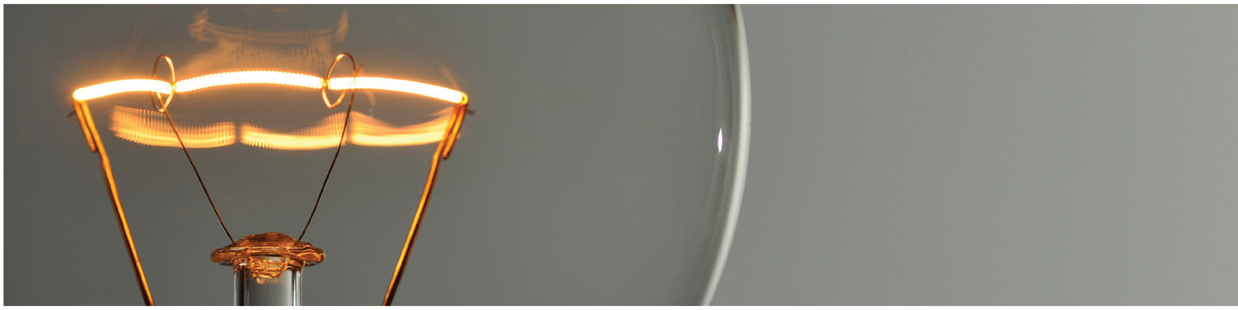
Innovation ushers in the modern era of compliance

How natural language generation is changing the game for anti-fraud, anti-money laundering and anti-corruption

Authors:
Daniel Krittman, Analytics Principal, Deloitte Transactions and Business Analytics LLP
Philip Matthews, Analytics Senior Associate, Deloitte Transactions and Business Analytics LLP
Mary Grace Glascott, Product Marketing Manager, Narrative Science



Contents

The era of modern compliance is here

This whitepaper, co-authored by Deloitte and Narrative Science, will discuss how the world of compliance is rapidly changing. Leading organizations are realizing that operating cost centers with a "check-the-box" compliance approach is a thing of the past. Instead of playing catch-up with increasing regulatory requirements and unrelenting fraud, corruption, and abuse, these firms are staying ahead of the curve by implementing innovative technologies that expedite and improve processes around data validation, fraud detection, investigation, and reporting. The era of modern compliance is here.

The stakes are high

The stakes have never been higher for those charged with overseeing compliance, anti-fraud, and anti-money laundering efforts, as demanding regulations and subsequent enforcement actions are on the rise. In 2014, the SEC increased anti-fraud enforcement actions by approximately 50 percent and new investigations by 30 percent.[1]

Those who try to circumvent ever-increasing regulatory requirements, or those who fail to fully comply with them, could be subject to crippling fines and legal action that may include imprisonment. And prosecutions are no longer happening only at the corporate level; individual prosecutions are escalating, making this a personal liability issue for those at the helm. As the investor Warren Buffett argues, "The way to change behavior is to have the fear that somehow it is going to come home to them and hit them hard. If your only fear is that you are going to have to write a big check, [little will change]; I believe very much in the prosecution of individuals."[2] Although financial services institutions bear the brunt of the regulators' force, they are not alone. Actions outside of financial services are increasing as well, including enforcement against virtual currency firms, casinos, and lending organizations.

For fraud specifically, corrupt accounting activities, fraudulent claims reporting, and data breaches deplete revenue and reputation; healthcare fraud alone costs the nation approximately $68 billion annually.[3] Legal and internal audit teams are accountable for identifying and communicating this activity in order to mitigate damages and prevent them from occurring in the future. But this proves to be a tall order, particularly in the realm of accounting fraud and bribery, with 45 percent of organizations in the U.S. reporting that they suffered from some type of fraud in the past two years.[4]

Firms are coping with this new environment by significantly investing in compliance headcount and technology. Non-interest expenses (e.g. salaries, technology, and compliance costs) at the six biggest U.S. banks rose nearly 12 percent from 2009–2014.[5] As compliance positions require specialized skills and exposure to rigorous standards, talent is highly sought after and firms are willing to pay. Yet attrition is high, resulting in a constant training cycle of new talent, as well as inconsistent reporting processes.

Investments on the technology side have grown substantially, particularly in the area of advanced analytics, business intelligence, and case management, with regulators pressuring smaller firms to adopt more automated solutions and larger firms to upgrade their current solutions' sophistication. In the constant search for best-of-breed capabilities, firms are becoming less hesitant to remove current platforms and replace them with new ones. For AML in particular, 55 percent of banks interviewed by the research firm Aite Group have either recently switched one or more vendors or are planning to do so within the next two years.[6]

Yet, despite significant investments in these tools to identify and report on fraudulent and suspicious activity, employees are still spending tremendous amounts of time manually sifting through false positives, tuning predictive models and business rules, interpreting analysis output, and reporting findings to key stakeholders. Much of this time is spent trying to understand what went wrong instead of predicting what is likely to happen next.

