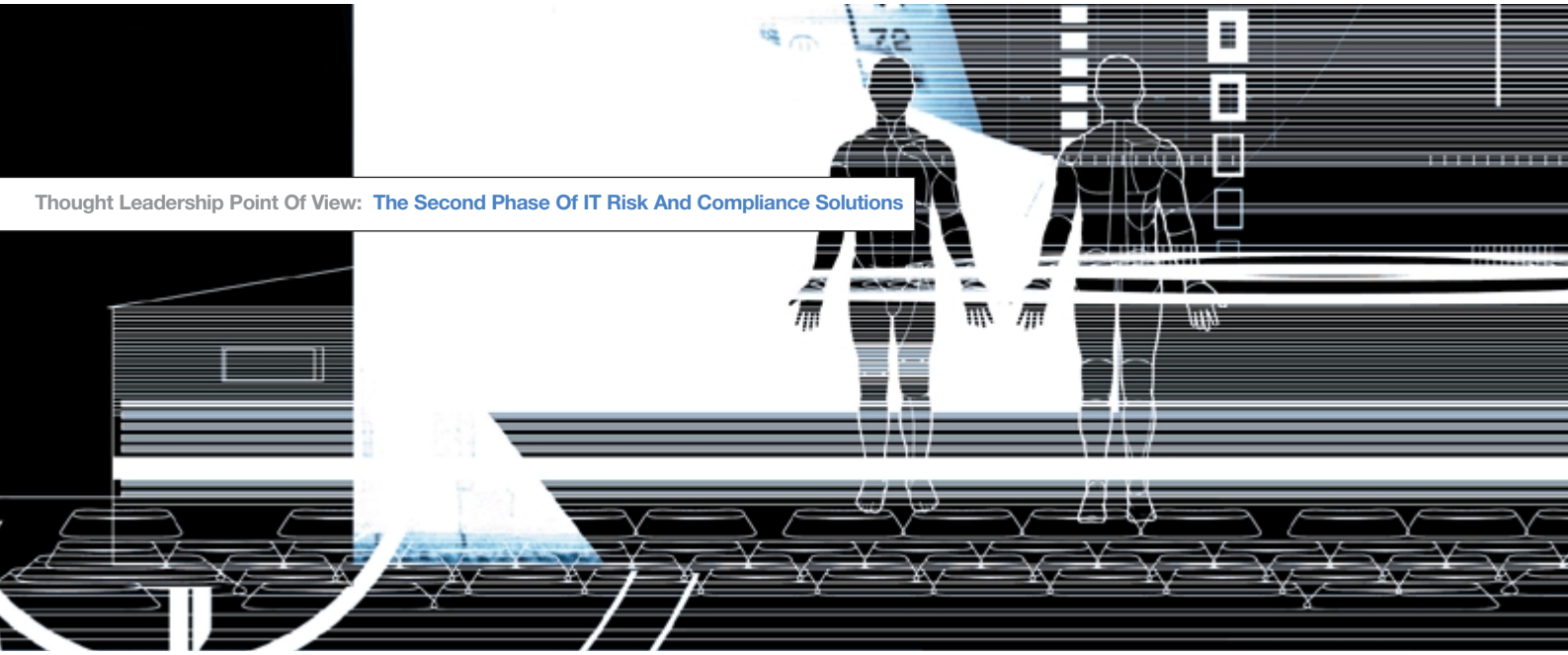


Thought Leadership Point Of View: The Second Phase Of IT Risk And Compliance Solutions

Significantly Reducing The Cost Of Maintaining Governance, Risk Management And Compliance Across The Enterprise

industry direct ltd

"...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

"BSI Management Systems main objective is to provide a single framework in Risk Management for Corporate Governance.

BSI Management Systems supports the IBM recommendation to use ISO standards as the foundation for an integrated IT governance approach in support of efficient risk management and compliance policy."

Robert Whitcher; BSI Management Systems
Global Product Manager Business Continuity, ISMS & ITSM.

BSI Management Systems

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.

