Guidelines for Collecting Forensic Computing Evidence in order to reinforce the Detection of Money Laundering Activities in the Central Bank of Ecuador

Flores Armas, D.A.
2012
Guidelines for Collecting Forensic Computing Evidence in order to reinforce the Detection of Money Laundering Activities in the Central Bank of Ecuador

By Flores Armas, Denys Alberto

Dissertation submitted to the University of Derby in partial fulfilment of the requirements for the award of Master of Science in Forensic Computing and Security

2011 - 2012
Abstract

The *Financial Action Task Force* (FATF, 2003) issued 40 Recommendations and 9 Special Recommendations (FATF, 2001) in order to help financial institutions implement anti-money laundering methods and techniques to protect the international financial systems from the evolving money laundering typologies, including financing terrorism and drug dealing.

On the other hand, the *Bank for International Settlements* (BIS) issued two frameworks to help financial institutions; in particular, the central banks, to secure their financial transactions by means of an adequate measure of capital and liquidity. The Basel II framework (BIS, 2006, p.1, 7, 8) intends to secure the surrounding requirements governing the capital adequacy in the whole banking system, including the central banks. Additionally, the Basel III framework (BIS, 2010, s.1) strengthens the global liquidity regulations in order to absorb shocks arising from financial and economic stress.

However, these recommendations and frameworks have some limitations such as the lack of both *Computer Forensic Practices* and *IT Management* considerations, the consequences of which may cause that the anti-money laundering evidence identified in the *Central Bank of Ecuador* (BCE) cannot be admissible during criminal and civil litigations in the Ecuadorian jurisdiction, and at the same time, dismissed if this evidence is required for investigating money laundering activities overseas (FATF, 2003, rec. 1, 2, 39; 2001, lit. V).

Therefore, considering that information is an important asset that needs to be protected (BS ISO/IEC, 2007, p. viii), money laundering-related information has to be properly managed within the BCE. Then, this *Anti-Money Laundering (AML) Framework* provide guidelines in order to understand what the *Central Bank of Ecuador* (BCE), should be doing in terms of money laundering detection. Similarly, this *AML Framework* incorporates the FATF recommendations and the Basel frameworks on its scope, so its general principles and characteristics can be applied by outlining a straightforward process aligned with the *IT Managements objectives* in terms of security and risk assessment, along with the necessary practices to assure digital evidence *identification, collection, acquisition, and preservation* (BS ISO/IEC, 2011b) in a forensically sound manner.
Acknowledgements

First of all, thanks to my Lord Jesus for giving me His blessings and strength to achieve another challenging goal in my life. Also, special thanks to my family and friends in Ecuador whose encouragement and faith have helped me to overcome difficulties in spite of the distance between us. I want to thank my friends in England and those I met from all over the world, for the pleasant memories shared with me... God bless you all.

Thanks to my lecturers and tutors in the University of Derby for supporting my learning during my time as student; a very special acknowledgement to Mr. Richard Self, for his knowledge, patience, and constant academic support to achieve the challenging outcomes of this project.

I also want to acknowledge the support received by the Central Bank of Ecuador; in particular, thanks to Mr. Christian Ruiz, General Manager of this institution, who kindly extended his sponsorship to develop this project.

Finally, a special acknowledgement to the National Polytechnic School as well as the National Secretariat of Higher Education, Science, Technology, and Innovation of Ecuador which have made it possible to undertake a postgraduate course in the University of Derby.

Denys A. Flores
# Table of Contents

Abstract ........................................................................................................................................ i

Acknowledgements ....................................................................................................................... ii

Table of Contents .......................................................................................................................... iii

List of Tables .................................................................................................................................. vi

List of Figures and Illustrations ...................................................................................................... vi

Terms and Definitions .................................................................................................................... vii

1. Introduction ................................................................................................................................. 1
   1.1. Project Rationale .................................................................................................................... 1
   1.2. Project Aim and Objectives .................................................................................................. 2
       1.2.1. Project Aim ................................................................................................................... 2
       1.2.2. Project Objectives ........................................................................................................ 2

2. Literature Review .......................................................................................................................... 3
   2.1. Introduction ............................................................................................................................ 3
   2.2. Identification and Protection of Capital Assets ................................................................. 4
   2.3. The Need of Anti-Money Laundering Policies .................................................................... 5
       2.3.1. Regulating Disclosure of Money Laundering Information ......................................... 6
       2.3.2. Regulating Employee Behaviour ................................................................................ 7
       2.3.3. Regulating Customer Activity .................................................................................... 7
   2.4. Scope of a Money Laundering Detection Strategy .............................................................. 9
       2.4.1. Measuring the Effectiveness of the Detection Strategy ............................................. 10
   2.5. Legal Instruments in the Ecuadorian Laws to Criminalise Money Laundering Activities .... 11
2.6. Conclusions

2.6.1. Lack of Forensic Computing Practices within the Anti-Money Laundering Recommendations

2.6.2. Information Technology Management Considerations are not part of Anti-Money Laundering Procedures

2.6.3. Money Laundering Detection using Technology is not fully covered within the Anti-Money Laundering Recommendations

2.6.4. Refined Research Questions

3. Description of the Anti-Money Laundering Framework

3.1. Introduction

3.2. Defining the Anti-Money Laundering Framework

3.3. Enhancing the Anti-Money Laundering Framework

3.3.1. Adopting the PDCA Process

3.4. Adapting the PDCA Process for Money Laundering Detection

3.4.1. Identifying the Scope of the AML Framework

3.4.2. Aligning Know-Your-Customer Policies with Money Laundering Detection Requirements

3.4.3. Aligning Computer Forensic Practices with Know-Your-Customer Policies

3.4.4. Understanding the Case Requirements before Investigating Money Laundering Activities

3.4.5. Adapting the Top-Down Approach for Customer Data Analysis

3.4.6. Applying the Top-Down Approach for Evidence Acquisition and Examination

3.4.7. Evaluating Evidence Admissibility

3.4.8. Aligning Money Laundering Risk with Information Security Requirements

3.5. Conclusion

4. Conclusions and Recommendations

4.1. Conclusions
List of Tables

Table 2.1-Legal Instruments to Repress Money Laundering in Ecuador ................................. 12
Table 4.1-BS ISO/IEC 27000 Standards in the Current Research Scope ............................. 19
Table 4.2-Alignment of the PDCA process with the AML Framework .................................. 20

List of Figures and Illustrations

Figure 4.1-Anti-Money Laundering Framework .................................................................. 17
Figure 4.2-PDCA Process of the AML Framework .............................................................. 22
Figure 4.3-Know-Your-Customer Policies Workflow .......................................................... 24
Figure 4.4-Computer Forensics-Based Detection Procedure ............................................. 27
Figure 4.5-Digital Evidence Analysis during a Money Laundering Investigation ............... 30
Figure 4.6-Creating Database Logs as Evidence Files ..................................................... 31
Terms and Definitions

The following are a list of terms and their definitions, which are cited in this piece of work. Please, refer to this section, if required.

**Anti-Money Laundering Framework** is a conceptual framework comprised of a component-based model and a PDCA process, which has been developed, as part of this research, in order to reinforce the detection of money laundering in the Central Bank of Ecuador.

**Bank for International Settlements or BIS** assists central banks in their pursuit of monetary and financial stability, to foster international cooperation in those areas and to act as a bank for central banks. (http://www.bis.org/about/index.htm)

**BS ISO/IEC 27000 standard series** is an internationally recognised standard family for implementing and operating an information security management system, according to a model which has been crafted by experts in the field (BS ISO/IEC, 2009).

**The Central Bank of Ecuador, Banco Central del Ecuador or BCE** is the institution in charge of promoting, and contributing the economic stability of Ecuador. (http://www.bce.fin.ec/)

**Compliance Officer** is responsible for the implementation of the strategies, policies, procedures, processes and related reporting, in compliance with all applicable laws and regulations. (http://www.compliance-officer.org/)

**Computer Forensic Investigation** is the science dedicated to a proper identification and collection of computer evidence for its later use in a civil or criminal case (Solomon et al., 2011, ch. 3).

**De-normalised database** is an effort to optimize performance while maintaining data integrity by grouping redundant information in data structures to optimise query results. (http://computerresearch.org/stpr/index.php/gjcst/article/view/94/86)

**Ecuadorian Bank Board** is the highest authority in the Bank and Insurance Superintendence comprised of a chairman and three members. This board issues the resolutions for regulating the Ecuadorian financial and insurance system. (http://www.sbs.gob.ec/practg/sbs_index?vp_art_id=581&vp_tip=2)

**Electronic Discovery or e-discovery** is the process of identifying, preserving, collecting, reviewing, analyzing and producing information that is stored electronically during civil and criminal investigations so that relevant information for pre-trial motions and for the trial itself can be obtained. This electronic information includes email, instant messages, word processing files, spreadsheets, social networking content, and any other electronic information that may be stored on desktops, laptops, file servers, mainframes, smart phones, and employees’ home computers or on a variety of other platforms (Osterman Research, 2010).

