جـامـعـة الـشـرق الأوسـط للدراسـات العـليا
MIDDLE EAST UNIVERSITY FOR GRADUATE STUDIES

"Design of Anti Money Laundering Framework for Jordan"

تصميم نموذج فعال لمكافحة غسل الأموال في الأردن

By

Kamel A.A.AL-Mahameed

Supervisor

Professor Mohammad A. Al-Fayoumi

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Information System

Department of Computer Science

Faculty of Information Technology

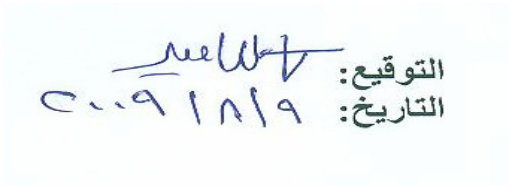
Middle East University for Graduate Studies

Amman - Jordan

July, 2009

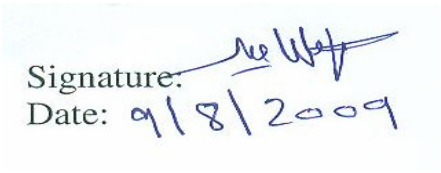
جامعة الشرق الأوسط للدراسات العليا
إقرار تفويض

أنا كامل علي المحاميد أفوض جامعة الشرق الأوسط للدراسات العليا بتزويد نسخ من رسالتي للمكتبات أو الهيئات أو الأفراد عند طلبها.



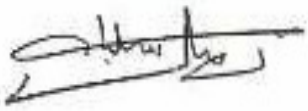
Middle East University for Graduate Studies
Authorization Statement

I am Kamel A.A.AL-Mahameed; authorize the Middle East University for Graduate Studies to supply copies of my Thesis to libraries or establishments or individuals on request.



Examination Committee Decision

This is to certify that the thesis entitled "Design of Anti Money Laundering Framework for Jordan" was successfully defended and proved on August 2009.

Examination Committee Members	Signature
1. Professor Mohammad A. Al-Fayoumi Department of Computer Information Systems; Faculty of Information Technology; Middle East University for Graduate Studies.	
2. Professor Nidal Shilbayah Department of Computer Science; Faculty of Information Technology; Middle East University for Graduate Studies.	
3. Professor Musbah Aqel Department of Computer Science; Faculty of Information Technology; Middle East University for Graduate Studies.	
4. Dr. Abdelfatah Aref Tamimi Dean, Faculty of Science and Information Technology; AL-Zaytoonah University of Jordan.	

Dedication

First and foremost, I dedicate this thesis with love to my treasured parents, who taught me the value of education and who made sacrifices for their children, so that we could have the opportunities they did not have. It is also dedicated to my valued wife and much-loved kids, for their encouragement and love without whom none of this would have been even possible.

Acknowledgments

Many people have encouraged and supported me throughout the writing of this thesis. I would like to acknowledge their contribution by mentioning their names. This research would not have been possible without the great support of them.

Firstly I express my unreserved gratitude and sincere appreciation to my supervisor, Professor Mohammad A. Al-Fayoumi who cautiously and with great care and attention advised and motivated me to produce the final results. Without his supervision the thesis would never have been completed in a satisfactory manner, he was abundantly helpful and offered invaluable assistance, support and guidance.

I am also indebted for the help and expertise provided to me by the members of the Examination committee, without their assistance this study would not have been successful.

Deepest gratefulness to her Excellency Mrs. Khuloud Saqaf, deputy governor of the Central bank of Jordan, and all the officials of the Anti Money laundering Unit at the bank, for helping providing information and encouraging my efforts.

Not forgetting to mention my friends in general and my best friends in particular Mr. Omar S.Al-Masri, Mr. Ramez H.Mallouk, Mr. Ghaleb H.Abbadi, and Engineer Hassan N.Hijazeen who always been there with their valued advice and expertise.

Countless thanks to Central Bank of Jordan Library officials, who offered the library resources and helped me, search for the right books and papers.

I would further like to convey thanks to the Information Technology Faculty members at the Middle East University for Graduate Studies, for helping and encouraging my efforts by providing the library resources and computer laboratory facilities.

Last but not least I would like to express my wholehearted love and gratitude to my dearly-loved family; especially my parents, brothers and sister, my valued wife and my beloved kids Hamzah, Ali, and gorgeous daughter Shatha, for their understanding, endless love, and their never ending moral support and prayers which always acted as a guide through the duration of my academic life.

List of Figures

Figure 2.1: Current model reporting SARs to AMLU-JO	**13**
Figure 2.2: Structure of the current AMLU-JO	**15**
Figure 2.3: Steps of SARs at AMLU-JO	**18**
Figure 2.4: Stages of Money Laundering world wide	**22**
Figure 3.1: Components of AML System	**28**
Figure 3.2: Proposed Logical Diagram for AMLU & DRC. Site	**43**
Figure 3.3: Proposed Backup Connection for AMLU & world	**44**
Figure 3.4: Proposed detailed diagram for AMLU inside network	**47**
Figure 3.5: AMLU-JO Connection with the World	**49**
Figure 3.6: AMLU-JO Security Regions	**52**
Figure 3.7: Database Security Modules	**55**

List of Tables

Table 3.1: Description of AMLUsoft the component of AML System	**37**
Table 3.2 : AMLU Infrastructure Components Description	**38**

Abstract

The objectives of this thesis is to point out and help design and implement an electronically secure framework, for the Anti Money Laundering system working in Jordan particularly and international in general instead of the current manual system, this design is based on a secure network between the Anti Money Laundering Unit, member Banks and financial institutions, from one side and international networks involved in Anti Money Laundering, which will allow Anti Money Laundering Unit at Central Bank of Jordan, member banks and financial institutions to consolidate all of the output from their various anti-money laundering detection and prevention systems and have them processed centrally at the Anti Money Laundering Unit, this secure network should take into consideration the current up and running Real Time Gross Settlement System for Jordan, and the connection between international SWIFT network.

This study also aims to explain how Anti Money Laundering Unit in Jordan, structure is being set up and why; identify the policy priorities best served by current developments, the obstructions and problems of the current process and the contradictions arising in the tracking down of these policies; and analyses the discrepancies between the governance framework and its expected effectiveness. It overcome and examines the obstacles faces regimes, institutions and policies governing the fight against Anti Money Laundering at the local and global level by focusing on the Jordanian drive against money laundering crime.

ملخص

ا لهـدف من هذه الدراسة هو الإشارة والمساعدة في تصميم وتنفيذ حل إلكتروني لنظام مكافحة غسل الأموال في الأردن بشكل خاص ودوليا على وجه آمن وشامل العموم ، بدلا من النظام اليدوي العامل حاليا ، هذا التصميم المقترح سيبنى على شبكة آمنة بين وحدة غسل الأموال والبنوك والمؤسسات المالية الأعضاء في النظام من جهة، وبين الشبكات العالمية المعنية بموضوع المكافحة من جهة أخرى، الأمر الذي سيتيح ، والمؤسسات الأعضاء تدعيم الأموال في البنك المركزي الأردني لوحدة مكافحة غسل وتوحيد المخرجات المتعلقة بالنظام من مختلف أنظمة المكافحة ،والكشف عنها، والوقاية منها ،ومعالجتها مركزيا في الوحدة المشكلة لهذا الخصوص. هذه الشبكة أن تأخذ بعين الاعتبار نظام التسويات الإجمالي الفوري الأردني العامل الآمنة يجب حاليا ، كما يجب مراعاة الربط مع شبكة سويفت الدولية.

كما تهدف هذه الدراسة إلى توضيح التركيب الحالي لوحدة غسل الأموال في وجه من خلال تلك الأردن،والسبب في ذلك، وكيفية تطبيق السياسة العامة على أفضل البنية،وبيان العراقيل والمشاكل العملية والتناقضات التي تنشأ في السعي لتطبيق هذه بين الطريقة العاملة والمخرجات المتوقعة. وسيتم البحث في السياسات، وتحليل التباين تواجه النظم والمؤسسات والسياسات التي تنظم مكافحة طريقة التغلب على العقبات التي الصعيدين المحلي والعالمي من خلال التركيز على الإجراءات غسل الأموال على الأردنية لمكافحة جريمة غسل الأموال.

LIST OF ABBREVIATIONS

ACH Automatic Clearing House
AML Anti Money Laundering
AMLU Anti Money Laundering Unit
AMLU-JO Anti Money Laundering Unit of Jordan
Basel committee in banking supervision
CBJ Central Bank of Jordan
DMZ demilitarized zone
DRC Disaster Recovery Site
E-Government Electronic Government
FATF Financial Action Task Force
HTML Hyper Text Mark-up Language
I-Banking Internet Banking
IMF International monetary fund
KYC Know your customer
LAN Local Area Network
MIS Management Information System
ML Money Laundering
OFAC Office of Foreign Assets Control
RFP Request for proposal
RTGS-JO Real Time Gross Settlement System – Jordan
SAR Suspicious Activity Report
SVPN Secure Virtual Private Network
SWIFT Society for Worldwide Inter-bank Financial Telecommunication
TAD Technical Architecture Document
TCP/IP Telecommunication Protocol / Internet Protocol
XML Extensible Mark-up Language

TABLE OF CONTENTS

Title i
Authorization Statement ii
Committee Decision iii
Dedication iv
Acknowledgment v
List of Figures vi
List of Tables vii
Abstract in English viii
Abstract in Arabic ix
List of Abbreviations x

CHAPTER ONE: ANTI MONEY LAUNDERING
1.1 Introduction 1
1.2 Problem Definition 2
1.3 Area Under Study 4
1.4 Objectives of The Study 5
1.5 Significant of The Study 5
1.6 Motivation 6
1.7 Contributions 7
1.8 Limitations And Delimitations 8

CHAPTER TWO: LITERATURE REVIEW
2.1 Introduction 9
2.2 History of AML efforts 9
2.3 Money Laundering Risks 10
2.4 Technical Research, Development And Implementation 12
2.5 Current AML Systems 14
2.6 Tasks of The AMLU-JO 15
2.7 Steps of SAR's at AMLU-JO 16
2.8 Stages of Money Laundering 19
2.9 AML Regulators And Institutions 22
2.9.1 Financial Action Task Force 22
2.9.2 Office of Foreign Assets Control 23
2.9.3 Basel committee in Banking Supervision 24
2.9.4 International Monetary Fund 24

CHAPTER THREE:THE AML FRAMEWORK

3.1 Introduction 25
3.2 AML Solutions – overview 26
3.2.1 Role of Technology on AML 27
3.2.2 A classic AML Solutions 29
3.2.3 Traditional Configuration of AML 29
3.2.4 Traditional AML Detective Approaches 30
3.3 Efficient AML Wide-Ranging Solution Features 32
3.4 Used Methodology 34
3.4.1 AML Technical Education And Awareness 34
3.4.2 Model Design And Development 34
3.4.3 Secure Network and Software Operational Activities 35
3.5 The Proposed AML Infrastructure in a Glance 36
3.5.1 AMLU net Alert Message Flow 38
3.5.2 The AML Software Application 40
3.6 Impact Changes on Jordanian Financial Institutions 41
3.7 New Proposed Design In Detail 43
3.7.1 Network Security 46
3.7.2 Proposed Environment Security Region 47
3.7.3 Concepts of AMLU Security Areas 48
3.8 Specific Security Issues 54
3.9 Efficiency of The New Proposed Design 56

CHAPTER FOUR: RESULTS AND DISCUSSION

4.1 Introduction 57
4.2 Technology - Answer of Awareness 58
4.2.1 How Does Jordan Measure up Regarding This Study? 58
4.3 Advantages of The Design 60
4.4 Validation of The Results of The Design 61
4.5 Securing AMLU Transactions 62
4.6 Protecting Anti Money Laundering Alerts Records 62
4.7 Particular Vulnerabilities, Troubleshooting & Auditing 63
4.8 Firewall Configuration, Securing The Data, Reporting & Review 64
4.9 Key Features & Key Functionality 66

CHAPTER FIVE: FUTURE WORK
5.1 Conclusions 68
5.2 Future Work 70
5.2.1 Other Information Gaps 70
5.2.2 Recommendations For Future Work 71

References 73
Appendix A 78
Appendix B 79
Appendix C 80

CHAPTER ONE

MONEY LAUNDERING

1.1 Introduction

Money Laundering as defined by the Jordanian AML Law No. 46 for the year 2007 is " Every conduct involving acquisition, possession, disposing of, moving, managing, keeping, exchanging, depositing, investing of funds or manipulating it's value or movement and transferring, or any action that leads to conceal or disguise it's source, origin nature place, disposition mean, ownership or related rights, with knowledge that the funds are proceeded of one of the crimes stipulated in the law." [http://www.amlu.cbj.gov.jo/].

In other words it means the goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the work. Money laundering is the processing of these criminal proceeds to cover their illegal origin. This process is of critical importance, as it enables the criminal persons to enjoy these profits without knowing their source by others [Robinson].

Illegal weapons sales, smuggling, and the activities of organized crime, including for example drugs trafficking can generate huge amounts of proceeds. Misuse, insider trading, corruption and computer fraud schemes can also produce large profits and create the incentive to legitimize the unwell-gotten gains through money laundering [Robinson]. When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by covering the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

Money laundering can, and do, appear in any country in the world, especially the countries with difficult financial systems [Kochan]. Countries with careless, ineffective, or corrupt AML Infrastructure are likely good targets for such criminal activities.

1.2 Problem Definition

Jordanian Banks and involved financial institutions who involved by the Jordanian AML law have tens of varying applications to serve its business functions; most of these financial institutions use separate, unrelated applications to cover different aspects. This causes serious obstacles in the information flow within the institution and leads to different versions of similar data, which frequently results in incomplete compliance or, at the very least, inefficient and costly processes. Also some suspicious transactions require immediate action, and this can't be materialized by using the manual or individual separate system which is mostly dependent on person's judgment.

Currently used AML either in Jordan or world wide are mainly manual solutions focused heavily on detecting transactions, produce out a steady stream of alerts for investigation, the ability to manage these alerts and investigate them effectively and efficiently was far less successful as the number of alerts needing checking often fill up investigators, If you can generate alerts but you can’t process them, you still haven’t solved the problem [Truman]. A manual system could never be completely satisfactory as a complete automatic transaction monitoring at least for the larger institutions, and then for all the country.

The huge volume and variety of transactions makes the manual analyses and investigation more difficult for the investigator and the analyst. The challenge lies in scanning through millions of data elements and identifying the links between them, then reporting to the

AMLU using pre-printed forms used for that purpose. AMLU-JO instructs by the law that all the banks should develop an integrated information system for maintaining records and documents related to money laundering, where transactions and transaction-related need to be tracked and should be easily traceable and reported to the AMLU-JO and relevant Jordanian authorities [http://www.amlu.cbj.gov.jo/].

