What is Conduct Risk and How Can Technology Mitigate it?

By Brian Fahey, CEO, MyComplianceOffice

Conduct risk poses an existential threat to companies across industries and jurisdictions because regulators, auditors and other oversight professionals are increasingly holding senior managers accountable for the actions of individuals associated with a firm.

But what exactly is conduct risk, and how can technology help mitigate it?

Defining Conduct Risk

Conduct risk is a form of business risk that refers to potential misconduct of individuals associated with a firm, including senior executives, staffers, vendors, customers, agents and other third-parties affiliated with the firm. Conduct risk is typically associated with human misbehavior, unlike many other forms of business risk, such as a major network outage caused by systemic failure.

Areas of conduct risk that most commonly occur include conflicts of interest, such as improper trading or incentive practices. The forms of misconduct that are most harmful to a firm include deliberate malfeasance, repeated infractions, or isolated breaches coupled with aggravating factors, such as injury. In many cases, a breach entails collusion among perpetrators across enterprise bounds, such as an employee and a third-party sharing material non-public information (MNPI).

To be sure, most employees try earnestly to adhere to their organization's conduct policies. But it takes just one unexpected infraction to damage a company's brand and bottom line — sometimes irreparably.

Conduct Risk as Top Regulatory Enforcement Priority

Across industry sectors, the Foreign Corrupt Practices Act (FCPA) requires listed companies 1) to make and keep books and records that accurately and fairly reflect transactions that could considered bribery, such as gift and hospitality expenses; and 2) to devise and maintain an adequate system of relevant internal controls.[1] In the financial industry, U.S. Securities and Exchange Commission (SEC) Code of Ethics Rule, which requires registrants to establish a standard of business conduct of all supervised persons, was one of the agency's top deficiency areas in 2017.[2] In reaction to the financial market crisis of 2008, the U.K. Financial Conduct Authority (FCA) expanded its Senior Managers and Certification Regime (SMCR) to hold more individuals accountable for their conduct.

The Breakdown of the Classic People, Processes, Policies Triumvirate

To avoid increasingly costly fines and censure, many firms rely on compliance professionals to help them develop, policies, procedures and codes of conduct (employee and supplier) that comply with state and federal rules and reflect the culture of the firm. Qualified compliance professionals have the expertise to help develop and update the compliance program as rules and regulations change.

But they often do not have access to the daily business interactions in other departments. The compliance and senior management teams must rely on the "tone from the middle," that critical middle layer of executive management that interacts directly with supervised persons. Moreover, they typically lack the technical skills needed to manage systems and data, which are an indispensable means of breaking organizational silos to connect people, processes and policies.

The ability to bridge data stores can help compliance professionals mitigate the risk of misconduct. Unfortunately, most firms continue to manage compliance data inefficiently across such disconnected sources as email, network folders, and hardcopy files — manual methodologies that increase the time it takes to manage compliance as well as the risk of processing errors. This also makes it impossible to glean more advanced insight by cross-referencing information across data sources.

There often are blind spots across physically dispersed teams

In the absence of integrated technology solutions, there often are blind spots across physically dispersed teams or insular teams that operate separately from others in the organization. Indeed, especially in mid-tier and large companies, the left hand often does not know what the right hand is doing. For instance, an employee might be planning to give a gift to an executive at a company that, unbeknownst to the employee, is an acquisition target. A gift that would otherwise be an acceptable form of business courtesy could thus be considered a form of bribery post-merger.

Three of the Most Common Conduct Risk Scenarios

Anti-Bribery and Corruption (ABC)

In recent years, regulators around the world have been investing substantial resources to combat anti-bribery and corruption (ABC) law violations, which can arise in many forms within an enterprise.

Do any of the following scenarios sound familiar?

For instance, an employee might receive a gift or expense entertainment involving a third-party vendor, above limits that might otherwise be an accepted business courtesy. An employee might give a lavish gift to a customer or prospective client. A sales team might be inappropriately incentivized and thus compromise the interests of customers. Or a supervised employee might expense a gift or hospitality on behalf of a politically exposed person (PEP) in an effort to influence a business deal.

