feature

Technology and Regulatory Compliance in Global Organizations

Stuck Between a Rock and a Hard Place

For big corporations, doing business in today's world comes with the good (profits, shareholder satisfaction, growth into new and emerging markets), the bad (regulations, laws) and the ugly (competition).

The recent economic downturn that virtually brought the world to its knees was largely attributed to greed and avarice within the financial sector of the major economies "encouraged" by the lack of proper enforcement of regulations that the gatekeepers were supposed to enforce. According to Lord Adair Turner, speaking as chair of the UK Financial Services Authority on 6 February 2013, "The financial crisis of 2007 to 2008 occurred because we failed to constrain the financial system's creation of private credit and money."[1]

Complete collapse experiences were avoided by governments proactively bailing out major players and initiating fiscal policies aimed at restoring confidence in the economies. The changes did not stop there, as regulatory agencies also underwent a raft of restructuring, realignment and reassignment. For example, in the UK, the Financial Services Authority (FSA) was replaced by the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA), which was a move toward greater scrutiny of the financial sector, and the Commission de Surveillance du Secteur Financier (CSSF) in Luxembourg embarked on a recruitment drive and increased the size of its teams to cope with the increased scrutiny of financial institutions.

These agencies invariably went back to doing the task they were originally created to do by beefing up capabilities and resources to facilitate the effective monitoring of the letter and the spirit of the regulations in their various jurisdictions. Big companies suffered massive penalties for being noncompliant. For example, in April 2013, the UK Financial Conduct Authority fined EFG Private Bank, a UK subsidiary of the Switzerland-based EFGI Group, UK £4.2 million for anti-money laundering (AML) failures. This followed the UK £8.75 million fine given to RBS-owned private bank Coutts the previous year for deficiencies in its AML procedures.

Suddenly, financial institutions can no longer only pay lip service to regulatory compliance because regulators now have capabilities that allow them to perform assessments at a level of detail previously unimagined.

Senior officials of institutions with huge responsibilities to their shareholders are embarking on a zero-tolerance policy to noncompliance within their firms, and rightly so. However, the challenge for the majority of global firms is how to comply with regulations in the various jurisdictions in which they do business while still upholding the corporate agenda of centralization, harmonization, and streamlining of processes and procedures with a view to economies of scale.

Taking the CSSF in Luxembourg as an example, the regulations on governance and oversight stress the retention of "decision-making centers," knowledge and expertise in Luxembourg when activities are being offshored. It also says that the institution client data cannot be stored overseas unless a certain number of criteria are met. These conditions include the explicit consent of the client to have data hosted out of the country and the segregation and encryption of the data while they are hosted outside of the country.

Now, one can argue that meeting the spirit or the letter of these regulations is not rocket science and the regulations could be easily followed. The reality, however, is that various compliance and legal teams will have very diverse views. These views are based largely on the all too familiar challenges of lack of clarity of the regulatory requirements, lack of prior engagement by regulators of stakeholders for whom these rules are meant, and very ambiguous regulations that serve to enrich the pockets of legal counsels but create a nightmare for institutions when it comes to implementation.

Ola Bello, CISM, CISA
Has worked in IT in various roles for 20 years. Bello has concentrated on information security during the last 10 years, and his last two roles have been as information security manager and information security officer of a large investment bank. He is also a working group leader in the ISACA® Luxembourg Chapter, where he leads the Technology Compliance Working Group.

©2016 ISACA. All rights reserved. *www.isaca.org*

This article is not about who is accountable for understanding regulations (the regulator? Or the regulated?). The focus is to posit how to remain compliant while looking after the bottom line. This is the rock and hard place between which global organizations find themselves: choosing whether to implement exactly correct controls in each jurisdiction or to implement consistent, global controls that are adequate.

The Role of Compliance

What is the role of compliance teams within these large global organizations? Most financial institutions have local compliance teams whose role is to understand the laws and regulations of the jurisdiction in which they operate and to ensure that all compliance risk are identified and highlighted.

The challenge for compliance teams becomes how to articulate the requirements in "tech speak." For example, a regulation may say data must be encrypted, but does not provide guidelines on minimal standards expected or what controls to implement in ensuring compliance. This creates a situation in which the solution implemented may not be adequate in meeting requirements because the regulation was not explicit.

