Information Technology Audit Considerations When Designing Audit Coverage For AML Applications

Peter D. Wild, FCA, CAMS

The views expressed in this paper are solely those of the author and do not represent those of JPMorgan Chase.
IT Audit Considerations When Designing Audit Coverage for AML Applications

Table of Contents

1. Introduction.............................................................................................................................................. 3
2. A Brief History of Auditing .................................................................................................................. 3
3. The AML Application Suite ................................................................................................................. 5
4. Information Technology Control Categories for Application Systems .............................................. 5
   4.1. Security Operations .......................................................................................................................... 5
   4.2. Technology Operations .................................................................................................................... 6
   4.3. Change Management ....................................................................................................................... 6
   4.4. Vendor Management ....................................................................................................................... 6
   4.5. Business Resiliency ......................................................................................................................... 6
   4.6. Information Management ............................................................................................................... 6
5. AML Application Controls that may require special audit emphasis ................................................. 7
   5.1. Know Your Customer ....................................................................................................................... 7
   5.1.1. Automated Auditing ..................................................................................................................... 8
   5.2. Sanctions Name Screening .............................................................................................................. 9
   5.2.1. Automated Auditing ..................................................................................................................... 10
   5.3. Transaction Monitoring .................................................................................................................. 11
   5.3.1. Data Input .................................................................................................................................... 11
   5.3.2. Monitoring Logic .......................................................................................................................... 11
   5.3.3. Application Performance ............................................................................................................ 12
   5.3.4. Data Output .................................................................................................................................. 13
   5.3.5. Automated Auditing .................................................................................................................... 13
   5.4. Case Management .......................................................................................................................... 13
   5.4.1. Data Input .................................................................................................................................... 13
   5.4.2. Access Control ............................................................................................................................ 14
   5.4.3. Data Output .................................................................................................................................. 14
   5.4.4. Automated Auditing .................................................................................................................... 15
6. Model Risk Management ....................................................................................................................... 16
7. Conclusion ............................................................................................................................................. 18
8. References ............................................................................................................................................. 19
1. Introduction

This paper is intended to provide a high-level introduction to some of the important considerations that should be kept in mind when designing the Information Technology {IT} audit coverage for the suite of applications that support the Anti-Money Laundering {AML} and Sanctions Screening business processes in a Financial Institution {FI}. It is possible that the AML Auditor may not be familiar with IT Audit techniques and it is also possible that the IT Auditor may not be familiar with AML audit requirements. This paper aims to assist that partnership in the design and maintenance of effective AML audit coverage and offers some suggestions on how the power of software can be harnessed to improve audit depth and efficiency, this is referred to as Automated Auditing.

The scope of this paper does not include the following topics:

- The business processes to create and maintain the AML and Office of Foreign Assets Control {OFAC} risk profiles of the FI’s customers, products and geographies.
- The Audit Risk Assessment process which is more than adequately covered in the ACAMS Audit White Paper by Jonathan Estreich entitled “How to build an Audit Risk Assessment Tool to Combat Money Laundering and Terrorist Financing” ¹.
- A complete and well-designed program of audit coverage will also include a Continuous Auditing component. Using this approach to monitor the important Key Performance Indicators {KPIs} and regulatory changes, the auditor will be in a position to make appropriate changes to the Audit Plan in flight in order that it remains contemporary with the changing AML risks.

In this paper, the use of the term “audit” is intended to be synonymous with the independent testing requirement of Section 352 of the USA PATRIOT Act.

2. A Brief History of Auditing

In the early days of financial reporting, in England, the auditor was basically an historian who provided an opinion on the truth and fairness of a set of financial statements as of a certain date which covered the results of the previous financial period. He had reviewed every transaction and placed a neat tick against every entry in the leather-bound General Ledger and Cash Book. His duty at the shareholders’ meeting was to read out the Balance Sheet, the Profit and Loss Account and the Audit Report. This was because, at that time, printing was not only expensive, but also the postal service was not considered reliable. At that time, there was a limited number of ways in which the accounts could be wrong. The auditor was defined as “a watchdog and not a bloodhound” in the UK court case of Kingston Cotton Mills Co. Ltd. in 1896¹ and therefore not expected to find fraud.
As companies grew, mechanization permitted transaction volumes to increase to the point where the auditor could no longer review every transaction. The introduction of computerization also gave birth to the systems approach to auditing and shifted the emphasis to testing the effectiveness of controls, within the business process, that are designed to either prevent or detect erroneous transactions. This also provided the opportunity to harness the power of computer software to support the audit process and improve the quality of the audit coverage.

