Compliance & Ethics Professional®

December 2017

SCCE

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org

Meet Michael Levin

Senior Director of Compliance, Ethics & Business Practices
Freddie Mac in McLean, VA

See page **16**

by Yaron Hazan

Will compliance become the new Sarbanes-Oxley?

» Industry-driven standards raise the bar of compliance even higher than regulatory scrutiny.
» No identified breach does not mean your organization is compliant.
» Risk assessments are important but will not tell the complete story.
» Culture is the basis for appropriate behavior.
» An effective compliance program is one that would pass the investigation test.

Throughout the last 10 years, compliance became—mainly for financial institutions—one of the biggest risks. These days, corporations from all industries invest in compliance programs and acknowledge the significant risk. The understanding that compliance is an important issue is driven by two main forces:


Hazan

Regulatory arena: Legislation evolved, and regulators' expectations were clarified through new rules and fines; standards and requirements are published at a higher frequency than ever.

Industry standards: Banks and leading corporations set their expectations through contracts, questionnaires, audits, and reviews. The message is clear and direct: Either you can demonstrate compliance, or the business relationship will be in danger.

While regulators seem to compete with each other on the strictness of the requirements, companies struggle to achieve an effective compliance program that would be strong enough to meet industry expectations.

What defines a compliance program as "effective" or "strong"?

Measuring a compliance program can be done using several methods/indicators:

1. Number of identified breaches
2. Audit/regulatory review findings
3. Assessment of residual risk and level of exposure
4. Adherence to adequate procedures (e.g., standards published by regulators/ global organizations)
5. Indicators for a holistic compliance culture

Breach identification: Limitations of size

Large banks and corporations struggle to identify all breaches that have occurred. Stakeholders cannot be sure the organization implemented a comprehensive program that will identify all breaches and that the risk of non-compliance is under control.

Audit findings: Current programs

Internal and external reviews focus on the design of the control environment and the effectiveness of the critical controls. The reviews are as good as the leading auditor's understanding of the matter, and they usually focus on the same findings identified in other business units/territories. In many cases,

audit review findings and real weaknesses are not identical.

Risk assessment

The risk of non-compliance is assessed by senior managers. The reliability of these assessments is always questionable due to the following paradox:

- If leadership acknowledges there are weaknesses in the control framework, why are these not managed?
- Managers may believe that a "green" ranking is the goal in order to demonstrate strong managerial skills.
- Managers may feel that ranking a risk as "red" or "critical" will convince management to increase budget and recruit additional employees to the team.

Managers may feel that ranking a risk as "red" or "critical" will convince management to increase budget and recruit additional employees to the team.

These examples explain some of the challenges that arise while conducting risk assessments in various companies. Still, the biggest challenge in relying on risk assessments is the fact that if we look at the companies that were found guilty of violating the law, they all conducted risk assessments prior to the ruling.

Adherence to adequate procedures

In order to face the abovementioned challenges, regulators publish their perspective of a gold standard. For example, *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, published by the SEC in 2012, as well as *The Bribery Act*, published in 2010 by the UK government, both try to set the standard for anti-corruption compliance programs.

Although it is not fair to ignore the importance of procedures, top-level commitment, due diligence, risk assessment, communication and training, and ongoing monitoring as the basic elements, an organization may invest in these aspects and still fail to comply with the main regulatory requirements (e.g., by bribing government officials to gain business in developing countries). There are some foundations that come first. These foundations will not work on a stand-alone basis. An organization should maintain the abovementioned elements on top of these foundations: culture, evidence, investment, and automation.

Culture

As described in my article published in the June edition of *Compliance & Ethics Professional*, "Compliance begins in Kindergarten: Practical implementation of a compliance culture,"[1] there are educational elements for a compliance culture that are not taken into account. Examples of the basic principles for implementing a compliance culture are:

- Clear message from leaders covering limits and expected behavior
- Role models
- Compensation and sanctions
- Cooperation between business teams and functions
- Experience-based learning

Most organizations are not there yet; some do not know how to implement such a culture;

and in any case, it is not easy to measure this element.

Evidence: Investigation/regulatory review

A comprehensive compliance program is a program that, in times of a real test, would serve the organization as a shield against regulatory fines, reputational damage, or even potential criminal proceedings.

A major issue large organizations face when they are under investigation is the ability to provide evidence that management has invested enough to ensure that processes are aligned with the relevant regulation. In any legal proceeding, judgment is based on evidence; hence, the importance of documentation and data mapping increases, and the procedures that were improved define relevant data as a potential "record" for legal proceedings. The critical point in time that reflects the organization's program effectiveness is the outcome of such an investigation. If an organization could not provide the relevant documentation to prove right deeds, the result is regulatory sanction.

Investment: Financial measures

Another way to test how seriously the program is taken by leadership is the price. Business leaders measure success by numbers and costs. For them, budget discussions should be the same for compliance and other functions. When senior managers heard that my compliance team should be tripled compared to previous year, they could not understand why they should pay for such a dramatic increase in operational costs. If cost is increasing, leaders expect an improved results. Isn't that the case?

Any business operation should have key performance indicators (KPIs). What should be the KPIs for an ever-growing compliance program that is a "cost center" and not considered a "growth engine"?

Business leaders measure success by numbers and costs. For them, budget discussions should be the same for compliance and other functions.

