Data Analytics Audit Considerations When Designing BSA/AML Audit Testing

Lindsay M. Dastrup, CAMS-Audit, CRCM, CIA, CFSA
The views expressed in this paper are solely those of the author and do not represent those of American Express Company.
# Table of Contents

Executive Summary .................................................................................................................. 3
Introduction ............................................................................................................................... 4
Data Analytics ........................................................................................................................... 5
Audit—Overall Process ............................................................................................................. 6
Audit Approach—Testing ......................................................................................................... 7
  *Customer Due Diligence* ...................................................................................................... 7
  *Sanction Screening* .............................................................................................................. 8
  *Suspicious Activity Monitoring* .......................................................................................... 8
  *Currency Transaction Reporting* ........................................................................................ 10
Impact to the Company ........................................................................................................... 10
Conclusion ............................................................................................................................... 11
Works Cited ............................................................................................................................. 13
Executive Summary

The purpose of this paper is to demonstrate the benefits of data analytics in providing more robust audit coverage of a Bank Secrecy Act/anti-money laundering (BSA/AML) audit in order to provide a higher level of assurance of BSA/AML regulatory compliance.

We live in a world where there are professional money launderers who sell their services to criminals. As such, there is a continuous effort to identify new methods to evade detection as financial services companies continue to improve the sophistication of their BSA/AML programs. The increased proliferation of alternative payment methods, including, for example, global remittances and mobile money, introduce potential new laundering vehicles and increased challenges for financial services companies. Also, increased product and services innovations will continue to evolve industry vulnerabilities. Despite these changes, there is still a focus on less sophisticated money laundering techniques, ranging from structuring to rapid movement of funds. As long as there are very large financial services companies with millions of customer relationships, even these base methods will remain a challenge to identify and intervene.

Regulators and the U.S. government view financial services companies as essential allies in the fight against money laundering and, therefore, the obligations of financial services companies have steadily increased in recent years and there is no reason to believe their obligations will lighten anytime soon as regulators and the U.S. government continue to issue BSA/AML guidance to help financial institutions strengthen their BSA/AML programs.

As a result, financial services companies have devoted significant resources to build out and improve AML compliance systems. That process will continue indefinitely as regulatory requirements and expectations expand due to the changing and evolving money laundering environment as money launderers look to different means to transfer illicit proceeds through the financial systems.

Capturing data is critical, but it is only the input. Financial services companies need to do something with it to actually create value; otherwise, the companies just added cost and companies need high performance data analytics to appropriately analyze and interpret the large amount of data.

The variety aspect\(^1\) of big data ensures that there is almost always a new way of delivering value or a new way that existing information can be leveraged to solve new problems. Big data is not a problem to be solved. It is an intermediary step to becoming a smarter company.

For many financial services companies, the internal audit (IA) function is essential for helping to identify and prevent money laundering, to improve process and control monitoring and promote policy and regulatory compliance as IA is commonly used as the third line of defense to identify weaknesses in a BSA/AML program and is commonly used as the independent testing function of the BSA/AML pillar.

Traditionally, IA has focused testing on a sample basis and gaining insight from data that exists in individual transaction systems to perform its work. In recent years, however, advances in technology solutions that encompass company-wide data analytics are transforming this area and allowing the evaluation of complete population of data sets to identify weaknesses in a BSA/AML program.

\(^1\) The variety aspect of big data refers to the fact that big data systems contain data that is diverse, including the range of data types and sources.
Introduction

Big data\(^2\) is a term describing a situation where the volume, velocity, and variety of data exceed a company's storage or compute capacity for accurate and timely decision making. Consequently, big data is intensifying the need for data quality (e.g., capturing the right data in the right data fields) and governance for embedding analytics into auditing, and for issues of regulatory compliance.

Data analytics is the process of examining big data to uncover hidden patterns, unknown correlations, and other useful information that can be used to make better decisions. By having the capability to leverage an enterprise-wide data warehouse\(^3\) containing data from multiple transaction systems, the data analytics provides full population coverage consistently rather than relying on sample-based testing. Having access to the full population of data increases the likelihood that IA will identify anomalies that require investigation and lead to better recommendations to improve the BSA/AML program to comply with regulatory requirements and expectations and to make the program more efficient and effective.

Traditional IA methodologies,\(^4\) such as sample-based testing, have served their purpose well for decades. However, as the business landscape for most financial services companies becomes increasingly complex and fast paced, there is a movement toward leveraging advanced business analytic techniques to refine the focus on risk and derive deeper insights into the company. Leading IA functions are embracing recent enhancements in data mining technology and data visualization tools to deliver results more dynamically in response to risk, to dive deeper into organizational data and to deliver profound fact-based insights. Data analytics holds incredible promise to enhance the IA process. The key to delivering on this promise is asking the right questions, embedding analytics into the culture of the IA function and aligning the analytics implementation with the planning process and overall organizational operational and strategic audit objectives.

