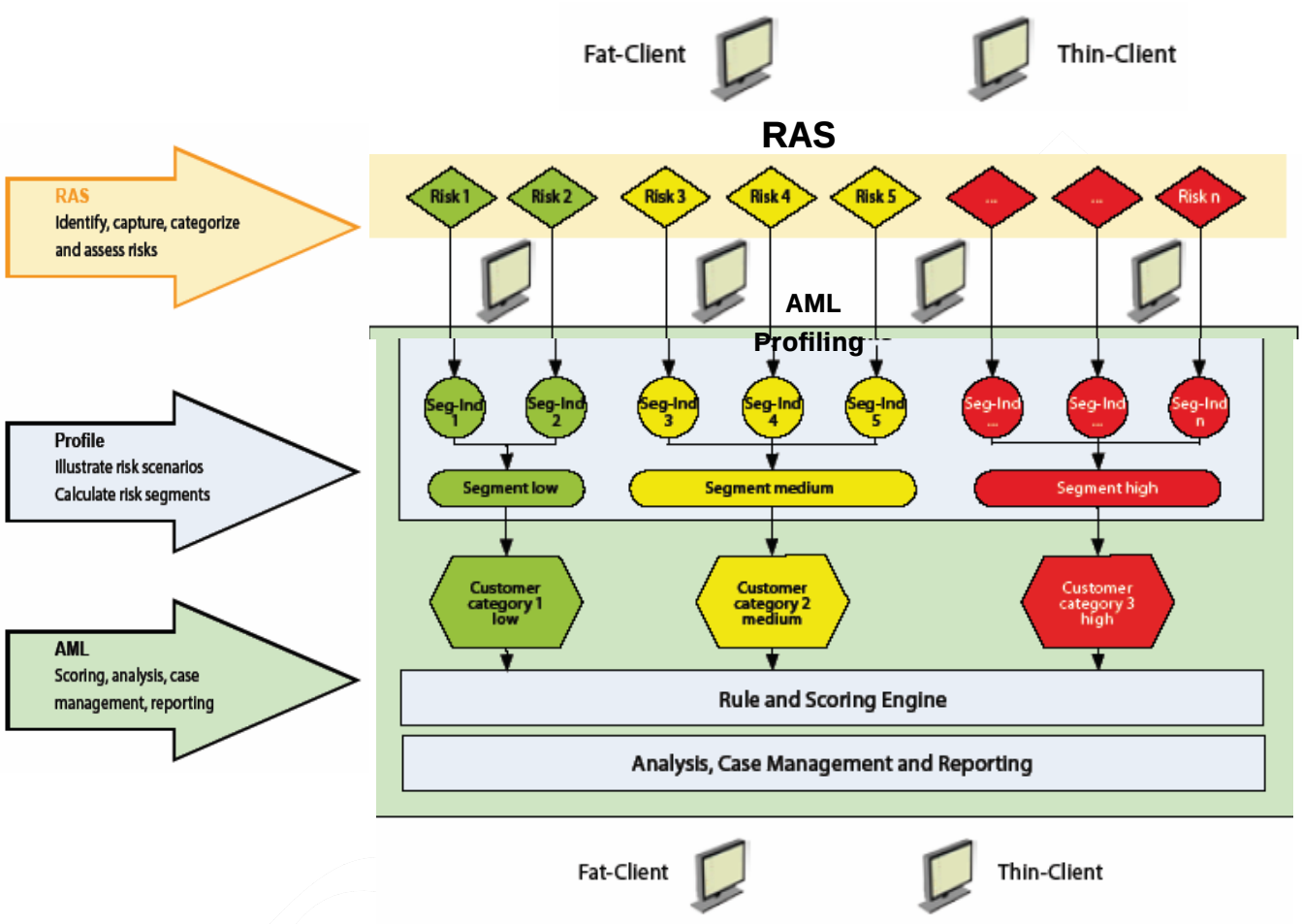
TOR (Terms of Reference)

for AML/CFT Solution

Basic Requirements

To ensure best possible fit and flexibility to Uzbekistan system relevant parties and organizations, the software is recommended to be modular and separated into different "Building-Blocks" / Modules.



The modularity is also motivated by the situation, that some organizations, who might have some "fragments" of an entirely required and FATF compliant solution in place, prefer to acquire only completing module to integrate into installed base.

So as much as techn. and economically reasonable and possible installed base shall be protected.

In general the overall recommended solution, compliant to, auditable by the international FATF40 + 9 recommendations should consist of following functional modules.

A. Risk assessment

B. New customer acceptance (KYC)

C. Module for the prevention and detection of money-laundering activities

D. Module for Customer Risk Rating and Dynamic Segmentation

E. Module for the real-time filtering of transactions and customers through sanction lists (e.g. OFAC, EU, etc.)

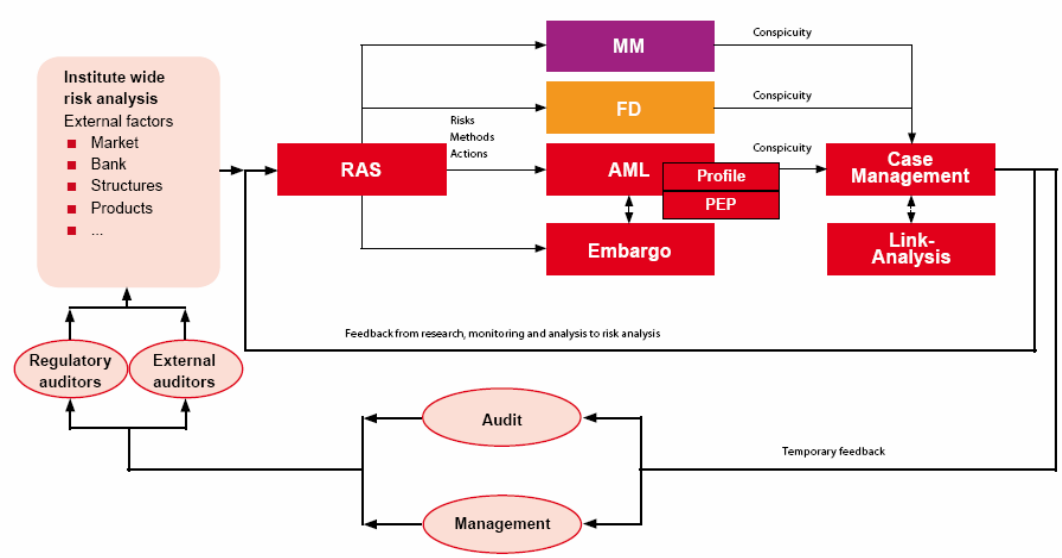
F. Pilot dashboard for analysis and review overall group wide risk situation

A. Risk assessment

A database supported "Risk-Assessment System" shall help users to organize, administer and manage their institution specific compliance and financial crime risks.

The work process embedded in this Module should ensures that all risks relating to money laundering, financing of terrorism and financial fraud are identified, described and evaluated.

