rolle des Bargeldes

Ein Vorteil von so einem Datenpool ist, dass irgendwann, irgendwo das Geld wiederauftaucht (außer es wird gleich in Ausland transferiert). D.h. Bargeld ist ja, ein Bestandteil des Zahlungssystems, aber das Ausmaß der Verwendung vom Bargeld hängt wiederum von den Aktivitäten/Zielen der einzelnen Person ab (das Zahlen von kleineren Rechnungen vs. Geldschmuggel).
Mithilfe von statistischen Analysen möchte man eben die sog. „dunkeln Ziffern an Geldern“ schätzen. Die Idee ist, dass man auf Basis unterschiedlicher Kerngrößen/Kennzahlen schließen könnte, ob ein Geldstrom zu den definierten Kriterien passend ist oder „da muss es mehr geben“. Darüber hinaus könnte man in weiterer Folge Netzwerkanalysen durchführen (wo sich bestimmte Netzwerke bilden und wo man personelle oder räumliche Netzwerkentwicklungen abhängig den Geldströmen beobachten kann). Damit man kriminelles Geld oder Geld mit krimineller Herkunft waschen kann, braucht man Experten (Anwälte, Steuerberater, Banken, etc.), die dann das Geld tatsächlich waschen können. In so einem Fall spricht man von einem geschlossenen Netzwerk, das irgendwo organisiert ist.

Mag. Oliver Floth

Interview Partner	Mag. Oliver Floth Deputy head AML Erste Group Bank AG
Date	12.06.2018
Time	15:00 – 16:00
Language	German
Communication	In person

SARs/STRs/UTRs

In Österreich wird es versucht nur jene SARs zu melden, von denen tatsächlich geglaubt wird, dass sie inhaltlich wichtig ist. Die Anzahl der STRs sollte von den eingesetzten IT Systemen eher nicht grob fluktuieren. D. h., ein neues IT System generiert vielleicht bessere Treffer (im Kontext von Alarms), aber in Wirklichkeit der größte Vorteil von den neuen IT-Systemen ist, egal ob es um intelligentere Systeme (wie z. B. AI), dass die "false positives" reduziert werden. D. h., der Einsatz vom neuen IT-System kann zwar die Anzahl von Alarms (od. Alerts) reduzieren; die Anzahl der STRs an die FIU bleibt aber ungefähr gleich. Das Ziel von den IT Systemen ist eher diese: die Anzahl der "false positives" zu reduzieren, damit man sich auf jenen Fällen besser konzentrieren kann, die tatsächlich interessant sind.

Wichtigste Faktoren im Kampf gegen Geldwäscherei (IT, interne Prozesse, Mitarbeiter)

Die Mitarbeiter sind mindestens genauso wichtig wie die IT. Die IT Systeme sind wichtig, um Alerts zu entdecken. Aber, aus der Sicht der Kampf gegen Geldwäscherei oder Terrorismusfinanzierung, die wirklich spannenden Fälle werden normalerweise von den Mitarbeitern identifiziert. D. h., die Mitarbeiter sind die Ersten, die mitbekommen, wenn ein Kunde von denen ein ungewöhnliches Verhalten aufzeigt. Außerdem ist der regelmäßige Kontakt zu Kunden auch sehr wichtig (egal ob es sich um direkten Kontakt zu Unternehmen handelt, Informationen zum monatlichen Transaktionsverlauf, Informationen zu Änderungen des Geschäftszwecks oder Ähnliches). Der regelmäßige Kontakt zwischen den Kundenbetreuern und den Kunden bringt die Informationen, die man benötigt. Die Rolle des Kundenbetreuers ist somit sehr wichtig. Man kann das Ganze mit dem Begriff "Three lines of defence" bezeichnen, wobei das first line der Kundenbetreuer bzw. die Kundenbetreuerin ist. Der klassische KYC-Prozess erfordert das interne Ablegen von vielen Dokumenten. Der Kunde aber wirklich zu kennen – das tun die Kundenbetreuer. Daher, es ist essenziell, dass sichergestellt wird, dass es regelmäßig Schulungen gibt und dass der Kontakt zwischen Compliance und Kundenbetreuung aktiv ist. Man möchte den Kundenbetreuern zeigen und erklären, dass Compliance kein "Business Verhinderer" ist, sondern helfen möchte, gewisse Problematiken leichter zu identifizieren. Die größte Angst der Kundenbetreuer ist vielleicht, dass die Mitarbeiter Unwissenheit haben und somit eine objektive Einschätzung (zum Kundenverhalten oder zu bestimmten Transaktionen) schwierig ist. Wenn man aber die Kunden kennt, wenn es sich um ein plausibles Geschäft handelt, spricht es nichts dagegen, dieses Geschäft auch durchzuführen. Eine der wichtigsten Aufgaben von Compliance ist die Kundenbetreuer so zu unterstützen, sodass sie Verständnis (zum Thema Compliance) haben und in so einem Gebiet wie Compliance auch wohlfühlen.

Interne Organisation: Skills und Fähigkeiten der Mitarbeiter

Ein Mitarbeiter allein kann nicht alle wichtigsten Skills in sich vereinen. Man muss zwischen diversen Expertenbereichen unterscheiden. Die IT Skills sind natürlich ein wesentlicher Faktor, d. h. es gibt Mitarbeiter in der Geldwäsche-Abteilung, die im Endeffekt IT-Spezialisten sind und wissen was für die Finanzinstitution gefährlich ist (im Kontext von GW/TF). Sie

stellen auch sicher, dass im Hintergrund die IT Systemen funktionieren bzw. wenn es Änderungen oder Anfragen bzw. Wünsche gibt, wie das System neu kalibriert werden muss. Der nächste Expertenbereich ist zuständig für Sanktionen und Embargos - der Grund ist, dass die Sanktionen mit der Zeit komplizierter geworden sind. Früher waren es Personen oder Güter auf den Sanktionslisten, die überprüft worden sind und bei einem Treffer war relativ klar und eindeutig, was man machen kann und was nicht. Jetzt ist die Situation mit den Sanktionen sehr detaillierter und somit komplizierter geworden. Aktuell ist es so, dass man bspw. nur gewisse Geschäfte unter bestimmten Bedingungen machen darf. Wenn jemand sich damit nicht tagtäglich beschäftigt, ist es schwieriger sich mit dem Themaauseinanderzusetzen und sich gut genug auszukennen. Es gibt weitere Expertenbereiche, wie z. B. Mitarbeiter, die sich nur mit den gemeldeten Alerts beschäftigen und diese analysieren. Es gibt Mitarbeiter, deren Aufgaben sich eher auf der internen Organisation und Trainings fokussieren. Ganz wesentliche Aufgabe ist die Governance Funktion. Es wird versucht gewisse Standards für die gesamte Bankengruppe zu etablieren und um sicherzustellen, dass die Standards gefolgt werden, sind die Governance-Experten da.

Evaluierung eigener AML Politik

Rein von der IT-technischen Seite ist die Anzahl der Alerts eine wichtige Kennzahl (wie viele Alerts werden generiert, welche Szenarien wie viele Alerts generieren). Man versucht, natürlich, diese zu optimieren. Außerdem sind die Geschwindigkeit und der Aufwand auch wichtig, mit denen man die Alerts abarbeitet. Es wird genauer untersucht, wie viele SARs von den jeweiligen Einheiten gemeldet worden sind. Falls es ein Peak gibt, wird genauer hinterfragt und untersucht wieso. Wichtig ist zu erwähnen, dass bevor man bestimmte Sachen (Rules, Alerts, Szenarien, etc.) implementiert, diese vorher gut testen muss. D. h., man kann eine sehr gute Regel implementieren, die in Theorie sehr gut kling, wenn man aber sie testet, könnten als Ergebnis unzählige Alerts generiert werden, die schließlich nicht abgearbeitet werden könnten. Daher ist das Testing im Vorfeld ein wesentlicher Bestandteil, um die Qualität der Alerts beibehalten zu können. Verfügt man über unlimitierte Ressourcen, wäre man in der Lage sein, alle Transaktionen, die bestimmte Bedingungen erfüllen, zu überprüfen und genauer zu analysieren. Das würde aber in der Realität zu sehr viele Alerts führen, die man einfach nicht abarbeiten kann. Es ist wichtig zu erwähnen, dass man nicht bei jedem Alert den Kunden kontaktieren muss, weil ja bei bestimmten Transaktionen die Geschäftsbeziehung klar und plausibel ist. Ein Beispiel: ein österreichischer Konzern transferiert Geld zu einem anderen Konzern - bei so einer Transaktion braucht man die Kunden nicht sofort bzw. nicht jedes Mal kontaktieren.

Die Kosten für Compliance

Die Kosten für Compliance sind gestiegen und werden in der nahen Zukunft auch nicht weniger. Der Grund ist, dass die regulatorischen Anforderungen immer mehr werden. Je größer ein Finanzinstitut ist, desto größer ist der interne (AML) Apparat und desto höher sind die Compliance Kosten. Das wäre ein "barrier to entry" für Kleinbanken: die Kosten, die man hat und das Geld, das investiert werden muss, um die rechtlichen Anforderungen wirklich zu erfüllen, sind einfach sehr hoch. Umso kleiner eine Bank ist, umso "kostensensibler" ist sie. Deswegen gibt es verschiedene Modelle, bei denen Teile der KYC und Compliance Prozesse ausgelagert werden und das ist ein Grund, warum in letzter Zeit die FinTechs entstanden sind. Wenn z. B. eine kleine Bank alles Mögliche "screenen" oder z. B. "Online-Identifizierung" ermöglichen möchte, ist das einfach viel zu teuer und die Bank kann sich das einfach nicht leisten. In diesem Sinn können die FinTechs solche und andere Tätigkeiten von den kleineren Banken übernehmen. Die großen Banken können sich alle Tätigkeiten leisten, obwohl es kaum jemand gibt (von den Banken), der eine rein interne (d. h. in-house) IT Infrastruktur (d. h. SW und HW) aufgebaut hat. Außerdem es gilt: je höher die Anzahl von genutzten Core-

Systemen, desto schwieriger ist es diese zu synchronisieren.

Kommunikation mit A-FIU

Initial bekommt man das Feedback bzw. die Anforderung, das STR um bestimmte Informationen zu erweitern: z.B. Dokumente zu wirtschaftlicher Eigentümer, Historie von relevanten Transaktionen und andere Informationen. Die Mitarbeiter der A-FIU fragen meistens nach mehr Informationen, aber danach passiert relativ wenig und man erfährt selten, was dann tatsächlich passiert ist. Es wäre natürlich uninteressant zu wissen, was mit dem STR passiert ist, weil man dann extra Arbeit investiert, um eben alle notwendigen Informationen aufzubereiten. Meistens führt das zu Situationen, wenn eine Kundenbeziehung hinterfragt bzw. auch beendet wird. Es wäre dann natürlich schön zu wissen, ob die Arbeit, die die Compliance Mitarbeiter machen, auch Früchte trägt. In Österreich werden grundsätzlich eher wenig SARs geschickt. Man wird aber oft und genauer hinterfragt, wieso bestimmte Transaktion als verdächtigt oder auffällig beurteilt wurde, was sind die konkreten Gründe für das STR. In Österreich gab es in letzten Jahren wenige Fälle, wann Leute wegen Geldwäscherei auch verurteilt worden sind. Das kann man als "frustrierend" bezeichnen, da man eigentlich mehr meldet und wirklich davon ausgeht, dass es in vielen Fällen tatsächlich zu Geldwäscherei gekommen ist bzw. sich um Geldwäschefälle handelt.