Data analytic procedures are a much more cost-effective way to collect audit evidence. IA teams may not be making best use of the discipline. According to a 2013 survey\(^5\) conducted by PricewaterhouseCoopers (PwC) of IA Groups, 81 percent of respondents considered data analytics important to improve the quantification of issues; 85 percent of respondents considered data analytics important to strengthen audit coverage; and 74 percent of respondents considered data analytics important to gain a better understanding of risks.

The following sections define data analytics and data analytic methods, the process to incorporate data analytics into the audit process, examples of how data analytics can be used to identify weaknesses or inefficiencies in a BSA/AML program and the benefits of utilizing data analytics.

\(^2\) The SAS White Paper “Big Data Meets Big Data Analytics” notes that up to 85 percent of an organization’s data is unstructured—not numeric—creating a challenge for performing data analytics as the data is not uniformed.
\(^3\) Accenture White Paper - “Applying Analytics to Transform Internal Audit for High Performance.”
\(^4\) Deloitte White Paper—“Adding Insight to Audit: Transforming Internal Audit.”
\(^5\) The survey also noted that few Internal Audit Groups use data analytics with 31 percent of respondents stating that data analytics are used regularly. Additionally, the survey noted that some of the biggest challenges with data analytics include developing a methodology, acquiring analytical capability and selecting the right tools and technologies.
Data Analytics

Data analytics refers to qualitative and quantitative techniques and processes used to enhance productivity and business gain. Data is extracted and categorized to identify and analyze behavioral data and patterns, and techniques vary according to company requirements. In addition, data analytics is an analytical process by which insights are extracted from operational, financial, and other forms of electronic data that are internal or external to the company. These insights can be historical, real-time, or predictive and can also be risk focused (e.g., controls effectiveness, fraud, waste, abuse, policy/regulatory noncompliance) or performance focused (e.g., increased sales, decreased costs, improved profitability) and frequently provide the how and why answers to the initial what questions frequently found in the information initially extracted from the data.

Data Analytics Methods

Depending on the audit objective and data landscape and technical requirements, the company may have very different ideas about working with big data. Two scenarios are common:

1. One scenario consists of a complete data scenario whereby entire data sets can be properly managed and factored into analytical processing, complete with in-database or in-memory processing and grid technologies. For example, a complete data scenario can be the evaluation of customer due diligence (CDD) for all new accounts over a 12-month period.

2. Conversely, targeted data scenarios use analytics and data management tools are used to determine the right data to feed into analytic models, for situations where using the entire data set is not technically feasible or adds little value. For example, a targeted data scenario can be an evaluation of certain transaction monitoring rules based on initial evaluation results, such as those that generate a large portion of false alerts.

Furthermore, data analytics require that the systems utilized are evaluated from an information technology perspective to ensure the systems with key BSA/AML data are correctly interfacing with upstream and downstream systems. This ensures data is completely, accurately and timely captured in the BSA/AML systems for evaluation or processing, such as the capture and verification of customer data or the sanction screening of customer data. The integrity and quality of data is an ongoing challenge within many areas of a company. For IA, questionable data can create risks regarding the integrity of the audit findings and the ability to complete the required data analytics. This requires the audit team to identify the information sent from the upstream systems to the BSA/AML systems and the information sent from the BSA/AML systems to the downstream systems.

Overall, data analytics is used to extract large volumes of information and analyze the information based on the audit objectives to identify potential issues with BSA/AML operations that most likely cannot be identified through sample testing. This allows greater coverage of higher risk BSA/AML processes. Data analytics is crucial as it is designed to meet the rising need to transform the growing amount of data confronting all financial services companies into usable information for use by their senior management and stakeholders.

---

6 KPMG White Paper - "Data Analytics for Internal Audit."
7 SAS White Paper "Big Data Meets Big Data Analytics"
Audit—Overall Process

The following is a data analytics process model\(^8\) for leveraging data analytics within an IA project:

1. Define the audit objective(s).

Overall, the audit objective is to ensure that the company’s BSA/AML program is aligned to regulatory requirements and expectations and that the program is being executed accordingly. Audit objectives should be delineated further by the key BSA/AML areas applicable to the company, such as governance, training, CDD and sanction screening. Defining the objectives up front will save considerable time over the long run and help in planning what data sources will be needed and who IA will have to work with to gain access to the data.