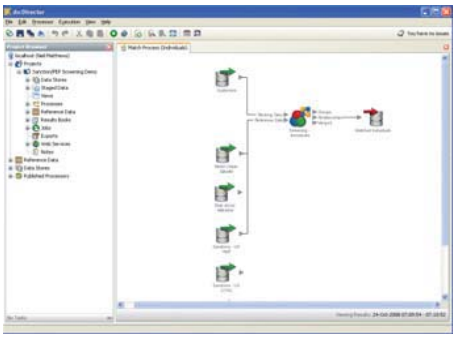
The risk assessment should deliver a quantified assessment of compliance risk, based on screening a sample of an organization's customer database.
The auditors use such a compliance screening software / module and their preferred Sanctions & PEP Screening list.



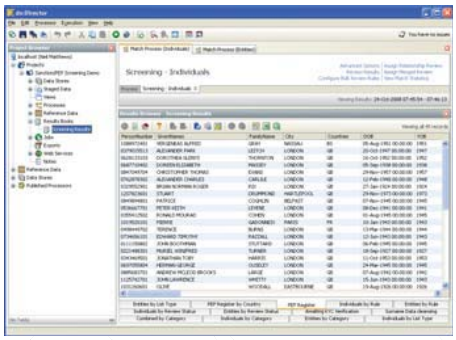
The Risk assessment should deliver:

- a report stating the number of Politically Exposed Persons (PEPs), financial criminals, other criminals, terrorists, disqualified directors etc in the sample and

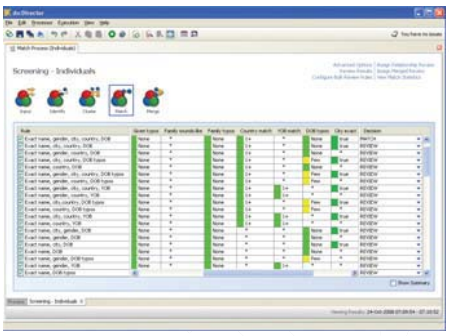
- statistical projections of the user possible overall exposure;
- full Sanctions & PEP Screening list profiled for selected matches;
- a complete list of users customer matches with the screening list profile ID which enables the user to conduct further investigative checks;
- a presentation of the findings of the risk assessment,
- hard copies of the documentation: - Risk Audit report,
  - selected screening list
  - customer profiles



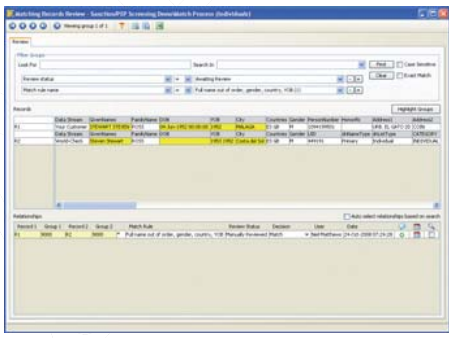
Configuring the process



The screening results browser



Refining the rules



Match results and definitions

These findings form the basis for the individual IT research targets of any institution.

Key Features of Risk analyses that should be covered are:

- General description of the approach to identify, categorize and evaluate risks
- Acquisition of organizational-, product and customer structure of the institute
- Assignment of the products, customers, transactions, access to different input channels and structures as well as processes per business unit
- Centralized description and centralized /decentralized validation of identified risks per organizational unit, product and customer group
- Analysis of the threat index per organizational unit, customer group and product (group)
- Description of the measures concerning risk management. Transfer of the identified risks into the IT-based AML research system / Module (If available)
- Permanent logging of all entries within the system assures that internal and external auditors are able to relate to the progression of the threat analysis

B. New customer acceptance (KYC)

This module should support comprehensive Know Your Customer (KYC) enhanced due diligence with the customer documentation and verification control.
The solution's flexibility should allow the user/Client organization to fully integrate all of their own policies, and procedures including checking of related persons and entities as well as re-documentation policies.
In one view, the module should presents all the vital data the client organization need to ensure their standards are being enforced.

With U.S. and international policy-makers – such as the Financial Action Task Force (FATF) and the European Union – imposing tougher know-your- customer (KYC) standards for banks they have become increasingly important to the prevention of identity-theft fraud, money laundering and terrorist financing.

One aspect of KYC is verifying that the customers are not on any list of known fraudsters, terrorists or money launderers, such as the Office of Foreign Assets Controls, United Nations or European Union lists.
Beyond name matching, a key aspect of KYC is to profile the risk of (potential) new clients before giving them access to the financial organization's resources. By focusing account-monitoring activities on clients with a high-risk profile, organizations can reduce the overall burden and expensive investigation resources can be allocated more effectively, limiting false positives and increasing the rate of investigative success. Furthermore, KYC enables financial institutions to fight financial crime while having minimum impact on customers whose business transactions and intentions are 100% legitimate.

C. Module for the prevention and detection of money-laundering activities

The overall technological AML approaches should be based on a solution that should supports money-laundering officers/compliance officers in monitoring all clients and their transactions.

The combination of pattern recognition, time series, cluster and link analysis, as well as text and data mining, forms the basis for the effective tracking of money laundering.
The solution should further then provides sound evidence of why certain behaviors are identified as being conspicuous and should give a complete overview of customer behaviors and supplies the user with all necessary customer, customer group, account and transaction information.
Known money laundering typologies and new patterns needs to be recognized by the system, using mathematical and statistical methods creating a dynamic profile for every customer and every customer group to track customer and customer group behavior over time.

Changes in customer behavior and deviations from group behavior need to be detected immediately by the system by means of these adaptive client profiles, and presented to money-laundering officers as potential risks.
External data (e.g., sanctions lists from the EU, OFAC or PEP databases) are used to be integrated into the AML process.

All clients and transactions shall be checked against these lists, and in the event of any match, these are then displayed in the system as being conspicuous. Along with the mathematical-statistical analysis process, money-laundering officers can set individual criteria and typologies in the system to identify possible money-laundering scenarios.

Clients and transactions needs to be checked against these criteria and typologies and displayed in the system as being conspicuous in the event of a match or suspicion of money laundering.

All system settings, typology definitions, etc., needs to be carried out by the money laundering officer.
Conspicuous events identified by the AML solution should be possible to be displayed with all other details online for the money-laundering officer to access. The entire data collection procedure, and the measures taken thereafter, needs to be documented in full by the AML Solution
This workflow, and the tamper-proof logging process, should allow individual steps, both in processing and monitoring, to be viewed at any time.
The comprehensive reporting shall supports the money-laundering officer in the periodic and historical reporting process, as well as in creating suspicion alerts and preparing change reports. Reports in which individual cases are detailed, or the results of a period of time are illustrated in summary and by means of an index, should be possible to be adapted and accessed individually

D Customer risk rating + dynamical. Segmentation

Modules for "Profile" analyses makes it possible to build up behavior based client groups – referred to as Peer Groups – which are dynamically formed, on the basis of the clients´ transaction behavior.
In this process clients with similar patterns of behavior are each allocated to one peer group or to one risk class respectively. Adaptive profiles are formed for clients and peer groups, which describe the behavior of the individual client and of the peer group to which he/she belongs.
The comparison of client profiles and peer group profiles provides early, revealing indications of significant changes in behavior and thus of possible cases of money laundering.

Anti-money laundering and terrorist financing solution modules and functions as well as Software solutions for Fraud detection usually use client groups, based on core data and characteristics.

In this respect such "Profiler Modules" extends the research systems, to include dynamic, risk-oriented formation of client groups.
These peer groups are characterized by a high degree of reliability, because the group to which a client belongs is determined by the "hard facts" of transaction behavior, rather than the "soft factors" of "Cozy data" and core data. With the comparative consideration of the adaptive profiles, changes in clients´ behavior (and potential instances of money laundering associated with them) are recognized early.

