Why Compliance Programs Fail

Too often, compliance programs seem to be working as intended—until regulators or crises prove otherwise.

ASTRID LUDEMANN

Senior Manager

Business Intelligence and Investigations

London, UK

astrid.ludemann@kroll.com

JUSTINE RADNEDGE

Manager

Business Intelligence and Investigations

London, UK

justine.radnedge@kroll.com

In recent years, compliance programs have moved further up the agenda of corporate boards, reflecting the greater scrutiny corporate behavior is receiving from governments and regulators, investors, employees, customers and the public at large. A properly implemented compliance program provides crucial assurance to all stakeholders that the organization's personnel are abiding by all applicable regulations, internal ethical principles, codes of conduct and other guidelines governing their actions.

The unfortunate reality, however, is that many compliance programs fail to avert the transgressions they were designed to prevent. On the surface, a compliance program may appear to provide systems for identifying and mitigating risks such as money laundering, bribery and corruption, cyber breaches, safety deficiencies and numerous other concerns. In the program's implementation, however, gaps can occur that will hinder its effectiveness. Because months or even years can pass between an incident's occurrence and its detection, compliance programs often appear to be working even though they are not. An organization can have all the pieces in place to show that it is a good corporate citizen—until a regulator comes knocking on the door or a rogue employee commits fraud, whereupon the company discovers that its compliance program isn't as robust as it was thought to be.

There are a number of key reasons for the failure of compliance programs.

PERMITTING A DISCONNECT BETWEEN THE COMPLIANCE DEPARTMENT AND THE REST OF THE ORGANIZATION

Organizations commonly design their compliance programs with little or no input from the people who will have to adhere to them. Compliance departments thus may impose requirements that seem reasonable in theory but in practice are onerous. Common examples include requiring excessive information before undertaking a transaction and implementing controls that do not align with normal business processes. This creates the perception among operational staff that compliance requirements are the tail wagging the dog.

This situation all but invites employees to develop workarounds, giving the impression that all necessary boxes have been checked while in reality overlooking the substance behind the compliance requirements. Such workarounds put the company at risk of non-compliance.

FAILING TO KEEP PACE WITH CHANGE

Given that regulatory regimes and organizational risk profiles are both highly dynamic, compliance programs cannot simply be a static set of rules. The leveraging of personal data for marketing purposes, for example, was a legitimate, organic response to the growth in online business until the EU's General Data Protection Regulation placed stricter constraints on what was permissible. Organizations should be mindful of changes required by their compliance programs (whether due to regulatory requirements or best practices) when moving into new markets or adopting new business models.

UNDERESTIMATING BAD ACTORS

Organizations often implement compliance regimes and controls specifically designed to satisfy regulatory requirements. This approach can fail to take into account the motives and often considerable skill and experience of those who would attempt to circumvent those controls.

FOCUSING ON MECHANICS RATHER THAN MINDSET

If an organization views its compliance function primarily as a set of obligations to fulfill, its compliance education and training is likely to be perfunctory, and compliance will be regarded by managers and employees as less important. Companies with strong compliance programs instill a culture of integrity through clear communication about the need for compliance. They provide regular training in decision-making practices with which employees can successfully navigate real-world scenarios. Fostering a compliance mindset throughout the organization also makes it more likely that legal, sales, human resources and other functions will approach compliance challenges collaboratively.

ALLOWING RELATIONSHIPS TO OVERRIDE POLICY

Much of the conflict between the compliance department and day-to-day business operations derives from the fact that so much of commerce—within the organization as well as between the organization and the world at large—is based on personal relationships. Personal relationships are built on trust, and trust exempts people from the dispassionate questioning that is central to a compliance mindset. In truth, robust compliance arrangements can strengthen relationships by sending a clear and consistent message to external stakeholders. The reality that a rigorous compliance program can coexist with strong professional relationships should be constantly reinforced.

Most organizations rely on internal audit or similar functions to periodically assess the performance of their compliance programs. Generally, these efforts involve verifying that the necessary compliance procedures are in place. This is a good first step, but just as financial audits are not designed to identify fraud, corruption or money laundering, a standard compliance audit—even when conducted by independent outside parties—can sometimes fail to uncover problems. For deeper insight into whether and how their compliance procedures are being circumvented, organizations must move beyond compliance auditing to *compliance stress testing*. Compliance stress testing applies an investigative mindset to the compliance program itself, identifying and probing weak points to test the company's ability to detect and mitigate risk. Beyond merely confirming adherence to procedures, stress testing goes further to determine if risks are actually being addressed. Are assets that have been posted for collateral valued accurately, and can they be recovered? Have red flags in required credentials and documentation been identified and acted upon? Were transactions flagged as potentially suspicious actually reviewed and escalated? Did quality control procedures check for the weaknesses that lead to product failure?

Compliance programs are essential for ensuring adherence to regulations and avoiding proscribed practices. To work as designed, compliance programs themselves must undergo review and examination. Compliance stress testing provides a rigorous means of identifying and remediating weaknesses before regulators and crises bring them to light—which is often too late.