De-risking vs. risk-based approach

Es ist klar, wie man mit Kunden und/oder Geschäften im Sanktionsbereich umgeht. In allen anderen Fällen muss man eine einfache "Kosten-Nutzen-Rechnung" machen; man muss sozusagen abwiegen, ob ein bestimmtes Geschäft oder Geschäft mit bestimmten Kunden rentabel ist (z. B. Großkunden mit Geschäftsbeziehungen nach einem Land mit höherer Risikoeinstufung). Man muss sich einfach folgende Frage stellen: ist es wirtschaftlich sinnvoll, wenn man sich immer wieder mit dieselben x Kunden tagtäglich beschäftigt und ihre tägliche Transaktionen analysiert - ist dieser Mehraufwand tatsächlich wirtschaftlich sinnvoll? Daher muss intern entschieden werden, ob bestimmte Risiken angenommen werden oder nicht. In Bereichen wie "Operationelles Risiko", "Geldwäsche" oder "Compliance" gibt es keine klare Regelung in diesem Kontext. Es wird immer mehr Richtung "Risk-Return Decision" gegangen. D. h. jede Bank muss entscheiden, ob bestimmte Geschäfte, die z. B. ein hohes Reputationsrisiko mit sich bringen, eigentlich eingegangen werden sollen. Zum Beispiel: es Gibt Geschäfte mit Großkunden (z. B. "Offshore"-Kunden), die rein-rechtlich keine "show stopper" sind, jedoch mit Reputationsrisiko zu tun haben. Rein rechtlich spricht es nichts dagegen, wenn man Geschäfte mit Offshore Großkunden macht und meistens steckt dahinter nichts Illegales. Aber, es existiert ein Reputationsrisiko. Man muss sich daher im Vorfeld fragen und entscheiden, ob dieses Risiko eingegangen wird oder nicht, weil es sich eben um einen Großkunden handelt oder man entscheidet sich nach dem Motto "dieses Reputationsrisiko ist viel zu groß für mich". Es ist deswegen wichtig, dem Management die Möglichkeit zu geben, eine auf Fakten basierende Entscheidung zu treffen.

Strafen für die Finanzinstitute wegen mangelhaftes AML

Man muss sehr stark unterscheiden, um was für Verfehlungen es sich handelt. Wenn z. B. der Personalausweis von einem bestimmten von der Revision ausgewählten Kunden abgelaufen ist, handelt sich meistens um einen Einzelfall, der man nie abstellen kann und da muss man vorsichtig sein, wie stark man das bestraft. Wenn es aber systematische Fälle gibt, bei denen man sagt, bspw. "ich mache kein Transaktionsscreening für wirtschaftliche Eigentümer" (wenn man bewusst aus unterschiedlichen Gründen auch immer die notwendigen Maßnahmen nicht umsetzt) - in diesem Fall müssen die Strafen härter sein. Erfolgt in so einem Fall keine harte Strafe, würde das ein schlechtes Zeichen für die anderen Banken sein, die diese Arbeit tun. Es gibt ein grundsätzliches Problem beim Compliance: wenn man lange alles richtig tun und nicht bestraft wird, kommt langsam der Schlendrian. D. h. man wird langsam betriebsblind. Aus

diesem Grund sind die Strafen wichtig, da man sich dadurch bspw. zweimal überlegt, ob ein bestimmtes Geschäft sich lohnt und ob so lukrativ wäre oder nicht.

Meinung zur rechtlichen Situation in Österreich

Das Problem der Geldwäsche, besonders das Problem der Terrorismusfinanzierung, ist ein (oder wird langsam zu einem) länderübergreifendes Problem. Das Thema Terrorismusfinanzierung ist sehr spezifisch, damit man alle Aspekte davon in einem einzigen Gesetz zu konsolidieren. Es wird geglaubt, dass es bei den Banken so viele Informationen gibt, sodass man Terrorismusaktivitäten alleine aufgrund des Zahlungsverhaltens identifizieren kann. Im Fall von Geldwäsche und Terrorismusfinanzierung wird man immer auf einer Seite das Strafrecht und auf der anderen - jene Gesetzte, die von verhaltungsrechtlicher Natur sind, haben.

Referenzmodell für CDD

Grundsätzlich muss man sagen, dass die gesetzlichen Vorgaben zu ca. 80% der Fälle und die Vorgehensweise bei verschiedenen Fällen definiert haben - PEPs, Treuhand Kunden, Kunden aus Drittländern mit hohem Risiko, etc. D. h. die gesetzlichen Vorgaben sind gegeben und werden von allen Banken umgesetzt. Bei den anderen 20% wäre es schwierig, diese zu vereinheitlichen. Der Grund dafür ist, dass heutzutage man in unterschiedlichen Ländern unterschiedliche Regelungen hat. Die lokalen Gegebenheiten kann man nicht ignorieren. Ein Beispiel: Für ein „Hochrisiko“ Land A wären Kunde vom selben Land keine „Hochrisiko“ Kunden sein. Und das ist auch in Ordnung so, sonst hätte man nur „Hochrisiko“ Kunden und daher kein richtiges Risikomodell. So wie der Regulator bspw. die Regelungen für „Hochrisiko“ Kunden definiert hat, ist in Ordnung. Aber, da die Geschäftsmodelle sehr unterschiedlich sind bzw. auch die Kundenstruktur sehr unterschiedlich sein kann, muss man sehr wohl verschiedenen Institutionen gewisse freie Hand geben, um selber zu beurteilen und wenn das nicht der Fall wäre, dann wäre auch die jährliche Risikoanalyse, die der Bank macht, sinnlos. Man hätte ein für alle Institute gleiches Risikomodell, das einmal nur kalibriert wird und mit dem man arbeitet.

Wieso muss man GW bekämpfen?

Die Idee und die Gründe für den Kampf gegen Geldwäscherei kann man aus der Geschichte ablesen. Man muss einfach sicherstellen, dass illegales Geld gestoppt wird und nicht ins Handel kommt. Dasselbe gilt für Terrorismusfinanzierung: man muss sicherstellen, dass die Terroristen keine Möglichkeiten haben, Geld frei zu transferieren - weil offensichtlich dahinter Straftaten geplant sind bzw. geplant werden. Die Idee, Gelder zu verfolgen und sie von den Verbrechern wegzunehmen - das ist eine uralte Idee.

MSc. Felix Timm

Interview Partner	MSc. Felix Timm Research assistant at the chair of Business Information Systems at the University of Rostock
Date	07.06.2018
Time	10:00-10:20
Language	German
Communication	Phone

Idee für das R-CO

Die große Vision und Motivation hinter dem R-CO ist ein gemeinsames Bild bzw. eine gemeinsame Grundlage zu schaffen, wie man die relevante Gesetzte praktisch umsetzt. Dieses gemeinsame Bild soll dann nicht nur die Finanzinstitute, sondern auch für den Gesetzgeber und für die Wirtschaftsprüfungsunternehmen relevant sein.

Vorgehensweise beim Entwickeln vom R-CO

Wir haben Zugang zu relativ breiter Datenbasis gekriegt und zusätzlich Gespräche mit GW Beauftragten von verschiedenen Finanzinstituten anonymisiert durchgeführt. Im Laufe des Projekts haben wir nicht nur die internen Abläufe, sondern auch die internen organisatorischen Strukturen analysiert. Das Ziel war ein Modell zu entwickeln, nicht nur auf Prozessbasis, sondern auch auf Basis der gesamten Unternehmensarchitektur.

Konkreter: Das Modell kann man als Ergebnis von durchgeführten Workshops zum Thema „Compliance“ und Interviews mit Experten aus den Finanzinstituten sehen.

Im Laufe des Projekts wurden folgende Daten erfasst und auf drei Ebenen abgebildet:

- Daten, die Einfluss auf der Risikobeurteilung von Kunden haben
- Benutzte IT-Systeme

Dabei wurden folgende drei Ebenen definiert:

- Geschäftsebene: welche Funktionen und Prozesse intern abgespielt werden
- Datenebene: welche Daten werden dazu genutzt
- IT Ebene: welche IT Bestandteile werden dafür genutzt

Einsatzmöglichkeiten vom R-CO

Die Einsatzmöglichkeiten vom Referenzenmodell hängen davon ab, wer das Modell eigentlich einsetzt und wer daran interessiert ist. Auf einer Seite hat man die Finanzinstitute - die haben ein sehr gutes Verständnis von den regulatorischen Anforderungen, auf der anderen: Es ist interessant auch zu wissen, wie die Finanzinstitute das Ganze („Compliance“) organisatorisch implementieren.

Daniel Thelesklaf

Interview Partner	Daniel Thelesklaf Director of the FIU of Liechtenstein, Chair of Moneyval and Member of the Egmont Committee
Date	-
Time	-
Language	German
Communication	Written Q&A

Die Anzahl der SARs/STRs/UTRs nimmt in den letzten Jahren europaweit zu. Einer der Hauptgründe dafür ist die Umsetzung der 4. ML EU-Richtlinie. Können Sie behaupten, dass die Finanzinstitute (unabhängig von ihrer Größe) mit zahlreichen Vorschriften und Verpflichtungen "überflutet" sind und wenn ja, welche Auswirkungen hat diese "Überflutung"? Glauben Sie, dass neben den nationalen Regelungen ein direkter Zusammenhang zwischen den internen Kernkompetenzen der Finanzinstitute und der Anzahl der gemeldeten SARs/STRs/UTRs zu den nationalen FIUs besteht? Oder die Finanzinstitute werde einfach immer vorsichtiger?

1. Ich kann die Sorgen wegen der "Überflutung" nachvollziehen, aber andererseits stiegen auch die
2. volkswirtschaftlichen Kosten von Kriminalität stark an. Der Anstieg der VM („Verdachtsmeldungen“
3. – Anm. d. Verf.) ist sicher auch auf die gesteigerten Erwartungen der Aufsichtsbehörden zurück zu
4. führen. Daneben spielt aber auch eine Rolle, dass dem Schutz der Diskretion des Kunden nicht
5. mehr die gleiche Rolle hat wie früher. Allerdings ist eine Steigerung der Anzahl der VM noch kein
6. Erfolg: entscheidend ist allein, was damit dann auch gemacht wird.

Die Kosten für Compliance steigen. Welche Auswirkungen (finanzielle und andere) haben bzw. können die zunehmende Zahl nationaler Regelungen auf die kleinen Finanzinstitute haben? Was könnten die "kleineren" Finanzinstitute tun, um die Kosten stabil zu halten und damit weiter wettbewerbsfähig zu sein?

7. Solange die Compliance-Kosten noch weit hinter den Boni für die Bankleitung zurückbleiben,
8. mache ich mir um das finanzielle Überleben der Banken keine Sorge. Richtig ist aber, dass
9. steigende Kosten aufgrund der economy of scales von großen Instituten besser "verdaut" werden
10. können als von kleinen. Wenn das mit den Kosten also wirklich stimmt, dann müsste es zu einem
11. Konzentrationsprozess kommen. In der Schweiz findet das ja bereits statt.

