Title: The Competent Complier: How FIs Can Prepare for the Future of Regulation
Author: Dr. Alec Shuldiner, Basel Consulting, www.baselconsulting.com

Summary: Ever-increasing regulation appears to be the norm for the financial services industry. Although the sources of that regulation are many and changing, certain common capabilities are increasingly emphasized in the majority of these regulatory demands. Financial institutions which internalize relevant competencies will be able to handle both current and future requirements, those which do not will struggle.

****

Regulatory requirements in the financial services industry have been growing more complex and onerous year by year for at least the last couple of decades. Nor is there much reason to believe this trend in regulatory overhead has played itself out (see box: "What drives regulation?"). The current sources of inspiration—continuing economic uncertainty and the consumer concerns it fosters, the ongoing international push to reduce the size of global "black" financial flows available to criminals, and the amount of recently-issued regulation which has yet to be worked out in practical terms—are all still running strong, promising new demands still to come. For FIs, the question then is not simply "how do we comply?" but as important, "how do we remain compliant in the face of an ever-shifting compliance target, and how do we do so at an acceptable cost in terms of time and resources?"

What drives regulation?

- Internal to financial industry:
  - New theories (e.g., quantifiability of operational risk)
  - New technologies (e.g., the Internet)
  - New products (e.g., derivatives)
  - Newly discovered sources of actual or potential financial instability (e.g., chance of breakdown in integrated payment processing systems)
- External to financial industry:
  - General market volatility (e.g., dot-com boom and bust)
  - Public perception of financial industry and business in general (e.g., Enron/Ahold scandals)
  - Change in political leadership (regulating bodies are usually politically independent, but the legislation governing their activities is not)

The Current State of Change

FIs must concern themselves with general corporate regulation as well as with the specialized requirements handed down by financial authorities. Even in the simpler cases—Dutch investment firms operating solely in the Netherlands, for example—there has been considerable change in just the past couple of years in domestic directives, general and financial alike. All publicly-listed companies must concern themselves with the Corporate Governance Code, which was updated only just this past year, and which has implications even for privately-held firms. This Code, like America's Sarbanes-Oxley Act, is intended to improve corporate governance activities and to increase the transparency of those processes, allowing market pressures to supplement governmental authority.

The Netherlands has also introduced an entirely new regulatory regime specifically for financial services. Various parts of the Financial Supervision Code are being rewritten (most notably the *Wet financiële dienstverlening* or "Law Governing Financial Services") and radical organizational changes are underway as well. Previous to 2002, Dutch FIs were regulated by sector and thus were typically responsible to only a single regulating body. Now, although the number of regulating agencies is being reduced (De Nederlandsche Bank and the Pension- and Verzekeringskamer are merging), regulation is by function, which means that a single institution will in most cases be responsible to both the DNB and the Autoriteit Financiële Markten, guaranteeing to the one that it is sound financially, and to the other that its commercial offerings are in accordance with the rules governing market access.

The DNB, spurred on by the new Basel accords, is in the midst of a massive upgrade of its own operations and is now entering a period of particularly energetic oversight activity, necessary to fulfill its obligations under "Pillar II" of these accords. Pillar II demands that financial regulators review each bank's internal evaluations of its credit, market, and operating risks, and provide for increased capital holding requirements in those cases where a bank is found wanting. The immediate result is a particularly intensive period of interaction between regulator and regulated, one which is expected to last well into 2007.

So much for the simplest cases. When we move beyond them to the multinational FIs matters grow exponentially more complex. If operating in the US—and all of them do—these top-tier banks face a slew of recent legislation including The Patriot Act and the even more demanding Sarbanes-Oxley Act [SOX]. For FIs, the anti-money laundering provisions of the Patriot Act are of concern: they require extensive reporting of suspect transactions, demand training of bank personnel in methods for detecting money laundering, and raise the bar generally for "know your client" regulations. SOX mandates, among other points, more intensive communications with shareholders, the creation of ethics policies, the preservation of paper trails, and direct involvement of senior management with financial reporting, all designed to make corporate governance more rigorous and transparent (and, in the event of a failure in such governance, to make assignment of blame unambiguous). SOX affects every company listed on a US exchange.