While money laundering might occur in any Country, they have particularly significant economic and social cost for developing countries[Cornez], because these markets likely to be small and, therefore, more susceptible to disturbance from criminal or terrorist influences. Money laundering has significant economic and social impact for countries with precious financial systems because they too are susceptible to disruption from such influences. In the end, the economy, society, and security of countries used as money-laundering platforms are all imperilled. The magnitudes of these adverse Consequences are difficult to establish, however, since such adverse impacts cannot be quantified with precision, either in general for the international community, or specifically for an individual country.

On the other hand, the effective framework for AML, have important benefits, both locally and globally. These benefits include lower levels of crime and corruption, enhanced stability of financial institutions and markets, positive impacts on economic development and reputation in the world community, enhanced risk management techniques for the whole country's financial institutions, and increased market integrity [Woods].

1.3 Area Under Study

This study will provide a review of the current position and trend in AML enabling technologies in Jordan. The objectives are to do research in Jordan to identify opportunities for collaboration, between AMLU-JO, member banks and financial institutions, and to suggest ways to process, after providing a secure design for the AMLU Infrastructure in Jordan. The term "Member banks and financial institutions" is meant to include all involved foundations and related information access technologies and systems. Of special interest are AMLU-JO infrastructure and policies to promote these new technologies; new Jordanian experimental facilities established for the development and evaluation of new AML technologies, including the Society for Worldwide Inter-bank Financial Telecommunication SWIFT ;Real Time Gross Settlement System of Jordan RTGS-JO , current situation; and human interaction technologies.

While AMLU-JO, the member banks and financial institutions, are more largely interested in technologies for AML as a computer-based information construction, access, and management to improve the quality of monitoring and transfer of Alerts information to and from information systems; between both of them in the ability to conduct efficient and effective searches of AML databases; and in the quality of content in those databases. These technologies, as where as the manual system used, can address problems such as information overload, insufficient speed of information processing, multi-language information, and intellectual rights protection [Weaver]. The recent large-scale Jordanian experiments in electronic AML were to be examined as means of integrating these technologies and delivering the final proposed results.

1.4 Objectives of The Study

The overall objectives of the study are as follows:-

a. To Design a successful secure network solution, to fight Money Laundering, integrated with the current running applications, RTGS-JO system and the SWIFT network.

b. To provide the involved AML member banks and financial institutions in Jordan with an easy way to compact Money laundering integrated with the existing system around the world.

c. To provide a Technical Architecture Document TAD, for the proposed design to help assist the AMLU-JO implementing the AML Law technically and enhancing operational activities of AMLU-JO and other parties involved.

1.5 Significant of The Study

The importance of the study is timely development in implementing the Law Preventing and Combating Money Laundering, with a broad action plan developed outlining measures to be taken by all parties involved in Jordan.

The right choice to improve access to AML is technology which was the best answer to solve all obstructions and obstacles applying the Law [Cornez]. In order to monitor transactions effectively it's vital to have a single view of all activity across the AMLU-JO, by participants, by accounts and by network channels, the following are the main advantages expected from the whole proposed study.

1.6 Motivation

Most of the work described in this thesis was visualized at the CBJ Where the AMLU-JO housed, the reasons for carry out the research work at CBJ were:-

a. I served at the central bank of Jordan's Computer Department for more than 21 years leading technical teams of network engineers, database administrators and programmers, during this period he has been the Information Technology technical audit lead with nominated committees to audit and supervise some local banks, the researcher also been nominated as Technical Manager for infrastructure, technical support and security management for a period of two years where he managed and supervised day-to-day activities and consulted on vast issues related to Information Technology and computer security issues, have a good understanding of assessment practices in SWIFT,RTGS-JO, E-Government, returned cheques, and other technical projects.

b. Over the past years CBJ. have started making it compulsory for local banks and financial institutions to implement risk management procedures, and recently AML plain road obliged by the Law No. 46; this provides an early indication to me of the potential this full secure network of AML has to sustain and improve, including communication between AMLU-JO actors which leads to decrease the risk-based approach to banking regulation of the AML prevention rather than traditional rule-based compliance method can be effective [http://www.amlu.cbj.gov.jo].

c. In their fear and commitment to combat Money Laundering, financial institutions have invested in technology, but have

done so without a central governing strategy, which leads to a divisional structures; unable to communicate or share information effectually.

d. If this goal is to be reached, most organizations will need to consolidate their efforts, removing the organizational and technological obstacles that have obstruct their ability to get an enterprise-wide view of suspicious activity.

e. In addition, they need to achieve a step change in the accuracy of their detection capabilities and the efficiency of their investigatory processes.

f. However Including the researcher himself, and the above reasons, awareness that the target will not be met without the enterprise-wide analytical capabilities and efficiencies delivered by technology should be growing. Most of the financial institutions obliged by the Law ,who currently don't have a software solution that enables an enterprise-wide approach , their investigatory effectiveness and performance would be enhanced if their current solution allowed them to automatically identify links between individual alerts.

1.7 Contributions

To solve the problem described in the previous sections, this thesis introduces a complete secure automated infrastructure and a flexible environment to efficiently deal with AML compliance requirements, which allow the AMLU-JO and the law supervision , compliance officers and analysts to get a complete view of criminal acts from Money Laundering, and the risk they represent to the business between all involved financial parties in Jordan, including the SWIFT network and the National Payments System of Jordan (Real Time Gross Settlement System – Jordan / RTGS-JO housed in the Central Bank of

Jordan). This secure Framework provides support for AMLU-JO and member financial institutions. We achieve it with a creation of central AML control unit. This study can then be work in order to implement the solution.

The research builds on previous and ongoing work on hardware and software architecture and our approach differs from previous work in this area by way of thinking about all the different kinds of need that relate each component to other application, middleware, and system components. In addition, our framework is prepared to deal with completely active secure architectures that are only known at runtime.

In this thesis, we present a generic design for self-belief image and management and describe an actual implementation of this architecture. The final will be deployed successfully in centralized system. This demonstrates the effectiveness of the researcher's approach in improving the quality of the proposed automatic secure infrastructure with respect to the manual way used to trace the Money Laundering Alerts.

1.8 Limitations And Delimitations

This research was faced out with the following parameters:

1. The AMLU-JO is relatively new, and has the confidentiality orders; this impacts the amount of information available to the researcher.

2. Only AMLU-JO was included in this research.

3. As confidentially, and limitation of software resources, we can't implement physically the proposed infrastructure.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Governments recognized that criminal organizations, through the giant profits earned from drugs, could contaminate and corrupt the structures of the countries at all levels. Money laundering is a truly global phenomenon [Truman], helped by the International financial community which is a 24hrs a day business. When one financial centre closes business for the day, another one is opening or open for business.

Efforts to launder money have been growing fast in recent years in response to sharp opposite legal procedures from the world governments. The international community has witnessed the use of increasingly sophisticated methods to move illegal money through financial systems across the globe and has acknowledged the need for improved wide-ranging cooperation between all parties involved to fight these criminal activities.

This research is offered as a tool to the AMLU-JO to establish an automated secure infrastructure and improve their legal and institutional procedures, and their preventive measures according to the international standards and best practices.

2.2 History of AML Efforts

Money laundering as an expression is one of fairly recent origin. The original sighting was in newspapers reporting the Watergate scandal in the United States in 1973. [Woods].The expression first appeared in a judicial or legal context in 1982, since then, the term has been widely accepted and is in popular usage throughout the world.

Money laundering as a crime only attracted interest in the 1980s, [Weaver] essentially within a drug trafficking context. It was from an increasing awareness of the huge profits generated from this criminal activity and a concern at the massive drug abuse problem in western society which created the impetus for governments to act against the drug dealers by creating legislation that would deprive them of their illicit gains.

AML efforts are not new. In fact, for many years, the international, especially US banks, have already been continuously implementing AML solutions, in order to comply with the Bank Secrecy Act. However, with the events of 9/11, the AML efforts have come into the limelight once again and the US government is started to get stricter in this area [Robinson]. Of late, governments in other countries have started making it compulsory for their banks and financial institutions to implement AML procedures. For the banks, it is not easy. Most times, AML efforts are purely compliance and regulatory requirements and produce little or no tangible returns. Banks hence try to see how to minimize the cost of AML efforts [Broome].

As always, most banks say that they are able to comply with the requirements - a tweak here and there on the systems and amendment to AML policies and procedures will do the job, and typically take a tactical approach to the problem. However, criminals have grown more sophisticated over the years and therefore further demands and requirements are continuously being put on the institutions to comply with the law. History hence teaches us that investing in a strategic solution is important [Truman].

2.3 Money Laundering Risks

ML poses serious threats not only to financial institutions but also to the nation. The risks faced by financial institutions are:

1. Reputation risk: The integrity of the banking and financial services marketplace depends heavily on the perception that it functions within a framework of high legal, professional and ethical standards.
2. Operational risk: It can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. A public perception that a bank is not able to manage its operational risk effectively can disrupt or adversely affect the business of the bank.
3. Concentration risk: This risk relates to the exposure of banking and financial services market place to a single customer or groups of related customers.
4. Legal risk: Banks may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practice due diligence.

Country is also at risk because money laundering provides the energy for drug dealers [Lilley], terrorists, arms dealers and other criminals to operate and expand their criminal enterprises. Hence, the government regulatory bodies partnering with the financial institutions and law enforcement agencies have initiated elaborate AML programs to track and prevent financial crimes.

Money laundering is a threat to the good functioning of a financial system. In law enforcement investigations into organized criminal activity, it is often the connections made through financial transaction records that allow hidden assets to be located and establish the identity of the criminals and the criminal organization responsible [Lilley]. When criminal funds are derived from robbery, extortion, misuse or fraud, a money laundering investigation is frequently the only way to locate the stolen funds and restore them to the victims.

Most highly, however, targeting the money laundering aspect of criminal activity and cheap the criminal of his ill-gotten gains means hitting him where he is vulnerable. Without a usable profit, the criminal activity will not continue.

2.4 Technical Research, Development And Implementation

Many researchers and individual institutions did some researches in the area of AML. In this thesis we will discuss some of these researches. In [Hanna], the researchers suggested and build a software solution, to detect and prevent AML, then generating an alert report, which has to be analyzed manually, the way to report to AML investigation central unit wasn't identified as it was focused on regulations. This strategy lacks the integration with other applications, and the information exchange between parties especially the AML central unit, actually they customized monitoring software, without completing the whole cycle of detecting and preventing on real time.

Most of the researchers as in. [Hanna], and solution providers as in. [SWIFT], and lawmaker as in. [FATF], have been directed at the creation of a system of laws, regulations, and institutions-the prevention and detection structure of the AML for financial institution's individual use, then reporting manually, by different ways to the specified control unit, as shown in figure 2.1. How well the system works in a global or even local secure network as an integrated system wasn't identified, integrated with other solutions, for reporting alerts to a centralized control unit, from different financial institutions.

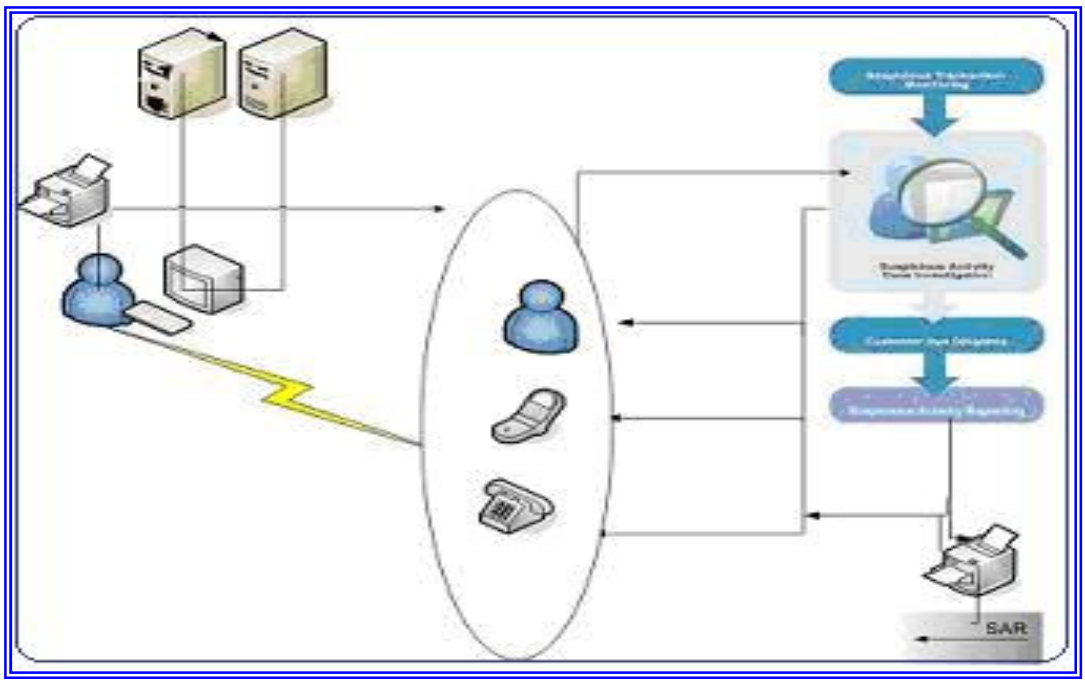


Figure 2.1: Current model reporting SARs to AMLU-JO.

A work that is related to our thesis is in, [SWIFT], the SWIFT committee, established a powerful secure network for member banks world wide, for fund transfers, this project is dedicated for money transfer between banks, we will benefit in our thesis from their ideas building our design.

We will try to benefit in this thesis from [Tanenbaum]; [White]; [Comer] and [Matthews]; where some of the most important hardware security issues design guidelines proposed. The author introduced two obvious design guidelines. The first design guideline focuses I-Banking Infrastructure Security Advice and Security Policy where he highlights that Security Advice and policy are the two results of the risk assessment and risk management on how to secure and patch the

network, application, database and other services that have vulnerability either in its management, process and I-Banking Infrastructure.

The second guideline focuses on methods for securing and hardening I-banking infrastructure, the author pointed out that It is possible to design the security tools; for instance, server protector, data security application, network and intrusion detection application (cryptography, firewall and intrusion detection system) in the process of securing and hardening the infrastructure.

Unfortunately, there is no information available on the structure of the network, how it is built, and types of protocols used in the countries that implemented such a project, as it is kept unknown to others considered as the right of the institution who implemented the solution, however we will try to benefit from the experience of some of the global Central Banks, such as, [Crimes Section], and, [Drayton], who has implemented an end-to-end solution, in which will assist in their fight against money-laundering, this thesis will try to focus the light on their experience if possible.

