THE GENERAL COUNSEL’S GUIDE TO GOVERNMENT INVESTIGATIONS

EDITION 1.0

A PUBLICATION OF THE GOVERNMENT INVESTIGATIONS & CIVIL LITIGATION INSTITUTE
The

General Counsel’s Guide to Government Investigations

Edition 1.0
GOVERNMENT INVESTIGATIONS & CIVIL LITIGATION
INSTITUTE ADVISORY BOARD

Jamie Brown
Attorney & Consultant, Jamie A. Brown, LLC

Vikramaditya Khanna
William W. Cook Professor of Law, University of Michigan Law School

Christopher Liwski
Senior Corporate Counsel, Sanofi US

Ashish Prasad
Co-Founder, GICLI
Vice President & General Counsel, eTERA Consulting

Patrick Oot
Co-Founder, GICLI
Partner, Shook, Hardy & Bacon L.L.P.

Claudius Sokenu
Deputy General Counsel, Global Head of Litigation & Global Head of Regulatory Compliance, Andeavor

Vincenzo Toppi
Director, CohnReznick LLP

EXECUTIVE DIRECTOR
Barbara Hanahan
Chapter 17

Compliance Monitoring

By Wayne Matus and Brandon Daniels

To focus the observations of this chapter, we will review the evolution of governance, risk management and compliance ("GRC") principles, including the introduction of personal liability, the role of monitoring and the three lines of defense at which an organization can mitigate risk. We will analyze certain sectors that are subject to a relatively high degree of regulatory scrutiny due to the nature of their areas of commerce, or economic and societal criticality. While we recognize that this does not address the needs of all organizations, we intend to provide guidelines that can be applied on a risk-weighted basis by many correlated and subsidiary market participants. Also, the business processes, solutions and outcomes described are not prescriptive and represent target state principles for organizations grappling with many different competing priorities. This chapter will emphasize the three core tenants of an effective compliance monitoring program: data, policy and culture. Finally, to enable the operational application of the observations, we will overlay an analysis of exemplar types of monitoring in production at large global corporations and financial institutions and the data types that are integral to their function,

Wayne Matus is a Managing Director of UBS and Global Head of eDiscovery. He works with eDiscovery stakeholders and partners to manage retrieval, processing, review, and production of materials in internal investigations, regulatory investigations, and litigation for business divisions world-wide. His responsibilities include Information Governance, privacy, and cross-border eDiscovery. Formerly a trial lawyer and law firm partner, Wayne has received numerous awards, authored several publications, and served on a number legal institutes’ faculty. Brandon Daniels is President of ExigerTech and Global Head of Analytics. He leads Exiger’s Technology Division and Analytics Practice, overseeing the execution of data-driven solutions in the firm’s regulatory and financial crime compliance efforts. A regulatory expert and technology practitioner, Brandon has over 15 years’ senior management experience across the financial services, life sciences, and energy sectors.
and discuss the key challenges that organizations face in implementing them.

I. GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE – THE BEDROCK OF COMPLIANCE MONITORING

“The financial crisis can be traced back to failures of corporate governance and risk management systems. At some institutions boards of directors and senior managers did not sufficiently comprehend aggregate risk within their firms and lacked a sufficiently robust risk framework—that is, the people, systems, and processes for monitoring a complex set of risks. In some cases, bank compensation programs were structured to share upside benefits but not the downside risks. Inadequate and fragmented technology infrastructures hindered efforts to identify, measure, monitor, and control risk. And some of these institutions’ risk cultures lacked effective credible challenge from independent risk managers, audit, and control personnel. While these problems existed to some extent at banks of all sizes, it was in the largest, most complex banking institutions that the problems were most pronounced and where they created the greatest potential threat to the stability of the financial system.”

-Thomas Curry, Comptroller of the Currency

For all industries understanding, resolving and monitoring the root causes of the last decade’s economic turmoil has taken center stage. One of the key themes of this overhaul is a consensus that the poorly understood, managed, and reported risk of the early 2000’s was at the epicenter of the quake that shook the global economy. As a reaction, industry stakeholders have spent years defining and debating how to establish regulatory standards that create guardrails and diagnostics for critical areas of commerce. The industry

---

continues to wrestle with balancing the potential crippling weight of overregulation with the specter of unmanaged risk yet again endangering our way of life.

