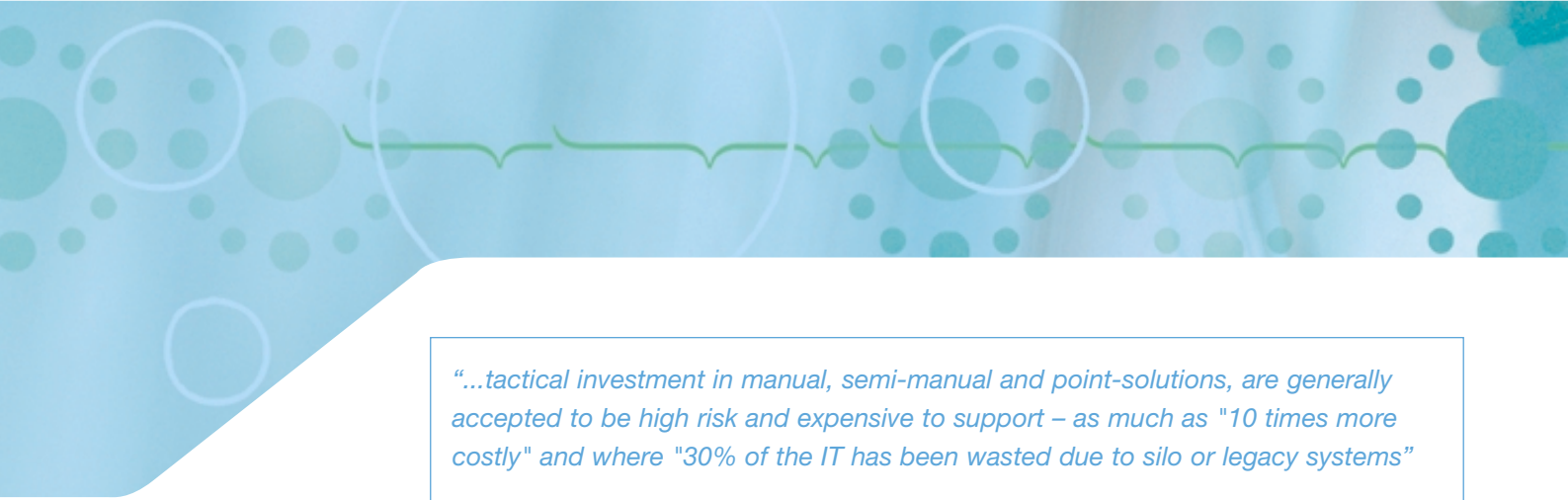




Thought Leadership Point Of View: [The Second Phase of IT Risk and Compliance Solutions](#)

**Significantly Reducing the Cost of Maintaining
Governance, Risk and Compliance Across the Enterprise**



“...tactical investment in manual, semi-manual and point-solutions, are generally accepted to be high risk and expensive to support – as much as "10 times more costly" and where "30% of the IT has been wasted due to silo or legacy systems”

Contents

Introduction 3
#1. The cost of Governance, Risk and Compliance 4
#2. The vision of integrated Enterprise Risk Management (ERM) 5
#3. Building efficient Governance, Risk and Compliance 6
#4. Efficient IT governance through infrastructure integration 6

Introduction.

This Point of View is designed for business and IT executives in enterprise or mid-market organisations to demonstrate how to engage Governance, Risk and Compliance in the second phase of this market for IT solutions. The first phase of risk and compliance solutions was a combination of tactical investment in manual, semi-manual and point-solutions, which are generally accepted to be high risk and expensive to support – as much as "10 times more costly" and where "30% of the IT has been wasted due to silo or legacy systems" according to independent analysts.

The second phase of Governance, Risk and Compliance is driven from a strategic and integrated perspective, with the aim of reducing both cost and risk. This will be achieved by integrating the needs of business, accounting, compliance, risk and IT executives with those of auditors, who have direct or indirect responsibility for ensuring efficient compliance to regulations, policies or standards, and integrated risk management.

To reduce the substantial cost of maintaining, monitoring and reporting on Governance, Risk and Compliance, an integrated policy foundation is available to achieve an holistic risk management and compliance execution enterprise-wide. This foundation is the Committee Of Sponsoring Organisations (COSO) Enterprise Risk Management Integrated Framework (www.coso.org) with implementation by applying best practice through application of ITIL (Information Technology Library), CoBIT, ITGI (IT Governance Institute), ISO 20000 (IT Service Management), ISO 27001 (Information Security Management).

There are, however, different approaches to the discipline of Governance, Risk and Compliance, whereby the publicly owned enterprise is being directed by auditors and regulators into a proactive approach using COSO Enterprise Risk Management and an associated IT best practice.