2. Determine what analytics are relevant in achieving the audit objective(s).

Engage information technology (IT) auditors early in the process and work with them to identify and characterize the diverse operating systems, applications and data sources that require access. Collaborating with IT auditors early will establish a technical architecture that will suit the data analytical requirements and support audit efficiencies. Data analytics should be discussed for each area of the BSA/AML audit, including what data should be analyzed, what systems stored the data and ways to extract the data.

3. Identify relevant IT systems and assess availability and quality of data.

The IA team should identify the key IT systems that perform critical BSA/AML activities. Key systems include customer onboarding systems (e.g., new accounts systems), automated transaction monitoring systems and sanction screening systems. In order to perform data analytics procedures, auditors need effective access to the data that underlies a specific BSA/AML process area. Limitations of IT systems can include the data availability and quality as there may be a variety of disparate information systems with different data formats, incomplete data sets and inconsistent data quality.

4. Acquire data (i.e., extract, transform, load process).

The acquisition of the data will require the partnership with the business owners of the systems. This usually requires the IA team to have read-only access to the systems. Benefits of having access to the systems is less downtime for the IA team as it can immediately execute testing; and the IA client is not overwhelmed with extracting the data. However, if IA is unable to gain access to the systems, IA will need to rely on the business owners of the systems to acquire the data. This will require IA to verify the accuracy and completeness of the data to ensure the data is reliable for data analytics.

5. Develop and implement data analytics.

The development of data analytics may require time as the IA team familiarizes itself with the systems and better understand what data can be extracted and how the data can be used. The implementation of data analytics may result in further analytics as the initial results may indicate anomalies that require

---

\(^8\) The KPMG article “Data Analytics for Internal Audit” outlines a more detailed approach for implementing data analytics in an internal audit project.
further investigation. Specifically, the data anomalies will be targeted in order for the IA team to identify the entire impacted population.

Overall, the IA team should develop a data analytics process that meets the needs of the team and provides reasonable assurance that the audit objectives are met. Developing a data analytics process requires considerable planning during the audit to ensure the correct data can be extracted and analyzed.

Audit Approach—Testing

The purpose of this section is to highlight higher risk BSA/AML areas that tend to be automated at large financial services companies and recommend how data analytics can improve the audit approach. Data analytics allows for the identification of anomalies, which can be further investigated and may require sample testing of the anomalies to confirm the exception and identify the root cause.

Customer Due Diligence

One component of BSA/AML compliance program is the adoption and implementation of a comprehensive CDD program for all customers (e.g., Customer Identification Program [CIP], know your customer [KYC] processes and enhanced due diligence [EDD] processes). This program begins with verifying the customer’s identity and assessing the risks associated with that customer.

Data analytics allows testing the entire population of new accounts to verify if CDD information was obtained and verified within a reasonable time as defined by a company’s policies and procedures. The population of new accounts, such as deposit accounts, credit card accounts and checking accounts, should be extracted over a specified timeframe, which usually consists of 12 months. The data fields extracted should align with company’s CDD requirements.

Per review of the data, anomalies can be identified and further investigated. Such anomalies can consist of the following:

- New accounts with missing CDD information that were approved. For example, CIP requirements require that the name, date of birth, identification number and physical address be obtained and verified for new customer relationships. Using data analytics, new accounts approved without this information or without this information verified can be easily identified for further investigation.
- New accounts with illogical information that were approved. For example, accounts with taxpayer identification numbers that do not have nine digits, taxpayer identification numbers that have nine consecutive digits, or taxpayer identification numbers in which all digits are the same number can be easily identified for further investigation.
- Accounts that have not undergone periodic CDD refresh or refresh was performed untimely as defined by a company’s policies and procedures. Customer information should be refreshed based on customer risk profile, which should include AML risk. Higher risk accounts should be refreshed more frequently than lower risk accounts.
- Business accounts that operate in a prohibited industry that were approved as defined by a company’s policies and procedures. This does not necessarily refer to prohibited countries as defined by the Office of Foreign Asset Control (OFAC). For example, many companies define the industries that may not use its products or services, such as the adult entertainment industry.
• Accounts that are not risk assessed as high, medium, or low AML risk. Accounts should be risk assessed to determine the level of CDD, and the risk assessment process should be aligned to the BSA/AML risk assessment methodology.

Sanction Screening

Data analytics allows testing of the entire population of accounts to verify the completion of initial sanction screening prior to account opening or shortly thereafter, to verify the completion of ongoing sanctions screening and to verify the completion of Specially Designated Nationals (SDN) screening. Untimely or incomplete screening may indicate system issues such as balancing controls as sanction screening is an automated process.