The movement to consistently demonstrate GRC principles, as a single unified concept and not discreet functions, is at the forefront of this effort and at the vanguard of corporate and policy scholarship. And, although members of an interdependent framework exist in an effective corporate risk management strategy, each of these mechanisms for managing threats to the lawful and ethical operation of a business maintains a distinct genesis and evolution. As an example, corporate governance – defined as the practices and procedures an organization uses to manage decision-making where the interests (represented by relative definitions of gain and risk-appetite) of internal and external stakeholders are balanced to achieve optimized outcomes – can be found as early as 1602 in the creation of the Dutch East Indies Company. The incarnation of corporate governance that is most familiar to western corporate citizens was largely sculpted by committees of industry, regulatory and professional bodies coming together to establish standards for listed companies. Progressive, and in some instances aspirational, initiatives such as the Cadbury Report (1992), the Greenbury Report (1995), the Combined Code (1998), Turnbull Report (1999) and the Organization of Economic Cooperation and Development (“OECD”) Principles (1999) were a response to a crisis in investor confidence and a demand for transparency, honesty and accountability in risk versus benefit decisions, financial performance and the accurate reporting of results.

Even today, corporate governance continues to evolve as a key focus of government and industry efforts. Last November, aligned to Prime Minister Theresa May’s comments that she wanted to “see

---

changes in the way that big business is governed,” the United Kingdom (“UK”) Government’s Department for Business, Energy and Industrial Strategy (“BEIS”) published its Green Paper, Corporate Governance Reform, setting out broad topics for consideration. This paper spurred public debate in a “cross-section of business and society” as to the limits of current corporate governance practices to address issues in executive pay, the voice of non-shareholder stakeholders and the decision-making of private companies. The UK government’s response to this consultation period and debate, published in August of 2017, will undoubtedly continue to influence governance best practices and push the boundary lines of what is commonly perceived as the application of good corporate governance. Where GRC may represent a holistic control environment, each area under this umbrella represents a robust and complex domain.

Despite the focused efforts to improve governance, risk management and compliance as individual functions, the area of GRC has also evolved in its own right, inside and outside of defined industry and government committees. GRC has organically developed in the aftermath of major events in economic history, including the financial market collapse and deep depression of the 1930’s; the Enron and WorldCom scandals, the reputational destruction of Arthur Andersen and the resulting enactment of the Sarbanes-Oxley Act in 2002; and the 2008 financial crisis followed by sweeping financial regulatory overhaul imposed by The Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010. The resulting product is a management framework of interconnected

629 Kylie MacLellan, Key excerpts from the leadership launch of Britain's Theresa May Reuters (2016), http://uk.reuters.com/article/us-britain-eu-may/key-excerpts-from-the-leadership-launch-of-britains-theresa-may-idUKKCN0ZR1MY?mod=related&channelName=gc05.

controls that are consistently and constantly monitored for adherence and efficacy.

One critical landmark in the definition of GRC was the coalescence of the Committee of Sponsoring Organizations of the Treadway Commission (“COSO”) in 1985. The conglomerate is jointly sponsored by five industry groups: the American Accounting Association; the American Institute of Certified Public Accountants (“CPAs”); Financial Executives International; the Institute of Internal Auditors; and, the Institute of Management Accountants. COSO has transformed the nature of compliance development and management. Most notably, the 1992 “Internal Controls – Integrated Framework” paper has set the tone for twenty years of GRC controls management. Although COSO did not specifically name GRC, the paper proposed a method for designing, implementing and executing a system of internal controls.

In the paper, COSO set forth five critical and integrated components for establishing an internal controls system. First is the control environment, a defined set of standards, processes and structures that provide the basis for carrying out internal controls across an organization.631 Second is a business’s risk assessment process. A risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives.632 Third, control activities are the actions established through policies and procedures that help ensure management’s duty to mitigate risks to the achievement of the entity’s objectives.633 Fourth, the evaluation of information and communication supporting controls in an organization.634 Information is necessary for an entity to carry out internal control responsibilities to support the achievement of its

632 Id.
633 Id.
634 Id.
objectives.\textsuperscript{635} And communication is the continual and iterative process of providing, sharing and obtaining necessary information.\textsuperscript{636} The fifth and final component is monitoring. In the COSO components, monitoring is both a separate and ongoing evaluation of the internal controls system overall and of the functional efficacy of the components of each control.\textsuperscript{637} Monitoring is not only a component, it is the thread that holds together the remaining components integral to an effective control. Today, the COSO guidance is as inherent to the way corporations and financial institutions manage risk and monitoring as the hub is to the spokes.