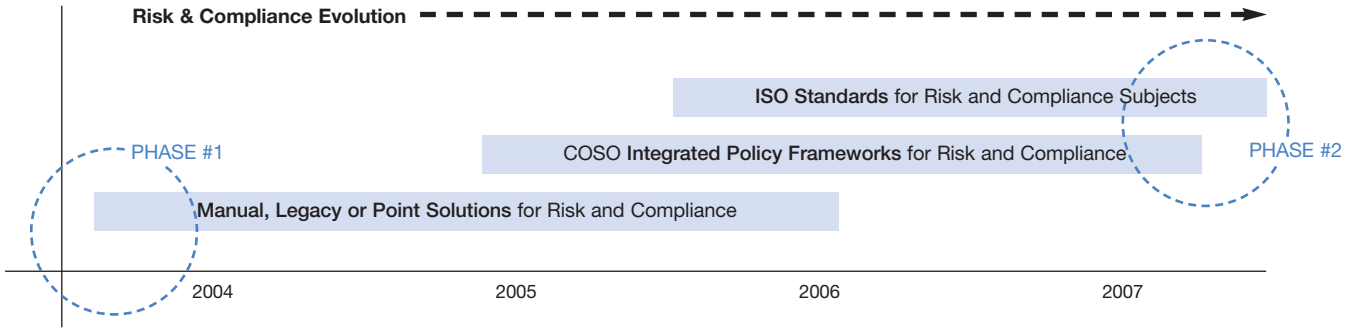


Figure One: *Risk and Compliance Phase 1 & 2. © Copyright Industry Direct Ltd.*

> *"...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"*

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.)

#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?

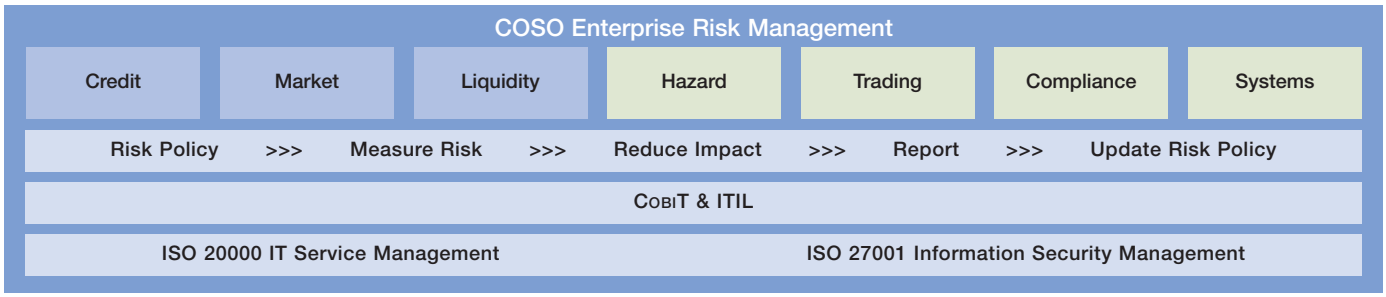


Figure Two: *Integrating Enterprise Risk Management with IT. © Copyright Industry Direct Ltd.*

#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.*

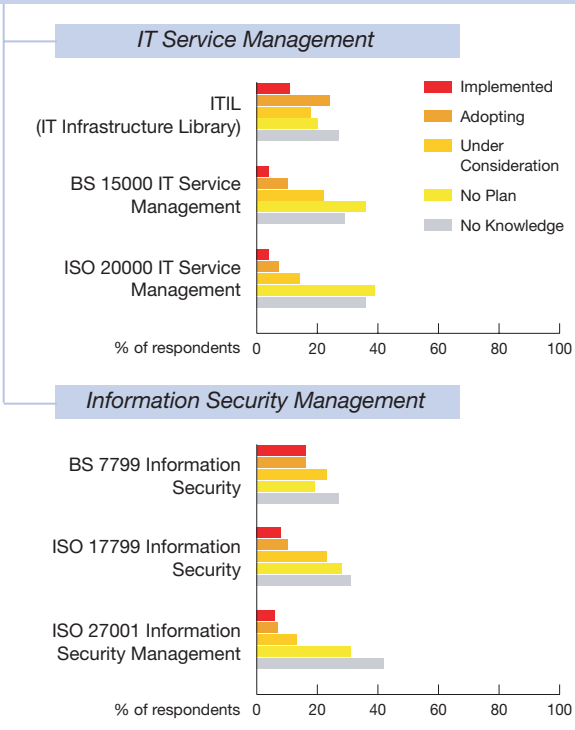
Consequently, today, many audit firms are supporting clients in the development of an integrated ERM policy. Scaling out from their original investments and creating a structured approach for more reliable IT investment and an integrated IT infrastructure is critical for the successful implementation 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.

#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.

In Q4 2006 IBM Software Group sponsored an IDL project to profile United Kingdom organisations and identify their strategic priorities for Governance, Risk and Compliance, and the software solutions they intended to implement as the basis to reduce cost and risk. Significant extracts from this study are included in this document.

