Automation of BSA/AML Activities

Dave Dekkers – November 2013

Abstract
This paper highlights the possibilities regarding automation of BSA/AML activities. Automation helps take the pain out of labor intensive BSA/AML activities. This paper describes how to leverage automation and presents an overview of rationale, effective approaches, efficiency gains and advice to consider when automating BSA/AML activities.
EXECUTIVE SUMMARY

BSA/AML activities are seen as a necessary burden by many financial institutions due to the labor intensive nature of the work and the high costs. A key strategy regarding BSA/AML compliance activities should be to improve efficiency whilst fulfilling audit and regulatory requirements. This white paper will introduce aspects of automation of BSA/AML activities to improve accuracy, efficiency and effectiveness.

Regulatory pressure is building on BSA/AML officers as governmental efforts to reduce terrorism, crime and tax evasion increase. The growing demand for more information and increased scrutiny of customer activity are a daily challenge with executing BSA/AML compliance activities. Non-compliance leads to high fines being levied and occurs almost on a regular basis.

Keeping up with the information demand from both internal and external stakeholders leaves BSA/AML officers time-strapped and anxious to find better ways (to comply). Typical solutions to getting more done in less time include better time-management, more (experienced) staff, better tools and automation. When the Patriot Act was enacted, the development and implementation of BSA/AML tools increased significantly, and many viable automated solutions are available today. With so many to choose from, the importance of how and when to apply them is even more essential, as this requires insight into the specific business processes being utilized and the goals to achieve compliance.

This white paper will highlight some of the possibilities in advancing the BSA/AML officer’s and overall compliance functions, to be more effective in their choice of what functions to automate and how to maintain adequate control over the data being analyzed. This white paper provides some concise approaches that can be used to develop a more efficient BSA/AML operation in a multi-phased model approach which will certainly provide a competitive edge to compliance.

At the same time, the goal of this white paper is to provide suggestions that make (automated) BSA/AML activities significantly easier to audit and incrementally improve monitoring and compliance.

By improving an institution’s automation, they are able to develop more effective and efficient ways to deliver accurate and timely information to stakeholders and decision makers. Obtaining and assessing trends from the very beginning will provide an insight to criminal activity and possibly an edge over competitors, allowing an institution to more quickly prepare and change processes to reduce the impact from these types of transactions.

1 The Global Cost of Anti-Money Laundering Compliance (see Sources / Work Cited)
BACKGROUND

Many BSA/AML officers are faced with a daily challenge to maintain awareness of and comply with the applicable laws and regulations, follow up on activities that are odd in nature (suspicious activity), reporting to and informing senior management and the Board of activity, and keeping other departments from launching potentially risky or non-compliant products or services.

As time management definitely helps with controlling these demanding functions, automation can really help BSA/AML officers be much more effective in what they do. Automation in the context of this white paper is something completely different than implementing a couple of information systems to do the work, as automation needs to provide actionable results.

This white paper highlights the possibilities to improving the BSA/AML officer functions, by helping them make the right decisions on what to automate and how to maintain adequate control, particularly related to auditability and improving audit review results.

In this white paper the focus is on automating BSA/AML officer activities in the following categories:

- **Pillar I – Customer – Verification & Validation**
  - Customer Identification
  - Customer Due Diligence
  - Ongoing Validation

- **Pillar II – Customer Behavior – Verification & Validation**
  - Transaction Monitoring
  - Sanction / Terrorist Finance Filtering
  - Behavior Monitoring
  - Risk Assessments
  - Enhanced Due Diligence

- **Pillar III – Reporting**
  - Regulatory Reporting
  - Management Reporting
  - Dashboards

- **Pillar IV – Strengthen your BSA/AML operations**

Each of the above categories will be reviewed and the types of automation possibilities are described below. The automation should also fulfill the requirement to keep the automation auditable, so the BSA/AML officer remains in control.

---

2 BSA/AML Compliance Program—Overview (see Sources / Work Cited)
SOLUTIONS FOR AUTOMATION OF BSA/AML ACTIVITIES

This white paper will not provide a “one-size-fits-all” solution. What this white paper will provide, is a good overview on what can be automated in the BSA/AML context and provide valuable insights into selecting the (nearly) perfect approach in handling your specific daily BSA/AML challenges with automation.