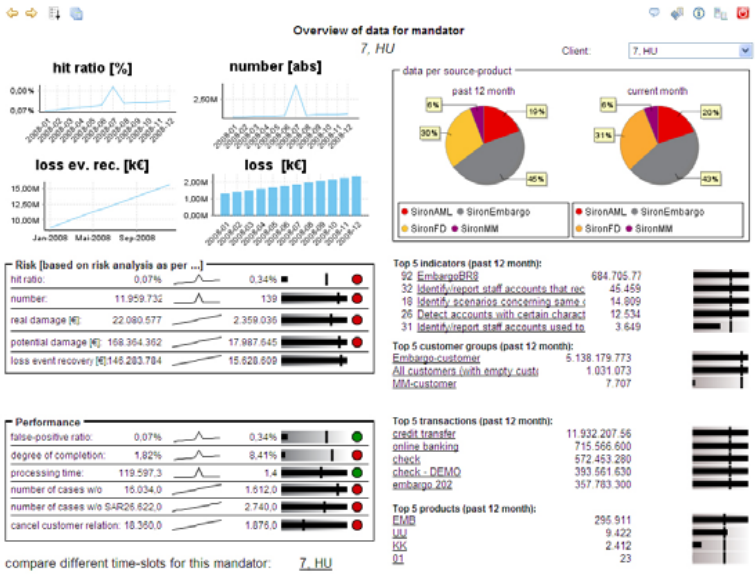
E. Module for the real-time filtering of transactions and customers through sanction lists (e.g. OFAC, EU, etc.)

Real-time monitoring of all client relationships to ensure compliance with regulations, regarding sanctions and embargos is covered by "real-time filtering module.
The legislative authorities have obliged credit institutions, in national and international laws and directives, to introduce "appropriate business-related and client-related security systems to combat money laundering, the financing of terrorism and activities based on fraud..." and also to investigate conspicuous transactions.
With the implementation of the regulations according to the Law on Central Bank of Uzbekistan (The Bulletin of the Oliy Majlis of Uzbekistan, #12, 1995, p. 247), Law on Banks and Banking (The Bulletin of the Oliy Majlis of Uzbekistan 1996, #5-6, p. 54), Banking Secrets (The Bulletin of the Oliy Majlis of Uzbekistan, 2003, #9-10, Article 54), Banking Regulations (The Bulletin of the Oliy Majlis of Uzbekistan, 2003, #9-10, p. 144) and based on the Law on Combating Money Laundering and Terrorist Financing (The Bulletin of the Oliy Majlis of Uzbekistan, 2004, #9, p. 160) for commercial banks to combat money laundering and terrorist financing., the objective is to prevent the financing, planning and carrying out of acts of terror.
Sanctions are directed against persons, groups and organizations. Sanctions lists are published by i.e. the EU, OFAC, Bank of England amongst others, and are of a mandatory nature. It should be ensured that the persons, groups and organizations, subject to the sanction, do not have funds and economic resources placed at their disposal, either directly or indirectly.
Module or sometimes also called the "Agent" ensures, by means of the continuous monitoring of clients/suppliers and of the payment transactions, with respect to the sanctions lists, that business relationships with sanctioned persons and payments from and to this circle of individuals are recognized in time and stopped.
The Software / Agent for Embargo monitoring should definitely fulfill the legal requirements for the identification of persons and organizations who are subject to international sanctions.

F. Pilot dashboard for analysis and review overall group wide risk situation

A clear view of the corporate realities can become clouded by poor visualization of performance indicators. Many of fashionable dashboards bear the risk to misled decision makers / compliance officers:
- colors and contrasts can steer managers' attention to the unimportant,
- lose themselves in details,
- create false connections
and
- use quite confusing presentation formats.

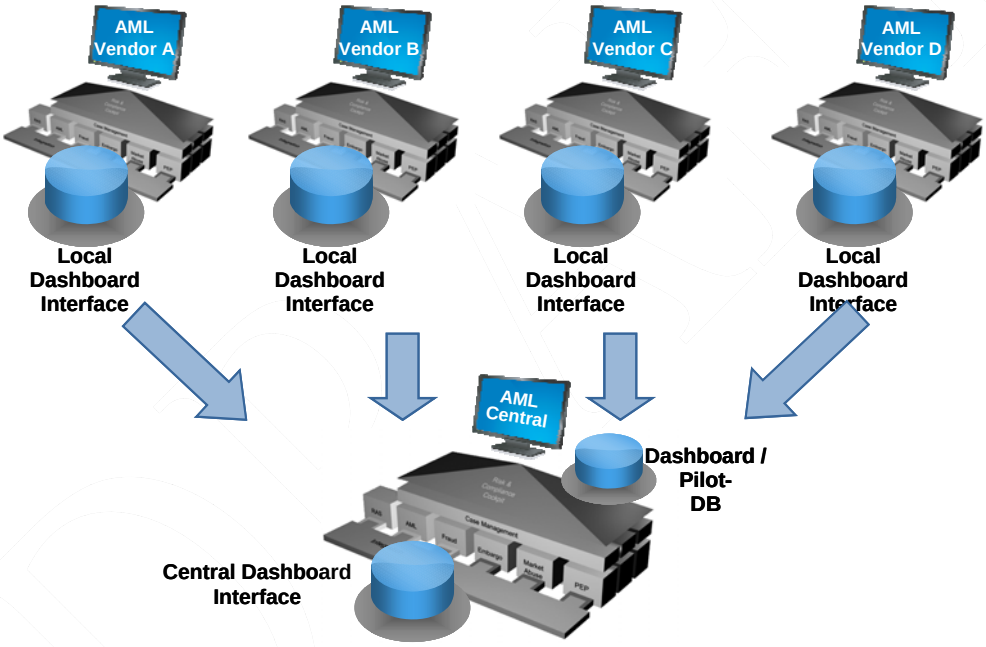
A useful and state of the art pilot or dashboard module / tool Solutions should build bridges between the complexity of real systems and the information-processing processes of the human brain.
Complexity and dynamics should become manageable using the correct performance indicators at the right time and in the correct presentation form.
Further this parameters should be adoptable by Bank / organization own trained IT-Staff rather than to call-in always vendor specialists.


Overview of data for mandator
7, HU
Client:
7, HU
hit ratio [%]
number [abs]
loss ev. rec. [k€]
loss [k€]
data per source-product
past 12 month
current month
SironAML SironEmbargo
SironFD SironMM
Risk [based on risk analysis as per ...]
hit ratio: 0,07% 0,34%
number: 11.959.732 139
real damage [€]: 22.080.577 2.359.036
potential damage [€]: 168.364.362 17.987.645
loss event recovery [€]: 146.283.784 15.628.609
Top 5 indicators (past 12 month):
92 EmbargoBR8 684.705,77
32 Identify/report staff accounts that rec 45.459
18 Identify scenarios concerning same c 14.809
26 Detect accounts with certain charact 12.534
31 Identify/report staff accounts used to 3.649
Top 5 customer groups (past 12 month):
Embargo-customer 5.138.179.773
All customers (with empty custo 1.031.073
MM-customer 7.707
Performance
false-positive ratio: 0,07% 0,34%
degree of completion: 1,82% 8,41%
processing time: 119.597,3 1,4
number of cases w/o 15.034,0 1.512,0
number of cases w/o SAR26.622,0 2.740,0
cancel customer relation: 18.360,0 1.876,0
Top 5 transactions (past 12 month):
credit transfer 11.932.207,56
online banking 715.566,600
check 572.463,280
check - DEMO 393.561,630
embargo 202 357.783,300
Top 5 products (past 12 month):
EMB 295.911
UU 9.422
KK 2.412
01 23
compare different time-slots for this mandator: 7, HU

In the current economic climate, in which financial organizations lack the budget for large-scale technology replacement, the emergence of agnostic technology platforms, able to consolidate information drawn from the numerous detection systems already in place, provides a means to leverage, rather than abandon, existing technology investment.

