Legal, Compliance and Technology Executive Series

Sponsored by: Forensic & Integrity Services

In the digital era, compliance programs must connect many data streams and analyze employee behaviors in order to uncover and mitigate hidden risks from within.

Lisa is the global head of compliance of a company that is aggressively expanding into new markets to achieve its revenue goals. Amid this rapid growth, the global sales force increases – and any misconduct can expose the company to significant reputation, legal and compliance risks that could derail its ultimate growth objectives.

If an employee goes rogue, how will you know?

Of special interest to:

General counsel

Chief risk officers

Chief compliance officers

Information security officers

Corporate security officers

Others responsible for managing risk and security

The better the question.
The better the answer.
The better the world works.

Building a better
working world

What are the challenges?

Within the boundaries of privacy laws, Lisa's company monitors its employees' electronic communication (e.g., emails, instant messages), social media activities and network access data (e.g., logins, large data transfers).

Yet its compliance monitoring program remains fragmented. Different streams of data — for example, sales transactions and emails — are siloed, limiting the company's ability to uncover risk indicators that could reveal illicit intent. In addition, traditional surveillance technologies, such as automated alerts based on keyword searches in text, generate many false positives to sift through.

Many companies use analytics to glean insights from their finance and customer data. Similar strategies with a heavy focus on behavioral analytics, guided by a holistic approach to link relevant data, can be used to combat employee conduct risks. How can Lisa make progress?

Five insights for executives

1 Rogue employees are seizing new opportunities to profit themselves at the expense of shareholders

Our world is increasingly connected with its reliance on technology, which has provided more means for malicious employees to commit misconduct and wreak havoc than ever before. Social media has opened more communication channels for fraudsters to carry on bribery and other illegal behaviors, and cryptocurrency has made it difficult to trace unlawful transactions. The dark web has also made it easier to conduct illicit transactions.

Employee misconduct is a risk that impacts all industries

The most common sales misconduct risks in pharmaceutical companies come from employees inadvertently or intentionally engaging in improper pharmaceutical sales and marketing tactics, such as off-label promotions, kickback payments, physician referrals and unreported adverse events.

In the financial services sector, high-profile incidents of misconduct continue to grab the headline related to insider trading, banking sales practices and foreign exchange trading. According to a recent white paper by the Federal Reserve Bank of New York, "Root cause analysis of many recent cases of misconduct in the financial sector, however, suggest that misconduct is … the result of wider organization breakdowns." The Australian Government established the **Hayne Royal Commission** on 14 December 2017 to inquire into and report on misconduct in the banking, superannuation and financial services industry, in light of scandals related to the **industry's promotion of an aggressive, sales-driven culture**.

2 Legacy compliance programs struggle to handle the increasingly complex fraud environment

An effective compliance program should retain, integrate and scrutinize a wide range of data sources, such as emails, voicemails, instant messages and social media posts. Traditional tools have proved insufficient for integrating disparate data sources, especially unstructured and structured data sources, at the same time, as well as some new data sources, such as audio logs.

In addition, the data sources are often segregated and therefore can't offer a full picture of employee activities, and traditional keyword search technologies can be easily circumvented. As a result, important events are buried within the fragmented data, while enterprise security and compliance teams are drowning in false positives and siloed alerts that are not prioritized.

3 The penalties for inaction, or ineffective actions, are steep

With outmoded surveillance capabilities, institutions risk criminal indictments, multibillion-dollar fines and reputational damage. Money that might otherwise be earmarked for growth and expansion is instead wasted on covering legal costs, fines and operational fixes, while spooked customers look to take their business elsewhere, prompting revenue losses.

Regulators expect organizations to establish robust surveillance capabilities to monitor the behavior of insiders against fraudulent activities. Prosecutions and regulatory enforcement stemming from noncompliance related to employee behavior, such as corruption, bribery, rogue trading and insider trading, are on the rise around the world. According to Bloomberg, large financial firms have paid fines in excess of $320 billion worldwide in connection with employee misconduct.[1]

[1] "World's Biggest Banks Fined $321 Billion Since Financial Crisis," Bloomberg, March 2, 2017.

