

Risk Management

Are you feeling Lucky?

David Alderson, Managing Director
Management Services 2000 Ltd



Management Services 2000 Ltd.
Middleton House, 38 Monkgate, York, YO31 7PF, U.K.

Web: www.ms2m.com

Telephone: 01904 659009
Facsimile: 01904 659006

I have not produced this paper as the result of professing to be a compliance or audit expert, but as someone who has lived through T & C since its introduction. My experience in the industry over the past 25 years, and my work with clients has provided an opportunity to see first hand how firms from across the industry have coped with successive regulators. As a result I have been able to put together my thoughts on risk management which I hope will be useful.

The only constant in Financial Services is change. It is no longer true to claim that regulation only applies to one or two areas of the business. No one is now immune to regulation and with customer acquisition costs increasing and everyone chasing the same customer, it is also true to say that every part of the business has a role in the sales effort and the responsibilities that brings.

In the past the focus of the regulator seemed to be towards Point of Sale. The face to face contact that a consumer had with an adviser was seen as the area which exposed the company to the greatest risk and this is where compliance departments applied the most effort and introduced the most control.

But Regulation never was about protecting the consumer just at the time they saw an adviser or were receiving advice. The FSA wanted to ensure that the consumer's interests were being catered for whilst they were being marketed to and after the sale was made. Improving post-sale customer protection, prompt and accurate customer care and Approved Persons in the back office have become key external influences. All this has created a minefield of opportunity for companies to fall foul of the Regulator, as the industry as a whole tries to come to terms with what this means for back office staff and indeed for senior management, where ultimately the buck stops.

With the decision to regulate mortgage advice, many organisations find themselves subject to regulation with which they are unfamiliar and ill equipped to cope. With time on their side it may be tempting to cruise their way toward N3 but experience has shown that this kind of apathetic approach has cost others dearly. When FPC became a prerequisite, the industry had plenty of notice that it would need to get all its advisers qualified. However, a mad dash for the finishing line meant hundreds didn't make it in time as examination boards were inundated with last minute requests for exam sittings. The cost to the industry in terms of loss of business production should have been foreseen but hindsight is a wonderful thing.

Now more than ever, an organisation must identify the complexities of the relationships between its different departments and the complexities of the different ways in which they have contact with their customers. With the consolidation of the industry and increased merger and acquisition activity over recent years these boundaries are even more blurred.

A helicopter view of the organisation simply doesn't provide enough detail and can be a recipe for disaster. I can guarantee that individual companies within a group and even individual departments within those companies will have different systems doing the same job. More often than not these systems provide conflicting management information some of which may be extremely damaging.

The dilemma is which data is correct and which system do you trust? One size fits all is not necessarily the answer. What is key is to make sure that there is real integration of systems and that existing processes, whether technology driven or paper based, are not allowed to become a barrier to permitting that integration to occur. Organisations need to take a holistic approach to systems and controls and ensure that there is cohesion of technology that supports the business and manages all the risks effectively.

At the very least, the person at the top of the tree must have confidence in the quality of the management information being provided about risk exposure across all areas of the business. Gone are the days of passing the buck, denying all knowledge and sending for the whipping boy. This simply won't wash with the Regulator.

Organisational structures have to be expertly documented and rigidly adhered to in order not to unwittingly expose the organisation, a department or an individual under the new regime.

Compliance should not be an edict, it must be a mindset and a culture which permeates through an organisation. For this to be the case it needs to be demonstrated and communicated regularly. A compliance culture can only exist where it is clearly understood by everyone in the organisation and is reinforced on an ongoing basis. It's not enough for the people at the top to have a vision of what compliance should be and then not be able to articulate it in a way which leaves everyone in no doubt about what's expected of them.

I have come across organisations who worked really hard to get everything in place for N2 but who simply haven't been able to embed that hard work for the long term. What I suspect we may see in the coming months is companies given a clean bill of health as part of the initial risk assessments by the FSA but who find themselves, for whatever reason, slipping back to the good old ways. The consequences are obvious.