In this respect many banks that are now in the critical implementation stages of their AML projects has among others one main concern.
This is the challenges of accessing data from multiply sources, integrating multiple AML & compliance systems, core IT infrastructure and group level data aggregation & reporting.

Considering the economic rewards, financial organizations must address these issues, consistent and credible.
Such an integration and aggregation of installed base as well as new AML solution module should be possible to fit under one umbrella / dashboard to realize as much as possible and as less as reasonable data consolidation to manage the organization wide entire AML/CFT solution.
This could help to increase efficiency while protecting reasonable installed based and still staying in line with regulator conform / compliant management and compliance offers information.



III.3 Full Functional Specifications focuses on the individual modules that together make up the integrated AML/CFT system.

1. System Architecture

1.1 System Information Architecture

The solution needs to offer:

Functional:

- Multi-Client Capability (Multi-Company Capable) including Capability to Separate, Confidentiality, Controllability of Processes
- General Customization (possibility for customer(s) to adapt the software to individual necessities, such as company policies etc.)
- Multi-Language Capability
- a coherent business architecture model (data function/process, workflow or object)
- a possibility for the customer to adapt the software to individual necessities
- a documented functional model
- the basic system on a client server architecture
- a SW-Design/Architecture document
- Exchangeability of modules with different release levels
- Multi currency support
- Multi user support / flexible user authorization
- High flexibility / ability to parameterize without the support of the vendor

Technical:

- Scalability
- Modular system design
- Audit security (including dual control and audit trail)
- Availability under any platform (OS / DBMS)
- Support secure connections (e.g. https, SSL)

1.2 Programming Language

- Based on Java
- Programming language: 4 GL

1.3 Web-Technology

- Compliant solution to established standards in the field of Web-Technology (e.g. J2 EE Version 1.3 Servlet API Version 2.3, JavaServer Pages Version 1.2, Java Development Kit (JDK) 1.3

1.4 Modularity (2nd dimension of modularity)

The solution has to

- be built (technically) in a modular way (i.e. presentation, business layer, data access)

- be built (functionally) in a modular way in line with recommended Building Blocks listed under item III.2
- provide the possibility for a physical installation of only selected modules
- provide the possibility to add further modules

1.5 Workflow & Collaboration

- Workflow support – The workflow has to support by various possibilities to generate mails (automatically and manually triggered)
- Workflow definition – Possibility to define different workflows based on transactional/customer data checking results – adoption of workflow to banks standards and structure
- Collaboration of users – multi log-in support

1.6 Interfaces

The Solution needs to offer in general open interfaces to:

- a Message Based Interface support (e.g. MQ-Series)
- a flexible Interface Message Generator
- Web Services for connection to other systems
- the availability from core system to other applications
- standard interface to commonly used ERP-Systems (e.g. SAP, Peoplesoft, etc.)
- connectivity to commonly used BI-tools (e.g. Cognos, Business Objects, etc.)
- an interface to MS Office (MS Excel, MS Word, …)
- an interface to and from Unicenter / Service desk
- connection to single sign on (e.g. LDAP, Active Directory)

In particular following should be realized and included:

Graphical User Interface:

- Standardized screen layout
- Standardized user interface
- Standardized user interface
- Menu adjustment by user and user group
- Drill down capability support by user interface
- Capability to display the bank logo on the screen
- Allowing high productivity

User Interface – Multilingual:

- Availability of Russian user interface (Uzbek Language Interface – optional)
- Availability of English user interface
- Possibility to switch the user interface language from Russian (Uzbek) to English
- Possibility to add additional languages

User Interface – Validation:

- Plausibility/Consistency Check (checks for inconsistent and non-plausible data)
- Checks for data completeness (e.g. mandatory data fields)
- Standard user interface
- Flexibility of user interface (generic) without support of vendor

1.7 Print Functions

- Support of all workstations and PC print software
- Print screen function
- Availability of Cut and Paste function
- Definition of automatic print out (daily, weekends, holidays, weekly, monthly, etc.)
- Possibility to print all generated analyses and reports
- Print to PDF feature

1.8 Specific Function Requirements

- Possibility to screen XML
- automatic update of suspicious lists
- Support of batch and online operational modes
- Providing of multi-currency support
- Interfacing with a generic case management
- Seamless integration of filtering and AML on one platform

2. Data Architecture

2.1 Data Storage

- Support of all industry and standard databases (DB/2, Oracle, SQL-Server)
- Database designed on a relational schema
- Storing of all data records in the database
- Database designed on an oriented schema
- Guaranteeing of data integrity in a distributed environment
- Providing of roll forward/rollback mechanisms to ensure database integrity
- Including data management environment to enable optimum database performance
- Enforcing of referential integrity on database level
- Supporting of database reorganization without interruption of service
- Supporting of decentralized storage
- Providing a detailed logical data model
- Providing a detailed physical data model
- Possibility to add data fields and other sources of information
- Possibility to manage data older than 3 years

- Automatic data import directly from the transaction processing systems (DP - domestic payments/ CBP - cross boarder payments) – on a current-real time basis
- Possibility to exclude specified transaction types from monitoring in general

2.2 Report Generator

- Possibility to include external data bases into reports
- Possibility to set up freely user-defined (ad-hoc) reports
- Possibility to use all data fields of the entire system without any restrictions
- Performing of basic mathematic calculations
- Execution of reports at the client or at the server
- Possibility of graphical presentations
- Possibility to export the reports and graphical presentations into common MS Office applications
- Possibility to create combined fields

2.3 Reports – Multilingual

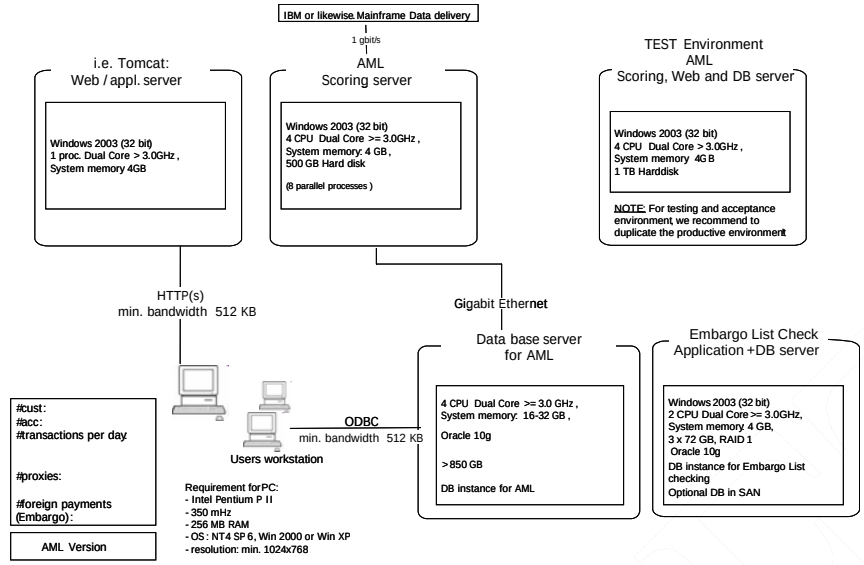
- Producing internal reports in English and Russian language (Uzbek Language – optional)
- Possibility to add additional languages without limitations
- Supporting of multiple character sets within one installation
- Support of UNICODE character sets
- Supporting of all European character sets
- Supporting of Japanese character sets