**Electronically Stored Information, Electrically Stored Information, or ESI** is the data stored in electronic media such as documents, databases, transcripts, and audio/visual recordings. (http://www.opengovdata.org/home/8principles)
**ETL process** is a process in database usage and especially in data warehousing that involves extracting data from operational or archive systems, transforming it to meet business needs, and loading it into a target data warehouse. (http://etl-tools.info/en/bi/etl_process.htm)

**Fuerzas Armadas Revolucionarias de Colombia or FARC** is the Colombian Guerrilla established in 1964 as the military wing of the Colombian Communist Party. (http://www.globalsecurity.org/military/world/para/farc.htm)

**Financial Action Task Force or FATF** is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. (http://www.fatf-gafi.org/)

**Financial Intelligence Unit or FIU** is a financial intelligence organisation which analyzes information that has been obtained concerning unusual or unjustified financial operations or transactions. In Ecuador, the FIU was launched in 2006, following the introduction of the country’s first Anti-Money Laundering legislation. (http://www.anti-moneylaundering.org/southamerica/Ecuador.aspx)

**Forensic Computing Evidence** is any data stored or transmitted using a computer that support or refuse a theory of how an offense occurred (Casey, 2011).

**International Assessment and Strategy Center** is a "think-tank" focused on medium and long-term security issues and their impact on the security of the United States and her key interests and allies. Work is performed at both open-source and classified levels and includes specialized investigative work. (http://www.strategycenter.net/)

**National Assembly** is the organism which exercises the legislative power in Ecuador. (http://www.asambleanacional.gov.ec/)

**Predicate Offences** are offences related to money laundering within categories given by the FATF (2003, p.15), such as participation in criminal groups, terrorism, human trafficking, sexual exploitation, drug dealing, etc.

**South American Financial Action Task Force or GAFISUD** is an inter-governmental organisation comprised of South American countries in order to combat money laundering and terrorism financing. (http://www.gafisud.info/home.htm)
1. Introduction

1.1. Project Rationale

Since the adoption of the American Dollar as national currency in the late 90’s, Ecuador emerged as target of transnational criminal groups; mainly, due to some flaws in its former anti-money laundering laws which could not effectively support financial institutions to investigate, and denounce such illegal activities (Deutsche Welle, 2010). Additionally, the presence of the FARC, the Colombian guerrilla, in the Ecuadorian-Colombian border, became a serious problem for the Ecuadorian authorities to stop the incursions of terrorists in the country, the purpose of which was moving drugs, and laundering drug trafficking proceedings (International Assessment and Strategy Center, 2010).

Conversely, during the last years, this scenario has changed due to the important efforts made by the Ecuadorian government to stop money laundering, including a successful military campaign to assist Colombia on dismantling some FARC’s camps (Colombia Reports, 2010). Furthermore, Ecuador issued a law to strengthen the sanctions related to money laundering activities (National Assembly, 2005), which made the GAFISUD acknowledge the important contribution of Ecuador in fighting against money laundering (Inter Press Service, 2010).

Nonetheless, recent questionable statements such as the existence of Chinese and Russian mafias in the country (International Assessment and Strategy Center, 2010, p.74), influenced the FATF to blacklist Ecuador (FATF, 2010a) due to money laundering and terrorist financing risk (International Relations and Security Network, 2010), along with lack of political commitment to address these issues (The Economist, 2010). As a result, President Rafael Correa wanted to restore the country’s image by urging the financial institutions, particularly the Central Bank, in order to revise and reinforce their anti-money laundering strategies (Inter Press Service, 2010).

Hence, the rationale of the current project is to assist the Central Bank of Ecuador ‘BCE’ in reinforcing its money laundering detection strategy by developing guidelines to obtain relevant forensic computing evidence considering the application of IT standards and
international regulations. Moreover, the author, as citizen and sponsored student by the Ecuadorian government, wants to demonstrate that computer forensic practices are important to adopt inside the BCE in order to align the Information Security goals with the organisational objectives related to money laundering detection.

1.2. **Project Aim and Objectives**

1.2.1. **Project Aim**

To assist the BCE in reinforcing its money laundering detection strategy by developing guidelines to obtain relevant forensic computing evidence by considering the application of IT management standards and international regulations.

1.2.2. **Project Objectives**

a) To identify a set of recommended practices in the field of forensic computing by analysing the *BS ISO/IEC 27000 standard series* so that relevant evidence can be properly identified, analysed, and presented

b) To identify a set of financial and legal considerations by analysing international anti-money laundering laws, treaties, and regulations. E.g. FATF recommendations and Basel Frameworks

c) To develop guidelines in order to reinforce the current money laundering detection strategy of the BCE considering the possible gaps in both the legal and the digital evidence handling tasks
2. Literature Review

2.1. Introduction

In 1990, the Financial Action Task Force ‘FATF’ issued 40 Recommendations (FATF, 2003) in order to help financial institutions to implement anti-money laundering methods and techniques to refrain the misuse of financial systems to launder drug money. Then, further revisions in 1996, 2003, and 2004 helped to reflect the evolving money laundering typologies in these recommendations, including terrorism financing which were fully covered and discussed in the FATF IX special recommendations (FATF, 2001).

On the other hand, the Bank for International Settlements ‘BIS’ issued two frameworks in order to help financial institutions; in particular, the central banks, to secure their financial transactions by means of an adequate measure of capital and liquidity. First, the Basel II framework (BIS, 2006, p.1, 7, 8) intends to assure the surrounding requirements governing the capital adequacy by regulating all the relevant financial activities in the whole banking system. Additionally, the Basel III framework (BIS, 2010, s.1) outlines the reforms to strengthen the global liquidity regulations so that the banking sector can be able to absorb shocks arising from financial and economic stress, and therefore, achieve more resilient banking activities.

Conversely, the FATF recommendations are general principles to be adopted instead of being a framework, so it is difficult to devise how to implement them by following a well-defined process. However, due to the fact that the requirements outlined in the Basel III framework follow the existing application scope of the Basel II Framework (BIS, 2010, par.10), these complementary financial standards can be used to apply important business requirements whilst implementing the FATF Recommendations.

As a result, in the following sections, both the FATF 40 recommendations and its IX special recommendations are discussed, considering their main features in order to understand what the BCE, should be doing in terms of money laundering detection. Similarly, some of the requirements outlined in the Basel II and III frameworks are discussed within the context
of the FATF recommendations so that important characteristics associated with anti-money laundering detection can be identified.

Hence, in section 2.2 the importance of protecting capital assets from money laundering activities is discussed. Then, in section 2.3, the need of establishing anti-money laundering policies is explained, considering internal and external disclosure regulation of money laundering-related information, along with the importance of tracking customer activity, and defining employee responsibilities.

Later, in section 2.4, the scope of any money laundering detection strategy is covered, considering not only the requirements for evidence admissibility, but also the requisites to measure its effectiveness.

Next, in section 2.5, the legal instruments that have been included in the Ecuadorian anti-money laundering law are briefly discussed to understand what is expected from the BCE in order to detect money laundering activities in the country.

Finally, conclusions outlining the main gaps and challenges in money laundering detection are given along with refined research questions.

2.2. Identification and Protection of Capital Assets

The BIS has suggested that any financial institution should properly identify and measure its sources of Core and Supplementary Capital, along with liquidity sources due to the fact that they constitute minimum capital requirements for the proper operation of any financial institution (BIS, 2006, p.6, 14).

Firstly, Core Capital, Equity Capital or Tier 1 Capital (BIS, 2006, s.49 (i-iii)), is a key capital element comprised of Regulatory Capital and Risk-Weighted Assets, which are useful to identify and measure the sources of capital, and assess their risk, respectively (BIS, 2006, p.12). In fact, this allows protecting them from unexpected financial exposures by identifying which the core capital sources are, and define methods to protect them.

Second, Undisclosed Reserves of Capital, Supplementary Capital, or Tier 2 Capital is the capital reflected in the profit and loss account, so it has to be considered as a minimum capital
requirement in terms of financial transparency (BIS, 2006, s.49 (iv)). Particularly, measuring this form of capital enables to identify the possible financial losses not yet identified (BIS, 2006, s. 49 (vii - x)).

Third, measuring liquidity is important in order to identify the concentration of funding per funding source in order to prevent liquidity problems (BIS, 2010, s. 151). In fact, measuring liquidity enables to secure the liquidity capacity of any financial institution so that it can be able to face economic stress during critical events (BIS, 2010, s.1).

Finally, considering that any assets or property should be confiscated when directly or indirectly related to either money laundering, or terrorism financing (FATF, 2003, rec. 3, 13, 38; 2001, lit. III), the Central Bank of Ecuador ‘BCE’ should identify and measure its minimum sources of capital in order to not only prevent the injection of unlawful capital assets in the institution, but also to identify the financial risk if they are confiscated due to money laundering activities. In fact, this recommendation has been enforced in the Ecuadorian Legal System in order to comply with the international expectations to combat money laundering (National Assembly, 2010, art. 1(c)).

Hence, since unlawful assets can be confiscated if found related to money laundering events, the BCE must prevent money laundering activities by identifying, measuring and protecting its minimum capital requirements.

