Optimization of Technology to Meet Regulatory Expectations

Philip Tu, CAMS-FCI
# Table of Contents

I. Executive Summary ........................................................................................................... 1
II. Introduction .......................................................................................................................... 3
III. Cyber Security ................................................................................................................... 3
IV. Transaction Monitoring .................................................................................................... 4
V. Computer Assisted Auditing Technique (CAAT) ............................................................. 10
VI. Conclusion ........................................................................................................................ 12
VII. Appendices ...................................................................................................................... 13
      A. Works Cited .................................................................................................................... 13
I. Executive Summary

The once antiquated belief that big banks are invincible and above the law has now been mostly eradicated. This is largely attributed to corporate and financial entities within the past two decades that have failed miserably due to an outdated paradigm, but also to when they thought that rules and regulations do not apply to them. Banks have come to realize that if they are to operate in this heightened regulatory environment for the long haul, they are to remain dynamic and to continuously strive to evolve for the better. If not, inaction or lack of demonstration of ongoing improvements to adhere with current rules and regulations along with keeping up with industry standards and practices, will result in fines and penalties and ultimately their demise. Albeit the mammoth size of some financial institutions, banks need to be cognizant and determine if they can wittingly turn a blind eye, postpone addressing any noncompliance at hand and face the inevitable consequences at a later time.

Previously, a portion of the revenue generated from banks’ profits was utilized to outweigh any costs incurred from compliance and legal expenses. These allocated funds were taken out from what is known as the “war chest” to combat matters relating to regulatory noncompliance. This was a common practice across the financial sector and was seen as a favorable alternative to mitigate any lack of management oversight and staffs wrongdoing. The purpose of this was to protect the revenue generators (i.e., traders) that were well compensated for taking excessive risks. However, if this mentality and method to operate is allowed to persist, the situation may be exacerbated as time lapses and puts banks in a much more detrimental state. In addition, with the upward trend of monitorship tethered to banks by regulators, banks need to consider the long-term costs of regulatory noncompliance or employees’ negligence. Furthermore, the question of sustainability will come into play if banks need to maintain the increasing costs of hiring and maintaining the resources to manage these remediation efforts.

In the forefront of these changes to comply with regulatory expectations, is the need to invest in technology and particularly in transaction monitoring to ensure the capture of activities that may be deemed suspicious and warrant for suspicious activity report (SAR) filing. However, the challenge for many banks is determining the correct allocation of funds and investments towards which areas that are in the direst need of improvements.

The banks that will perform on an optimal scale in the next decade will be determined not only on their quarterly and annual results on profitability and uptick on share price, but more so to how they adapt and change to regulatory pressures to mitigate both inherent and residual risks. Further to this development, is to change a corporate culture that was once conducive to misconduct and behavior to one that fosters a compliant and collaborative mindset from all facets within a financial
institution. To achieve this feat, banks need to be accountable for any mishap and be reprimanded when there is a breach of adherence to rules and regulations or that of policies and procedures. Training needs to be targeted for misconduct and if noncompliance was to continue, repercussions may include an impact to compensation or staffs dismissal. If there are no consequences to staffs’ wrongdoing, then repeat offenders are given the liberty to do as they please with lack of supervision or oversight.

As ongoing employee training is one of the four pillars/elements to an effective anti-money laundering (AML) program, training needs to be targeted to staffs that are not adhering to policies and procedures.

The bar has been raised and shareholders are now not only looking to see increasing share prices, but to see which banks are able to stay out of the limelight from regulatory scrutiny. To achieve this, banks need to allocate adequate time and resources into technology (i.e., systems), compliance and audit. This will help them come out from the normalcy of responding and extinguishing out regulatory concerns and problems at the spur of the moment to the resolve of finding a long-term solution to remedy the problems at hand.

