

White Paper

Integrated Compliance Management:

‘Turning an obligation and an expense into an opportunity and a value’

Chris Kind, Project Risk Leader, idRisk Ltd.



ChrisKind@idrisk.com

4 October 2004

“How can my company do compliance more effectively at less cost to gain a competitive advantage?”

Integrated Compliance Management

CONTENTS	PAGE
Introduction	1-2
Section 1: Background and Drivers	3-7
Section 2: Implications and Response Options	8-12
Section 3: Integrated Compliance Management – A Practical Way Forward	13-25
Conclusions	26-27
References	28-30

All Rights Reserved

No part of this paper may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher, idRisk Limited.

INTRODUCTION

Scope

This paper considers compliance against the background of increasing rafts of laws, regulations and associated guidance on how businesses should govern themselves and manage their risks. These are being called “*good governance regulations*”. Within this broad scope, the focus is on regulations affecting UK businesses and financial institutions in particular.

The main regulations considered include:

- The Combined Code on Corporate Governance, affecting all London Stock Exchange listed companies;
- The Financial Services Authority’s Handbook of rules and guidance, for financial institutions operating in the UK, including the implementation of Basel II, the Capital Adequacy Directive and various other EEA directives;
- The United States’ Sarbanes-Oxley Act.

All of these regulations come with direct and indirect penalties for businesses and how they affect the fundamental practices and behaviours of business organisations.

The scope of the paper does not extend to compliance with other more specific laws affecting UK businesses, such as the EU Working Time Directive¹, health and safety, environmental compliance. However, it is recommended that these other aspects of compliance should also be managed within an integrated approach.

Objectives

This paper has three objectives:

1. To review the overall drivers behind the current wave of corporate governance based compliance regulations;
2. To consider some of the key implications and options facing businesses;
3. To propose a practical way forward for businesses i.e. Integrated Compliance Management (ICM) within an Enterprise Risk Management framework (ERM).

The paper presupposes that:

- Good businesses plan and organise themselves so that they are able to continue to meet their goals in changing economic, social and regulatory environments.
- Good governance compliance can be achieved as a consequence of operating both profitably and ethically, and by using the profits in a manner that benefits all stakeholders in the business fairly.

¹ although this has been estimated to be the single biggest compliance cost for UK businesses (The Sunday Times, Business Focus, March 7th 2004)

Enterprise Risk Management

Compliance risk sits and should be managed within the Enterprise Risk Management framework² since it is just one of an organisation's operational risks which are, in turn, just one area of an organisation's overall business or enterprise risks.

Organisations that approach compliance within an overall enterprise risk management structure will be able to cost-effectively demonstrate ongoing compliance and, at the same time, improve overall risk management and business performance. Using ICM, an organisation will seek to minimise its risks whilst maximising the return on investment derived from becoming compliant. Furthermore, the drivers and problems affecting good governance compliance are most effectively addressed by approaching the issue proactively, not reactively.

The key proposition for businesses is that they should ensure that their compliance management is fully integrated into the fabric of the business planning, operations and governance framework, and not treated as a separate 'bolt-on' reporting exercise.

Integrated Compliance Management (ICM)

Integrated Compliance Management is a framework and approach that enables compliance to be incorporated fully and effectively with the business planning, operational management and risk management activities of an enterprise.

As a broad statement, in order to achieve compliance, Chief Executive Officers need to demonstrate that:

- Their organisations are competent;
- They are identifying and managing the risks as they arise;
- They have control of the business;
- Controls, processes and early warning systems are in place.

The ICM approach advocated in this paper incorporates gap analysis, record keeping, supervisory and reporting activities with a development plan and several powerful technologies, so that compliance practices will fully satisfy management and regulatory expectations in the near and longer term.

This approach will provide organisations with a rapid, flexible response to future business and regulatory changes, as well as incorporating a Compliance Maturity Profiling (CMP) tool for measuring and reporting continual improvement against good governance standards.

ICM is designed to use the latest thinking, practices and technologies to help organisations better deliver or upgrade their existing compliance activities, thereby generating positive value from what is otherwise viewed as a cost.

² Enterprise Risk Management is described in the References section of this paper. It is now also sometimes being called Enterprise Performance Management by some commentators.

SECTION 1: BACKGROUND AND DRIVERS

New regulations are increasing the level of compliance required

Compliance is becoming a matter of law rather than voluntary management. Compliance with increasingly intrusive government regulations is one of the key risks of modern businesses and one that is testing many to their limits. The following are just some of the recent and imminent corporate governance regulations with which businesses have to contend.

Table 1 – “Good Governance” Regulations

REGULATION	SOURCE	START DATE	AFFECTS
The New Combined Code ³	UK	1 November 2003	All UK LSE listed plcs
Mortgage Conduct of Business (MCOB)	UK	31 October 2004	Mortgage sector
Operating and Financial Reviews ⁴	UK	1 January 2005	All UK LSE listed plcs
International Accounting and Financial Reporting Standards	EU	1 January 2005 ⁵	All companies
Insurance Conduct of Business (ICOB) ⁶	UK	14 January 2005	Insurance sector
Integrated Regulatory Reporting ⁷	UK	1 April 2005	All regulated companies
Sarbanes-Oxley ⁸	USA	15 April 2005 ⁹	All US companies
Reporting and Audit Requirements ¹⁰	EU	1 July 2005	Insurance and Mortgage sectors
“Euro-Sarbox” ¹¹	EU	est. mid 2005	All companies
Basel II	BIS ¹²	31 December 2006 ¹³	Financial sector
3 rd Capital Adequacy Directive (CAD III)	EU	31 December 2006	Financial sector
Solvency II	EU	est. 2008	Insurance sector

³ http://www.fsa.gov.uk/pubs/ukla/lr_comcode2003.pdf

⁴ <http://www.dti.gov.uk/cld/financialreview.htm>

⁵ With the possible exception of IAS 32 and IAS 39 which are still in discussion.

⁶ Policy Statement PS04/1: Insurance selling and administration & other miscellaneous amendments. 341 pages www.fsa.gov.uk/pubs/policy/04_01

⁷ http://www.fsa.gov.uk/pubs/policy/04_08/index.html

⁸ Management assessment of internal controls (including external audit) <http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf>

⁹ This date applies to non-US parent companies with US subsidiaries. 15 April 2005 is the date for US Parent companies.

¹⁰ FSA PS04/9 http://www.fsa.gov.uk/pubs/policy/ps04_09.pdf

¹¹ “Euro Sarbox” is intended to be implemented via amendments to the EU Accounting Directives, i.e. the 4th Company Law Directive of 25 July 1978 on the annual accounts of certain types of companies (78/660/EEC) – as amended by Directive 2003/51/EC of 18 June 2003 and the 7th Company Law Directive of 13 June 1983 on consolidated accounts (83/349/EEC) as amended by Directive 2003/51/EC of 18 June 2003 (see http://europa.eu.int/comm/internal_market/company/board/index_en.htm) and the 8th Company Law Directive on Statutory Audit (see http://europa.eu.int/comm/internal_market/auditing/officialdocs_en.htm). See also Gartner FirstTake 17 March 2004, Debra Logan.

¹² Bank of International Settlements

¹³ The Advanced Measurement Approaches for Operational Risk and the Advanced Internal Ratings Basis approach for Credit Risk will not come in until the end of 2007. See Consensus achieved on Basel II proposals 11 May 2004. <http://www.bis.org/press/p040511.htm>

In essence, if businesses are not acting ethically (compliantly) towards their business partners, their behaviour will be regulated. Increasingly, as business ethics are perceived to diminish, more regulations are introduced.

Business failures are another cause of the regulatory momentum

Over the last decade or more there has been a series of well-publicised major events that have damaged customers and shareholders. In many cases, the injured parties thought that the companies were reputable and were being regulated. Consequently, pressure was put on governments to respond. Tightening of laws and new regulations are the results.

Table 2 – Examples of General Corporate Governance Failures

ISSUE	CORPORATE GOVERNANCE FAILURES
Frauds	Barlow-Clowes, Polly Peck, Enron, WorldCom, Parmalat
Strategy failures	Long Term Capital Management, Equitable Life
Governance & control failures	Barings, Shell, National Australia Bank, Ahold, Lloyds' of London, Independent
Consumer protection failures	Pensions mis-selling, Endowment mis-selling
Innovative products failures	Split Capital Investment Trusts, Precipice Bonds

In effect, the majority of organisations are finding themselves being regulated in respect of good governance because a minority of people, who are running businesses, are either not regulating their own behaviour or not controlling sufficiently well the behaviour of their employees to generally accepted standards. These businesses may even be in a completely different sector.

Good governance in practice too often has not matched the theory

In too many cases, what is actually going on within the operations of a business does not match the theory, framework and management structure that the top of the organisation either think is happening or say is happening. Evidence of this managerial detachment and dilution of training, competence and supervision is reported in the world press almost daily.