Nor is this the end of compliance, or compliance-type worries: each central bank may choose to interpret Basel II differently and thus may pass on different requirements to those banks operating in its country. Furthermore, publicly traded FIs must also report in a separate accounting regime (GAAP) if traded on the US markets, and even those accessing only the relatively undemanding bond market must still be quite careful not to run afoul of rating agencies, for example, which serve a quasi-regulatory function. And these matters, too, evolve over time.

Core Compliance Competencies

None of the compliance requirements described above are arbitrary, and while the regulations may be numerous, the justifications behind them, even taken altogether, are few in number. All of the regulations mentioned above are designed to do some or all of the following: to balance risk with reserve capital within each FI and the financial system as a whole; to guarantee that shareholders have sufficient—and sufficiently accurate—information about the companies they own; to detect illicit flows of money; to address the potential for systemic breakdowns; and to encourage responsible and moral business behavior.

Similarly—and this is the good news—the corporate skills required in order to remain in compliance with all of these regulations are also limited in number. Setting aside ethics (a core competency which should hardly have to be legislated), the compliant FI must assess its risks accurately, keep its core technologies sufficiently flexible so that radically new reporting requirements do not require a complete overhaul of the company's IT systems, promulgate its control and risk measurement systems not just throughout its own operations but also into the operations of its business partners, and, wherever possible, eschew complexity. A host of details must be attended to—information must be collected from every corner of a financial group's operations and disseminated to a wide variety of interested parties, including management, the board, regulators, and the investing public—but the core competencies of compliance are limited in number. Some more on these skills, then, below.

Risk Assessment

No regulatory body has done more to encourage the spread of risk assessment as a discipline in financial services than the Basel Committee on Banking Standards. The first set of Basel Accords focused on credit risk, namely the likelihood and effect of client defaults. Basel II, so-called, refines those requirements and adds a set of rules for evaluating and reducing operational risk, primarily the chance and consequence of inadequate attention to internal procedures or systems. The common element throughout is *risk assessment*: the enumeration and weighting of possible undesirable events.

Risk assessment in some areas—most notably credit risk—can be conducted with considerable precision, but operational risk assessment remains more art than otherwise: credit risk is calculated by making reference to statistically determined default probabilities, but these actuarial principles do not offer the same insight into internal fraud, for example, or the chance of a damaging public disclosure. Ironically, bank operations, even in such relatively standardized areas as cash machine logistics or call centers, remain less susceptible to rigorous analysis than do bank customers. Furthermore, credit risk ultimately devolves to one thing: the probability and effect of default. Where operational risk is concerned, however, the types of undesirable events to be anticipated are legion.

Risk assessment capabilities must, therefore, be upgraded. Without statistical tools or a tightly limited range of negative outcomes, operational risk assessment requires a great deal of custom work, and especially so where the financial institution is exploring new ground. E-banking and many other IT-intensive activities present a particular and growing challenge in

this respect. Risk assessment in these areas cannot be done via checklist nor by individuals who do not possess considerable technical knowledge. Also, it is best done not after-the-fact but as part of the development process itself. Ideally and practically, operational risk assessment should be a continuous process, the goal of which is not simply to produce static summary documents, but to tap the awareness of potential weakness which exists at the operational level on an on-going basis.

This can only be done if a bank's operational management understands and can contribute to operational risk assessment. The insight into the firm's day-to-day activites which those managers then generate should be used as the basis for meeting the demands from Basel and elsewhere. Approached in this manner, risk assessment is transformed from a frequently sterile exercise into a capability which significantly enhances an FI's competitiveness, in addition to keeping it on the good side of regulators.

Flexible Technology

Some argue that the multiplicity of regulatory demands requires a monolithic response: an integrated system that allows an institution to take advantage of the common demands of Basel II and SOX, for example, which do share certain operational risk requirements. But some bankers are leery of this approach, concerned that massive investments in enterprise solutions are destined to become that most-feared of IT horrors, the legacy system. No doubt some of these total compliance solutions can answer current requirements, but what the prospect of future regulation makes clear is that the ability to evolve those systems radically is a must.