Today, the external auditor’s opinion, which is included in a set of financial statements, is expressed as:

The financial statements referred to above present fairly, in all material respects, the financial position of the Company as of December 31, XXXX, and the results of its operations and its cash flows for the year then ended in accordance with generally accepted accounting principles in (the country where the report is issued).

The financial statements are required to be materially correct - rather than precisely accurate - hence the use of the term “present fairly, in all material respects”. The Generally Accepted Accounting Principles support the concept of materiality and this is interpreted to mean that each balance is correct to within a margin of approximately 5% depending upon the context. Therefore the accounting processes and financial reporting is tolerant of an acceptable error rate - as is the audit process.

In the AML world, there is the requirement to review customer transactions for patterns of potentially suspicious activity. The existing transaction processing systems which supply the financial accounting reporting systems are now supplying the data for the AML applications. Because the AML regime has very little tolerance for error, the auditor needs to adopt a different mindset that expects a much greater degree of precision and accuracy. Now the auditor must also place a greater emphasis on the design of a new level of controls in order to not only prevent AML events in the future but also detect those which may have occurred in the recent past. Therefore the concept of materiality, in the traditional financial context, cannot be considered a factor in either the design of the AML business processes and supporting computer systems or the related audit tests.

Today, the vast majority of organizations, which are required to have a AML program, need to place significant reliance on computer systems in order for it to be effective. It therefore follows that successful AML audit coverage will be dependent upon good quality IT Audit support.

This paper attempts to describe some of the important elements of an effective IT Audit approach to the AML operational processes with the emphasis on the controls which operate at the application systems level. It should be remembered, however, that, to be effective, the application controls must be supported by not only effective manual or clerical controls, but also by the general IT controls which operate at the infrastructure level (which are not within the scope of this paper).
3. The AML Application Suite

The AML program will typically be supported by the following applications:

A **Know Your Customer** {KYC} application which records the results of all levels of Customer Due Diligence.

A **Sanctions Screening** application which compares the names of all customers, on a periodic basis, with the list provided by the relevant jurisdictions - such as OFAC in the USA - of the names of those with whom transactions are forbidden. This comparison must also be performed on wire transfer and ACH transactions whilst they are being processed. It also required during customer on-boarding. All name matches that are found must be reported to the local agency and the transaction must be frozen or rejected. There is also the requirement to identify Politically Exposed Persons {PEPs} who may represent a higher AML risk.

A **Transaction Monitoring** application which analyzes the financial transactions for patterns of potentially suspicious activity which may be indicative of a predicate crime.

A **Case Management** application which records the results of the investigations of potentially suspicious activity alerts and, when appropriate, files the Suspicious Activity Reports {SARs} electronically with the Financial Crimes Enforcement Network {FinCEN} in the United States or a Suspicious Transaction Report {STR} with the appropriate agency in foreign jurisdictions.

There is also an application to fulfill the requirement, in the USA, to file **Currency Transaction Reports** which is outside the scope of this paper.

4. Information Technology Control Categories for Application Systems

What follows is a list of standard categories of the Information Technology controls which should operate over and within all computer applications. The IT Audit plan should be designed to test them, over a reasonable period of time, as suggested by the Audit Risk Assessment.

As mentioned previously, this list does not include the controls at the infrastructure level, such as the controls over the communications network and systems software.

4.1. **Security Operations**

Security and access control management should include strong password syntax rules, the logging, reporting and escalation of security events, the administration of all types of users, this includes privileged access which is often required when the emergency Break Glass procedures are invoked to remediate a production problem. All user access rights should be recertified on an annual basis.
4.2. Technology Operations
The production environment must be managed to ensure that computer processing is appropriately scheduled, monitored against the Service Level Agreements (SLA) with problems being promptly reported, analyzed and resolved. The backups of the data, programs and systems software must be taken at an appropriate frequency and stored in a secure offsite location.