The evidence is also there in the form of massive Errors and Omissions (E&O) and Directors and Officers' liability (D&O) insurance claims. The self-insured claims costs for some financial services organisations are now so large that they eat up a majority of the profits that they have worked so hard to increase by cutting costs. Ironically where cost cutting has been achieved by replacing experienced staff with cheaper inexperienced people the problem has been exacerbated.

The FSA has a key regulatory role

In the UK, the Financial Services and Markets Act 2000 (FSMA) reorganised good governance related regulation under the auspices of the Financial Services Authority (FSA). The FSA has since then been in the process of taking over and implementing its responsibilities by developing its organisation and regulatory approach. This includes creating a raft of regulations and guidance for organisations to read, digest and act upon.

The FSA is an independent regulator with statutory powers that make it responsible for establishing rules for businesses, as well as authorising, monitoring and if necessary disciplining businesses wishing to carry out certain “regulated activities”¹⁴, particularly within the financial sector.

The FSA is not primarily concerned with risks which threaten only the owners of financial businesses, except in so far as these risks may have an impact on its Statutory Objectives.¹⁵

The FSA takes a leading role in protecting organisations’ customers, shareholders and other stakeholders. It supervises all companies listed on the London Stock Exchange and has particular duties in respect of financial institutions, amongst several other special duties, including the regulation of the Lloyd’s insurance market.

The FSA has four objectives, five points of interaction with regulated firms and six regulatory fundamentals on which it bases its activity. These are therefore key points of reference against which businesses need to form their compliance strategies and practices.

The FSA's four statutory objectives

The Financial Services and Markets Act 2000 (FSMA) requires the FSA to pursue four objectives¹⁶. These are to:

1. Maintain confidence in the UK financial system;
2. Promote public understanding of the financial system;
3. Secure the right degree of protection for consumers;
4. Help to reduce financial crime, focusing on money laundering, fraud and dishonesty and criminal market misconduct.

The FSA's five main points of interaction with regulated firms

1. *Determining satisfaction of the threshold conditions*, which include legal status, supervision and resources;
2. *Baseline monitoring* to ensure that firms comply with the regulatory requirements on a continuing basis;
3. *Sector reviews and thematic work* to assess the risks posed by a particular issue;
4. *Programmes designed to mitigate specific risks in individual firms*;
5. *Work undertaken after particular risks have escalated or crystallised*.

The FSA's six regulatory fundamentals

The FSA follows a risk-based regulatory approach, which concentrates most attention on those organisations that present the greatest risk to the FSA’s four statutory objectives. In working towards its statutory objectives, the FSA bears in mind six fundamentals:

1. The need to use resources in the most economic and efficient way;
2. The responsibilities of the management in regulated firms;
3. The need to balance the burdens and restrictions on firms with the benefits of regulation for consumers and the industry;
4. The need to allow innovation;

¹⁴ The Financial Services and Markets Act 2000 (Regulated Activities) (Amendment) (No. 1) Order 2003 lists a number of activities which fall under FSMA and include “Contracts of insurance” and “Participation in Lloyd’s syndicates”.

¹⁵ SYSC 1.2

¹⁶ Sections 2 (2) and 3 to 6 of the FSMA.

5. The international character of financial services and markets and the UK's competitive position;
6. The value of competition between financial firms.

Some businesses maintain that regulators are over-reacting¹⁷

Over-regulation in the UK in the Financial Industry is widely recognised as being a significant commercial and economic danger to UK businesses and therefore the UK economy as a whole.

It might perhaps be conceded that “a relatively few bad apples have contaminated the barrel” and there is a danger that UK businesses may now be finding themselves in a situation where they are too tightly regulated in comparison with their foreign competitors. It is a situation that organisations are in the process of working through with their regulators.

Certainly in respect of Financial Institutions, the Financial Services Authority has put considerable effort into consulting with businesses in order to learn their perspectives and problems and it is trying not to be over prescriptive or burdensome compared to other competing countries.

The compliance function is still finding its level in organisations

The profile of compliance in many firms has increased enormously as a result of the increased regulation. Compliance Officers have a challenging and, some may say, unenviable job. As yet there is no such thing as a typical Compliance Officer in terms of expertise, position, responsibilities, authorities, rewards and budget.

An organisation's attitude, investment and approach to its compliance function can be a revealing prima face indication of its overall business attitude and the quality of its general management. In some organisations the Compliance Officer is held in high regard, given a high level and profile in the organisation and given authority to match. In others it can be completely the opposite.

Effective management depends on staff complying with the company's policies, procedures and standards. Therefore the compliance function in an enterprise must be integrated with both executive and line management. Ideally, Compliance needs to have weight in the business planning and decision making process.

Compliance has a range of issues and challenges

Qualitative research on the opinions of financial institutions' Compliance Officers offer insight into how compliance issues are viewed from within UK business today.¹⁸

“Financial institutions are horrendously sales led. Compliance is at the bottom of the list.”

“One of the biggest cost challenges is how do you sell anything and still stay compliant?”

“Compliance should be part of strategy.”

“Compliance should sit right at, or just below Board level – but it doesn't.”

“There is a lot of taking eyes off the business front end to look internally.”

“Corporate governance/compliance is about structure and understanding how structure works.”

¹⁷ This was a sentiment expressed by several Compliance Officers at breakfast seminars hosted by idRisk, Applix, and Nimbus Partners.

¹⁸ Research Findings Active Compliance Briefings; April & May 2004, IdRisk Ltd, Nimbus Partners, Applix.

“Process mapping makes sense to get an immediate understanding of what is going on.”

“Smaller firms just cannot afford the compliance team and they are concerned about their ability to stay in business.”

“Compliance is seen as a business blocker but needs to be seen as a business enabling unit”

“How can my company do compliance more effectively at less cost to gain a competitive advantage?”

Compliance is the responsibility of everyone in an organisation

The focus of general risk management by many businesses is still largely on functional activities and organisational structure, rather than on personal ethics and competencies. It tends to focus on the staff rather than on the directors and the top executives, even though it is at a high and personal level that the tone is set for the rest of the organisation and where the most costly damage can be caused to customers and investors. Regulatory requirement is one of the key catalysts in getting leaders to turn their scrutiny on themselves. One of the fundamental bases for the regulation by the FSA is at the individual level. The FSA sets out principles by which it expects businesses and individuals to conduct themselves, and it takes the approach that companies must be run by “fit and proper persons” or “approved persons”. Regulations now go beyond the directors of an organisation to the senior management and then to all officers with customer or other stakeholder responsibility and onto staff for, for instance, money laundering.

The costs of non-compliance outweigh the costs of compliance

Non-compliance incurs a wide range of “official” penalties up to and including fines, increased regulatory capital and solvency requirements, imprisonment of senior officers of the companies and withdrawal of licences to trade. However, by far the highest costs for businesses resulting from major compliance failures are from damage to businesses’ reputations – the “knock-on” business impact.

The commercial, as opposed to regulatory, costs of compliance failures are manifested in many ways, starting with increased complaints and reduced operating efficiencies, escalating to legal and compensation payments, reduced sales, reduced credit ratings and ultimately reduced stock prices. In the worst cases, the cost is complete failure of the business, as was the case for Barings Bank.

On the other hand, the costs of obtaining regulatory compliance are one of business’ biggest criticisms. Feedback from US businesses on their costs of implementing Sarbanes-Oxley indicate increases of 25% in audit fees in 2003 following an average rise of nearly a third the year before. In addition, firms are experiencing significant increases in non-executive director fees and directors and officers’ liability insurance.¹⁹

Regulators are aware of the operating costs of compliance, the increase in pressures and the consequent negative international competitiveness potential, and are trying to weigh the balance with avoiding further damaging corporate governance failures.

Using compliance as a trigger to more effective management behaviours and practices is the way to change a cost into a value.

¹⁹ Survey by Foley & Lardner, a US law firm, as reported in Financial News 24-30 May 2004.

SECTION 2: IMPLICATIONS AND RESPONSE OPTIONS

Compliance implications are broadly the same for all firms

The implications of the increasing regulatory regimes and the response options available are broadly the same for all organisations, assuming that their first goal is to respond in the most effective (least disruptive) way to achieve good governance compliance.

Some of the most challenging implications of compliance that are facing businesses at the moment are:

- *Organisations will face increasingly tougher solvency, governance and stress testing requirements* to which they must work and on which they must report;
- *Regulators are setting tougher customer service and delivery expectations*, including the need to monitor the supply chain;
- *Existing information and reporting systems in many organisations are inadequate* to enable managers to know factually and with evidence, which parts of the operations are currently “good” and which are “bad”;
- *Historic documentation of activity and subsequent record keeping practices may be inadequate* to meet the new regulatory expectations;²⁰
- *Developing and keeping records is presenting considerable organisational and logistical challenges* so that records are up to date and contain *relevant* data to ensure that businesses are compliant at all times;
- *New investment may be needed to deliver training and competence standards* to the regulatory and business standards expected;
- *Care needs to be taken to avoid creating a whole new parallel function and expense in Compliance*, but rather Compliance needs to catalyse a consistent and high service quality that is embedded within the normal operating processes and systems of the organisation;
- *Whatever is done immediately, its legacy needs to be usable over the medium to long term*;

The Integrated Compliance Management approach and its technology basis are designed to respond to all of these issues in a logical and effective way.