2.3. The Need of Anti-Money Laundering Policies

The Ecuadorian Legal System allows the establishment of policies and procedures to prevent money laundering in financial institutions (National Assembly, 2005). Thus, the recommendations given by the Financial Action Task Force ‘FATF’ (FATF, 2001; 2003; 2004) have been analysed to achieve this aim. In fact, their main aspects are discussed, considering the regulation of internal and external disclosure of money laundering information, the definition of both employee screening and customer activity control policies, along with the establishment of effective detection procedures.
2.3.1. Regulating Disclosure of Money Laundering Information

As suggested by the FATF, if the Central Bank of Ecuador ‘BCE’ either suspects, or has reasonable grounds to suspect that funds linked to banking transactions are the proceedings of money laundering, or its predicate offences, this institution must promptly report these transactions to the Financial Intelligence Unit ‘FIU’ (FATF, 2003, rec. 13). Furthermore, as specified in the Ecuadorian anti-money laundering law (National Assembly, 2005; 2010), the disclosure of this information must be regulated via internal and external policies.

First, defining Internal Disclosure policies is important in order to regulate the dissemination of money laundering-related information to assist authorities and auditors within the BCE whilst investigating complex, or unusual transactions performed by any customer (FATF, 2003, rec. 11). In fact, this internal regulation of customer information related to money laundering is closely related to the definition of customer due diligence policies which are further explained section 2.3.3.

Secondly, External disclosure policies enables the BCE to effectively establish domestic co-operation channels between the Ecuadorian FIU, national law enforcement agencies, local supervisors, and other parties involved in money laundering investigation (FATF, 2003, rec. 31). Also, they allow sharing information with external bodies worldwide (FATF, 2003, rec. 40) in order to facilitate mutual co-operation, whilst investigating cross-border money laundering activities, by providing accurate information to competent authorities (FATF, 2003, rec. 33). For instance, this can be achieved by deploying a computerised data base to effectively disseminate critical information whilst investigating money laundering or terrorist financing cases (FATF, 2003, rec. 19).

Similarly, supervisors within the BCE must ensure that information about money laundering reports are available for relevant external parties, and decide which information related to such reports should be publicly available (BIS, 2006, s. 811).

Thus, supervisors within the BCE should establish criteria to regulate the disclosure of information related to money laundering if it is required to be disseminated within the institution, or shared in mutual cooperation with external parties. Particularly, this is very important so that the BCE can comply with requirements of transparency and accountability.
(BIS, 2006, s. 779) when critical financial information is related to capital requirements, actual risk profile, and the capital adequacy of the institution (BIS, 2009, s. 4, p. 29; 2006, s. 809).

2.3.2. Regulating Employee Behaviour

In order to properly manage critical information related to money laundering in the BCE, the implementation of procedures and controls to ensure adequate screening when hiring and training employees is important (FATF, 2003, rec. 15).

Specifically, according to the criteria given by the FATF, the BCE should regulate the following aspects related to employee behaviour, and cooperation in money laundering detection (FATF, 2003, rec. 14):

a) Protect sensitive information related to money laundering and its *predicate offenses* from being disclosed by the BCE’s directors, officers, and other employees
b) Find legal provisions to protect the BCE’s directors, officers, and employees after having collaborated in criminal or civil cases related to money laundering, or its predicate offenses
c) Prevent the unauthorised disclosure of *Suspicious Activity Reports ‘SARs’*, or related information, which is or has been reported to the FIU
d) Verify the validity of agents that are employed to provide money exchange service using wire transferences (FATF, 2001, lit. VI, VII).

However, even though the FATF has given these criteria for employee screening, they do not specify the way of ensuring the protection of information *before, during and after acquiring contractual obligations* with an employee. Thus, it would be necessary to identify an effective way to align employees’ responsibilities with the money laundering detection requirements given by the FATF.

2.3.3. Regulating Customer Activity

The FATF advices that *Customer Due Diligence Policies* must be set in the BCE in order to identify customers, validate their identification data, and keep records of their identity *before, during, and after* any financial event (FATF, 2003, rec. 5).
First, **before a financial event** (see p.25), identification and verification of existing customers, new customers, casual customers and beneficial owners must be supported by copies or records of official and reliable documents (FATF, 2003, rec. 5 (a), (d); rec. 10). Additionally, in case of **politically exposed persons**, beyond the controls already mentioned, the **BCE** must conduct enhanced monitoring activities of their business relations (FATF, 2003, rec.6 (b), (d)) such as market risk assessment by identifying risk exposure groups (BIS, 2006). In fact, it can be inferred that **assessing market risk** can help the **BCE** monitor the relationship between customer’s business activities and **market risk**; especially, if they are **politically exposed persons**.

Second, **during any financial event** (p.25), like establishing business relationships or conducting transactions, records of identity data must be kept along with transaction validation, and personal information verification (FATF, 2003, p.5). Thus, validating transactions is important in order to identify suspicious transactions or patterns that may be linked to money laundering. Additionally, since non-financial businesses and professions, along with non-profit organisations may be money laundering targets (FATF, 2003, rec. 11), additional transaction verification and data validation requirements related to such businesses or professions have to be considered.

Finally, **after any financial event** (see p.26), information must be kept for at least five years along with customer identification data and all necessary transactional records (FATF, 2003, rec. 10) in order to evaluate and determine to either finish the relationship with a suspicious customer (FATF, 2003, rec. 5), or make a **Suspicious Activity Report ‘SAR’** (FATF, 2001, lit. IV), if required.

Therefore, assessing **Market Risk** should be considered not only to monitor customer’s business activity before and during a financial event (FATF, 2003, rec. 5 (d)), but also to justify **SARs** by providing evidence which links potential money laundering activities with **market behaviour**. Also, analysing a single or a group of exposures, as part of the **market risk assessment** strategy (BIS, 2009, s. 27, p.15), money laundering risk can be associated to **risk concentration sets** (FATF, 2004, p.17). Thus, monitoring transactions before, during and after a financial event allows the **BCE** to promptly report money laundering suspicions to the **FIU**.
for its later investigation by means of SARs (FATF, 2004, p.25) supported by market movement evidence related to the business profile of a suspicious customer.

2.4. Scope of a Money Laundering Detection Strategy

As national responsibility, the Central Bank of Ecuador ‘BCE’ should find the way to develop special techniques for investigating money laundering. In fact, this can be achieved by establishing permanent or temporary groups specialised in asset investigations which are able to identify and acquire evidence supported by documents, information, and transactional records so that they can be used during investigations, prosecutions and related actions (FATF, 2003, rec. 27, 28, 30).

First, due to the fact that criminal and civil litigations, including money laundering cases, may require to find admissible evidence stored in electronic media, the BCE should consider the adoption of Electronic Discovery or ‘e-discovery’ strategies (Osterman Research, 2010) in which the process of collection, preservation, validation, identification, analysis, interpretation, documentation, and presentation of Electronically Stored Information ‘ESI’ as evidence, can sometimes rely on the proper application of Computer Forensic Practices and Tools (Palmer, 2001). Moreover, regarding the production of any information, supervisors\(^1\) in the BCE should be allowed to monitor, and ensure compliance in the application of practices to combat money laundering, including conducting inspections, compelling the production of relevant ESI, and impose administrative sanctions for failure to comply with such requirements (FATF, 2003, rec. 29).

Conversely, due to the fact that money laundering activities can affect the minimum capital requirements of the BCE (see s. 2.2, p.4), the revision of capital assessment procedures also entails the revision of money laundering detection strategies because these may be considered as supporting capital assessment processes (BIS, 2006, s.721), and therefore, attached to the following financial regulations:

a) Align capital targets with the financial institution’s risk profile (BIS, 2006, s.721)

---

\(^1\) Supervisors are designated competent authorities responsible for ensuring requirement-compliance in the financial institution to combat money laundering and terrorist financing (FATF, 2003, p.17).
b) Incorporate the relationship between the amount of capital held by the bank and its risks along with the strength and effectiveness of the operational risk measurement methodologies (BIS, 2006, s.723)

c) Support supervisors to evaluate the capital needs and their risks in the financial institution for fostering an active dialogue inside or outside the financial institution (BIS, 2006, s.722). I.e., establishing internal and external disclosure policies

d) Establish internal controls over the disclosure process for assessing the appropriateness of the disclosures, including validation and frequency of them (BIS, 2009, s.14, p.12). I.e., assessing the effectiveness of the evidence used in the production of SARs

Finally, by including computer forensic practices, the BCE should be able to provide ESI, as admissible evidence derived from the application of a proper anti-money laundering strategy. Also, by aligning the business goals with the detection strategy to measure, and secure the minimum capital requirements, the BCE should be able to identify the operational risk linked to money laundering activities so that more effective controls can be provided based on the suspicious activities detected and the evidence behind them.

Hence, the BCE management strategy can be involved in the application of the policies (BIS, 2009, s.16, p.13) for the effective communication of money laundering risk. Moreover, any necessary adjustments to the strategic plan can be justified, considering the previous statement (BIS, 2006, par. 743) in order to continuously improve the overall anti-money laundering strategy.

2.4.1. Measuring the Effectiveness of the Detection Strategy

In order to measure the effectiveness of its detection strategy, the BCE should apply the following statistics (FATF, 2003, rec. 32):

a) Number of SARs received and disseminated by category (e.g., money laundering and terrorist financing investigations)

b) Number of prosecutions and convictions related to SARs

c) Percentage/Number of property frozen, seized and confiscated related to reported suspicious events
d) Number of SARs on mutual legal assistance, or international requests for co-operation

On the other hand, considering the relationship between the BCE’s capital assets and the operational risk (see s. 2.4, lit. b), the effectiveness assessment through statistics may not be enough because the relationship between money laundering risk and business lines is omitted (Financial Services Authority, 2008, p. 9). In addition, in order to identify these business lines, the operational risk in the BCE has to be measured by applying methodologies based on risk sensitivity and sophistication levels (BIS, 2006, par. 645-646).