2.5 Current AML Systems

The Jordanian and global laws applies to all Jordanians and foreign institutions, local and foreigners carrying out financial, economic, or monetary activities in Jordan. It requires all financial institutions, including banks, entities providing credit; brokers; payment services; securities traders; insurance companies; etc… and foreign financial institutions to take action to prevent and combat money laundering. In particular they have to (1) develop AML procedures, (2) establish internal control and audit procedures, (3) appoint specialized staff to carry out AML activities, (4) keep records for a period of at least 5 years, (5) identify and report both high-value and suspicious

transactions to the AMLU-JO, and (6) obtain suitable measures to prevent money laundering activity.

The AMLU-JO was established by Law No. 46 of the Year 2007, as an independent authority with lawful personality "Financial Intelligence Unit" housed in the Central Bank of Jordan. The Unit is headed by the National Committee for Combating Money laundering. The unit specialized in getting doubtful Activity Reports requests and analyzes related information, then provided that information for further action to be taken to experienced local supervisory. The structure of the unit is shown in figure 2.2.

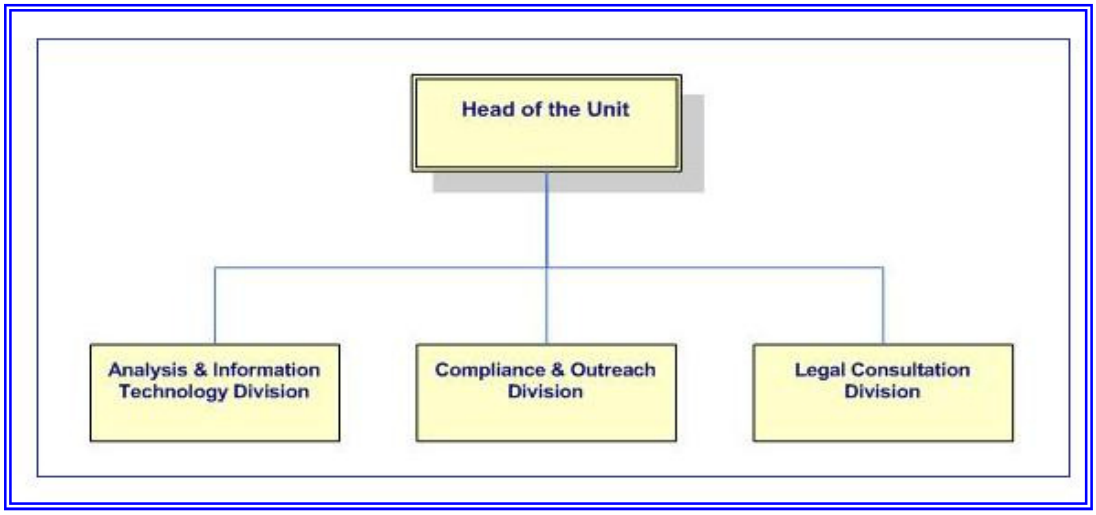


Figure 2.2: Structure of the current AMLU-JO.

2.6 Tasks of The AMLU-JO

1. Receive Suspicious Activity Reports SARs.
2. Request and analyze related information.
3. Provide competent local official parties with such information when needed for further action.
4. Broadcast periodic statistics regarding suspicious transactions.

5. Prepare a report and submit it to the General prosecution.

Today all economically developed countries, including Jordan widely use new information technologies in industrial, commercial and banking environments. It is explained by the fact that traditional methods do not make it possible to gain a correct understanding of a modern information flow or make a deep analysis of dynamic processes of the allowed economic activities. Firms want the technology to work smarter to increase the productivity of their people, improved efficiency and business Controls and to decrease the cost of running.

Money laundering involves transforming money from crime (dirty money), [Weaver] into money that:-

1. Has the appearance of coming from a legal source, and
2. Makes the criminal origin of the money difficult to go after (clean money).

From the above it is noted that effective money laundering enable criminals to remove themselves from their criminal activities, making it is harder to take legal action to them, and remove their proceeds. Laundering money also enables criminals to take advantage of the benefits of their crimes including investing their profits for future criminal activity [Weaver]. Criminals use the financial system to make payments and transfers of funds from one account to another, to hide the source and useful ownership of money. The main objective is to legitimize income from the original criminal sources. In short, they aim to turn dirty money into clean funds.

2.7 Steps of SAR's at AMLU-JO

The main method for detecting suspicious transactions remains staff awareness. The next most common methods are examining reports

created by exceptional value flags and reviews of sample transactions by the compliance departments developed IT systems as a key means of identifying suspicious transactions, with a similar number utilizing external IT systems, following are the steps of handling SAR's at AMLU-JO:- [http://www.amlu.cbj.gov.jo]

1. The unit receives Suspicious Activity Reports SARs, from all parties obliged by the provisions of the Law to report any suspicious transactions.
2. After receiving SARs the specialized division will then carry out the appropriate analysis & inquiries which will enable the evidence or suspicions of money laundering to be confirmed or rejected.
3. The division can supplement the information received by asking for additional information from internal, external or international sources; any request for additional information is made by the division according to the procedures set by the committee.
4. The division will submit a final report containing the result of the inquiries, assessing all the information and proposing any actions to be taken to the head of the unit who will take the decision whether to fill a report to the Prosecution General or save the collected information about the case in the unit’s data base.
5. Once sufficient and supporting information regarding suspicious transactions is available, the unit will prepare a report and submit it to the Prosecution General.

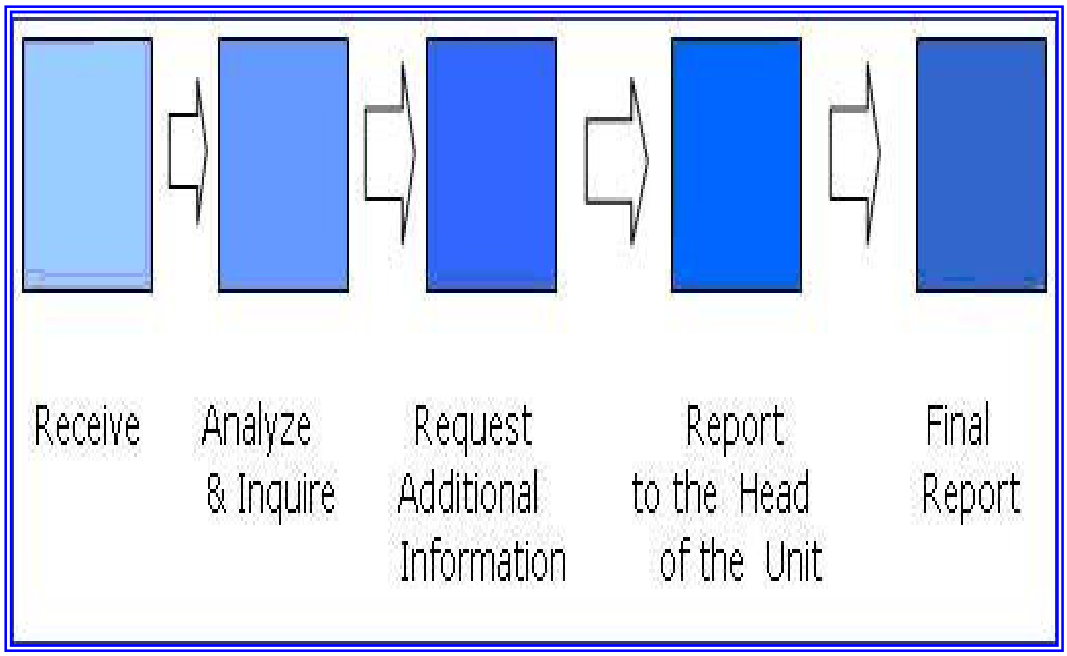


Figure 2.3: Steps of SARs at AMLU-JO

The main method for detecting suspicious transactions remains staff awareness. The next most common methods are examining reports created by exceptional value flags and reviews of sample transactions by the compliance departments developed IT systems as a key means of identifying suspicious transactions, with a similar number utilizing external IT systems.

Many organizations are finding it difficult to justify the perceived high Cost of implementing a technical solution, and there are cost effective Technologies available that will help them meet their compliance obligations. Cost pressures and difficulties with training mean that such a relatively low usage of IT to assist with AML is

unlikely to be sustainable in the long term. One key driver for automation through technology is the tight time frame for reporting suspicious transactions.

Many banks are struggling to design and implement an effective AML strategy. One challenge remains the sheer cost and scale of such operations [Broome]. Typical AML rollouts, even in a smaller institution, can easily run into the tens of millions over multiple years, and there's often no clear end date in sight for the projects themselves, despite having deliverables dates fixed in stone by external factors such as legislated compliance dates. We are unable to estimate the full cost of the compliance strategies, emphasizing the confusion surrounding these systems.

2.8 Stages of Money Laundering

There are a large number of techniques used by money launderers to achieve their goals. These are increasingly difficult or clever ways to launder funds – money launderers target the least obvious, least regulated and most vulnerable elements of the global financial system to carry out their activities [Woods]. The stages of ML are as follows:-

1. Placement

Placement is actually considered the first stage in the laundering cycle. Money laundering is a "cash-demanding" business, generating huge amounts of cash from criminal behaviour (such as drugs where payments takes the form of cash in small amounts). The money is placed into the financial system (banks accounts or retail economy or smuggle out of the country). The aim is to remove the cash from the location of purchase so as to avoid finding by the government authorities and to transform it into other asset forms; for example: traveler's cheques, cash money. In review these stage are summarized in the following steps:

- Placing cash money in the financial system.
  - ☒ Direct: cash deposits or close bags.
  - ☒ Indirect: use of front man or organization.

2. Layering

In the second stage laundering or what is called layering, there is the first attempt to cover up or hide the source of the ownership of the money by creating difficult layers of financial transactions designed to cover the audit trail and provide secrecy. The purpose of layering is to disassociate the illegal money from the source of the crime by intentionally creating a complex network of financial transactions aimed at conceal any audit trail as well as the source and ownership of dirty money.

Typically, layers are created by moving money in and out of the bank accounts of carrier share companies through electronic funds' transfer... Other forms used by launderers are complex dealings with stock, commodity and futures brokers, the chances of transactions being traced is not then so important. (Split the criminal funds into various deposit accounts to hide their origin).

- Core activity of money laundering process.
  - Objective is to break the paper trail or audit trail.
  - Use of many transactions, bank accounts.

3. Integration

The last stage in the laundering process is Integration at which the money is included or integrated into the legal economic and financial system and is take in with all other assets in the system. Integration of the "cleaned / or not dirty" money into the economical system of the country is accomplished by the launderer making it appear to have been legally earned. By this stage, it is extremely difficult to distinguish legal or illegal assets.

- Methods popular to money launderers at this stage are:
  - ☒ The establishment of unidentified companies' in countries where the right to secrecy is guaranteed. They are then able to grant themselves loans out of the laundered money in the course of a future legal transaction. Furthermore, to increase their profits, they will also claim tax relief on the loan repayments and charge themselves interest on the loan.
  - ☒ The sending of false export-import invoices overvaluing goods allows the launderer to move money from one company and country to another with the invoices serving to verify the origin of the monies placed with financial institutions.
  - ☒ A simpler method is to transfer the money (through electronic fund transfer) to a legal authorized bank from a bank own by the launderers. (Moving back the covered funds and bringing them back together in one account or multiple accounts so that they appear legal).
    - Money cannot be related to illegal origin.
    - Money invested in legal businesses.

The scope for AMLU-JO and any AML Units and software providers is to be the blameless means of transport for money laundering, should be apparent from this description. They could become involved in any of the three stages. When a client deposits cash money, either in a series of small transactions or in large amounts, there is always a possibility that the money may be placing the income of criminal activity. Figure 2.4: illustrates these stages.

Figure 2.4: Stages of Money laundering world wide.

2.9 AML Regulators And Institutions

Different International AML organizations involved in the process of AML include:

- Financial Action Task Force FATF.
- Office of Foreign Assets Control OFAC.
- Basel Committee.
- International Monetary Fund IMF.

2.9.1 Financial Action Task Force

FATF stands for the Financial Action Task Force on Money Laundering which was established by the Group of Seven Nations summit in Paris in July 1989 to examine methods to combat money laundering. The main global policy making body for AML controls frameworks and controls is the Financial Action Task Force [FATF]; It is the inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. It works to generate the necessary

political will to bring about legislative and regulatory reforms in these areas.

The FATF has published 40 Recommendations + 9 Special Recommendations on Terrorist Financing in order to meet this objective. The 40 recommendations were reviewed and updated in 2003 to make them more relevant and reflect the increasing sophistication of the launderers and therefore increased requirements of the financial system to combat them. The 40+9 recommendations are now much more stringent than most legislative requirements in the developed world and almost without exception those in developing economies [Broome]. In response, most governments in the developed world (who are members of the FATF) are enhancing or overhauling their existing legislative and regulatory requirements to conform to the requirements of the FATF 40 recommendations.

2.9.2 Office of Foreign Assets Control

The Office of Foreign Assets Control OFAC of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under US jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments. [OFAC]

Careful and diligent compliance with OFAC regulations was underscored by the events of September 11th. Now more than ever,

American and International business organizations and institutions are evaluating methods to comply with OFAC compliance regulations.

2.9.3 Basel Committee in Banking Supervision

The governors of central banks in different countries tuned the Basel committee that enhanced many disciplines in fighting money laundering; Basel committee issued the Basel principals to hinder money laundering [Basel].

2.9.4 International Monetary Fund

The IMF issued an announcement asking all its members to fully comply with the United Nations instructions to counter terrorism [FBI].

CHAPTER THREE

THE AML FRAMEWORK

3.1 Introduction

Within the next sections, I will present a detailed picture of developing and important features in the area of AML secure design framework. The range of this section is extensive and attempts to address software as well as hardware issues involved in the development of such a framework.

Therefore it will address issues such as the design method proposed, rapid technology development approaches, member banks and financial institutions issues involved in AML, and the final design proposed. This chapter also attempts to address the features of the proposed design in details through some illustrating Figures and description of each step in the proposed design.

As brought onward in the previous chapters, the underlying basis it is a mandatory for the local Jordanian banks and financial institutions to implement a strong internal AML system, and as the Jordanian AML Law No. 46 For the year 2007, obliged banks and involved parties to develop AML procedures, identify and report both high-value and suspicious transactions to the AMLU-JO, and obtain suitable measures to prevent money laundering activity [http://www.amlu.cbj.gov.jo]. There are heavy penalties by the Law for non-compliance such as heavy fines, asset penalty. Rather they address the entire area from AMLU perspective, the reader is cautioned that although AML software solutions have been in use in Jordan, this area remains undeveloped as expected from a high risk automated solutions.

3.2 AML Solutions –Overview

Superior regulatory focus on governance, and the resulting increase in the accountability of senior management for AML, appears to have driven up the amount of independent monitoring and testing of AML systems and controls. More banks report that they have a monitoring and testing program in place, and banks report that a wider range of functions within their organization are involved in this. The key to successful testing and monitoring, however, relies on a strong drive from senior management as well as effective and timely follow-up and feedback of improvements into current systems and controls.