2.4 Standard Reports / Report Generation

- Possibility to provide historic and current case and decision reports
- Possibility to customize the layout of standard reports
- Possibility to include user defined field into standard reports
- Possibility to run standard reports with user defined sorting criteria
- user-defined adaptations of standard reports have to be saved and restored
- Possibility to produce reports at any time
- Possibility to predefine day, hour and minute to run a report
- all report results be provided both as a print-out as well as on-line
- Support of multi-dimensional reports

3. Technical Systems Architecture

3.1 Technical Systems Architecture



Example configuration

3.2 System Platform

- Solution has to run on open platform (server)
- Client has to run on an industry standard platform

3.3 Server Platform

- Possibility to port the system to different OS/Hardware Platforms
- Aligning with 3-tier environment
- The solution has to run on load sharing clusters

3.4 Client Platform

- Support of an installation without administrator privileges
- Support of an operation without administration privileges
- Possibility to use application from central installations (Citrix, Terminal-Server, etc.)

3.5 Connectivity

- Supporting of platform-independent database connectors like JDBC

3.6 Middleware

- XML Based

3.7 Network Equipment

- Support of HTTP or HTTP/s network protocols

4. System Integration

4.1 Implementation Planning

As far as integration of an AML/CFT solution is not just like easy and isolated Office application and even so independent of the fact if it is a green-field or a solution enlargement implementation several steps should be done in proper way.

A proven methodology contains six main phases:

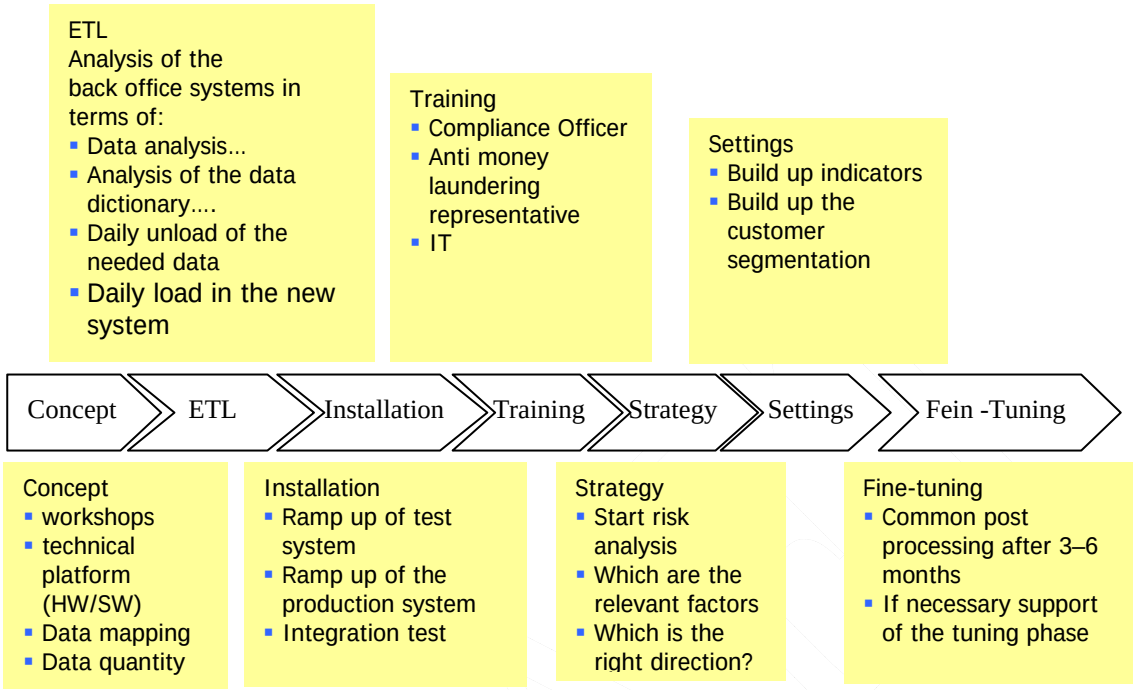
a) business analysis,
b) data & hardware,
c) installation,
d) configuration,
e) run & accept
and
f) deployment.

In the analysis phase, an assessment of the business alerts required (based on a best practices risk library) is documented in a requirement workshop.

In the analysis phase the data requirements required for the AML solution and the sizing of the servers are calculated.
The data/hardware/installation phases are used for installation and data verification delivered by the organization / financial institution.
The configuration phase is the definition and configuration of the system based on the results of the requirement workshop according to user requirements at the customer's environment.
Finally the acceptance and deployment of the solution takes place when daily feeds are loaded into the system and are fine tuned according to the user requirements.

Each phase throughout the project focuses on delivering deliverables for which the customer/organization is normally required by the system integrator to sign off, although known as acceptance milestones.
This method ensures next steps can be taken having joint acceptance by both parties before proceeding with subsequent steps.
The approach is phased and quickly identifies potential bottlenecks/issues (if any) between customer and vendor /system integrator.
This in turn keeps a project focused and allows for a fast and efficient implementation.

A recommended implementations team structure can consist of two or three consultants in four roles (one project manager, one business analyst, one implementation consultant and one trainee) to deliver the following deliverables by means of these activities/phases:



4.2 Data Migration and Test methodology and tools

- Table orientated data set up

1)	**Project management**	
2)	**Technical kick off / definition of project**	Definition project team / responsibilities
		Architecture (Hardware and Software), scenarios
		Sizing
		Architecture of interface to Siron®AML
		Definition milestones and deliverables (customer), scheduling
3)	**Milestone: Project plan accepted (incl. delivery dates)**	
4)	**Milestone: Hardware available (prod env). OS, DBMS provided by bank**	
5)	**Installation Basic System & Integration (productive environment)**	Server
		Data base server
		Clients
		Integration MS Office
		technical acceptance

6)	**MileStone: technical acceptance**	
7)	**Training**	Training preparation: adjustment to customer specific environment
		Administration (IT) / technical
		Users
8)	**Issue of threat analysis (Risk-Analyses Software)**	Settings
		Users
		Base Data
		- Category of risks
		- Characteristics
		- Measures
		- define organizational units and bus. Areas
		Risk factors
		Central Assessment
		Decentralized Assessment
		Define reporting (Hazard study)
9)	**Go live**	
		Editing of a customer specific operational manual
		Support on start of production
		Implementation & Acceptance protocol
10)	**Milestone: Acceptance of Implementation**	
11)	**Optional services**	Definition of backup system
		Connection to other implemented AML modules, Software tools and to the overall AML system Software

5. Systems Operations

5.1 Availability

- Default system availability - 7 days a week 24 hours a day

5.2 Scalability

- Full scalability of all components
- The system must be scalable by a minimum of 100% concerning the following items: retail accounts, retail customers, international accounts, international customers, average transaction per day and max. transaction day within 12 months.