Finally, the relationship between operational and money laundering risk can be justified as shown in the following propositions, based on the statements discussed before:

a) Since the operational risk is closely related to the business lines (prop. 1),

\[ \text{operational risk} \rightarrow \text{business line identification} \] (1)

b) And these can be also linked to money laundering risk (prop. 2);

\[ \text{money laundering risk} \rightarrow \text{business line identification} \] (2)

c) Then, operational risk implies money laundering risk identification (prop. 3):

\[ \text{if} \ (1) \rightarrow (2) \therefore \text{operational risk} \Leftrightarrow \text{money laundering risk} \] (3)

Hence, the detection strategy should be assessed not only by implementing the statistics given by the FATF, but also by measuring the operational risk so that the risk of loss resulting from inadequate or failed internal processes (BIS, 2006, par. 644), can be linked with the effectiveness of the money laundering detection strategy, and aligned with the operational risk assessment strategy.

2.5. **Legal Instruments in the Ecuadorian Laws to Criminalise Money Laundering Activities**

The FATF states that money laundering must be considered a serious offence which has to be criminalised in every country (FATF, 2001, lit. I). Also, in case that the offence is committed in other country, but represents either a predicate offence, or collateral offence in
the local jurisdiction, it can be managed as both domestic and external offence (FATF, 2003, rec. 1, 2, 39; 2001, lit. V), due to the fact that business relationships may entail cross-border transactions (FATF, 2003, rec. 7). Hence, in order to achieve this aim, the Ecuador’s National Assembly issued a Law to Repress Money Laundering (National Assembly, 2005) and its correspondent Reformatory Law (National Assembly, 2010) in which the following main aspects are covered (Table 2.1):

Table 2.1-Legal Instruments to Repress Money Laundering in Ecuador

<table>
<thead>
<tr>
<th>Scope</th>
<th>Instrument</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Money Laundering Enforcement</td>
<td>- Prevention, and sanction of money laundering and predicate offences (National Assembly, 2005, art. 1)</td>
</tr>
<tr>
<td></td>
<td>- Reporting of unusual banking transactions using SARs supported by legal admissible evidence (National Assembly, 2005, art. 2)</td>
</tr>
<tr>
<td></td>
<td>- Establishment of policies and procedures to prevent money laundering in the Ecuadorian financial institutions (National Assembly, 2005, art. 8 (a))</td>
</tr>
<tr>
<td></td>
<td>- Prevention of unauthorised disclosure of money laundering information (National Assembly, 2005, 4th general provision)</td>
</tr>
<tr>
<td></td>
<td>- Confiscation of unlawful assets (National Assembly, 2010, art. 1(c))</td>
</tr>
<tr>
<td>Anti-Money Laundering Strategies</td>
<td>- Registration of customer’s information using electronic media (National Assembly, 2005, art. 3 (a))</td>
</tr>
<tr>
<td></td>
<td>- Recording financial information (National Assembly, 2010, art. 4 (a))</td>
</tr>
<tr>
<td></td>
<td>- Monitoring of financial transactions greater or equal than USD $10,000,00 (National Assembly, 2005, art. 4 (c))</td>
</tr>
<tr>
<td>Extradition</td>
<td>- Allowance to perform the necessary actions and efforts to recover unlawful assets of Ecuadorian origin which may be held abroad (National Assembly, 2005, art. 1 (b))</td>
</tr>
</tbody>
</table>

Therefore, as final consideration, any money laundering strategy adopted inside the BCE should consider within its scope, the legal instruments presented in the anti-money laundering laws in Ecuador so that it can be supported by the local law, and by the recommendations given by the FATF.
2.6. Conclusions

2.6.1. Lack of Forensic Computing Practices within the Anti-Money Laundering Recommendations

Even though the usage of e-discovery practices, including Computer Forensics procedures may be implemented to comply with the FATF 40 recommendations (see s. 2.4, p.9), these practices are not explicitly discussed within the anti-money laundering recommendations issued by the FATF (2001; 2003; 2004). Moreover, there is no evidence of internationally recognized or standardised computer forensic procedures related to money laundering detection, mainly due to the constant improvements in technology and the demanding training of computer forensic investigators (Jansen, 2010, p.84).

Hence, it is very unlikely that such practices have been adopted by the BCE in its anti-money laundering strategy, considering that they are not mentioned in the FATF recommendations. Also, if they have not been adopted by the BCE yet, the consequences may be the inaccurate delivery of SARs, the evidence of which must be supported with appropriate digital evidence, which admissibility in court during criminal and civil litigations relies on the procedure for discovering and disclosing such evidence (SANS, 2010). Furthermore, the lack of guidelines to obtain digital evidence in a forensically sound manner can not only delay the reporting process, but also produce that the digital evidence recovered in Ecuador cannot be used in other countries.

2.6.2. Information Technology Management Considerations are not part of Anti-Money Laundering Procedures

After reviewing the FATF recommendations and the Basel Frameworks, there is no strong linkage between these financial frameworks and Information Technology Management considerations. Moreover, since majority of anti-money laundering procedures inside financial institutions worldwide are intensive to create and maintain (Le Khac and Kechadi, 2010, p.577), the lack of IT Management considerations may reduce their effectiveness despite they follow the recommendations given by international bodies like the FATF. Also, if a proper IT Management strategy regarding money laundering is not properly set in the BCE,
the whole internal security may be compromised if the procedures are accessed by criminals with the purpose of bypassing their internal controls (Liu and Zhang, 2008, p.1; 2010, p.210).

Therefore, the BCE should consider not only the financial recommendations suggested in the FATF recommendations and Basel frameworks, but also the implications of implementing them as business goals which have to be aligned with the IT Management strategy for security and risk assessment (Calder and Watkins, 2008, p.45).

2.6.3. Money Laundering Detection using Technology is not fully covered within the Anti-Money Laundering Recommendations

Regarding money laundering threats by means of new and emerging technologies, the FATF indicates that the BCE should adopt policies and procedures to prevent them, considering that technology can act in favour of keeping launderers anonymous; specially, in non-face-to-face transactions (FATF, 2003, rec. 8). Similarly, the BCE should collaborate in proposing enhancements in the current techniques of cash management in order to make them more secure and less vulnerable to money laundering activities (FATF, 2003, rec. 20).

Hence, due to these reasons, the BCE must rely on a proper application and support of the technology available not only to keep records of every single suspicious transaction (FATF, 2003, rec. 11), but also to examine the digital evidence collected in order to deliver accurate and admissible SARs. Therefore, timely assistance may be provided to competent local and international authorities who may require the disclosure of this information during prosecutions (see s. 2.3.1).

2.6.4. Refined Research Questions

After reviewing the frameworks issued by the Bank for International Settlements (BIS, 2006; 2009; 2010) and the recommendations delivered by the Financial Action Task Force (FATF 2001; 2003; 2004), the gaps to solve in terms of money laundering detection to assist the Central Bank of Ecuador are:

a) How to summarise the concepts and definitions previously identified into an Anti-Money Laundering Framework
b) How to align the concepts and definitions previously identified with the IT Management objectives in terms of information security

c) How to define guidelines for handling computer forensic evidence which can support the IT Management objectives related to money laundering detection, the anti-money laundering recommendations given by the FATF, and the capital adequacy requirements defined by the BIS
3. Description of the Anti-Money Laundering Framework

3.1. Introduction

As part of the research strategy, it is necessary to define a knowledge baseline in order to compare the current strategy with a set of best-practices which can justify further actions to change or improve the BCE’s strategy.

Therefore, an Anti-Money Laundering (AML) Framework has been developed in order to not only provide the baseline for evaluating the BCE’s money laundering detection strategy, but also define guidelines to strengthen the BCE’s strategy by incorporating IT standards and computer forensic strategies to ensure evidence admissibility whilst detecting money laundering events.

a) A component-based model considering the FATF recommendations (FATF, 2001; 2003), along with some financial considerations in the Basel Frameworks (BIS, 2006; 2009; 2006)
b) A Plan-Do-Check-Act (PDCA) Process to define a money laundering detection strategy, aligning Information Security requirements and anti-money laundering business goals

However, in order to provide understandability for the reader, in the following sections, the main aspects that have been considered to develop this framework are discussed.

Hence, in sections 3.2 and 3.3, the AML framework definition and its enhancements are discussed, considering the alignment of this framework with the Plan-Do-Check-Act (PDCA) process. Later, the actions taken in order to adapt the PDCA process for money laundering detection is explained in section 3.4. Finally, a general conclusion about the development of the AML framework is given in section 3.5.

3.2. Defining the Anti-Money Laundering Framework

Initially, it was assumed that the FATF recommendations (FATF, 2001; 2003) and the Basel frameworks (BIS, 2006; 2009; 2006) may provide specific guidelines to define an anti-money laundering detection procedure. However, once these documents were reviewed (see s.
2, p.3), it was found that defining a detection procedure is not enough to detect money laundering activities. In fact, this one is just an element of the AML framework obtained from analysing the FATF recommendations and Basel Frameworks (Figure 4.1).