A compliance officer's secret weapon

Leading organizations have realized the constant game of catch-up is simply not working. Compliance officers need to be forward-looking, with the ability to employ automated solutions that augment human expertise to increase efficiency in the identification and reporting of suspicious and fraudulent activities. They need to enable transparency in the analytical process, so all stakeholders can clearly understand the impact that various data models have on determining outcomes. They need automated reporting to articulate what happened, why, and what's likely to happen next to internal stakeholders and potentially regulatory bodies. And they need it in natural language.

While natural language processing (NLP) is not new to the world of compliance; natural language generation (NLG) is a relatively new concept. Legal entities and law enforcement have been using NLP to analyze unstructured data to uncover hidden patterns and anomalies in large quantities of text through topic tagging and sentiment analysis, pinpointing key concepts and phrases that can help identify suspicious or potentially illegal activity. Conversely, NLG enables compliance teams to automatically identify the most interesting and important information trapped in structured data and produce language that provides situational context, explanations and potential next actions.

Advanced NLG systems, like Narrative Science Quill™, generate intelligent narratives that communicate what is most interesting and important in the data and are tailored to meet the needs of the intended audience. Since NLG is machine-based, these narratives can be produced at a scale only possible with technology, while potentially reducing inaccuracies associated with human error, and enabling auditability of the process, so all analytical decisions can be traced back to the system of record.

Deloitte is working with Narrative Science to integrate Quill into some of its existing business intelligence, analytics, and case management systems. Quill delivers narrative explanations to guide users along the analytic process by providing context to dashboards and alerts, as well as explanations of the models and rules that generate them. Quill can also be used to enhance or potentially even replace the current reporting layer of existing systems.

Instead of pushing out traditional production reports that may be difficult to interpret and require customization for each specific audience (e.g. various regulatory bodies, internal audit and legal teams, executives), Quill can automatically generate natural language reports highlighting the most relevant information for each audience.

Leading firms are turning to Advanced NLG systems to generate regulatory reports in order to explain and trace the logic of analytic platforms. Specifically, Deloitte is piloting the use of Quill to automate the narrative component of Suspicious Activity Reports (SARs) to assist with anti-money laundering compliance, provide detailed fraudulent activity reports for internal audit teams, and explain the impact that threshold changes and model tuning may have on analytic efforts.

Anti-fraud and anti-corruption: from cost center to innovator to revenue generator?

Fraud analytics sits at the nexus of technology and techniques; combining human expertise with automation and analytical tools in order to detect fraudulent activity, such as improper transactions or bribery. Using the structured data generated by Deloitte's proprietary technology combined with the advanced natural language generation capabilities developed by Narrative Science, fraudulent activity may be identified more quickly and easily. When integrated with predictive analytic techniques and case management, this forward-looking analysis can help identify signs of potential corruption before it has even occurred.

The general process of fraud analytics involves gathering and storing relevant data and mining it for patterns, discrepancies, and anomalies. For example, anomaly detection through pattern analysis can identify significant gaps, outliers, and inconsistencies within data models. Link and network analysis can help uncover hidden relationships across separate data sets to identify facilitators who may be setting up front companies that enable money laundering, for example. These can become valuable capabilities for analysts spearheading a fraud or corruption investigation.

Whether in a compliance function, internal audit or elsewhere in an organization; the essential work of fraud and AML analysts has long been thought of as a cost center component. But what if the same data required for compliance efforts could help change the cost center paradigm? What if the tools and techniques described herein could do more than simply help fight malfeasance?

The data collected and analyzed in order to generate a narrative can (and likely, should) be utilized for other purposes. Consider the scenario whereby nefarious activities are combatted at the same time that customer/client risk rankings are utilized to devise fee strategies or segment populations for targeted services. The very components used to generate an internal audit or compliance insights could potentially be used to generate revenue.

NLG for AML: automating the SAR narrative and explaining analytics

Per Aite Group's report "AML Vendor Evaluation: Managing Rapidly Escalating Risk":

"It's a tough time to be an AML executive. Penalties for AML violations are escalating, it's increasingly difficult to find good AML analysts to work mounting alerts, and new technologies and payment mechanisms are further adding to the compliance burden. It's no wonder FIs are increasingly looking to more robust technology to help facilitate compliance."[7]

Each year, AML analysts receive millions of alerts of unusual activity, requiring the analyst to further investigate and determine if the activity is indeed suspicious. If so, a Suspicious Activity Report (SAR) is required to be filed to FinCEN within 60 days. Large financial institutions can generate thousands of SARs every year, so AML compliance costs can be substantial. In addition, as AML analysts are susceptible to turnover, or these capabilities may be outsourced, so SAR reports are often inconsistent.

A typical SAR has five components; the first four can be auto-populated by many case management systems. However the last portion, the SAR Narrative, cannot. When FinCEN[8] rolled out its new SAR forms in 2012, it underscored the importance of the narrative with this statement: "The narrative section of the report is critical to understanding the nature and circumstances of the suspicious activity. The care with which the narrative is completed may determine whether the described activity and its possible criminal nature are clearly understood by investigators."[9]

With Quill, the SAR Narrative can be automatically generated, while communicating the key "who, what, when, and where" aspects of the suspicious activity. Deloitte is piloting Quill to write SAR narratives on demand, ensuring accuracy and traceability of the reports. Per Aite Group's AML Vendor Evaluation Report:

Using a combination of data analytics and cognitive computing, Quill can quickly convert case data into SAR narratives, saving analysts the time and effort of writing the reports themselves. Using Quill also ensures that the SAR narratives are complete and consistent across the firm.

