

# Enterprise risk management: a long-term solution for compliance, governance and sustained growth in shareholder value

## Introduction

In recent years, shareholders, pension holders, investors and society at large have suffered enormous loss as a result of numerous and catastrophic corporate failures. As the means of reducing the potential for such loss, improved corporate governance has become an inescapable must for businesses around the globe. Irrefutably, effective governance is only possible through a functional system of internal control, which itself is wholly dependent on a culture of sustained and proactive enterprise risk management (ERM).

As one of the most effective means of managing compliance and avoiding the risk of non-compliance, ERM is also increasingly recognised by forward-thinking organisations as the best long-term, sustainable and cost-effective solution to meeting the compliance mandates as required by the Sarbanes-Oxley Act and the ever increasing compliance requirements companies face today.

While ERM is both the foundation of any functional system of internal control and governance, and the most cost-effective platform for continued and long-term compliance, ERM is also the most efficient, effective and proactive approach to increasing shareholder value.

Therefore, and as most analysts and leading businesses thinkers agree, an effective long-term solution for compliance, governance and sustained growth in shareholder value is to integrate a formal technology-based system of sustained, repeatable and continuously improving enterprise risk management into the heart of all business processes, practices, control and governance activities.

## Enterprise Risk Management: A fundamental component of internal control and effective corporate governance

As ‘the internal means by which corporations are operated and controlled’<sup>1</sup> and thus ‘the process by which corporations are made responsive to the rights and wishes of stakeholders’,<sup>2</sup> effective corporate governance is universally accepted as the means by which a corporation actively increases shareholder value while simultaneously reducing the likelihood of loss.

In recent years, however, there have been a ‘series of high-profile scandals and failures where investors, company personnel and other stakeholders suffered tremendous loss’<sup>3</sup>. In a move to reduce this risk, shareholders, investors, regulators, pension holders and society at large are increasingly demanding improved governance within the global corporate community.

Consequently, as the number and severity of corporate failures has increased steadily over the last decade, so too has the development of standards, guidelines and codes of conduct to assist corporations in improving their governance efforts. While these standards, guidelines and codes all differ in origin, they share one core tenet - the foundation of good governance is an effective system of internal control.

**Author: Hewitt Roberts, CEO, Entropy International**

Copyright Entropy International 2005. All rights reserved.

As the primary means of setting and monitoring performance in relation to corporate objectives and the control mechanisms that enable the identification and management of risks in relation to meeting those objectives, an effective system of internal control is the essential ingredient of effective corporate governance.

Although there are a myriad of internal control guidelines and frameworks one can work to, in recent years two complementary frameworks for internal control have emerged as the de facto standards by which companies should be regulated and measured and thus increasingly look to when adopting a framework for internal control best practice. These frameworks are commonly referred to as the Turnbull framework and the COSO framework.

*Risk and control are virtually inseparable – like two sides of a coin – meaning that risks first must be identified and assessed; then managed and mitigated by the implementation of a strong system of internal control.*

The Turnbull framework is based on the 1999 publication Internal Control: Guidance for Directors on the Combined Code. This framework, the work of Nigel Turnbull and the Institute of Chartered Accountants in England and Wales (ICAEW), is itself the latest in a series of mutually reinforcing and continuously improving governance guidelines developed in the United Kingdom. The roots of the Turnbull framework lie in the work of Sir Adrian Cadbury (The Cadbury Report - 1992) and build upon subsequent UK contributions including: The Rutterman Report – 1994; The Greenbury Proposals; and Hampel's Combined Code – 1998.

The COSO framework is based on the 2004 publication Enterprise Risk Management: Integrated Framework. This was published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and although American in origin, it has a similar heritage to the Turnbull framework in that it builds upon earlier efforts to provide guidance for improved governance. The 2004 COSO framework complements and improves on the 1987 publication of the Treadway Commission – Internal Control – Integrated Framework.