Compliance responses need to be planned in the right context

Some of the most important considerations facing organisations as they respond to the new regulations include:

- *The scale of the change needs to be appreciated fully*, including the risks and potential financial implications, positively and negatively;
- *You need to know where you are now, where you want/need to be and what is needed to close the gaps*;
- *A cross-functional response is necessary*. This is something that will need to be repeatable, changeable and improvable every year going forward;
- *Do the job thoroughly, even if it means changing your business processing model*. Quick fixes without taking some time to develop a strategic good governance plan will not be risk

²⁰ Such as how long and how well records are kept

management or cost effective in the long run because gaps will occur and wrong responses will be started on, necessitating new starts (and additional costs);

- *Decisions on compliance responses must be what each organisation considers to be appropriate for its particular circumstances* – and the Board and Executive have to be prepared to explain and justify their decisions and actions (or inactions);
- *Key stakeholders to be involved* to input views as well as to carry out decisions, and keep the rest of the organisation informed of the changes, the organisation's response plan and what is expected of each job function and individual;
- *New tools may be needed to link appropriate policies, standards, competencies and procedures* from the top to the bottom and across the business;
- *New tools may be needed to report promptly reliable and relevant information* from the bottom and the corners to the top, and vice versa;
- *A cost-effective way may need to be found to link the myriads of information sources* into a consolidated, timely and informative picture.

Recent developments make integrated compliance possible

In formulating practical forward-looking responses to the new compliance-driven challenges, organisations are fortunate that there are two particularly exciting developments enabling organisations to turn compliance needs and costs into an opportunity and a value.

1. Organisational silos are being broken down

Techniques and points of view from a variety of different groups and thought leaders are starting to come together. Leaders in Risk Management are sharing ideas and understanding those working in Information Systems. The same applies with Audit, Compliance, The Board, Finance, Sales, Actuarial, Human Resources etc.

Gradually each business function is realising and accepting that achieving (and, more significantly, maintaining) effective good governance compliance is too big and complex for each technical group or organisational silo to solve, and that working with colleagues in other areas help.^{21 22 23 24}

Acceptance, understanding and belief in this development by the leaders and key managers in an organisation are the key first steps to enable it to move ahead positively.²⁵

²¹ AMR Research Report Thursday February 26th, 2004. Planning for a Sustainable Compliance Architecture

²² “To date, financial services institutions have taken a short-term view of compliance, building point solutions to cover each new piece of legislation. To remain competitive, an integrated approach is essential. An integrated, enterprise-wide framework is a vital step in catering for common compliance needs.” Sian Jones, managing analyst, Datamonitor quoted in Insurance Times

²³ McKinsey Quarterly 2003 Number 3, What CEOs Really Think About Information Technology, Eric Monnoyer

²⁴ Enterprise Governance, Getting the Balance Right, February 2004, the Chartered Institute of Management Accountants (CIMA) and the International Federation of Accountants (IFAC)
http://www.cimaglobal.com/downloads/enterprise_governance.pdf

²⁵ PricewaterhouseCoopers 7th Annual Global CEO Survey – Managing Risk, an Assessment of CEO Preparedness
[http://www.pwc.com/Extweb/insights.nsf/docid/5E17EFE50B9800AB80256E1A004ACB4D/\\$file/CEOSurvey_04.pdf](http://www.pwc.com/Extweb/insights.nsf/docid/5E17EFE50B9800AB80256E1A004ACB4D/$file/CEOSurvey_04.pdf)

2. **Computing capabilities have advanced considerably**

Effective computer systems are essential to enable the ongoing cost effective delivery of an acceptable level of risk management, risk based capital calculation and allocation, and supervision and control in any but the most basic organisations.

The web-based and interactive capabilities of the various technologies and software systems that organisations have accumulated over the years and are currently being developed, are becoming able to link together to provide practical, powerful, quick and cost effective communication platforms, data storage and analytical capabilities.^{26 27 28}

This advance means that legacy systems can be used in a new network of information systems and the cost of delivering improved management information, monitoring and control processes is reducing.

These two current developments enable any organisation to develop an integrated compliance approach that can seamlessly fit within an overall Enterprise Risk Management approach.

Organisations have three compliance response options

There are three options open to organisations trying to respond to the wave of good governance compliance regulations:

Option A: Do nothing – wait and see.

Option B: React defensively by filling in the forms and doing just enough (hopefully) to pass the latest regulatory hurdle so that the organisation can then get back to business as it always has done. The compliance people can then be focused on getting through the next regulatory hoop .

Option C: Use the regulatory compliance deadlines and reporting requirements positively as an opportunity to collect, document and consolidate enough information about how well the organisation is managing itself to be able to demonstrate this to regulators and any other stakeholders. Also use this information to plan and execute a positive Integrated Compliance Management framework.

Option A. Do nothing – wait and see

Unfortunately, this is not really an option as it is becoming *illegal* to transact regulated business without having the necessary regulatory approvals or exemptions – complying.

In addition, delaying action means that:

- The back-log of preparatory work increases, and it will still have to be done;
- The time left to do the work before the regulatory deadline reduces;
- Responses become more of a panic and less well thought through;
- The number of budget cycles over which to spread the investment reduces; The organisation still needs the same level (or more) of investment and so the investment pressure on each budget cycle increases;

²⁶ McKinsey Quarterly 2003 Number 3, Designing IT for Business

²⁷ McKinsey Quarterly 2004 Number 2, A New Era in Corporate Governance – Information Technology’s Role in Governance, Ken Berryman and Tom Stephenson

²⁸ Celent Communications report - Responding to a Dynamic Regulatory Environment: IT Evolves to Support European Regulatory Reporting, as reported in Operational Risk magazine, May 2004.

- The organisation will not be able to respond to enquiries by the FSA as to how it is and can achieve compliance.

Option B. React defensively, achieve minimum compliance

The objectives of minimum compliance are to:

- Hang onto the operating licence, since non-compliance can lead to being put out of business by the regulator;
- Avoid the regulator's fines, which can be substantial;
- Keep the directors out of jail; there are senior executives currently in jail in the USA for corporate offences involving non-compliance and poor governance;
- Avoid bad publicity which leads to damaged reputation and ultimately loss of business.

This may seem to be the obvious choice for most organisations, especially those that are smaller, very lean, embattled or over-stretched. For many organisations it may be the *only* short-term option that the organisation has the capacity (or capability) to select.

An organisation may pass the regulatory tests in the first year for a variety of reasons, such as:

- A sympathetic regulator not applying the full force of the new regulations in the first year in order to help regulated organisations with the change;²⁹
- A convincing submission, a “good bluff” or a just-convincing-enough story;
- A regulator may not have sufficient resources itself to probe into the reported information and claims;

However, reacting defensively is also not really an option beyond the very short term, even for those organisations under resource pressures. A defensive, reactive approach will not enable an organisation to continue to comply in the medium term, let alone the long term, because regulators tend to increase their attention on their regulated organisations (especially those that seem to be trying to only do the minimum), even if some broad concessions are made in the first year to help well intentioned organisations transition into a new or more intensive regime.

Being continually on the back foot and fighting fires is inefficient, uneconomical and stressful. It ultimately makes the organisation more risky and therefore a worse regulatory and investment proposition.

What is more, a short-term response without sufficient consideration of the medium to long term objectives of the business and without taking an integrated, enterprise-wide approach is likely to be the most cost inefficient. This is the classical mode of starting on an apparent “quick win” only to find that the resulting system cannot fulfil all requirements once these are better understood and cannot easily be modified or extended to accommodate changes.

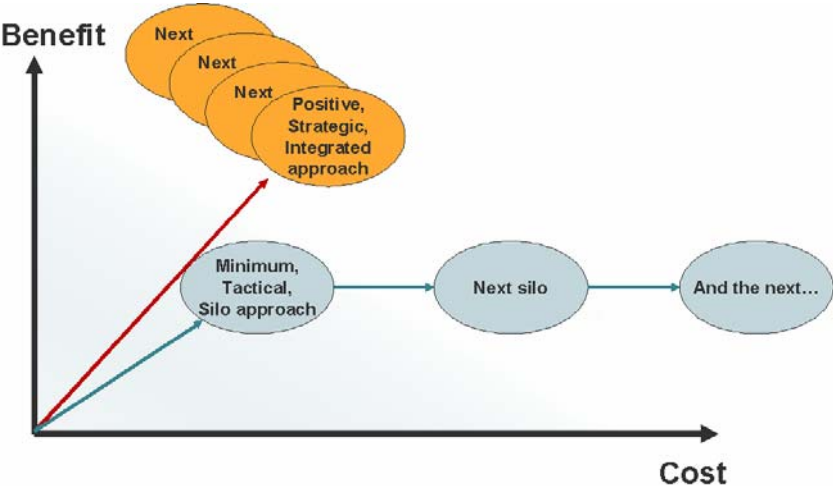
Fire prevention, rather than fire fighting, is a lot less expensive in the long term. Therefore, sooner or later, all regulated organisations will have to move to a positive, proactive approach to compliance.

