Saw Centre for Financial Studies

Industry Working Paper Series 07-02

The Future of AML/CFT – Technology, Data, People

Rohan Bedi*
NUS Business School
National University of Singapore

**Executive-in-Residence*
Saw Centre for Financial Studies
NUS Business School
National University of Singapore
Singapore 117592
Tel: 97629060
Email: rohanbedi@rohanbedi.com
http://www.rohanbedi.com

The Future of AML/CFT – Technology, Data, People

Abstract

This paper provides important insights on the future of money laundering and terrorist financing risk management with a focus on technology. It highlights that there are new expectations from financial crime professionals in banks to be technology savvy. Implementation of prevention software is a key risk management issue and should not be thought of as just another software project. The active engagement of financial crime professionals before, during, and after the project - determines the overall risk-focus of the program and also impacts on the cost escalation of the project. The paper highlights the importance of understanding the different capabilities of prevention software and provides valuable tips to evaluate technology from an end-user/ productivity perspective. Specifically, effective charting is needed to reduce manual dependence in the investigations process and control operational risk. The importance of electronic KYC data is underscored as is the need for the AML/CFT program to be dynamic and enhance its KYC databases to include even non-public domain information from reliable sources. Similarly, training capabilities should be enhanced, for example, training on recognition of abnormal body language especially for CFT purposes. The capability to deliver a technology driven ongoing awareness program is increasingly becoming important. In its annexure, the paper highlights key technology implementation approaches and risks in the context of outsourcing/ offshoring.

April 2007

Keywords: AML, CFT, KYC, Future, Technology, Money Laundering, Terrorist Financing, Financial Crime, Risk Management, Fraud, Implementation, Outsourcing, Offshoring

Contents

No. Topic **Page**

1. Anti-Financial Crime – New Skill Set

With an increased focus in the anti-money laundering and anti-terrorist financing field on the usage of detection technology, the skill set required by financial crime professionals in banks, including money laundering reporting officers, is undergoing a transformation.

Anti-Financial Crime

Owners of the AML/CFT Technology Project.

There is increasingly an expectation that these professionals wear many hats including specifically being technology savvy. However, experience by banks suggests that financial crime specialists understand risk but are not necessarily as comfortable with a technology implementation, to which many have never been exposed to. In a fast paced field, these professionals have to invest significant time just to keep abreast with regulatory and risk developments. Nonetheless, there are new expectations from them and in the context of an AML/CFT technology project, they are the overall owners of the piece and should be clear on what they want, specify it properly, and test that they get what they want. Specifically, their new role encompasses:

- **Pre-project** - financial crime professionals help during the Request for Proposal (RFP) stage in the selection of the package by an early definition of their “wish-list”. This takes account of the broad capabilities that they want to see in any solution selected by the project team. It may well be that an external consultancy firm facilitates the RFP process. Furthermore, technology is an expensive game with both initial implementation costs and also annual maintenance costs. The fact is that if the banks risks require, adoption of a specific technology may be essential – this is where the financial crime professional’s inputs becomes critical.

- **During the project phase** - they play the lead role in domain training as well as taking ownership for the business requirements document (created by the project team) including standardized detection scenarios, charts, reports (operational, risk, MIS (& regulatory reporting), investigation processes (includes workflows), training material and play a role in the user acceptance testing process. Professional project managers try to keep a tight leash to ensure that time-line and cost escalations do not happen. They do not agree easily to incremental ad-hoc demands from financial crime professionals. Hence, these professionals need to do their initial ground-work thoroughly to ensure that they map all key risks, work-flow issues and reporting requirements into the initial implementation itself. Failure to do so would lead to multiple phases of business requirements, cost escalation and push-back on timelines for rectification owing to other priorities.
- **Post-project** - they have to ensure that new risk issues/ changes are reflected in detection rules being used. Ongoing maintenance may require a separate product team under the overall ownership of a key financial crime professional. Moreover, they have to establish their ownership for the investigations unit in an offshoring/ outsourcing situation, as countries operations transition from project mode to business-as-usual mode.