In addition to GRC maturing and becoming fashionable amongst regulated organizations, changes in the law have accentuated the demand for robust GRC functions that conduct compliance monitoring. Of note, the trend towards management and board level certifications, confirming the efficacy of compliance policies and procedures with the potential attachment of personal liability in the circumstance of negligence, has heightened board and executive level sensitivity to managing GRC risks on a continuous basis. With cautionary tales for compliance officers that fail to build effective programs – a prime example being the recent settlement between the former Chief Compliance Officer of MoneyGram International, Inc., Thomas Haider, and United States (\textquotedblleft US\textquotedblright) Attorney\textquoteright s Office for the Southern District of New York (\textquotedblleft SDNY\textquotedblright) and the Financial Crimes Enforcement Network (\textquotedblleft FinCEN\textquotedblright) for claims brought under the Bank Secrecy Act/Anti-Money Laundering laws and regulations (\textquotedblleft BSA/AML\textquotedblright) – GRC demands a level of accountability and awareness that has shifted compliance from passive to active and has turned investigations from episodic to business-as-usual (\textquotedblleft BAU\textquotedblright) activities in the form of continuous compliance monitoring.

\textsuperscript{635} Id.
\textsuperscript{636} Id.
\textsuperscript{637} Id.
The topic of compliance monitoring in a global and heterogeneous universe of industries, market demands and public interests conjures a different image in every sector. However, for all industries, monitoring is a key component of an effective GRC strategy. Monitoring can take two primary forms: monitoring for the underlying risk in a given business activity; or monitoring the execution and efficacy of the controls performed to mitigate the underlying risk. This distinction is the fabric for the final conceptual element in the definition of compliance monitoring – the three lines of defense.

The three lines of defense are the levels at which an organization can monitor and mitigate its risk. Although most mature in banking, this conceptual design for compliance monitoring has wide applicability in all commercial organizations. The first line, or front line, is the business itself. This includes the sales, operations and executive staff responsible for generating revenue. The inclusion of the business in compliance monitoring is an essential component of a successful risk management program. It provides both accountability and awareness to the people most influential to the culture and practices of an organization. It also provides an immediate first-hand assessment of the underlying risk that the business is attempting to mitigate. The Office of the Comptroller of the Currency (“OCC”) defines this as any organizational unit that: “(i) engages in activities designed to generate revenue for the parent company or Bank; (ii) provides services, such as administration, finance, treasury, legal, or human resources, to the Bank; or (iii) provides information technology, operations, servicing, processing, or other support to any organizational unit covered by these Guidelines.”

The second line is typically defined as the risk management or compliance functions of an organization. Although these functions

---

are part of the organization, they are considered independent “check and balance” functions for the business. Again, the OCC defines this as, “any organizational unit within the Bank that has responsibility for identifying, measuring, monitoring, or controlling aggregate risks.” The second line is typically responsible for ensuring the conclusions of the first line, assessing any gaps, monitoring ongoing activity and assisting in the remediation of weaknesses. This is a proactive and integrated function in the organization and, in many cases, is the center of excellence of compliance monitoring and improvement.

The third and final aspect of the three lines of defense is the role of internal audit. What is most remarkable about the third line of defense is its independence. In not only OCC definitions, but in common practice, this form of independence is not duplicated elsewhere. Reporting lines, incentives, budgets and procedures are commonly all separate from the functions they monitor. Internal audit’s remit is to assess the efficacy of governance, risk management and compliance practices of the organization, including the abilities of the first and second lines of defense to monitor risk management and control objectives. The three lines of defense construct is a key pillar in risk management and sits side-by-side with the five components of internal control systems and the unified concept of GRC itself.

II. DATA, POLICY AND CULTURE IN COMPLIANCE MONITORING

“There is no standard regulatory metric, nor is there any prescription. Is culture about the right ‘vibe’? If so, that’s not very satisfactory. One way of knowing when culture has failed is when things go wrong and get worse or just go wrong again. This may be worth some thought. How quickly does it take for problems to escalate to the right person or group of persons for effective decision making or action? How many problems linger in the inbox

639 Id.
or the draft box or the bottom drawer beyond their easily fixable date? How difficult is it to fix things once they are detected? How long? How soon? How hard? These questions beg qualitative or numerative answers that may be capable of measuring and, in a proxy sense, giving us a metric for how well an organisation is able to deal with things that don’t go well or don’t go according to plan.”

- Mark Steward, Director of Enforcement and Market Oversight
Financial Conduct Authority ("FCA")

On March 20th 2017, Ravi Menon, Managing Director of the Monetary Authority of Singapore ("MAS"), delivered keynote remarks at the Australian Securities and Investments Commission Annual Forum, where he stated that culture is a defining element for the future state of compliance. Menon stressed that MAS would look beyond the question of “Is this legal?” to the larger question of “Is this right?” He also proposed that the rapid advancement of technology would be the sands upon which compliance risk would shift. Menon highlighted the double-edged sword presented by emerging technologies, pointing out both the challenges and benefits of algorithmic decision-making and vast sums of enriched data points generated by financial institutions about people, places and things. The intersection between the amorphous and qualitative measures of compliance and the increasingly complex and voluminous quantitative variables upon which it may be measured creates a hurdle for most organizations when defining and monitoring compliance standards. Whether manual or automated, compliance monitoring is the analysis of data indicative of risk, generated during business activities, against compliance 

---


requirements. In the equation of compliance, data, in many forms, is the operand and policy is the operator.