PILLAR I: PERSONAL IDENTIFICATION INFORMATION AND VALIDATION

The first activity that can be automated for increased efficiency is Know Your Customer (KYC). KYC activities can be split into several steps that can be automated in a state machine (SM) to assist in finding anomalies.

Customer Identification

Automation in customer identification requires thorough knowledge of the laws to adhere to, as these requirements will strongly determine the kind of solutions to apply. Automation should be used to reduce manual work to an absolute minimum. In respect to customer identification, that means that customers provide the information electronically and SM automation will perform the essential validations (against, for example, blacklists and lost-and-found archives). The highlighted results of the validation will be reviewed by BSA/AML professionals.

The described steps create a much more cost efficient and more customer friendly (paced) process (in both speed and availability). Another positive side effect is that the activity --registration and validation-- is electronically registered as well, to comply with audit requirements.

The audit requirements for Customer Due Diligence rely particularly on the authenticity, completeness and the validation that took place. The policies, procedures and processes can be enforced through automation as well. During validation and completeness checks, findings are logged, corrected and monitored. Customers are automatically notified when certain information is not yet provided. Automated reminders make your follow up activities more effective and faster, more efficient and less labor intensive, as well as result in more accurate information.

Customer Due Diligence

Customer Due Diligence’s (CDD) purpose is to make sure that the gathered information accurately represents the customer. Recommendations given by the Financial Action Task Force (FATF) stipulate validations to be done by utilizing independent sources. Electronically linking to services for validation purposes is a convenient and efficient manner to validate the details received from a customer. Validation services are executed as steps in a state-based machine to automate the customer due diligence processes.

Further automation is possible (in some countries) by deferred identification, which relies on an identification payment made from an existing account at another bank to the “virtual” new account with the “new” bank. When the identification payment does not result in a match between names, an action is generated to follow up with the customer. Automation of verifying missing details can be taken to the level of auto-blocking the new account if certain information is not provided, or by sending automatic reminders to both customer and bank staff. Automation makes CDD much more efficient, less laborious and customer friendly.

Auditors challenge the adequate validation of identification. Automation helps enormously as long as the automated process:

- Collect facts.
- Makes precise and accurate decisions based on the collected factual information.
• Records the performed steps.
• Provides automated conclusions for validation by investigators.

Sanction / Terrorist Finance / PEPs Filtering of Customers

An essential part of your BSA/AML program and customer due diligence processing is the validation of the customer information against sanction lists. Politically Exposed Persons (PEPs) have received more attention in European and Asian countries, due to corruption and transparency laws.

Automating the validation of potential customers against sanction entities lists and PEPs lists is done by list filtering solutions. The moment matches are found between names on the sanctions list and one of your prospective customers, an alert is created that requires investigation.

Automated list filtering solutions save a lot of time and make the name comparison more objective. The efficiency gain and labor intensiveness can be improved further by higher quality and contextual customer information in combination with high quality watch lists.

The list filtering solution should document all of the matched records, even though the matches might not have “qualified” for the BSA/AML officer to take a look at them (false positives). The importance of this information is crucial when validating if a correct comparison was made, and when fine-tuning the list filtering engine to find the balance between reducing the number of false positives and avoiding false negatives.

Auditors play a key role in challenging the choices made when configuring the list-filtering algorithms in order to comply with regulations. Answering the questions of auditors will also better prepare you for the examination by regulators.

Ongoing Validation

Ongoing validation of changes with respect to customers is important in protecting an organization from surprises. Certain events can impact customers good or bad so it is important to review all customers against the earlier mentioned Sanction Entities Lists and PEPs lists on a periodic basis. As far as the automation of ongoing validation, the same principles apply as for the initial validation.

Historical recordkeeping in relation to ongoing validation can help creation of white lists to help to reduce the number of false positives, by means of validated exempts.
In online banking, banks are forced by legal requirements to make sure that new customers are actually who the customers claim to be (throughout their relation). To validate the customers’ identity and “innocence” a number of automated monitoring activities can be implemented, protecting the banks reputation, but also the customer from being compromised: for example account takeovers.