Overall, it’s important to understand that an AML/CFT technology project is a *risk management project* and not just another software project even if it employs professional project managers on the business and technology side.

Capabilities of Different Technologies

- **Rules Engine** - Detection scenarios or rules monitor the three "Vs" relevant to money laundering detection: velocity, value and volume. They can be set up based on value thresholds and other criteria (e.g. same originator/beneficiary; origination/ destination; transaction type/events; customer static data (e.g. monitor flag set). Rules can be layered (e.g. If this &/or this).

- **Statistical and Profiling Engine** - Offers a more flexible rules system based on relative, rather than absolute, thresholds of suspicion ie, rules get customized for a specific customer's account profile to detect deviations from "normal" behavior in the past (based on standard deviations or variances). The business rules can also be modified to take account of unanticipated variability i.e., fine tuned.

- **Neural Networks -** An artificial intelligence-based solution predicated on training the system to expect certain activity patterns and detect deviations from those patterns. These models score any new activity as to its likelihood of being suspicious. Such predictive modeling must have historical data for known good and bad activities to train the models – this may not exist. If built with data based on activities that "should be" suspicious, this may not be accurate.

- **Peer Group Analysis -** Works with both statistical and profiling engines & also neural networks to facilitate peer comparisons. This assumes that the banks customer data on their KYC system identifies peer groups clearly and interfaces with the AML software to allow the peer comparisons. Detection rules for CFT purposes can be created in the context of value thresholds set on peer groups (rather than stand-alone on accounts/customers which potentially would generate unmanageable alerts).

- **Link Analysis** - Used as a data mining tool to explore hidden associations e.g. people, bank accounts, businesses, wire transfers and cash deposits. Links in apparently unrelated persons, places and events can be highlighted with visualization tools (e.g. by i2 Inc.) to highlight networks of activity (legal and illegal) and help to focus investigations. Temporal link analysis factors in time into the investigation. Visual link analysis charts have provided powerful solutions in fraud and AML/CFT investigations involving the flow of funds or commodities, complex timelines of events, multiple financial transactions and intricate relationships between companies and individuals.

- **Time Sequence Matching -** To discover time ordered events, such as the deposits of sequentially numbered monetary instruments and the rapid movement of funds. Like link analysis, it helps to uncover suspicious connections or links between customers, accounts or groups of accounts.

- **Name Recognition Technology -** To match names (and aliases) in account and transaction parties with sanctions and high-risk lists of persons and entities (and alias where available). Helps to spot misspelling, abbreviations, juxtaposition, sound-alike variants. Can also be used to highlight links in different people and entities. Needs a good quality Know Your Customer database (e.g. World-Check, Factiva, Complinet, LexisNexis[1] etc.) to perform to top-value i.e., good input leads to good output.

The above technology pieces are not exhaustive.

[1] Differences exist between existing vendors in terms of breath of coverage and information collection processes

2. Key Issues

There is a need for financial crime professionals to understand and keep their focus on some key issues. This will help them in dealing with the challenges of change that technology implementation creates.

2.1 Technology

1) Understanding Capabilities

They need to increase focus on understanding the various types of transaction monitoring technology. These technologies have the capability to help companies analyze the behavior of their customers, employees, and partners in every transaction across the organization, from every angle – past, present, and future. Based on this understanding, financial crime professionals need to upgrade their skill set to enable them to implement effectively:

- **Rules Engine –** They need to have the ability to set-up multi-layered rules based on the banks risks. Unique risks specific to the operations (country, business, entity, product, transaction) need to be studied including by looking at data/ internal surveys (or other means). Fine tuning of rules to ensure that that risk and effort are aligned, is also important.
- **Statistical and Profiling Engine** - Rules setup must not just be for comparisons with account history but also of actual versus expected transaction profile. This is in order to take account of the risk that using the previous 6 months data may allow large fund movements to go through undetected. Moreover, a fundamental question that needs answering is whether the profile taken when the account was opened is still valid.