N2 was not a destination – it was the start of a journey. The post N2 world is one in which the FSA has openly stated that its supervisory approach to firms will reflect the extent to which they contribute to the achievement of their statutory objectives. The FSA Handbook is clearly intended to move firms in this desired direction. The challenge for firms, and particularly for senior management, is to clearly demonstrate the alignment of firm-wide risk management processes, systems and controls with individual responsibilities. This is at the core of the Approved Persons Regime. In attempting to meet this challenge in an effective and efficient way, there are opportunities for Senior Managers, Compliance Officers and Internal Auditors to create a dynamic culture of compliance, supporting Approved Persons through robust and effective systems and controls.

The problem may be that management of risk has become an industry in itself, but management is a word used often by many, but rarely understood.

The dictionary definition for 'Management' says – administration, care, charge, conduct, control, guidance, negotiation, operation, oversight, superintendence, supervision. I've never seen mentioned the more usual practice of "seat of pants flying".

As an industry that has always struggled to explain risk to our clients, if we add trouser seat management are we really in danger of disappearing up our own oxymoron? It's clear that elimination or minimisation of risk is in itself a tricky business. We have to ensure the risk is documented. Not just at the time it is identified but on an ongoing basis. The remedial actions must be identified and then followed through. All this must be recorded to provide an audit trail. "If it ain't documented it didn't happen". Identified risks, even when they have been rectified should be revisited to ensure there has been no relapse. There must also be regular reporting of control breaches – those near misses.

Each risk identified must be handled responsibly. Responsibility for risk should not be assumed but allocated. It needs to be very clear who in your organisation should be dealing with any particular risk, what their responsibilities are and whom progress should be reported to.

Assessing the size and impact of the risk on the fundamental well being of the organisation should be common practice. A probability/impact analysis often helps to focus the mind on the true nature of the exposure because it forces you to question the appropriateness and the effectiveness of all the other areas of your business and their processes. I have often seen senior management undertaking this exercise for one risk, only to spot several others of equal seriousness.

Adequate reporting of risk is vital to the survival of the business. Key exposures should be reported daily, operational risks monthly, and strategic risks quarterly. Remember however, that its quality not quantity that counts. Deciding on the type of reports you produce is largely a matter of choice so long as they are accurate and comprehensive.

The conduct of everyone in the organisation potentially exposes it to risk. Having identified a risk and having delegated responsibility for eliminating or minimising it, do you have the confidence that the person will do all that is necessary? Compliance is about attitude and behaviour as much as anything else.

The new regime of risk based regulation with all the new rules and guidance, ushers in a sea change in terms of attitude for everyone from the top down. It fundamentally questions historical management styles, the behavioural skills of senior managers and record keeping practices and procedures. For risk management to work it must be intrinsically linked to business strategy and objectives. In essence business risk management needs to become part of the day to day business behaviours and practices.

There should be a high awareness of the benefits that are reinforced and driven from the top. Ongoing practices down the line must support good risk management and control – not just periodic process. Escalation of risks and issues should become part of normal reporting and monitoring flows. You only need one disaster to see how inadequate your disaster recovery plans are. Include your disaster recovery plan as part of your risk assessment – the FSA define this as unforeseen interruption. Test your plan often and thoroughly.

The FSA needs to obtain assurances that a firm's regulated business is being managed and controlled from the very highest level. Senior managers must ensure that they have the ability to evidence to the FSA how their business is controlled up to and down from Board level.

A compliance culture will, eventually, reduce the costs of compliance but to demonstrate and evidence this there needs to be a new generation of Key Performance Indicators and Management Information. All this will require real integration of systems. With the FSA working towards encouraging real time streaming of information directly to them, if you haven't got integration and accuracy it will show.

Whatever systems you put in place for risk management, make sure they add value to the business quality and do not just satisfy Regulator requirements.