Organizations often lack the capacity to monitor employee activities to curtail ABC misconduct. For example, when firms submit data related to gifts and entertainment activity, it tends to be entered as free-form text, making incident reporting arduous and time-consuming, if not impossible.

Scenario #1

Regulators recently ordered a hedge fund in a multi-million-dollar bribery scheme to implement new deterrents, and to retain an independent auditor to oversee the changes to its compliance program. The company implemented new software with user-definable rules that enable compliance officers and supervisors to automatically monitor employee gifting activities against company policies such as thresholds and the explanation and size of gifts.

An automated conduct risk management solution that tracks a firm's ABC policy as well as supervised persons and their third-party affiliations makes it not only possible but easy to monitor gifts and entertainment activities to spot problematic relationships and thus thwart corruption.

A move is afoot to mandate a new International Organization for Standardization (ISO) Anti-bribery Management System (ABMS) standard, ISO 37001, developed in partnership by dozens of global entities to help prevent, detect and address bribery and corruption. If the standard becomes mandated as anticipated, companies will need far more rigorous ABC policies and data management controls.

Personal Trading / Personal Account Dealing

Notwithstanding regulators' efforts to publicize enforcement cases involving trading or investment self-dealing as a deterrent, data disconnects exacerbate the challenge of thwarting related offenses. An employee might trade securities of a company in which he or she is or plans to be a director; or may unwittingly buy or sell shares of a company in which his or her firm is planning to make an investment.

These scenarios can impugn the company if an individual executes a trade or deal for the benefit of the firm's account. In that case, not only is the individual on the hook for misconduct, but his or her firm is in jeopardy should the improper trading or investment deal-making come to light.

Companies that host regulated non-public information are obligated to prevent improper disclosures. Ideally, a centralized database identifies affiliations between supervised persons, their third-party affiliations and trading and investment activities that are precleared through compliance.

Scenario #2

In February 2018, the SEC instituted an enforcement action against Deutsche Bank Securities, which agreed to repay more than $3.7 million to impacted customers. The SEC investigation found that traders and salespeople made false and misleading statements while negotiating certain securities transactions, and the firm failed to have compliance and surveillance procedures to prevent and detect the misconduct.[3]

Particularly for trading and investment firms, the ability to associate a firm's policies and procedures with individuals and entities across myriad dimensions – accounting for complex hierarchical affiliations with a company and its subsidiaries, for instance – can yield invaluable compliance insight. This sophisticated data cross-referencing makes it possible to monitor employee trading and investment activities in an effort to protect information barriers and lower the risk of trading misconduct.

Regulators are already leveraging their vast data stores to conduct sophisticated data mining and analysis to thwart trading and investment misconduct. For instance, under the Dodd-Frank Act, the SEC is authorized to go directly to investment advisors' custodian banks to examine potential improprieties.[4] However, the bank does not notify its customer when the SEC approaches it to investigate a breach. Because the SEC is equipped with sophisticated analytic tools, it can see problems a compliance team may not. Thus, it behooves registrants to routinely conduct their own data mining and analysis to identify inappropriate trading and investment activities before regulators do.

Lacking visibility is no longer a good defense

Regulators know that technology is now available to cross-check across siloes to correlate data that supports the compliance function more effectively, as this is what they themselves are doing. Making the case that staffers or supervisors lacked visibility is no longer a good defense should a breach occur.

Conduct risk management software enables firms to automate trading and investment policy management with 100% trade capture, referencing a comprehensive global security master that is linked to a database of company and contact information, dramatically enhancing surveillance.

Outside Business Activities and Third-Party Conflicts

Employees, especially senior executives, are often engaged in outside business activities (OBAs) or relationships with third-party service providers. And supervisors often do not know all of their third-party service providers despite the fact that those entities may be interacting with multiple individuals in the firm. These common data disconnects can lead to compliance breaches.

When the human resources department inputs a new employee or when a line of business engages a service provider, direct questions should be asked to identify if the employee or vendor has a relationship with the firm or with a company affiliated with the firm. Supervisors may be asking the correct questions but not have a central repository to validate if responses represent a conflict.