Transaction Monitoring

Automated transaction monitoring solutions can help BSA/AML officers to monitor customer’s activity. Automation can perform the laborious work of reviewing transactions in a quick and efficient manner, no matter how many transactions. From experience, implementing transaction monitoring is best accomplished with the following strategies:

- Use standardized solutions
- Start small, build out only when there is enough experience to take it to the next level
- Slowly add more scenarios where you see fit
- Discuss monitoring scenarios with peers
- Learn from experiences and cases that have happened
- Build statistics on the number of alerts, to determine non-performing scenarios
- Trends pass which makes monitoring a constant evolution
- Adhere to the guidance set out for model risk management

The challenge with transaction monitoring is that criminals regularly change their modus operandi to not get caught. When selecting an automated transaction monitoring solution make sure it has the features and flexibility to keep up with trends and changes in criminals’ techniques.

Learning a new solution requires adaption, due to different methodologies, algorithms and techniques. Staying flexible, to learn and adapt where necessary to build better insights on how the solution work to identify these changes.

A transaction monitoring audit begins with reviewing inter-agency guidance, as well as any earlier legislator feedback and ensuring that improvements are correctly and sufficiently implemented. Auditors will keep a keen eye on any required best practice pattern available. Also, legislators will monitor if it is used in the right context and that future legislation can be covered quickly.

Sanction / Terrorist Financing Monitoring of Transactions

List Filtering should be automated for the screening of incoming and outgoing transactions against sanctioned and terrorist entities. List filtering solutions will provide important protection against regulatory fines, and good solutions will provide detailed recordkeeping of the activities. Some solutions allow further automating the list filtering by supporting construction of specific list filtering rules built on additional intelligence and experience when dealing with e.g. particular lists, countries and/or currencies. The automation examples allow your bank to maintain a higher level of automation without human intervention, so-called straight-through-processing.

---

3 Supervisory Guidance on Model Risk Management (see Sources / Work Cited)
Bribery and corruption laws across the globe further dictate screening transactions against lists of Politically Exposed Persons. Many BSA/AML officers tend to ignore it as it is not yet a legal requirement in all countries, but (knowingly) facilitating bribery and corruption will harm a bank’s reputation.

Auditors place much scrutiny on the list filtering algorithms results as it is very important not to have any false negatives. If regulators find a false negative, expect to meet extreme focus on your algorithms and in-depth analysis. As such, be prepared for some very specific and detailed questions that you need to answer in equal detail, a process that will cost a lot of extra time.

**Behavior Monitoring**

Behavior monitoring looks at the customer’s details, activities – both financial and non-financial – and compare that with expected activity. Behavior monitoring will provide the best opportunity to find suspicious activity as long as there is sufficient focus on the following matters:

- Data quality will strongly influence accuracy of the analysis results
- Change in behavior can occur due to seasonal influences – know what periods are vulnerable or have a higher chance for false positives
- Different geographical regions have different behaviors (e.g. preferred payment means)
- Look for unexpected patterns and fluctuations in relationships between accounts and/or customers (to find money mules, account takeover fraud, layering and concealment of funds)
- Compare apples with apples, not apples with oranges, as categorization is key in monitoring
- Is your behavior monitoring explainable to an auditor or regulator (no black box approach)?

Automating the monitoring of customer’s behavior is done with statistical, neural networking and all sorts of other methodologies to determine suspicious behavior. When selecting a vendor for behavior monitoring consider the following takeaways:

- Do not be afraid to ask more than you would need today, this is a long-term investment
- Ask their reference customers to fill in a pre-defined list of questions, to get a more structured discussion and avoid getting sidetracked.
- Be aware of tie-ins that might cost you dearly
- Does it sufficiently support the automation of BSA/AML activities that you envision (e.g. auto filling of standardize reporting and legal documents)?
- When considering on-premises solutions or Cloud services:
  - Consider and search for hidden costs (during setup, running and departure of cloud strategy)
  - Consider privacy (of the bank and its customers)
  - Consider quality and uptime
- Can you share the investment with other stakeholders? For example: Fraud and BSA/AML are other sides of the same medal.
- Is your solution future proof, is it flexible enough to handle upcoming changes in your infrastructure, products and services, and even more important the ever-changing laws and regulations?