²⁹ This was the case with the introduction of the Combined Code in September 1999

Option C. React positively, achieve effective compliance

A positive approach to compliance for organisations to take is the approach of Integrated Compliance Management (ICM). The framework, approach and benefits are described in Part 3 of this White Paper.

Figure 1 – The Benefits of Integrated Compliance versus a Minimum Response



SECTION 3: INTEGRATED COMPLIANCE MANAGEMENT – A PRACTICAL WAY FORWARD

Key Features

Integrated Compliance Management is about helping organisations, and Compliance Officers in particular, achieve short, medium and long-term success. Integrated Compliance Management is a framework and development approach devised by idRisk consultants that combines risk management and compliance policies and processes with supporting computer systems in order to create a sustainable, cost-effective compliance infrastructure that will fully integrate with the business operations, risk management and internal audit. The development approach is a step-by-step process for achieving ongoing effective regulatory compliance that helps move an organisation through a logical progression, largely at its own speed.

Through ICM what starts as a compliance activity will create organisational value and will fully contribute to all the other business and risk management activities of the organisation. This enables both the compliance function and the enterprise as a whole to avoid gaps, duplications and, even more destructive, contradictions of responsibilities and activities across the organisation.

ICM enables organisations to move their risk management approaches away from defensive fire-fighting approaches onto positive, fire-preventative, progressive, joined-up approaches.

The ICM approach avoids reinventing the wheel each year, while making progressive steps forward, combining efforts across the organisation, driving out costs and creating value by minimising the errors and incidents that translate into expenses and damage to customer relations and reputation.

The approach and framework have the added benefit of enabling an organisation to achieve comprehensive Enterprise Risk Management to a level and in a way that suits each individual organisation.

ICM is about effective planning and commitment, as much as it is about effective execution. Experience in a wide variety of risk management and change management projects has consistently taught the wisdom of detailed business planning. This means:

- Considering the wider and longer term implications of the immediate issues and actions within the context of the organisation's business goals and the requirements that need to happen (and not happen) in order to achieve those goals;
- Fully and unequivocally engaging all the Board and Senior Executives' active support, understanding, agreement and commitment to compliance's immediate and longer term goals, its roles, responsibilities and authorities;
- Developing a clear knowledge of the business' existing organisation, policies, processes, systems and people before embarking on a fix-it campaign.

Key Benefits

The approach provides an organisational, process and systems platform for cost effective continuous improvement in compliance and linkage with Enterprise Risk (Performance) Management and Business Intelligence Systems. The benefits of ICM are extensive for all organisations and are easiest to achieve for smaller, less complex enterprises. Key benefits include:

- Delivering effective risk and cost management;
 - Operational and compliance cost minimisation by building on existing platforms and practices, sharing information and avoid duplications;
 - Reduced economic (and potentially regulatory) capital requirements through reducing operational risks;

- Providing a way for easier compliance with future regulations;

- Managing compliance proactively, whilst improving business processes and performance;
 - Improved efficiency of business processes by clearer and wider identification of processes and linkage horizontally and vertically;

- Generating a holistic view of compliance, integrated across all business processes (both financial and operational) and with a supporting IT infrastructure;
 - Better corporate governance through improved practices, risk information and reporting to operations and decision makers;
 - Quick and powerful risk adjusted profitability calculations and pricing using OLAP³⁰ technology;

- Grasping an opportunity to improve by streamlining the way organisations operate, whilst also being compliant;
 - Reduced operational losses through improved knowledge of risk points in operational processes and better, quicker management information;

- Providing a return on investment by gaining maximum benefit from the investments in compliance infrastructure and technologies that organisations need to make;
 - More accurate forecasting for business plans by fully considering the risk management and compliance implications in the planning and decision-making process.

³⁰ OLAP is On Line Analytical Processing. Applix's TMI is a leading example.

A 3-Dimensional Framework

Integrated Compliance Management follows the idRisk Integrated Compliance Management Framework. This framework has been carefully constructed to be compatible with specific compliance requirements and integrate them with a wider Enterprise Risk Management approach.³¹

The framework's three dimensions are:

- THE RISKS DIMENSION covering the range of risks to be managed;
- THE ORGANISATION DIMENSION representing the different levels of organisational unit granularity at which risks must be managed;
- THE PROCESSES DIMENSION describing the major areas, processes and systems that play a part in the identification and management of risks.

Figure 3 - The idRisk Integrated Compliance Management Framework



Dimension 1 - RISKS

It is usual for organisations to consider their risks in different categories. For instance, banks commonly use Credit, Market and Operational (and sometimes something like Strategic to include the main business risks not otherwise categorised) as their risk categories. An alternative categorisation for industrial companies is Strategic, Financial, Operational and Hazard.

From a compliance perspective, the regulations are generally non-prescriptive in respects of risk categorisations³². Regulators want to see that organisations have logical and robust approaches to risk

³¹ These include the COSO Enterprise Risk Management Framework, the AS/NZS 4360 Risk Management Standard, the AIRMIC / IRM / ALARM Risk Management Standard, the Treasury Board of Canada Integrated Risk Management Framework, the HM Treasury Risk Management Framework, the Office of Government Commerce (UK) Risk Management Framework.

³² The exceptions may be the implementation of Basel II, which has defined event categories for the advanced Operational Risk approaches, and FSA PS04/16 – The Integrated Prudential Sourcebook for Insurers

identification, assessment and management that are appropriate for each organisation's particular circumstances. The risks are often common to many parts of the organisation and occur at many different levels.

A very important aspect to be managed within the evaluation and response process is that risks may mitigate one another or aggregate with each other. Mitigating one risk often increases one or more other risks, and with regard to a given action, there is risk of doing it and risk of not doing it. Thus the interaction between different risks is often complex. Correct evaluation of risk mitigation, interaction or aggregation is a critical part of building up an accurate overall risk picture for organisations.

Dimension 2 – ORGANISATION

Organisational structures can vary considerably even between similar organisations operating in the same field. There are often vertical and lateral inter-relationships between many parts of the organisation including operative functions and support functions. Modern organisations can be complex. Anyone who has worked in a large matrix organisation will be able to vouch for this.

Organisational complexity is a risk in itself. It can cause confusion over responsibilities and authorities and can increase the risks of duplications, contradictions and gaps. Each of these issues needs to be carefully considered within a risk management compliance response.

Consideration also needs to be given to the granularity of organisational unit at which risk is to be assessed and mitigated. Is it to be at the group level, the company level, the divisional level or the departmental level? Risks that are significant at a department level may be insignificant at a group level, but on the other hand, some risks buried deep in a single department can expose the entire group reputation. Risks need to be assessed and analysed at fine levels of granularity, but then 'rolled up' and aggregated for senior executive consumption whilst still providing 'drill-down' visibility for risk 'hot spots'.

Dimension 3 – PROCESSES

The front face of the idRisk ICM framework, Processes, comprises the five layers in which a typical organisation functions generically in its business operations, its compliance and its risk management:

- 3.1 External environment;
- 3.2 Internal environment;
- 3.3 Governance process;
- 3.4 Risk management process;
- 3.5 Risk management systems.

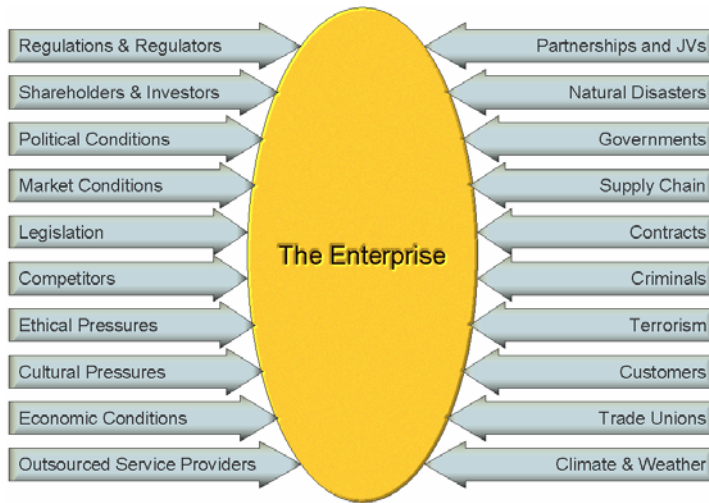
Each layer of this face affects different parts of organisations in different ways, each has different risks associated with it and each in turn has an effect on the identification and management of risks across organisations.