Conversely, as stated by Marshall and Rossman (2011, p.79), a conceptual framework can be developed from the literature review. Thus, the AML Framework provides an understandable approach, outlining not only the FATF recommendations, but also some of the surrounding financial and legal considerations given by the Basel frameworks, and the Ecuadorian legislation, respectively, which were identified in the Literature Review chapter (see s.2, p.3). Actually, adopting this framework allows defining a proper anti-money laundering strategy by covering the whole set of best-practices so that this form of financial crime can be effectively detected.
Nonetheless, since this **framework** is based in the **FATF recommendations** (FATF, 2001, 2003, 2004), it has some limitations such as the lack of both **Computer Forensic Practices** and **IT Management** considerations (see s. 2.6.1 and 2.6.2, p.13) due to the fact that these recommendations are neither a money laundering detection process, nor a strategy.

Consequently, since information is an important asset in any organisation which needs to be protected (BS ISO/IEC, 2007, p. viii), it is necessary to identify the way in which the information related to the components of the **AML Framework** (Figure 4.1, p.17) can be aligned with Information Security management considerations. In the next section, the solution to this problem is explained.

### 3.3. Enhancing the Anti-Money Laundering Framework

The **AML Framework** has to be aligned with the **Information Security** management requirements, along with the necessary practices to handle money laundering-related evidence in a forensically sound manner. In fact, **Information Security** requirements are important to protect information (BS ISO/IEC, 2007, p. Vi; 2009, p.1), such as **capital asset information** (see s. 2.2, p.4), so it can be used to reveal money laundering activities.

Conversely, since the **FATF recommendations** do not consider **Computer Forensic practices** (see s. 2.6.1, p. 13), the **AML Framework** has to incorporate them in order to ensure a reliable and proper delivery of **Suspicious Activity Reports ‘SARs’**, based on an adequate handling of **digital forensic evidence**.

Finally, since decision-making support like process implementation, measurement, and auditing activities are excluded from the scope of this research, the **BS ISO/IEC 27000 standards** that must be analyzed in order to align the **AML Framework** with **Information Security** are shown in Table 3.1:
Table 3.1-BS ISO/IEC 27000 Standards in the Current Research Scope

<table>
<thead>
<tr>
<th>Standard</th>
<th>Characteristics</th>
<th>Security Directives</th>
<th>Risk Directives</th>
<th>Excluded</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27000:2009</td>
<td>Overview and Vocabulary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO/IEC 27001:2005</td>
<td>Requirements</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO/IEC 27003</td>
<td>Implementation Guidance</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>ISO/IEC 27004</td>
<td>Measurement</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Consequently, guidelines to reinforce the BCE’s money laundering detection strategy can be delivered, considering Information Security requirements) for protecting capital asset information. In fact, this can be achieved by adopting the PDCA process in order to align the AML Framework with the Information Security requirements.
3.3.1. Adopting the PDCA Process

Adopting the PDCA process allows aligning its phases with the AML Framework requirements (Table 3.2), following the model proposed in the BS ISO/IEC 27005:2011 standard (2011a, p. 9).

**Table 3.2-Alignment of the PDCA process with the AML Framework**

<table>
<thead>
<tr>
<th>PDCA Phases</th>
<th>Information Security Management</th>
<th>AML Framework Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plan</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish AML Requirements</td>
<td>Define the Scope</td>
<td>- Consider the Legal Instruments (L) within the AML framework scope</td>
</tr>
<tr>
<td></td>
<td>Define the Policies</td>
<td>- Protect information systems related to managing capital asset information (AP)</td>
</tr>
<tr>
<td></td>
<td>Define an Incident Management Strategy</td>
<td>- Establish Internal and External Disclosure Policies (IEDP)</td>
</tr>
<tr>
<td></td>
<td>Define a Risk Treatment Plan for ML detection</td>
<td>- Define Know-Your-Employee (KYE) and Know-Your-Customer Policies (KYC)</td>
</tr>
<tr>
<td>Define the Information Security Risk Strategy</td>
<td>Define Control Objectives based on Risk Treatment Plan</td>
<td>- Define actions before, during, and after a money laundering incident takes place in order to align KYC policies with an incident management strategy</td>
</tr>
<tr>
<td>Do</td>
<td>Implement and Operate the AML Framework</td>
<td>- Consider the assessment of operational risk (ORA) for Money Laundering Detection</td>
</tr>
<tr>
<td></td>
<td>Implement the Risk Treatment Plan</td>
<td>- Define control objectives for risk treatment regarding the scope, policies, procedures, documentation and record requirements</td>
</tr>
<tr>
<td>Check</td>
<td>Monitor and Review the AML Framework</td>
<td>- Ensure the effectiveness of the detection procedure, and disclosure policies (DPA)</td>
</tr>
<tr>
<td></td>
<td>Review and monitoring of ML risks</td>
<td></td>
</tr>
<tr>
<td>Act</td>
<td>Maintain and Improve the AML Framework</td>
<td>- Ensure the implementation of relevant updates and enhancements to the AML Framework</td>
</tr>
<tr>
<td></td>
<td>Conduct regular revisions and enhancements</td>
<td></td>
</tr>
</tbody>
</table>
This alignment is necessary because the *FATF recommendations* (FATF, 2001; 2003; 2004) and the *Basel Frameworks* (BIS, 2006; 2009; 2010) are not enough to define an anti-money laundering strategy because they do not consider *security breaches, organisational asset misuse, and digital evidence handling*.

First, a security breach, or *attack* is ‘an attempt to make unauthorized use of an asset within the organisation’ (BS ISO/IEC, 2009, p.1). Then, *money laundering activities* can be considered as a *security breach* because, although they may not be directly related to computer crimes, they involve the misuse of the financial assets to launder unlawful proceedings (Le Khac and Kechadi, 2010, p.577).

In contrast, since such assets can be tangible and intangible (BS ISO/IEC, 2009, s. 2.3), *money laundering detection* is not merely related to the application of financial considerations, indeed, it involves the *deployment of security policies* to protect the *Information Systems* (tangible assets) which manage the *Financial Information* (intangible assets). Thus, applying security policies and financial considerations can support the delivery of SARs based on accurate information, as *digital evidence*.

Finally, aligning the *AML framework* (see s. 3.2, p.16) with *IT management standards* (see s. 3.3, p.18) is important for handling *money laundering-related evidence*. In fact, admissible digital evidence may be an important asset to justify suspicious transactions. Also, since the acquired evidence can be requested in cross-border investigations (FATF, 2003, rec. 40), this alignment can ensure proper management of the information related to *minimum capital requirements* (see s. 2.2, p.4).

In summary, the *PDCA process* (BS ISO/IEC, 2005) has been adopted by aligning the *AML Framework* requirements with the *PDCA phases*. As a result, *money laundering investigations* can be supported by *Suspicious Activity Reports* based on admissible digital evidence, which has been obtained from secure information related to the *BCE’s capital assets*. However, in order to integrate financial considerations and Information Security requirements, the *PDCA process* has to be adapted for money laundering detection.
3.4. Adapting the PDCA Process for Money Laundering Detection

As mentioned in the previous section, in order to enhance the AML Framework (Figure 4.1, p.17) by incorporating the Information Security Management requirements (BS ISO/IEC, 2009), it is necessary to adopt the PDCA process (BS ISO/IEC, 2005, p.vi) so that the AML Framework requirements can be aligned with the PDCA phases (Figure 3.2). However, this process has to be adapted to the context of money laundering detection to handle related evidence (BS ISO/IEC, 2011b) in a forensically sound manner.

Figure 3.2-PDCA Process of the AML Framework

First, it is required to identify the scope of the AML framework, to define business objectives related to money laundering detection perfectly aligned with a strategy to protect information assets (BS ISO/IEC, 2009, s.3.2.1).

Second, Know-Your-Customer ‘KYC’ policies are required to be aligned with the money laundering detection requirements (FATF, 2001, lit. IV), and included in the PDCA process. Since they play an important role to regulate customer behaviour, their contribution is important to support financial transparency requirements (BIS, 2006, s. 779) and to comply with the anti-money laundering law in Ecuador (National Assembly, 2005; 2010)

Finally, since digital evidence must be relevant, sufficient, and repeatable (BS ISO/IEC, 2011b, s. 5.3), the KYC policies have to be aligned with Computer Forensic practices. Particularly, the top-down approach (Zhang and Wang, 2009, p.104) has been adopted to
analyse digital evidence related to money laundering by converting general aggregation levels of information into specific relevant pieces of evidence.

Hence, identifying the AML framework scope, aligning KYC policies with money laundering detection requirements, and aligning KYC policies with Computer Forensic practices are discussed in the next subsections in order to cover the most relevant aspects that have been adopted for adapting the PDCA process (Figure 3.2, p.22) for detecting money laundering.

3.4.1. Identifying the Scope of the AML Framework

Adopting Information Security Management strategies (BS ISO/IEC, 2009, s.3.2.1) allows defining clear requirements about what is intended to achieve by protecting information assets from security breaches. Particularly, when detecting money laundering, these security requirements have to be linked not only to the FATF recommendations (FATF, 2001; 2003; 2004), but also to the financial goals discussed in section 2.2 (p.4) regarding the adequate management of minimum capital requirements in the Basel framework (BIS, 2006). In fact, since the legal aspects and the location of tangible and intangible assets (BS ISO/IEC, 2009, s. 2.3) must be considered, the Legal Instruments provided by the Ecuadorian legislation and the identification of the information systems in charge of managing Capital Asset information in the BCE should be included in the AML Framework Scope.