As customer behavior monitoring relies on profiles (aggregates) built through time, auditing is relatively limited in what you can do. The only manner to make sure if the customer behavior profile is correct is by performing model validation. Model validation can be done by hand, which is very labor intensive, or by applying a number of automated steps to make validation efficient:

- Request the BSA/AML solution provide the logic behind the profile (aggregation process).
- Obtain or create a tool that is able to apply the logic of the profiling based on a number of (to be profiled) activities.
To validate the “end” state of a profile, be sure to provide the activities that are profiled in correct date sequence and reverse data sequence. Both should lead to the same results.

- Make sure to do at least five validations in a manual way, to avoid the situation where the tool to validate the model, has its own deficiencies.
- The steps to validate the model can be re-used by auditors if a larger set of profiles needs to be validated.

Risk Assessments

In automated BSA/AML solutions, risk matrices can be a powerful tool to highlight high-risk customers. Please consider the following topics:

- Consider the following areas when making a risk matrix: customers, transactions, geography, products and employees
- Other points of interest are historical risk scores and changes in customer details
- Use risk scores to set priority of generated alerts
- Use risk scores as a filter in your Enhanced Due Diligence process
- Validate risk matrices at least every quarter
- Automation of risk scoring saves a lot of time and allows more frequent re-evaluation and to build a better view on the risk related to the bank’s customers

Auditors can use risk matrices to determine how risks are assessed, as risk matrices are objective and very transparent. Auditors and regulators that are provided with a report of changes to the risk matrices and the results that were produced are more likely to be positive about your BSA/AML activities.

Enhanced Due Diligence

Enhanced Due Diligence (EDD) lends itself for SM automation as typical validation steps can be automated using already available data or validation services. Add to that the logging of these validation steps onto a customer’s risk profile, and you build a wealth of information which can be effectively and efficiently used in decision taking by an analyst.
PILLAR III – REPORTING

Reporting is a required and essential part of your communication to management, auditors and regulators with a concise status about the BSA/AML activities. The information provided is the basis for their decisions, so make sure the reporting is accurate.

Regulatory Reporting

Regulatory reporting allows for extensive automation because:

- The high degree of standardization of the regulatory reporting;
- The information needed for the regulatory report is available from the case investigation in the monitoring solution, as well as your narrative.

Automating regulatory reporting enables:

- Reduction of errors;
- Speeding up the completion of the investigative process;
- Enhancing the quality of the regulatory report (by validating the reporting for missing information).

Auditing of regulatory reports focuses particularly if the fields are being filled in properly and if there are internal guidelines that enforce:

- Writing good narratives on the suspicious activity;
- Complete and verified evidence supporting the narrative;
- A clear log of time and activities.

An important lesson that can be learned from requests for additional information is how to improve your reporting to regulatory bodies.

Management Reporting

Management reporting is used to inform colleagues and senior management about BSA/AML details of activity on a periodic or ad-hoc basis. Operation departments want to have reports about payments that have been blocked or put on hold, statistics and reasons around the activities.

As the goal of automation in BSA/AML activities is to remove unnecessary distraction and offload relatively simple activities. Take these points to maximum returns from your reporting automation:

- Summarize the information to report on, by whom, how to obtain it, how often/periodic it is requested.
- Per department, validate if that is the required reporting, and if there are additional reporting requirements.
- Are available reporting tools proficient?
- Define a priority list of reports.

Reports are required in each organization and the reporting solutions are typically available to produce these required reports. Many BSA/AML solutions come with standardized reporting that meets the needs at a very basic level. Ask vendors how reports can be easily customized to fit the organization’s needs.
Auditors will request insight where reports are based on, the reason for the report, who is able to view the information and if it is allowed to link information together. Please consider these types of questions when using reports of automation of BSA/AML activities, and write down the answers to these questions in reporting requirements or supporting documents.