Bußgelder und Strafen: Glauben Sie, dass die Bußgelder und Strafen für fehlerhafte AML bei den Finanzinstituten in den letzten Jahren die gewünschten Auswirkungen hatten? Ist z.B. die Inhaftierung von Bankern eine angemessene Maßnahme (natürlich bei grober Verletzung der AML Regelungen und bewiesene absichtliche Vernachlässigung der AML Verpflichtungen)? Welche Auswirkungen würde so eine Maßnahme auf der Stabilität der Finanzmärkte haben?

12. Es geht nicht darum, möglichst viele Banker zu verhaften Das Risiko, für Geldwäsche
13. strafrechtlich zur Verantwortung gezogen zu werden ist immer noch verschwindend klein. Die
14. Strafverfolger müssen aber weit mehr als früher die Bekämpfung der GW zu einer Priorität
15. machen.

De-risking vs. risk-based approach: Die de-risking Vorgehensweise wird von den Finanzinstituten nach wie vor weitgehend gefolgt. Was sind Ihrer Meinung nach die wichtigsten Auswirkungen dieses Ansatzes? Es ist bekannt, dass das de-risking zu unerwünschten Effekten führt (alternative nicht-regulierte Transaktionen und Finanzdienstleistungen). Kann dies zu einer weiteren Erhöhung der Kriminalitätsrate und damit zu einer Situation führen, in der die Finanzinstitute mit einer Zunahme der Verdachtsfälle für GW zu kämpfen haben?

16. De-risking ist zwar eine verständliche Reaktion, aber es ist der falsche Ansatz. De-risking führt
17. letztlich zu einer Erhöhung der GW-Risiken, da es Teile des Geschäfts in den informellen, nicht
18. überwachten Sektor verdrängt. Eigentlich müsste de-risking ja zu einer Abnahme der VM

19. (zumindest der "de-riskenden" Bank) führen.

Unterschiede zwischen den Ansätzen im Kampf gegen GW in verschiedenen Ländern. In 2006 Prof. Brigitte Unger von der Universität Utrecht (Professorin für Finanzwissenschaft an der Universität Utrecht) schrieb Folgendes im Hinblick auf die Internationalität des Kampfes gegen GW: **"***the problem is that, despite harmonizing efforts at both European and international level, national legislations criminalizing money laundering continue to differ. Most countries have criminalized serious offences but have nevertheless, adopted different approaches to what constitutes a serious crime for the purpose of. Thus, the predicate offences that generate proceeds vary from one country to another.***"**

20. Ich halte diese noch bestehenden kleineren Unterschiede für ein akademisches Problem. In
21. der Praxis spielen nicht die Unterschiede im Strafrecht eine große Rolle, sondern die
22. unterschiedlichen Prioritäten der nationalen Behörden.

Internationale Barrieren. Was sind Ihrer Meinung nach die größten Hindernisse, die derzeit eine Belastung für den internationalen Kampf gegen ML darstellen?

23. Mangelnder Fokus der Aufsichtsbehörden auf GW; mangelnde Ausstattung und Kenntnisse
24. der Behörden in vielen Ländern; Korruption; fehlender politischer Wille.

Was ist aus Ihrer Sicht ein erfolgreiches AML-Framework (in einem Finanzinstitut)? Was sollte der Fokus eines solchen AML-Frameworks sein: zahlreiche erfahrene Mitarbeiter, ein zuverlässiges Software-Kernsystem, gut dokumentierte interne Prozesse, andere?

25. Eine gute Mischung aus Allem.

Warum sollten die Länder die Geldwäsche bekämpfen? Neben den historischen Gründen, welche anderen Faktoren sollten heutzutage im Hinblick auf die Gründe für den Kampf gegen GW berücksichtigt werden.

26. Wer GW nicht bekämpft befördert Kriminalität.

Glauben Sie, dass die Finanzinstitute ein gemeinsames Framework (ein Referenzmodell) für den Kampf gegen ML brauchen? Oder muss jedes Finanzinstitut seine Verpflichtungen auf seine Art und Weise erfüllen?

27. Ich denke es wird zu mehr Gemeinsamkeiten kommen und das ist auch gut so.

Appendix II: Questionnaire

The following questionnaire is based on the Wolfsberg Principles for AML/CDD internal assessment and other resources[476] and was developed by Ilian Berov, a student at the Vienna University of Technology, to support the evaluation process in the context of AML/CDD as part of his master's thesis. All data and information will be treated confidentially, appropriately secured, not published and only analysed for the purposes of the evaluation.*

Ilian Berov
ilian.berov@gmail.com
+ 43 699 116 575 262
May 2018

AML/CDD Questionnaire	
I. Overview	
1. Number of employees (2018)	
2015	
2. Number of employees Compliance/AML (2015)	
3. Number of cash and non-cash transactions yearly (2015)	
4. Detected suspicious/unusual account activity (2015)	
5. Number of **forwarded** cases to Geldwäschemeldestelle (2015)	
6. Number of **confirmed** fraud and/or money laundering cases (2015)	
7. Number of Applications (Software tools, Services, Third-Party Sources, etc.) used to support the internal AML policy (2015)	
8. Number of internal AML/CTF trainings (2015)?	
Key events in the context of the internal AML policy in 2015: no change since 2014, optimization of the internal processes, use of a new AML software and tools, re-assessment of the internal risk- and control-policy, re-organisation, other improvements or deterioration compared to 2014?	
2016	
9. Number of employees Compliance//AML (2016)	
10. Number of cash and non-cash transactions yearly (2016)	
11. Detected suspicious/unusual account activity (2016)	
12. Number of **forwarded** cases to Geldwäschemeldestelle (2016)	

[476] Questionnaires from London Stock Exchange Group (https://www.lseg.com/), Maybank (http://www.maybank.com/) and Cimb Bank (https://www.cimbbank.com)

13. Number of **confirmed** fraud and/or money laundering cases (2016)	
14. Number of Applications (Software tools, Services, Third-Party Sources, etc.) used to support the internal AML policy (2016)	
15. Number of internal AML/CTF trainings (2016)?	
Key events in the context of the internal AML policy in 2016: no change since 2015, optimization of the internal processes, use of a new AML software and tools, re-assessment of the internal risk- and control-policy, re-organisation, other improvements or deterioration compared to 2015?	
2017	
16. Number of employees Compliance/AML (2017)	
17. Number of cash and non-cash transactions yearly (2017)	
18. Detected suspicious/unusual account activity (2017)	
19. Number of **forwarded** cases to Geldwäschemeldestelle (2017)	
20. Number of **confirmed** fraud and/or money laundering cases (2017)	
21. Number of Applications (Software tools, Services, Third-Party Sources, etc.) used to support the internal AML policy (2017)	
22. Number of internal AML/CTF trainings (2017)?	
Key events in the context of the internal AML policy in 2017: no change since 2016, optimization of the internal processes, use of a new AML software and tools, re-assessment of the internal risk- and control-policy, re-organisation, other improvements or deterioration compared to 2016?	

II. General AML/CTF Practices:	Yes	No
23. Has your institution been subjected to sanctions or punitive actions in relation to AML/CFT by the regulators/law enforcer in the past five years?	☐	☐
24. Does your institution have an appointed senior officer responsible for your institution's day to day AML/CFT-program?	☐	☐
25. Has your institution been subjected to inspection by the regulator? If yes, please provide the last date of inspection.	☐	☐
26. In addition to inspection by the regulator, does your institution have an internal audit and compliance function or other independent third party to monitor and review the effectiveness of the AML/CFT policy and compliance program on a regular basis?	☐	☐
27. Does your institution's AML/CFT policies and procedures apply to all your branches and subsidiaries both in the home country and in locations outside of your home country?	☐	☐

III. AML/CTF Policies, Practices and Procedures:	Yes	No
28. Has your institution developed written AML/CFT policy and procedures, approved by the Board covering the following:	☐	☐
a. establishing the true identity of customers and beneficial owners, collecting and recording sufficient information on the customers;	☐	☐
b. screening customers and transactions against sanction lists issued by competent authorities/international bodies; If so, please select the particular Sanction list(s) that are used in your AML program and state how frequent the screening is conducted (for new and for existing customer): ☐ UN ☐ FMA ☐ OFAC ☐ Others: …….. ☐ EU **Frequency**	☐	☐
c. prohibiting accounts/relationships with shell banks/anonymous accounts;	☐	☐
d. conducting the appropriate customer due diligence on politically exposed persons (PEPs), reliance on intermediaries, beneficiary accounts, non-face-to-face business relationships, higher risk customers and existing customers;	☐	☐
e. detection, monitoring and reporting of suspicious transactions to authorities;	☐	☐
f. record retention procedures that comply with applicable laws;	☐	☐
g. risk based assessment of its customers and to conduct the appropriate level of customer due diligence;	☐	☐
h. the roles and responsibilities of key personnel in relation to anti-money laundering and anti- terrorism financing compliance.	☐	☐
29. Does your institution follow FATF recommendations on money laundering and terrorist financing?	☐	☐
30. How frequent does your institution screen its existing customer database?		
31. Does your institution provide services to Offshore Banks, Internet Banking based institutions or banks located in high risk areas as highlighted by FATF?	☐	☐
32. Has your institution developed an Internal Audit function in order to test the system for prevention of ML/TF and reviews your institution's AML/CFT Compliance policy and program? If yes, how frequently?	☐	☐

IV. Transaction Monitoring:	Yes	No
33. Does your institution have a monitoring program for unusual and potentially suspicious activity that covers funds transfers and monetary instruments such as travelers checks, money orders, etc.?	☐	☐
VI. AML/CTF Training	Yes	No
34. Does your institution provide AML/CTF training to relevant employees that includes: • Identification and reporting of transactions that must be reported to government authorities. • Examples of different forms of money laundering involving the institution's products and services. • Internal policies to prevent money laundering.	☐	☐
35. Does your institution employ third parties to carry out some of the AML functions of the institution? If so, does your institution provide AML/CTF training to relevant third parties, that includes: • Identification and reporting of transactions that must be reported to government authorities. • Examples of different forms of money laundering involving the institution's products and services. • Internal policies to prevent money laundering.	☐	☐

Space for additional information and comments:

(Please indicate which question the information is referring to.)

Bibliography

(Gesetzentwurf) Bundesgesetz, mit dem das Bundesgesetz über die Erbringung von Zahlungsdiensten 2018 erlassen wird (ZaDiG 2018), Fassung vom 25.06.2018. (2018). BgBl. I Nr. 17/2018. Retrieved June 25, 2018, from https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00011/fname_679293.pdf

(Gesetzentwurf) Strafprozessrechtsänderungsgesetz 2014. (2014). *Bundesgesetz, mit dem die Strafprozessordnung 1975, das Jugendgerichtsgesetz 1988, das Suchtmittelgesetz, das Staatsanwaltschaftsgesetz, das Geschworenen- und Schöffengesetz 1990 und das Gebührenanspruchsgesetz geändert werden*. 38/ME. Retrieved June 27, 2018, from https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00038/imfname_349181.pdf

ACAMS Today. (2017, June 9). *Artificial Intelligence: The Implications of False Positives and Negatives*. Retrieved June 7, 2018, from ACAMS Today: https://www.acamstoday.org/artificial-intelligence-the-implications-of-false-positives-and-negatives/

ACAMS Today. (2017, March 6). *De-Risking and Financial Inclusion*. Retrieved June 9, 2018, from ACAMS Today: https://www.acamstoday.org/de-risking-and-financial-inclusion/

Accenture. (2017, September 22). *Leveraging machine learning within anti-money laundering transaction monitoring.* Retrieved June 26, 2018, from Accenture: https://www.accenture.com/_acnmedia/PDF-61/Accenture-Leveraging-Machine-Learning-Anti-Money-Laundering-Transaction-Monitoring.pdf

addendum. (2017, October 10). *Wien als Drehscheibe für Terror-Gelder*. Retrieved June 9, 2018, from addendum: https://www.addendum.org/terrorismus/terrorismus-finanzierung/

Aite Group. (2014). *Global AML Vendor Evaluation: Managing Rapidly Escalating Risk.* Retrieved June 28, 2018, from https://narrativescience.com/DesktopModules/EasyDNNNews/DocumentDownload.ashx?portalid=0&moduleid=2058&articleid=80&documentid=60

Alldridge, P. (2013). *Forfeiture, Confiscation, Civil Recovery, Criminal Laundering and Taxation of the Proceeds of Crime* (1 ed.). Hart Publishing.