That IT development is required to deal with the latest generation of compliance requirements goes without saying, and likewise it is certain that in some cases outsourcing that development is the best answer. But whether done in-house or not, a choice may always be made between more and less flexible technologies. The same applies for IT development which is undertaken for reasons other than enhancing compliance. Regardless, the wise choice at this juncture is to demand flexibility: security, functionality, cost-effectiveness, and other elements which used to be necessary trade-offs for flexibility are no longer so. Given this, the context of a rapidly developing regulatory environment demands that flexibility be made an absolute prerequisite where IT is concerned. Learning to manage flexible systems—developing the necessary technical and design expertise, as well as the specialized operational capabilities that flexibility requires—is another compliance necessity which likewise increases an FI's overall competitiveness.

Managing Control and Risk in Partnerships

E-banking has changed the face of financial services, but perhaps as radically it has changed what goes on behind that façade. Delivery of e-banking products typically involves a network of services, not all of which are provided by the bank itself. These include technical development and maintenance, hosting, and possibly part of the transaction processing as well. But while elements of an e-banking service can be outsourced, risk cannot be. Indeed, FIs, in outsourcing, take on something of the relationship to their suppliers that the various regulators have to these same FIs: it becomes their job to guarantee the contractor's compliance with security and other operational and technical standards. Similar challenges are encountered wherever outsourcing is used, which is to say in an increasing range of bank activities.

Growth in outsourcing and the inherently distributed nature of Internet services places a premium on careful supplier selection and on effective contract creation and management. FIs must develop minimum standards to be met by potential business partners, standards which guarantee that suppliers which are not able to match or exceed the bank's own control and risk practices are weeded out. In addition, they should focus on improving their ability to contract quickly and cheaply, and should develop methods for measuring the success of different contract arrangements over time. In an environment which stresses a heightened awareness of operational risk, only FIs with superior partnering skills will be able to bear market and regulator scrutiny comfortably.

Avoiding Complexity

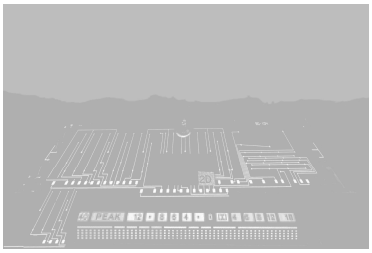
The essence of the theory of market discipline is that greater transparency into a company's operational capabilities will encourage greater competency therein. This theory lies at the heart of SOX and the Dutch Corporate Governance Code, and the concept of transparent operations and the market discipline which is assumed to result also makes up the third pillar of Basel II. Dutch banks, like Dutch homes, are now supposed to keep their curtains drawn back. But it does little good if the market cannot understand what it sees when peering in the window, and far less should the view reveal a mess. Royal Dutch/Shell has finally bowed to market demands that its confusing corporate structure be simplified, and FIs which maintain a similarly rococo organizational schema would do well to follow.

Nor does this principle apply solely to those rooms visible to the passerby. Complexity anywhere within the organization makes control and risk assessment that much more difficult and, by providing more hiding places for fraud and incompetence, it increases operational risk. And since operational risk is measured both at the level of individual activity and in summary across the entire enterprise, this principle must be pushed as a corporate value at every level of the organization. Designing for simplicity requires a particular mindset and unique skills, neither of which are common. Mastering this ability will provide FIs with long-term benefits not only in compliance but ultimately in competitive capacity as well.

Basel III

How will internalizing these capabilities enable an FI to deal with future regulation as well as the current compliance challenge? Imagine Basel III. Basel II raised the bar by greatly refining the credit and market risk formulae for regulatory capital and by introducing operational risk as a separate contributor to the capital requirements calculation. Those operational risk measurements, like Basel I's credit risk metrics, are relatively crude. It seems a safe prediction that as operational risk practice grows more sophisticated the regulators will eventually seek to find a way to spread best practice standards across the industry. As like as not the Basel Accords will be used as the means to do so, just as best practice credit risk measurements are now being disseminated by means of Basel II.

If this logic holds then Basel III may be expected to bring with it not only new requirements for operational risk management, but also new reporting demands designed to provide regulators with proof of banks' compliance in this area. The bank which runs streamlined operational systems designed on sound risk management principles and built using flexible technologies will have an advantage, as will the bank which has constructed those systems on the basis of reliable, properly documented and risk assessed partnerships. But don't take my word on it: next month, an interview with the DNB.



Dr. Shuldiner is founder and principal consultant at Basel Consulting, a design and management consultancy focused on risk assessment, innovation strategy, and fraud minimization.

Please direct feedback or questions on this article to alec@baselconsulting.com.