Many banks that are in their current predicament with fines and monitorships, are results of the failure to execute and follow through with a well-documented AML program, or on the contrary, failure to identify gaps/breaks with their current programs/controls and policies and procedures. Instead of identifying which controls are not operating effectively and need improvements, they over engineer a problem that is in need of simplification. The purpose of risk assessments or implementation of an adequate transaction monitoring system is to simply detect material risks that need to be mitigated and to unravel root causes of these key risks. The purpose of this white paper is for banks to actively seek assistance and allocate the adequate resources to either staffing or technology (i.e., systems) to perform on an optimal scale to meet regulatory expectations, if they are already not doing so.
II. Introduction
In the current heightened regulatory market environment, financial institutions need to be flexible, transformative and adaptive to an ever-changing and evolving regulatory landscape. To accomplish this, they need to assess as to whether existing resources are adequate, such as to meet regulatory expectations. Areas of focus will include whether they need to increase staffing levels or alternatively, increase efficiency with the utilization of technology and be less reliant on hiring additional staff. The underlying dilemma for banks to contemplate when combating financial crime and regulatory noncompliance is to determine whether to heavily invest in people or that of technology. Challenges will include finding a happy medium that is targeted toward areas in compliance, quality assurance and audit functions that need to make a determination as to whether to invest for the short term (quick fix) versus the long term (sustainability).

Before deciding as to which choice is the optimal selection, one first needs to understand what regulators are looking for that deem financial institutions to be in good standing/satisfactory with rules and regulations and at par with current industry standards and practices. The table below provides an overview of what regulators are looking for during their reviews relating to cyber security:

III. Cyber Security

<table>
<thead>
<tr>
<th>NY DFS: Cyber Sec Exam</th>
<th>Key State and Federal Cyber Security Regulators</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Corporate governance</td>
<td>State Attorneys General</td>
</tr>
<tr>
<td>• Cyber security process integration</td>
<td>FTC</td>
</tr>
<tr>
<td>• Resources - info sec, risk mgmt</td>
<td>CFPB</td>
</tr>
<tr>
<td>• Shared infrastructure risk</td>
<td>DHS</td>
</tr>
<tr>
<td>• Intrusion detection</td>
<td>HHS</td>
</tr>
<tr>
<td>• Authentication - multifactor</td>
<td>FCC</td>
</tr>
<tr>
<td>• Server and database configurations</td>
<td>Federal Prudential Regulators</td>
</tr>
<tr>
<td>• Testing, monitoring, pen-testing</td>
<td>State Prudential Regulators</td>
</tr>
</tbody>
</table>
With the heightening of cyber-crime, institutions need to consider not only increasing spending in technology (i.e., implementing governance framework), but also that of hiring adequate resources (i.e., information technology and compliance staffs) to safeguard against these types of attacks. The "responsibility for cyber security in financial firms is moving beyond IT departments and should include an advocacy and awareness role for compliance professional and an oversight role for boards, according to industry regulators experts."\(^6\)

In addition, as referenced by the Financial Industry Regulatory Authority (FINRA) around effective cyber security practices, it includes “dedicating resources to achieve the desired risk posture.”\(^7\)

With the proliferation of cyber threats, banks need to strategize and determine what the appropriate allocation of resources is needed to combat this heightened risk as it becomes pervasive across the financial industry. Playing defense and addressing cyber attacks after they occur are no longer sufficient or adequate in safeguarding banks. Instead, “to protect themselves, banks need to ensure they are investing appropriately not only in preventive controls, but also detective and response/resilient efforts. They need to create an overarching governance process and answer strategic decisions about what to build, buy, or outsource.”\(^8\) To accomplish this, banks need to strengthen their technology infrastructure and hire the right resources to ensure the following technical controls are in place and adequately tested.