In smaller enterprises, the approach can be more crisis-driven and a reactive approach more likely. However this is increasingly unsustainable as customers, auditors, regulators, insurers, ratings agencies and venture capital firms start to mandate a formalised Governance, Risk and Compliance policy that is robust, best practice and standards based – this is risk and compliance phase #2.

IBM applies Thought Leadership in IT to compelling business cases to achieve reduced cost, improved efficiency, higher competitiveness and reduced enterprise risk compared with manual or non-integrated IT legacy systems. (Please note that IBM does not make a corporation compliant or formulate risk policy – that is the role of the auditor or attorney working with the corporation's officers with responsibility for compliance policy execution and monitoring.)

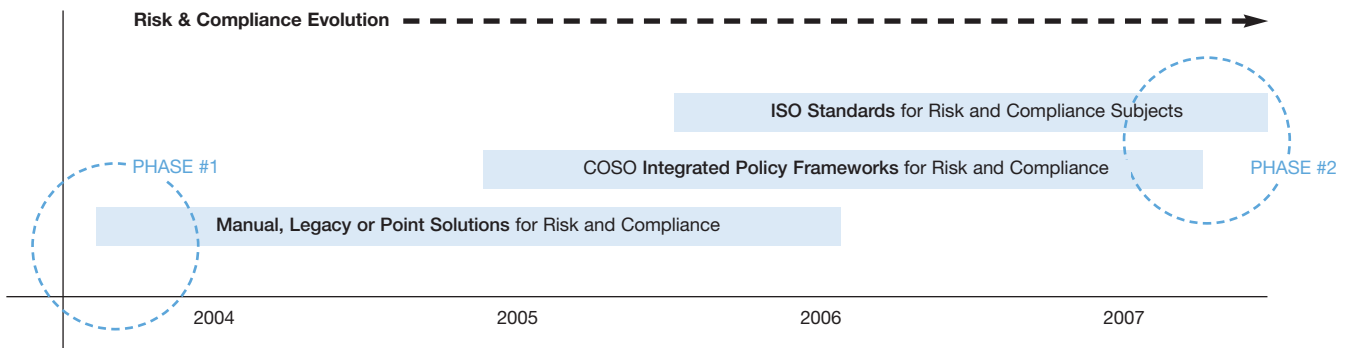


Figure One: Risk and Compliance Phase 1 & 2. © Copyright Industry Direct Ltd.

“Fundamentally therefore, to reduce compliance costs and similarly reduce risk over manual or non-integrated IT systems, it is necessary achieve efficiencies through a better integrated approach to the IT system”

#1. The cost of Governance, Risk and Compliance.

The Sarbanes Oxley Act, which covers internal controls for financial reporting, is now influencing smaller publicly and privately held corporations, as well as government organisations, due mainly to the influence of auditors, venture capital firms and the publicly traded customers of privately held companies. But Sarbanes Oxley is one regulation amongst many, and for some industries there are multiple Governance, Risk and Compliance drivers, with the list growing significantly.

The problem is not one of becoming compliant, or of developing a risk management policy, as there is already plenty of advice and counsel available from the audit and attorney community, as well as from people filling the corporate roles of Chief Compliance Officer or Chief Risk Officer who create compliance policies for their employers.

The problem for the corporation is to manage the cost of sustaining Governance, Risk and Compliance, including monitoring and reporting. Efficiency is critical, not just to manage costs, but also to reduce risk compared with manually dependent or non-IT integrated information and control systems from disparate vendors. There have already been defections from the NASDAQ that cite the cost of meeting US control regulation as the reason for their exit. The average cost to a Fortune 1000 company in meeting internal control compliance requirements of Sarbanes Oxley has been stated by analysts as being in the US \$5 million to US \$10million range, which has largely been the cost of audit fees in creating the policies – and this is in relation to Sarbanes Oxley alone!

IBM understands the need for an integrated Governance, Risk and Compliance strategy that ensures investment is targeted centrally and locally, with returns maximised in terms of both business and technology value, which is the foundation of the business case. Fundamentally therefore, to reduce compliance costs and similarly reduce risk over manual or non-integrated IT systems, it is necessary to achieve efficiencies through a better integrated approach to the IT system – which probably enjoyed minimal attention to compliance in either the original design or the evolution of its applications or infrastructure. So what is the best approach to match IT Governance with the dynamic growth in Corporate Governance?