Anti-Money Laundering Forum. (2009, November). *History of the European Union Anti-Money Laundering and Financing of Terrorism Directives*. Retrieved June 8, 2018, from Anti-Money Laundering Forum: https://www.anti-moneylaundering.org/Europe.aspx

Arnold, M. (2018, April 9). HSBC brings in AI to help spot money laundering. *Financial Times*. Retrieved May 8, 2018, from https://www.ft.com/content/b9d7daa6-3983-11e8-8b98-2f31af407cc8

Association of Certified Anti-Money Laundering Specialists (ACAMS). (2012). *Study Guide for the CAMS Certification Examination (Fifth Edition).* Miami, USA.

Bedi, R. (2010, January). *The Future of AML/CFT – Technology, Data, People.* Retrieved June 9, 2018, from National University of Singapore: http://www.nus.edu.sg/sawcentre/docs/future-aml_edit.pdf

Benson, P. R. (2009, July). *Meeting the requirements of ISO 8000.* Retrieved June 26, 2018, from Massachusetts Institute of Technology: http://mitiq.mit.edu/IQIS/Documents/CDOIQS_200977/Papers/01_05_T2C.pdf

Bernasconi, P. (1988). *Finanzunterwelt. Gegen Wirtschaftskriminalität und organisiertes Verbrechen.* Zürich / Wiesbaden: Orell Füssli Verlag.

BIS Research. (2017). *Global Anti Money Laundering (AML) Software Market - Analysis and Forecast (2017-2023)*. Retrieved June 26, 2018, from BIS Research: https://bisresearch.com/industry-report/global-anti-money-laundering-software-market-2023.html

BMDW (Bundesministerium für Digitalisierung und Wirtschaftsstandort). (2018). (Begutachtungsentwurf) Risikobewertungsausnahmeverordnung - RAV, Fassung vom

26.06.2018. *Vereinfachte wirkungsorientierte Folgenabschätzung*. Retrieved June 26, 2018, from https://www.ris.bka.gv.at/Dokumente/Begut/BEGUT_COO_2026_100_2_1518640/BEGUT_COO_2026_100_2_1518640.pdf

Bongard, K. (2001). *Wirtschaftsfaktor Geldwäsche.* Deutscher Universitätsverlag, Wiesbaden. doi:https://doi.org/10.1007/978-3-322-81052-6

Brocke, J. v. (2015). *Referenzmodellierung: Gestaltung und Verteilung von Konstruktionsprozessen.* Logos Verlag Berlin.

Bundesgesetz betreffend ergänzende Regelungen zur Durchführung des Zollrechts der Europäischen Gemeinschaften (Zollrechts-Durchführungsgesetz - ZollR-DG), Fassung vom 25.06.2018. (1994). BGBl. Nr. 659/1994. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004913

Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG), Fassung vom 25.06.2018. (1993). BGBl. Nr. 532/1993. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004827

Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG), Fassung vom 31.12.2016. (2016, December 31). BGBl. Nr. 532/1993. Retrieved June 20, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004827&FassungVom=2016-12-31

Bundesgesetz über den Betrieb und die Beaufsichtigung der Vertragsversicherung (Versicherungsaufsichtsgesetz 2016 – VAG 2016), Fassung vom 31.12.2016. (2016, December 31). BGBl. I Nr. 34/2015. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009095&FassungVom=2016-12-31

Bundesgesetz über die Ausgabe von E-Geld und die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten (E-Geldgesetz 2010), Fassung vom 25.06.2018. (2010). BGBl. I Nr. 107/2010. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007043&Artikel=&Paragraf=14&Anlage=&Uebergangsrecht=

Bundesgesetz über die Beaufsichtigung von Wertpapierdienstleistungen (Wertpapieraufsichtsgesetz 2007 – WAG 2007), Fassung vom 31.12.2016. (2016, December 31). BGBl. I Nr. 60/2007. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20005401&FassungVom=2016-12-31

Bundesgesetz über die Bilanzbuchhaltungsberufe (Bilanzbuchhaltungsgesetz 2014 – BiBuG 2014), § 43, Fassung vom 20.06.2018. (2013). BGBl. I Nr. 191/2013. Retrieved June 20, 2018, from https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008571&Artikel=&Paragraf=43

Bundesgesetz über die Durchführung internationaler Sanktionsmaßnahmen (Sanktionengesetz 2010 – SanktG), Fassung vom 25.06.2018. (2010). BGBl. I Nr. 36/2010. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006805

Bundesgesetz über die Einrichtung eines Registers der wirtschaftlichen Eigentümer von Gesellschaften, anderen juristischen Personen und Trusts (Wirtschaftliche Eigentümer Registergesetz – WiEReG), Fassung vom 05.08.2018. (n.d.). BGBl. I Nr. 136/2017. Retrieved August 5, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009980

Bundesgesetz über die Einrichtung und Organisation des Bundeskriminalamtes (Bundeskriminalamt-Gesetz – BKA-G), Fassung vom 25.06.2018. (2002). BGBl. I Nr. 22/2002. Retrieved June 25, 2018, from

https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001745

Bundesgesetz über die Erbringung von Zahlungsdiensten 2018 (Zahlungsdienstegesetz 2018 – ZaDiG 2018), Fassung vom 06.10.2019. (2018). BGBl. I Nr. 17/2018. Retrieved October 6, 2019, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010182

Bundesgesetz über die internationale polizeiliche Kooperation (Polizeikooperationsgesetz – PolKG), Fassung vom 25.06.2018. (1997). BGBl. I Nr. 104/1997. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10006019

Bundesgesetz über die polizeiliche Kooperation mit den Mitgliedstaaten der Europäischen Union und der Agentur der EU für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol), (EU – Polizeikooperationsgesetz, EU-PolKG), Fassung vom 25.06.2018. (2009). BGBl. I Nr. 132/2009. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006630

Bundesgesetz über die Wirtschaftstreuhandberufe (Wirtschaftstreuhandberufsgesetz 2017 – WTBG 2017), Fassung vom 20.06.2018. (2017). BGBl. I Nr. 137/2017. Retrieved June 20, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009983

Bundesgesetz über die zusätzliche Beaufsichtigung der Kreditinstitute, Versicherungsunternehmen und Wertpapierfirmen eines Finanzkonglomerats (Finanzkonglomerategesetz - FKG), Fassung vom 26.06.2018. (2004). BGBl. I Nr. 70/2004. Retrieved June 26, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003448

Bundesgesetz über Privatstiftungen (Privatstiftungsgesetz–PSG), Fassung vom 05.08.2018. (n.d.). BGBl. Nr. 694/1993. Retrieved August 5, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10003154

Bundesgesetz vom 22. Oktober 1969 über die Verwahrung und Anschaffung von Wertpapieren (Depotgesetz), Fassung vom 25.06.2018. (1969, October 22). BGBl. Nr. 424/1969. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002142

Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB), § 165, Fassung vom 20.06.2018. (2017, September 1). BGBl. I Nr. 117/2017. Retrieved 20 June, 2018, from https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296&Artikel=&Paragraf=165&Anlage=&Uebergangsrecht=

Bundesgesetz vom 26. Juni 1958, betreffend das Finanzstrafrecht und das Finanzstrafverfahrensrecht (Finanzstrafgesetz - FinStrG.), Fassung vom 25.06.2018. (1958, June 26). BGBl. Nr. 129/1958. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10003898

Bundesgesetz vom 28. November 1989 zur Regelung des Glücksspielwesens (Glücksspielgesetz – GSpG), über die Änderung des Bundeshaushaltsgesetzes und über die Aufhebung des Bundesgesetzes betreffend Lebensversicherungen mit Auslosung, Fassung vom 25.06.2018. (1989, November 28). Retrieved from https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004611&FassungVom=2018-06-25&Artikel=&Paragraf=31c&Anlage=&Uebergangsrecht=

Bundesgesetz vom 7. Juli 1988 über die Besteuerung des Einkommens von Körperschaften (Körperschaftsteuergesetz 1988 – KStG 1988), § 13, Fassung vom 25.06.2018. (1988, July 7). BGBl. Nr. 401/1988. Retrieved from

https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004569&Artikel=&Paragraf=13

Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), Fassung vom 23.09.2019. (2018). BGBl. I Nr. 111/2018. Retrieved September 23, 2019, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536

Bundesgesetz zur Verhinderung der Geldwäscherei und Terrorismusfinanzierung im Finanzmarkt (Finanzmarkt-Geldwäschegesetz – FM-GwG), Fassung vom 25.06.2018. (2016). BGBl. I Nr. 118/2016. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009769

Bundesgesetz, mit dem das Alternative Investmentfonds Manager-Gesetz – AIFMG erlassen wird, Fassung vom 25.06.2018. (2013). BGBl. I Nr. 135/2013. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008521

Bundesgesetzblatt für die Republik Österreich, ausgegeben am 30. Juli 1993. (1993, Juli 30). BGBl. Nr. 527/1993. Retrieved June 20, 2018, from https://www.ris.bka.gv.at/Dokumente/BgblPdf/1993_527_0/1993_527_0.pdf

Bundesgesetzblatt für die Republik Österreich, Teil I. (2017, Juli 26). Retrieved June 25, 2018, from https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_107/BGBLA_2017_I_107.html

Bundeskrimimalamt Österreich. (2018, February 14). *Hinweise zur Einbringung sowie der Bearbeitung durch die Geldwäschemeldestelle.* Retrieved June 25, 2018, from Bundeskrimimalamt Österreich: https://bundeskriminalamt.at/308/files/Geldwaeschemeldung_Info.pdf

Bundeskriminalamt Deutschland. (2017). *Financial Intelligence Unit Deutschland: Jahresbericht 2016.* Bundeskriminalamt Deutschland, Zentralstelle für Verdachtsmeldungen, Wiesbaden. Retrieved June 22, 2018, from https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/FIU/Jahresberichte/fiuJahresbericht2016.pdf?__blob=publicationFile&v=6

Bundeskriminalamt Österreich. (2016). *Geldwäsche Jahresbericht.* Retrieved May 2018, from Bundeskriminalamt Österreich: http://www.bmi.gv.at/cms/BK/publikationen/files/Geldwschebericht_2016_WEB.pdf

Bundeskriminalamt Österreich. (2017). *Geldwäsche Jahresbericht.* Retrieved September 2019, from Bundeskriminalamt Österreich: https://bundeskriminalamt.at/308/files/Geldwaesche_17_web.pdf