Investment: What is the price of an effective program?

In most cases, companies fail when they try to implement a compliance program, since they do not expect and assess the resources needed. For an organization that did not have a compliance officer/team, recruiting one senior expert is a 100% increase in terms of cost and investment. Stakeholders may honestly say they have done enough to align with industry expectations and standards, but the paradox is that once you start with the design of a program, you just start to realize how complex it is.

Automation

We are experiencing today the digital era in which consumers expect to receive any type of product or service electronically—web-based and immediately.

Proactive and modern management will search for the most up-to-date solutions that will provide automated controls and reduce labor compliance-related costs.

Currently there are no compliance systems that provide end-to-end solutions to compliance needs, and the question is, why?

Traditionally, banks and large corporations increased the investment in compliance only because they had to; therefore, the relevant

solutions they used were partial, narrow, and provided an answer only to a small part of the compliance process's challenge.

Within this category, leading examples are: the transaction monitoring (TM) solutions, customer and third-party screening, and negative media screening, not to mention the various workflows that do not provide any professional value add other than organizing processes.

Breach reports, audit findings, risk assessments, and procedures provide an incomplete view of the program's effectiveness.

It has been recognized through global surveys that compliance officers do not rely on their systems and seek additional ways to make decisions. The bottom line is that senior management as well as the board of directors cannot attest that their compliance program is effective.

How all this is connected to Sarbanes-Oxley

According to the Sarbanes-Oxley (SOX) standards, corporations are required to declare that the supporting processes that impact the financial reports are efficient and tested. This requirement resulted in SOX-driven processes and controls in a checklist approach to ascertain that the output from the financial reports is reliable. The law requires the CFO and the CEO to sign that they personally checked the processes supporting the numbers published in the financial statements and that these are reliable.

The advantage is reliable standardization when consolidating data for financial statements. The sign-off is provided by the CEO and CFO and audited by accounting firms. Is this where we are heading in the compliance domain?

A recently published rule by the New York State Department of Financial Services requires regulated institutions to submit annual attestation, including board resolution and compliance reports covering the effectiveness of anti-terrorism transaction monitoring and sanctions screening.[2] Naturally, it will create assurance processes around the compliance domain, and banks will create a checklist to test their compliance environment. The new regulation will force senior leaders to be involved and understand how effective their program is.

Will this achieve the desired outcome?

Summary

Compliance programs are based on the regulatory arena and industry standards, learned through painful experiences from organizations that were found non-compliant and from the experiences of leading consulting firms.

The common methods for testing a compliance program rely on a traditional perspective that seeks measurable processes and outcomes. In most cases, the program is not effective and fails the most important test: the crucial time of regulatory investigation.

Breach reports, audit findings, risk assessments, and procedures provide an incomplete view of the program's effectiveness. Non-experienced organizations will need to start with a holistic program that includes these elements and the traditional approach. Assurance reviews and annual attestations will add comfort that senior leaders are involved. Still, the programs would not be effective, not to mention cost-effective. To my view, these are the missing foundations for an effective compliance program:

- Culture
- Systems
- Documentation

These are the cornerstones for an effective compliance program that are hard to test, and unfortunately, they are first tested during an investigation.

Culture

For the culture aspect, see my article in June edition of *Compliance & Ethics Professional*. Elements of a compliance culture could be tested, and the assessment of the design may be comprehensive.

Is this enough to determine that the implementation of a compliance culture is effective? Can leaders attest that the compliance program matches the regulatory expectation? The checklist will not tell the story.

Technology and systems

This aspect is even more problematic to test.

Which systems provide adequate solutions for compliance? There are workflow systems that support the completion of a certain process. There are data management systems that provide management information. Still, all current systems provide a partial solution to the needs of compliance. In order to attest that the compliance processes—in the example given above covering anti-money laundering—are effective, leaders rely on old-fashioned and partial systems that, in the most optimistic view, provide a 90% false positive alert for the TM example.

In many areas in life, the invention of one domain arrived from other domains. Current financial technologies (fintech) trends brought sophisticated technology solutions to new industries and use cases.

I had the opportunity to review a few dozen systems in the past 18 months as a mentor for start-ups in a fintech hub and as a consultant. There are some successful systems that provide real effective solutions to compliance-related challenges. Testing with the old-fashioned system, that all stakeholders would admit does not provide the expected results, means nothing.

Testing with the old-fashioned system, that all stakeholders would admit does not provide the expected results, means nothing.

Documentation

Documentation is critical, but the importance is learned when it is too late. Can an organization work in "investigation mode" as a routine? Effective documentation is a combination of systems, processes, and culture.

I believe that turning compliance into a structured process and providing annual attestation is only halfway. The unfortunate outcome might be that once attested as effective leaders, managers would feel it is time to pull the brakes, focus on budget perspectives, and find themselves exposed as before. ✳

1. Yaron Hazan: "Compliance begins in Kindergarten: Practical implementation of a compliance culture" *Compliance & Ethics Professional*, 2017;14(6):81–83.
2. New York State Department of Financial Services Superintendent's Regulations: "Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications." Available at http://on.ny.gov/2xK03da.

Yaron Hazan *(yarok02@yahoo.com) works as the Financial Crimes Solutions subject-matter expert at ThetaRay in Hod Hasharon Isreal.*
bit.ly/li-YaronHazan