Policies, or the procedures and controls that represent or reinforce those policies, in large corporate organizations are characterized by a systematic, documented and process-driven set of rules that are increasingly reinforced by technology. These controls and procedures may be encountered in the form of process documentation, checklists, disclosures or risk evaluation procedures applied to situations identified as integral to the performance of a policy or points in time where policy assessment indicators, in some form of data, are available for review. For example, in retail mortgage lending, a control may be the requirement to evidence the completion of a certain set of disclosures when underwriting a mortgage for a US military veteran under the guidelines of the Servicemembers Civil Relief Act. This control could go through multiple checks, where different groups require reaffirmation and evidence of the control, such as credit risk. Legal and compliance groups maintain independent controls as they usher the mortgage application through an approval process. Similarly, in pharmaceutical sales, pharmaceutical companies must evidence that all requests from healthcare professionals for educational materials describing off-label use of a product are referred to an independent medical affairs function. Ensuring that such requests are handled in a regimented fashion and that no referrals revert to commercial conversations can be critical to avoiding litigation, enforcement actions and the potential for millions of dollars in fines, settlements and legal fees. These are just two examples from two major sectors that represent thousands of controls and different procedural methods of employing these controls, where each organization would be required to consistently monitor and enforce the applicable policies.

Although polices allow a company or institution to establish a set of desired standard operating procedures ("SOPs"), a lack of adherence to these policies and the haphazard completion of controls can still open the organization to risk. Or, on the other end of the spectrum, the purposeful evasion of these controls can create even more
substantial risk for an organization if the activity is systemic. The ability to prioritize and emphasize these SOPs and ensure that shortcuts are not taken on checks and balances, even in strained circumstances, is the second layer of compliance monitoring. This is an element of compliance defined by organizational values or “culture” and is often demonstrated by employee conduct. Culture is not only a matter of adhering to policy, it encompasses how an organization addresses and escalates risk that has been identified and, more importantly, sensitizes employees to conduct risk that is outside of a policy or control framework.

III. COMPLIANCE MONITORING THROUGH THE LENS OF OPERATIONAL PRACTICES AND DATA SOURCES

“In [one] sense, ‘big data’ is a continuation of an old theme. In another sense, the developments in data over the last 10 to 15 years represent a wholly new phenomenon, in the same way that satellite imaging is completely different from surveying a landscape from the top of a hill. At that scale, patterns become evident that would have been impossible to piece together by considering one plot at a time. This means that both market participants and regulators have new opportunities for developing knowledge. Moreover, this is a qualitatively different kind of knowledge, encompassing entire data sets in one pass rather than slowly accumulating insight from individual experiences.”

- Commissioner Kara Stein, Securities and Exchange Commission (“SEC”)

There are four data streams that dominate the corporate landscape and are the currency of compliance monitoring programs. These data types are: web content (published material, sites, social media, knowledge databases, etc.); unstructured internal data (electronically

---

held text and multimedia); structured data (financial, relationship, or operational databases); and, network and infrastructure metadata. These four data types can be represented in thousands of systems and in thousands of forms. They are individually and together the fundamental elements of understanding an organization’s adherence to compliance controls and conduct standards. In previous examples, in banking and pharmaceuticals, information may go through a risk-based analysis supported by a systematized set of rules to evaluate the data or a routinized checklist that is conducted by a human. In either instance, the data disseminated to represent the completion of this disclosure could be of a wide variety such as an executed PDF, a field in a database, or a video from an online notary.

IV. COMPLIANCE MONITORING AND INVESTIGATION TECHNIQUES IN STRUCTURED DATA

“Successful BSA/AML compliance is a company-wide endeavor, dependent on the actions of employees throughout the organization, including frontline personnel responsible for customer identification program compliance, business line employees that feed data into the transaction monitoring and filtering programs, technology experts that build and manage the monitoring and screening systems, and BSA/AML compliance employees who investigate suspicious activity, file required reports, and oversee the entire BSA/AML program.”

- American Bankers Association

Compliance programs designed to monitor and mitigate the risk of violating BSA/AML and Office of Foreign Assets Control of the Treasury Department (“OFAC”) requirements have become a central focus for regulatory and enforcement bodies over the last

---

fifteen years. As the control of funding has manifested as one of the most effective weapons in the fight against terror, crime and states that jeopardize human rights and global stability, the organizations that police this activity have become more rigid in their application of compliance monitoring standards. Since its enactment in 1970, the Bank Secrecy Act has stood apart from other laws because of its prescriptive outline of acceptable money laundering compliance program. The four pillars of the compliance program described in BSA are: internal policies, procedures, and controls; a designated compliance officer; an employee training program; and, an audit function to test the program. To this day, these four pillars remain the recognized minimum standards for a compliance program.