- **Neural Networks** - Neural networks need training/ retraining and can generate excessive alerts if this is not done properly. In the past this needed hiring of a neural network expert or a statistician to build the classification models. This is now much easier with specialist classifier technology tools that solve classification and categorization problems based on patterns learned from historical data. Nonetheless, this is the role of a specialist other than the financial crime specialist but it needs supervision to ensure that risk issues are adequately captured.
- **Peer Group Analysis -** Identification of peer groups is the main skill required. Focus should be on categories that are known to be high-risk for money laundering and terrorist financing e.g. cash-intensive businesses, jewelers, exporters-importers, charities, students etc.
- **Link Analysis** - Link analysis can be performed on a specific data-set pertinent to a specific case (e.g. people, organizations and businesses involved). This needs identification. It is also performed at a more general level to expose and analyze money laundering or terrorist financing networks that are hidden and for which there is no specific case.
  - It uses data sources that could include SAR (suspicious activity reports), CTR (currency transaction reports) (where applicable), other financial transactions, business relationships, etc. and brings in time as a dimension.
  - Networks can be defined and the technology used to perform an analysis of the network periodically. This would help to detect and report the network trends and even issue an alert when there is a significant change in the trend.
  - The process of setting up the data sources and parameters for link analysis is akin to the process of identifying and setting up parameters for detection rules under the rules engine.

- **Time Sequence Matching -** Similar to link analysis in that it can be used for a specific case or more generally to identify hidden relationships. Setting up the parameters to perform the data mining is the key skill.
- **Name Recognition Technology –** Skill to be acquired is how to use this technology. This requires the setting of parameters to perform the search including the sensitivity of the search and weights to be assigned to particular variables. The experience of vendors is that staff needs a degree of hand-holding over a few weeks before they can perform the search effectively to derive full value.

Broadly, the above technologies confer the ability to detect not only known but previously unknown suspicious behaviour; and ensure high detection rates through building customer and account profiles based on transactional customer activity across all lines of business.

2) Factoring in Risk

It is important to understand what the piece can do and also in what risk situations it should be employed. For example:

- If the branch operations are small then rules based reports generated internally may suffice.
- Peer group analysis is essential for creating detection rules for terrorist financing (e.g. on students). Creating rules directly on the customer/account level runs the risk of many false positives (meaningless alerts wasting time). Given the time sensitivity of terrorist financing/ the small amounts involved and the need to also monitor behavioural anomalies, peer group analysis is increasingly important.
- Where the business profile includes sensitive businesses (e.g., jewelers) or is in a country/territory regarded as high-risk for money laundering or terrorist financing or where

the operations are spread out geographically or international in nature; there link analysis may be critical to have as a technology.

- Time sequence matching is a key tool where deposits or issuance of monetary instruments is a regular business and can help expose early stage laundering schemes.
- Besides the above technologies, managing identity theft is a critical risk to manage and can include the use of other solutions (and databases) such as a passport check on machine readable passports.

Holistic Risk Based Approach

As can be seen above, various techniques may highlight specific risks. Hence to get an overall risk score on an entity, it is appropriate to adopt a combination of the technologies. This is of course an expensive route which the larger banks should invest in where their operations are diverse geographically and/or they have peculiar business or country risks.

Self Risks

Lastly, the financial crime professional has to guard against the risk of him/her fine tuning the alerts to fit the budget for staff costs! This is important because the fine tuning process can lead to unrealistically high value thresholds or key detection scenarios not being turned on at all because the alerts are too many to manage. The fine-tuning process should therefore be realistic and *internal audit* must check the parameters set, in order to establish whether the process has been perverted.