5.3 Performance

- Measure and report in elapsed time
- Providing a performance management-tuning

5.4 Archiving

- Possibility to store all alerts in an archive
- Possibility to archive old cases (older than 6 years can be archive by data base mechanisms)
- access to archived data for end-users

5.5 Data Backup

- Automatic and regular data back-up mechanism
- Partial and full back-up manage
- Possibility for online back-up during system operation

5.6 Remote Operating

- Support of remote operating

5.7 Disaster Tolerance

- The solution requires continuous availability. The bank operates a two data center model for core systems with either live/live or live/standby mode depending on system requirements defined elsewhere in this document. The proposal must illustrate in words and diagrams how the solution design provides continuous availability for the system, its management facilities and any subsystems (for example databases) required for operation. The solution must be able to activate the continuous availability proposition without requiring the invocation of manual data recovery procedures

6. Security

6.1 Authentication & Authorization

- Support of single-sign-on (SSO) e.g. LDAP, ActiveDirectory
- Support of integration into a central authorization system
- Support of an authorization concept that ensures that users can only access those data that they have to access according to a need-to-know principle (authorization, granular rights administration)
- Authorization on a users level
- Authorization via role concept

6.2 Confidentiality

- Passwords and sensible system data have to stored and transmitted in an encrypted way
- Support of encryption for data transmission
- The solution must provide the total segregation and full confidentiality of data for each bank and it has to include the necessary facilities to prevent any unauthorized personnel from accessing information of another bank / unit.

- Flexible definition of password rules
  - Min. password length
  - Min number ob capitals
  - Min number of small letters
  - Min number of special characters
  - Min number of digits
  - Number of retries before blocking a customer
  - Max password validity period
  - Min number of password cycles

6.3 Traceability

- Support the logging of reading and writing accesses in order to provide a traceability of all system-/data changes
- Possibility for the integration into a central logging system (-> output of all writing accesses (= security class 2) via XML)
- Audit trail(s) are highly recommended to express high accountability to those FATF auditors who will finally proceed the real audit but also to prevent for unexpected surprise for the implementation team and management.

  A clear audit trail that highlights the date/person making amendments and where possible/ practical - the actual amendment. It's not recommended to assume that the audit trail is good until considered sensitive activities are tested. - Remember that good input leads to good output. It's easy for users to criticize a vendors product but if the necessary "KYC-data" is not of quality (missing, incomplete, incorrect, fragmented) or is not properly interfaced with the AML/CFT solution, the output will fall short of user expectations.

6.4 Other Security Requirements

- Availability of a security concept for the product

7. Documentation

7.1 User Manual

- User manual in English and Russian language (Uzbek optional)
- Context sensitive online help (number of pages)
- documentation available on paper or electronically (CD)
- immediately updated documentation after release-change

7.2 Online Documentation

- Online help in English and Russian language (Uzbek optional) (number of pages)
- Configuration guide to describe business configuration of implementation (number of pages)
- technical documentation that explains interfaces and the technical structure of the system in English and Russian language (Uzbek optional)
- operations manual in English and Russian language (Uzbek optional)

- implementation guide to describe technical aspects of implementation (number of pages)
- full description of all error situations and clearance
- full description of restarting
- full workflow description

8. Vendor Assessment

8.1 Product Strategy

- source code available via escrow agreement
- Two releases in one calendar year
- Guaranteeing of historical data adoption /upward compatibility
- Project support offered by vendor
- Standardized Implementation process offered by vendor
- System training offered by vendor
- Specialists support offered by vendor (onsite / offsite)
- Technical support offered by vendor (SLA)
- First level support (local in Uzbekistan)
- Second level support ...
- Roadmap
- Coverage of all aspects of financial crime

9. Monitoring Scope

The solution has to:

- screen all transactions of a client from all core banking systems
- generate a long-term profile for each customer / account. Profile definition can be adapted to banks requirements and legal requirements.
- cover all requirements of the new regulation in Uzbekistan regarding anti money laundering and terrorism financing. Especially the risk based approach is covered by a wide set of statistical functions for a dynamic profiling and time line analysis.
- handle high volumes of data from different platforms. Some clients need to cover more than 100 mio. transactions a day (inwards/outwards swift, transfers, deposits/withdrawals, purchases/sales, others)

10. Administration functions

10.1 Multi-organization and international solution

The solution has to support:

- multi client capability, multi country capability, multi currency capability, multi language capability and multi user capability.
- Show reference customers for each aspect

10.2 Access Control

- The solution has to support a strict separation of data per institute as well as a across client view on data (super-user). Give examples, references, detail information, certification is recommended by at least one of the leading Auditors (PWC, KPMG,...)
- Each user is assigned to one client (institute, mandatory) and only views data of his client. Only a "super-user" is allowed to view data across clients.
- In addition within one institute for each user and component, access rights can be defined (read, write, delete, check).
- In addition to this for each user limitation to data can be individually defined (e.g. User A is not allowed to view employee data, User B is allowed)
- Access control within case management: possibility to delegate cases to other teams/users...
- Adoption to banks structure, flexibility...

10.3 Profiling, Parameterization & Monitoring Rules

10.3.1 Profiling & Risk rating

- Easy to use dialog for creating/changing complex rules
- The solution has to provide static and dynamic profiles
- Static profiles: build on base of all available customers standing data (branch, name, nationality, age, DOB, profession, addresses, ...)
- Dynamic profiles: based on all available transactional and statistical data (behavior of the customer or his peer group). Examples: sum, number, min, max, avg, sdv for each transaction type...
- Automatic creation of statistical data for each account per month. These data have to contain more than 60 statistical key figures, which are base for dynamic profiles and indicators.
- Possibility of segmenting customers into multidimensional peer groups and sub groups based on:
  - Demographic / static data
  - Behavioral data

- Statistical data
- Transactions Value
- Transactions Velocity
- Volume of transactions.