In 2001, with the enactment of the USA Patriot Act, the requirement for every BSA/AML program to meet these minimum standards was set in stone. Recruited in the fight against organized crime and terror, banks are now responsible for identifying any transaction “derived from illegal activities or conducted in order to hide or disguise funds or assets derived from illegal activities” and filing Suspicious Activity Reports (“SARs”) with FinCEN to guard against being complicit in the flow of illegal funds. In practice, this requirement – and those established by similarly situated organizations such as the Financial Action Task Force (“FATF”) and MAS – became one of the single largest operational challenges in banking history. Facilitating trillions in transactions and funds transfers, in many instances as a correspondent bank (a financial institution providing services on behalf of another), banks were forced to build transaction monitoring and filtering programs at almost an unfathomable scale. Also, with the requirement to evaluate flagged transactions for potential SAR activity, transaction review teams and financial crime investigation groups within banks grew from dozens of individuals to major immutable banking operations consisting of thousands of employees or contractors stretching all three lines of defense.

644 31 C.F.R 103.18(a)(2) 2006.
Finally, the design and implementation of governance to support each constituent part of the program drove thousands of questions across the industry, including - Which function should own the transaction monitoring system, IT, Finance, AML, the Line of Business? What typologies are correlated to our risk assessment? How do we render these typologies in scenario logic, or code, so that we can assess the information available in our transaction databases? Who is qualified to approve that scenario logic? What are the processes and procedures for assessing transactions for suspicious activity? When is it appropriate to notify a customer, or close an account? Who approves the filing of a SAR? The ultimate list of considerations was daunting and the answers often lead to complex stakeholder groups with competing incentives, diverse backgrounds and gaps in communication. However, years later, the immovable object in AML, Counter-Terrorist Financing (CTF) and OFAC programs is the accurate and effective deployment of transaction monitoring systems and the consistent investigation of the “alerts” produced by said systems.

Transaction monitoring systems require three operative components to function effectively: transaction and customer data; policies or rules; and the ability to present flagged transactions per those rules. However, each of these requirements is rife with impediments and challenges to operational consistency. Take, for example, the data element of transaction monitoring systems. Often drawing from diverse data sources in multiple formats, the unexpected mutations of data can render programs useless. In transaction monitoring and filtering, information from different transaction types (wires, credit cards, ATMs, debit card purchases, securities clearing, checks, etc.), platforms (core banking systems, SWIFT messaging, Credit Card Networks, CHIPS, etc.), and processes (Know Your Customer (“KYC”), Lending Application, Suitability, etc.) are all drawn into one environment. Very often, these platforms were created for a purpose other than the management of financial crime.

Systems like SWIFT, created to facilitate the interbank flow of funds, are not geared toward the transparent and complete presentation of transaction details. For instance, in the case of trade
records, the MT 700 series dealing with letters of credit and other trade related messages is often sparse in terms of detail and forces any system to revert to a manual review of any transaction of interest. In other instances, where data source complexity is not the issue, accuracy is. KYC records languish in disrepair, disabling institutions from picking up on high-risk customers that could jeopardize the organization’s financial crime posture. Or, the translation of data from source systems, like the truncation of an address removing a sanctioned country or the incorrect mapping of a transaction code, to a compliance surveillance system can cause substantial harm to a bank’s ability to monitor suspicious transactions or sanctioned entities.

We see the results of these challenges in many public enforcement matters such as *US v. Wachovia*, where Wachovia was found to be complicit in facilitating the transfer of funds through correspondent accounts for casas de cambio ("CDC") correspondent accounts linked to drug trafficking organizations. The culprit, in many instances, was the lack of enhanced due diligence to expose and correct clearly falsified customer and counterparty records used in high-risk transactions. Further, the inability for Wachovia to run even simple scenarios against the transaction data, identifying structuring or high-value round-dollar transactions used by the drug cartels, impacted its ability to demonstrate adherence to the BSA/AML regulations. In another high-profile matter with M&T Bank, the failures were in the management of the compliance program itself, or the lack thereof. The Federal Reserve Bank of New York cited in their agreement with M&T, “the most recent inspection of M&T conducted by the Federal Reserve Bank of New York (the "Reserve Bank") identified deficiencies in M&T's firm-wide compliance risk management program with respect to compliance with BSA/AML Requirements; the Bank's internal controls, customer due diligence procedures, and transaction monitoring processes with respect to compliance with BSA/AML Requirements; and WTC's due diligence practices for foreign correspondent accounts.” These enforcement actions in BSA/AML and OFAC control lapses and others like BCCI and Commerzbank have driven unprecedented regulation into the BSA/AML and OFAC monitoring space.