**Dashboards**

Reporting in many circumstances, is often not frequent enough to provide senior management with sufficient information on which to base their compliance and processing decisions. Most departments require just simple overviews; while others might need more detailed and comprehensive data.

Dashboards allow for quick consumption of information if there is a high demand on getting current but high level statistics on BSA/AML activity. Dashboards reduce time BSA/AML staff needs to spend on preparing reports.
PILLAR IV – STRENGTHENING THE BSA/AML OPERATIONS

BSA/AML officers are required to educate themselves with the latest criminal activity, schemes and techniques used to launder money or perform other financial crimes. BSA/AML officers must educate and create awareness throughout their organization about the risks their financial institution faces.

Training of the BSA/AML teams

Constant training and awareness verification are essential in keeping up with the latest developments, so BSA/AML team members need to participate in training and industry events like:

- Conferences / Webinars
- Local Chapter / Peer meetings
- Risk Meetings
- Awareness sessions with other teams / departments

Training staff is very important to ensure that regulations are met while helping staff to better handle challenging BSA/AML operations. Producing quality training is labor and time intensive, as well as providing the training. Automation in the form of computer-based training and webinar subscriptions ensures that training is received in a consistent manner, while giving staff the freedom to follow training at their own pace and convenience. Another advance of providing computer-based training or video-based training is that you can test staff at the end of the training. Such a questionnaire provides feedback on their competence level or quality of the training. To comply with legislation, auditors will request records of adequate training and awareness sessions to prove the up-to-date skill-set of the BSA/AML staff.
CONCLUSION

Why Automate BSA/AML Activities?

Automation of BSA/AML activities is essential in protecting the reputation of financial institutions, while creating a much more structured method of dealing with BSA/AML activities. The level of success of the automation of monitoring the BSA/AML activity and the quality of the results is directly dependent on a number of factors:

- The extent of automation that is actually possible for a particular activity
- The reduction of manual labor by automated analysis and categorization;
- The quality of the results of the BSA/AML activities automation;
- The price of the BSA/AML automation;
- The remaining amount of manual work after the automation has been performed.

Steps to build the solid foundations of successful automation of BSA/AML activities are:

- Describe what can and needs to be automated and how that should be done to obtain the required results.
- Identify maximum effectiveness of your investments and where it allows for a continuous process without human intervention.
- Build in quality measures for source information.
- Describe quality gains due to better decision information for the investigators.
- Validate all of the automated results to assure optimal reliability and high quality reporting.
- Maximize transparency in activities and decisions.

Automation auditability

An extremely important factor in successful automation of BSA/AML activities is being able to explain how you came to certain (if not all) results and what you did with the obtained results. Especially detailing the how, why, what, when and where will provide you with enormous advantages when dealing with auditors and regulators. Having clearly documented your automated BSA/AML processes will allow you and your organization to:

- Validate completeness of your controls;
- Validate correctness of your BSA/AML automation for reliable results;
- Show understanding and (correct) interpretation of internal guidelines and regulations;
- Increase effectiveness of your organization.

Without automation of AML/BSA activities you will find yourself, reducing your ability to be accurate, efficient and effective in an effort to handling your day-to-day tasks.
BSA/AML Compliance Program—Overview (online manual)
Link: http://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_007.htm

Supervisory Guidance on Model Risk Management

The Global Cost of Anti-Money Laundering Compliance
Author: Sven Stumbauer - Managing Director - Veris Consulting, Inc.

<table>
<thead>
<tr>
<th>GLOSSARY</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSA / AML</td>
<td>Bank Secrecy Act / Anti-Money Laundering</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>EDD</td>
<td>Enhanced Due Diligence</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically Exposed Person</td>
</tr>
<tr>
<td>State Machine (SM)</td>
<td>A model of behavior composed of a finite number of states, transitions between those states and actions. A finite state machine is an abstract model of a machine with a primitive internal memory.</td>
</tr>
<tr>
<td></td>
<td>Link: <a href="http://en.wikipedia.org/wiki/Finite-state_machine">http://en.wikipedia.org/wiki/Finite-state_machine</a></td>
</tr>
</tbody>
</table>