4.3. Change Management
It is important that a formal Systems Development Life Cycle (SDLC) is followed for both the development of new systems as well as changes to existing applications. This requires separation of the Production, Testing and Development environments which often relies upon access control to limit access to the minimum as defined by the user job function. A strong and disciplined testing methodology is essential to a satisfactory AML program. It is important that the program code is managed effectively and this typically involves the use of program library software to enforce version control. Strong controls are also required over Emergency Changes when problems with production processing are being urgently remediated.

4.4. Vendor Management
Vendors need to be managed in order that they respect all internal policies and standards of the FI and meet the SLAs.

4.5. Business Resiliency
The ability to recover the AML Suite of applications quickly is dependent upon an effective recovery plan which has been subjected to periodic and realistic testing. This testing should not only include moving processing to the recovery site, but also the move back to the production site - which is often a more significant challenge.

4.6. Information Management
This category has two important areas: Data Confidentiality and Data Integrity.

Data Confidentiality covers the classification of data into Highly Confidential and Confidential to ensure that there is appropriate protection over the data wherever it is stored and how it is transmitted across the networks. Particular attention must be paid to the protection of data used in the Test and Development environments. This is particularly important when a copy of production data is used for testing.

Data Integrity includes all the controls that ensure that the data is complete, accurate and timely. All file transmissions should be subject to reconciliations which prove that the correct number of records has been received. The file attendance controls will identify missing, late and duplicate files as they are received as defined by the SLAs. The edit features of the application should ensure that any erroneous data is identified and is subject to a correction process before being accepted for
further processing. The exception reports provide an opportunity for another decision point to review unusual data values for acceptability.

5. AML Application Controls that may require special audit emphasis

The Audit Risk Assessment will guide the auditor in designing the appropriate audit coverage when the IT Application Controls are being considered for testing. All the IT Control categories should be covered, for each application, within a reasonable period of time, at least on a three year cycle.

What follows are some of the special considerations with respect to IT Controls that should be considered when designing the audit coverage for each AML application. There are also some suggestions for Automated Auditing, these are not exhaustive, but are intended to stimulate discussion on the subject. Using Automated Auditing routines to provide independent error and exception reporting is extremely powerful. This provides the opportunity to effectively review the whole population and it can reduce the need for some of the manual testing using sampling.

5.1. Know Your Customer

The KYC process should be closely integrated with the customer on-boarding process to ensure that business is not conducted with a prospective customer until the required level of due diligence process has been satisfactorily completed. The prospective customer names must be compared with the latest OFAC and PEP lists or their equivalent in other jurisdictions. The FI will also have a list of customers with whom it does not wish to do business and this is often considered to be highly confidential and, therefore, access and changes to this list must be strictly controlled.

Since KYC applications must cater for all the FI’s customers and record the correct combination of products and geographies, it is likely to be a very complicated set of rules. It is important to ensure that, as a result of each change to the program code, the KYC records retain their integrity. If a program change corrects an existing defect which had resulted in incomplete records, then those records need to be remediated promptly and this may need to be a manual process. It is also possible that a change could cause some records to become “orphans” and therefore inaccessible until a subsequent correcting program change. This situation demands comprehensive and rigorous testing. The auditor should review the testing management processes, including the quality of the test data that is used.

The KYC application may have a formula which calculates an AML risk score or ranking for each customer based upon the profile in respect of the products and the geographies. This may mean that it could be classified as a Model and therefore be subject to the requirements of OCC 2011-12 “Supervisory Guidance on Model Risk Management”3 which will be discussed later in this paper. This calculation should be tested to ensure it complies with the KYC Due Diligence policy and all manual
overrides of the automated risk rating must be reported in order to ensure they can be properly authorized.

Accurate KYC metrics are very important in order to support, for example, effective management of workflow queues for renewals. With renewals, the frequency should be based upon AML customer risk so that high risk customers are renewed every year and low risk customers on, perhaps, a cycle of once every three years. The system should present the customer records for renewal at the appropriate time and warn if there is a backlog. Often the records are placed into work queues for each of the users and it is necessary for a supervisor to have the ability to re-assign work dynamically in order to smooth out peaks and troughs to keep the work on schedule. These queues should be reviewed for completeness and accuracy and the queue management functionality should be tested. The periodic reconciliation of the KYC records with the Customer Information File should also be tested.