---

Key stakeholders truly understand the triggering mechanisms underpinning legacy BSA/AML and OFAC monitoring systems, as well as the next generation systems that will ultimately replace them. Organizations must adopt a purpose driven approach that embed their risk mitigation strategies within their technology platforms. No longer can system opaqueness used as reasonable grounds for compliance gaps. Regulatory mandate that companies understand and ultimately adopt technological and analytics based solutions to mitigate risk.

The first of its kind, the New York Department of Financial Services (“NYDFS”), a notoriously stringent regulator, issued its final regulation on banking transaction monitoring and filtering program requirements, Part 504. An extremely comprehensive and prescriptive regulation, NYDFS calls for banks to clearly establish, document, harden and potentially automate BAU monitoring programs, from payment data to investigation findings. In this regulation NYDFS communicates three objectives, to clarify requirements, demand accountability, and emphasize a firm’s need for robust transaction monitoring controls. However, the regulator does not stop there. NYDFS specifies the need for precise items such as, “protocols setting forth how alerts generated by the Transaction Monitoring Program will be investigated, the process for deciding which alerts will result in a filing or other action, the operating areas and individuals responsible for making such a decision, and how the investigative and decision-making process will be documented.” For filtering solutions, NYDFS specifies, “The technology used in this area may be based on automated tools that develop matching algorithms, such as those that use various forms of so-called ‘fuzzy logic’ and culture-based name conventions to match names. This regulation does not mandate the use of any particular technology, only that the system or technology used must be reasonably designed to identify prohibited transactions.” In effect, the regulator, demands each regulated institution adopt and adhere to a COSO compliant AML and OFAC set of internal controls to ensure there is “governance, oversight, and

646 Written Agreement by and among M&T Corporation, Manufacturers & Traders Trust Company and Federal Reserve Bank of New York.

647 New York, Department of Financial Services, Sec. § 504, Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications. www.dfs.ny.gov/legal/regulations/adoptions/dfsp504t.pdf.
accountability at senior levels”. The NYDFS first defines the controls in the three overarching definitions for the control environment:

1) “Each Regulated Institution shall maintain a Transaction Monitoring Program reasonably designed for the purpose of monitoring transactions after their execution for potential BSA/AML violations and Suspicious Activity Reporting, which system may be manual or automated…”

2) “Each Regulated Institution shall maintain a Filtering Program, which may be manual or automated, reasonably designed for the purpose of interdicting transactions that are prohibited by OFAC…”

3) And, “Each Transaction Monitoring and Filtering Program shall require…identification of all data sources that contain relevant data…validation of the integrity, accuracy and quality of data to ensure that accurate and complete data flows through the Transaction Monitoring and Filtering Program…data extraction and loading processes to ensure a complete and accurate transfer of data…governance and management oversight, including policies and procedures governing changes to the Transaction Monitoring and Filtering Program to ensure that changes are defined, managed, controlled, reported, and audited…vendor selection process if a third party vendor is used to acquire, install, implement, or test the Transaction Monitoring and Filtering Program or any aspect of it…funding to design, implement and maintain a Transaction Monitoring and Filtering Program that complies…qualified personnel or outside consultant(s) responsible for the design, planning, implementation, operation, testing, validation, and on-going analysis of the Transaction Monitoring and Filtering Program.”
Second, NYDFS mandates that controls, “be based on the Risk Assessment of the institution.” Third, as part of the control environment definition, NYDFS requires senior management oversight, information sharing and communication, including “governance and management oversight, including policies and procedures governing changes to the Transaction Monitoring and Filtering Program to ensure that changes are defined, managed, controlled, reported, and audited.” This is reinforced by Section 504.1 of 504, which states that NYDFS has “identified shortcomings in the Transaction Monitoring and Sanctions Filtering programs of these institutions attributable to a lack of robust governance oversight, and accountability at senior levels.” The certification requirement is thus intended to effect stronger governance processes and executive accountability at covered institutions. In this context, the certification process begins with “Tone at the Top” that empowers and drives effective compliance programs. Finally, the NYDFS instructs firms to harden the monitoring control environment by constantly monitoring the efficacy of the control utilizing “protocols setting forth how alerts generated by the Transaction Monitoring Program will be investigated, the process for deciding which alerts will result in a filing or other action, the operating areas and individuals responsible for making such a decision, and how the investigative and decision-making process will be documented; and... be subject to an on-going analysis to assess the continued relevancy of the detection scenarios, the underlying rules, threshold values, parameters, and assumptions.”