3) End-User/Productivity Perspective

It is also important for the financial crime specialist to be able to evaluate the transaction monitoring technology from an end-user's perspective. This approach will necessarily have a *significant impact on productivity and quality of risk management*. This is not the technical evaluation (e.g. integrate with diverse systems; scalability with spikes in transaction volumes; security etc.) which is separate. However, some points are linked to the technical evaluation.

Don’t miss these key points:

Quality of information in an Alert

- Alerts should be supported by historical and contextual information to ensure high productivity in investigations.
- This includes drill-down ability to, for example, highlight related transactions (that generated the alert) and related alerts (e.g. a daily and monthly alert shares the same transaction references) where possible.
- System generated risk scores for the alerts (based on the risk model set-up within the system) add value in terms of where to focus investigative energies.

Reducing Manual Investigation Processes/ Dependence

Investigations

Reduce manual dependence through charting.

Charts are a critical part of an “intelligence driven” approach to investigations.

- Profiling information should be available at the account and customer (& ideally at the customer’s customer level by a pseudo-customer created by the software) level.
- Charts supporting a particular alert to profile the account/ customer (relative to history/peer comparisons or alert (wherever possible e.g., periodic alerts related to monitoring of a new network uncovered earlier). For link analysis special visualization tools exist.
- Charts help in reducing manual investigation processes thereby significantly enhancing productivity and standardization of investigation processes/ lesser chances of slippages in the process. Charts can, for example, highlight through separate colours/ a flashing portion of the

graph, where deviations from normal behaviour/ peers is significant. This would reduce the time spent by analysts to identify key anomalies.

- If an average investigator can handle 10 alerts/cases in a day, effective charting can double productivity.
- Many banks automating their AML/CFT investigations miss this very critical point on the need for charts to support investigations.

Work-flow Issues

- Ability of the solution to automatically merge multiple alerts relating to the same entity, into one alert. This could be for the customer or at the customer's customer level e.g. remittances come in from an originator company that can have the originator name in short e.g. GE for General Electric, with other remittances having the full name.
- Ability of the solution to "deselect" alerts which are on accounts where earlier alerts were closed in the last 6 months (the alerts still need some investigation to ensure that they don't represent a new trend).
- Ability for an analyst to pick up multiple alerts from the "all alerts" queue.
- Ability to prioritise high-risk alerts and give visibility to alert status for effective controls.
- Ability to restrict what an analyst can do, for example, escalations of investigations from the outsourced investigations unit to the in-country unit can be a restricted systems authority for supervisors only.

Product Efficiencies

- An easy system for analysts and compliance officers to be trained on and use.
- Email system interface with the technology used and capability to ensure audit trails for emails sent out to branch offices and replies received.

- Where searches on watch-lists (high-risk lists/ sanctions) or on the customer database are done through the solutions search option, the performance time is critical to review.
- Quality of information that the system picks up for the SAR report i.e., the information should be complete with minimum manual intervention to fill in the SAR report.
- System interface for e-SAR filing (via encrypted email link) with the external bodies where SARs can be filed online. Automatic receipts saved as part of the audit trail.
- Ability to create and tune/modify new/ existing detection scenarios easily as market and criminal behaviour changes or based on periodic reviews. This includes the ability to perform sensitivity analysis on various If-Then iterations of threshold values and other variables in the detection scenarios, in order to ensure a risk-based approach and adequate staffing.
- Ability to create and modify reports on the fly.
- Flexibility of the system with capability of accommodating changes in the business (e.g. adding newly acquired banks, lines of business, new products and customers).
- Record-keeping i.e., storage (includes investigations related documentation and emails), archiving and search capability for historical alerts. (For example, archive all alerts that have been generated over the previous 6 years, plus all the alerts that have been reported over the previous 12 years.)
- Ability to roll-back alerts in case of data problems and/or program/system errors.