Though the AML systems of today are becoming much clever with applications of newer technology and techniques, hence, an effective AML full solution should have a synergy between the technology-driven integrated systems and human investigative skills that can both work together to combat Money Laundering and suspicious financial activities, Show that money laundering is becoming more and more of a cross-border phenomenon and new crime strategies are coming up almost daily. [Weaver].

The primary objective of AML software is to prevent or minimize the extent of money laundering that takes place among the transactions done by an organization.

From the researchers point of view, the AMLU-JO supposed to be the national operator of the whole suggested system, it is important to find a single solution that would be scalable and flexible enough to work in a number of geography and regulatory environments, the system also should be tailored to the requirements of those environments, different operating systems, and different platforms and yet support a centralized secure structure.

Almost all AML local regulators in the world agree that information technology plays a vital role in ensuring an effective AML strategy for financial institutions. Responding to complex and continually changing organizational risk exposures depends on information technology operations and requires a high level of information technology effectiveness.

3.2.1 Role of Technology on AML

Emerging technologies can assist banks aggregate and assess risk, and create the connectivity to reuse information across the organization.

However, while there are dozens of vendors offering technologies in this field, implementation rates are not as high as we expect. In fact, it's still possible to ask the local regulator, AMLU-JO, for permission to submit AML compliance reports in Writing, if your business does not have access to a computer, while few organizations would survive for long in a totally information technology-free state.

Within today's automatically successful managed world, it has become mandatory for the banks and financial institutions to implement a strong internal AML System, this is obliged by the law AML, in which There are serious penalties for non-compliance such as heavy fines, asset penalty and even suspension of the license of the financial institution [Hetzer]. Trends show that money laundering is becoming more and more of a cross-border phenomenon and new crime strategies are coming up almost daily. A functional AML system should have:

1. Interfaces that integrate with the international network of financial and regulatory institutions and enhances the capability for information processing.
2. An enterprise-wide architecture that integrates internal core financial applications and facilitates information flow; and

Traceability across the applications within the financial institution.

3. Transaction monitoring system having the intelligence to detect and alert suspicious activities.
4. Case management workflow to efficiently investigate and action the alerts.
5. Customer risk assessment model to restrict entry of unwanted entities into the financial system.
6. Efficient reporting system for both regulatory and internal control reporting. Figure 3.1 illustrates these components

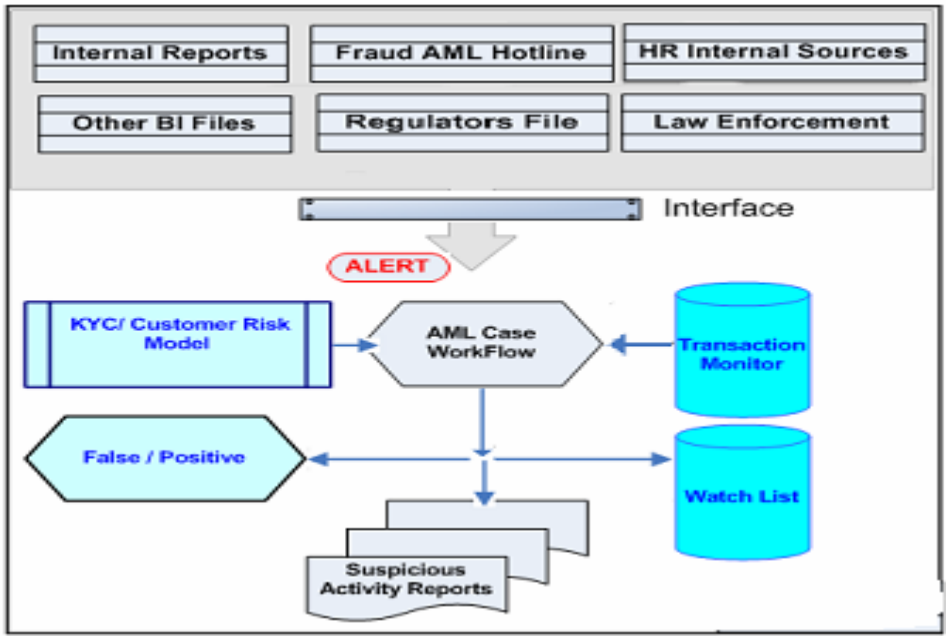


Figure 3.1: Components of AML System.

3.2.2 A classic AML Solutions

While countermeasures to all three phases of money laundering are important, laundered money is most vulnerable to detection at the placement stage, for this reason, international regulatory and law enforcement efforts have concentrated especially on developing methods to make it difficult to place illegal funds without detection by developing measures.

3.2.3 Traditional Configuration of AML

The first step in the AML initiative was setting up the legal structure which would become a major tool for fighting the money laundering activities [Truman]. The different laws and acts, such as the Bank Secrecy Act and the Patriot Act, evolved focusing on this area. These laws spell out the mandatory requirements to be followed by the financial institutions. The major requirements are:

1. Retention and traceability of financial transactions.

2. Reporting of certain suspicious financial transactions.

In addition to these laws [Basel]; [OFAC], there are several guidelines and recommendations developed by international bodies that help the financial institutions to set up appropriate checks and balances so that it satisfies the regulations and help them fight financial crimes. The focus areas are:

1. Customer identification and customer due diligence: Measures to establish the identity of the clients and beneficial owners; collect and record the proofs establishing the identity, commonly referred to as know your customer (KYC).

2. Continuous monitoring of the customer transactions and identifying suspicious activities.

3. Reporting on suspicious activities SAR and policy violations.

4. Establishment of a compliance office and internal audit function.

5. Continuous employee education and training.

It should be noted that each of the individual phases (placement, layering and integration) will be composed of a variety of individual activities that may vary across institutions and countries. Additionally, the numbers of channels through which the monetary transactions are enabled are multifarious. This duo combination greatly complicates the approach to detect money laundering. Traditional approaches to the detection of money laundering activities followed a labour intensive, manual approach.

3.2.4 Traditional AML Detective Approaches

Conventional investigative approaches could be classified into:-

a. Identification of money laundering incidences,

b. Detection avoidance and;

c. Examination of money laundering activities.

These approaches relied to a great extent on field activities such as surveillance/discreet enquiries, interviews, search warrants, subject interviews and the like. Data sources for following up on important leads are likely to be fragmented. Such an investigative approach consumes substantial time and resources. Law enforcement officials may work on a particular case for many years before they can piece together sufficient evidence to persecute a criminal. Given that the volume of financial data and transactions has increased in a variety of

ways, such techniques need to be supported by automated efforts for money laundering pattern detection.

The complexity of banking and financial services operations have also made it difficult to keep track of the various patterns of money laundering. Launderers are willing to shift their patterns of activities from physical cash to conversion to monetary instruments, reliance on wire transfers and use of non-bank money transmitters. Wire transfer transactions may be made using a variety of mechanisms, such as shell companies and front corporations, false invoicing, etc. The similarity between legitimate and illicit businesses in terms of cash turnover has also been used by launderers to obscure the trail of funds. This calls for automated methods to monitor financial transactions and to detect instances of money laundering.

A great deal can be done to fight money laundering, and, indeed, many governments have already established broad AML regimes. These regimes aim to increase awareness of the phenomenon – both within the government and the private business sector – and then to provide the necessary legal or regulatory tools to the authorities charged with combating the problem.

Some of these tools include making the act of money laundering a crime; giving investigative agencies the authority to trace, seize and ultimately confiscate criminally derived assets; and building the necessary framework for permitting the agencies involved to exchange information among themselves and with corresponding persons in other countries. It is critically important that governments include all relevant voices in developing national AML programs.

They should, for example, bring law enforcement and financial regulatory authorities together with the private sector to enable financial institutions to play a role in dealing with the problem. This

means, among other things, involving the relevant authorities in establishing financial transaction reporting systems, customer identification, record keeping standards and a means for verifying compliance.

Unfortunately there is no wide-ranging automated system and a flexible environment with a secure network to efficiently address AML compliance requirements, which allow the AMLU-JO, compliance officers and analysts to get a complete view of their customers and the risk they represent to the business between all involved financial parties in Jordan, including the SWIFT network and the National Payments System of Jordan

3.3 Efficient AML Wide-Ranging Solution Features

The researcher's point of view, of the features that makes AML an effective solution are listed as follows:-

a. Enterprise-wide secure broad network architecture for the AMLU-JO that integrates internal core financial applications and facilitates information flow and traceability across the applications within the financial institution such as SWIFT and RTGS networks; to be able to combat money laundering. Figure 4, illustrates the proposed model.

b. Solid security infrastructure for the AMLU-JO Disaster Recovery site Connectivity, in different physical location, Figure 3.2. Illustrates the structure.

c. A user friendly, flexible, secure, parameterized, bilingual (Arabic, English), designed and built using the latest technology and standards, able to meet the Alum's current business requirements and future plans with great security and accuracy, and supports the best business practices and processes with great precision. The

infrastructure must cover all the aspects to achieve a full configuration including hardware, software. The thesis suggests this at both the AMLU-JO and the participant's side. This system should have at least the following aspects:-

1. Transaction monitoring system having the AMLU-JO to detect and alert suspicious activities; including SWIFT and the RTGS-JO networks to allow them to take the right actions.

2. Case management workflow to efficiently investigate and action the alerts.

3. Customer risk assessment model to restrict entry of unwanted entities into the financial system; and

4. Efficient reporting system for both regulatory and internal control reporting.

5. Interfaces that integrate with the international network of financial and regulatory bodies and enhances the capability for information processing, between the AMLU, and governance regime. Figure: 3.1, Shows the proposed logical diagram for these interfaces.

The new model design will allow all parties involved in the suggested secure network ("AMLU and members to):-

a. Connect to the available network securely.

b. Establish a secure connection for both the governance regime, and the financial institutions, sharing all parties (RTGS-Jo, SWIFT Network).

3.4 Used Methodology

Essentially the study has been divided into phases that are described below:-

a. AML Technical Education and Awareness.

b. Model design and development.

c. Secure network and software Operational activities.

3.4.1 AML Technical Education And Awareness

a. Government Awareness. Understanding about AML and terrorist financing issues within government agencies in Jordan at low level. General Technical awareness training covering the nature of the issues, global developments, identifying methodologies, and outlining the Law and its main elements, will be provided to key agencies.

b. Financial Institutions cooperation and Awareness. Awareness will be conducted to explain why money laundering is a problem and to describe the responses that are being put in place. They will deal in particular with the technology related to money laundering purposes, and will include security issues, network design and both the RTGS-JO and SWIFT international network.

3.4.2 Model Design And Development

a. The thesis will assist in developing reporting forms and processes, and administrative rules relating to the operation of AMLU; determining the extent to which reporting will be done electronically; starting internal training for AMLU on its basic role and operation-and developing instructions and directives to

be provided to financial institutions. A vision of a suitable IT system for AMLU will be designed, to make the choice easier for the AMLU when deciding to customize or outsource the software which will be connected to the suggested secure network, and by minimizing the cost of AML efforts.

b. In addition, by designing a technical architecture document for the whole study, it will help in developing knowledge and encourage training for the staff of AMLU on money laundering technical issues, so that they can develop a range of complementary policy responses depending on this. Financial institutions will be assisted in developing internal procedures and regulations on AML. The possibility of developing a good trustable relationship between AMLU and other well-established regional AMLU will also be explored.

3.4.3 Secure Network And Software Operational Activities

a. The needs here fall into two obvious areas. The first concerns the need to train investigators who will have involvement in AML cases on dealing with the software implemented and integrated with the network. Second, there is the issue of compliance education for the AMLU and regulatory agencies, Training will be conducted, where appropriate, by technical consultants engaged under the Law, but additional resource persons may also be brought in, as necessary, to conduct targeted workshops on special areas. The training programs will be designed and implemented in close consultation, wherever possible, with existing training institutions, technical training documents and topics will be suggested in the thesis.

b. Investigative Training, general suggestions to the AMLU investigators, to conclude training programs to the financial

institutions involved with a specific money laundering focus built on components that could be tailored to suit each participant with a vision to the future needs to keep the network and systems updated, up and running.

c. Implementation Arrangements; the thesis recommends that AMLU will be the administrative Agency for the whole project. It will establish an interagency national coordination committee comprising representatives from each of the implementing financial institutions and that will enable them to cooperate and, where appropriate, coordinate domestically with each other concerning the development and implementation of the secure network and activities to combat money laundering. The thesis point of view is that the project will be implemented over one year. We suggest that the project will require consulting services (international) and (domestic), who will assist in organizing workshops and training at required centers as well as helping build the recommended secure infrastructure, they will also be engaged in an international consulting issues for international cooperation, reviews will be conducted by AMLU, the Government, and the consultants to consider the reports.

d. Some important Hardware and software Security recommendations and some standards of security policy will be documented in this study.

3.5 The Proposed AML Infrastructure in A Glance

We believe that a typical AML broad System environment must consists besides the secure network, of an application software, as described in Table: 3.1 ,and integrates with a combination of individual components that interact with each other to provide alerting services, Table: 3.2 gives a detailed description of each component.

Application	Description of Application
AMLUsoft Jordan	Outsourced / customized AML Software product which processes and that exchange AML ALERT Messages, between internal institutions branches by using the AMLU database application through the AMLU network. AMLU database Access and AMLU Entry are licensed to products that are provided by AMLU. This AMLU software also offers the functionality to send ALERT messages for member banks through the Amulet interface.

Table: 3.1 Description of AMLUsoft the Component of AML System.

Table 3.2 gives a detailed description of individual components that interact with each other to provide alerting services for the AML system of Jordan as illustrated above:-

Component	Description of Component
AMLUnet	AMLUnet Link, Which is software component that is required in order to connect to AMLU network.
AMLUmid	Middleware component that is used in order to link back-end applications and workstations to AMLUnet, which acts as the Alert messaging concentrator.
MQ	Message Queue. IBM middleware component that is used in order to link back-end applications through the AMLUnet.
AMLUsec	Hardware Security Module. A hardware device that is tamper-resistant and that ensures the secure storage and the processing of Alerts secrets. Like tokens or cards.
HTTPS	Secure Hypertext Transport Protocol. A protocol that is used in order to access web servers that are hosted on AMLUnet. The HTTPS proxy, which is a part of AMLUnet, used for routing purposes.
Vendor product	Allows connecting to additional services hosted on AMLUnet. These products connect to AMLUnet.
AMLUfire	Network component for the connection AMLUnet, which implements network security that is based on IPsec.
AMLUcert	A certificate issued by AMLU. Which acts as the certification authority on AMLUnet?

Table: 3.2 AMLU Infrastructure components description.