By looking at each of these frameworks more closely, it is clear that in both cases the heart of an effective system of governance and internal control is proactive, effective and sustained enterprise-wide risk management (ERM). According to the Institute of International Auditors, 'risk and control are virtually inseparable – like two sides of a coin – meaning that risks first must be identified and assessed; then managed and mitigated by the implementation of a strong system of internal control'<sup>4</sup>.

## **ERM and the Turnbull framework**

The Turnbull Report (Internal Control: Guidance for Directors on the Combined Code) stipulates that internal control is a system that includes 'control activities; information and communication processes; and processes for monitoring the continued effectiveness of the system of internal control'<sup>1</sup>.

Turnbull and the ICAEW view internal control as the system that 'encompasses the policies, processes, tasks and behaviours that taken together facilitate its effective and efficient operation by enabling [a company] to respond appropriately to significant business, operational, financial, compliance and other risks to achieving its business objectives'<sup>1</sup>.



Diagram 1: The Turnbull Framework<sup>5</sup>

From this perspective, and as shown in diagram 1, the Turnbull framework can be seen as three interconnected and mutually reinforcing functions, the heart of which is risk management. If functioning properly the framework will serve to reduce risk, stimulate corporate performance, improve leadership within an organisation, demonstrate accountability and transparency, improve overall corporate responsibility, improve access to capital markets and maximise shareholder value.

This inner risk management core provides the means for:

#### **Risk identification:**

Identifying risks that could affect the corporation and thus an early warning system for uncertainties that could compromise performance and profitability objectives.

#### **Risk assessment:**

Assessing the likelihood and severity of an identified risk and thus its relative significance to the business.

#### **Risk response:**

Responding appropriately to all identified risks and determining whether to avoid, accept, reduce or share an identified risk. These response decisions are made with reference to corporate strategy and objectives and the risk management philosophy and risk appetite of the corporation.

Internal control, as depicted by the second and middle ring in diagram 1, relies wholly on the inner risk management system and becomes the foundation for the outer and penultimate function of overall governance.

With effective and sustained enterprise risk management firmly in place, the framework is then capable of delivering effective internal control. Internal control comprises four essential and component parts. These are - the behaviour of the organisation, the overall control environment of the corporation, monitoring activities, and the information and communication processes.

**Organisational behaviour:**

The first component, organisational behaviour, is affected by the environment in which an organisation operates and determines the ethics, values, integrity and competence of the people within the framework. Organisational behaviour will affect and be affected by:

- o the tone of governance and control in the corporation;
- o corporate strategy and the performance and profitability objectives set; and
- o the risk management philosophy, risk appetite and risk tolerance of the corporation.

**Control environment:**

The second component of internal control is the overall control environment within a business. This typically includes:

- o the activities that ensure performance objectives are met and that risk responses are effective; and
- o measures such as policies, procedures, training, responsibilities, authorities and approvals.

**Monitoring:**

The third component, monitoring activities, provides the means for on-going monitoring of corporate performance and the internal control function. Monitoring activities would typically include:

- o the processes for monitoring corporate performance and the continued effectiveness of the system of internal control; and
- o auditing and assessments to identify and rectify deficiencies in the system of internal control.

**Information & Communication:**

The fourth and final component of the internal control function is the information and communication processes within the control system. Information and communication would define:

- o the manner in which the organisation collects and communicates information to facilitate governance and control; and
- o the means by which pertinent information flows in a timely fashion within the governance framework to ensure corporate strategy and performance objectives are met.

With functional and mutually supporting risk management and internal control systems in place, the framework can then meet the overall requirements of an effective system of corporate governance. These requirements, as represented by the outer ring in diagram 1 are to:

**Protect shareholder rights:**

- o recognising the rights of all shareholders as protected by law;
- o providing access to timely and relevant information;
- o ensuring the equitable treatment of all shareholders;
- o the preservation of voting rights and meaningful participation in AGMs;
- o election of the board;
- o transferring and conveying shares;
- o participating in decisions regarding fundamental corporate changes; and
- o participating in the profit of the corporation.