Evolving the Risk Focus

- MIS generated from the system that highlights key risk factors for example, the kind of alerts getting generated and the kind of SARs getting filed (e.g. 30% linked to PEPs and property investment). This feeds back into training and potentially in resource allocation/ specialization. This also helps to identify the need for new detection rules.

Audit Trail

- A clear audit trail that highlights the date/person making amendments and where possible/ practical - the actual amendment. Don’t assume that the audit trail is good, test it for activities you consider sensitive.

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.

4) Managing Key Activities

During the project phase of an offshoring/ outsourcing model, the Country Money Laundering Reporting Officers (MLROs) (as users) take ownership for managing the user acceptance testing process and for setting up of the in-country investigation unit for investigations escalated to the in-country team. Many of these professionals have been through similar tasks including managing retrospective data remediation exercises, look-back for SAR filing etc.

5) Role Definitions

Role Definitions

It’s critical that these close all cracks.

There is a need for clear role definitions with an organization chart that maps the entire AML/CFT space both before and after the technology project, to ensure that activities do not fall between cracks. Role descriptions should be both high-level and prescriptive so that there is sufficient clarity. Specifically, the AML/project governance structure should be a ‘good fit’ i.e., the oversight committees (group risk, business (risk & implementation) and project) should be manageable while ensuring that adequate representation/ buy-in is obtained. Given below are indicative role definitions of two critical teams:

Anti-Financial Crime – Group-Wide Function

Most large banks have such a centralized group function that plays a key role. This team takes on overall ownership of money laundering and terrorist financing risk mitigation strategy, policies and minimum standards and their implementation. They also prioritise new country implementations of AML/CFT technology based on their risk assessments. Specifically:

- They develop group policies in order to mitigate Bank-wide AML/ Regulatory risk. As part of this role they assess group-wide risks and share assessments, monitor global regulatory developments/actions, benchmark the banks global practices to market leaders/peers, and provide topical guidance to plug risk management gaps as they arise.
- They also develop strategies including: KYC data remediation/ consolidation, Know Your Employee, developing a high-level group-wide monitoring and KYC technology adoption strategy, detailing a group-wide information sharing policy to manage risks, detailing group-wide awareness program approach leveraging technology, and an anti-identity theft program strategy.

Product Focus

Depending on the scale of the banks operations, there may be a need for a separate Product Team under the overall ownership of a key financial crime professional from the group function. The role of the Product Team would be as below:

- They define product strategy driven by the approved group risk mitigation strategy. They identify risk management and KYC process automation solutions and keep them standard and current. This includes related documentation such as the Business Requirements document, functional specifications etc.

- They determine functionality, scope of use, scale of investment and schedule for replacing applications. They also prepare and publish a product enhancement road map.
- They define and maintain a list of standard set of detection scenarios, reports, and charts specified by businesses for aiding investigations. They also play a key role in evolving these in order to ensure effective risk mitigation through the product. (Country compliance determines (in agreement with the product team) the specific detection scenarios applicable and the related thresholds for their country operations; and same for reports/charts.)
- They develop strategy for product and domain training and awareness and ensure its delivery. This role includes acting as the central repository of all training and awareness material (presentations, videos, audios etc.).
- Strategic vendor management once the AML/CFT software project has been full implemented and phased out.

A good product team will have a mix of both domain and project management specialists with a systems skill set.

2.2 Data

6) Enhance KYC Databases

Many banks rely on one or two database vendors for their Know Your Customer screening requirements against sanctions (e.g. OFAC) and high-risk lists (e.g. against PEP and suspect terrorist lists). However, it is important for banks to supplement the products of these vendors with their own high-risk lists which could include:

Databases

These must be built on an ongoing basis.

- Sanitised risk-related information on SAR filings in the countries where they operate (even in the US, guidance issued on the law allows such an approach) without discussing the fact of SAR filing and as part of a larger database of other high-risk persons/entities (e.g. where SAR filing was not done but the customer was put on watch or names from the banks own media searches)
- Intellectual Property Rights database of high-risk persons/entities e.g. ICC CCS UK, MPAA (where agreed to be shared by them) etc.
- Other public records e.g. police records, in markets where such databases are available/ accessible easily (ideally electronic databases) and considered necessary to review for specific cases.
- Lost and stolen passports data where available.