3.5.1 AMLU net Alerts Message Flow

Alert messages are built in the AMLU/Jordan. Alert messages can be entered directly by using a screen-based message entry product, or they can be entered through a link to a back-office application (AML Application).

a. The AMLUnet creates the AMLU protocol for the Alerting message. Then it calls the local AMLUnet Link software in order to request transportation through AMLUnet.

b. The AMLUnet Link encapsulates the Alerting message load with an AMLUnet Alert message cover, and sends it

through an established TCP/IP connection to the AMLUfire.

c. The AMLUfire has established IPsec tunnels with the AMLUnet central systems through the AMLUnet network. These tunnels are established over physical lines between member banks and financial institutions premises and the AMLUnet.

d. The AMLU central systems are connected to the AMLUnet application servers at AMLU, which send back an AMLU Alert response to the initial member's response.

e. Then an Alert response message is received, you are assured that the AML application will deliver the original Alert message to the intended receiver. On the other hand, a NOT okay message indicates that an error occurred and that the Alert message cannot be delivered to the intended receiver.

Both AML Models solution makes use of the established SWIFT network, and RTGS system within the institutions to transfer the required data from the commercial banks. This takes advantage of the commercial banks' existing investment in SWIFT and leverages the functionality of the SWIFT messaging network, without an increase in cost. This thesis believes that the AML solution is a unique project that enables AML agencies to utilize existing electronic funds transfer infrastructures, and RTGS to detect potential money-laundering transactions. Automated AML systems may be an important component of an effective overall AML control environment. The following factors are commonly considered as being important to a successful AML system development and implementation:

a. A clear understanding of what the system will deliver and what constraints will be imposed by the limitations of the available data.

b. Consideration of whether the supplier has the skills, resources and ability to deliver the promised service and provide adequate ongoing support.

c. Maintenance of good working relations with the vendor, for example when work together to agree detailed system configuration. Use of recommended hardware, not necessarily a financial institution's own standard, to reduce Processing problems or otherwise finding a solution that is a good fit with a institution existing infrastructure.

d. A full understanding of the data being entered into the system and of the business's needs.

e. Regular cleaning and database maintenance.

f. Careful consideration of the risks of charge a personalized seller of the system, which may be incompatible with future standard product upgrades.

g. Continued allocation of sufficient resources to make sure manual internal suspicion reporting is efficient, as AML can increase, but not replace, human awareness in day-to-day business.

3.5.2 The AML Software Application

The Areas that AML Packages Cover the following:-

- Funds Transfer: examples of these are transactions using SWIFT and, and RTGS.
- Current Account Activities: examples include deposits, withdrawals, check clearing and monetary instruments

- Currency & Cash Transactions
- Electronic & Online Activities: examples include electronic payments online & clearing house (ACH) transactions.

3.6 Impact Changes on Jordanian Financial Institutions

As we noticed through out this research and If not sure of the levels of risk within the member banks and financial institutions, the study already cleared out and the point of doing a risk based assessment to target the most risky elements of the business regarding Money Laundering. Similarly the study suggested performing impact assessment analysis, or a gap analysis between the current framework and the requirements under the new legislation under the designed infrastructure.

The study can help implement some of these specific improvement projects as it cleared out the scope up the specifications required for IT solutions. It also suggests performing training or design training programs for the member's banks.

The researcher also recommends performing some sort of supervision visits done by the AMLU of Jordan to assess readiness for the new supervision regime. In the short term, Jordanian financial institutions and member banks must be considering their resource requirements to plan for and address the change required to their AML structure if they already have one.

This will require an impact assessment be performed between their current structure and that required under the new or proposed legislation – it is not a valid excuse to put this off until the legislation is finalized – as there is an already there the FATF 40+9 recommendations.

This impact assessment will allow firms to focus their resource assessment in terms of the people, process and technology needs for implementation and an estimate of the timelines involved.

Values that study add to the financial sector and AMLU of Jordan is as follows:-

- Reputation risk improvement.
- Lower risk of financial penalties.
- Multi corrective local team with access to global leading practice.
- Demonstrates to the regulator appropriate tone from the top.
- Allows institutions and AMLU of Jordan to focus on high risk areas.
- Allow linkage, dependency and conflict to be objectively identified across the AMLU and institutions.
- Tailored relevant solutions.
- Independent assurance on upgraded environment and feedback on level of readiness prior to a supervisory visit.

Given the constant regulatory pressures, changes in environment and need to provide long term support and functional expertise to the banking and financial services clients, the Financial Solutions setup an AML Center of Excellence, within its Banking & Financial Services Practice. AMLU Design has been developed to match to the AML requirements as defined by the key AML regulations across the world like FATF.

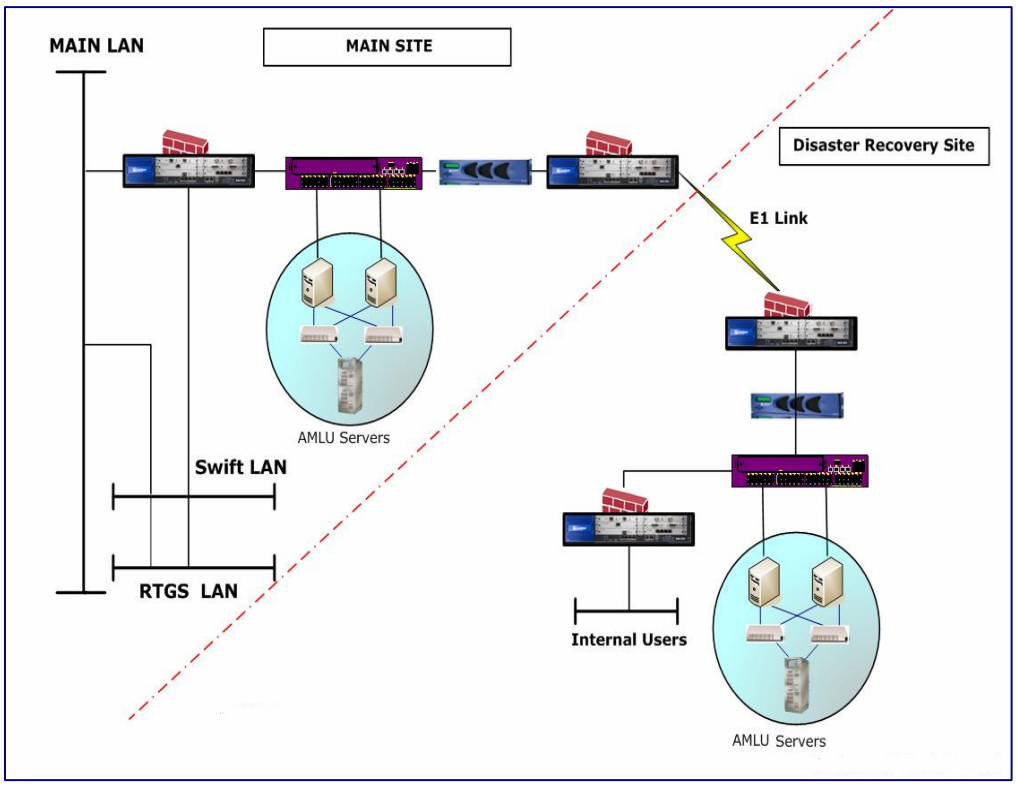


Figure 3.2: Proposed Logical Diagram for AMLU & DRC. Site

The proposed design Compliance is a broad AML and Compliance solution that enables AMLU of Jordan and Financial Institutions to achieve regulatory compliance, mitigate risk, safeguard reputation and retain customer loyalty. Its modular and scalable architecture enables financial institutions of all types and sizes to comply with local and global AML regulations. As shown in Figure: 3.2 above.

3.7 New Proposed Design in Detail

This study is in two parts. The first part is a fairly detailed look at the work done in developing a common standard for perimeter defence for an enterprise that comprises many relatively autonomous organizations. However, while perimeter defence is very important, it is

not enough. The second part of the case study examines a specific security implementation that is designed to protect sensitive data at all times,

It is coated; as backup connection should be implemented for the entire network to prevent any point of failure for the whole network Figure: 3.3 illustrate Backup connection for the network which uses the same hardware blocks, switches and routers.

The perimeter defence solution has been drafted as the AMLU standard but not yet implemented. However, the proposal some of the results of these study are included. The second

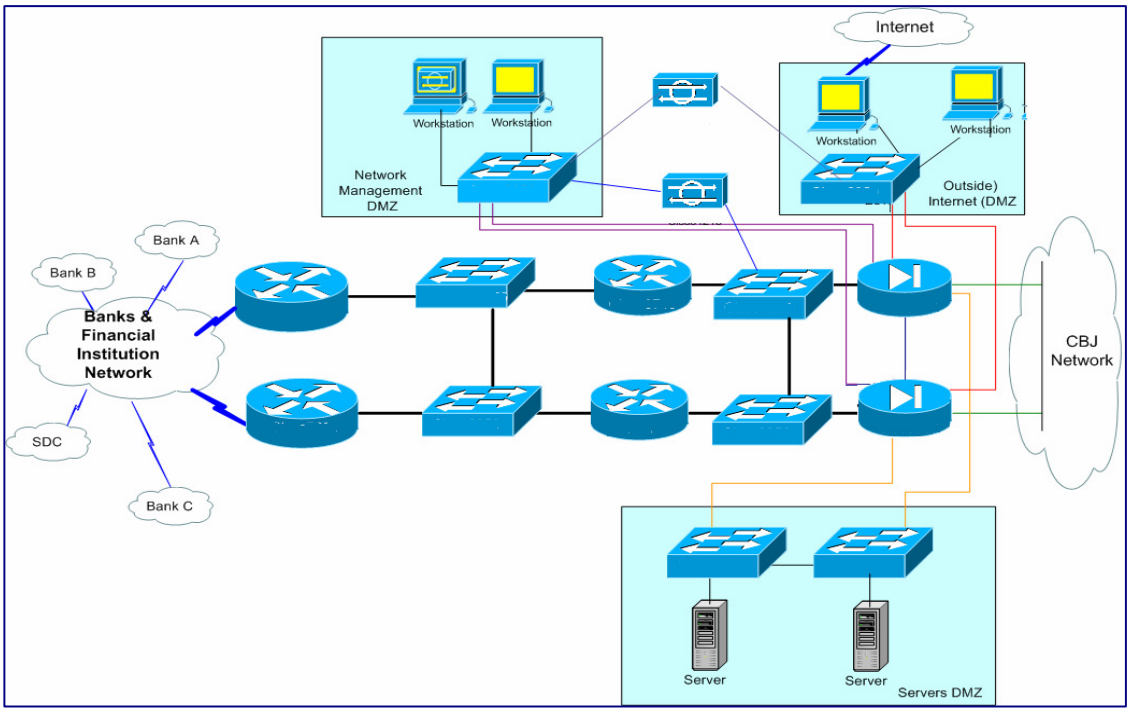


Figure 3.3: Proposed Backup Connection for AMLU & world.

Part of the study reports on a solution that has already been implemented in the AMLU.

The security framework for the Disaster Recovery Connectivity is based on the security region framework. This framework takes into account the points discussed below.

Security has been the task of specialized appliances: firewalls, intrusion detection or prevention systems, antivirus software and so on. Since most attacks initially came in from the Internet, bolting discrete devices to the Wide Area Network border, where the private and public networks met, worked well.

Additionally, threats are appearing on the inside of the network, circumventing the elaborate firewall and antivirus protection at the WAN perimeter. In fact, the typical IT administrator finds out that there is a new threat on the Internet because it's already appeared inside the enterprise network.

In addition to being ineffective against the spread of viruses and worms within an enterprise, conventional protect-the-border strategies also leave the corporate LAN wide open to inappropriate access by intruders. Intruders—whether digital or human—can pretty much go anywhere on the network, causing any number of problems. Instead the LAN itself must play an active role in defending the network and the resources on the network from inappropriate access or attack.

To address all of these business needs the solution would be a purpose-built machine that combines a full range of security services with an equally comprehensive set of proven networking capability. Eventually, however, the success of such a solution will depend on the extent that it fulfills key criteria, not only in the areas of security and networking, but also in the critical categories of performance and reliability, flexibility and compatibility, and scalable management.

Additionally, as an option of the researcher, an application acceleration platform which allows higher utilization of the bandwidth between the two sites, thereby reducing the need to upgrade the current E1 line if future speeds are required. A clustered environment in both the main site and disaster recovery site is a must to make sure no chance for fail down in the main servers. Figure 3.2

3.7.1 Network Security

AMLU and all Member banks and financial intuitions including SWIFT and RTGS-JO should have their own network infrastructure. Regardless of the option chosen, all members are ultimately responsible for ensuring their own security.

The AMLU should embark on two very significant network security initiatives that will have a major impact on internal network security and on the security of service delivery. First of all, the AMLU Public Key Infrastructure, which offers protection to all desktop systems in the AMLU. The Unit should lead and by adopting both the any good public Key Infrastructure technology and a certificate policy of the member banks and financial institutions. The second major initiative in this area is the development of a Secure Channel, which will be a common network service offering to succeed AMLU net. The Secure Channel will offer network services, security services (access control, authentication, authorization, confidentiality, data integrity and non-denial), Directory services, and support for common applications. The Secure Channel will be a major infrastructure component for the AMLU Online system.

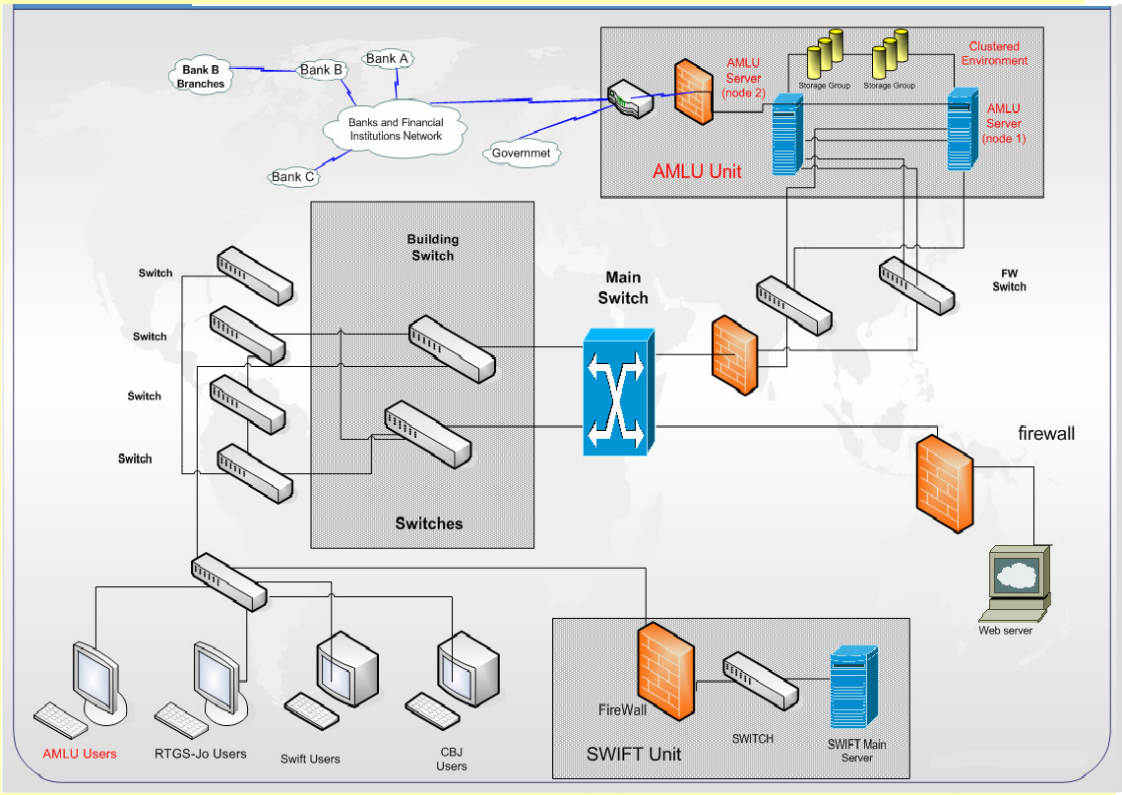


Figure 3.4: Proposed Detailed Diagram for AMLU inside network

3.7.2 Proposed Environment Security Regions

We suggest dividing all involved parties in separate departments and group ranging from very large units with small road and expand permission to small, highly focussed units. All rely on communications networks. As some departments have already established their own networks, others use the common network services available from local Telecommunications and Informatics Services. However, all units and departments are faced with the need to address perimeter defence. All member banks and government units are required to comply with the AMLU security Policy which has to be identified. But departments are individually accountable for protecting their assets. This is influential in determining the security approaches and solutions.

