ELSAG DATAMAT

AML – Anti Money Laundering

White Paper

1.   The company

A constant quest for innovation, effective solutions and customer satisfaction are the key values in the patrimony of ElsagDatamat, who has been supporting Organizations for nearly a century in their way through technological and industrial innovation.
With a long-standing experience and proven ability in developing new technologies to provide innovation and competitive edge for its customers, ElsagDatamat has more particularly been in the Banking and Finance market for over 30 years, servicing more than 250 customers.

Moreover, seizing a challenge in the mid 90s with a major Islamic Bank in the Middle East which consisted in the re-engineering of the Core system, ElsagDatamat has developed a special mastering of Islamic procedures. This constitutes a useful patrimony at the service of those Commercial Banks who need to offer, in dedicated branches, banking services compliant with the Islamic rules.

Together with a rich offering of a whole Banking platform based on new generation technologies, ElsagDatamat provides solutions always designed and developed with an eye on the future as well as services that go beyond the sole maintenance and support. In fact, consultants, developers, analysts, programmers are dedicated to guide successfully Customers before, during and after implementations and to support them in their evolution towards innovative services and products.

2. The mission

We care for you. You care for the Customer

As market researches have recently stressed, the growing trend that pushed banks and financial institutions towards more and more sophisticated tools to keep up with the innovative technological propelling force is now addressing the traditional bank branch, forcing it to leverage its services to its new mission: anticipating customers' needs with adequate products and services.

This is why it becomes vital for banks to heavily invest in systems that not only secure streamlined services on the new delibery channels, as their customers now demand to access and operate directly, but are also capable to guarantee maximum accurate, effective, and timeliness responses in the care of the customer at the branch.

This means both putting the Customer at the heart of the process and winning the challenging task of integrating the complex business processes with the network delivery channels and core systems. A challenge that ElsagDatamat took up with its offering to the Banking market, designing and developing highly performing modules, where Technology is at the service of the Bank to better care for the Customer.

3.   Anti Money Laundering Principles

"*The integrity of the financial sector depends on the ability of banks and other financial institutions to attract and retain **legitimate funds** from **legitimate customers**. Illicit activities, such as **money laundering, fraud,** and other transactions designed to assist criminals in their **illegal ventures** invariably damage the **reputation of the institution involved.**"*   (Federal Reserve)

Addressing and combating money laundering activity is a challenge that has been involving a larger number of Banks, Financial Institutions and Intermediaries across the world. Recent international events, that are heavily influencing the business climate, have imposed on governments worldwide to introduce strict regulations in terms of money laundering monitoring, detection and alert.

Organizations that do not comply with such programs can be seriously damaged as they are considered accountable in case of illegal activities held by their customers and many of them are facing the issues with finding the right solution among those on the market.

An effective solution should guarantee that Organizations are able to protect their business, their legitimate customers and their investments by providing them with the most appropriate tools to monitor, investigate and report suspicious behavior.

The AML System conforms with the best international banking practices and supervisory requirements, such as the "Know Your Customer" and the "Customer Due Diligence" Rules issued by the Basle Committee and complies with the FATF-GAFI AML/CFT Standards and Methodology to protect banks against economic and financial crimes and money laundering activities.

ElsagDatamat's solution allows the bank governing the opening and activity of bank accounts in local and foreign currencies of customers that include residents, non-residents, natural and juristic persons (public and private), individuals, corporate and multilateral organizations to which the Customer Due Diligence and Record-keeping rules are applied.

The solution outlines the standard requirements applicable to all banks and stresses internal controls to prevent customers from practicing unlicensed banking activities in domestic and foreign currencies including accepting deposits, transferring funds, marketing investment products, selling mutual fund or offering credit cards.