- Possibility to take over the screening results from embargo screening – especially for the customers data
- Possibility to use bank-defined risk modeling & assessment logics for the customer risk rating (e.g. based on customers data, product usage, transactions and profiles)

10.3.2 Parameterization & Monitoring Rules

- possibility to exclude certain products (data type) from monitoring in general
- Possibility to use watch lists from the sanction list-checking module for AML monitoring (without double load and maintenance. Example: an account for which a transaction produces a sanction list match, has formerly been involved in a money laundering or a fraud case)
- possibility to assign a risk category to the watch lists
- Possibility to define white customer lists
- Possibility to organize the white listing per data field and per detection scenario
- Possibility to create different types of rules and monitoring strategies for different types of transactions and customers/groups of customers
- Possibility to use all transactions of all accounts for an analysis via an amount-threshold / sum-threshold value and freely defined transaction types as well as currencies that can be set manually

10.3.3 Monitoring Process

- Flexibility to define account type & customer type specific (Saving account, Current account etc) defaults for mandatory & optional fields (besides the regulatory mandatory fields)
- Data interface can be extended by bank without need of the vendor
- Support of peer group analysis and a graphical link analysis
- The link analysis based on monitored transactions and the flow of transactions
- Possibility to focus on particular Correspondent relationships and the omission of others
- Possibility to identify group relationships (e.g. all directors of xyz ltd, or all companies with Mr. A B as shareholder or introducer)
- "fuzzy logic" match with the different watch lists

- support the monitoring of wire transfers, covering all parties involved in the transaction and providing the ability to conduct analysis of all parties
- possibility to monitor the relevant data on a weekly/monthly/quarterly basis
- possibility to perform what-if analysis (in order to proof the changes of new monitoring rules)
- possibility to filter all transactions for special beneficiaries for all accounts over a certain period of time
- possible to especially evaluate the following attributes: purpose of use, ordered, recipient, banks (ordering bank, recipient bank), detailed ordered description (address-name), SWIFT attributes incl. "raw entry data"

10.3.4 Reports and Statistics

- Possibility to set up and automatically run a report based on user-defined criteria
- Pre defined reports (number of report definitions)
- User defined reports possible (without IT knowledge)
- Possibility to produce ad hoc reports based on various (user defined and online changeable) parameters
- possibility to develop and store queries and report definitions
- possibility to add own customized reports in future without any programming effort by the vendor
- possibility to predefine the notification-letters (format & content) which can be created ad-hoc to be sent to the authorities
- possible to store all notifications which are created for the authorities within the system and in connection with the notified data (transactions, customer)
- Solution has to provide of the following analysis for support of detailed investigations of alerts:
  - Graphical trend analysis
  - Links maps / flow maps
  - Behavioral charts
  - Statistics on all aspects (alerts, reports, monitoring results,...)
- Possibility to evaluate volumes (create statistics) on daily / weekly / monthly / quarterly / yearly base

10.3.5 Manual Workflow/Case Management

- Possibility to display the following data fields of transactions and customer data sets:
  - Internal transaction code
  - Beneficiary / account with institution
  - Originator / ordering institution
  - Amount, currency
- Fraud: Possibility to assign alerts/cases (red flags) to departments, to users and/or to specific user profiles by system and manually
- AML: Possibility to assign alerts/cases (red flags) to customers and/or to specific customer profiles by system and manually

- Possibility to change the priority of an alert (case) or the risk score manually (overrule system-based priorities)
- Possibility to customize the alert/case workflow (review and approval process, definition of activities etc.)
- Possibility to monitor the progress of cases being investigated and track the activities
- The solution has to show all information connected to the alerts (detailed information, reason for the alert, scoring level/risk category)
- Implementation of drill down (from rough to detail) functionality
- Possibility to create open a new case manually by user (e.g. following an external request for information)
- Possibility to select all alerts by user comments entered manually in the online report (the user is able to select and print his comments by account, date and subject)
- Possibility to do an "age-wise" analysis and view lifecycle of alerts at a summary level e.g.: no. of days open, etc
- Possibility to show/see the alert history
- The system should have an effective way of notifying the user of new alerts
  - E-mail
  - popup windows
- Possibility to define and use text modules (predefined) for escalation notification
- a mechanism to receive email responses within the system and store them appropriately against each case automatically
- Support of due diligence process with user defined questionnaires
- Possibility to define and use text modules (predefined) for evaluation comments
- Possibility to add supporting documentation/images to the alert by the users
- The solution has to allow risk-weighting of alerts
- Possibility to combine the working instructions (based on the compliance manual) with the tool
- Possibility to attach documents (storage audit secure in database or file system)
- Possibility to generate SAR/STR (country specific)

10.3.6 Product Support

- The maintenance service includes 1st, 2nd and 3rd level Support. Based on the requirements of the client (small banks to large data center installations) some clients like to install an own 1st level support

10.3.7 Training

In accordance to and to be compliant to FATF 40 audits, Financial institutions should develop programmes against money laundering and terrorist financing.

As far as those programs should include also compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.

In this respect an ongoing employee-training program and an audit function to test the system, is required. By a comprehensive range of training, services shall be secured by practically oriented seminars for IT specialists and end users.

Trainers shall have a high degree of specialist knowledge as well as reasonable years of project experience so that they should employ practice-oriented methods to guide participants through the seminar topics and prepare them specifically for their future tasks.

Such trainings could be realized either by the vendor it self or by their qualified certified partners / System Integrators, in order to offer internationally active clients a comprehensive training portfolio on site and in the language of the respective country. All seminars should follow a modular structure in line with the overall modularity of the awarded solutions. (Introductory, advanced and revision courses) Refresher and news courses should be optional to provide those returning to training and anyone else interested the opportunity to receive a rapid introduction to a specific topic.

10.3.8 General overview about compatible and compliant Third-Party main Platforms, interfaces and Databases

Operating Systems Compatibility

- Windows
- All Unix
- Linux
- Sun Solaris
- IBM AIX

Databases Compatibility

- DB2
- SQL-Server
- Oracle
- MySQL
- Sybase
- VSAM
- Sesam
- Access

Web Server Compatibility

- IBM Websphere
- BEA Weblogic
- Apache Tomcat
- Oracle Application Server (OAS)

Interfaces Compatibility

- SAP (BCA, LM, DM)
- Temenos
- Kordoba
- I-flex
- Alldata
- Actis
- Prang
- Swift

IV. Organizational Impact and recommendations correspondent to AML / CFT Solution recommendations

IV.1 Mandate of internal control system of commercial banks is as follows:

- Effective detection and prevention of transactions involving funds or other assets with the purpose of money laundering and terrorist financing;
- Prevent deliberate or unintentional involvement of the commercial bank in the criminal activities, penetration of criminal capital into its authorized funds (capital), and criminals taking over management of the commercial bank;
- Ensure strict compliance with the requirements of legislation on countering money laundering and terrorist financing.

IV.2 Main objectives of the internal control system of commercial banks are as follows:

- Undertaking steps for adequate screening of clients according to the legislation, these Regulations, and internal documents;
- Identification and screening of client's real owners as well as taking justified and feasible actions to establish the sources of funds and other assets used in the transaction;
- Identification of questionable and suspicious transactions based on the criteria, determined in these regulations and internal records;
- Timely submission of documents about suspicious transactions identified in the course of internal control to the department;
- Suspension of transactions, which must be reported in particular cases except for transactions for depositing the funds wired to the account of a legal entity or an individual for three days from the date of the transaction, and inform the headquarters of the department about this transaction on the day of suspension;
- Maintain confidentiality of the data related to combating money laundering and terrorist financing;
- Promote storage of information on monetary or other transactions as well as identification data and materials for customer due diligence in the legally stipulated timeframe;
- Timely and systematic provision of reliable information and materials essential for making appropriate decisions to the management of a commercial bank;
- Forming a database of suspicious transactions completed or attempted, persons (management, founders, shareholders, members) related to the clients, who performed suspicious transactions and mutual exchange of this information with other commercial banks and government bodies according to the current legislation;
- Review of internal control system of other domestic and foreign banks in establishment of correspondent relations;
- Taking special measures particularly focusing on prevention of the risk of utilization of commercial banking services to commit offences, inter alia, related to money laundering and (or) terrorist financing, utilizing advanced technologies, which enhance the degree of anonymity;
- Identification of persons involved in terrorist financing based on queries in the client base.