Up to this point, member banks have developed or adopted their own individual perimeter defence solutions and this has resulted in a

variety of approaches that, in some cases, harm group interoperability and could make it difficult to realize some of the AMLU objectives. The overall objective of the Baseline Requirements for IT security Region standard [FATF] that has recently been completed is to assist departments and agencies to secure government networks and implement perimeter defence measures in a consistent manner.

Note that the IT Security Regions address only perimeter defence. They are not intended to meet all of the IT security requirements needed to safeguard end systems, applications or data as this the responsibility of each member on its own.

3.7.3 Concepts of AMLU Security Areas

Network security is concerned with countering threats that originate in the external network (i.e. the network external to the enterprise) and those from within the network itself. Although Internet-based threats are pervasive and growing rapidly, for most organizations insider threats constitute the dominant threat to networks and end-systems. The insider threat originates from three sources: hostile insiders; compromised nodes; and human, system or configuration errors.

- **Network security Fulfils Three Functions**
  a. It protects the network itself from accidental and malicious threats.
  b. It protects end-systems and applications using network facilities from malicious traffic.
  c. It supports the provision of services to protect user data in transit.

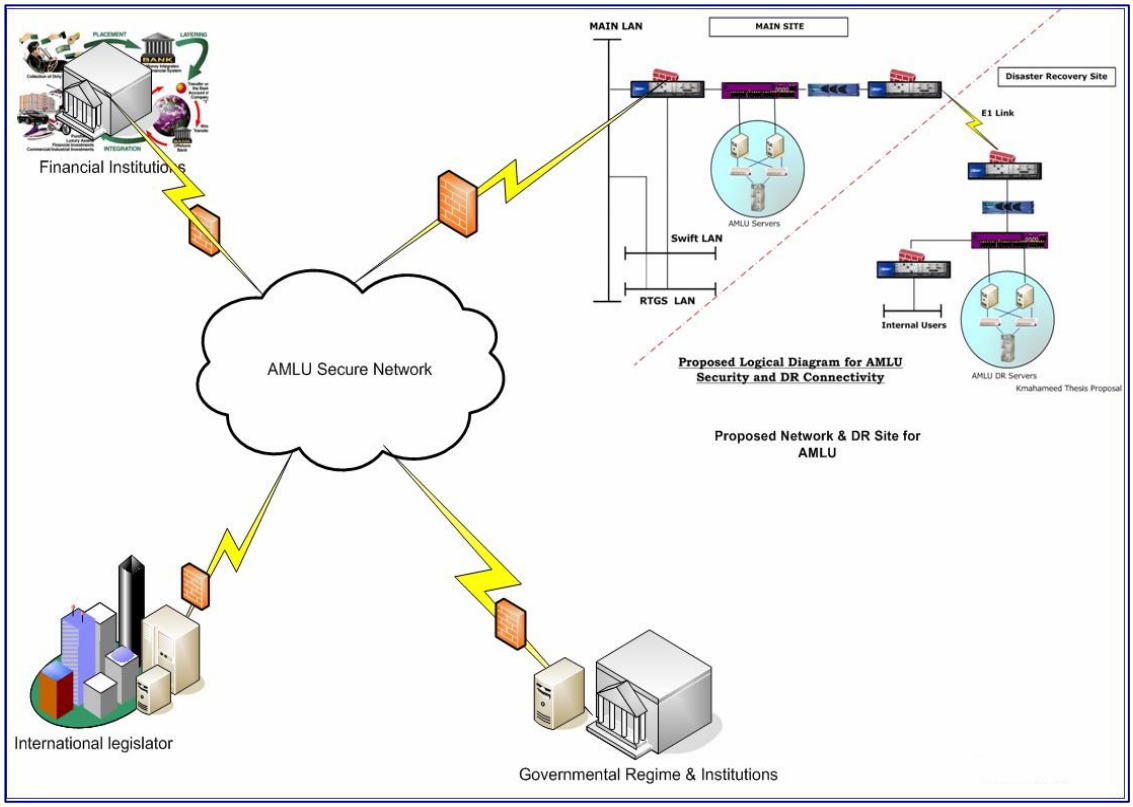


Figure 3.5: AMLU-JO connection with the world

The idea here of physical security Areas is to be well established. For example, we suggest here that the Security Policy identifies five types of physical security area: a Public Area, a Reception Area, an Operations Areas, a Security Area, and a High Security Region.

These physical security regions are distinguished by the strength of perimeter defence, the degree of control over the individuals and equipment allowed in the region, the degree to which movement within the region should be monitored, and the trust assigned to the individuals allowed in the region. For example, the public is allowed access to a Public Region without an escort but access to a High Security Region is strictly controlled and movement is often monitored. The type of region determines the sensitivity of data that can be

processed the region (e.g. sensitive data cannot be processed in a public region).

Similarly, the concept of a security domain is a well-accepted construct for establishing security boundaries and accountabilities. An AMLU Security region is a special type of security domain that is defined as a networking environment with a well-defined boundary, a security authority which is supposed here the AMLU.

Different types of IT Security Regions are distinguished by their characteristics which are defined by technical security requirements for interfaces, traffic control, data protection, host configuration control and network configuration control.

- **Security Regions in Depth**

The AMLU model should define seven types of security regions:

1. A Public Region, which is entirely open and includes public networks such as the Internet. No restrictions are placed on this Region as it is entirely outside the control of the AMLU. The Public Region environment is assumed to be extremely unfriendly;
2. A Public Access Region, which mediate access between operational systems and the Public Region. This Region is a tightly controlled domain that protects internal AMLU networks and applications from a hostile Public Region environment and also acts as a screen to hide and limit exposure of internal resources from the Public Region. Access to AMLU Online services will be implemented in the Public Access Region.
3. An Operations Region, which will provide a relatively secure network environment and is the standard

environment for routine AMLU operations but is not suitable for sensitive or critical applications.

4. A Security Region, which will provide a tightly controlled network environment suitable for critical servers or systems processing sensitive information.
5. A High Security Region, which will provide a tightly controlled network environment suitable for safety-critical applications or systems processing classified information like the AML application.
6. A Special Access Region, which will be a tightly controlled network environment suitable for special processing needs.
7. A secure extranet Region, which will support directly, connected extranet services with highly trusted partners.
8. So as described in the previous sections and as illustrated in Figure 3.3. The AMLU Security Regions will define the network limitations and associated outer limits defence requirements by:
    a. Defining the entities that populate network security Regions.
    b. Identifying discrete entry points.
    c. Filtering network traffic at gateways.
    d. Monitoring the state of the network.
    e. Authenticating the identity of network entities.
    f. Monitoring network traffic at the entry points.

The logical model of perimeter defence has two components: border Integrity, which addresses the threat of unauthorized network interfaces; and Traffic Control, which counters threats such as denial of service, malicious traffic and unauthorized content.

An illustration on how the AMLU Security Regions might be realized in practice is shown in Figure: 3.6 The AMLU common backbone network has been implemented as an Operations Region. All departments access the Public Region (e.g. Internet) through this common backbone using one of the Public Access

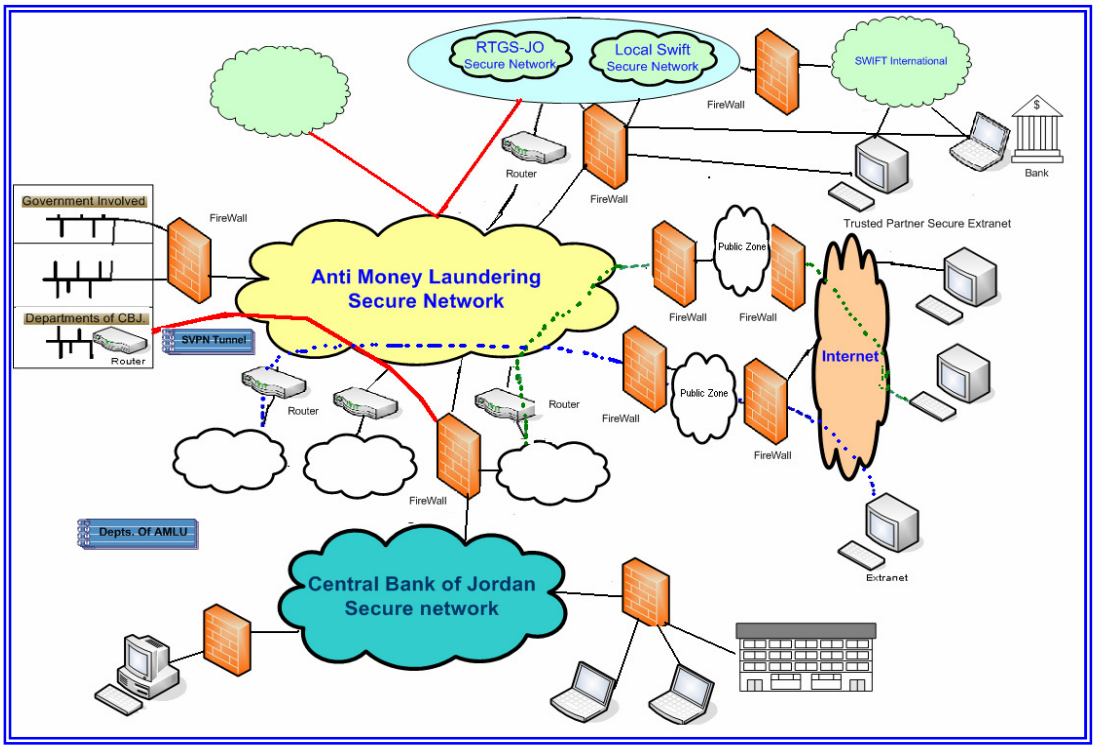


Figure 3.6: AMLU-JO Security regions

Regions provided as part of a common infrastructure. Department X implements three Regions: two Operations Regions and a Security Region. Each of these Regions has a single point of presence in the AMLU inter-network as shown by the fire-walled connection to the backbone figure 3.3. One of the Operations Regions is implemented as two enclaves that are connected via a secure tunnel over the AMLU

backbone. Department x also supports a secure extranet connection to a trusted partner.

Department Y implements three Operations Regions and supports mobile users through secure remote access to one of these Regions. Departments X and Y share Data Link and Physical Layer infrastructure between Operations Regions installed in a building.

Department Z implements a Security Region as two enclaves connected by a secure tunnel. Department Z uses a full VPN to provide confidentiality of traffic as it moves across the backbone. Department C also implements an Operations Region and supports extranet services to partners.

☑ ***Public Access Area***

At this point, only the public access region has been specified in detail but, given the critical role of the public Region as the buffer between the hostile public Internet and the internal resources, one could argue that this is the most critical Region. Figure 6.2 illustrates the three components of the public access Region, an external access network, a demilitarized Region DMZ and an internal access network. Firewall type devices would normally be placed at both the internal and external access network boundary points with the DMZ. Application proxies for common government services and applications such as e-mail, web access, remote/mobile access and extranet services would normally be located in the DMZ.

As illustrated in Figure: 3.6, Public Access Regions could be implemented for a single department or several departments could share a single public access Region.

3.8 Specific Security Issues

The heart of the system is a browser-based public key infrastructure plug-in that uses standard HTML tags and works with any web browser. Two keys are used for this key, one for digital signature the other for encryption. User authentication can be as simple as a password or can be based on much stronger methods including biometric techniques. The system should permit creation of legally-binding transactions over the Internet. Because AMLU use a variety of document formats and processing techniques in their offices, the application should be developed to accommodate a variety of input data formats, including fax, XML, scanned data and direct browser entry. Whatever the source of the input data, it is all encrypted and stored in the database. An audit trail function should apply to the AML data collection process.

An important innovation allows the developer to define the specific fields that are to be protected from unauthorized access. Encryption can then be performed selectively at the field-level of the database.

The data security module controls every user's session-access to AML data on the central servers at AMLU. Access control functionality is based on who the accessing party is and what they are able to do and see. Security at the member bank and all other involved institutions level limits the member's ability to view and modify records over the Internet to the records of those AML. Logs are maintained on AML file activities so that all changes are tracked. No data is ever deleted. Figure: 3.7 illustrate the overall process.