Importantly, the sources of information must extend beyond third party products that rely only on public domain open-source information to also cover: third party products that cover public domain closed-source (which involves payment of subscription of some sort); and other non-public domain information (e.g. information from the MPAA). The caveat is that these should be *reliable sources* especially if a temporary freezing/ blocking of the transaction is required under the countries laws.

7) Think Creatively

The UK FSA wants banks to think laterally and to make a creative use of feedback from law enforcement. They call it the ‘intelligent use of intelligence’. Examples include using court orders to evaluate risks on other clients; using data such as lists of stolen passport numbers and from intelligence from law enforcement on carousel and tax credit fraud, in order to better identify and target suspect activity.

8) Improve Data Quality and Ensure Electronic Availability

Risk-focused data remediation to improved the data quality/ ensure that regulatory enhancements are kept up with, plus integrating systems to ensure that a consolidated view of a client’s data is obtained – are all key focus areas for banks. Importantly, KYC data (and not just data on transactions) must be available electronically particularly where an offshoring/ outsourcing model is being implemented. Electronic availability also ensures that checks on data-quality are faster and more accurate. Moreover, the implementation of KYC process technologies (case based with risk scoring capabilities) would also help in improving data quality.

2.3 People

Training & Awareness

9) Training has to be risk-focused and capabilities should be enhanced as issues become more transparent. For, example, there is a need to increase focus on understanding the "body language" of a customer (see www.lichaamstaal.com/english/) to see if there are signs of discomfort when certain questions are asked which represent information that a customer should normally be able to provide. This approach is particularly important for spotting potential terrorist financing cases as the Sept 11 terrorists highlighted. Role play as part of the AML/CFT training will help to reinforce this.

10) While the role of the board (&/or audit committees) and senior management in AML/CFT is understood in the US and UK; in Asia-Pacific this role is not as well understood. As a result of this, “tone at the top” on AML/CFT issues is not of the required quality and this requires targeted training and awareness initiatives.

[Regulators in the region (other than the *Philippines* – a former FATF black-listed country) have so far shied away from requiring technology and this has also caused poor “tone at the top”]

11) Internal audit in Asia-Pacific are also in need of focused training and awareness initiatives. They need to develop “expert person” competencies within their group so as to be able to live up to their key role as one of the “pillars” of an effective AML/CFT system.

12) Lastly, ongoing awareness building of front-office and back-office staff using technology needs focus on. This could be through newsletter subscription, sharing a new case study every

day (e.g. in the form of a 5 minute movie emailed daily), screensavers etc. Other measures include the MLRO joining into business discussions.

More broadly, technology is one component and the need for trained investigators once a full-capability system is installed, is all the more so. Technology creates new capabilities which then have to be understood and fully utilized. The risk factor of all sophisticated technologies is that many of the features don’t get used because the persons involved don’t want to take the effort (e.g. MS-Excel). Hence a sophisticated system may be purchased but it’s also important for *internal audit* to study what was purchased and what actually got implemented.

3. Conclusion

In conclusion, financial crime professionals particularly in *Asia-Pacific*, have to move out of their comfort zones and enhance their skill sets to prepare them for the future of AML/CFT which will largely be technology and KYC database driven.

Their approach has to become more dynamic with a focus on ongoing program enhancement to manage old risks better, manage new risks and regulatory requirements i.e., developing new rules and scenarios as they emerge. A renewed focus is needed on CFT looking beyond simple name matching to peer group analysis, link analysis and focus on "body language" in the front office. And of course, professional certification programs need to update their curriculums to reflect the growing importance of technology for AML/CFT.