First, incorporating the Legal Instruments in the AML Framework enables the BCE to identify the scope of the anti-money laundering enforcement in the Ecuadorian legislation. For instance, the sanctions applied to money launderers (National Assembly, 2005, art. 1), and the admissible evidence that should be included as part of the Suspicious Activity Reports ‘SARs’ should be considered (National Assembly, 2005, art. 2).

Second, as discussed in section 2.2 (p.4), Capital Assets can be seized if related to money laundering activities (FATF, 2003, rec. 3, 13, 38; 2001, lit. III). Then, sources of Core and Supplementary Capital, along with Liquidity sources (BIS, 2006, p. 6,14, 155, 156) must be identified. Thus, as part of a proper Information Security Management strategy (BS ISO/IEC, 2007, s.7) to detect money laundering, the Information Systems related to Capital Assets have
to be protected in order to establish policies to secure the information related to them, which may be used as digital evidence during civil or criminal litigations.

Therefore, once the capital sources have been identified, the establishment of policies related to money laundering detection within the BCE can be supported by accurate financial information, and the effective application of the national legal instruments available.

3.4.2. Aligning Know-Your-Customer Policies with Money Laundering Detection Requirements

Although the AML Framework discusses the requirements to establish Internal and External Disclosure Policies, Know-Your-Employee policies, and Know-Your-Customer policies, the latest are the most relevant because SARs must demonstrate illegal customer activities. Thus, in this section the KYC Policies (Figure 4.3) are explained.

![Figure 3.3-Know-Your-Customer Policies Workflow](image)
A) **Before an Incident:**

Before a financial event takes place, the verification of customers (FATF, 2003, rec. 5 (a), (d); rec. 10) should go further and conduct enhanced monitoring activities of customer’s business relations (FATF, 2003, rec. 6 (b), (d)) based on *market risk assessment and risk exposure groups identification*.

First, *Market Risk Assessment* is important in order to monitor the relationship between customer business activities and market risk; especially, if these customers are politically exposed persons (FATF, 2003, rec. 6(c)). Therefore, the methodologies for assessing market risk (BIS, 2006) should be considered not only to enhance monitoring activities of customer’s business activity, risk profile and source of funds (FATF, 2003, rec. 5 (d)), but also to justify SARs by providing evidence which links potential money laundering activities with *Market Risk* assessment information.

Conversely, *Risk Exposure Group Identification* is advisable so that the BCE can analyse a single or a group of exposures as part of its *Risk Concentration* strategy (BIS, 2009, s. 27, p.15). Consequently, a proper anti-money laundering strategy should identify the possible anti-money laundering exposures in *risk concentration sets* (FATF, 2004, p.17).

Concluding, assessing *market risk*, and identifying *risk concentration* sets allows enhancing the validation of customer’s business activities; especially, if they are politically exposed persons. Also, implementing these considerations within the *KYC policies* allows identifying *risk concentrations per each segment of the market* (BIS, 2009, s. 32, p.16), enhancing the overall risk exposure assessment by considering the correlated risk factors that may arise from market risks (BIS, 2009, s. 28, p.15-16).

B) **During any financial event:**

During the course of any financial event, records of identity data must be kept along with transaction validation, and personal information verification (FATF, 2003, p.5) in order to identify suspicious transactions, or patterns that may be linked to money laundering activities. Additionally, since *non-financial businesses and professions*, along with *non-profit organisations* may be money laundering targets (FATF, 2003, rec. 11), further transaction verification and data validation requirements related to such businesses or professions have to be considered.
Therefore, if any transaction matches any of the previous criteria, the BCE should report such concerns to the FIU for its later investigation by means of SARs (FATF, 2004, p.25). Moreover, if money laundering suspicions are related to market movements, the generation of SARs should be supported by market movement-related evidence, considering the Market Risk Assessment information.

C) After any financial event:

Once the financial event finishes, related information must be kept for at least five years along with customer identification data and all necessary transactional records (FATF, 2003, rec. 10) in order to evaluate and determine:

a) Whether or not carrying on with further financial event with such customer; e.g. opening an account, establishing business relationships, or performing other transactions (FATF, 2003, rec. 5)

b) Make a SAR in relation to that customer (FATF, 2001, lit. IV) under suspicions or demonstrated events related to money laundering

Thus, keeping records and financial information after any financial event allows the BCE reconstructing individual transactions (including the amounts and types of currency involved) to provide evidence of criminal activity.

3.4.3. Aligning Computer Forensic Practices with Know-Your-Customer Policies

As mentioned in the previous section, money laundering, and its predicate offences are criminal activities mainly performed by customers which may use the BCE’s assets in order to change illegal income into legal (Le Khac and Kechadi, 2010, p.577). However, the PDCA process (BS ISO/IEC, 2005) does not incorporate Computer Forensic practices.

Consequently, Computer Forensic practices (Figure 3.4, p.27) have been incorporated in the PDCA process (Figure 3.2) as part of the incident management strategy.
This approach allows the BCE to investigate money laundering incidents by the application of computer forensic practices to handle digital evidence based on customer information. In addition, following Computer Forensic practices to handle money laundering evidence provide a straightforward process, which any external party can follow in order to achieve the same outcomes (ACPO, 2011, principle 3); in particular, whilst collaborating with money laundering investigations overseas (FATF, 2003, rec. 40).

Finally, in order to cover the scope of the KYC policies, this detection procedure incorporates a 3-phase model (Grobler, Louwrens and Von Solms, 2010, p. 678) which has been applied before, during, and after any money laundering incident takes place. Also, the activities outlined in the Case-Oriented Evidence Model proposed by Zhang and Wang (2009) are included to understand, analyse, evaluate, and report money laundering activities.

Therefore, as shown in Figure 3.4, this simple process may assist the BCE in aligning the KYC policies with an incident management strategy to detect suspicious transactions before, during, and after any financial event. In the following sections, the detection strategy implemented in the AML Framework for the BCE is explained.
3.4.4. Understanding the Case Requirements before Investigating Money Laundering Activities

Before detecting a money laundering event (Figure 3.4, p.27), it is necessary to understand the case since money laundering activities are different from any other form of crime (Zhang and Wang, 2009). Hence, understanding the background and evidence sources within the context of the Know-Your-Customer (KYC) policies is required so that the employees in charge of money laundering investigations can know what exactly they should be looking at before a money laundering incident occurs.

Understanding the case background involves identifying the risk concentration sets to identify customers who are more likely to be involved in money laundering activities, and investigate them as soon as possible; for instance, when they are politically exposed persons (FATF, 2003, rec.6 (b), (d)).

Then, identifying evidence sources within corporative databases (Wright, 2009a) is required. As a result, the BCE’s databases related to the Information Systems in charge of managing Capital Asset Information can be used as evidence sources. Besides, whilst performing this, documents with valuable customer information should be transferred to electronic formats (Panigrahi, 2011, p.325).

Accordingly, once the background and evidence sources have been identified, business goals according to the KYC policies can be defined (Panigrahi, 2011, p.325), considering not only the anti-money laundering requirements, but also the evidence related to them in order to prove money laundering activities, and violation of the BCE’s KYC policies (Kieseberg et al., 2011, p.282).

3.4.5. Adapting the Top-Down Approach for Customer Data Analysis

Once the relevant evidence sources have been identified when understanding the case, the top-down approach suggested by Zhang and Wang (2009) can be adapted into a real-world database analysis scenario in order to define how the evidence should be identified, collected, acquired, and preserved (BS ISO/IEC, 2011b) during any money laundering incident.
First, considering that digital evidence must demonstrate relevance, sufficiency, and repeatability (BS ISO/IEC, 2011b, s. 5.3), the top-down approach proposes to analyse the case, converting general aggregation levels of information into specific relevant pieces of evidence (Zhang and Wang, 2009, p.104). Additionally, by following the top-down approach, the Case Analysis phase is justified by a logical method to validate the steps followed so that their repeatability can be ensured at any stage of the investigation (BS ISO/IEC, 2011b, s. 5.3.3). Hence, relevant information can be extracted from the evidence sources (case attributes) in order to collect sufficient evidence. For instance, recognizing the case attributes can provide relevant evidence (Pavlou and Snodgrass, 2008, p. 30:3), such as background, identity data, location, and time of the money laundering event.

Next, taking into account that preserving information in common database repositories for further forensic analysis is important (Computer Database, 2011), analysing the acquired information should be required not only for verifying customer information during any financial event, but also for its subsequent storage into a de-normalised evidential database. Consequently the BCE can justify actions (BS ISO/IEC, 2011b, s. 5.3.5) to detect money laundering events whilst facing evaluations by independent assessors or authorised counterparties (BS ISO/IEC, 2011b. s. 5.3.2).

Finally, conventional computer forensic practices might not be suitable when analyzing large amount of transactional data stored in database servers (Wright, 2009a) since they are considered mission-critical devices (BS ISO/IEC, 2011b, s. 7.1.3.3). Therefore, the PDCA process of the AML Framework can be adapted for money laundering detection by defining a proper evidence examination strategy to analyse large transactional data sets (BS ISO/IEC, 2011b, s. 5.2 (b)) which is explained in the next section.