In terms of practical advice there are three areas that can immediately impact the efficacy of transaction compliance programs. One, the identification, assessment and remediation of critical data sources and elements which allow transaction monitoring and filtering systems to operate. Not all 50, 100, or 150 data points collected on a customer are necessary, or of consequence. Risk weight data elements, prioritize those at the top of the list, and ensure their accuracy. As valiant as the effort may seem, to get several million customers to answer countless questions or boil the ocean across an organization for a piece of internal data,
it can become a distraction. Take the top 30 data points and drive them to accurate results for all customers using artificial intelligence ("AI") diligence tools, Customer Information Program ("CIP") questionnaire technology, KYC follow-ups, proprietary data searches (World Check, Factiva, LexisNexis), and open web content. In compliance monitoring, accurate data is the foundation of a functioning program.

Second, learn from the past. Take SAR activity, UARs and industry benchmarking and consistently backtest both investigations and transaction monitoring procedures in multiple scenarios. For instance, in the case where the SAR filed from a scenario does not correlate to the risks covered by that scenario, determine whether or not that typology is covered by internal systems. Also, determine whether investigations procedures would have picked up other types of SARs that may be incidental to the typology covered by the applicable scenario. For instance, a common mistake is failing to diligence counterparties in a transaction, in at least simple screening or adverse media checks, in instances where the scenarios that are alerted are customer based. Although this brings in web content, a challenging and unwieldy data type, it can vastly improve the accuracy and quality of an organization’s alert generation. The industry, in order to achieve a sustainable productivity level in monitoring systems, must see a shift in model tuning, moving away from the red-herring of false positives and towards a dynamic risk-based approach for identifying key risk indicators. The final point is to thoroughly document processes, governance and standards. Through documented processes, metrics, key performance indicators ("KPIs") and management information ("MI"), an organization can benchmark, measure and improve its compliance monitoring program.

Transaction monitoring as an archetype of compliance monitoring in structured content, whether monitoring gifts and entertainment expenses for Foreign Corrupt Practices Act ("FCPA") violations or analyzing inventory to detect washed assets, teaches two core lessons. First, the unproductively of modern transaction monitoring
systems creates the need for some form of AI-driven solution, as a monitoring system is only as good as the policy driven rules used to currently detect problematic activity. Second, the underlying quality of data is integral to the function of monitoring systems, and if your monitoring systems consume inaccurate data, they will complete inaccurate analysis, return inaccurate results and drive inaccurate conclusions.

But, data quality is just one component of a broader data governance framework that in the coming years must incorporate significantly more data attributes to support future, AI-based transactional monitoring systems. Modern transaction monitoring systems rely on just a handful of data points that are internally stored and periodically updated at fixed intervals. Such narrow, periodically updated data models support rule based systems that lack the breadth of data and open source information needed to truly drive AI based solutions.

The key to transitioning to next generation, AI driven monitoring systems is the pairing of unstructured data with structured content to drive more targeted scrutiny of client and counterparty behavior. Next generation, automated due diligence systems are at the forefront of this evolution. These systems deemphasize legacy data frameworks that rely solely on customer provided data stored in large mainframe intensive IT infrastructures in favor of open-source, unsupervised methods. No longer will it be necessary for organizations to constantly monitor and update customer data using manually intensive, operationally focused processes. AI-based solutions will replace these legacy KYC/CDD mechanisms with automated, real-time, and technology focused processes that extract key customer and counter-party information from open sources, and, just as importantly, utilize machine learning techniques to identify hidden patterns and relationships that ultimately help inform more accurate risk measures. The byproduct will be far less labor-intensive transaction monitoring programs that are adaptable to changes in transaction behavior and thus produce far fewer yet more productive alerts. These systems will leverage advances in behavioral analytics, automated pattern analysis, and machine learning.
V. COMMUNICATIONS IN UNSTRUCTURED DATA AND METHODS FOR MANAGING CONDUCT AND BENCHMARKING CULTURE

“There are understandable, human tendencies that can cause each of us to avoid rocking the boat. People want to be team players. Those behavioral traits can be amplified through a firm’s culture, which can weigh on one’s willingness to do the right thing. This is, unfortunately, what seems to have occurred [at] one of the largest retail banks in the United States. Whether to obtain a bonus or simply to keep a job, employees felt they had to keep quiet and meet sales targets despite the cost to customers.”