Of course all this is fine if you are one of the few firms left who hasn't outsourced its back office functions. Embedding a compliance culture in your own firm is one thing but ensuring that same degree of compliance exists within a third party organisation is a very different proposition. For any firm considering outsourcing the back office there are some critical considerations to make.

Sir Howard Davies has been clear about this when he said ' It is absolutely vital that outsourcing does not

involve loss of control over the quality and performance of the function'.

So where do you start and how do you make sure your interests are being protected by the third party? The first thing is the business case for outsourcing. This business case should justify the outsourcing proposal by proving an overall benefit based on both quantitative and qualitative terms. Your business case will define the scale of change that the outsourcing will initiate and provide a baseline against which the implementation of the proposal can be measured. Ultimately your business case should provide a basis for an outsourcing champion or sponsor to win support from all the key stakeholders.

The selection process is possibly the most difficult. First you need to establish a selection criteria and research the market. Who are your competitors using and are they happy? Establishing a selection timetable and developing a tendering process which eventually creates a shortlist all takes a great deal of time. Eventually you will get around to the beauty parade and then the final decision. Having found your provider the next step is compliance due diligence. This is where you apply your own standards of compliance and risk management to that of the third party. If they can't satisfy your standards then leave them alone. Interrogate them about their risk management policy, management controls, audit and compliance arrangements, their compliance history and importantly their systems reliability.

The mistake many firms make is that they tend to deal with only one point of contact at the third party supplier. Have regular contact and meetings with the third party's own compliance team and this will quickly surface issues and concerns. This might seem time consuming but unless you are willing to put your firm in the hands of lady luck I would suggest you make the time. The FSA make it perfectly clear that a firm cannot contract out of its regulatory obligations. At the very least you are obliged by the FSA to have contingency arrangements in place should they be needed.

Based on all the above my answer to risk management is simple but it is not easy. Systems integration is the only real way to cover all the bases. Of course I would say that and it's not a new idea. I've lost count of the number of times an IT Director has told me that's what they are attempting to do, only to go on to learn about a myriad of "special circumstances".

So why don't we have an industry where this utopia exists? Why do projects for systems consolidation and integration fail? In my opinion there are two main reasons why they fail – cost and risk. Systems don't come cheap nor does IT expertise. Most firms have multiple platforms, and the number of legacy systems running today's financial services industry has never been higher. Within this there is a real underestimation of the complexity of integration.

As with risk management the answer to successful integration of IT is simple but the process isn't easy. Careful up front analysis of what already exists, identification of the gaps between systems, data quality issues and resources all need thorough consideration before you develop a strategy and a plan. In the drive for consolidation and integration some of your systems will have to go and some will have to be replaced with more suitable systems which will allow for continued flexibility to take account of ever changing legislation and product development.

As I said the second reason is risk. It's too easy to say our existing systems are established and reliable, that the pioneers of new technologies get scalped and the settlers get all the land. But is the greater risk associated with not doing anything? Could it be that the very nature of their legacy makes them old and vulnerable? Believe me, there are new and increasingly sophisticated systems that can support fresh

initiatives.

The long terms benefits of consolidation far outweigh the short-term costs. In an environment that is becoming increasingly competitive, legacy systems often prevent the company from supporting high levels of customer service and can impede any move towards greater efficiency and business growth. The high expense of too many systems is not good for shareholder or member value, and ultimately will weaken the company. Let's not forget that standing still is going backwards.

The performance of firms and their senior management has probably never been under more scrutiny than it is today from Regulators, investors, the media and the general public. Risk based assessment, the provision of explicit statements concerning corporate governance and prudential standards, has made dynamic performance measurement and monitoring a pre-requisite for the demonstration of effective corporate management. Is your firm up to the task? If you need to toss a coin in the air at this point then you lose.

Regulation is here to stay, with all that it entails. It is not a game of chance and it won't go away but you can make sure the odds are in your favour.