**Preserve stakeholder rights:**

- o ensuring corporate responsibility and maintaining a licence to operate;
- o recognising the rights of stakeholders as established by law (e.g. health & safety, environmental stewardship, disclosure); and
- o encouraging active cooperation between stakeholders in creating wealth, jobs and sustainable and financially sound corporations.

### Uphold the responsibilities of the board:

- o ensuring strategic guidance of the company;
- o being accountable to shareholders;
- o effectively monitoring management;
- o acting in good faith, on a fully informed basis and with due diligence and care;
- o acting in the best interest of the company;
- o meeting their financial and fiduciary responsibilities;
- o ensuring ongoing compliance with applicable laws and regulations;
- o setting strategy and performance objectives and effectively and efficiently allocating resources to meet the objectives set; and
- o monitoring performance in relation to strategy and objectives and deploying resources in response to deviations from objectives set.

Enable reporting, disclosure and accountability to provide:

- o accurate and timely disclosure to all stakeholders (particularly shareholders) of all significant matters regarding the organisation, its performance, financial situation, ownership and governance; and
- o transparency and reporting of all material financial and non-financial risks to the corporate objectives set.

Clearly, the Turnbull framework acknowledges that ‘the management of risks significant to the fulfilment of business objectives plays a key role in the company’s system of internal control and corporate governance’<sup>1</sup> and that ‘a sound system of internal control depends on a thorough and regular evaluation of the nature and extent of the risks to which the company is exposed’<sup>1</sup>.

*The management of risks significant to the fulfilment of business objectives plays a key role in the company’s system of internal control and corporate governance.*

As is obvious therefore, a corporate governance framework fashioned in accordance with the Turnbull approach is centred on risk management and is only effective when enterprise risk management is at the heart of a corporation’s governance efforts.

### ERM and the COSO framework

Like the Turnbull framework for internal control and corporate governance, the 1992 COSO Internal Control – Integrated Framework was ‘designed to help businesses and other entities assess and enhance their internal control systems’<sup>3</sup> and also has at its core enterprise risk management.

This framework has since been incorporated into policy, rule and regulation and is used by thousands of enterprises to better control their activities in moving toward achievement of their objectives<sup>3</sup>. Furthermore, the COSO framework is recognised by the US Securities and Exchange Commission (SEC) through the Public Companies Audit and Oversight Board (PCAOB) as an approved control model for Sarbanes-Oxley compliance and other listing requirements<sup>6</sup>.

Given the alarming number and impact of governance failures over the last decade however, ‘recent years have seen heightened concern and focus on risk management’ and as such in 2001 COSO initiated a project to improve on the 1992 framework and provide key principles and concepts, a common language and guidance to enable organisations to evaluate and improve their organisations’ enterprise risk management<sup>3</sup>.

The conclusion of this project was the 2004 publication of Enterprise Risk Management – Integrated Framework which incorporates the Internal Control – Integrated Framework within it and provides a ‘more robust and extensive focus’ on enterprise risk management.

Consequently, the 2004 COSO framework, like the 1992 framework before it, is expected to become widely accepted by companies, other organisations, stakeholders and all interested parties as the standard for satisfying regulated and legislated internal control, risk management and reporting requirements<sup>3</sup>.

Looking more closely at the COSO framework and the familiar ‘COSO cube’, as depicted in diagram 2, the components of a functional system of governance, internal control and risk management are<sup>3</sup>:

**Internal environment:**

- o the tone of the organisation;
- o the basis for determining how risk is viewed and addressed by an organisation;
- o integrity, ethical values, competence, authority, responsibility; and
- o the environment in which an organisation operates, which influences and is influenced by corporate strategy and mission, risk management philosophy and risk appetite and tolerance.

**Objective setting:**

- o the setting of corporate objectives in line with strategy/mission and risk appetite; and
- o the identification of potential events (uncertainties – risk and opportunities) that could compromise meeting those objectives.

**Event identification:**

- o identification of uncertainties (events) in the form of risks and/opportunities.

**Risk assessment:**

- o assessment of risks (typically likelihood and impact) to business objectives.

**Risk response:**

- o the decision to avoid, reduce, share or accept an identified risk.

