

JRF  
6,3

## The Michael Mainelli column

### Competitive compliance: manage and automate, or die

280

#### **You have paid the compliance costs – now read the textbook**

It had to happen; now we have the definitive UK corporate governance textbook: *Corporate Governance* by Dr Kathryn Vagueur (see Vagueur, 2005). And it is good. Dr Vagueur not only lays out the essentials of governance, she also includes challenging true/false, multiple choice, in-depth, and case-study questions. Hers is a significant work and a good starting point for people interested in the history and current state of corporate governance. She points out that societal demands for corporate governance, and we all know exactly (sic) what that means, have led to numerous different forms in the US, UK, France, and Germany, each exactly (sic) meeting its society's needs perfectly.

Naturally, we find different forms for governance within these countries for listed firms, large private firms, and smaller firms, let alone government entities or non-governmental organizations (NGOs). We really do not know what we want in each country, before considering imposing standardized international structures. Further, she highlights one of the great contradictions of most organizations: why is the finance director (or CFO) responsible for both the reporting of performance and the delivery of a large element of performance, i.e. financial efficiency? This contradiction vexes one of the key elements of good governance: compliance – i.e. proving that you are doing what you say you are doing.

One could almost caricature two contradictory finance directors – one, the MBA-trained aggressive financial engineer full of off-balance sheet vehicles, sale and leaseback schemes, and highly geared derivative strategies; the other, a stereotypically dull numbers person insistent on chasing down the final penny and presenting an accurate report of the exact state of today's affairs regardless of any political discomfort. In today's typical board, most finance directors are expected to mix parts of both, with attendant conflict and tension about how far they have swung to one extreme or the other. This tension was touched upon in an earlier paper (Mainelli, 1999) that postulated the need to separate the "compliance" functions of the finance director from the "operational" functions. Perhaps compliance has grown so large that finance directors need to be replaced by a "compliance director" and a "financial engineering director."

#### **We compete under the consequences of compliance**

Governance is not compliance, and compliance is not just about regulation, but the Centre for the Study of Financial Innovation's annual "Banana Skins" (Centre for the Study of Financial Innovation, 2005) survey shows that top risk for banks is "too much regulation," up from sixth out of 30 in 2003. From a city of London perspective the burden of regulation and quasi-regulation is increasing:

The author would like to thank Dr Kathryn Vagueur for the advance manuscript that inspired this column, and Freddie McMahon for being the "grit" that forced this paper forth.

- *Corporate governance*: the 1992 Cadbury Report, 1995 Greenbury Report, 1998 Hampel Report, 1999 Turnbull Report, 2003 Higgs report, German KonTraG corporate governance reforms, Sarbanes-Oxley Act 2002, and the OECD Principles of Corporate Governance.
- *General compliance*: Basel 2, Sarbanes-Oxley (Section 404), the Patriot Act, Anti-Money Laundering, the Financial Services Modernization Act, the Insurance Mediation Directive, Privacy and Electronic Communications (EC Directive) Regulations, the Freedom of Information Act 2000, substantially different International Accounting Standards (e.g. IAS 39), Data Protection Act 1998, and the Financial Groups Directive.
- *Regulators' rules*: those from the FSA, SEC, OCC, BAFIN, etc., let alone SAS 70 or ISO 9000 as voluntarily incurred compliance, or industry trade association voluntary compliance codes.
- *General business regulation*: health and safety, COSHH, taxation, equal rights, etc.
- *Future planned regulation*: Markets in Financial Instruments Directive (MiFID), Equal Treatment Directive, Market Abuse Directive, Occupational Pension Fund Directive, Pension Directive, Capital Requirements Directive, Credit for Consumers Directive, Sales Promotion Regulation, and the Unfair Commercial Practices Directive.

### **What's a poor financial institution to do? Fight back!**

Historically, compliance has been seen as an overhead or "cost of doing business." But today the costs are significant. The top 1,000 US corporations spend an average of \$5.1 million on Sarbanes-Oxley compliance alone according to Korn/Ferry. Financial institutions with exemplary compliance functions improve capital efficiency and reduce compliance costs resulting in competitive advantage; poor compliance functions consume staff, investment, and capital.

What should we make of the following quotes?:

Up to 15 percent of support staff at Dresdner Kleinwort Wasserstein are working on compliance projects or financial regulations, Stephen Ashton, director of global IT business management at the investment bank, revealed last week (*Computer Weekly*, February 1, 2005).

Regulatory controls take up a sizeable proportion of spend. Basel 2 and Sarbanes-Oxley compliance is chewing up 40 percent of investment spend (Kevin Lloyd, Barclays CTO, *Computer Weekly*, June 15, 2004).

Both quotations resonate with people in the financial services industry. The numbers, 15 percent of support staff and 40 percent of IT investment, are not questioned. While the numbers are probably unscientific, their casual acceptance in conversations indicates the depth of accord with the sentiment implied – compliance is inflating out of control. One internal approach for large organizations is to institute enterprise risk/reward management systems (see Mainelli, 2003). However, this is no longer enough; large financial organizations have to change their external environment. Financial institutions have two obvious avenues to fight back at over-regulation – managing compliance and automating compliance. Too little has been done on both fronts.