<table>
<thead>
<tr>
<th>No.</th>
<th>Technical Controls(^7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Identify and assess management</td>
</tr>
<tr>
<td>2</td>
<td>Data encryption</td>
</tr>
<tr>
<td>3</td>
<td>Penetration testing</td>
</tr>
</tbody>
</table>

Furthermore, regulators such as FINRA are further reinforcing and advocating the need to fight cyber-crime and the Federal Reserve Bank of New York is also adding resources to strengthen their taskforce to manage the upward trend of cyber threats. During a keynote address at the OpRisk North America conference in New York (March 2015), Sarah J. Dahlgren, head of the Financial Institution Supervision Group at the Federal Reserve Bank of New York, deemed cyber threat “as the risk most likely to cause the next financial crisis.”\(^10\)

IV. Transaction Monitoring (TM)
Similarly, just as there is a necessity for institutions to strengthen their technology infrastructure and to assess their hiring needs, a comparative assessment needs to be made with transaction monitoring (TM). The onus falls with banks as albeit they may have a TM system in place, they need to periodically ascertain and confirm if there are adequate alerts being generated and whether those alerts are leading to SARs being filed with the Financial Crimes Enforcement Network (FinCEN). If there is a high volume of false positives (i.e., alerts) that do not result in SAR filing, this would be an indication that tuning of threshold values may be necessitated with the TM systems. If so, caution needs to be applied when making modifications to thresholds, because if they are set too high, this will severely reduce the number of alerts being generated. On the contrary, if thresholds are set too low, this will add to the surplus of false positives (alerts).

Keeping this in mind, there is a demand for banks to onboard staffs with the adequate skills set to probe into areas that are illogical and question the effectiveness of existing thresholds or detection scenarios. Below are examples of a few financial institutions that encountered challenges with their TM systems.

### Penalties/Fines and systems failure:

1. **SCB**: “300 million penalty by DFS”—TM systems failed to detect a “significant number of potentially ‘high risk transactions.’”\(^4\)

2. **Wachovia**: “Lacked adequate systems and controls to monitor transactions conducted by its international correspondent bank customers for potential money laundering or other suspicious activity. Wachovia’s automated transaction monitoring systems were inadequate to support the volume, scope, and nature of international money transfer transactions conducted by the bank.”\(^14\)

3. **RBS**: “Technology failure—600,000 missing payments after glitch”\(^13\)

4. **Bank Atlantic**: “Did not have adequate systems to monitor wire transfer operations for compliance with the suspicious activity reporting requirements.”\(^15\)

5. **Commerzbank AG**: “Weaknesses in its transaction monitoring system and failure to implement internal controls to appropriately manage risk relating to foreign correspondent banking business.”\(^16\)

### Root Causes
From the above examples, the root causes of the penalties/fines and systems failures may be attributed to the following:

A. Staff may not have the adequate skillsets for their roles and responsibilities
B. Lack of or incomplete policies and procedures with omission of key controls
C. Inadequate training or lack of training assessments to demonstrate staffs’ comprehension to current policies and procedures

Resolution: Increase Staffing with Adequate Skillsets
In the current heightened regulatory environment, banks need to bear in mind that although there is a high demand (i.e., price/cost) for seasoned staff who specialize in alert investigations, compliance, SAR writing or audit, the following needs to be factored in for consideration.

Cost/Benefit Analysis and Short Term versus Long Term (Sustainability)
1. Invest in staff for the long haul for sustainability versus hiring consultants and temporary workers who leave after one year without the transfer of knowledge
2. Hire local staff versus staff sitting in hubs or the parent office that is offshore
   ➢ IT supports staff to assist in the current time zone
3. Input a capacity plan to anticipate an uptick of transactions/alerts
4. Discuss with business to determine if de-risking is feasible or optimal
   ➢ Pros and cons of time spent vetting a high-risk client/high-risk locale/high-risk product versus not onboarding the client or exiting the client account/relationship
5. Invest in staff that are performing in the top percentile

In addition to contemplating about increasing staffing levels, keep in mind that compliance-related costs fall under regulatory costs and further elaborated below by the Organization for Economic Cooperation and Development (OECD).