Five insights for executives

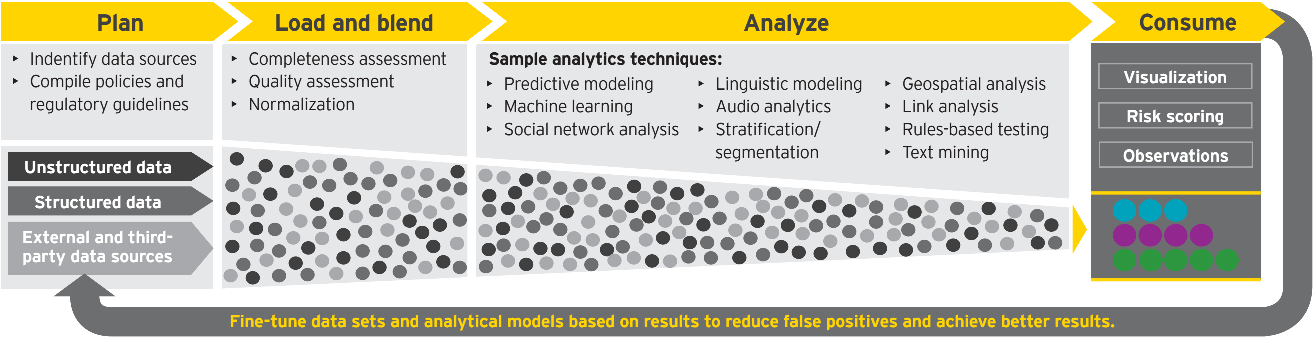
4 Identifying noncompliance requires a holistic approach bolstered by analytics

With so much at stake, analytics should be the cornerstone of any compliance program. Analytics transforms employee data into insights, showing what is happening, along with the how and the why.

The most commonly used tool in compliance monitoring is behavioral analytics. Behavioral analytics focuses on the emotional or evaluative content of electronic communications and matches the uncovered patterns to those that have previously been linked to misconduct, fraud or noncompliance. Social networking analytics, another commonly used tool, helps identify relationships between seemingly normal behaviors to reveal hidden intent.

However, analytics can be effective only with the right data. Sound information governance hygiene is critical for understanding data sources that serve as the foundation of surveillance programs.

Figure 1. A surveillance analytics implementation workflow example



Plan

- Indentify data sources
- Compile policies and regulatory guidelines

Load and blend

- Completeness assessment
- Quality assessment
- Normalization

Analyze

Sample analytics techniques:

- Predictive modeling
- Machine learning
- Social network analysis
- Linguistic modeling
- Audio analytics
- Stratification/ segmentation
- Geospatial analysis
- Link analysis
- Rules-based testing
- Text mining

Consume

Fine-tune data sets and analytical models based on results to reduce false positives and achieve better results.

5 With so much at stake, the time to act is now

With the future accelerating toward us, you can't be slowed down by the tools of the past. In this digital era, the risk landscape evolves rapidly. Without an integrated compliance program powered by behavioral analytics and more, threats can go undetected or be difficult to surface — until the damage is done, and your company is facing fines, litigation, revenue loss and reputational wounds.

In Lisa's sector, insider trading, securities fraud and anti-money-laundering concerns are ever present, just to name a few. But equipped with an integrated monitoring program supported by its key stakeholders, the compliance function can work more effectively and efficiently, and the company can continue moving forward with confidence in the new and rapidly shifting digital era.

Thanks to Lisa's proactive efforts, new light has been cast into her company's dark corners, and potential threats have fewer places to hide.

Here are the key steps in implementing surveillance analytics capabilities, within the parameters of privacy and data protection law:

1. Adopt a cross-functional governance model to gain deep understanding of the organization's data sources and their interrelationships
2. Establish risk indicators by using data from past internal incidents, as well as fraud and noncompliance data obtainable in the public domain
3. Use analytics tools to transform and combine risk indicators into risk scores that will help guide the escalation decisions
4. Enforce access control to protect sensitive data and to comply with the relevant privacy and data protection laws

For more information, visit us at:

ey.com/analytics

Author:

Todd Marlin
Global and Americas Forensic Data Analytics Leader
Forensic & Integrity Services
+1 212 773 7709
todd.marlin@ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.
For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority — no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

EYG no. 000172-19Gbl
BSC no. 1812-2973285

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

Any reference to legal rulings and interpretations of their impact is not legal advice. You should consult your legal advisor for guidance on how the cited cases may be applicable to or impact your situation based on the facts of any particular matter.

ey.com