Bundesministerium für Finanzen. (2016). *Veröffentlichung von Statistiken gemäß Artikel 44 Abs. 3 der 4. Geldwäsche-Richtlinie.* Retrieved June 8, 2018, from Bundesministerium für Finanzen: https://www.bmf.gv.at/finanzmarkt/geldwaesche-terrorismusfinanzierung/AT_AML-CFT_data_Art._44_of_4AMLD.xlsx

Bundesministerium für Finanzen in Zusammenarbeit mit den zuständigen Ministerien und Behörden. (2015-2016). *Nationale Risikoanalyse Österreich.* Retrieved June 26, 2018, from https://www.bmf.gv.at/finanzmarkt/geldwaesche-terrorismusfinanzierung/Nationale_Risikoanalyse_Oesterreich_PUBLIC.pdf

CaseWare Analytics. (2016, March 17). *Bank Fined Millions for AML Compliance Failures*. Retrieved June 8, 2018, from CaseWare Analytics: https://www.casewareanalytics.com/blog/bank-fined-millions-aml-compliance-failures

CaseWare Analytics. (2017, January). *Trying to find the right AML software? Here's what you should consider*. Retrieved June 26, 2018, from CaseWare Analytics: https://www.casewareanalytics.com/blog/trying-find-right-aml-software-here%E2%80%99s-what-you-should-consider

CEB. (2013, October). *Anti-Money Laundering: Technology Abstract.* Retrieved June 26, 2018, from CEB: https://www.scribd.com/document/165605842/AMLReport

CEB. (2016, February). *Combatting Rising Threats with Aging Infrastructure.* Retrieved June 26, 2018, from CEB: https://www.baesystems.com/en/cybersecurity/download-csai/resource/uploadFile/1434592077284

Celent. (2016, August 21). *Artificial Intelligence in KYC-AML: Enabling the Next Level of Operational Efficiency*. Retrieved June 7, 2018, from Celent: https://www.celent.com/insights/567701809

Chohan, U. W. (2017, August 25). *Cryptocurrencies: A Brief Thematic Review.* doi:https://dx.doi.org/10.2139/ssrn.3024330

Competitive Enterprise Institute. (2001, May 5). *Why the War on Money Laundering Should be Aborted.* Retrieved June 6, 2018, from Competitive Enterprise Institute: https://cei.org/outreach-regulatory-comments-and-testimony/why-war-money-laundering-should-be-aborted

Correia, C. (2015, October 8). *False positives: a growing headache*. Retrieved from The Global Treasurer: https://www.theglobaltreasurer.com/2015/10/08/false-positives-a-growing-headache/

Coucil of Europe. (1990, November 8). *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.* Retrieved June 25, 2018, from https://rm.coe.int/168007bd23

Der Standard. (2018, March 30). *Raiffeisen International fasst 2,7 Millionen Euro Strafe aus*. Retrieved June 7, 2018, from Der Standard: https://derstandard.at/2000077101697/2-748-Mio-Euro-Geldstrafe-fuer-Raiffeisen-International

Devisengesetz 2004, Fassung vom 25.06.2018. (2003). BGBl. I Nr. 123/2003. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003062

Die Presse. (2016, September 23). *Was Banken (nicht) gegen Geldwäsche tun.* Retrieved June 8, 2018, from Die Presse: https://diepresse.com/home/wirtschaft/international/5090622/Was-Banken-nicht-gegen-Geldwaesche-tun

Dorfleitner, G., Hornuf, L., Schmitt, M., & Weber, M. (2017). *FinTech in Germany.* Springer International Publishing. doi:https://doi.org/10.1007/978-3-319-54666-7

Dudovskiy, J. (2014). *Deductive Approach (Deductive Reasoning)*. Retrieved June 26, 2018, from https://research-methodology.net/research-methodology/research-approach/deductive-approach-2/#_ftn1

Eckelsberger, G., Sim, P., & Florian, S. (2017, April 4). *Moskau–London–Gänserndorf*. Retrieved May 11, 2018, from Dossier: https://www.dossier.at/dossiers/geldwaesche/moskau-london-gaenserndorf/

Encyclopaedia Britannica. (2018, June 26). *Hezbollah*. Retrieved June 26, 2018, from Encyclopaedia Britannica: https://www.britannica.com/topic/Hezbollah

European Central Bank. (2016, May 4). Press Release: ECB ends production and issuance of €500 banknote. Retrieved June 20, 2018, from https://www.ecb.europa.eu/press/pr/date/2016/html/pr160504.en.html

European Central Bank. (2017, February). *List of monetary financial institutions and institutions subject to minimum reserves and list of monetary financial institutions in the acceding countries.* Retrieved May 18, 2018, from European Central Bank: https://www.ecb.europa.eu/pub/pdf/other/mfilist-200702en.pdf?d4d33f0c77592764fc0e44d728fe6933

European Commission. (2016). *Monitoring implementation of EU directives.* Retrieved June 25, 2018, from https://ec.europa.eu/info/law/law-making-process/applying-eu-law/monitoring-implementation-eu-directives_en

European Union External Action. (2018, June 26). *Consolidated list of sanctions*. Retrieved June 26, 2018, from European Union External Action: https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions

EUROPOL. (2015, May 12). *Large Chinese Money Laundering Network Dismantled*. Retrieved June 25, 2018, from EUROPOL: https://www.europol.europa.eu/newsroom/news/large-chinese-money-laundering-network-dismantled

EUROPOL. (2016, February 17). *Directors of Chinese bank arrested in Spain in money laundering probe*. Retrieved June 25, 2018, from EUROPOL: https://www.europol.europa.eu/newsroom/news/directors-of-chinese-bank-arrested-in-spain-in-money-laundering-probe

EUROPOL. (2017). *From Suspicion to Action.* doi:https://doi.org/10.2813/308061

Ferguson, A. (n.d.). *Money Laundering.* Retrieved 05 02, 2018, from The Organization of American States: http://www.cicad.oas.org/apps/Document.aspx?Id=3095

Fiedler, I., Krumma, I., Zanconato, U. A., McCarthy, K. J., & Reh, E. (2017). *Das Geldwäscherisiko verschiedener Glücksspielarten.* Springer Gabler, Wiesbaden. doi:https://doi.org/10.1007/978-3-658-16625-0

Financial Conduct Authority. (2017, March 31). *New technologies and anti-money laundering compliance.* Retrieved June 8, 2018, from Financial Conduct Authority: https://www.fca.org.uk/publication/research/new-technologies-in-aml-final-report.pdf

Financial Intelligence Unit - Nederland. (2014). *Annual Report 2014: FIU-the Netherlands.* Retrieved June 26, 2018, from Financial Intelligence Unit - Nederland: https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/5276-fiu_jaaroverzicht_2014-engelsweb2.pdf

Financial Service Authority. (2016, August 25). *Automated Anti-Money Laundering Transaction Monitoring Systems.* Retrieved June 26, 2018, from Financial Service Authority: https://www.fca.org.uk/publication/archive/fsa-aml-systems.pdf

Finanzmarktaufsichtsbehörde (FMA). (2011-2012). *FMA Circulars on prevention of Money Laundering & Terrorism Funding.* Retrieved June 7, 2018, from Finanzmarktaufsichtsbehörde (FMA): https://www.fma.gv.at/en/fma/fma-circulars/#58

Finanzmarktaufsichtsbehörde (FMA). (2012, April). *FMA Circular on the Anti-Money Laundering Officer.* Retrieved June 26, 2018, from Finanzmarktaufsichtsbehörde (FMA): https://www.fma.gv.at/download.php?d=1600

Finanzmarktaufsichtsbehörde (FMA). (2017). *Financial Markets Anti-Money Laundering Act (Finanzmarkt-Geldwäschegesetz (FM-GwG)).* Retrieved May 15, 2018, from Finanzmarktaufsichtsbehörde (FMA): https://www.oekb.at/dam/jcr:aca4a107-79ad-4736-8ab8-9082db60076d/OeKB-FMGwG-I118-2016-en.pdf

Finanzmarktaufsichtsbehörde (FMA). (2018). *FinTech-Navigator*. Retrieved June 8, 2018, from Finanzmarktaufsichtsbehörde (FMA): https://www.fma.gv.at/querschnittsthemen/fintech/fintech-navigator/

Finanzmarktaufsichtsbehörde (FMA). (2018, May 8). *FMA Guide on ICT Security in Credit Institutions.* Retrieved June 7, 2018, from Finanzmarktaufsichtsbehörde (FMA): https://www.fma.gv.at/download.php?d=3371

Finanzmarktaufsichtsbehörde (FMA). (2018, March). *FMA-Rundschreiben Risikoanalyse zur Prävention von Geldwäscherei und Terrorismusfinanzierung.* Retrieved June 27, 2018, from Finanzmarktaufsichtsbehörde (FMA): https://www.fma.gv.at/download.php?d=3332

Finanzmarktaufsichtsbehörde (FMA). (2018). *The role of the various authorities and institutions in Austria*. Retrieved June 25, 2018, from Finanzmarktaufsichtsbehörde (FMA): https://www.fma.gv.at/en/cross-sectoral-topics/prevention-of-money-laundering-terrorist-financing/the-role-of-the-various-authorities-and-institutions-in-austria/

Frey, E. (2008, July 4). Nine jailed over Bawag bank fraud. *Financial Times*. Retrieved May 11, 2018, from https://www.ft.com/content/1403e252-49ef-11dd-891a-000077b07658

G7 Paris Summit. (1990, July 16). *Economic Declaration.* Retrieved June 25, 2018, from http://www.g8.utoronto.ca/summit/1989paris/communique/index.html

Gajewski, T. (2004, January). *Referenzmodell zur Beschreibung der Geschäftsprozesse von After-Sales-Dienstleistungen unter besonderer Berücksichtigung des Mobile Business.* Retrieved

June 26, 2018, from Universität Paderborn, Heinz Nixdorf Institut: https://www.hni.uni-paderborn.de/publikationen/publikationen/?tx_hnippview_pi1%5Bpublikation%5D=7785&tx_hnippview_pi1%5Bfelder%5D%5Blade%5D=2019

Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG). (1992, Juli 15). BGBl. I Nr. 34/1992. Retrieved June 20, 2018, from http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl192s1302.pdf

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Fassung vom 26.06.2018. (2015, July 17). BGBl. I Nr. 31/2015. Retrieved June 26, 2018, from http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf

Gessler, R. (2014). *Entwicklung Eingebetteter Systeme.* Springer Vieweg, Wiesbaden. doi:https://doi.org/10.1007/978-3-8348-2080-8

Gewerbeordnung 1994, § 365n, Fassung vom 20.06.2018. (1994). BGBl. Nr. 194/1994. Retrieved June 20, 2018, from https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10007517&Artikel=&Paragraf=365n&Anlage=&Uebergangsrecht=

Hammer, M., & Champy, J. (1994). *Business Reengineering – Die Radikalkur für das Unternehmen.* Campus Verlag Frankfurt.

Hansen, Hans Robert; Mendling, Jan; Neumann, Gustaf. (2015). *Wirtschaftsinformatik.* De Gruyter Oldenbourg.

Harris, K. (2016, August). *Implementing an effective Anti-Money Laundering System.* Retrieved June 26, 2018, from ACAMS: http://files.acams.org/pdfs/2016/Implementing_an_Effective_Anti-Money_Laundering_System_K_Harris.pdf

Hilzenrath, D. S. (1999, October 28). *Tiny Island Shelters Huge Cash Flows.* Retrieved October 3, 2019, from Washington Post: https://www.washingtonpost.com/wp-srv/WPcap/1999-10/28/057r-102899-idx.html?