Regulatory Costs
“The term ‘regulatory costs,’ as used by the OECD, embraces all of the costs attributable to the adoption of a regulatory requirement, whether direct or indirect in nature and whether borne by business, consumers, government and its respective authorities (i.e., taxpayers) or other groups. The figure below sets out a taxonomy of regulatory costs.”
Albeit there is a high demand and short supply of compliance/audit staff, which in turn drives up the hiring cost, there is no exception to the rule as per the FFIEC BSA/AML Exam Manual, which states the following:

“The bank should assign adequate staff to the identification, evaluation, and reporting of potentially suspicious activities, taking into accounts the bank's overall risk profile and the volume of transactions. Additionally, a bank should ensure that the assigned staff possess the requisite experience levels and are provided with comprehensive and ongoing training to maintain their expertise. Staff should also be provided with sufficient internal and external tools to allow them to properly research activities and formulate conclusions.”

When there is confirmation that the underlying cost for compliance/regulatory costs has been budgeted and approved, the next forward action is to ascertain that there are resources to adequately complete checks to make sure what information from the source systems are published
adequately to the TM systems such as Detica, Mantas, or Actimize. Technology can only be optimized to meet regulatory expectations when there is validation that information going into the TM systems is complete and accurate.

Referencing from the Wolfsberg Group statement on *AML Screening, Monitoring and Searching (2009)* around the automated transaction monitoring systems, one of the focuses was to maintain a risk-based approach (RBA).

**RBA (Wolfsberg)\(^{19}\)**

“Risk profiles will vary between financial institutions and also between business units within an institution depending on the products and service offered by each (i.e., retail, private banking, correspondent banking, broker dealer etc.). The framework used to monitor transactions should reflect this risk assessment with greater attention focused on those business areas and types of activity considered to represent the highest risk.”

In addition, the Financial Action Task Force (FATF) also touches on this subject.

**RBA (FATF)\(^{24}\)**

“[An] RBA to AML/CFT means that countries, competent authorities and financial institutions, are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively.”

Taking the Wolfsberg Group statement and FATF Guidance for an RBA into account, careful attention should be placed on both the IT person responsible for the system changes and also that of the alert investigator reviewing alerts subsequent to any threshold tuning/changes. An assessment should be made as to whether both parties understand their roles and responsibilities.

Diagram A (see below) suggests that any threshold tuning, should also incorporate a qualitative component. This is essential to ensure the optimization of technology as alerts are reviewed to incorporate the following:\(^{11}\)

- **Customer Data** – “Investigators should have access to customer data attributes necessary to understand the customer’s background and business or banking activities.” This may include:
  - ✓ Name
  - ✓ Address
  - ✓ Occupation or industry
  - ✓ Entity type (partnership, limited liability corporation, corporation, trust, private investment company)
  - ✓ Income
• **Account Data** – “Investigators should have access to the account data necessary to understand the nature of the account, as well as the identifies of individuals or entities that have access to, influence over or an interest in the account.”

• **Transaction data** – “Investigators should have access to the transaction data necessary to understand the nature of the transactions being reviewed.”

• **Prior SARs** – “Knowledge of prior SAR filings in relation to the customer or a customer’s account will aid in determining the effectiveness of alerts being reviewed by investigators. Alerts of customers or accounts with previous SAR filings may be viewed as more effective than alerts for customers or accounts with no such previous filings.”

• **Prior alerts** – “An understanding or prior alerting activity and alert dispositions will aid in understanding the kinds of activity that have been subject to previous review and to assist in determining the effectiveness of alerts being reviewed by investigators. Recurring alerts for repeated, non-suspicious activity may be viewed as less effective than alerts for different potentially suspicious behaviors.”

Threshold Tuning of TM Systems
Quantitative versus Qualitative Approach (Diagram A11):

---

Regulatory Expectations

“To ensure the integrity of the data, tune/ enhance monitoring scenarios, and validate the effectiveness of the systems on an ongoing basis.”