- William Dudley, President and CEO, Federal Reserve Bank of New York

Culture and conduct have been hot topics with nearly every major financial regulator in recent years, but the industry initially pushed back against perceived gray areas and vague definitions. However, with the recent change in political sentiment, particularly in the US and European Union (“EU”), regulators across the globe are revisiting the idea of culture as a key ingredient of corporate compliance, meaning it is once again up to financial institutions to interpret and measure this seemingly elusive concept. To accomplish this, without suffering set-backs in compliance controls

or creating a messy patchwork of disparate approaches to risk management, financial institutions and multinational corporations are turning to surveillance in communications and operational systems to find ways of standardizing the measures and metrics of culture. Still nascent in nature, we see organizations adopting the three lines of defense in the monitoring of communications for the purpose measuring risk and culture. To feed this control framework, both corporation and financial institutions have turned to surveillance platforms. Also, taking a page from transaction surveillance, keywords, known as lexicons, have become poor substitutes for typologies and scenarios. However, these lexicons are both over and under inclusive and are not fit-for-purpose when determining the nature and severity of risk in an organization. The question arising from this conundrum, is how do we get to this “gray area” that is constantly changing in nature, language and actors?

William Dudley, President and CEO of the Federal Reserve Bank of New York, defended regulators’ emphasis on culture at the Cornell College of Business Annual New York City Predictions Event. He argued that bad behavior rarely falls into a “gray area,” citing blatant instances of misconduct, including traders “getting together in chat rooms trying to talk about how they can collude to rig a market,” or “consciously doing things to evade any money laundering rules and sanctions.” This assumption, in terms of the explicitness of the behavior evidenced in these communications, is accurate in spirit but wanting in practice. Despite blatant references to collusive practices, the traders often spoke in dense jargon. Using slang like East London Cockney, traders would refer to the size, currency and timing of trade execution in incomprehensible ways such as, “I gt a bully betty at the bell.” If you are scratching your head at the meaning of that phrase, you are not alone. Lawyers

spent months and years pouring over texts, Bloomberg Chats, and phone calls to break the code.

Despite not knowing exactly what they are looking for, regulators still expect organizations to meet the standard of good culture. And courts are not shy to condemn behavior which is detrimental to a fair and transparent market. Citigroup trader, David Madaras, was fired in December 2014 for allegedly affirming another trader’s comment on a client’s proprietary position when he responded, "he’s a seller/fking a," in a 2011 chat. Madaras was allegedly involved in multiple inappropriate components of the chat which revealed the price of the client’s trade, Judge Alison Russell ruled in a judgment on May 26, 2017.\footnote{Gower, Patrick. \textit{Citigroup Wins U.K. Lawsuit Over Firing of 'Good Guy' FX Trader}. Bloomberg, 31 May 2017, www.bloomberg.com/news/articles/2017-05-31/citigroup-wins-u-k-lawsuit-over-firing-of-good-guy-fx-trader.} After many of his colleagues won their tribunal matters, Madaras was held accountable for the conduct he evidenced in his communications. But how do we stem this activity sustainably in the future?

As Menon stated in his keynote remarks at the Australian Securities and Investments Commission Annual Forum, “Ultimately, it is the financial institution itself that must bear the responsibility for getting the culture right.”\footnote{Reading Room, Financial Regulation – The Forward Agenda Monetary Authority of Singapore (2017), http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2017/Financial-Regulation.aspx.} Dudley went further to caution that organizations using existing regulations and law as the guide for good behavior will not go far enough. In the absence of regulatory or legal measures of culture, organizations will have to carefully craft, document and execute their own interpretation of culture. This is why it is so important right now for corporations to start adopting a harmonized approach to developing, enforcing and policing metrics that connote a culture of compliance.
Recent advances in cognitive computing may hold the key to making this possible by moving discreet culture indicators out of gray areas and into black and white clarity, as Dudley suggests. The use of cognitive computing in conduct surveillance, for example, can identify early-indicators and patterns of misconduct, negative sentiment, and systemic pressure across various internal data streams, including email, chat, calls, and HR systems to create a set of metrics around controls violations or misconduct found. Andrew Bailey, Chief Executive Officer of the FCA, confirmed that regulators examine these early indicators and smaller behaviors as the best markers for culture, saying, “culture is characterized by a pattern of behaviors.”

The 2016 UK Market Abuse Regulation ("MAR") could be a fulcrum for a new kind of surveillance, moving first and second line defense methods from ad-hoc manual review to automated and real-time analytics of not only misconduct but to the evidence of good conduct and adherence to controls. The introduction of AI as an enabler for the business and an investigative tool for compliance, will let organizations sculpt the ideal control environment and redefine the very nature of monitoring to meet growing scale and complexity demands. However, the opportunity to learn lessons from prior missteps in structured data monitoring, could lead to better outcomes. Identifying at the outset the appropriate data sources, the iterative testing process to achieve success, and a focus on risk-based analysis, and not just pure volume, could lead to sustainable compliance in the context of conduct and culture.