4. The solution

ElsagDatamat's Anti-Money Laundering end-user Solution is a WEB (Open system) multilanguage, modular and flexible system, offering to the Bank a strategic tool for the prevention, detection and management of "sensitive events" with the following set of functions:

- ❖ **KYC (Know Your Customer)**
- ❖ **Rules and Indicators Configuration**
- ❖ **Operation Monitoring**
- ❖ **Transaction Processing**
- ❖ **Reporting**

It is based on the International Best Practices as well as on the official Recommendations by:

- ❖ FATF (Financial Action Task Force)
- ❖ GAFI (Global Antifraud Initiative)
- ❖ FBI (Federal Bureau of Investigation)
- ❖ Basel Committee on Banking Supervision
- ❖ UIC (Ufficio Italiano Cambi) – Italian Regulatory AML Authority

The system integrates with the Bank subsystems to provide an overall investigation service. It is accessed only by authorized Users and Supervisors, and accesses are monitored through a proprietary Standard Management of the Authorization and Profiling procedures.

The AML System runs within two main integrated areas:

1. Procedure Area
2. Function Area

The Procedure Area manages:
- ❖ the monitoring of all transactions
- ❖ the reports generation of suspicious transactions
- ❖ the Profiling of AML Customer & Transaction types

The Function Area manages:
- ❖ the configuration of rules to detect suspicious transactions
- ❖ the reporting of suspicious transactions to the authority concerned
- ❖ the investigation on high risk customers and suspicious transactions through ad-Hoc inquiry
- ❖ queries on the Global Customer Position

4.1. Modules overview

4.1.1. Know Your Customer

The KYC Module interfaces the Bank's Information System and manages Customers and Walk-in Customers' data to provide Alerts and Reports to the Bank and Central Bank. The

information related to Customers is also verified against official files such us NCCT File and Offshore Financial Centers.

It manages the:

- ❖ Customer Personal Data
- ❖ Customer Identification Document Data
- ❖ Customer Activity Data
- ❖ Guardian or Trustee for the incapacitated person
- ❖ Customer Financial Data
- ❖ Company Information
- ❖ Company Financial Data
- ❖ Customer Evidences
- ❖ Customer links

Any other form of queries on customers can be easily implemented to meet specific requirements.

4.1.2. Rules and Indicators Configuration

Suspicious transactions are identified on the basis of a cross-comparison between the transaction (according to the type or to the subsystem of origin) with the rules or paths that are defined/customized upon system configuration according to the Bank's specific needs. Such rules and paths can be modified or new ones implemented at any time through a proprietary Configuration Management System.

The existence of one or more indicators does not necessarily mean that a money laundering transaction is taking place, but it raises some concerns (Alert) and leads to further investigations.

Indicators must necessarily evolve and will need to be added, removed or amended as the Bank's personnel, supported by an initial adequate training provided by ElsagDatamat, reach a sound judgment on what "suspicious transactions" are.

ElsagDatamat's proprietary powerful table driven structure adapts flexibly to customization and allows:
- ❖ to define the "sensitive events" to be submitted to the Monitoring engine on the basis of predefined parameters, that include those compliant with the regulatory agencies and internal policies;
- ❖ to define Parameters and Rules for the management of the different functions of the Solution

Once created, the AML Data Dictionary represents the tool to customize the data patrimony analyzed and customize the rules generating suspicious transactions

4.1.3. Operation Monitoring

This process, based on a monitoring engine, allows minimization of Money Laundering risks as the system is basically able to detect unusual patterns of transactions and trends indicating potential criminal activities.

It is highly flexible and manages, according to the international authorities requirements and to the rules configured in the system, the Suspicious Transactions Indicators related to the following issues:

- ❖ Cash and Other transactions
- ❖ Foreign Currencies Transactions
- ❖ Dormant Accounts
- ❖ Bank Accounts
- ❖ Credit Activities
- ❖ Drafts
- ❖ Changes in Branch Transactions

4.1.4. Transaction Processing

This on-line set of functions allows a comprehensive management and processing of the banking and financial transactions, both on-line and batch, coming from the information system and selected on the basis of the parameters previously configured:

- ❖ Inquiry on Daily Transactions
- ❖ Inquiry on Suspicious Transactions
- ❖ Inquiry on the Historical Suspicious Transactions
- ❖ Suspicious Transaction Stand-Alone Data Entry
- ❖ Inquiry on the Global Customer Position
- ❖ Alert
- ❖ Watch list

Inquiry on Daily Transactions

Enquires about all the transactions uploaded in the daily transaction database on the basis of customizable selection criteria.