IV.3 In order to achieve the goals and objectives of the internal control system, the Internal Control Service (responsible officer) performs the following functions:

- Taking measures stipulated in the legislation, these Regulations, and internal documents to prevent the risk of use of commercial bank services for offences including money laundering and/or terrorist financing;
- Monitoring compliance of commercial bank with requirements of current legislation and internal policies and procedures;
- Preparation and submission of proposals to the management in order to address identified flaws and violations in the activities of the commercial bank with regard to non-compliance with the domestic legislation and internal regulations;
- Monitoring of remedial actions to address the flaws and shortcomings in the organization and functioning of the internal control system found in the course of the audit by the authorized representatives of the Central Bank of Uzbekistan (hereinafter – Central Bank), staff of Internal audit service of the commercial bank, external auditors, and the officers of the Department;
- Interaction between the Central Bank and Department on organization of internal control, prevention and remediation of violations of legislation, these Regulations and internal documents.

IV.4 Based on the legislation and these Regulations, every commercial bank is required to develop a statute determining the mandate, rights, and responsibilities of the Internal Control Service, get it approved in the Board meeting and enact it.

This statute should contain the following data on the Internal control system:

- Its mission and objectives;
- Means to ensure its independence from other units of the commercial bank;
- Its relations with other units of the commercial bank and Internal audit service of the commercial bank;
- The right to obtain information essential for implementation of own functions as well as responsibilities of other units of the commercial banks to cooperate on provision of this information;
- Right to review potential violations of domestic legislation and internal policies of the commercial bank;
- Right to freely express and disclose the data received to the Chairman of the Board of the commercial bank, and if necessary, the Board of the Bank;
- Responsibility to submit appropriate report to the Board Chairman of the commercial bank;
- Responsibilities for counseling the Board of the commercial bank on the issues of compliance with the legislation and standards including information on the changes in this area; Recruitment requirements and procedures; Responsibilities for regular training at the special courses.

IV.5 Based on the requirements of these Regulations, commercial banks must annually develop and approve internal regulations, which should reflect:

- Regulations for customer due diligence including identification of clients and real owners of the clients and undertaking ongoing monitoring of client transactions;
- Procedures of processing essential information and ensure its confidentiality;

- Procedures for provision of information on the violations of legislation by the internal control service officers of to the manager of the Internal Control Service of the headquarters of the commercial bank (hereinafter – manager of the Internal Control Service);
- Qualifications-based requirements for training of human resources;
- Criteria for identification and signs of the questionable transactions;
- Measures for prevention of the abuse of advanced technologies for the purposes of money laundering and (or) terrorist financing, etc.
- Internal regulations are approved by the Board of the commercial bank.

IV.6 Internal control system of a commercial bank is organized with consideration of specific features of banking operations, its main activities, client base, and risks related to clients and transactions.

IV.7 The structure of commercial bank's internal control system including its branches is determined by the Board of the commercial bank and may be reviewed according to the recommendations of the Central Bank.

IV.8 Commercial bank's internal control service includes the internal control system of the headquarters of the commercial bank and internal control system or responsible officer at every branch of the commercial bank.

IV.9 The Internal control system shall be adequately staffed for effective performance and implementation of internal control objectives.

IV.10 Head and officers of the Internal Control Service shall be appointed by the order of the chairman of the board of a commercial bank.

Head of commercial bank's internal control system shall have university degree in business or law and management experience involving financial transactions of a unit of a commercial bank for at least three years.

Appointee for the position of an official, manager or officer of internal control service shall:

- Have knowledge of banking and financial legislation including regulatory documents of the Central Bank;
- Command the knowledge of accounting regulations and regularly undergo training courses at specialized courses.

IV.11 Following persons cannot be appointed as a manager or an officer of an internal control service:

- Those who demonstrated mismanagement of a unit or dishonest demeanor in their performance and personal behavior;
- Those previously prosecuted for economic offences.

IV.12 A commercial bank, 10 (ten) days after making a decision on establishment of an internal control system, appointment of the manager of internal control service, must inform the Central Bank accordingly attaching the personal data of the appointees.

IV.13 Manager and officers of internal control service are entitled to:

- Demand essential accounting and management records from the management and staff of the commercial bank's units for internal control purposes;
- Make copies of the documents received, receive copies of files and other records kept at electronic databases, local area networks, and off-grid computer systems of the commercial bank for internal control purposes;
- Request and receive the support from experts of other units of the commercial bank;
- Enter the premises of commercial bank's units and the premises used for storage of documents (archives), cash, and valuables (vaults), computer databases with written consent of the chairman of the board of commercial bank;
- With written consent of the chairman of the board or duly authorized deputy, order the management of the branches of commercial banks to suspend transactions related to terrorist financing;
- Submit proposals to the chairman of the board of commercial bank on further actions on client transactions including suspension of transactions to obtain additional information or verify existing information on the client or transaction according to the legislation;
- Perform other actions according to these Regulations and internal documents.

IV.14 The manager and officers of internal control service cannot sign or clear payment orders, loan and accounting records.

IV.15 In implementing their functions the manager and officers of internal control system must:

- Undertake all essential measures within their competence to achieve the goals and objectives mandated by these Regulations and internal policies;
- Ensure safekeeping and return of documents received from appropriate units of commercial bank;
- Ensure confidentiality of information received in undertaking own functions;
- Perform other duties according to these Regulations and internal documents of the commercial bank.

IV.16 The manager of internal control service shall report directly to the chairman of the board of commercial bank and shall be independent from other units of the commercial bank.

Officers of the internal control system shall report directly to the manager of internal control service.

IV.17 The staff of commercial bank units shall provide assistance to the internal control service in implementing their functions according to these Regulations and internal policies.

IV.18 The procedures for interaction of the officers of commercial bank units with the manager or officers of internal control system shall be established by internal documents approved by the Board of commercial bank.

IV.19 Commercial banks must undertake regular staff re-training to ensure awareness of the officers about latest achievements including information on modern money-laundering and terrorist financing techniques, methods and trends, and clear explanation of all aspects of the legislation and responsibilities to combat money laundering and terrorist financing.

IV.20 Measures to be taken by Financial Institutions and Organizations to ensure AML /CFT continuity

Unplanned messaging downtime is costly to productivity, the bottom line and your reputation and to loss of data which is by FATF required to keep up and running.

In this respect Operation continuity plans up to Disaster recovery organization should be prepared.

How to take a proactive approach to exchange messaging availability and secure continued AML process as well as Fraud detection, will cover by far more than only the AML/CFT solution.

Entire data center recovery and redundant Telecommunication concepts should be even so considered during AML/CFT planning and implementation.

Strategies to optimize the health and availability of each individual institute exchange environment and ensure business continuity should be planed to:

- Prevent the institute for loss of data, reports and history for RAS
- Prevent the institute and organization for loss or damaged reputation
- Prevent the institute for claims, investigation and consequently becoming excluded from international business by FATF / IMF sanctions.

To ensure its own ability to judge its own risk and to control it's internal process of RAS should be mandatory and mentioned explicitly.

Organizational measures to take should be individually referred and taken from the attached FATF rules and regulations.

In terms of Technology and system / solutions it will be not covered by this TOR entirely but as an individual Disaster recovery / Business Continuation plan and project.