What is the adoption status of these standards and frameworks in support of efficient risk management and compliance?



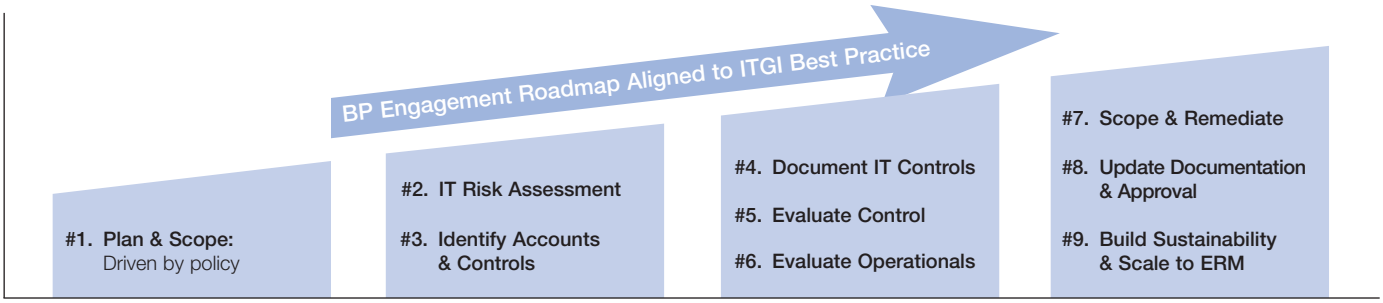


Figure Three: *BP Engagement Roadmap Aligned to ITGI Best Practice. Roadmap © Copyright ITGI.*

"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"

#4. Efficient IT Governance Through Infrastructure Integration.

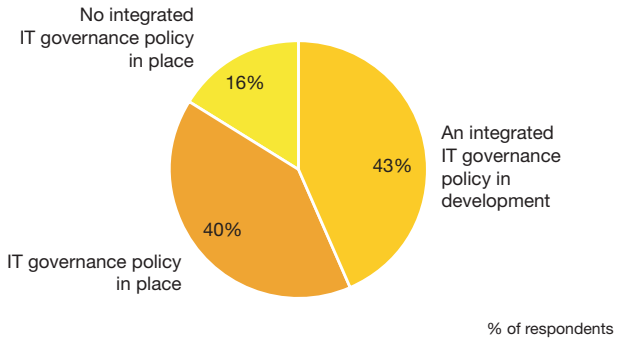
In building efficient integrated IT Governance to match the needs of Corporate Governance, consolidation is feasible and in fact desirable. Many corporations engage risk and compliance management from a tactical operations perspective by having individual responsibilities for different compliance issues – 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.

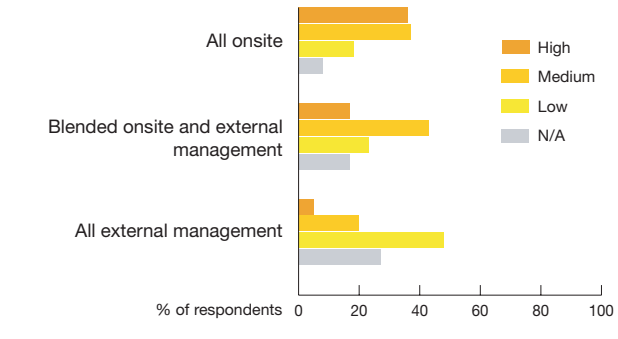
Strategically, the relationship between application controls and IT general controls is such that IT general controls are needed to support the functioning of application controls, and both are needed to ensure complete and accurate information processing. Therefore, the strategy recommended by IBM is 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.

What is the status of integrated IT governance to support risk management and compliance?

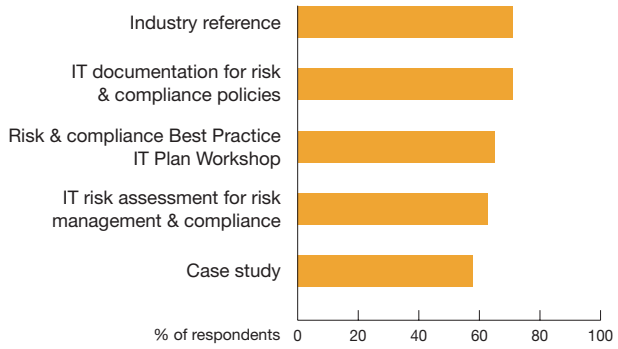


What priority is investment in these IT delivery models to support improved efficiency for risk management and compliance?