The five management Process layers interact with the Organisation and Risk dimensions of the 3-dimensional cube model. Through analysing the interaction of processes, people and systems that overlay the organisational structures it is possible to identify and map the inter-relationships in a clear and logical manner. This map then forms the basis for detailed analysis and response planning.

Layer 3.1 - External Environment

At the highest level, compliance regulation is about overseeing how organisations operate within the external environment. Figure 4 illustrates some of the many external interfaces that organisations have and that need to be considered in both the business planning and risk management processes.

Figure 4 – The External Environment of an Organisation



Amongst the external influences are the various stakeholders in the business, including shareholders and investors, customers, suppliers, employee representatives (such as trade unions and professional associations). Some of the risks can be controlled or mitigated more easily than others. Regulatory compliance focuses particularly on customers, shareholders and investors.

The compliance process needs to start with a clear understanding of, and alignment with, the organisation’s various stakeholders and the expectations that they have of the business.

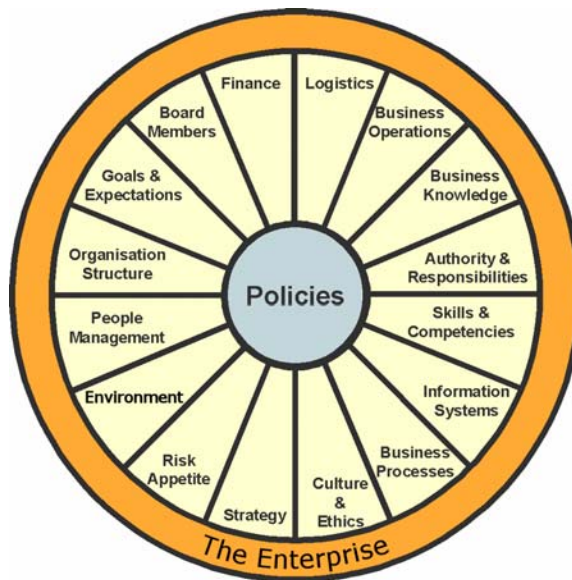
Layer 3.2 - Internal Environment

How well organisations interface with their external environment is a function of their internal environment. This internal environment is made up of all the functions in the organisation and, more importantly, the people. Compliance activity needs to establish its place, role and responsibilities, expectations and interfaces with its “internal customers”.

Arguably, this is the single most important and most difficult aspect of the whole integrated compliance process and is the next frontier in achieving good corporate governance, good operational risk management, and therefore compliance, in practice as well as in theory.

Figure 5 (overleaf) shows the internal environment in the form of a wheel. This particular model presents the organisation’s policies as the hub of the wheel, around which all other internal components revolve. These policies are made by the Executive Management and are the means by which the senior executives convey messages as to the culture, ethics and ways of working of the organisation. Everything else is driven by these policies. Policy-making is part of the governance framework, to be discussed in the next section.

Figure 5 – The Internal Environment of an Organisation



Boards and Executive Teams own the overall business process and delegate responsibilities and authorities (hopefully matching each other) to designated persons and bodies.

Fundamentally, failures in the internal environment are more often than not the underlying causes of the strategic and operational losses that are increasingly making the headlines and which have become the initiators of extended regulatory compliance activity.

Layer 3.3 - Governance Process

The third management framework layer of the 3-dimensional model is the governance process. This is how organisations go about managing themselves, having established an organisation structure and culture. The diagram in Figure 6 (overleaf) illustrates the issues and activities involved in this process.

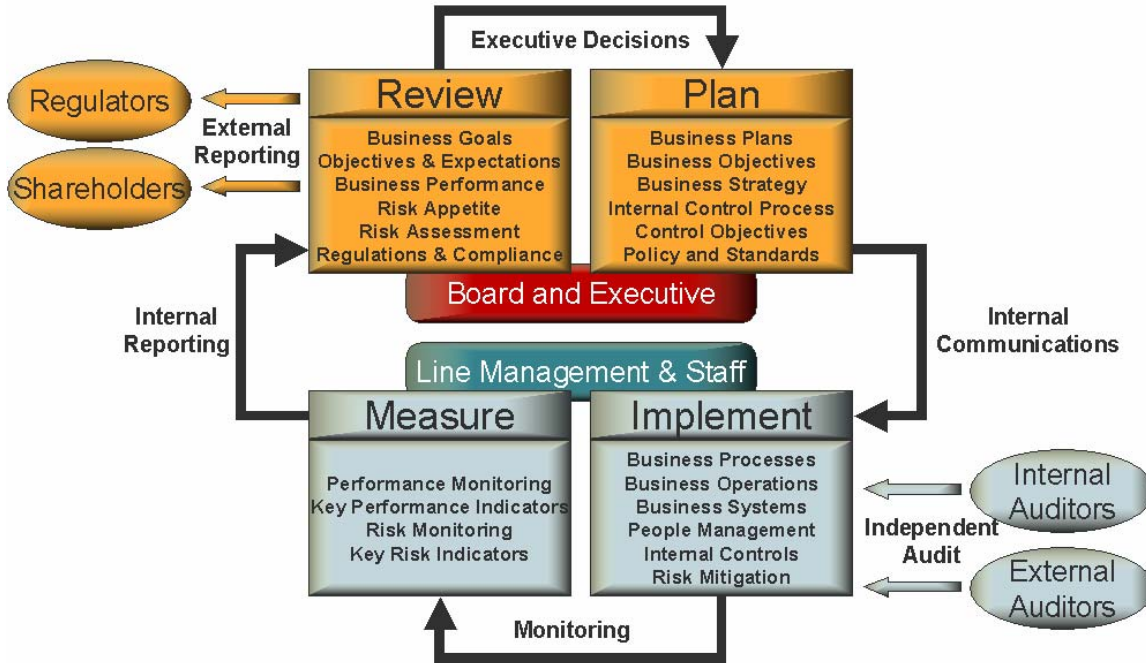
There are innumerable diagrams illustrating this overall business operational process with variations on the Plan, Implement, and Measure and Review theme. However, they all address the same fundamental issues and involve ultimately a cyclic and hopefully ever changing and improving process.

The FSA Handbook addresses the overall governance structure that it expects to see in two main blocks.³³

- High Level Standards - relating to the overall principles that The FSA expects its regulated businesses to follow, expectations of senior management and identifying specific functions relating to general management and customer management where the individuals responsible have to be personally approved as fit and proper;
- Business Standards – where different “Prudential sourcebooks” apply to different regulated business functions including investment of customer funds, conduct of business with customers, training and competence and money laundering.

³³ <http://www.fsa.gov.uk/vhb/>

Figure 6 – The Governance Process



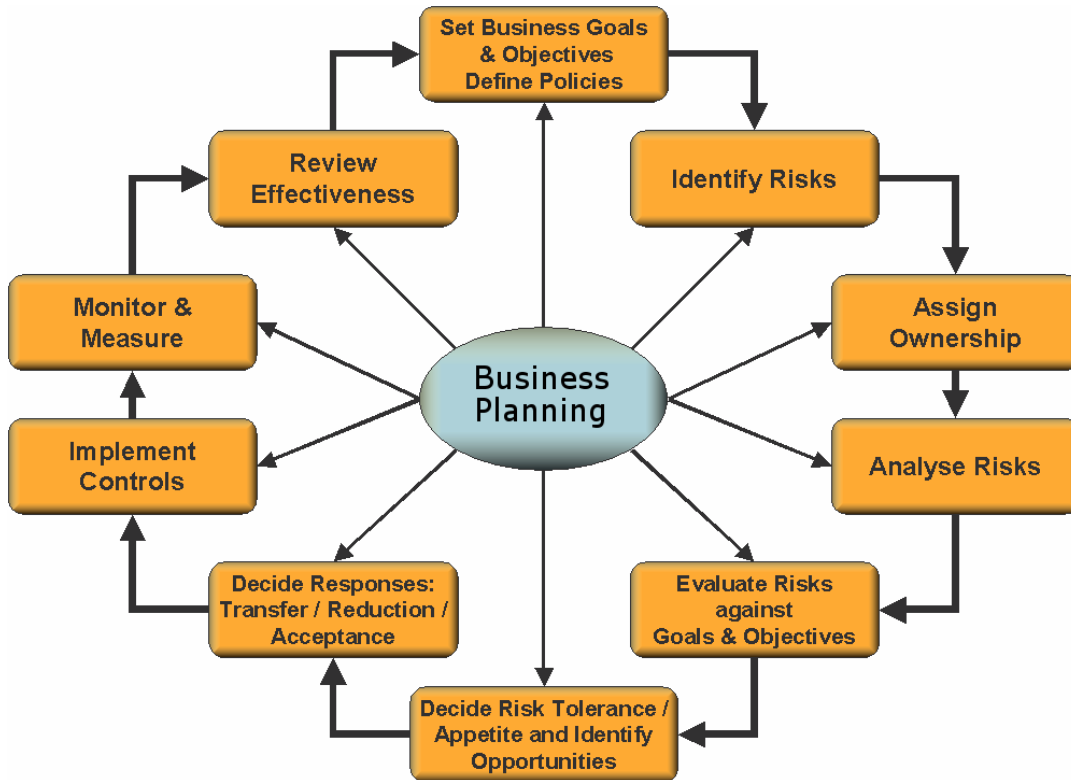
Compliance activity needs to understand fully and, where necessary challenge, organisations' governance processes since failures in these will leave the door open for breach "opportunities" at any point in the business. If businesses' operational fundamentals are wrong, both on paper and in practice, the chances of "compliance breaches" occurring increase significantly.