5.1.1. Automated Auditing

Consideration should be given to designing audit tests in the following areas:

1. Incorrect values in certain fields such as:
   - Next renewal dates in the past or too far in future
   - Last renewal dates outside the frequency required by policy
   - Non-existent product codes
   - Invalid country codes
   - Invalid currency codes
   - Invalid workflow queue codes
2. Multiple customers with the identical Social Security Number or Tax Identification Number.
3. Extracting samples of KYC records in order to review the quality of the evidence to support the customers who have been assigned High, Medium and Low AML Risk Ratings.
4. Determining that the renewal of the KYC data has been performed in accordance with the timing commensurate with policy in respect of the AML Risk Ratings.
5. For new customers in the previous year, comparing the date of the completion of the KYC review to ensure it is before the date of the first transaction.
6. Replicating the calculation of significant KPI’s such as renewal volumes and renewal lateness.
7. Comparing the KYC customer records with those on the Customer Information File for completeness to ensure that a current KYC record exists for every customer.
5.2. Sanctions Name Screening

The screening of names against the Specially Designated National \{SDN\} list provided by OFAC - or the equivalent list for other foreign jurisdictions - and also a PEP list must occur in three distinct places:

- During customer on-boarding.
- During the processing of certain transactions, such as wire transfers and ACH transactions.
- Periodic comparison of the authoritative list against the FI’s customer names, given the fact that the official lists are constantly having names added.

The common requirements in each of these different system environments, which need to be tested, are:

1. It essential to be able to easily demonstrate that all customers, accounts and transactions are included for screening with the appropriate control totals and reconciliations.
2. All the relevant data fields must be mapped precisely and correctly, from the source transaction processing systems, without any data truncation.
3. The OFAC list of names - or the local equivalent - must always be the very latest.
4. The Change Management and testing processes over the screening logic are critical and may have to be subject to the requirements of OCC 2011-12 Supervisory Guidance on Model Risk Management, which will be discussed, in more detail, later in this paper.
5. The challenge with OFAC name screening is establishing and maintaining the thresholds which define the proximity of the matches. The auditor should review the periodic validation that is required. This involves testing below the threshold to demonstrate that nothing of significance is being missed. The design of the test data used for this testing should be reviewed in order to ensure that it provides positive confirmation of the validity of the thresholds.
6. In the case of wire transfers and ACH payments, the screening has to be done as part of the actual transaction processing. The suspect matches need to be visually reviewed very promptly by experienced personnel who decide whether to block or reject the payment. The history log of their actions should be tested for completeness and accuracy. Transactions which are a match must be placed in a blocked account and reported to OFAC or the local equivalent agency.
7. In the case where an FI has a number of different locations where sanctions screening takes place, it is important to test that the results are the same in all locations and this includes the facility provided for screening during client on-boarding.
8. The change management and access controls over the special internal lists are very important. What is often called the “Black List” contains the names that the FI does not wish to do business with and the “White List” is used to suppress the reporting of matches.
5.2.1. Automated Auditing

1. Consideration should be given to downloading the current SDN List from the OFAC website and writing a computer program to convert this data into a file which is identical in format to the customer file that is subjected to the periodic name screening. The current sanctions screening production application is then copied into a test environment and executed against the test SDN file that was created. This should result in a 100% match, but any differences need to be explained and the alternative procedures for these situations must be reviewed. Consideration should be given to making this test a step in the regular change control process.

2. This test above can be supplemented by adding names where:

- the sequence of multiple names is changed as in:
  
  Maria Isabel Carrasco Maubras Gonzales
  Maria Gonzales Carrasco
  Isabel Carrasco Gonzales Maubras

- and single characters are changed:
  
  Maria Gonzalez Carrasco
  Isabel Carasco Gonzales
5.3. **Transaction Monitoring**

Transaction monitoring systems are typically run after the transactions have been executed in the source systems. This can be weekly and/or monthly. The source transaction processing systems often have been in place considerably longer than the requirement for the stringent transaction monitoring requirements of today.