Hitt, J. (2000, December 10). *The Billion-Dollar Shack.* Retrieved May 8, 2018, from The New York Times Magazine: https://www.nytimes.com/2000/12/10/magazine/the-billion-dollar-shack.html?pagewanted=1&_ga=2.247849223.1828965103.1525703032-900460161.1525703032

Hufnagel, S. (2004). *Der Strafverteidiger unter dem Generalverdacht der Geldwäsche gemäß § 261 StGB: eine rechtsvergleichende Darstellung (Deutschland, Österreich, Schweiz und USA).* Tenea Verlag Ltd.

Hughes, J. R. (2017, October 5). *The Importance of Incorporating Data Privacy into Anti-Money Laundering and Anti-Corruption Compliance Programs.* Retrieved June 26, 2018, from ACAMS: http://files.acams.org/pdfs/2017/The_Importance_of_Incorporating_Data_Privacy_J.Hughes.pdf

International Compliance Association. (2018). *International Compliance Association*. Retrieved May 9, 2018, from What is money laundering?: https://www.int-comp.org/careers/a-career-in-aml/what-is-money-laundering/

International Money Fund (IMF). (2011, November). *Anti-Money Laundering/Combating the Financing of Terrorism - Topics.* Retrieved June 26, 2018, from International Money Fund (IMF): https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm

International Money Fund. (1998, February 10). *Money Laundering: the Importance of International Countermeasures--Address by Michel Camdessus*. Retrieved June 26, 2018, from International Money Fund: https://www.imf.org/en/News/Articles/2015/09/28/04/53/sp021098

Interpol. (2018). *Money Laundering*. Retrieved June 25, 2018, from https://www.interpol.int/Crime-areas/Financial-crime/Money-laundering

Intra-governmental Group on Geographic Information (IGGI). (2012, November). *The Principles of Good Data Management.* Retrieved June 26, 2018, from Intra-governmental Group on Geographic Information (IGGI): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/14867/Good_dataMan.pdf

IRS. (2018). *Statistical Data - Money Laundering & Bank Secrecy Act (BSA)*. Retrieved June 26, 2018, from IRS: https://www.irs.gov/compliance/criminal-investigation/statistical-data-money-laundering-bank-secrecy-act-bsa

IRS. (2018). *The Foreign Account Tax Compliance Act (FATCA)*. Retrieved June 27, 2018, from IRS: https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca

Kanas, A. (2005, May). *Pure contagion effects in international banking: The case of BCCI's failure.* Retrieved September 28, 2018, from Journal of Applied Economics, Vol. VIII, No. 1 (May 2005), 101-123: https://ageconsearch.umn.edu/bitstream/37495/2/kanas.pdf

Kirsch, S. (2006). *Systematik der Geldwäschetechniken.* Hamburg: Diplomica Verlag GmbH. Retrieved May 7, 2018, from https://www.diplom.de/document/224806

Koning, P. d. (2017, Macrh). *Risk Management in TOGAF & Risk Modeling in ArchiMate.* Retrieved June 19, 2018, from https://www.i-to-i.nl/wp-content/uploads/2017/04/Risk-Modeling-With-Archimate-Pascal-de-Koning-mrt2017.pdf

Kotusev, S. (2017, June). *A Frameworks-Free Look at Enterprise Architecture.* Retrieved June 27, 2018, from http://www.academia.edu/26851970/A_Frameworks-Free_Look_at_Enterprise_Architecture

Kotusev, S. (2017, November). *Enterprise Architecture on a Single Page.* Retrieved June 26, 2018, from https://www.researchgate.net/publication/320935167_Enterprise_Architecture_on_a_Single_Page

Kotusev, S. (2018, April). *Fake and Real Tools for Enterprise Architecture.* Retrieved June 27, 2018, from https://www.researchgate.net/publication/324954484_Fake_and_Real_Tools_for_Enterprise_Architecture

KPMG. (2014). *Global Anti-Money Laundering Survey.* Retrieved June 26, 2018, from KPMG: https://assets.kpmg.com/content/dam/kpmg/pdf/2015/03/global-anti-money-laundering-survey-latest.pdf

Kumar, A. (2017, September 11). *To truly transform KYC and AML operations adopt AI and ML*. Retrieved June 26, 2018, from Finextra: https://www.finextra.com/blogposting/14485/to-truly-transform-kyc-and-aml-operations-adopt-ai-and-ml

Kurier. (2016, July 31). Aktion scharf gegen Geldwäsche in Österreich. *Kurier*. Retrieved June 25, 2018, from https://kurier.at/wirtschaft/aktion-scharf-gegen-geldwaesche-in-oesterreich/212.742.601

Lewis, M. (2018, February). *Deferred Prosecution Agreements: Key Differences Between the US and UK.* Retrieved September 28, 2018, from https://www.oliverwyman.com/content/dam/marsh/Documents/PDF/US-en/Marsh%20Insights_Deferred%20Prosecution%20Agreements.pdf

Lilley, P. (2013, September). *Money Laundering Statistics.* Retrieved from Dirty Dealing: http://www.dirtydealing.org/pages/money_laundering_statistics.htm

Maxwell, N. J., & Artingstall, D. (2017, October). *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime.* Retrieved June 26, 2018, from The Royal United Services Institute: https://rusi.org/sites/default/files/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwell_artingstall_web_3.pdf

McKinsey & Company. (2017, June). *Risk analytics enters its prime*. Retrieved June 26, 2018, from McKinsey & Company: https://www.mckinsey.com/business-functions/risk/our-insights/risk-analytics-enters-its-prime

McKinsey & Company. (2017, November). *The new frontier in anti–money laundering*. Retrieved June 26, 2018, from McKinsey & Company: https://www.mckinsey.com/business-functions/risk/our-insights/the-new-frontier-in-anti-money-laundering

MDirector. (2017, January). *What is Cross-Channel Marketing?* Retrieved June 26, 2018, from MDirector: https://www.mdirector.com/en/digital-marketing/cross-channel-marketing.html

Mei, D., Ye, Y., & Gao, Z. (2014, January). *Literature Review of International Anti-Money Laundering Research: A Scientometrical Perspective.* doi:https://doi.org/10.4236/jss.2014.212016

Merriam-Webster. (2018, May). *compliance*. Retrieved from Merriam-Webster: https://www.merriam-webster.com/dictionary/compliance

Merriam-Webster. (2018, June 26). *contextualization*. Retrieved June 26, 2018, from Merriam-Webster: https://www.merriam-webster.com/dictionary/contextualization

Merriam-Webster. (2018, June 26). *detecting*. Retrieved June 26, 2018, from Merriam-Webster: https://www.merriam-webster.com/dictionary/detecting

Merriam-Webster. (2018, June 26). *false positive*. Retrieved June 26, 2018, from Merriam-Webster: https://www.merriam-webster.com/dictionary/false%20positive

Merriam-Webster. (2018, June 26). *preventing*. Retrieved June 26, 2018, from Merriam-Webster: https://www.merriam-webster.com/dictionary/preventing

Microsoft. (2017, April). *Windows Network Architecture and the OSI Model*. Retrieved June 26, 2018, from Microsoft: https://msdn.microsoft.com/en-us/windows/ff571073

Mills, H. (1980, December). *The management of software engineering: part I: principles of software engineering.* doi:https://doi.org/10.1147/sj.194.0414

Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime. (1999). *Communique.* Moscow, Federal Republic of Russia. Retrieved May 18, 2018, from https://www.justice.gov/sites/default/files/ag/legacy/2004/06/09/99MoscowCommunique.pdf

NICE Actimize. (2017, March). *Customer Due Diligence (CDD) Market Survey.* Retrieved June 26, 2018, from NICE Actimize: https://www.niceactimize.com/Lists/WhitePapers/Fighting_AML_CDDMarketSurveyResults.pdf

Noran, O. (2006, January). *Using Reference Models in Enterprise Architecture: An Example*. Retrieved June 26, 2018, from https://doi.org/10.13140/2.1.2782.1124

Notariatsordnung (NO), Fassung vom 25.06.2018. (n.d.). RGBl. Nr. 75/1871. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001677

Office of the Comptroller of the Currency - U.S. Department of Treasury. (2002, December). *Money Laundering: A Banker's Guide to Avoiding Problems.* Retrieved June 26, 2018, from Office of the Comptroller of the Currency - U.S. Department of Treasury: https://www.occ.treas.gov/topics/bank-operations/financial-crime/money-laundering/money-laundering-2002.pdf

Office of the Comptroller of the Currency. (2002, December). *Money Laundering: A Banker'Guide to Avoiding Problems.* Retrieved May 19, 2018, from Office of the Comptroller of the Currency, U.S. Department of the Treasury: https://www.occ.treas.gov/topics/bank-operations/financial-crime/money-laundering/money-laundering-2002.pdf

Oracle Inc. (2006, December). *Utilities Customer Care and Billing 2.3.1 Utility Reference Models*. Retrieved June 26, 2018, from Oracle Inc.: https://docs.oracle.com/cd/E28945_01/index.htm

Organisation for Economic Co-operation and Development (OECD). (2007). *Report on tax fraud and money laundering vulnerabilities involving the real estate sector.* Retrieved June 19, 2018, from Organisation for Economic Co-operation and Development (OECD): http://www.oecd.org/ctp/exchange-of-tax-information/42223621.pdf

Organisation for Economic Co-operation and Development (OECD). (2009). *Money Laundering Awareness: Handbook for Tax Examiners and Tax Auditors.* Retrieved from Organisation for

Economic Co-operation and Development (OECD): http://www.oecd.org/tax/exchange-of-tax-information/43841099.pdf

Organisation for Economic Co-operation and Development (OECD). (2014, April). *Illicit Financial Flows from Developing Countries: Measuring OECD Responses.* doi:http://dx.doi.org/10.1787/9789264203501-en

Pasley, R. S., & Anderson, K. M. (2012). *Study Guide for the CAMS Certification Examination* (5. ed.). Miami, USA. Retrieved May 9, 2018, from http://na-sj13.marketo.com/rs/582-QUS-045/images/5th_Edition_CAMS_Study_Guide.pdf

Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007, December). *A Design Science Research Methodology for Information Systems Research.* doi:https://doi.org/10.2753/MIS0742-1222240302

Perry, J. M. (2000, October 18). *Watergate Case Study*. Retrieved June 25, 2018, from Columbia University: http://www.columbia.edu/itc/journalism/j6075/edit/readings/watergate.html

Petrunov, G. (2009, May). *Initiatives to counter money laundering: global, regional, national.* Retrieved from Center for the Study of Democracy: http://www.csd.bg/fileadmin/user_upload/PRV/Iniziativi_protivodeistvie_izpirane_na_pari.pdf

Politico. (2018, April 5). *Europe is losing the fight against dirty money.* Retrieved June 20, 2018, from Politico: https://www.politico.eu/article/europe-money-laundering-is-losing-the-fight-against-dirty-money-europol-crime-rob-wainwright/

PR Newswire. (2017, September 19). *European Financial Services Providers face overall Anti-Money Laundering Compliance costs of $83.5 billion a year*. Retrieved June 26, 2018, from PR Newswire: https://www.dowjones.com/insight/morning-risk-report-compliance-spending-rise-europe/