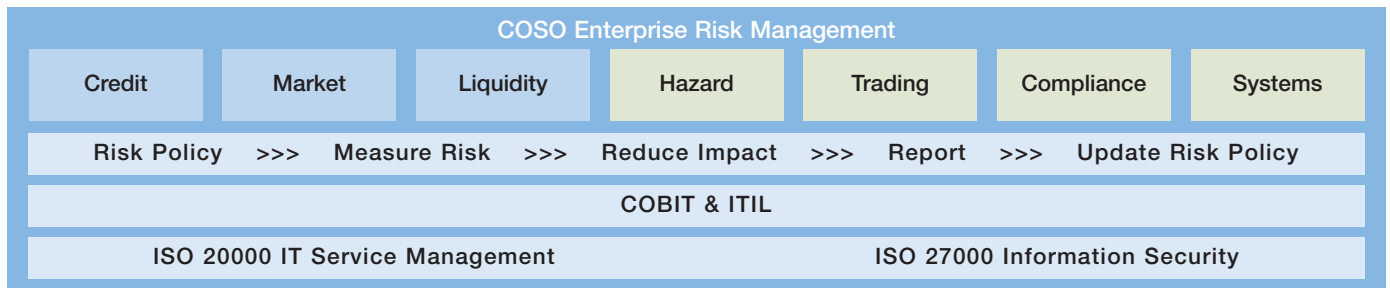


Figure Two: COSO Enterprise Risk Management. © Copyright Industry Direct Ltd.

#2. The vision of integrated Enterprise Risk Management (ERM).

The Sarbanes-Oxley Act makes corporate executives explicitly responsible for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting. For most organisations, the role of IT will be crucial to achieving this objective.

The US audit community based their initial Sarbanes Oxley risk assessment on the SEC recommended Committee of Sponsoring Organisations (COSO) – Internal Controls Integrated Framework. This was then interpreted from an IT perspective by the IT Governance Institute (ITGI) IT Control Objectives for Sarbanes Oxley. This guidance and suggestion of best practice using CoBIT creates the foundation for IT Governance and a model for efficient Sarbanes Oxley implementation across an organisation.

Today, the more holistic COSO Enterprise Risk Management (ERM) Integrated Framework for risk management policy is emerging since its introduction in Europe by the Institute of Internal Auditors in October 2005.

ERM & The US Institute of Internal Auditors

In 2005 the Institute of Internal Auditors (www.theiia.org) recommended to their nearly 100,000 members running Internal Audit departments in corporations worldwide, the following approach to implementing the vision of ERM:

IIA NOTE: Many of the risks that could result in substantial losses to an organisation are within operational areas. The CAE can ensure that the agreed upon audit plan includes those areas and is well balanced and effective. The IIA advocates for an enterprise risk management (ERM) process that takes into account all aspects of an organisation, rather than one that focuses only on the financial issues. For more about ERM, refer to COSO – at www.coso.org.

Consequently, today, many audit firms are supporting clients in the development of an integrated ERM policy. Scaling out from their original investments and creating a structured approach for more reliable IT investment and an integrated IT infrastructure is critical for the successful implementation of the ERM policies. Even in the mid-market, where a more crisis-driven approach may have applied in the past, there is compelling business value in the lower cost and risk of an integrated rather than fragmented IT support for these best practice policies.

**IDL Point of View:
Integrated Governance, Risk and Compliance**

“there are many common factors across multiple Governance, Risk and Compliance drivers that can offer an integrated re-useable strategy, which is more secure from an IT Governance perspective, and significantly lower in cost”

#3. Building efficient Governance, Risk and Compliance.

As an IT organisation becomes more focused on being aligned with the business – and its integrated ERM policies as recommended for example by ITIL – IT infrastructure needs to become more integrated. This is where the IT Governance Institute (ITGI) is a valuable guide. The ITGI recommendations include a 9-step roadmap, a foundation for achieving efficient Governance, Risk and Compliance, and upon which offerings are based.

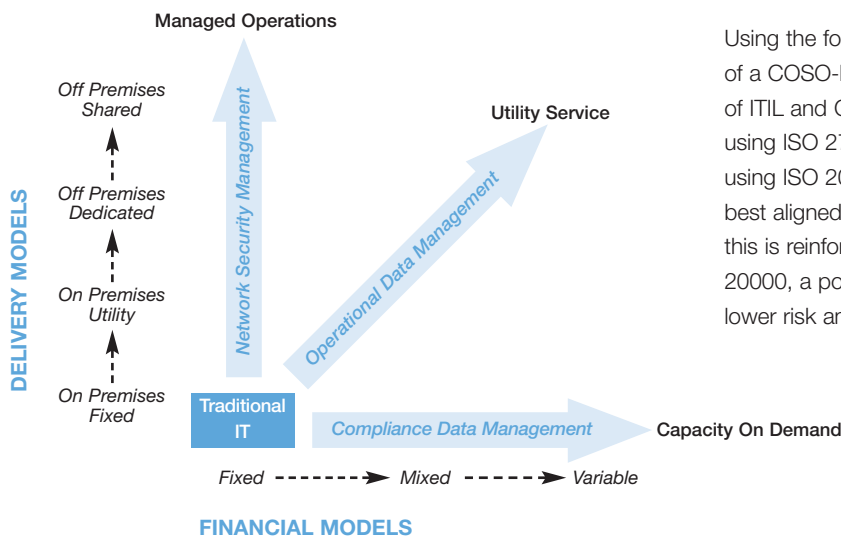
#4. Efficient IT governance through infrastructure integration.