Institutions need to ascertain if their current systems (i.e., transaction monitoring) are reliable and operating in accordance to their intended design and purpose. Examples of recent bank penalties and fines were not only a result of whether the bank had a system (i.e., transaction monitoring) in place, but more so if the system was operating effectively to generating adequate alerts to identifying suspicious activity. Learning from these bank penalties, “the company’s systems must be independently tested for accuracy, use reasonable filtering criteria and generate monitoring reports that identify unusual activity.”

Below are checks that institutions can test to ascertain if they have controls in place to address the following or whether their systems (i.e. transaction monitoring) are operating effectively. As there is currently an upward trend of dependence on automated TM systems to meet regulatory expectations, assurance and trust on their completeness and accuracy must first be validated internally.
<table>
<thead>
<tr>
<th>No.</th>
<th>Systems/Technology Checks: Transaction Monitoring²</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ongoing validation of the transaction monitoring system (including recalibration of scenarios based on lessons learned from SARs filed) and the end-to-end process.</td>
</tr>
<tr>
<td>2</td>
<td>Developing and executing a sound and efficient scenario tuning methodology and approach.</td>
</tr>
<tr>
<td>3</td>
<td>Performing AML red flag gap analysis/ worst-case scenario analysis, data validation, scenario logic validation, customer segmentation validation.</td>
</tr>
<tr>
<td>4</td>
<td>Recommending improvements to scenarios/thresholds.</td>
</tr>
<tr>
<td>5</td>
<td>Periodically reviewing AML transaction monitoring systems and functions to determine if enhancements are needed.</td>
</tr>
<tr>
<td>6</td>
<td>Assessing current organizational structure and control framework, designing a target operating model, developing policies and procedures, and evaluating and enhancing detection scenarios.</td>
</tr>
<tr>
<td>7</td>
<td>Identifying source systems and transaction codes, ensuring accurate data feeds, selecting scenarios aligned to the institution's risks, performing quantitative analysis to calibrate the systems, using the analyses and available KYC data to segment the customer base in a meaningful manner, and testing the output and effectiveness of the generated alerts to drive further recalibration of the thresholds and scenarios.</td>
</tr>
<tr>
<td>8</td>
<td>Having adequate policies and procedures and experienced personnel to investigate the alerts generated by the transaction monitoring system.</td>
</tr>
<tr>
<td>9</td>
<td>Generating effective scenarios that highlight unusual activity, to assist in pre-emptively identifying activity that may later be flagged and referred by law enforcement.</td>
</tr>
<tr>
<td>10</td>
<td>Documenting a robust tuning methodology (inclusive of change control documentation and rationale for tuning) that is acceptable to regulators.</td>
</tr>
<tr>
<td>11</td>
<td>Achieving global consistency - For larger institutions with a global footprint, ensuring each region as hired the right people, implemented adequate detection scenarios and instituted strong controls to manage the end-to-end transaction monitoring process has become a significant challenge. This is due to geographical distance from the head office, differences in regulatory requirements, and misinterpretation of regulations and/or internal policies and procedures.</td>
</tr>
</tbody>
</table>

V. Computer Assisted Auditing Technique (CAAT)¹⁸, ²⁰, ²²

There has been an upward trend to utilize data analytics (CAATs) to assist with audit work across the industry. One of the drivers for this transformation stems from the need to
meet regulatory expectations and to give assurance that testing is less prescriptive and more risk based. 

From a maturity level of where banks are at with the utilization of data analytics, the average scoring (rating) has been at around two or three with five being at the highest level of maturity. SCB is currently at a one or two maturity level rating given that the bank is still at its infancy with the implementation/utilization of CAATs. However, the bank hopes to increase utilization of CAATs from 1 percent to 10 percent globally across the network in the foreseeable future.