Layer 3.4 - Risk Management Process

The risk management process sits beneath the overall business governance process because it is a sub-part of it and it enhances the operational aspects of the business. It is again a cyclic process, which should constantly modify and improve to adjust for changing business circumstances and rising expectations. The COSO³⁴ diagram shown in the References at the end of this paper represents the same fundamental process.

³⁴ The Committee of Sponsoring Organisations of the Treadway Commission <http://www.coso.org/>

Figure 7 – The Risk Management Process Framework



Layer 3.5 – Risk Management Systems

This fifth Processes layer constitutes the computerised operational, information, financial, reporting, analysis and management systems that enable modern businesses to function at all, let alone efficiently and cost efficiently. The connectivity and roles of the various computer systems is complex in most instances.

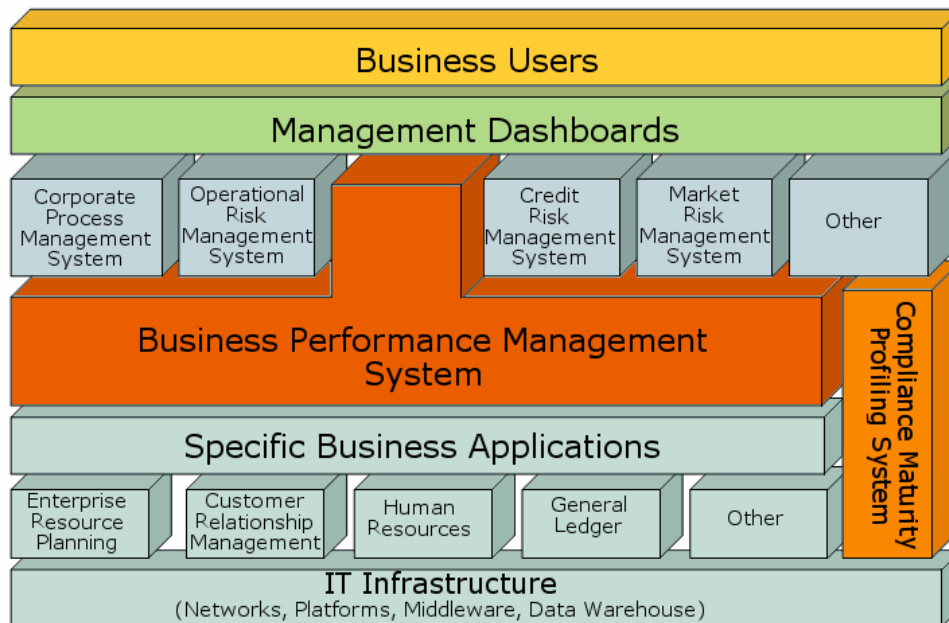
Risk Management Systems are one of the key foundations of an Integrated Compliance Management process. To be effective, Information Technology needs to be given equal importance within the overall business risk management framework.

The combination of risk management systems and their “user interfaces” has six components:

1. IT Infrastructure and Specific Business Applications;
2. Business Performance Management System;
3. Process Management and Risk Management Systems;
4. Compliance Maturity Profiling System;
5. Management Dashboards;
6. Business Users.

Approaching the Risk Management Systems architecture requirements in an organised and logical way using the six-component architecture framework outlined below enables organisations to establish clear needs requirements that will fulfil the obligations of compliance at the same time as improving risk management and business performance.

Figure 8 – The idRisk Risk Management Systems Architecture



3.5.1 IT Infrastructure and Specific Business Applications

Starting from the bottom, these components cover the various hardware and software platforms and communication systems that constitute the underlying major organs, arteries and nervous systems of organisations. The challenge to businesses in this area is to generate superior returns on their IT investment by using the technology and resulting information to become more effective and efficient. Legacy issues from mergers and acquisitions and badly configured or out of date systems further complicate the sources of potential compliance and risk management information.

One of the fundamental issues for obtaining risk management and compliance information from the existing legacy systems is that the information that is needed for compliance and risk management may well have not been collected in the first place. Systems may have been purchased and programmed at a time when the information needed had not been identified.

Another key issue is that of data quality. Failures or laxness in applying the surrounding process, training and competency, and checks and supervision has meant that the quality of data that has been entered varies greatly from area to area, year to year and operator to operator.

There are massive data issues to resolve for many organisations and the best that most of these can do in the short term is to instigate a flexible approach where data can be augmented and improved in the future.

IT systems are an area that is fraught with problems and pressures due to organisations looking for so called “quick wins”, ignorance of what information is needed now and may be needed later and poor communication between stakeholders, users and systems professionals.

The Integrated Compliance Management approach recognises and responds to these fundamental issues by linking organisations’ varied information sources and departments and minimising the time and expense required to re-engineer legacy systems.

3.5.2 Business Performance Management Systems (BPM)

BPM systems (including On-Line Analytical Processing (OLAP) systems) extract, analyse and report information to managers for business planning and for managing Key Performance Indicators. Historically, the software has focused on budgeting and financial performance. New challenges for these systems are coming from increasing regulatory requirements governing capital levels to meet statutory solvency requirements,³⁵ the need to analyse and undertake “what if” analysis on various different risk scenarios, and the need to extract and analyse risk related information (risks, losses, control costs) from many systems across organisations.³⁶

3.5.3 Process Management and Risk Management Systems

These systems collect operational and risk data associated with specific business activities; for instance, in the case of a bank, credit risk management and the market risk resulting from managing the overall financial risk exposure within a portfolio of investment and trading positions. For an insurance company, the equivalent is managing the risk profiles in its underwriting portfolios and in its claims and reinsurance arrangements.

There is a multitude of specialist Risk Management Information Systems (RMIS) on the market. Most have been developed for a specific task and then have tried to widen their capabilities into other associated areas, with varying degrees of success. Organisations can greatly benefit from careful research of the available tools, especially determining their strengths and limitations as well as the communication with other specialist systems. Consultants, such as idRisk, with knowledge of the market and an understanding of businesses’ needs can make the selection process less risky.

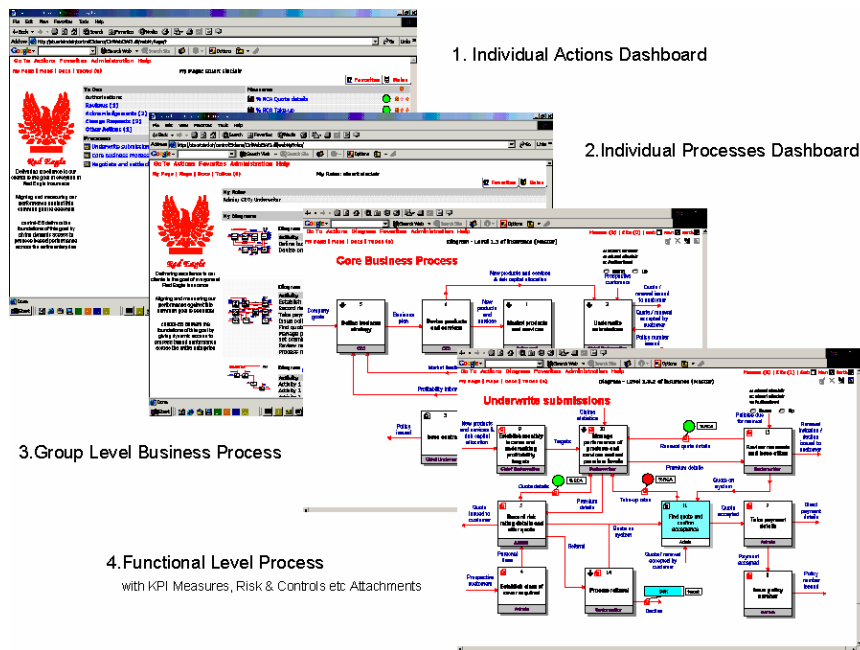
Corporate Process Management (CPM) systems enable organisations to establish a clear vertical and horizontal picture of the linkages in their business processes from a high level, broken down all the way through the organisation to individual operations and business units. The best systems link electronically with information from other systems to highlight performance and risk, as well as feeding back selected information to managers within their individual dashboards and scorecards. Figure 9 (overleaf) shows some screens from a CPM system developed by idRisk and Nimbus Partners.³⁷

³⁵ Pillar 1 of the New Basel Capital Accord affecting banks and Solvency I and II from the EU affecting insurance companies