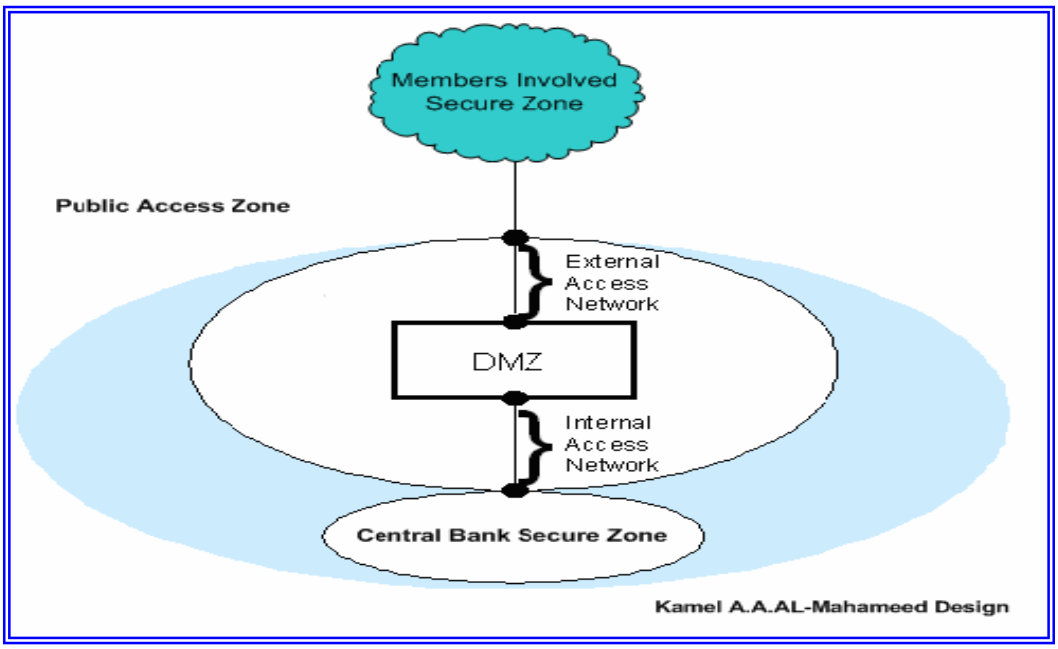


Figure 3.7: Database Security Module

The plug-in is capable of encrypting data for the AML file such that the file can be seen only by decrypting the data, a task that requires both positive authentication of the user and confirmation of the user's authorization to view the data. Data submitted via the web application is encrypted and then transmitted to the server where the data is decrypted, enhanced and formatted. After the operation has completed all the production functions, the raw data is then re-encrypted using the public key of the contributing AMLU official and stored on the server. Only the AMLU authorised official can access the data at that point.

The use of selective field encryption means that non-sensitive information in the database can be made available to other AML professionals such as member financial institutions and government involved.

3.9 Efficiency of The New Proposed Design

To have an efficient AML system, we think the solution should have at least the following specifications:

- Analyze system performance at a sufficiently detailed level, for example on a rule by-rule basis, to understand the real underlying drivers of the performance results.
- Set systems so they do not generate fewer alerts simply to improve performance statistics. There is a risk of 'artificially' increasing the amount of alerts that are ultimately reported as suspicious activity reports without generating an improvement in the quality and quantity of the alerts being generated.
- Deploy analytical tools to identify suspicious activity that is currently not being flagged by existing rules or profile-based monitoring.
- Allocate adequate resources to analyzing and assessing system performance, in particular to define how success is measured and produce strong objective data to analyze performance against these measures.
- Consistently monitor from one period to another, rather than on an intermittent basis, to ensure that performance data is not unclear, for example, unplanned decisions to run particular rules at different times.
- Measure performance as far as possible against like-for-like comparators, e.g. peers operating in similar markets and using similar profiling and rules.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Introduction

Outside terms of proposed design results which lead to implementation, and getting the most of the criteria's mentioned in the previous chapters, the researcher's point of view is that implementing an AML solution is pretty much similar to implementing any business-critical software or hardware application or solution. The AMLU of Central bank of Jordan, or member's bank and financial institutions in our case and the government sector involved should note that similar to other good quality software or hardware applications, good quality AML solutions come with a number of customizable features and administrator modules for control. It is hence imperative that a member's bank or financial institutions forms a core team or a committee which gets well trained on the AML inclusive solution results so that they are able to use and develop on all the features of the solution if implemented at the AMLU-JO.

Thesis results should be distributed through the AMLU member's and parties involved if decided to be implemented a Request for Proposal (RFP) from different software and hardware providers. Who are interested in implementing such a solution, either the secure network or the AML software, for all members or members interested and don't have an installed solution at their premises or both solutions to be integrated for parties, the suggested committee will also coordinate with other aid organizations working in the area of AML, including the training being assumed.

The AMLU and all members of the system must be able to demonstrate results against a documented plan to mitigate risks facing

the whole structure of Compliance procedures, when poorly designed, implemented the structure; it can damage contacts with the parties involved. Regulators, however, are not asking for strictly set solutions. Each financial institution needs to collect customer information for risk rating, monitor transactions, investigate, and report as appropriate, and use the new technology proposed.

4.2 Technology - Answer of Awareness

Uncovered persons represent a particular risk for fraud, either because of an existing position of power and influence or because of prior activities. While some of this data is provided freely by regulatory bodies many institutions choose to subscribe to a single source that combines multiple versions of such lists with other research information. AML projects are often driven by an alarming compliance deadline, which can minimize the ability to integrate them into the broad IT infrastructure.

4.2.1 How Does Jordan Measure up Regarding This Study?

With Jordan's new AML laws having effectively been drafted and rolled out local executives are under considerable pressure to deliver AML fully automated systems on a very tight time frame. A major factor in those is technology expense, combined with a relative lack of automation in most systems.

All the above should be continued and completed by a good application, outsourced from a good vendor or tailored at the AMLU of Jordan and all the members involved in the solution. This software is part of the whole cycle to complete automated secure Alerts monitoring and reporting, as well as this software is the sole element of the infrastructure defined. The primary objective of AML solution software is to prevent or minimize the amount of money laundering that takes place among the transactions done by all parties involved. AML

solutions software try to achieve this objective by Preventing transactions done by confirmed/known money launderers, and/or Monitoring and reporting all transactions to identify those that involve money laundering. From our study and investigating for the good outsourced software solution the researchers advice that the primary AML solution modules should be as follows:-

- Filtering of known money launderers – Watch-list Filtering.
- Monitoring transactions to identify suspected money laundering, transaction monitoring.

We have to take into considerations that suggested AML solutions should provide the key functionalities – watch-list filtering and transaction monitoring, not only focus on watch-list filtering. Also this solution should not focus on the banking industry, but also to be adaptable to be used for other financial services firms and related industries.

The suggested AML outsourced software solution for any member bank or financial institution shouldn't be used in separation from institution's other applications, because it needs data from other databases to do the right job. It should integrate with the rest of the software and solutions that a banks uses, by the case of banks, and financial institutions AML systems need to integrate with banks' existing IT system, such as the core banking system, reporting system and the workflow system. It should have integration mechanisms that avoid duplication of data and enable integration using web-technologies to interface with the other applications.

These unusual or unexpected transactions which do not represent a risk but are flagged for compliance, can overload the system without creating any better efficiency. This leads us to select an Adaptive software Solution that Can Meet Current and rising AML policy, as

regulations continue to evolve and lawmakers consider new measures that will certainly require financial institutions to become even more responsible for all transactions. It is crucial to select technology that meets current regulations and can also adapt to meet new requirements as they emerge. It may be convince for some financial institutions to simply meet minimum compliance with basic technology that barely meets current regulations. This is a band-aid approach that will eventually cost more as the financial institution is forced to upgrade technology. As for this software providers should have keep up with latest development in AML regulation.

AML solutions capture a significant amount of transaction and customer data. These information and data can be used to provide value-adding customer intelligence to the member banks or financial institutions. Many good quality AML solutions today provide rich knowledge about a bank's customers.

4.3 Advantages of The Design

The advantages of the designed infrastructure include the following:-

a. Reviews the current legal scheme in Jordan's AMLU, designed to combat money laundering, with its current manual solution, the problems and AMLU future visions, and also identifies emerging trends in high technology and their possible effect on money laundering.

b. Provides the AMLU-JO, member banks, brokerages and insurance companies (all financial institutions), and the regime with effective, efficient and proven preventive and detective secure network solution that meet regulatory requirements, streamline operations and combat money laundering and financial crimes.

c. Improving access to AMLU-JO at Central Bank of Jordan by providing information and make it available to law enforcement, including improved access and extension of material from a suggested crime enforcement network.

d. Improving access and review of suspicious activity reports so that financial transactions related to possible money laundering offences are thoroughly investigated.

e. Encouraging relationship with financial community so that communication and coordination with law enforcement can be improved; and identifying emerging high-technology trends and considering their effect on money laundering [Cornez], include a discussion of high-tech replacements for traditional techniques of money laundering.

f. There are many other advantages to the creation of AMLU Secure Network Solution as well, and the benefits will only increase due to the network effects that will emerge when large numbers of researchers work together to prepare and implement the detailed function specification of the suggested software and build the secured network.

4.4 Validation of The Results of The Design

In order to validate the proposed standard, in-depth a study to the elements of the design should be made with selected members. The study should provide a reality check on the proposals and also produce some predefined and sometimes unexpected responses. An assistant was given during evaluating the result from specialized engineers to evaluate using the opnet tool for network evaluation and good results were summarized as good connection is established and monitoring results were good, from the researcher's point of view this is not the area to discuss the results as this is supposed to be done while implementing the solution during the final stages.

From the point view of the researcher, a very good support has to be indicated for the common perimeter approach. In some cases for members who already implement a similar security Region approach in their premises has to edge defence but the study would result in a common approach across the entire enterprise.

One concern not expressed in our study was the cost of implementing a system that involved more than one firewall, but from our point of view this is not a major concern for such project and such the environment of financial institutions.

4.5 Securing AMLU Transactions

As a result of the study the implementation issue of the proposed design infrastructure described above relates to the protection of AML information. However, before examining the details of the implementation, we talked about reviewing the more general background leading up to the specific implementation.

As Additional business requirement is that there would be legal and auditable records of contractual obligations and transactions. In the paper world, we trust the written records such as contracts and invoices because they are signed by persons authorized to act on behalf of the organization. In the digital world though, we need to guarantee the identity and authority of the sender and receiver, as well as the validity and integrity of the electronic document. In addition, there is a need to protect the integrity and validity of the transaction both before and after it has been transmitted electronically.

4.6 Protecting Anti Money Laundering Alerts Records

The root of this application is protecting AML Alerts records from unauthorized modification or disclosure while ensuring that relevant information is made available to authorized AMLU officials. AML Alert records are particularly sensitive but parts of them need to be

accessed by different AMLU officials who are often located in different places or even different departments like the government sector involved. Additionally some of the information may be useful to government involved sector.

An outsourced application should be developed for the AMLU to be used for monitoring analyzing and inspecting Alerts of Money Laundering.

This application should maintain an on-line and off-line version of Money Laundering records. Each Money laundering record contains such information as Money Laundering SAR, analysis of the Money Laundering details of any surrounded devices, and emergency contacts. In other words, the AML records are both complete and very sensitive.

The on-line version should be contained in an encryption-protected database: the off-line version is a portable AML record, in the form of a mini-HD. The main database is maintained as the central repository and is updated as needed by AMLU officials who are authorized to access the database. Updated data are re-issued, as appropriate, from the central database. The primary AMLU provider creates and has access to, the most complete record of a Money Laundering records. The record includes their all the information needed about Money Laundering criminals. Sensitive data on the central database should be encrypted at all times (and regularly backed-up to off-site storage). All transmitted records, such as updates to the central database from a member's banks or involved institution should also be encrypted and signed.

4.7 Particular Vulnerabilities, Troubleshooting & Auditing

E-mail , extranet services gateway were all identified as being prone to particular vulnerabilities and presenting problems for involved parties. In addition, web servers and proxies, virus scanning for web

content, Internet news groups, DNS were all identified as frequent sources of security alerts.

It was generally felt that some security services, such as virus scanning and content filtering might well be provided in a common public access Region, to fight against internet threats, as there will be a concern over accountability for security breaches. Each Member has different levels of accountability and different requirements regarding privacy protection. Since members are individually accountable for protection of their assets, the question of how accountability would be assigned in the event of incidents that occur when using common security services was fully expected. In spite of this, most members should indicate they would be comfortable sharing services with departments that had common requirements and similar levels of protection. However, one concern that of maintaining trust. While it is possible establish trust with other members by conducting detailed, one-on-one, inspections of configurations and security provisions, it is very difficult to have confidence that such trust is maintained as systems are in a continual state of change.

The responsibility of, troubleshooting and auditing of security breaches over the suggested secure network should be identified as a major role of the AMLU of Central Bank of Jordan. The internal breaches have to be treated as potential criminal investigations, as the AMLU should make a decision to prosecute in all cases of criminal misconduct.

4.8 Firewall Configuration, Securing The Data, Reporting & Review

Firewall configuration and filter management should be identified as tasks that require significant engineering effort. Firewall configuration in particular is a largely manual process that requires examination and cross checking by several individuals plus

independent verification of any changes to the rule set before any action is confirmed. As a result, strict procedures should be identified and put in place that will allow sufficient time for the installation and examination of proposed rule changes.

In summary, the draft standard for a common approach to the AMLU of Jordan, the researchers point of view is that defence based on IT security Regions is the best in this area as the researcher's point of view, as the standards of AMLU can be implemented without major impact on member banks or government departments. Work remains to be done on defining the requirements for the other security Regions but implementation of Public Access Region requirements can begin in the near future. Although the standard has been drafted from the perspective of a large public sector organization, many large private sector organizations with relatively autonomous divisions should adopt a similar approach to financial border defence against Money Laundering.

Financial border defence is very important but, as noted in the first part of this study, it is not intended to meet all of the IT security requirements to safeguard end systems, applications or data. In fact, the IT Security Region standard described above recognizes the need, to protect the confidentiality and integrity of Money Laundering data during transmission.

The particular example chosen for this second part of the case study has been selected for two reasons. Firstly, it recognizes that protection is needed over and above that provided by border defence. Data must be protected at all stages, whether in transit or in storage. Secondly, this solution was developed in direct response to the needs of the AMLU. The implementation described uses an established security technology public key infrastructure.

From our point of view there should be a clear allocation of responsibilities for reviewing, investigating and reporting details of alerts generated by AML systems responsible for this work should have appropriate levels of skill and be subject to effective operational control and quality assurance processes.

4.9 Key Features & Key Functionalities

The researcher also sees that the design of any AML system should have been developed using a flexible rule-engine based approach, which is complemented by the artificial intelligence. A selection of rules is pre-built into the engine which allows for meeting the standard AML requirements across the globe. These rules apply across different banking services like retail, corporate, insurance, cards etc. Its flexible engine can also be easily customized by bank's users to detect additional scenarios. The study resulted the allowance the transaction monitoring to be monitored at multiple levels.

The design also provided full functionality addressing a whole range of Know Your Customer, and AMLU of Jordan requirements including:

- Sanction Filtering against published watch lists like OFAC.
- Link Analysis to uncover hidden relationships between accounts and customers and then use them to detect suspicious activities involving multiple accounts/customers.
- Customer Risk Modeling enabling the customer risk score and customer segmentation into groups with similar risk profile.
- Risk-based Transaction Monitoring enabling customized monitoring of transactions based on the customer's risk profile.
- Alert and Case Management enabling quick and easy investigation of system generated alerts; it supports maintenance of electronic

case file along with the required workflow and record keeping activities for responding to regulatory inquiries.

- MIS Reporting to generate file reports with minimal manual intervention.