Pramod, V., Li, J., & Gao, P. (2012, July). *A framework for preventing money laundering in banks.* doi:https://doi.org/10.1108/09685221211247280

Profil. (2018, June 16). *Regierung nimmt Immobilienmakler von neuen Anti-Geldwäsche-Regeln aus*. Retrieved June 19, 2018, from Profil: https://www.profil.at/wirtschaft/regierung-immobilienmakler-anti-geldwaesche-regeln-10138662

PwC. (2017, October 2018). *Get ready for RegTech.* Retrieved 8 June, from PwC: https://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/emerging-regtechs-2017.pdf

Raj, D. A. (2018, March 1). *How Financial Institutions Can Use AI to Enhance Due Diligence*. Retrieved June 7, 2018, from https://www.trulioo.com/blog/ai-enhance-due-diligence/

Rechtsanwaltsordnung (RAO), Fassung vom 25.06.2018. (n.d.). RGBl. Nr. 96/1868. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001673

Reuter, P., & Truman, E. M. (2004). *Chasing Dirty Money: The Fight Against Money Laundering.* University of Maryland. Retrieved May 8, 2018, from https://piie.com/bookstore/chasing-dirty-money-fight-against-money-laundering

RiskScreen. (2017). *Infographic showing significant AML fines between March & June 2017*. Retrieved June 26, 2018, from RiskScreen: https://www.riskscreen.com/infographic-showing-significant-aml-fines-between-march-june-2017/

Rosemann, M., & Schütte, R. (1999). *Referenzmodellierung: Multiperspektivische Referenzmodellierung.* Physica, Heidelberg. doi:https://doi.org/10.1007/978-3-642-58670-5_2

Sanctions Alert. (2016, December 5). *Faulty sanctions screening software can lead to fine, underscoring need to have appropriate tools in place*. Retrieved June 26, 2018, from Sanctions Alert: http://sanctionsalert.com/faulty-sanctions-screening-software-can-lead-to-fine-underscoring-need-to-have-appropriate-tools-in-place/

Scheer, A.-W. (1999). *„ARIS — House of Business Engineering“: Konzept zur Beschreibung und Ausführung von Referenzmodellen.* Physica, Heidelberg. doi:https://doi.org/10.1007/978-3-642-58670-5_1

Scherschneva-Koller, E. (2015, November). Geldwäscheermittlungen im Spannungsfeld zum „Anfangsverdacht“ nach dem Strafprozessrechtsänderungsgesetz 2014. *(6)*, 532-536. Journal für Strafrecht. Retrieved from https://elibrary.verlagoesterreich.at/article/99.105005/jst201506053201

Schmalzl, J. (1995). *Architekturmodelle zur Planung der Informationsverarbeitung von Kreditinstituten.* Physica-Verlag Heidelberg. doi:https://doi.org/10.1007/978-3-642-52411-0

Schneider, F., Dreer, E., & Riegler, W. (2006). *Geldwäsche* (1 ed.). Gabler Verlag. doi:https://doi.org/10.1007/978-3-8349-9239-0

Schott, P. A. (2006). *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (2 ed.). The World Bank. doi:https://doi.org/10.1596/978-0-8213-6513-7

Schütte, R. (1998). *Referenzmodellierung: Anforderungen der Praxis und methodische Konzepte.* Wiesbaden: Deutscher Universitätsverlag. doi:https://doi.org/10.1007/978-3-663-07676-6_4

Security Watchdog. (2017, August 4). *The impact of GDPR on KYC*. Retrieved June 26, 2018, from Security Watchdog: https://www.securitywatchdog.org.uk/latest-news/2017/the-impact-of-gdpr-on-kyc

Sen. Kerry, J., & Sen. Brown, H. (1992, December). *The BCCI Affair: A Report to the Committee on Foreign Relations.* Retrieved May 8, 2018, from https://fas.org/irp/congress/1992_rpt/bcci/?_ga=2.81780887.1828965103.1525703032-900460161.1525703032

Shelton, D. (2003). *Commitment and Compliance.*

Statista. (2018). *Statistiken zu bargeldlosen Zahlungen in Österreich*. Retrieved June 26, 2018, from Statista: https://de.statista.com/themen/4198/bargeldloser-zahlungsverkehr-in-oesterreich/

Stessens, G. (2000). *Money Laundering: A New International Law Enforcement Model.* Universitaire Instellung Antwerpen, Belgium.

Strafprozeßordnung 1975 (StPO), Fassung vom 25.06.2018. (n.d.). BGBl. Nr. 631/1975. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326

The Basel Committee on Banking Supervision (BCBS). (1988, December 28). *Prevention of criminal use of the banking system for the purpose of money-laundering.* Retrieved June 26, 2018, from The Basel Committee on Banking Supervision (BCBS): https://www.bis.org/publ/bcbsc137.pdf

The Council of the European Communities. (1991, June 28). *Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.* Retrieved June 25, 2018, from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0308:EN:HTML

The Egmont Group. (2018). *About Egmont Group*. Retrieved June 25, 2018, from https://egmontgroup.org/en/content/about

The European Commission. (2017, February 28). *EU assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.* Retrieved May 18, 2018, from The European Commission: https://ec.europa.eu/info/law/better-regulation/initiative/9559/attachment/090166e5b0a4a52e_en

The European Parliament and of the Council of the European Union. (2009, September 16). *Regulation (EC) No 924/2009 of the European Parliament and of the Council of 16 September 2009 on cross-border payments in the Community and repealing Regulation (EC) No 2560/2001.* Retrieved June 25, 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009R0924&from=EN

The European Parliament and of the Council of the European Union. (2014, April 16). *Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directives 2003/6/EC, 2003/124/EC, 2003/125/EC,*

2004/72/EC. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0596&from=EN

The European Parliament and of the Council of the European Union. (2016, July 14). *Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies.* Retrieved June 25, 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R1675&from=EN

The European Parliament and the Council of the European Union. (2001, December 4). *Directive 2001/97/EC The European Parliament and the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering.* Retrieved June 25, 2018, from https://eur-lex.europa.eu/resource.html?uri=cellar:57ce32a4-2d5b-48f6-adb0-c1c4c7f7a192.0004.02/DOC_1&format=PDF

The European Parliament and the Council of the European Union. (2005, October 26). *Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.* Retrieved June 26, 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060&from=EN

The European Parliament and the Council of the European Union. (2005, October 26). *Regulation (EC) No 1889/2005 of the European Parliament and the Council of the European Union of 26 October 2005 on controls of cash entering or leaving the Community.* Retrieved June 25, 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005R1889&from=EN

The European Parliament and the Council of the European Union. (2006, November 15). *Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds.* Retrieved June 25, 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006R1781&from=en

The European Parliament and the Council of the European Union. (2014, April 16). *Directive 2014/57/EU of the European Parliament and the Council of 16 April 2014 on criminal sanctions for market abuse (market abuse directive).* Retrieved June 26, 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0057&from=EN

The European Parliament and the Council of the European Union. (2015, May 20). *Directive (EU) 2015/849 of the European Parliament and of the Council.* Retrieved May 11, 2018, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_141_R_0003&from=ES

The European Parliament and the Council of the European Union. (2015, May 20). *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.* Retrieved June 25, 2018, from The European Parliament and the Council of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0847&from=EN

The European Parliament and the Council of the European Union. (2016, July 19). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* Retrieved September 23, 2019, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=DE

The European Parliament and the Council of the European Union. (2016, April 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council.* Retrieved May 11, 2018, from The European Parliament and the Council of the Union: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

The European Parliament and the Council of the European Union. (2016, April 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.* Retrieved June 26, 2018, from The European Parliament and the Council of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

The European Parliament and the Council of the European Union. (2018, April 17). *Directive (EU) (Proposal) of the European Parliament and of the Council laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences.* Retrieved May 11, 2018, from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180417_directive-proposal-facilitating-use-information-prevention-detection-investigation-prosecution-criminal-offences_en.pdf

The European Parliament and the Council of the European Union. (2018, May 30). *Directive (EU) 2018/843 of the European Parliament and of the Council.* Retrieved October 3, 2019, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN

The Financial Action Task Force. (2001, October). *FATF IX Special Recommendations.* Retrieved June 25, 2018, from The Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf

The Financial Action Task Force. (2003, February). *Report on Money Laundering Typologies 2002-2003.* Retrieved May 2018, from The Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/reports/2002_2003_ML_Typologies_ENG.pdf

The Financial Action Task Force. (2007, June 29). *Money laundering and terrorist financing through the real estate sector.* Retrieved June 19, 2018, from The Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20through%20the%20Real%20Estate%20Sector.pdf

The Financial Action Task Force. (2010, July). *Global Money Laundering & Terrorist Financing Threat Assessment.* Retrieved May 9, 2018, from The Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/reports/Global%20Threat%20assessment.pdf

The Financial Action Task Force. (2012, October). *International Standards on combating money laundering and the financing of terrorism & proliferation: The FATF Recommendations.* Retrieved May 18, 2018, from The Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

The Financial Action Task Force. (2013, October). *Money Laundering and terrorist financing through trade in diamonds.* Retrieved May 9, 2018, from The Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf

The Financial Action Task Force. (2013, June). *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals.* Retrieved June 8, 2018, from The Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf

The Financial Action Task Force. (2013, February). *Revised Guidance on AML/CFT and Financial Inclusion.* Retrieved June 26, 2018, from The Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf

The Financial Action Task Force. (2014, October). *Guidance for a risk-based approach: Banking Sector.* Retrieved June 8, 2018, from The Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf

The Financial Action Task Force. (2016, Semptember). *Anti-money laundering and counter-terrorist financing measures in Austria - 2016.* Retrieved May 2018, from The Financial Action Task Force: www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Austria-2016.pdf

The Financial Action Task Force. (2017, December). *Anti-money laundering and counter-terrorist financing measures in Austria - 2017.* Retrieved June 20, 2018, from The Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/FUR-Austria-Dec-2017.pdf

The Financial Action Task Force. (2017, November). *FATF Guidance on AML/CFT measures and financial inclusion, with a supplement on customer due diligence.* Retrieved June 26, 2018,

from The Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf

The Financial Action Task Force. (2018, March 16). *About the Non-Cooperative Countries and Territories (NCCT) Initiative*. Retrieved May 14, 2018, from The Financial Action Task Force: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/more/aboutthenon-cooperativecountriesandterritoriesncctinitiative.html?hf=10&b=0&s=desc(fatf_releasedate)

The Financial Action Task Force. (2018, November). *Anti-money laundering and counter-terrorist financing measures in Austria - 2018.* Retrieved October 5, 2019, from The Financial Action Task Force: http://www.fatf-gafi.org/media/fatf/documents/reports/fur/FUR-Austria-2018.pdf

The Financial Action Task Force. (2018). *Money Laundering*. Retrieved June 26, 2018, from The Financial Action Task Force: http://www.fatf-gafi.org/faq/moneylaundering/

The Financial Action Task Force. (2018, May 29). *The FATF Recommendations*. Retrieved June 25, 2018, from The Financial Action Task Force: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

The Financial Action Task Force. (2018, May 29). *Who we are?* Retrieved June 25, 2018, from http://www.fatf-gafi.org/about/

The Home Office of the United Kingdom. (2019, March 13). *Future technology trends in security.* Retrieved October 6, 2019, from The Home Office of the United Kingdom: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786244/HO_OSCT_Future_Tech_Trends_Final_Updated_13Mar19.pdf