Inquiry on Suspicious Transactions

Enquires on Suspicious Transactions, be it a list or a single one, in the appropriate Database in order to analyze the results of the Operation Monitoring, on the basis of customizable selection criteria.

Interface with the KYC management allows to have the detailed list of the information related to the Suspicious customer and all the customers linked to him.

The Users authorized can:
- ❖ Perform a query on all the information related to the suspicious transaction;
- ❖ Add a note;

Update and/or Cancellation are logged in the Audit Trail Database.

Inquiry of the Historical Suspicious Transaction

All Suspicious Transactions are archived in the historical Database on the basis of Rules and Parameters configured.
The selection criteria and the data displayed are the same as queries about suspicious transactions.

Suspicious Transaction Stand-Alone Data Entry

Autonomous insertion of any kind of Suspicious activities and behavior, adding to those who are not automatically detected.
The Data-Entry function is compliant with the information foreseen in the international standard reports.

Alert

Manual identification of a suspicious transaction among those present in the DB and/or reporting to the authorities concerned.
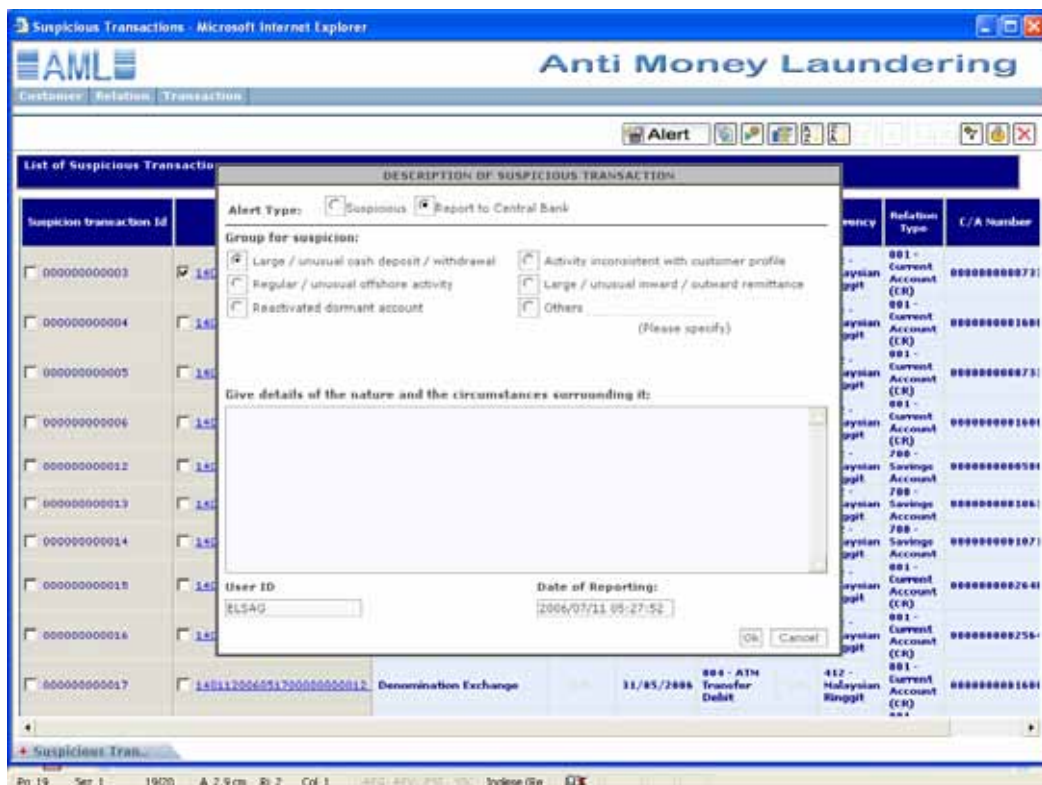
Reporting code transactions can be configured accordino to requirements.