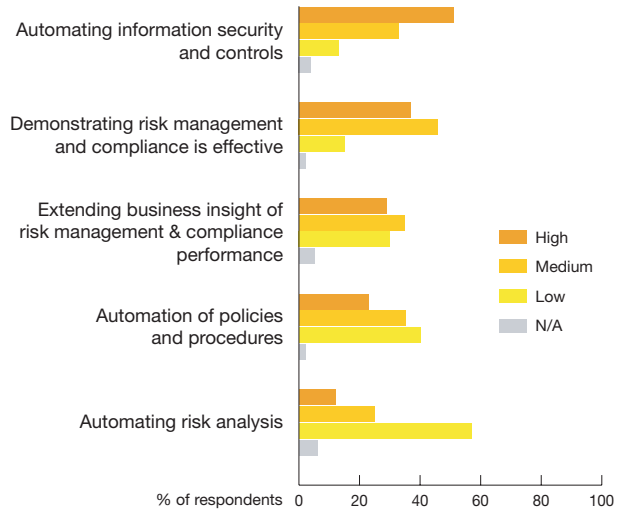


"Integration has proven benefit through lower cost and risk, in conjunction with more immediate management information synthesized throughout the enterprise."

What services are valuable to support IT risk & compliance solutions investment decisions?



What priority is investment in these IT software solutions to support improved efficiency for risk management and compliance?



#5. Risk Management And Compliance Policy Automation.

As the organisation moves to an integrated enterprise risk management policy, taking an holistic rather than only financial approach, then it makes sense to implement a similar integrated approach to IT Governance. Integration has proven benefit through lower cost and risk, in conjunction with more immediate management information synthesized throughout the enterprise.

In pursuit of integrated IT Governance, the CIO may choose to implement the emerging ISO series of standards to demonstrate best practice through independent certification that covers key aspects of integrated IT governance such as information security management (ISO 27001), IT service management based upon IT Infrastructure Library (ISO 20000). The planned risk management (ISO 27005) and business continuity (ISO 27006) standards will provide additional cover. This has significant benefit for the global organisation as an ISO foundation for IT Governance is established and ratified by applying the same international standards worldwide.

At the heart of greater efficiency and integrated IT Governance support of enterprise risk management is the middleware, and again if this can be similarly linked through compatible products, that are scalable and flexible to adapt to the different demands of risk management in life and pensions, general insurance and broker business, then the industry can identify with a common set of tools available globally.

The IBM middleware portfolio for Governance, Risk and Compliance comprises the widest range of compatible software products. IBM has arranged the products in predefined solution sets that can be implemented according to immediate priorities, and then scaled wider into the vision of integrated IT Governance.

#6. Preparatory Services.

In many cases, the sustained expansion of governance, risk management and compliance is opening new areas of the organisation to policy, and therefore to ensure low cost and low risk of IT support for policy, it is best to adopt an integrated and scalable strategy, based upon best practice frameworks and standards. The best practice Preparatory Services are designed to establish a scalable foundation and identify immediate priorities, creating the roadmap for solution implementation.

1 ***Risk & Compliance Best Practice IT Plan Workshop***

A 0.5 day best practice workshop to present the framework and standards based approach to IT support for governance, risk management and compliance policy, then decide priorities and outline a preliminary roadmap for sustained IT efficiency and low risk through integration and automation, rather than fragmented, silo or legacy systems.

2 ***IT Risk Assessment***

An on-site best practice assessment of existing IT support for governance, risk management & compliance policy, and a report on gaps to be closed, enabling an integrated low cost and low risk implementation of IT processes and controls in support of policy.

3 ***IT Documentation***

Formal documentation of IT processes and controls in support of governance, risk management and compliance policy, particularly necessary when new areas of policy are required to be integrated with existing policy and IT support.

#7. IBM Software Solution Set.

The recommendation is to address current governance, risk management and compliance policy with a strategic solution, rather than a "tactical" or "point" solution, by [i] developing a long–term strategic foundation for adherence to standards, regulations and frameworks [ii] reviewing the existing IT strategy in line with the longer–term view, to ensure new solutions are fully integrated and aligned to the strategy. Enterprise wide integrated solutions, leveraging the unique range of IBM software, bring significantly reduced cost of ownership, lower risk, higher consistency and longer term ROI, including simplified supplier management, centralised support, and asset reuseability.