**Control activities:**

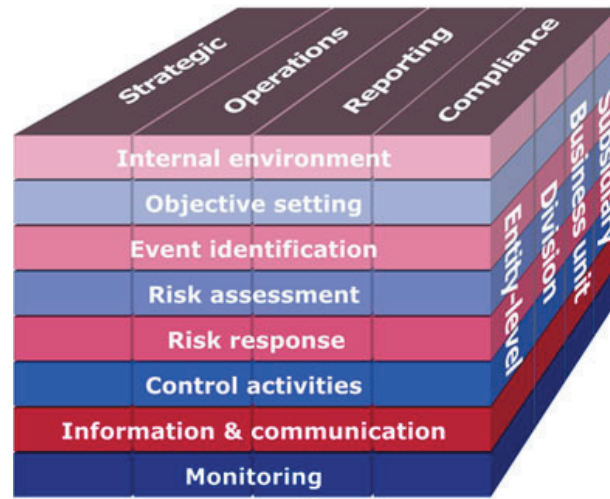
- o policies and procedures established to ensure risk responses are carried out; and
- o a range of activities that includes approvals, verifications, authorisations and recommendations.

**Information & communication:**

- o pertinent information identified, captured and communicated in a timely fashion;
- o access to internal and external information; and
- o the flow of information that allows for successful control actions from instruction on responsibilities to summary finding on management activities.

**Monitoring:**

- o the assessment of a system’s performance over time;
- o combination of ongoing and separate evaluations; and
- o management and supervisory activities.



**Diagram 2: The 'COSO Cube'**

As shown in diagram 2, the COSO framework can be seen as a cube. One side represents internal control components, the second side represents control objectives (strategic, operations, reporting, compliance) and a third side represents the organisational scope (entity, division, business unit, subsidiary) of the control system.

From this diagram and definition it is clear that the very foundation of the COSO framework lies in enterprise risk management and in the fact that 'all entities face uncertainty' presented in the form of risk and opportunity each 'with the potential to erode or enhance shareholder value' and that 'enterprise risk management enables an organisation to effectively deal with uncertainty and associated risk and enhances the capacity to build value'<sup>3</sup>.

*Enterprise risk management enables an organisation to effectively deal with uncertainty and associated risk and enhances the capacity to build value.*

## **ERM: At the heart of Turnbull and COSO frameworks for internal control**

As rapidly emerging 'standards' for corporate governance, and although different in origin and design, both the Turnbull and COSO frameworks have one very significant attribute in common – a core based on effective, enterprise-wide and sustained risk management.

As such, it stands to reason that if corporations exist as vehicles to meet the expectations and objectives of their shareholders and stakeholders, and if corporate governance is the process by which corporations are made responsive to rights and wishes of stakeholders, then enterprise risk management – as the fundamental core of control and governance - must itself be an essential ingredient of any sustainable and defensible corporate strategy aimed at increasing shareholder value through improved governance.

## **ERM: a long-term approach to Sarbanes-Oxley compliance**

Beyond the fact that ERM is a core component of internal control and thus fundamental to good governance, ERM is also increasingly recognised by forward-thinking organisations as a long-term, sustainable and cost effective solution to meeting the compliance mandates as required by Sarbanes-Oxley and the ever-increasing compliance requirements that companies face today.

## **Sarbanes-Oxley – the tip of the compliance iceberg**

Most executives in business today, and certainly any who work within publicly listed businesses, are only too familiar with the Sarbanes-Oxley Act of 2002.