Watch List

Creation of a proper list of customers to keep under control, where all the transactions, flagged as suspicious, reported and pending, present in the AML Customer Portfolio are

displayed. It allows also adding or removing customers/Customer codes and printing the list.

4.1.5. Reporting

This module allows the production of a STR with:

❖ XML File containing all the Suspicious transactions selected by the autorized Users;

❖ Excel, word, Acrobat file to be sent to the Central Bank by mail, email, fax or by hands;

Specific Suspicious transactions can be selected to be sent by email through an excel file to the Central Bank and to the Internal Management.

5. The Functional Flow and Logical Architecture

The Solution manages three main processes:
- ❖ Collection of daily transaction;
- ❖ Analysis of the suspicious transactions;
- ❖ Determination of transactions to be reported to the Internal & External Authority;
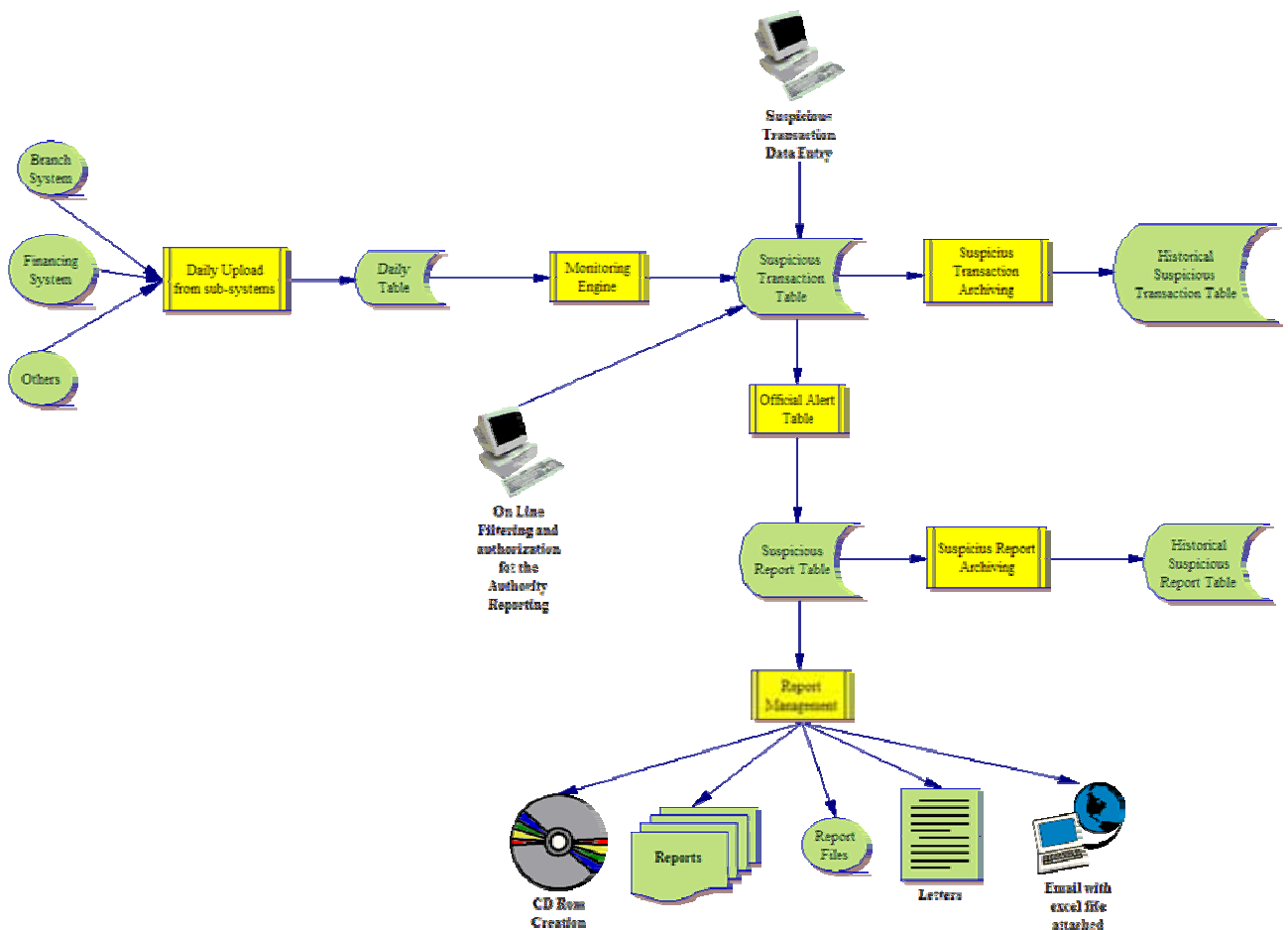
The first step is the collection of transactions from all the sub-systems connected. Every transaction is normalized to be uploaded into the Daily transaction table.