**3.4.6. Applying the Top-Down Approach for Evidence Acquisition and Examination**

The top-down approach can be very useful not only to identify the relevant pieces of evidence from large data sources, as it was explained in the previous section, but also to associate them with the business requirements outlined in the KYC policies in order to ensure the acquisition and examination of evidence supported by reliable information related to
suspicious transactions. Thus, in this section, the most relevant aspects considered in order to define the acquisition and examination phase during the investigation of money laundering events are explained (Figure 3.5).

**Figure 3.5-Digital Evidence Analysis during a Money Laundering Investigation**

A) **Evidence Identification:**

During the Case Understanding Phase, the business goals outlined in the KYC policies must be linked with evidence sources or case attributes stored in the BCE’s databases.

Then, a de-normalised database should be created to store relevant information extracted from the evidence sources (BS ISO/IEC, 2011b, s. 5.4.2) to support money laundering investigations (Panigrahi, 2011, p. 325).

B) **Evidence Collection:**

Collection of digital evidence requires moving potential evidence sources to a controlled environment for its later acquisition and examination (BS ISO/IEC, 2011b, s. 5.4.3). Particularly, considering that money laundering evidence is presented in logical form, the ETL process can be adopted to acquire, transform/clean, and load the evidential data into the de-normalised database. Thus, it ensures that, in spite of having different evidence sources (Cohen, Bilby and Caronni, 2011, p. 101), they can be securely collected, transformed, and loaded into the controlled environment, which would be the de-normalized evidential database in this case.

C) **Evidence Acquisition:**


Although, during criminal investigations involving fraud, an analysis of the whole database has been suggested (Panigrahi, 2011, p. 325), doing so may be counterproductive in money laundering investigations due to the large amount of transactional data. Therefore, the examination of the entire database can be omitted if the evidence sources have been properly identified and securely loaded into the de-normalised database. Consequently, stored procedures (Figure 3.6) may be used (Kieseberg et al., 2011, p.282) as evidence extractors to query the de-normalised database to retrieve information which can be stored as database logs in form of plain text files; e.g. CSV files.

```
CREATE PROCEDURE 'csv_log' (IN amount DECIMAL, IN start_date DATETIME, IN end_date DATETIME)
BEGIN
    SET @threshold = amount;

    SELECT * FROM `de-normalised_database`.tb_transactions
    WHERE tb_transactions.trans_amount >= @threshold
    AND trans_date BETWEEN start_date
    AND end_date
    INTO OUTFILE '/home/root/Documents/MySql Forensic Logs/backup.csv'
    FIELDS TERMINATED BY ','
    OPTIONALLY ENCLOSED BY '"'
    LINES TERMINATED BY '
';
END
```

Figure 3.6-Creating Database Logs as Evidence Files

Then, depending on the BCE’s needs, when detecting money laundering activities, these logs can be used as supporting evidence for Suspicious Activity Reports. As a result, security breaches against the KYC policies can be justified when transactions are greater that the designated threshold given by the FATF.

D) Evidence Preservation:

Digital evidence acquisition must be done in a least intrusive manner to avoid data alteration (BS ISO/IEC, 2011b, s. 5.2); particularly, since operations in transactional databases are not read-only, and can update, delete, or insert data (Ozsu & Valduriez, 2011, p.15). In fact, since database logs may represent snapshots regarding the current evidential state of money laundering activities, they may be considered a new form of volatile evidence and must be analyzed accordingly (Casey, 2010).

On the other hand, since traditional computer forensic techniques cannot be applied, such as shutting down the device and hard drive extraction, the normal operation of the database
server has to be protected (Wright, 2009b). Consequently, selective evidence imaging or triaging (Cohen, Bilby and Caronni, 2011, p.S102) can be used as a strategy to preserve evidence (BS ISO/IEC, 2011b, s. 5.4.5) by imaging only the relevant log files. Thus, the database server and the original log files can be protected against corruption and manipulation (ACPO, 2011, principle 1) because they constitute money laundering evidence.

3.4.7. Evaluating Evidence Admissibility

Once the case has been analysed, it is necessary to validate the forensically obtained evidence (Pavlou and Snodgrass, 2008, p.11) in order to know if it can be admissible in a money laundering case. This is an improvement which has been included as part of the PDCA process in order to verify whether or not the investigation has demonstrated an illegal activity related to money laundering, which, indeed, requires to be reported.

First of all, the obtained evidence has to prove a direct breach against the KYC Policies, which may involve customer information validation (FATF, 2003, rec. 5), suspicions regarding politically exposed persons (FATF, 2003, rec.6 (b), (d)), and money laundering risk exposures derived from either market risk (BIS, 2006, s. 49(xiii)), or subjacent risk concentration exposures (BIS, 2009, s. 27, p.15).

Secondly, the BCE must ensure that the obtained evidence is auditable (BS, 2008, p. 9-10), providing relevant information to reconstruct the sequence and details of activities related to the original data stored in the information systems in charge of managing the capital assets (BS, 2008, s. 4.5.4.1 (a)). Moreover, this linkage should support the acquisition of information stored as case attributes in the de-normalised evidential database.

Third, the BCE has to verify the information related to the suspicious business relationships and transactions (FATF, 2003, p.5), and the validity of the information processed by the Information Systems related to the Capital Assets). In fact, the BCE must ensure that the access to these information systems (BS, 2008, s. 4.5.4.3) has been done in read-only mode. As consequence, data integrity can be maintained by following the steps for acquisition and examination (see s. 3.4.6).
Hence, the case evaluation phase validates digital evidence by verifying not only the security breaches against the KYC policies, but also the integrity of the evidence related to Information Systems which have processed financial information.

3.4.8. Aligning Money Laundering Risk with Information Security Requirements

On top of defining a detection procedure, it is required that managers in the BCE are involved in the process to align money laundering risks with Information Security requirements (BS ISO/IEC, 2005, s. 4.2.1(2), s. 5.1(f)) in order to define a Risk Management Strategy related to money laundering detection.

First of all, the information security risks related to the information systems in charge of processing information of capital assets have to be identified (BS ISO/IEC, 2005, s. 4.2.1(d)).

Then, responsible persons, or ‘owners’ of these information systems have to be assigned in order to monitor threats and vulnerabilities related to these systems (BS ISO/IEC, 2009, s. 2.45, s. 2.46).

Conversely, regarding securing money laundering evidence, the following requirements should be considered:

a) Confidentiality: Protect the information from being disclosed by unauthorized persons, entities or processes (BS ISO/IEC, 2009, s. 2.9). In order to do this, the BCE should align the confidentiality requirements with the Internal and External Disclosure Policies

b) Integrity: Assure the accuracy and completeness of the information (BS ISO/IEC, 2009, s. 2.25). At this stage, the Information Security requirements should be aligned with the requirements for evaluating the information considered as evidence during money laundering investigations

c) Availability: Assure the accessibility and usability of the information related to money laundering detection upon demand by an authorized entity (BS ISO/IEC, 2009, s. 2.7) inside or outside the BCE. To achieve this, the BCE must consider the requirements of
Internal and External Disclosure Policies, and the document and record requirements adopted whilst defining the scope of the AML framework.

Finally, assessing the impacts related to security failures considering the loss of confidentiality, integrity or availability of money laundering-related information should be required (BS ISO/IEC, 2005, s. 4.2.1(e)) in order to define acceptable risk treatment controls.

Therefore, aligning Money Laundering Risk with Information Security requirements can help the BCE protect the information systems in charge of processing information related to capital assets in order to comply with availability, integrity, and confidentiality requirements whilst evaluating the admissibility of money laundering evidence. In fact, a detailed explanation of this process has been included in section, as part of the Guidelines for money laundering detection in the BCE.

3.5. Conclusion

After having applied the PDCA process outlined in the BS ISO/IEC 27001:2005 (BS ISO/IEC, 2005), it was found that this process had to be aligned considering, mainly, the KYC policies, and the detection procedure, in order to make it suitable for money laundering detection.

First, evidence analysis using the top-down approach discussed in section 3.4.5 (p.28), enhances the PDCA process for money laundering detection by aligning the KYC policies with a proper incident management strategy for evidence preservation (BS ISO/IEC, 2011b, s. 5.4.5). Thus, the scope of the KYC policies before, during and after a financial event is fully covered so that evidence can be securely obtained and analysed to support the creation of Suspicious Activity Reports (SARs).

Second, the computer forensic-based detection procedure (see s. 3.4.3, p.26) can assist the BCE to properly analyse suspicious transactions by not only identifying the evidence sources, but also storing them into a single repository (de-normalised database) for its later analysis. In fact, handling the evidence sources in a controlled environment (BS ISO/IEC, 2011b, s. 5.4.3) makes the original databases independent from the final evidential repository in order to protect them from manipulation (BS ISO/IEC, 2011b, s. 5.2).
Third, although not discussed as part of this chapter, whilst developing the AML framework, it was required to identify and evaluate options for risk treatment so that the risk assessment strategy (see s. 3.4.8, p.33) can be properly supported by control objectives. In fact, these control objectives (BS ISO/IEC, 2005, Annex A) support the definition of a risk treatment plan to implement and operate the AML Framework.