The Joint Committee of the three European Supervisory Authorities (EBA, EIOPA and ESMA) (ESAs). (2018, Janury 23). *Opinion on the use of innovative solutions in the customer due diligence process.* Retrieved June 28, 2018, from https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf

The Open Group. (2018). *ArchiMate® 3.0.1 Specification*. Retrieved June 27, 2018, from http://pubs.opengroup.org/architecture/archimate3-doc/toc.html

The Open Group. (2018). *The ArchiMate® Enterprise Architecture Modeling Language*. Retrieved June 27, 2018, from http://www.opengroup.org/subjectareas/enterprise/archimate-overview

The Open Group. (2018). *The TOGAF® Standard*. Retrieved June 27, 2018, from http://www.opengroup.org/subjectareas/enterprise/togaf

The Open Group. (2018). *TOGAF 8.1.1: Case Studies*. Retrieved June 26, 2018, from The Open Group: http://pubs.opengroup.org/architecture/togaf8-doc/arch/chap35.html

The Open Group. (2018). *TOGAF 9.2: Core Concepts*. Retrieved June 27, 2018, from The Open Group: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap02.html

The Organized Crime and Corruption Reporting Project. (2017, September). *The Russian Laundromat Exposed.* Retrieved May 8, 2018, from The Organized Crime and Corruption Reporting Project: https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/

The Permanent Subcommittee On Investigations. (2012, Juli). *HSBC Exposed U.S. Financial System to Money Laundering, Drug, Terrorist Financing Risks*. Retrieved May 8, 2018, from The Permanent Subcommittee On Investigations: https://www.hsgac.senate.gov/subcommittees/investigations/media/hsbc-exposed-us-finacial-system-to-money-laundering-drug-terrorist-financing-risks

The Secretary of the Treasury, the Board of Governors of the Federal Reserve System, the Securities and Exchange Commission. (2002, December 31). *A report to congress in accordance with § 356(c) of the uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism act of 2001 (USA Patriot Act).* Retrieved October 6, 2019, from U.S. Department of the Treasury: https://www.treasury.gov/press-center/press-releases/Documents/356report.pdf

The United Nations. (2005, July 29). *Resolution 1617 (2005).* Retrieved June 25, 2018, from http://www.un.org/ga/search/view_doc.asp?symbol=S/RES/1617%20%282005%29

The United Nations. (2006, September 20). *Resolution adopted by the General Assembly on 8 September 2006.* Retrieved from http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/60/288

The United Nations. (2018, June 26). *Consolidated United Nations Security Council Sanctions List*. Retrieved June 26, 2018, from The United Nations: https://scsanctions.un.org/consolidated/

The Washington Times. (2017, January 30). *Useless anti-money laundering laws.* Retrieved June 6, 2018, from The Washington Times: https://www.washingtontimes.com/news/2017/jan/30/useless-anti-money-laundering-laws/

The Wolfsberg Group. (2006, March). *Guidance on a Risk Based Approach for Managing Money Laundering Risks.* Retrieved June 7, 2018, from The Wolfsberg Group: https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/15.%20Wolfsberg_RBA_Guidance_%282006%29.pdf

The Wolfsberg Group. (2018, June 1). *Wolfsberg CBDDQ*. Retrieved June 25, 2018, from https://www.wolfsberg-principles.com/wolfsbergcb

The World Bank. (2016, October 7). *De-risking in the Financial Sector*. Retrieved June 9, 2018, from The World Bank: http://www.worldbank.org/en/topic/financialsector/brief/de-risking-in-the-financial-sector

Thomson Reuters. (2018, June). *About World-Check*. Retrieved June 26, 2018, from Thomson Reuters: https://risk.thomsonreuters.com/en/products/world-check-know-your-customer/about-world-check.html

Timm, F., & Sandkuhl, K. (2018, March). *Towards a Reference Compliance Organization in the Financial Sector.* Retrieved from https://www.researchgate.net/publication/324476981_Towards_a_Reference_Compliance_Organization_in_the_Financial_Sector

Timm, F., Zasada, A., & Thiede, F. (2016, September). *Building a Reference Model for Anti-Money Laundering in the Financial Sector.* Retrieved June 25, 2018, from https://www.researchgate.net/publication/306208418_Building_a_Reference_Model_for_Anti-Money_Laundering_in_the_Financial_Sector

Trend. (2016, April 5). *Panama Papers: RBI: "Gänzliche Durchleuchtung nicht möglich"*. Retrieved June 7, 2018, from Trend: https://www.trend.at/wirtschaft/raiffeisen-bank-international-panama-papers-6300194

Trulioo. (2015, February 11). *What happens when businesses don't comply with AML/KYC regulations?* Retrieved June 26, 2018, from Trulioo: https://www.trulioo.com/blog/happens-businesses-dont-comply-amlkyc-regulations/

U.S. Congress, Office of Technology Assessment. (1995, September). *Information Technologies for the Control of Money Laundering.* Retrieved June 26, 2018, from https://www.princeton.edu/~ota/disk1/1995/9529/9529.PDF

U.S. Department of Justice. (2017, February). *Documents and Resources from the December 11, 2012, HSBC Press Conference*. Retrieved from U.S. Department of Justice: https://www.justice.gov/archives/opa/documents-and-resources-december-11-2012hsbc-press-conference

U.S. Department of the Treasury. (2018, June 4). *Consolidated Sanctions List Data Files*. Retrieved June 26, 2018, from U.S. Department of the Treasury: https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/consolidated.aspx

U.S. Securities and Exchange Commission (SEC). (2018). *Sarbanes-Oxley Act of 2002 (SOX)*. Retrieved June 26, 2018, from U.S. Securities and Exchange Commission: https://www.sec.gov/spotlight/sarbanes-oxley.htm

Unger, B. (2007). *The Scale and Impacts of Money Laundering.* Cheltenham, UK: Edward Elgar Publishing. doi:https://doi.org/10.4337/9781781007624

Unger, B., Rawlings, G., Siegel, M., Ferwerda, J., de Kruijf, W., Busuioc, E., & Wokke, K. (2006). *The amounts and effects of money laundering.* Retrieved May 4, 2018, from Utrecht University

School of Economics: http://www2.econ.uu.nl/users/unger/publications/Amounts%20and%20Effects%20ML.pdf

United Nations Convention. (1988, November 23). *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.* Retrieved May 18, 2018, from https://www.unodc.org/pdf/convention_1988_en.pdf

United Nations Convention. (2000, November 15). *United Nations Convention against Transnational Organized Crime.* Retrieved May 18, 2018, from https://www.unodc.org/pdf/crime/a_res_55/res5525e.pdf

United Nations Office on Drugs and Crime. (2010, February). *Risk of Money Laundering through Financial Instruments.* Retrieved June 8, 2018, from United Nations Office on Drugs and Crime: https://www.unodc.org/documents/colombia/2013/diciembre/Risk_of_Money_Laudering_version_I.pdf

United Nations Office on Drugs and Crime. (2011, October). *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes.* Retrieved May 8, 2018, from United Nations Office on Drugs and Crime: http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

United Nations Office on Drugs and Crime. (2011, March 16). *UNODC on money-laundering and countering the financing of terrorism*. Retrieved May 18, 2018, from United Nations Office on Drugs and Crime: https://www.unodc.org/unodc/en/money-laundering/index.html

US District Court for the Southern District of Florida. (1982, November 10). *US v US$4,255,625.39 (1982) 551 F Supp.314. T.* Retrieved May 18, 2018, from US District Court for the Southern District of Florida: https://law.justia.com/cases/federal/district-courts/FSupp/551/314/2366254/

Verband österreichischer Privatstiftungen. (2018). *Facts & Figures - österreichische Privatstiftungen*. Retrieved from Verband österreichischer Privatstiftungen: http://www.stiftungsverband.at/pages/facts-figures/die-oesterreichische-privatstiftung.php

Verordnung der Finanzmarktaufsichtsbehörde (FMA) über die Anwendbarkeit vereinfachter Sorgfaltspflichten im Bereich des Schulsparens (Schulsparen-Sorgfaltspflichtenverordnung – Schulspar-SoV), Fassung vom 25.06.2018. (n.d.). BGBl. II Nr. 2/2017. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009772

Verordnung der Finanzmarktaufsichtsbehörde (FMA) über die Anwendung vereinfachter Sorgfaltspflichten im Bereich der Lebensversicherung (Lebensversicherung-Sorgfaltspflichtenverordnung – LV-SoV), Fassung vom 25.06.2018. (n.d.). BGBl. II Nr. 1/2017. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009771

Verordnung der Finanzmarktaufsichtsbehörde (FMA) über die Ausnahme von der Verpflichtung zur Aufzeichnung einer Risikoanalyse und der Anwendbarkeit vereinfachter Sorgfaltspflichten im Bereich des Betrieblichen Vorsorgekassengeschäfts. (n.d.). *BVK-Risikoanalyse- und Sorgfaltspflichtenverordnung – BVK-RiSoV, Fassung vom 25.06.2018*. BGBl. II Nr. 4/2017. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009773

Verordnung der Finanzmarktaufsichtsbehörde (FMA) über die Identifizierung von Sparvereinsmitgliedern (Sparvereinverordnung – SpVV), Fassung vom 25.06.2018. (n.d.). BGBl. II Nr. 62/2015. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009123

Vulliamy, E. (2011, April 3). How a big US bank laundered billions from Mexico's murderous drug gangs. *The Guardian*. Retrieved May 8, 2018, from https://www.theguardian.com/world/2011/apr/03/us-bank-mexico-drug-gangs?_ga=2.22389051.1828965103.1525703032-900460161.1525703032

Wasserman, M. (2002, Q1). *Dirty money.* Retrieved October 3, 2019, from Federal Reserve Bank of Boston: www.bostonfed.org/-/media/Documents/RegionalReview/dirty.pdf

Wertpapieraufsichtsgesetz 2018 – WAG 2018, Fassung vom 25.06.2018. (2017). BGBl. I Nr. 107/2017. Retrieved June 25, 2018, from https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009943

Wilson, J. (2013). *Essentials of Business Research: A Guide to Doing Your Research Project.* SAGE Publishing.

Wirtschaftskammer Österreich. (2017, November 11). *Länder- oder personenbezogene Embargos und Sanktionen*. Retrieved June 26, 2018, from Wirtschaftskammer Österreich: https://www.wko.at/service/aussenwirtschaft/Laender-_oder_personenbezogene_Embargos_und_Sanktionen.html

Wirtschaftskammer Österreich. (2018). *Economic situation and outlook.* Vienna. Retrieved from https://wko.at/statistik/prognose/outlook.pdf

Wirtschaftskammer Österreich. (2018, May 25). *IT-Sicherheit, Datensicherheit.* Retrieved June 7, 2018, from Wirtschaftskammer Österreich: https://www.wko.at/service/innovation-technologie-digitalisierung/it-sicherheit-datensicherheit.html

Zünd, A. (1990). (Treuhand-Kammer, Ed.) *Der Schweizer Treuhänder: Monatsschrift für Wirtschaftsprüfung, Rechnungswesen, Unternehmens- und Steuerberatung: offizielles Organ der Treuhand-Kammer, Der Schweizer Treuhänder*(64). Retrieved June 20, 2018, from http://lhzbw.gbv.de/DB=1/SET=2/TTL=41/SHW?FRST=45