1 ***Policy Definition & Documentation***

Description

The outline definition of policies with the level of analysis and discovery required to identify potential areas of risk. The solution provides a complete policy definition capability, and the detail of policy definition, which will determine the level of discovery required to extend business insight.

Integrated Solution

- Document corporate and business policies and their control points *(WebSphere Business Modeler)*.
- Develop, document and store corporate policies and other unstructured data such as company reports, auditors reports and other company documents *(DB2 Content Manager)*.
- Employees view the policies as well as providing application capabilities for employees to acknowledge understanding and adherence to those policies *(WebSphere Portal Server)*.
- A common platform for companies to easily document, evaluate and report the status of controls management across multiple initiatives in the enterprise *(IBM Workplace for Business Controls and Reporting)*.

2 ***Extending Business Insight***

Description

Extending Business Insight uses the foundation of Policy Definition & Documentation for asset discovery to identify and track all areas of IT assets and information in support of policy, and the foundation for scaling governance, risk and compliance across the enterprise.

Integrated Solution

- An enterprise-ready configuration management database and platform upon which to standardise and share information to integrate people, processes, information and technology *(Tivoli Change & Configuration Management Database)*.
- Move beyond ordinary searching with a unique ability to understand user intent and apply the context of user requests to enable the specific information to be delivered, to make purchases, answer questions, and solve problems *(WebSphere Content Discovery Server portfolio)*.
- The foundation for a strategic information integration framework that accelerate time to market for new applications, gain more value and insight from existing assets, and control IT costs *(WebSphere Information Integrator)*.
- An industry-leading platform for rapid assembly and broad deployment of integrated analytics embedded within applications *(DB2 Alphablox)*.
- A new level of accuracy, precision & fidelity to identity recognition using an integrated product portfolio *(DB2 Entity Analytics Solution – DB2 Identity Resolution, DB2 Relationship Resolution, DB2 Anonymous Resolution, and DB2 Entity Analytic Solutions Name Manager)*.

Continued...

3 *Information Security & Controls*

Description

The Security & Controls solution is based upon controls defined in two ISO standards – the ISO 27001 Information Security Management framework for the creation of an Information Security Management System [ISMS], and Information Security as part of the ISO 20000 IT Service Management Standard using ITIL, plus CoBIT framework for the implementation of an integrated systems management infrastructure.

Integrated Solution

Policy Definition

- Managed policy process, definition and life cycle management *(WebSphere Business Modeller, Integration Developer, Process Server Business Monitor)*.
- Policy creation, publication and management collaboration *(DB2 Content Manager)*.
- Distribute policy and acknowledgement of compliance *(WebSphere Portal Server)*.

Policy Execution

- Application and data access control, business continuity monitoring, and management of application infrastructure *(Tivoli Identity Manager, Federated Identity Manager, Access Manager, Risk Manager, License Manager, Compliance Manager, Storage Manager, Netview)*.
- Controlled policy based management of application development and maintenance *(Rational Software Architect, Data Architect, Test Manager, Portfolio Manager, Clear Case)*.
- Controlled data access and analysis of enterprise data for managing risk *(DB2 Entity Analytics)*.
- Supply secure application and data access for B2B, B2C and mobile applications *(DataPower Policy Execution Gateway, WebSphere Evenplace Portfolio, WebSphere Business Partner Gateway)*.

Policy Compliance

- Data collation & storage, with reporting of all security controls *(DB2 Warehouse Edition, DB2 Alphablox)*.
- Visualisation of controls and management reporting *(WebSphere Portal Server, Workplace for Business Controls & Reporting)*.

4 *Demonstrate Risk Management & Compliance*

Description

The business and operational reporting of risk management and compliance to the defined policies with incident management to ensure mitigation of risk.

Integrated Solution

- A framework for delivery of role–based information demonstrating the current status of compliance *(WebSphere Portal Server)*.
- Reusable service–oriented components, robust administration tools, and dashboard–specific features to accelerate the creation of standards–based, active dashboards *(IBM Workplace Dashboard Framework)*.
- A common platform to easily document, evaluate and report the status of controls management across multiple enterprise initiatives *(IBM Workplace for Business Controls and Reporting)*.
- Security incident management from a single web–based security console to ensure incidents are reported and managed within defined policies *(Tivoli Security Operations Manager)*.

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.

Compliance Disclaimer.

IBM's customer is responsible for ensuring its own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

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 organisations in formalisation 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.

Version 1.4 – October 2006

IDL industry direct ltd