In building efficient integrated IT Governance to match the needs of Corporate Governance, consolidation is feasible and in fact desirable. Many corporations engage risk and compliance management from a tactical operations perspective by having individual responsibilities for different compliance issues – for example, an Anti-Money Laundering Officer, a Basel II Committee, and a Sarbanes Oxley Committee.

This approach can be costly, as it leads to ‘point solutions’ from an IT or communications perspective, yet there are **many common factors** across multiple Governance, Risk and Compliance drivers that can offer an integrated re-useable strategy, which is more secure from an IT Governance perspective, and significantly lower in cost.

Strategically, the relationship between application controls and IT general controls is such that IT general controls are needed to support the functioning of application controls, and both are needed to ensure complete and accurate information processing. Therefore, the strategy recommended by IBM is to begin one’s consolidation efforts at the general controls level.

Using the foundation of ITGI recommendations for implementation of a COSO-based ERM policy framework allows for the application of ITIL and CoBIT, with the opportunity for certification of security using ISO 27001, and certification of IT service management (ITSM) using ISO 20000. These frameworks and certification standards are best aligned to an integrated rather than fragmented solution, and this is reinforced by analysts who suggest that by applying ISO 20000, a potential 48% TCO reduction is available – in addition to lower risk and higher resilience through integration.



© Copyright IBM 2006

Figure Three: Integrated Risk Management and Compliance On Demand

Risk Management and Compliance Subject	Integrated IBM Software Solution
Risk & Compliance Executive Dashboard	IBM Workplace for Business Strategy & Execution (WBSE)
Internal Controls and Reporting	IBM Workplace for Business Controls & Reporting (WBCR)
Sarbanes Oxley #404	IBM WBCR, WebSphere Portal, DB2 CM & DB2 UDB
EU Anti-Money Laundering Directive (Patriot Act)	IBM Entity Analytics; DB2
Solvency II	IBM DB2 UDB, IIA with IIW, WebSphere II
ISO 20000 IT Service Management	IBM Tivoli ITSM Solution Set
ISO 27001 Information Security	IBM Tivoli Security Solution Set

Figure Four: Example of Integrated IBM Software Solutions Aligned to Governance, Risk and Compliance

Clearly the emerging ISO 27000 or ISO 20000 standards are very valuable to certify aspects of the Governance, Risk and Compliance policy IT implementation. The NHS, for example, is just one government department that insists on vendors having ISO 20000 certification. A similar approach is anticipated from retailers and auto-makers as they introduce RFID to their supply chains, generating massive amounts of data whose value depends entirely on its proper management and distribution.

Therefore, from an IT perspective an integrated policy needs an integrated framework, based around the following priorities:

- Security
- Content management
- Service management and delivery
- Storage management, archiving and retrieval
- Continuity management

In addition, an example of a more specialised requirement may include entity analytics for fraud detection in conjunction with anti-money laundering.

Ideally, the route to integration would involve a single vendor with sufficient width and compatibility of offerings - both of which IBM is uniquely equipped to provide. The selection from IBM's integrated software portfolio shown above offers the coverage and depth required for the integrated risk management and compliance policy implementation in support of the integrated ERM framework, plus the potential to achieve a considerable reduction in TCO.

IDL Point of View:
Integrated Governance, Risk and Compliance

Acknowledgements

The guidance of these organisations is recognised by IBM in the preparation of this Point-of-View:

- IT Governance Institute "IT Control Objectives for Sarbanes Oxley"
- COSO Enterprise Risk Management Integrated framework
- COSO Internal Controls Integrated Framework
- The Institute of Internal Auditors.

Disclaimer

IBM have expertise in information technology solutions and do not have the skills to create Governance, Risk and Compliance policy and therefore IBM will not take any responsibility for making an organisation compliance or risk averse. This is the responsibility of the organisation's risk, compliance officers and board of directors working with expert advisers.

IBM is a trademark of International Business Machines Corporation.

This report has been compiled by:

IDL, 5 Kinsbourne Court, 96-100 Luton Road Harpenden,
Hertfordshire AL5 3BL, UK
Telephone: +44 (0) 1582 462266
Facsimile: +44 (0) 1582 461874
E-mail: idl@idlmail.com

IDL is an IT analyst with skills in training and enabling IT organizations in formalization of repeatable solutions by leveraging standards, frameworks and regulations in the field of risk management and compliance. The business benefits are substantially lower cost of ownership and lower risk by applying an integrated and scalable approach to IT governance in support of integrated corporate governance.

Copyright © 2006 Industry Direct Ltd. All rights reserved.