Widely seen as the most significant piece of corporate legislation affecting public companies since the US Securities Act of 1934, the Sarbanes-Oxley Act (SOA) was the United States' response to the recent and

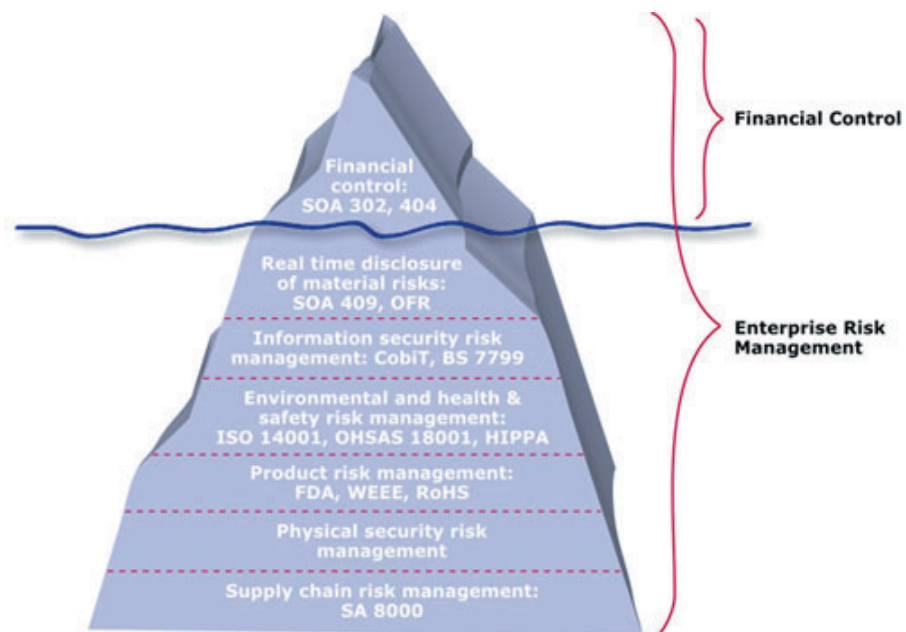
spectacular demise of Enron and the subsequent and enormous financial loss to shareholders, pension holders and public investment funds (see also the white paper Risk and Performance Management: Essential Components of Effective Corporate Governance at [www.entropyinternational.com](http://www.entropyinternational.com)).

The SOA was enacted to restore investor, shareholder and public trust and confidence in the corporate community by legislatively attempting to reduce fraud, conflict of interest and financial misrepresentation. This act, intended to improve financial control, reporting and transparency, is effectively legislation aimed at improving corporate governance and responsibility in listed (SEC regulated) businesses and has had an immense and irreversible impact on businesses around the globe.

With initial SOA compliance deadlines in 2004/2005 and penalties of up to a \$5M fine and 20 years imprisonment for the executives of organisations failing to comply with the Act, the reaction to and commensurate investment in compliance activity for Sarbanes-Oxley has been unprecedented. Understandably, as the first 2004/2005 compliance deadlines are limited to Sections 302 and 404 of the Act, virtually all of this expenditure, noise and compliance activity has been centred on these sections.

However, Sections 302 and 404 (financial control and reporting) are only the first in a series of other Sarbanes-Oxley compliance requirements and in time, regulated companies will be forced to comply with further sections of the Act and as most analysts and spectators agree, the most significant yet impending compliance burden will be Section 409 which calls for the real-time disclosures of material risks to performance.

Consequently, 'most companies that have taken steps to comply with the Sarbanes-Oxley Act have focused their energies on Section 404 ... but most managers have yet to tackle the potentially more onerous requirement – Section 409<sup>7</sup>. Given that Section 409 will require real-time reporting of all material financial and non-financial risks to a business, and as noted recently by John Hagerty of AMR Research in Boston, it is therefore Section 409 that 'will cause the most heartburn' of all the Sarbanes-Oxley mandates<sup>7</sup>.



**Diagram 3: The Compliance Iceberg**

As a consequence, and as shown in diagram 3, compliance with the financial control and reporting aspects of Sarbanes-Oxley is widely recognised as 'the tip of the compliance iceberg' and 'only one of a myriad of compliance requirements that companies are facing around the globe<sup>8</sup>'. In fact, it is estimated that 'between 2005 and 2009, companies will spend more than \$80billion on compliance-related work<sup>9</sup>'.