PwC utilizes Tableau and Spotfire (visual analytics tool) to assist with their testing and transferring voluminous amount of data to dashboards to assist with information analysis and queries. Below are some of the key items derived from the meeting with PwC and their analytics team.

A. **Demo 1: Journal Entries**
   - With the utilization of Tableau, able to transfer information from Excel documents to dashboards to perform the following:
     - Data completeness checks (before and after amounts) such as expected versus actual amounts/figures or beginning/ending balances
     - Queries can be run directly from the dashboards in Tableau with the flexibility for customization

B. **Demo 2: Mortgage Activity (Lending and Loan Work)**
   - With the utilization of Tableau, able to visually see mortgages’ cycle time (turnaround time of mortgages/applications) through graphs, charts and diagrams. Examples include the following:
     - Case Loads: How long it takes to complete loan applications
     - Fall out: Provide stats as to how many days have lapsed for loan applications that were not filed timely or within the average loan processing time
     - Top 10 contributors (staff): Resulting in delays to loans not being processed on time stemming from which areas/functions

1. To optimize the utilization of CAATs, perhaps to consider CAATs planning at least three months prior to actual planning of the audit. Assist in the following areas, but not limited to:
   A. Data profiling: Determine which information is pertinent versus those that are not
   B. Data integrity: Validation that data is complete and accurate
   C. Risk assessment: Identification of key risks or areas of concern/materiality
   D. Not limited to audit: Utilization of CAATs to optimize technology to meet regulatory expectations is transferrable and can be applied and utilized in compliance and other functions.
2. CAATs improve efficiency with the reduction of not only time and resources, but reduction of false positives
   A. This is advantageous when reviewing millions of transactions and line items
   B. Improve future audit time such as the following, but not limited to:
      - Reduce control testing in areas where there is minimal risk/impact
      - Reduce from a 100 percent sampling to a limited sampling methodology
   C. Focus on areas of heightened risks
   D. With the incorporation of CAATs, consider updating/transforming audit methodology on an ongoing (dynamic) basis to define what is deemed adequate (sample size) for testing

3. Consideration for having a U.S.-based CAATs support team to assist with the following:
   A. Identification of any illogical outliers (i.e., inaccurate exclusion logic) and provide feedback with a quick turnaround time (TAT) to perform the following:
      - Fine tune (recalibrate) the CAATs testing to create output/analysis before end of fieldwork
      - Mitigate any CAAT testing that may not be relevant for re-evaluation or to test during fieldwork

4. Albeit CAAT testing may be developed by audit, at the discretion of the audit function, they may share that information with the business or the second line, but be cognizant of the following:
   A. The business/second line needs to refresh the data to ensure there are controls to address the identified risks
   B. Ensure audit’s independence so that it does not result in owning the risk or performing updates to monitor the risk. The onus falls with the business/second line and audit will review this during their annual or periodic testing/audit work.

5. Utilize visual analytics tool (business analytics software) to help create dashboards and queries when analyzing large volume of data and below are the top three tools that are commonly used in the industry.
   A. Tableau
   B. Spotfire
   C. QlikView
VI. Conclusion

The purpose of this white paper was to present to the reader that combating financial crime and money laundering activity is constantly evolving and financial institutions need to be one step ahead of the game. With the optimization/utilization of technology, we hope to not only meet regulatory expectations, but to proactively prevent crime from taking place regardless of its locale. Taking into account the RBA guidance from the Wolfsberg Group and FATF, our methods of reviewing transactions, alerts and detection scenarios (along with codes, rulebook and typologies) should always be dynamic and amended according to any changes that coincide with the customers’ risk profile.