****

Annexure 1 – Key AML Technology Implementation Approaches and Risks

Annexure 1 – Key AML Technology Implementation Approaches and Risks

Annex 1.1 Phased Implementation Approach

- It is always better (and logical) to first automate KYC processes, bring the KYC data on file up to standard (data remediation), ensure that peer groups data is available in the source system - before implementing AML/CFT technology. This is particularly true for Private Banking operations. However, for reasons of regulatory pressure, this may not always be practical.
- Banks also take a strategic approach to their phased implementation approach. Besides money laundering/terrorist financing country risk, a key factor influencing banks implementing technology are their plans to upgrade their core system and their data-warehouse plans (if any). Ideally, they would like to do things in tandem logically. They build standard system interfaces which are reused for subsequent implementations with countries on the same core system, reducing system testing time and allowing concurrent rollouts.
- Banks implementing AML/CFT technology have found that it needs to be done incrementally i.e. turning on different modules in succession once the previous module has stabilized and also turning on detection scenarios incrementally/ in a risk-focused manner. Similarly, building *exclusion lists* for the name matching of customers (and linked accounts), account parties (e.g. signatories) and transaction parties (e.g. originator) against KYC databases of “bad guys”, is an important preliminary activity (different packages will differ on their capability to do this). This helps ensure that people and entities that have similar

sounding names but are not the relevant “bad guy”, are excluded from the alert queues in future system runs (the exclusion list is subject to periodic reviews). All this helps to manage potential operational bottlenecks related to the number of alerts and investigators deployed.

- Banks also like to take a phased approach to product coverage e.g. retail, corporate, treasury, trade, for transactions monitoring implementations. For sanctions filtering implementations a similar phased approach would cover extension of scope of initial implementations to SWIFT message types (e.g. securities) and other electronic entry/exit points e.g., country RTGS, Interbank payments, etc.

The above approach helps to mitigate the risk of failure and also to manage the project more effectively operationally.

Annex 1.2 Key Time-Line Risks

- Every AML technology project has a “critical path” which highlights activities that are dependant on each other. Most delays in project timelines happen because of technology issues linked to the “critical path”. For example, customization of the solution, data linked issues (data warehouse, data extraction), software patches for issues that come up in the User Acceptance Testing. Hence dependency management and risk management are critical.
- Data quality (e.g. identification of peer groups, key KYC data recorded in electronic form) and data mapping (what will come from where) issues are also key factors to manage. Data mapping for example, is dependant on the skills of the persons involved.
- Importantly, while any individual activity on the “critical path” may not have a significant impact, the cumulative impact of these activites is what project managers try to control.
- More broadly, concurrent rollouts create timeline risks.

Annex 1.3 Outsourcing/ Offshoring Risks

Most experienced compliance and financial crime managers are aware of these risks. Nonetheless, for good measure, given below is a list of some key risks:

- A key risk is that of staff turnover which needs to be managed by hiring the right profile of staff and taking steps to retain them effectively.
- Another key risk to manage is that of privacy of data. It is important to ensure that privacy considerations are imbedded into training and awareness approaches as well as in physical controls and reviews/audits.
- From a practical point-of-view, if KYC profiles are available only on paper, there will be push-back from units in-country who do not want to handle the new workload of queries on the KYC profiles of customers required for alert investigations i.e., proper review of beneficial ownership information may not be possible. This creates operational risks as this is a basic element of an effective alert review process.
- Clear ownership within the organization for the outsourcing is critical. Key to creating this ownership is effective ongoing engagement between the project team and the oversight committees/other stakeholders and also effective transition between the project and activities in business-as-usual mode.
- Through standardized (detection scenarios etc.) and “intelligence driven” approaches to the investigation processes (e.g. using charts) and training (e.g. refining training focus based on SAR filing patterns), including leveraging technology wherever possible, it is critical to manage a consistent quality of output and also reduce manual dependence wherever possible. This helps to control operational risks.