• New accounts/existing accounts/transactions\textsuperscript{10} that did not undergo sanctions screening or did not undergo sanction screening timely as defined by a company's policies and procedures.
• New accounts/existing accounts/transactions that have potential sanction matches that were not investigated in a timely manner or not investigated at all.

Suspicious Activity Monitoring

The purpose of BSA/AML transaction monitoring is to provide ongoing identification of suspicious activity from customer transaction data. Transaction monitoring is generally a two-stage process whereby first, instances of potentially suspicious behavior are identified and then these instances of potentially suspicious behavior are reviewed to determine if a suspicious activity report (SAR) should be filed.

To identify potentially suspicious behavior, most large financial services companies have implemented automated BSA/AML transaction monitoring systems that identify instances of potentially suspicious behavior.

Data analytics allows testing of the alerts generated by automated transaction monitoring rules to determine if the rules are ineffective or inefficient. Specifically, effectiveness is the ability to properly identify suspicious activity that exists or to minimize the number of “false negatives.”\textsuperscript{11} The risk mitigated by improving effectiveness is compliance risk, which is the risk of failing to identify the actual suspicious activity. Improving effectiveness is the company’s obligation in order to meet compliance with regulations, meeting legal obligations and protect its reputation.

Additionally, efficiency is the ability to properly identify non-suspicious activity or to minimize the number of “false positives.”\textsuperscript{12} The risk mitigated by improving efficiency is business risk, which is the risk of improperly allocating resources to review cases of non-suspicious activity. Improving efficiency allows the company to keep cost down without increasing the risk of non-compliance.

\textsuperscript{9} This approach can be used for the screening of Politically Exposed Persons (PEP) as sanctions screening and PEP screening are usually performed at the same time.
\textsuperscript{10} Transactions include travel booking, wire transactions, trade or financing transactions.
\textsuperscript{11} False negatives are instances of suspicious activity that are not identified by the existing automated transaction monitoring rules.
\textsuperscript{12} False positives are instances in benign activity of improperly being identified as potentially suspicious.
Overall, the use of data analytics usually does not require sample testing to confirm the rules are ineffective or insufficient as these metrics serve to provide management reasons to reevaluate their automated transaction monitoring rules.

Per review of the data, anomalies can be identified and further investigated. Such anomalies can consist of the following:

**Alert Rate by Rule:**
- Assess effectiveness of management monitoring controls (i.e., timely management reaction to changes in alert rate trends).
- Assess whether rule is operating per management’s expectations (expected hit rates are occurring and, if not, rules are being revisited and revised as needed).

**Alert Rate by Business Unit/Product/Geography:**
- Verify high-risk business units/products/geographic locations that are generating proportionately more alerts and thus receiving more attention by the company’s AML team.
- Verify low-risk business units/products/geographic locations that are generating proportionately fewer alerts and thus receiving less attention by the company’s AML team.

**Alert Inventory:**
- Identify individuals who are investigating and decision-making potential suspicious activity alerts at a greater rate than their peers. This may be indicative that the individual is not thoroughly investigating the alert according to the company’s policies and procedures and increase the risk of a SAR unintentional not being filed.
- Assess the aging of the alert inventory. The aging of the alerts is a good indicator that resources are insufficient to investigate the current workload.
- Assess the false alert rates by rule. Rules with high volumes of false alerts should be revisited and revised.

**SAR Conversion Rate by Rule:**
- Assess effectiveness of management monitoring controls (i.e., timely management reaction to changes in SAR filings).
- Assess whether rule is performing per management’s expectations (expected conversion rates are occurring and if not, rules are being revisited and revised as needed).
- Identify potentially inefficient rules and assess individual rule contribution to alert inventory.
- Identify potentially ineffective rules that rarely or never result in SAR filings as these rules may need logic changes to be effective.

**Conversion Rate by Business Unit/Product/Geography:**
- Verify high-risk business units/products/geographic locations that are generating proportionately more SARs.
- Verify low-risk business units/products/geographic locations that are generating proportionately fewer SARs.
SAR Inventory:
- Identify SARs filed for multiple accounts to determine if the accounts were escalated for review. Accounts with multiple SARs should be considered for termination.
- Identify SARs that were untimely filed, which is based on the initial detection of potential suspicious activity to the SAR filing date.

**Currency Transaction Reporting**

Data analytics allows the testing of all cash transactions to determine if all cash transactions were identified for currency transaction report (CTR) filing and if cash transactions were aggregated correctly.

- Cash transactions received at various payment locations that were not correctly and/or timely aggregated.
- Cash transactions that exceed the monetary threshold for which a CTR was not filed.