³⁶ See <http://www.applix.com/solutions/ProdSolsTCO.asp> for a leading example

³⁷ See <http://www.nimbuspartners.com/>

Figure 9 – The idRisk/Nimbus Corporate Process Management System



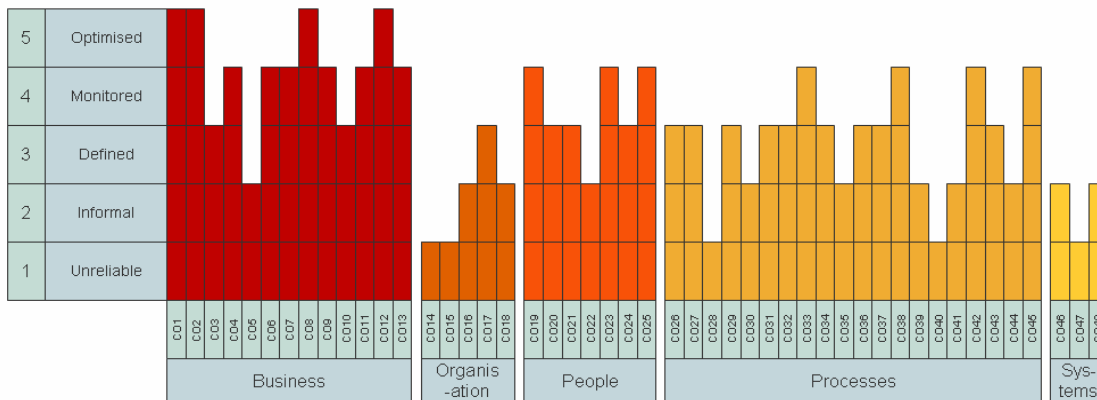
3.5.4 Compliance Maturity Profiling System

The operational, risk management and compliance performance of individuals and of business units varies within all organisations. In addition, some organisations set and follow more rigorous standards than others, and organisations need to be able to evaluate performance from one period to the next.

The issue here is one of capability in implementing good governance practices, rather than the statistics resulting from successes or failures. Capability Maturity Models are an ideal way to capture this soft information. They have been developed and used in the IT industry for several years. The technique is now being migrated into the compliance and risk management areas, linked in with Business Performance Management dashboards, and is being computerised and web-enabled for quicker, cheaper and more responsive applications.

Web based models, such as the idRisk Compliance Maturity Profiling (see Figure 10), enable quick and regular assessments to be made by management of progress and quality of compliance and risk management practices in a structured, repeatable and auditable format. The output will be timely and able to be “sliced and diced” to respond to different output receivers’ needs and authorities.

Figure 10 – The idRisk Compliance Maturity Profile (Control Activity Detail Not Shown)



3.5.5 Management Dashboards

Organisations are increasingly using various incarnations of dashboards and scorecards to provide more real-time performance information and to relate performance to reward. They are also requiring real time, but secure, accurate and relevant information to be fed back to operating managers in order for them to better anticipate, respond to and recover from problems.

Output from the various business and risk management systems fed through a Corporate Process Management system or Business Performance Management system is starting to enable managers to receive combined information from a multiple of sources and sub-systems – and in near real time.

3.5.6 Business Users

At the end of the day, compliance, risk management, business performance and risk and reward all come back to the business users operating throughout the organisation. An Integrated Compliance Management system will deliver the same quality of relevant information to any organisation member with access to a computer, so that both manager and managed can have the same information and an improved opportunity for positive performance achievement.

Summarising the Processes Dimension

The five process layers of the idRisk Integrated Compliance Management framework interact with the Organisation and Risk dimensions of the 3-dimensional cube model. Through analysing the interaction of processes, people and systems that overlay the organisational structures it is possible to identify and map the inter-relationships in a clear and logical manner. This map then forms the basis for detailed analysis and response planning.

Approaching the Risk Management Systems architecture requirements in a similarly organised and logical way using the six-component architecture framework outlined above also enables the organisation to establish a clear needs requirement that will fulfil the obligations of compliance at the same time as it improves risk management and business performance.

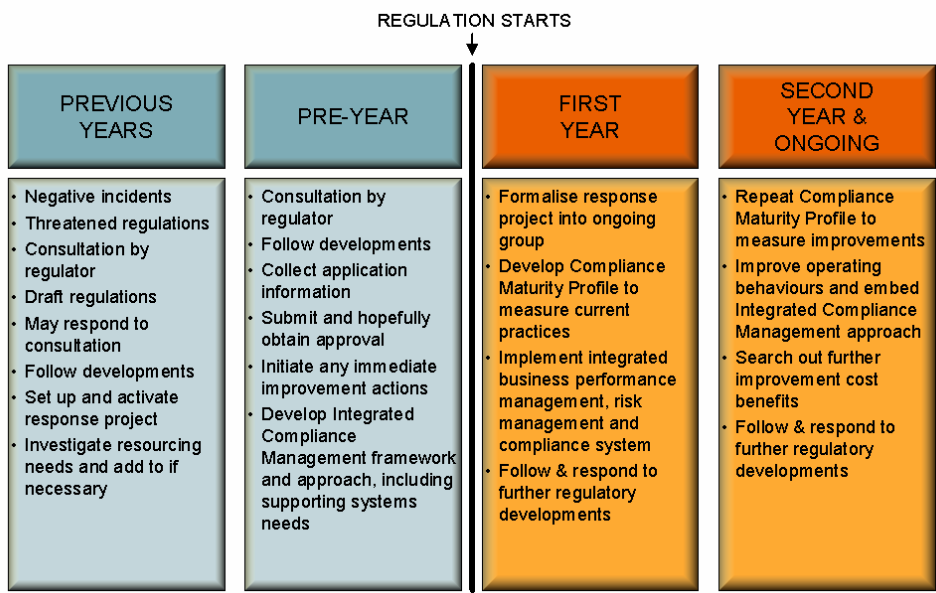
Putting Integrated Compliance Management into Practice

The first task is to formulate an Integrated Compliance Development Plan. The plan needs to take into account the implications and responses to compliance outlined in Section 2 of this paper and there are three things that organisations need to do once any initial approval applications have been prepared and submitted.

- 1. Catch up with any outstanding documentation and practices**
 - Consistently across the organisation
 - At all levels
 - In all operations
- 2. Plan for the future**
 - Including developing a system to measure and monitor improvements
- 3. Develop and embed good governance and compliance practices**
 - Consistently across the organisation
 - At all levels
 - In all operations

This simple high-level development sequence is represented generically in the diagram in Figure 11.

Figure 11 – Integrated Compliance Management Development Plan



CONCLUSIONS

- *There is no viable alternative to Integrated Compliance Management.* This White Paper puts the case that all organisations that need to become and remain “compliant” with the various and increasing corporate governance regulations need to follow an Integrated Compliance Management approach in order to cost-effectively maintain their compliance sign-offs. The alternative is a series of disjointed, and ultimately more costly, activities and special projects.
- *Compliance should be approached within an Enterprise Risk Management framework.* Compliance risk is just one of organisations’ operational risks which are, in turn, one area of organisations’ overall business, or enterprise risks. In order for compliance risk to be appropriately and cost- effectively managed, it needs to be integrated within organisations’ overall business planning, business operation and enterprise risk management processes and systems.
- *The COSO model should be the basis of the ERM framework.* There are variations on the theme of Enterprise Risk Management, but the COSO model is becoming generally accepted as the international basis. In the UK, the Combined Code follows a simplified version of COSO. It is therefore recommended that organisations adopt a COSO based Enterprise Risk Management approach and that their Compliance activities are integrated within this overall framework.
- *The most crucial element of compliance success or failure will continue to be the people operating in senior positions in businesses;* how they behave, what sort of example they set, what sort of standards they apply in rewarding themselves and their employees and how they monitor progress against business plan.
- *Good-governance compliance is not a one-off issue.* The regulations introducing and raising the profile mean that there is a complete *and permanent* increase in stakeholder expectations. This development is requiring many organisations to review and change their existing operating and reporting practices - “to do it differently around here”.
- *Departments acting in isolation unnecessarily increase compliance risk.* Each department needs its areas of responsibility and authority clearly defined and dovetailed with the other.
- *Departments acting together reduce compliance risk and create increased benefits.* Integrating the know-how, tools and supporting technologies developed by different departments will enable organisations to create more powerful and cost effective compliance responses.
- *An organisation and process structure flow chart is an essential common point of reference to identify, manage and report on risk points in business operations.* This needs to be electronically based, clearly documented, vertically and horizontally linked, owned by the businesses rather than the analysts and with real time selective desk top delivery, in order for it to be widely adopted and actively used. Without such a system, gaps and overlaps between functions and with external suppliers, outsourcers and customers are hard to see and it is these hidden areas where organisations key risks often lie.
- *A separate technology led response is unlikely to be an appropriate corporate governance compliance solution.* Rather, any new compliance systems need to be integrated with organisations’ other (often existing) risk management systems. The wider picture and end game needs to be first understood before compliance technology investments are made. These should be developed in a planned and linked series of small projects that respond to specific needs and deliver measurable benefits. “Think big and plan small”. Each compliance project needs to be planned to deliver its output within no more than six months and ideally within three months. Effective planning, people and data issues will be critical to success.
- *The overall integrated compliance solution in many cases will be a combination of pieces.* Systems improvements, policies and procedures, systems of check and supervision and individual training and competencies are all needed to deliver effective compliance and contribute to business improvements.