Summing up, the 3-phase model (Grobler, Louwrens and Von Solms, 2010, p. 678) which has to be applied before, during, and after any money laundering incident (Figure 3.4, p.27) enhances the AML framework by applying the top-down approach (Zhang and Wang, 2009) for evidence acquisition and examination aligned with the KYC policies. Moreover, ensuring consistency in the AML Framework requires the definition of control objectives so that confidentiality, integrity and availability requirements can be outlined into a strategy for money laundering risk management.
4. Conclusions and Recommendations

4.1. Conclusions

4.1.1. Relationship between Operational and Money Laundering Risk

In section 2.4.1 (p.10), it was explained that the *Central Bank of Ecuador ‘BCE’* has to measure the effectiveness of its detection strategy, based on some statistics given by *FATF* (2003, rec. 32). On the other hand, due to the fact that, institutional capital requirements have to be aligned with the institution’s risk profile (BIS, 2006, s.721), the inherent risk related to the capital amount held by the *BCE* should be assessed using *operational risk methodologies* (BIS, 2006, s.723). Moreover, by assessing the *operational risk*, the risk related to *business lines* can be also defined; in particular, *money laundering risk* (Financial Services Authority, 2008, p. 9), which may be useful to justify money laundering activities based on *market movement* and customer business activities (see s.2.3.3, p.7).

Therefore, measuring the effectiveness of detection procedures using the *FATF’s statistics* may not be enough because the *money laundering risk* related to *business lines* is not considered. Actually, assessing *operational risk* can provide information regarding the risk of loss resulting from inadequate or failed internal processes (BIS, 2006, par. 644), which can be derived from an inefficient *money laundering detection strategy*.

4.1.2. Weaknesses in the FATF Recommendations and Basel Frameworks

The *FATF recommendations* (FATF, 2001; 2003; 2004) are a set of best-practices to detect money laundering in any country’s financial system. However, these practices do not consider strategies to handle digital evidence, which may be a disadvantage in *money laundering investigations overseas* (FATF, 2003, rec. 40) because the lack of them may cause that such evidence is dismissed in court.

Also, both the *FATF recommendations* and the *Basel Frameworks* (BIS, 2006; 2009; 2010) do not consider *Information Technology Management* on their context, which may
reduce their effectiveness and compromise the internal security of a financial institution, taking into account that business goals must be aligned with the information security strategy (Calder and Watkins, 2008, p.45).

Therefore, this research has analysed not only computer forensic practices (see s.3.4.3, p.26), but also an information security strategy in order to mitigate the mentioned flaws and enhance money laundering detection. By these means, evidence stored in electronic media can be identified during any criminal or civil litigation (Osterman Research, 2010), including money laundering cases. Also, the alignment of the PDCA process (see s.3.3.1, p.20) with the anti-money laundering requirements discovered in the literature review, could define an information security strategy for money laundering detection.

4.1.3. Privacy Issues due to Inadequate Customer Information Handling

This research has found that Know-Your-Customer 'KYC' policies are the most important regulations for money laundering detection because Suspicious Activity Reports ‘SARs’ are based on these policies (FATF, 2001, lit. IV). As a matter of fact, the proper application of them provides evidence so that every SAR disclosed with the Financial Intelligence Unit ‘FIU’ can open a case related to money laundering (FATF, 2004, p.25). Additionally, majority of the evidence provided to the FIU via SARs is comprised of an extensive collection of customer’s suspicious transactions and customer personal data (FATF, 2003, p.5).

However, the FATF recommendations do not consider an appropriate handling of information, which is an important aspect when defining information security policies (BS ISO/IEC, 2007, s.5). Moreover, these recommendations do not establish a procedure to handle money laundering evidence, which is required to be kept for at least 5 years.

Therefore, this issue reveals a need to assess information exchange risk (BS ISO/IEC, 2007, s.6.2) in order to avoid privacy issues related to customer’s information handling because an over reliance on customer information collection is not enough to detect this form of crime.
4.2.  **Recommendations**

4.2.1.  **Protection of Capital Asset Information**

According to the *BIS*, the *BCE* should properly identify and measure its sources of *Core and Supplementary Capital*, along with *liquidity sources* because they constitute *minimum capital requirements* for the proper operation of any financial institution (BIS, 2006, p.6, 14). In addition, considering that these capital assets may be confiscated if found related to money laundering (FATF, 2003, rec. 3, 13, 38; 2001, lit. III), the *BCE* should identify and measure them in order to not only prevent the injection of unlawful capital in the institution (National Assembly, 2010, art. 1(c)), but also to identify the financial risk related to money laundering.

Now, regarding the *information systems* in charge of processing *capital asset information*, these have to be identified and registered in an inventory (BS ISO/IEC, 2007, s.7) so that the *information sources* can be categorised, and linked to the *BCE’s capital assets*.

However, neither the Basel Frameworks nor the FATF recommendations link *information systems* with the *minimum capital requirements* (BIS, 2006, p.6, 14). Therefore, it should be advisable that the *BCE* identify them in order to not only protect *capital assets* from money laundering, but also identify possible sources of evidence for money laundering activities.
5. Personal Reflection

Since Ecuador was blacklisted by the Financial Action Task Force ‘FATF’ due to misunderstandings related to ‘political commitment’ for detecting money laundering (The Economist, 2010), the Central Bank of Ecuador ‘BCE’ was required to regulate its financial activities, and prevent the occurrence of this form of financial crime (National Assembly, 2010). Then, as a sponsored student by the Ecuadorian government, I believed that my research project could provide important aspects in order to enhance the BCE’s detection strategy.

However, getting involved in this project was a significant challenge. In fact, money laundering is a crime related to narcotics trade, bank robberies, frauds, tax evasion, and even corruption (Scott-Joynt, 2002), the nature of which can have different causes and effects, making the analysis of money laundering very disperse. Furthermore, it was very difficult to devise which aspects should be included as a general strategy to strengthen the BCE’s detection strategy, considering the nature of this crime. Hence, I decided to narrow the context of this problem to banking transactions, and using, as preliminary information sources, the FATF recommendations and the Basel Frameworks.

Firstly, the Basel Frameworks (BIS, 2006; 2009; 2010) gave me a deep understanding of the financial requirements to secure capital and liquidity inside the financial institutions; meanwhile, the FATF recommendations (FATF, 2001; 2003; 2004) contributed to outline the practices that should be adopted so that money laundering activities can be detected. At this point, it could be devised that both international regulations can be complimentary one another, due to the fact that the minimum capital requirements (BIS, 2006, p.6, 14) in any financial institution should be secured from any form of financial stress (BIS, 2010, s.1), which may be related to money laundering activities.

Surprisingly, even though the correlation of both international regulations could outline a conceptual framework for money laundering detection, none of them considered the technological aspects related to crime detection and information security. Moreover, this flaw impacted in the research scope since the analysis of the BS ISO/IEC 27000 standard series
was considered, but there was no starting point to integrate information security with money laundering detection.

Subsequently, after a careful analysis of the PDCA process (BS ISO/IEC, 2011a, p.9), I realised that it was flexible enough to incorporate practices and strategies aligned with money laundering detection. Hereby, it was possible to define an information security strategy, named as Anti-Money Laundering ‘AML’ Framework, which is oriented to reinforce the detection of money laundering in the BCE by defining a process to plan, implement, monitor and control this conceptual framework.

Now, regarding the incorporation of computer forensic practices in the PDCA process, it was possible to outline a detection procedure which is aligned with the Know-Your-Customer ‘KYC’ policies (see s.3.4.2, p.24). For doing this, a 3-phase model (Grobler, Louwrens and Von Solms, 2010, p. 678) before, during and after any financial event takes place, was combined with a Case-Oriented Evidence Model (Zhang and Wang, 2009) in order to base the detection procedure on the analysis of suspicious transactions in the BCE’s financial databases. As a result, not only the financial databases linked to minimum capital requirements can be identified (see s.3.4.4, p.28), but also the evidence related to money laundering activities can be properly handled in order to provide relevant Suspicious Activity Reports ‘SARs’ which can be admissible in money laundering investigations overseas (FATF, 2003, rec. 40).

Summing up, even though developing a research project related to money laundering involved analysing large amount of information, the outcomes, in my opinion, are an important contribution to the Central Bank of Ecuador in order to reinforce its detection strategy. First, the AML Framework, incorporates some financial requirements given by the Basel Frameworks, and outlines an understandable model based on the FATF recommendations. Also, having adopted the PDCA model for information security management, allowed aligning the identified financial requirements with information security objectives, including the adoption of a computer forensics-based detection procedure in compliance with the KYC policies. Particularly, the resulting AML Framework has demonstrated being strong enough to help the BCE in defining an anti-money laundering
strategy. In fact, this framework has disclosed with my contacts in Central Bank of Ecuador, who have expressed interest in discussing this research with me.

Personally, I believe that even though a quantitative analysis could not be done, the AML Framework developed in this project proposes a new route for money laundering detection, which have awaken the interest of the Central Bank of Ecuador, during very critical moments of political and economical changes in this, my home country (Ghosh, 2012).
6. Bibliography and References


• Cohen, F. (2009) 'Two models of digital forensic examination', Fourth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, 21 May, Oakland, US.


FATF (2010b) FATF Public Statement, 28 October, [Online], Available: "http://www.fatf-gafi.org/document/55/0,3746,en_32250379_32236992_48966519_1_1_1_1,00.html" [Accessed 31 January 2012].