In addition to increasing regulatory reporting requirements, AML analysts are also dealing with larger volumes of superfluous and unproductive alerts from existing analytics and case management systems. Increasing unproductive alerts — or false positives — mean higher compliance costs, as analysts need to spend time interpreting the context of the alerts and evaluating if they are indeed suspicious, or just unusual. Optimizing the detection models to reduce false positives is time-consuming and resource intensive due to the reporting requirements of model changes. In fact, one bank states that nearly 75 percent of its analytics team's time is spent on documentation rather than producing new and better models.[10]

Analysts no longer need to spend time continuously tweaking models and sifting through false positives. By detailing the impact that model changes have on the accuracy of identifying suspicious activity through a natural language audit, NLG increases transparency of these tools and accelerates time to optimization. In addition, when it's time to show regulators the result of model tuning efforts, they can simply hand over the automated natural language report that identifies the trail of model tuning efforts.

Four steps to enable modern compliance

Modern compliance will require a mental shift, an embrace of automation, a commitment to demystify the black box, and a repeatable methodology to report with full transparency. Here are four steps that can help enable modern compliance:

1. **Provide relevant, compliant reporting.** Ensure all stakeholders, from internal audit and legal teams, to regulatory bodies, to chief executives, know what happened in a way they easily understand: natural language.

2. **Automate. Automate. Automate.** For many firms, collecting, validating, and reporting information has been a manual exercise, at least during the first two years following the implementation of new rules. Such processes are susceptible to errors and inconsistencies. Automating data gathering, validation, and reporting processes can help to reduce risk and improve accuracy from a regulatory perspective, and also frees employees to spend more time on high-value tasks.

3. **Avoid black boxes.** Answers alone from your analytic and case management systems should not be taken at face value. In addition to subject matter experts and trained professionals, technology that can explain the analytics performed "under the hood" and provide traceability back to the system of record will become the compliance officer's trusted ally as regulations and technological sophistication continue to increase.

4. **Shift the cost-center mentality.** By reducing manual reporting processes, Advanced NLG has enabled organizations to devote their employees to high value activities, making them more efficient and directly impacting the bottom line.

1 “Accounting irregularities have moved to the front burner at the SEC again — can you feel the heat?” Deloitte, 2015. http://www2.deloitte.com/us/en/pages/advisory/articles/accounting-irregularities-fraud-is-your-company-vulnerable.html

2 Katherine Rushton, “Warren Buffet calls for greater punishment for Wall Street rulebreakers,” The Telegraph, May 3, 2014, http://www.telegraph.co.uk/finance/businesslatestnews/10807082/Warren-Buffett-calls-for-greater-punishment-for-Wall-Street-rulebreakers.html

3 “Statistics,” BlueCross BlueShield, accessed September 15, 2015, http://www.bcbsm.com/health-care-fraud/fraud-statistics.html

4 Michael Cohn, “Accounting fraud on the rise at U.S. companies,” Accounting Today, February 19, 2014, http://www.accountingtoday.com/news/Accounting-Fraud-Rise-US-Companies-69646-1.html

5 Sarah Krouse and Emily Glazer, “J.P. Morgan, Goldman Sachs, Morgan Stanley, to form data company,” Wall Street Journal, August 19, 2015, http://www.wsj.com/articles/j-p-morgan-goldman-sachs-morgan-stanley-to-form-data-company-1440005471?mod=djemCIO_h

6 Julie Conroy, “AML Vendor Evaluation: Managing Rapidly Escalating Risk” Aite Group, June 2015.

7 Conroy, “AML Vendor Evaluation: Managing Rapidly Escalating Risk.”

8 FinCEN is a bureau of the U.S. Department of the Treasury. FinCEN’s mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities, http://www.fincen.gov/about_fincen/wwd/

9 “The FinCEN Suspicious Activity Report: Introduction and Filing Instructions,” Financial Crimes Enforcement Network, http://www.fincen.gov/whatsnew/pdf/TheNewFinCENSAR-RecordedPresentation.pdf

10 Conroy, “AML Vendor Evaluation: Managing Rapidly Escalating Risk.”

Contacts

Daniel Krittman
Analytics Principal, Deloitte Advisory
Deloitte Transactions and Business Analytics LLP
+1 212 436 6712
dkrittman@deloitte.com

Anthony DeSantis
Analytics Principal, Deloitte Advisory
Deloitte Transactions and Business Analytics LLP
+1 212 436 3307
andesantis@deloitte.com

Mohamad Said
Analytics Senior Manager, Deloitte Advisory
Deloitte Transactions and Business Analytics LLP
+1 212 436 6489
msaid@deloitte.com

Christina Tripodo
Analytics Senior Manager, Deloitte Advisory
Deloitte Transactions and Business Analytics LLP
+1 212 436 3289
ctripodo@deloitte.com