As money launderers and terrorists become more sophisticated, banks need to revaluate their risk appetite on a more frequent basis to determine as to whether they remain comfortable with the inherent risks at hand or of any residual risks that may need to be reexamined. If so, financial institutions need to be ready to make a determination as to whether to strengthen their current technology/TM systems, de-risk/exit certain high-risk customer base, hire additional staffs with the adequate skills set or provide targeted training to those that may need them. Regardless of the course of action, investments and allocation of resources still need to be made toward technology/systems or staff to help continue the combat against financial crime, money launderers and terrorists.
Works Cited

1. Cyber security Assessment – What Will the Regulators Be Looking For?  
   Buckley Sandler LLP – Digital Commerce & Payments Series Webinar  
   March 18, 2015  
   http://www.buckleysandler.com/uploads/1082/doc/BuckleySandler_Webinar- 
   Cybersecurity_Assessment_03.18.150.pdf

2. The Importance of a Strong AML Transaction Monitoring Governance Framework in Today's Regulatory  
   Environment  
   Protiviti  
   Framework-Protiviti.pdf

3. AML & Regulatory Compliance  
   K2 Intelligence – Our Services  
   https://www.k2intelligence.com/our-services/aml-regulatory-compliance/

4. Standard Chartered’s AML lapses provide crucial lessons on Internal Controls  
   Reuters – Financial Regulatory Forum  
   s-aml-lapses-provide-crucial-lessons-on-internal-controls/

5. The Internal Audit Analytics Conundrum – Finding your path Through Data  
   PwC – December 2013  
   http://www.pwc.com/us/en/risk-assurance-services/publications/assets/pwc-internal-audit-analytics- 
   data.pdf

6. Cyber security responsibility in firms widens to boards, compliance - U.S. regulators and experts  
   Complinet – Thomson Reuters Regulatory Intelligence by Emmanuel Olaoye, July 21, 2015

   FINRA – February 2015  

   Deloitte – 2015 (pg. 11)

9. As field of U.S. cyber security regulators thickens, some navigation tips  
   Complinet – Thomson Reuters Regulatory Intelligence by Julie DiMauro, July 8, 2015

10. NY Fed’s new cyber taskforce dismissed as “distraction”  
    Operational Risk & Regulation – March 24, 2015
11. Improve Threshold Values Tuning of Transaction Monitoring Systems by taking a Qualitative Approach
Protiviti

12. JP Morgan's new approach to probing suspect transactions sparks internal friction
http://www.reuters.com/article/2015/02/12/us-jpmorgan-antimoneylaundering-insight-idUSKBN0LG0D220150212

13. RBS could take until weekend to make 600,000 missing payments after glitch
The Guardian.com – by Sean Farrell and Carmen Fishwick: June 17, 2015

14. FinCEN Assessment of Civil Money Penalty In the Matter of Wachovia Bank
March 12, 2010

15. FinCEN Assessment of Civil Money Penalty In the Matter of Bank Atlantic
April 26, 2006

16. New York State Department of Financial Services In the Matter of Commerzbank, AG
March 2015
http://www.dfs.ny.gov/about/ea/ea150312.pdf

17. OECD Regulatory Compliance cost Assessment Guidance
2014
http://www.oecd-ilibrary.org/docserver/download/4214101e.pdf?expires=1441402705&id=id&accname=guest&checksum=E68A240206542D2488F7D0931517928E

18. Avoiding the drift – Optimizing and maintaining AML Surveillance Programs
PwC – October 2013

The Wolfsberg Group

20. The Internal Audit Analytics Conundrum – Finding your path through data
PwC - 2013
21. AML Topics Using Analytics to get the most from your transaction monitoring system  
PwC – March 2011  

22. Data analytics: How data analytics can help internal audit better understand risk  
PwC - 2012  

23. FFIEC – Federal Financial Institutions Examination Council Bank Secrecy Act / Anti-Money Laundering Info Base  
BSA/ AML Exam Manual  

24. Guidance For a Risk-Based Approach – The Banking Sector  
FATF – October 2014  

25. Consulting firms specializing in regulatory compliance  
• PwC, Protiviti, K2 Intelligence, Madison Consulting Group and KPMG