After that, the Monitoring Engine analyzes, according to the rules configured, the Daily transactions table to determine the suspicious transactions to be uploaded in the Suspicious Transaction Table. At the same time an alert is created through the Work-Flow Engine to be sent to the AML department or (in case of absence of a specific AML department) to the Users delegated to manage the AML Issues.

According to the alerts created, the User will be able to analyse all the Suspicious Transactions and decide which ones must be reported to the internal & External Authorities.

The last step of the process is managed through the engine that transfers all the Transaction to be reported into the Suspicious Report Table and through a subsequent step that creates the output of the solution.

Anti Money Laundering Architecture

This Architecture insures the following key features:

- ❖ easy maintenance, expandability, flexibility and encapsulation
- ❖ management of more presentation channels (multi-channels).
- ❖ sorting of the functions between the objects involved in the persistence and presentation of data, in order to minimize the coupling level between them.

❖ mapping of the standard application tasks (input, processing and output) on a graphic model that interfaces with the user within a multitier and Web-based enterprise dominium.
❖ separation of the application and its related responsibilities in three tiers (model, view and controller). Each tier relates to specific tasks and has specific responsibilities towards the other areas.
❖ Being the business logics separated from the data, it is easy to add or substitute a data source or to modify the data presentation format.

The MVC architecture allow the RBS System to be:

❖ **Open:** the standard technologies and protocols used guarantee the interoperability with the existing systems. Moreover, the system can be easily extendable with new functionality, should this be required.
❖ **Modular:** different components interact to provide the functionality required, but only the authorized ones are enabled and can run on different tiers. Various configurations can be made on the basis of the customer's requirements.
❖ **Secure:** the system environment is fully controlled through the use of certificates, SSL, HTTPS and digital signatures. A VPN can be used for the peripheral offices. The system can interface specific identity device controllers.
❖ **Scalable:** the application is distributed on more computers on the basis of the Bank's work load. A higher availability is achieved by using load-balancing techniques.
❖ **Reliable:** a high reliability is achieved by using clustering techniques.
❖ **Portable:** the application is independent from Hardware and Operating systems specific requirements.
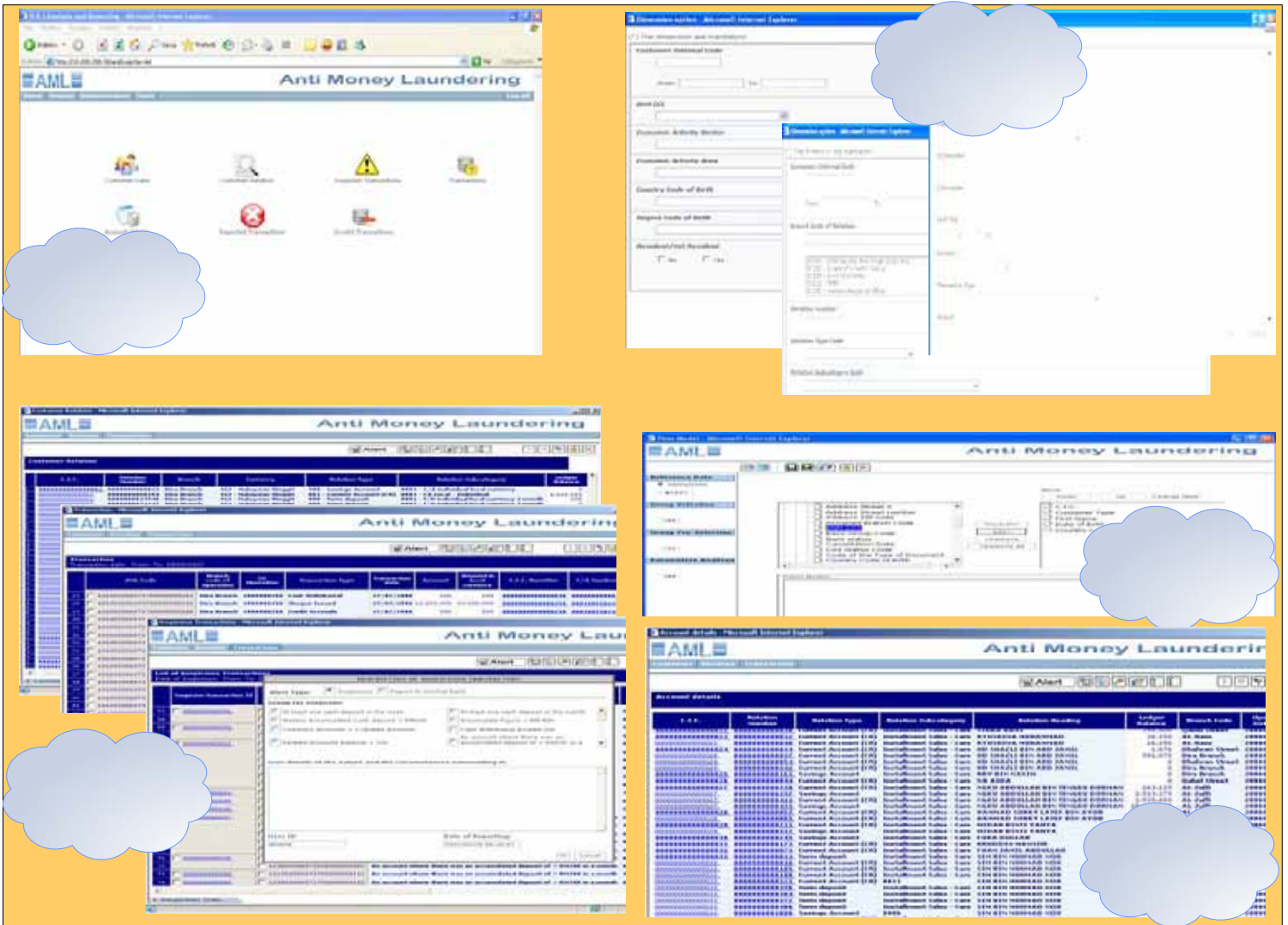
The Technology

Architecture

Elsag System is a Java Platform (J2EE Framework) System

The use of this platform makes the application completely independent from the hardware, the operating system, the database and the communication environment.

Reference	Suggested	Supported
Web Browser	Internet Explorer	Netscape
Web Server	Apache HTTP Server	IIS
Servlet Container	IBM WebSphere	Tomcat, JBoss, Sun One, Web Logic…
EJB Container	IBM WebSphere	JBoss, Sun One, Bea Web Logic
Message Server	IBM MQ Series	Oracle AQ
Operating System	IBM AIX – MS Windows Server	Linux, Unix, HP/UX, **AS400**, MVS
Data Base Engine	IBM DB2	Oracle, SQL Server

All the system software components are scalable on different Software and Hardware platforms as well as on any future release.

6. Screen Shoot

Home select function