Integrated Compliance Management

- *The cost of getting it wrong for organisations that need to be compliant will be much higher than the investment required for getting it right.*
- *Integrated Compliance Management is the best way forward.* All organisations have some sort of existing compliance practices; many are looking at revising and improving their practices now as a result of new and threatened regulatory changes. By applying the Integrated Compliance Management framework and approach, organisations can build on their existing work, turning the compliance obligation and cost into a business improvement opportunity and a value.

- KEY MESSAGES
 - Non-compliance costs money.
 - Effective compliance need not be expensive.
 - Using ICM is fully justified on any benefit-risk analysis.
 - Compliance must be an integral part of businesses, not a separate function.

REFERENCES

Enterprise Risk Management (ERM)

Enterprise Risk Management is an approach to business planning and management and to risk management that has been developed by leading practitioners over the last few years in response to “good governance” regulations and also in response to a desire of many leading organisations to better leverage their cross-functional expertise and develop a consolidated view of risk across the organisation.

ERM enables organisations to embed risk management in their normal processes and systems rather than create a new audit-style overhead. The approach is recommended by leading business and risk management organisations as being the best way forward for all types and sizes of organisations.³⁸

To quote from the COSO ERM Framework Executive Summary;

“Enterprise risk management is not an end in itself, but rather an important means. It cannot and does not operate in isolation in an entity, but rather is an enabler of the management process. Enterprise risk management is interrelated with corporate governance by providing information to the board of directors on the most significant risks and how they are being managed. And, it interrelates with performance management by providing risk-adjusted measures, and with internal control, which is an integral part of enterprise risk management.

Enterprise risk management helps an entity achieve its performance and profitability targets, and prevent loss of resources. It helps ensure effective reporting. And, it helps ensure that the entity complies with laws and regulations, avoiding damage to its reputation and other consequences. In sum, it helps an entity get to where it wants to go and avoid pitfalls and surprises along the way.

Enterprise risk management is defined as follows:

Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

This definition reflects certain fundamental concepts. Enterprise risk management:

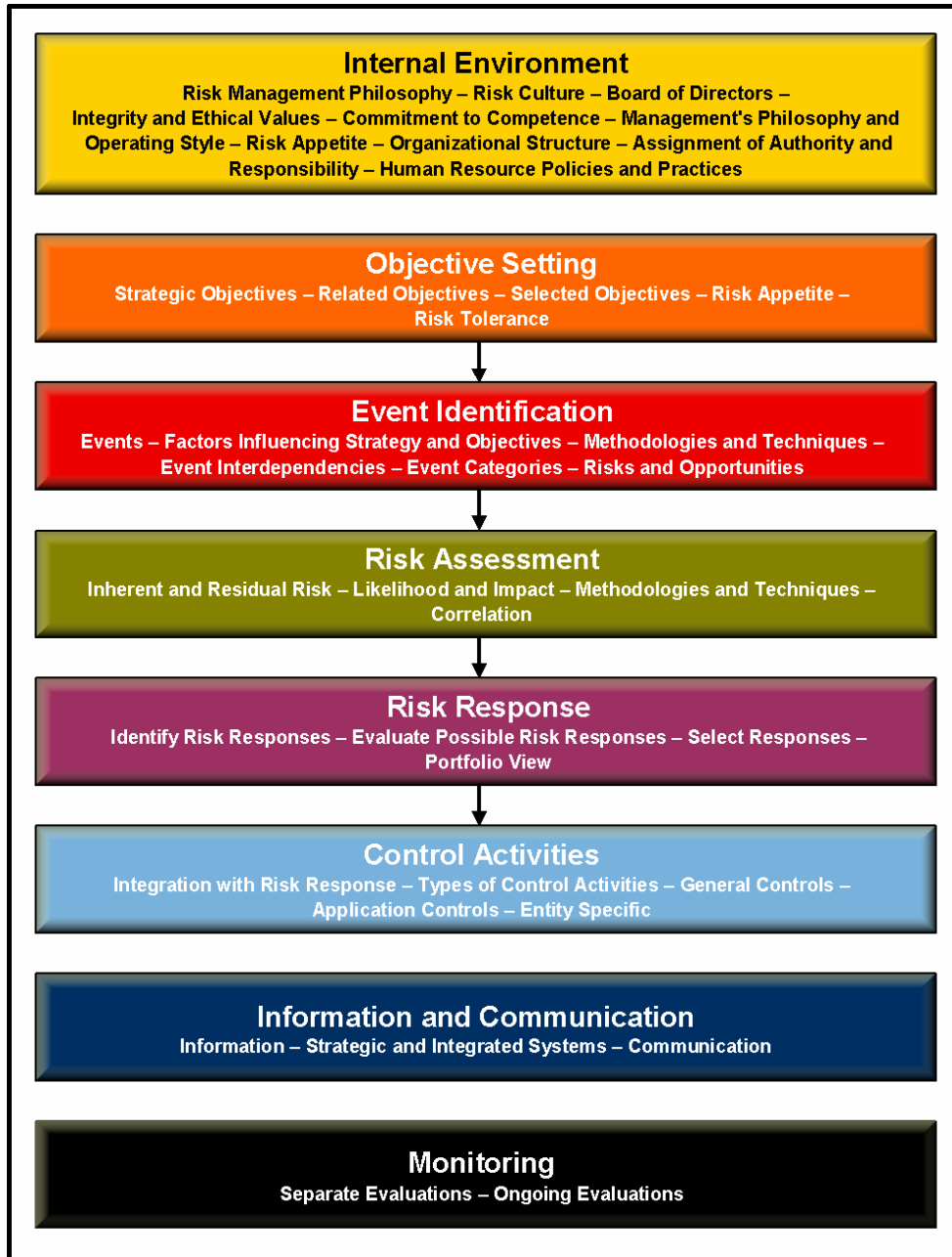
- Is a process – it's a means to an end, not an end in itself;
- Is effected by people – it's not merely policies, surveys and forms, but involves people at every level of an organization;
- Is applied in strategy setting;
- Is applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risks;
- Is designed to identify events potentially affecting the entity and manage risk within its risk appetite;
- Provides reasonable assurance to an entity's management and board;
- Is geared to the achievement of objectives in one or more separate but overlapping categories.

This definition is purposefully broad for several reasons. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across different types of organizations, industries and sectors. It focuses directly on achievement of entity objectives. And, the definition provides a basis for defining enterprise risk management effectiveness.”

The diagram in Figure 12 from the COSO paper represents a logical and practical risk management process that is suitable for all types and sizes of organisation.

³⁸ See especially the COSO Draft Enterprise Risk Management Framework [http://www.erm.coso.org/Coso/coserm.nsf/vwWebResources/PDF_Manuscript/\\$file/COSO_Manuscript.pdf](http://www.erm.coso.org/Coso/coserm.nsf/vwWebResources/PDF_Manuscript/$file/COSO_Manuscript.pdf) and the AIRMIC/ALARM/IRM Framework http://www.airmic.com/AIRMIC_RiskManagementStandard.pdf

Figure 12 - COSO ERM Processes (Components)



Acknowledgements

Many colleagues have contributed information and thoughts to this paper, especially John Sherwood, John White, John Shrimpton, Barry Hammond, Dion O'Leary, Ken Hall, Angela Darling, Mark Butterworth and Alan Duncan.

About idRisk

idRisk is an organisation of specialised, independent risk advisers who are experts in their respective fields and who provide customers with comprehensive, high quality unbiased advice on, and solutions to, all aspects of risk that a business may encounter. By creating an extended network of highly skilled consultants and combining them with leading edge technology and information processes, idRisk design, develop and deliver the best solutions to all major business risk areas. See the links in the footnote below for more information on idRisk, its consultants and partners.³⁹

About the Author

Chris Kind is a Partner and Business Stream Leader in idRisk. He specialises in the analysis and resolution of complex risk-related problems, particularly where multi-disciplinary approaches are required. He has an extensive general background in risk management, risk financing and insurance. Particular areas of focus include corporate governance risk management and compliance, Enterprise Risk Management, risk-adjusted business planning, the formulation and execution of risk management, risk financing and insurance strategies and demonstrating the value from risk management and insurance.

Contact Information

ChrisKind@idRisk.com

³⁹ idRisk homepage <http://www.idrisk.com>

idRisk one page outline http://idrisk.com/v2articles/155_What_is_idRisk.pdf