**Impact to the Company**

Data analytics provides a more robust audit approach through the evaluation of large amounts of data. Overall, the benefits of performing audit analytics fall into three main categories:

1. **Increase in Audit Quality and Decrease in Audit Risk**

Data analytics generally allow for more extensive audit procedures to be performed, particularly substantive audit testing. Instead of performing judgmental or statistical sampling, testing can be conducted across 100 percent of the population in a given audit area thereby removing sampling risk by gaining complete audit coverage over a population.

In addition, the use of data analytics can significantly reduce audit risk. Traditional audit approaches relied upon judgmental or statistical sampling for substantive testing. However, the use of data analytics allows entire populations to be subjected to broad ranges of test procedures. By comprehensive testing, auditors are able to achieve increased confidence and reduced risk in their audit procedures.

Since data analytics allows the review and analysis of all transactions that take place within a given business process during a set period, this results not only in additional insight into the nature of the business activities, but can also identify trends and anomalies that may indicate potential risk areas and concerns that require specific audit focus.

2. **Improved management/board of director reporting and thereby decision making**

The first step in any reporting and analytics initiative is to integrate, cleanse, validate and manage data as a valued asset so that management can use it to drive strategic decision making. With a comprehensive management solution that supports analytics and decision management, companies can fully exploit and govern information assets and uncover hidden insights that improve and enhance operational effectiveness.

Decision makers need business intelligence that allows them to understand the past, monitor the present, and access timely, accurate information needed for strategic decision making. By using data to make
informed decisions and meet business objectives, companies are able to build a culture of intent. This is crucial since data analytics identify key patterns, trends and opportunities for improvement, enabling management to gain insights into which BSA/AML initiatives are working, which are not, and to adjust accordingly.

3. Continuous monitoring/continuous auditing

The role of IA is evolving in many companies. There is a move away from the traditional cyclical approach to audit to one in which IA continually assesses areas of greatest risk and performs in-depth audits in targeted areas. Continuous auditing and monitoring techniques can enable this changing role by providing ongoing automated analysis that highlights areas of greatest risk and audit concern. Instead of providing a cyclical audit report to management, the results of continuous auditing and monitoring procedures can also be immediately provided to management to identify areas requiring investigation and response.

Overall, IA has the obligation to the company to provide insight into the current state of the BSA/AML program through periodic audits of the BSA/AML program and to deliver intelligent opinions to address future BSA/AML risks. Meeting these responsibilities will become the industry standard as IA continues to move away from tedious sampling techniques and toward the widespread adoption of data analytics and continuous monitoring.

Conclusion

BSA/AML has been a focus of regulatory and enforcement activities for several years, and with heightened concerns about the financing of terrorist organizations, BSA/AML likely will continue to be the subject of close scrutiny. Merely establishing a BSA/AML program is not nearly enough as financial services companies also must verify that its programs are operating effectively and efficiently. BSA/AML audit data analytics can help assess the BSA/AML program by acting as an early warning system when the program is not operating at desired levels.

Data analytics presents a significant opportunity to manage the rising cost of compliance and the risk of noncompliance. The cost of combating financial crimes and managing compliance is on a constant rise. Financial services companies are experiencing increasingly stringent regulations and regulatory scrutiny. This atmosphere has made effectiveness a business imperative.

Data analytics allows the identification of operational inefficiencies and exceptions and can provide a more conclusive statement regarding the control environment and effectiveness of the BSA/AML program because audits can evaluate large amounts of data versus standard sampling testing. Audits that use data analytics can better assess the control environment, which results in an IA function becoming a more effective and valuable resource for regulatory compliance and operational efficiency and can be viewed as a strategic partner in helping the company achieve its goals. In addition, data analytics should be used as part of a comprehensive BSA/AML audit program rather than on an ad hoc basis. Embedding data

---

13 Continuous auditing (CA) is the collection of audit evidence and indicators by an internal auditor on information technology (IT) systems, processes, transactions, and controls on a frequent repeatable and sustainable basis. Continuous monitoring (CM) is a feedback mechanism used by management to ensure that controls operate as designed and transactions are processed as prescribed.
analytics into the audit program can help IA drive enterprise effectiveness and results that add tangible value to the company.

Advances in technology and the massive proliferation of available information have created a new landscape for BSA/AML auditing. With IA now having access to a seemingly unlimited breadth and depth of information, the need has never been greater for the IA process to evolve by providing deeper and more relevant insights about a company’s BSA/AML program while maintaining and continually improving audit quality.


Pistalu, Teo. "Data Analytics for Internal Audit." KPMG. Print.