For example, according to the CSSF Annual Report 2013:

> *Despite the wide-spread use of cryptographic technologies, the CSSF noted that in some cases obsolete protocols were implemented, or encryption algorithms and key sizes were no longer in line with best practices. Transport media that are commonly reputed as secure, and were therefore generally non-encrypted by financial professionals, proved after thorough analysis to be insecure.*[2]

The question then becomes: Do compliance teams need to build technical capabilities to facilitate better appreciation of regulations from a technology standpoint and avoid unnecessary costs incurred as a result of the lack of detail?

The Role of Legal

When counsel is sought—both within organizations and externally—why are different messages given? This is not a rhetorical question, but rather, it is meant to be thought provoking.

Technology teams need clear guidance and find it frustrating when a requirement that is seemingly straightforward invokes lengthy debates and emotions. For example, a regulation may state that an organization "must always have permanent full control over the resources under their responsibility and the corresponding accesses to these resources, primarily for compliance and governance reasons and secondly to protect confidential data subject to professional secrecy." In this context, "permanent full control" in legal terms takes on different meanings, and having a stakeholder approve a request for access to a resource can be considered adequate in meeting the spirit of the regulations. However, from a technology perspective, this is definitely inadequate because it is as if saying, "I will keep the keys to the front door of my house, and I can give them to you whenever you want them. Once you have the keys in your possession, I do not know or care if you bring your entire clan to my house and destroy the contents—I am still safe and secure."

Bridging the Gap Between Legal and Compliance and Technology

The previous analogy is a classic example of the challenge facing global institutions in different jurisdictions, where, as an example, global firms need to make decisions to either implement technology that facilitates permanent and full local control over a resource managed in the local jurisdiction or build a centrally located and managed infrastructure to support a global organization.

Compliance with the local regulations in such cases will definitely require reengineering of tools, applications and infrastructure, which may result in huge cost implications that hurt the bottom line—and, invariably, unhappy shareholders.

©2016 ISACA. All rights reserved. *www.isaca.org*

On the other hand, institutions can take a level of comfort in a less-restrictive approach of, for example, simply having a local stakeholder give the approval and not invest in technology controls that will enforce full permanent control.

As the costs of compliance continue to rise and financial institutions become more regulatory risk averse, can huge investments in local technology controls be justified, especially when less expensive processes and procedures may suffice?

Compensatory Controls

Staying afloat means being profitable for companies, and the cost of implementing technology that ensures compliance with local regulations can have a major impact on the overall profit if not properly managed.

Legal and compliance always err on the side of caution with regard to the interpretation of regulations. The truth of the matter is that in a global organization, compliance in every jurisdiction where business is conducted will lead to the creation of "cottage industries" within the organization—a proliferation of discrete and dissimilar technology implementation—that contradicts the more efficient approach of centralization and harmonization of processes.

It is, therefore, sensible that adequate compensatory controls that are consistent and can be replicated across various jurisdictions should be the right approach and may suffice. These controls may include periodic reporting and metrics, service level agreements (SLA) or other contractual agreements between local and core groups, as well as local governance structure with clearly defined escalation paths into regional and global governance committees.

The major test is how to treat investor data in offshore locations, because most regulations are very strict where confidential investor data is concerned. Having a governance and oversight process in place will not suffice without adequate investment in encryption technology, for example. Having a contractual agreement between local and central groups within the organization does not exonerate the institution's accountability.

Profitability and Doing the Right Thing

How far can organizations push back the line between doing the right thing—albeit at a huge expense—and implementing controls that can be considered adequate in meeting the spirit of the regulations?

This is the rock and hard place situation that all global organizations grapple with regularly. Where the line is drawn between doing it right and having controls with appropriate mitigations will depend on the nature of the company's product offering and the risk appetite of the firm.

Endnotes

1 Positive Money, Financial Crisis & Recessions, *www.positivemoney.org/issues/recessions-crisis*
2 Commission de Surveillance du Secteur Financier (CSSF), *CSSF Annual Report 2013*, 2013, *www.cssf.lu/fileadmin/files/Publications/Rapports_annuels/Rapport_2013/RA2013_EN_full_version.pdf*

©2016 ISACA. All rights reserved. *www.isaca.org*