5.3.1. **Data Input**

At some point, in the past, a program change was made to each of the transaction processing source systems to create files of transactions and reference data for transmission to the transaction monitoring application. It is important to test that the correct data fields have been accurately defined and that no data truncation occurs. This data flow must be tested to ensure that all the controls are working effectively. It is necessary to be able to demonstrate that all the appropriate transaction records are being delivered to the transaction monitoring application. Whilst record counts will prove the completeness of the transmission, it may be more difficult to use this count to demonstrate that all the eligible transaction records have been included. In the case of a checking account application, for example, not all transactions need to be sent for monitoring - such as interest and bank charges. It is important for the auditor to understand where the actual elimination of the ineligible records takes place, whether it is before the file is sent or after it has been received. It is considered preferable to make the selection after receipt by the Compliance Department and the selection logic should be coded in a manner where a new record type would cause an error since this could indicate, for example, the introduction of a new product. A very effective control which proves the completeness of the transactions sent to monitoring is to use the same financial control totals, for each transaction type, as those which are posted to the General Ledger. File attendance controls must be tested to ensure that they are in accordance with the SLAs and, therefore, files which are late, missing or duplicated are handled promptly and appropriately.

5.3.2. **Monitoring Logic**

The logic used for monitoring financial transactions can be of two basic styles: value and volume and specific queries.

The value and volume approach requires that similar accounts are placed in the same peer group by virtue of the expected transaction activity for that customer type, taking into account the products used and the geographies involved. The monitoring logic will report the transaction activity of those accounts which is outside the thresholds set for the average activity for that peer group.

Specific queries are designed to identify transaction patterns that may be indicative of particular predicate crimes - such as Structuring and Human Trafficking. These are often referred to as “Typologies” or “Scenarios”.
Value & Volume logic

The Change Management and testing processes over the value and volume logic are critical and they may have to be subject to the requirements of OCC 2011-12 “Supervisory Guidance on Model Risk Management”, which will be discussed in more detail later in this paper. Consideration should be given to testing the following:

1. The assignment of the accounts into their Peer Groups, according to their AML risk profile, to ensure that every account resides in the appropriate group.
2. The change management process over the Peer Groups, including how accounts are added, deleted and moved.
3. The change management process over the thresholds for the Peer Groups with particular emphasis on the test documentation showing the results which support the validity of the thresholds.
4. The periodic validation of the Peer Groups, including the testing below the thresholds to ensure that there are no false negatives.

Typology Logic

Typologies are specific queries defining transaction patterns which are potentially suspicious and indicative of a predicate crime. The testing and validation of the typologies would most effectively be achieved by creating test data which is specifically designed to exercise all the logic paths in the program code. The auditor should review the Change Management process and expect that the test data is used and enhanced as necessary to reflect the nature of each subsequent change. Also the documentation describing the typologies and the computer source code itself should be regarded as confidential with appropriately strict access controls.

5.3.3. Application Performance

The execution times for transaction monitoring in large FI’s are often very long. Where, for example, the monthly run extends over twenty four hours, it is prudent to have checkpoints at certain intervals so, in the event of a systems problem, it will not be necessary to restart from the beginning. In these cases, consideration should be given to reviewing the trends in the execution times over a reasonable period – perhaps the previous twelve months. The statistics that should be reviewed, beyond online response times and batch execution times, to include CPU and disk utilization. It is important to understand the “head room” that is available. For example, as a rough guide, the CPU utilization, on average, should not exceed 80%. This should permit continued processing during peaks in transaction volumes. The other trend is the growth in the disk space used. The trends shown in these statistics should be considered in terms of the scalability of the application in the context of the growth in future transaction volume estimates. In order to keep pace with the growth, the lead time required to install faster or more CPUs and increase the disk space must be taken into consideration.
5.3.4. Data Output
The potentially suspicious alerts need to be transmitted to the Case Management application with appropriate control totals.

5.3.5. Automated Auditing
Consideration should be given to designing audit tests in the following areas:

1. Incorrect values in certain fields such as:
   - Invalid product codes
   - Invalid country codes
   - Invalid currency codes
   - Invalid Peer Group codes
   - Invalid workflow queue codes
2. Replicating the calculation of control totals over the data received from the transaction processing systems and the alerts sent to the Case Management application.
3. Replicating the logic of significant typologies.

5.4. Case Management
The case management application plays a crucial rôle in the investigation process since it records the evidence to support the final disposition of all the potentially suspicious alerts.