Scenario #3

In April 2018, a Chief Compliance Officer agreed to settle charges brought by the U.S. Financial Industry Regulatory Authority (FINRA) to resolve allegations that the defendant failed to reasonably supervise private securities transactions and the outside business activities (OBAs) of its registered representatives and multiple third-party firms, in violation of FINRA Rules 3280, 3110(a) and 2010. Without admitting or denying wrongdoing, the CCO agreed to a two-month suspension and financial penalties.[5]

Firms should get into the habit of adding conduct-relevant data into a centralized platform. This way, the platform, cross-referencing predefined thresholds and trends over time, can automatically flag conflicts, whether the company is on the giving or receiving end of questionable conduct.

For instance, an employee may have undisclosed relationships with a vendor or customer, or with a company in which his or her employer will soon have an investment stake. Or an employee may make a political contribution to a federal, state or local campaign that has ties to his or her employer. Without knowing these relationships exist, even a well-intended employee could be viewed as attempting to influence a deal or a politician, depending on how those relationships and deals evolve.

RegTech to the Rescue

As these scenarios suggest, when individuals cross the line from above-board business dealings to questionable conduct, the impact of a breach can be exponentially compounded by financial and other penalties, reputational harm, regulatory sanctions and criminal charges. For both intentional and unintentional misconduct, firms can pay the ultimate price and be forced to disband.

Firms are using software to better manage conduct risk

A growing number of firms are using software to better manage conduct risk. Such solutions help firms track and monitor conduct-related compliance process flows, with a centralized command control dashboard, behavioral risk scoring, document management, reporting, alerts as well as comprehensive approvals processing. However, such systems are only as good as the data that nourishes them.

Integrating Data into A Centralized Conduct Risk Management Platform

The moment a compliance procedure is introduced is the optimal time to define the data within a centralized platform to monitor the procedure. Data should be systematically mapped to monitorable controls before rolling out the procedure. But it's never too late to centralize and cross-reference data to eliminate conduct risk blind spots — even data housed in distributed data stores.

Conduct risk management systems demonstrate to regulators that a company is serious about monitoring its supervised persons, and can be used in defense of a conduct breach—which can occur in even the most thoughtfully safeguarded organizations. Automating process flows with relevant conduct data not only mitigates risk but offers a host of operational benefits. For instance, it reduces the manpower needed to manage compliance while tempering the impact of employee turnover.

When data and systems are configured to cross-reference the actions of supervised persons against a company's policies and procedures, the supervisory and compliance teams can easily and instantly view and share conduct risk insight even as compliance professionals come and go over time.

Without the ability to centrally manage conduct risk data, even firms that pride themselves on promoting cultures of compliance can overlook misconduct that could have been curtailed. Conversely, centralizing and cross-referencing conduct risk data enables firms to empower their people and processes with intuitive tools to manage conduct risk more easily, effectively and cost-efficiently.

---

1. *https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act*
2. *https://www.sec.gov/ocie/Article/risk-alert-5-most-frequent-ia-compliance-topics.pdf*
3. *https://www.sec.gov/news/press-release/2018-13*
4. *https://www.aba.com/Compliance/RegReform/Pages/RR_TitleMenu_Full.aspx*
5. *https://www.johnschapman.com/investment-fraud/former-osprey-partners-chief-compliance-officer-agrees-to-finra-sanctions/*

About the Author

Brian Fahey, Chief Executive Officer of MCO, has been delivering complex technology solutions to meet critical business objectives within the investment management industry for nearly 25 years. He has provided these solutions to large and small investment firms across US, Europe and Asia. His focus over the last 10 years has been building cost-effective conduct risk solutions that can adapt to rapidly changing business and regulatory environments.

About MCO

MyComplianceOffice (MCO) provides compliance management software that enables companies around the world to reduce their risk of misconduct. Its powerful platform lets compliance professionals demonstrate that they are proactively managing the regulated activities of the company, employees and third-party vendors. Available as a unified suite or à la carte, MCO's easy-to-use and extensible SaaS-based solutions get clients up and running quickly and cost-efficiently.

Visit us at
mycomplianceoffice.com