CHAPTER FIVE

FUTURE WORK

5.1 Conclusions

Within this study the researcher has offered a design for a secure framework solution, to fight against Money Laundering in Jordan, this design is integrated with the current running applications at Central Bank of Jordan, the RTGS-JO, and the SWIFT international network.

The study provided the full context and explored the possibility of within which the secure design, will assist AMLU-JO the member banks and financial institutions and the government sector involved, to achieve their goal, fighting against money laundering by Electronic means, this will also achieve better understanding for the parties involved and to become more sensitive to AML realities, develop their business plans accordingly, and successfully meet the needs and challenges of the AMLU-JO. The proposed design in this study is unique in its principles and infrastructure as there is no similar infrastructure for AML, that take into consideration all the elements to come up with a fully integrated hardware and software solution for AML.

In Chapter 1, the researcher outlined the introduction to the study and includes information related to the need of the study as follows:-

- Problem Definition.
- Area under Study.
- Objectives.
- Significant of the study.
- Motivation of the study.
- Thesis Contributions.

- Limitations and Delimitations.

Chapter 2 explored a review of the literature and related work. This review includes the history of AML technical research, development and implementation that are the structure of the new proposed project. The AMLU-JO duties and the cycle of Current AML procedures used the stages of suspicious reports and a brief discussion about the Financial Action Task Force, OFAC, Basel Committee and IMF are also reviewed.

Methodology of its basic approach to each task of the study is reported in Chapter 3. As the Methodology, AML Technical Education and Awareness were all discussed, Model design and development, Secure Network and Software operational Activities. Report plan which is a summary of the content of each chapter also declared at this chapter. It concluded that the most appropriate practical approach to achieve the objectives of the study would be to combine already existing information about the AML solutions and involved in that design. The setting for the study and subjects are described. The theoretical structure for the proposed design, their design, construction and application is also described in this chapter. This chapter also includes a detailed description of the procedures of the study and all the elements involved.

The results and discussion which are found in Chapter 4 consist of: an item by item analysis of the expected results of the study. A summary of presented technical architecture and diagrams for the study are also presented.

Chapter 5 includes a summary of the research, conclusions and recommendations. These brief concluding will:

- Present some general, overarching conclusions about the AML secure Infrastructure based on the research undertaken in this study; and

- Suggest some possible areas that should be taken into consideration during implementation of the design.

5.2 Future Work

While this thesis effort has shed important insight on developing the secure infrastructure for AML for the AMLU-JO of Central Bank of Jordan, it by no means offers a full analysis of all the dynamics of this emerging risky factor on the economic and financial sector in Jordan., while Money Laundering has come a long way both in world as well as in Jordan. In general, it is still a relatively new field for the area around. Significant information gaps about the Money Laundering software and hardware solutions still remain and by filling these gaps the world can strongly reinforce the business case for developing investments in Jordan regarding Money Laundering, fighting in electronically means by adopting full secure infrastructure.

For example, unlike many other high-tech solutions, AML has no standardized data on local financial areas such as secure infrastructure, what solutions to use, which provider to deal with, kind of database parameters etc. These types of information are critical in any business and especially more relevant in. It is recommended that AMLU of Jordan establish an AMLU collection Unit or system that can be used to develop and maintain a database of AML.

5.2.1 Other Information Gaps

National Awareness—most of the AML laws are unknown by beneficiaries of banks and financial institutions. Having better

information on the extent to which beneficiaries are involved in can help the economy position.

Government should pay attention to this issue by issuing some sort of brochures defining Money laundering and the penalties on such a crime.

By undertaking the study results, Workshops for specialized engineers and software developers, to identify how to develop a standardized efficient and secure design Framework for AML and -related software and hardware solutions would go a long way in Jordanian AML participation options.

A more detailed summary and assessment of the Technical Architecture Document, which represents the fulfillment of technical issues work plan, is a targeted communications document and user-friendly reference that contains specific technical information, about the needs of the infrastructure development and implementation as a brief simulation was made during the study which is not enough to estimate the efficiency of the solution proposed.

5.2.2 Recommendations For Future Work

In the future, the project results and design should be taken into consideration in expanded scope to find the faster determination of AML law enforcement, while thinking of developing and implementing any similar infrastructure.

We suggest that implementing the Framework will require consulting services (Local) and (International), who will assist in organizing workshops and training as well as helping build the recommended secure infrastructure, they will also be engaged in an international consulting issues for international cooperation, reviews

will be conducted by AMLU, the Government, and the consultants to consider the reports.

Another recommendation is start preparing a TAD, and a RFP for the proposed design to help assist the AMLU-JO implementing the AML Law technically and enhancing operational activities of AMLU-JO and other parties involved.

And last but not least be continued with other student in next years to upgrade this study, testing system results that can be a great project to simulate in the university.

REFERENCES

- Alexander, Richard.(1998).EU: The EC Money Laundering Directive, Journal of Money Laundering Control, Institute of Advanced Legal Studies, Vol. 2, No. 1.
- Bell, R E. (1998).An Introductory Who's who for Money Laundering Investigators, Journal of Money Laundering Control, Vol. 5, No. 4, pp. 287-295.
- Benarji, Ch. (2003).The United Nations Convention against Translational Organized Crime: A Study of Measures to Combat Money Laundering, Indian Journal of International Law, Vol. 42, afl. 4, pp. 549-564.
- Broome, John. (2003).Anti-Money Laundering: International Practice and Policies, second edition, Pearson education.
- Comer, Douglas E. (2005).Computer Networks and Internets, 4th Edition, Pearson Education.
- Cornez, Arnold. (2006).Offshore Money Book: The How to Move Assets Offshore for Privacy, protection, and Tax Advantage, 3rd Edition, Prentice-hall.
- Crimes Section. Cutting off the Lifeblood of Terrorists. Statement for the Record. House Committee on Financial Services. Washington, D.C.: October 3, 2001.
- Drayton, Fits-Roy.(2006).Dirty Money, Tax and Banking: Recent Developments Concerning Mutual Legal Assistance and Money Laundering, 'Harmful' Tax Competition and the Future of Offshore Financial Centers, Journal of Money Laundering Control, Vol. 5, No. 4, pp. 302-317.
- FBI, Federal Bureau of Investigation, Criminal Law and Criminal Justice, Vol. 11, 2003, pp. 204-219. US Department of Justice.
- Fisher, Jonathan. (2004).Money Laundering Law and Practice, 3rd ed., Oxford University Press.

- Hanna, Martin, S. (2004).E-Banking hardening security, 4th edition, NY.
- Hetzer, Wolfgang.(2003).Money Laundering and Financial Markets, European Journal of Crime, Criminal Law and Criminal Justice, Vol. 11, 2003, pp. 264-277.
- Johnston, Barry R and Carrington, Ian. (2006).Protecting the financial system from abuse - Challenges to banks in implementing AML/CFT Standards, Journal of Money Laundering Control, Vol. 9, No. 1, 2006, pp.48-61.
- Kochan, Nick. (2008).The Washing Machine: How Money Laundering and Terrorist Financing Soils, second edition, Washington D.C.
- Lee, Walter.(2002).Getting a Grip on Technology in Money-Laundering Prevention,2nd ed., NY.
- Lilley, Peter R.(2006).Dirty Dealing: The Untold Truth about Global Money Laundering,3rd edition,
- Matthews, Jeanna. (2007).Computer networking: Internet Protocols in Action, 3rd edition, NY.
- Maynard, Peter D. (2006).Abuse of Power: Starting the March to Restoring the Competitive Advantage of International Financial Centers, Journal of Money Laundering Control, Vol. 5, No. 4, pp. 325-329.
- Melnik, Steven, V. (2005).Anti-money-laundering responsibilities, 2nd edition, Washington.
- Olifer, Natalia. &Olifer, Victor. (2006).Computer Networks: Principles, Technologies and Protocols for Network Design, 2nd edition, printec hall.
- Pheiffer, Marcel. (1998).Financial Investigations and Criminal Money, Journal of Money Laundering Control, Institute of Advanced Legal Studies. Vol. 2, No. 1.
- Priess & Richard T,(1998).The Consequences of Anonymous Access to the Financial Payments System, Journal of Money Laundering Control, Institute of Advanced Legal Studies, Vol. 2, No. 1.

- Richards, J R.(1999).Translational Criminal Organizations, Cyber crime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators,2nd ed. CRC Press, Boca Raton, FL.
- Robinson, Jeffrey. (2007).The Laundrymen: Money Laundering the World's Third Largest Business, 2nd edition, Cambridge University Press, New York.
- Santini, Carlo,(2005).Globalization and the Offshore Dimension - Building Integrity, Confidence and Cooperation, Journal of Money Laundering Control, Vol. 5, No. 4, pp. 318-322.
- Santini, Carlo.(2004).Globalization and the Offshore Dimension - Building Integrity, Confidence and Cooperation, Journal of Money Laundering Control, Vol. 5, No. 4, pp. 318-322.
- Shahid, Nawaz; McKinnon, Roddy and Webb, Robert.(2005). Informal and Formal Money Transfer Networks: Financial Service or Financial Crime, Journal of Money Laundering Control, Vol. 5, No. 4, pp. 330-337.
- Stessens, G. (2000).Money Laundering: A New International Law Enforcement Model, 2nd ed., Cambridge University Press, New York.
- Tanenbaum, Andrew S. (2003).Computer Networks, 4th Edition, Pearson International Edition.
- Truman, Edwin M. (2006).Chasing Dirty Money: Progress on Anti-Money Laundering, second edition, Washington, D.C.
- Voluntary SAR Filings by Money Services Businesses Identify Patterns of Suspicious Activity." Press release. Washington, D.C.: FinCEN, October 22, 2001.
- Weaver, Constance A. (2006). All Is Clouded by Desire: Global Banking, Money Laundering, and International Organized Crime, 2nd ed.,
- White, Curt S. (2005).Data Communications and Computer Networks: A Business User's Approach, 3rd edition. Washington, D.C.
- Woods, Brett, F. (1998).Art and Science of Money Laundering, 2nd edition, Pearson Education.

- AMLU, Available from :(http://www.amlu.cbj.gov.jo/),[access on 20/3/2008].
- Basel Convention, available from :(http://www.basel.int/),[access on 22/5/2008].
- Central Bank of Jordan, available from :(http://www.cbj.gov.jo),[access on 23/6/2008].
- FATF.Cracks Down on Terrorist Financing. Press Release. Available from :(www1.oecd.org/fatf/),[access on 22/5/2008].
- FATF, Special Recommendations on Terrorist Financing. Washington, available from :(www1.oecd.org/fatf/),[access on 22/5/2008].
- Financial Action Task Force on Money Laundering. Basic Facts about Money Laundering. Available from :(www1.oecd.org/fatf/),[access on 22/5/2008].
- Financial Stability Forum. About the FSF. Available from :(http://www.fsforum.org/),[access on 23/5/2008].
- International Monetary Fund. Enhancing Contributions to Combating Money Laundering: Policy Paper. Prepared by the staffs of the International Monetary Fund and the World Bank. Washington, D.C.: IMF, 2001.available from:(http://www.imf.org/external/np/ml/2001/eng/042601.htm),[access on 17/10/2008].
- International Money Laundering Information Bureau. Available from :(http://www.imlib.org/),[access on 17/5/2008].
- National Money Laundering Strategy for 2000. Washington, D.C.: U.S. Department of the Treasury and U.S. Department of Justice, 2000.available from :(http://www.treas.gov/press/releases/docs/ml2000.pdf),[access on 20/7/2008].
- OFAC, Office of Foreign Assets Control, available from :(http://www.ustreas.gov/offices/enforcement/ofac/),[access on 27/6/2008].

- People. Available from: (http://people.exeter.ac.uk/watupman/undergrad/ron/methods%20and%20stages.htm), [access on 15/8/2008].
- RTGS-JO.available from :(http://www.rtgsjo.cbj.gov.jo/),[access on 25/6/2008].
- Schroeder, William.(2001).Money Laundering: A Global Threat and the International Community's Response, FBI Law Enforcement Bulletin: (May 2001), pp. 1-9. http://www.fbi.gov/publications/leb/leb.htm
- Swift international network. Available from :(http://www.swift.com/),[access on 25/6/2008].
- The Forty Recommendations. As updated. Paris: OECD. Available from :(www1.oecd.org/fatf/),[Access on 18/7/2008].
- World Bank website, deals primarily on the macro-economic consequences of money laundering. Available from :(http://www.worldbank.org/fandd/english/0397/articles/0110397.htm),[access on 2/9/2008].

APPENDIX A:

RTGS-JO.

Real Time Gross Settlement System - Jordan

RTGS-JO Is an electronic, central, real time, Gross sottement system. It is designed to handle Credit Transfers (Giro system). Settlement is final and Transfer orders are irrevocable. It also provides a central settlement point for all netting systems in the Kingdom.

Two basic elements were taken into consideration in designing the system, Safety & efficiency. Recommendations set by "Committee on Payments & Settlement Systems" (CPSS)/ BIS – Basle constituted a source for policy rules. For more information see http://www.bis.org/cpss/

Membership:

Membership is mandatory for all operating Commercial banks in Jordan.

The Basics of the system:

Basic Operational Features:

1- Use member banks' accounts held at the Central Bank of Jordan, "Central Accounts".

2- Use SWIFT as messaging system.

3- No overdrawing is allowed.

4- Final payments.

5- Irrevocable orders.

6- Central queue management.

7- FIFO mechanism plus optimisations Features.

Additional important Features:

1- Real Time continuous On Line Monitoring for members' accounts.

2- Intraday liquidity provision.

Central Accounts:

The Accounts of member banks in Jordan Dinar held at the Central Bank of Jordan are used as settlement accounts for the system. Balances in these accounts represent the legal Required Reserve plus any additional amounts. RTGS-JO uses SWIFT network as a High standard secured messaging system. //

From central Bank of Jordan Official Web Site. www.cbj.gov.jo/

APPENDIX B:

SWIFT

Society for Worldwide Inter-bank Financial Telecommunication:

- A co-operative established by and for the financial industry.
- A global provider of secure financial messaging services.
- Is the acknowledged leader in international standards-setting for the financial industry

SWIFT Enables its customers to automate and standardize financial transactions, thereby lowering their costs, reducing their operational risk and eliminating inefficiencies from their business operations. SWIFT also provides opportunities for its customers to create new business opportunities and revenue streams.

SWIFT has a record of success in terms of traffic growth, price reductions, security, reliability and resilience, standards-setting and expansion into new markets.

From SWIFT Official Web Site. www.swift.com/

APPENDIX C:

Licenced Visio 2003 drawing tool, smart draw 7, and Microsoft paint were used to draw the illustration figures.

OPNET's Configuration Auditing: which is an IT Sentinel perform automated and systematic configuration audits, analyzing an up-to-date model of the production network to diagnose device misconfigurations, policy violations, inefficiencies, and security gaps. Is used for simulating the network configuration as a breif limited simulation.

From OPNET official web site http://www.opnet.com/