5.4.1. Data Input
The data transmitted to the case management application should not only include all the alerts generated by transaction monitoring with the related transaction data but also the associated reference data for the respective accounts and customers in order to facilitate the investigation process. It is important that the investigator is presented with all the relevant information about the customer. The controls and reconciliation processes which ensure the integrity of this data should be tested.

This application will also typically include the facility to manage the queues of alerts as they are assigned and re-assigned amongst the investigators. This is important in order that the changing volume of alerts can be managed effectively to ensure that the legal deadlines are observed and that significant backlogs are not permitted to occur. The auditor should review the completeness and accuracy of the management of these queues and the queue management functionality.

In order to enhance the efficiency of dispositioning the alerts, the investigator should be presented with as much related information as possible about the account and the customer relationship. The aggregation of all this relevant internal and external data requires appropriate controls to ensure completeness and accuracy.
5.4.2. Access Control

In 1992, Congress passed the Annunzio-Wylie Anti-Money Laundering Act which provides a safe harbor for financial institutions and their employees from civil liability for reporting known or suspected criminal offenses or suspicious activity by filing a SAR. In order to claim the safe harbor defense, the SAR information itself and the existence of a SAR should be given the highest Confidentiality rating. Because the Case Management application records not only the SAR information, but also the details of all investigations, the security and control over access to the application and the data it maintains is extremely important and should be subject to rigorous audit testing. It should also be remembered that even the existence of a SAR cannot be disclosed to unauthorized parties. The underlying documents supporting the SAR filing are not subject to the same restrictions.

Consideration should be given to including the following in the audit coverage:

1. Review the design of the security architecture of the case management application to ensure that it provides the opportunity for appropriate division of duties and separation of the various types of investigation. For example, access to the investigations of employee fraud should be very limited. Also, in the case of a population of investigators in different jurisdictions, it will be necessary to ensure that all local privacy laws are enforced through access control.
2. Access to US SAR information must be restricted to authorized users who are part of the same legal entity and also they must be physically present at a location within the US borders.
3. The case management database should be encrypted and access by Data Base Administrators should be under dual control - especially when database utilities are used to correct data errors.
4. Data transmissions and data backups must be encrypted.
5. Controls over the test data that is used, during the Change Management process, should be the same as for the production database. This is particularly important when the test data contains a copy of actual production data. It is often appropriate to carefully restrict access to the Development and Test environments and the source code of the application. This can also mean that, for FIs in the USA, the program coding and testing must be performed by personnel inside the US borders.
6. The administration of the users must be very effective and ensure that all access is appropriately approved and recertified. Users who leave or transfer must have their access promptly removed. It is important for the auditor to understand the consequences of a user being completely removed from the system because, in some systems, this can mean that the results of their work may also be removed.

5.4.3. Data Output

In the USA, this application will most probably be the source for filing the SARs, within the required timeframes, with FinCEN and this must be done electronically.
The integrity of this process, in all jurisdictions, with control totals and confirmation of receipt is crucial.

It is also very important to have an alternative filing facility in the event of a system failure.

5.4.4. Automated Auditing

Consideration should be given to designing audit tests in the following areas:

1. Incorrect values in certain fields such as:
   - Invalid product codes
   - Invalid country codes
   - Invalid currency codes
   - Invalid dates
   - Invalid workflow queue codes

2. Extracting a statistical sample of cases where a SAR was NOT filed to manually test that the documentation adequately supports the decision. This would include where the decision was made just before the end of the filing deadline.

3. Extracting a statistical sample of SARs filed to review the documentation supporting the investigation process.

4. Replicating the calculation of significant metrics, such as:
   - Investigations which are late and beyond the required time limits
   - Percentage of Alerts to Case
   - Percentage of Cases resulting in a SAR
   - Late SAR filings

5. Typically, a sequential control number will be automatically assigned to an alert entering the case management application. All items on a report of missing sequence numbers of Alerts and SAR’s filed should be reviewed and satisfactory explanations obtained.

It is very strongly recommended that copies of the SARs, which have been reviewed during the course of the audit work, and any related identifiable Personal Information about the subjects mentioned in the SAR’s are NOT stored in the audit workpapers.
6. Model Risk Management

On April 4th, 2011, the OCC published “Supervisory Guidance On Model Risk Management” which is referred to as OCC 2011-12. This section of the white paper represents a very high-level introduction to this Guidance; it is strongly recommended that all AML auditors study this document.