**Managing compliance**

You cannot manage what you do not measure. Few financial institutions have any idea of the actual costs of compliance. Sure, measuring compliance is not straightforward. Large banks have a variety of different compliance units and compliance structures. Compliance can report to a global head or be combined with other functions or allocated to product lines. Much compliance is intertwined with normal procedures, e.g. know-your-client requirements are wrapped up in account-opening processes. An organization that seems to spend little on ostensible compliance may be superb in compliance because of smoothly functioning systems. An organization that spends an enormous amount on compliance may be ineffectual. Historic investments in compliance systems may lead to lower compliance costs today. Under-investment can lead to large apparent expenditure that is simple inefficiency. But just because measurement is not straightforward is no reason to evade it.

Global benchmarking of comparative compliance costs could work towards measures such as:

- cost and headcount per book;
- cost and headcount per P&L;
- cost and headcount per trading function;
- cost and headcount per unit revenue and per transaction;
- cost and headcount per legal entity;
- cost and headcount per regulatory jurisdiction;
- cost and headcount per customer;
- cost and headcount allocated to regulatory initiative, e.g. Sarbanes-Oxley, Basel 2, AML, etc.;
- cost per employee;
- incidents per . . . ; and
- losses per . . .

If financial institutions had benchmarks and solid data for compliance costs, such benchmarks would help them to:

- assess current compliance costs and identify areas for improvement internally;
- establish a baseline for future work on balancing the costs of compliance with “doing the business”;
- provide frameworks for proving that voluntary certifications and ratings, e.g. quality systems or fiduciary ratings, justified a reduction in direct regulatory oversight; and
- negotiate with regulators on obligations based upon the comparative costs they impose.

**Automating compliance**

Most industries faced with spiraling costs in an area that is essentially paperwork would “try to automate the problem away.” Financial services institutions have long resisted approaches that imply they could learn a lot from “sausage factories” (see Mainelli, 2002, 2004a). However, new approaches may permit large amounts of

compliance to be automated. At heart, compliance is investigating anomalies in order to understand them or to flag them upwards in the governance structure.

Where these anomalies are contained within automated transaction systems, they can be investigated using statistical techniques embedded in Dynamic Anomaly and Pattern Response systems (see Mainelli, 2004b). Automated systems can flag anomalies or exceptions upwards to humans in the governance structure. Financial institutions of the future cannot afford to have large numbers of staff ineptly and inconsistently looking for inconsistencies in thousands of transactions. Automated systems can help to flag regulatory submissions that are "out of line," trades that are likely to require manual intervention, or transactions with unusual amounts or fees. Some institutions will succeed in automating the bulk of compliance tasks, and this automation will give them a competitive edge.

### Future proof

According to Dr Vagneur, governance is:

... the act, manner or functioning of the rules, guidance and controls which determine a course of actions through an intended or emergent system of processes.

For too long financial institutions, supposedly exemplars of probity, have relied on emergent systems of processes, i.e. reacting to past events rather than designing forward control systems. Because of a groundswell of disappointment flowing from bad financial surprises, society has applied the blunt tools of law and regulation to financial institutions to impose norms from outside. The last column (Mainelli, 2005) showed that one front in this battle might be promoting voluntary or market-based operational risk standards, such as ISO 9000 or fiduciary ratings, which provide greater flexibility than regulation. If financial institutions want to take control of their destiny, they must begin to recognize that competing on the efficiency and effectiveness of compliance will be, whether they like it or not, as exciting a battleground as the forex markets or the retail mortgage markets.

The financial institution of the future, for a host of reasons, will be one that can demonstrate corporate governance, detect anomalies in transactions in real-time, and prove to regulators that it is well run. Further, the automation of compliance reinforces the confidence of regulators in the compliance function. While customer service, product innovation, and clever ways of using capital will always be important, the boring part of the finance director's role, compliance, may be the new battleground. On balance, it is more likely that the field will be lost by "compliance" rather than won. However, for financial institutions, perhaps a main-board director needs to be dedicated to the compliance battleground full-time. In the future, success-proofing may be proving that you comply.

### References

- Centre for the Study of Financial Innovation (2005), *Banana Skins 2005: The CSFI's Annual Survey of the Risks Facing Banks*, PricewaterhouseCoopers, New York, NY.
- Mainelli, M. (1999), "Whither the FD? Hello, risk/reward director!", *Handbook of Risk Management*, Vol. 30, Kluwer Academic Press, Dordrecht, pp. 5-7.
- Mainelli, M. (2002), "Industrial strengths: operational risk and banks", *Balance Sheet*, Vol. 10 No. 3, pp. 25-34.

- Mainelli, M. (2003), "The consequences of choice", *European Business Forum*, No. 13, Community of European Management Schools and PricewaterhouseCoopers, London, pp. 23-6.
- Mainelli, M. (2004a), "Toward a prime metric: operational risk measurement and activity-based costing", *The RMA Journal*, Special issue, May, pp. 34-40.
- Mainelli, M. (2004b), "Finance looking fine, looking DAPR: the importance of dynamic anomaly and pattern response", *Balance Sheet*, Vol. 12 No. 5, pp. 56-9.
- Mainelli, M. (2005), "Standard differences: differentiation through standardization?", *Journal of Risk Finance*, Vol. 6 No. 1, pp. 71-8.
- Vagneur, K. (2005), *Corporate Governance*, Pearson Education, Harlow.

(Michael Mainelli is Director, Z/Yen Limited (Michael\_Mainelli@zyen.com). Z/Yen Limited is a risk/reward management firm helping organizations make better choices. Z/Yen undertakes strategy, finance, systems marketing and intelligence projects in a wide variety of fields (www.zyen.com), such as developing a risk/reward prediction engine, helping a global charity win a good governance award or benchmarking transaction costs across global investment banks.)