This Guidance defines a Model as follows:
“The term model refers to a quantitative method, system or approach that applies statistical, economic, financial or mathematical theories, techniques and assumptions to process input data into quantitative estimates.”

In recent times, the regulators have required that this Guidance be applied to the software that supports Sanctions Name Screening and Transaction Monitoring. It may also have to be applied to the functionality that provides an AML customer risk ranking, but this is outside the scope of this paper.

Whilst the Guidance addresses quantitative models, it also states that qualitative processes “should also be subject to a rigorous control process.”

It also states:
“Program code implementing the model should be subject to rigorous quality and change control procedures to ensure the code is correct and can only be altered by approved parties and all changes are logged and can be audited.”

Effectively, this Guidance requires a very high degree of formality and discipline over the development and change management processes. It, therefore, follows that this should be reflected in the audit coverage of these areas, both in depth and frequency.

The Guidance also defines Validation as:
“Validation involves a degree of independence from model development and use. Generally, validation should be done by people who are not responsible for development or use and do not have a stake in whether a model is determined to be valid.”

This effectively means that whilst the regular control processes must be “rigorous” in of themselves, there is a requirement for an independent group, which is separate from Internal Audit, to perform the validation work annually and to approve the original implementation and all subsequent material changes.
The Guidance clearly defines the rôle of Internal Audit as:

“Internal Audit’s rôle is not to duplicate model risk management activities. Instead, its rôle is to evaluate whether model risk management is comprehensive, rigorous, and effective.”

Consideration should be given to testing the following areas:

- The Model Inventory for completeness and accuracy. It should include all models, whether quantitative or qualitative. It would be beneficial if this list also included important attributes about each item, such as purpose, location, vendor name, date of last change, location of the report showing the last test results, and the date and report covering the last validation results.

- A comprehensive review of the change management process, including the quality of the documentation and the quality and rigour of the testing. The Guidance states that: “Material changes to models should also be subject to validation.” This not only includes the conventional changes to program code, but also changes to parameters in a software package acquired from a third party vendor. Therefore, the quality of the test data is very important. It is prudent, for the FI, to develop and retain a set of test data which is supplemented during each change to add data that is specifically designed to test that particular change. This approach can also ensure that data is included to “test below the thresholds” which is a requirement. This technique is often referred to as “Base Case Testing” and can be very efficient because data has been designed to exercise the important logic paths of the application and the results have already been pre-calculated. This test data and the related documentation and change management processes should be subject to audit review.

- Review the annual validation process by a group independent of the model developers and users and it may be appropriate for them to perform their work in a separate computer environment with their own test data. The auditor should also consider reviewing the qualifications of the personnel performing the validation work.

- Review all the emergency changes that have taken place to ensure that the controls have not been compromised. It may be appropriate for emergency changes to the program code to be made under dual control.

- The Guidance requires detailed documentation to be created, maintained and retained over all the processes which involve the models. The auditor should ensure conformance with this during all aspects of audit testing.

- Review and test the management reporting over the AML models, including that which is submitted to the Board of Directors, as required by the guidance.
7. Conclusion

It is hoped that this paper provides some useful high-level guidance which will enhance the effectiveness of the AML audit program and support the partnership between Operational and IT Audit. As the independent testing expectations continue to mature, IT Audit techniques can continue to provide an effective contribution to improve the efficiency and effectiveness of AML audit coverage.

The annual AML audit report, to the Board of Directors, is obviously a very important document which, apart from providing a summary of the audit results, could also include an opinion on the quality of the controls operating over the applications which play such a significant rôle in the effectiveness of the overall AML program.
8. References


2. The judgment in the UK court case of Kingston Cotton Mills Co. Ltd. in 1896.  
   http://books.google.co.uk/books?id=mEkzAQAAMAAJ&pg=PA445&lpg=PA445&dq=kingston+cotton+mills+co.+ltd&source=bl&ots=RdmvMwSadA&sig=X8cHvDhHTY8pfAa9f4HztfYUajY&hl=en&sa=X&ei=laMSU7mcE8bT0wGLloBA&ved=0CC8Q6AEwAjgU#v=onepage&q=kingston%20cotton%20mills%20co.%20ltd&f=false

3. OCC 2011-12, Supervisory Guidance on Model Risk Management  