*Enterprise risk management is increasingly recognised by forward-thinking organisations as a long-term, sustainable and cost effective solution to meeting the compliance mandates as required by Sarbanes-Oxley and the ever-increasing compliance requirements which companies face today.*

Whether it is legislated or tacit, required by the SEC, the FDA, OSHA or the EPA, compliance requirements are increasing exponentially and like it or not we are now living in ‘the age of compliance’<sup>8</sup> (see Table 1 for an overview of the more significant compliance requirements ‘below the tip’ of the compliance iceberg).

As a result, and as active compliance is in itself an exercise in avoiding risk, ‘forward-thinking companies, having learned from their history of regulatory compliance, are putting a broad set of [risk and compliance] mandates in perspective, connecting the dots between overall compliance requirements’ and ‘looking to develop a comprehensive, phased approach to compliance and risk management beyond initial and individual compliance requirements’<sup>9</sup>.

**Table 1: Compliance requirements ‘below’ the surface**

Risk Management Discipline	Regulation/Standard/Code of Conduct	Compliance requirement	Jurisdiction
Enterprise-wide risk management	Sarbanes-Oxley Section 409	Real-time issuer disclosures on a rapid and current basis of material changes in financial and non-financial risks to the financial position of a business <sup>10</sup> .	USA (Securities and Exchange Commission regulated businesses)
Enterprise-wide risk management	Operating and Financial Review Report	As of April 2005, requires directors to report on current and future business developments and performance, particularly a description of the principal risks and uncertainties facing the business <sup>11</sup> .	UK listed businesses
Information security	BS EN/ISO 17799 & CobiT	Information security and control.	International
Information security	Financial Modernization Act of 1999 <sup>12</sup>	Also known as the “Gramm-Leach-Bliley Act” or GLB Act, includes provisions to protect consumers’ personal financial information.	USA
Information security	Data Protection Act <sup>13</sup>	Regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.	UK
Information security	Health Insurance Portability and Accountability Act of 1996 <sup>14</sup>	Also known as HIPPA, regulation to protect the privacy of personal health information.	USA
Environmental risk management	ISO 14001	Corporate environmental management.	International
Health & safety risk management	OHSAS 18001	Corporate occupational health and safety management.	International
Product risk management	The Waste Electrical and Electronic Equipment Regulation 2002 <sup>15</sup>	Also known as WEEE and the Product Responsibility Regulations. Aimed at reducing WEEE and encouraging reuse, recycling and recovery of electronic equipment.	European Union
Product risk management	The Restriction of Hazardous Substances in Electrical and Electronic Equipment Directive (2002) <sup>16</sup>	Also known as the RoHS Directive and aimed at protecting human health and the environment by restricting the use of certain hazardous substances in new electrical and electronic equipment.	European Union

## ERM – a comprehensive, long-term and cost-effective approach to compliance

If one accepts that compliance is a fact of doing business and that compliance requirements themselves will only increase and become more onerous in time, businesses today are faced with two clear options:

Option 1: manage compliance requirements independently and reactively as they appear on your radar screen (or in some cases windscreen); or

Option 2: ‘connect the dots’, move compliance from ‘project to process’<sup>17</sup> and use initial risk and compliance activity as a catalyst to develop a long-term, sustainable and repeatable enterprise risk management system for ongoing compliance.

Clearly, option 1 is easier and thus a more common approach and many companies facing Sarbanes-Oxley 404 compliance requirements, for example, have implemented knee-jerk and makeshift solutions to help with initial compliance projects.

However, living in the ‘age of compliance’ is now compelling boards of directors and senior management to think as strategically about risk and compliance issues as they do about revenue growth, product and service offerings, operational efficiency and cost containment<sup>18</sup>.

As a result, leaders of forward-leading companies recognize that, despite the challenges and complexity of the new regulations, by taking a proactive approach they not only can avoid a host of problems but can also position their organizations more strongly for the future<sup>18</sup>.

Consequently, whether it is Sarbanes-Oxley or ISO 14001, making the process of enterprise risk management a built-in rather than bolted-on foundation for compliance ensures that compliance programmes will be continuous, repeatable and future-proofed to meet the compliance requirements of tomorrow while providing a multi-disciplinary, enterprise-wide and cost-effective risk and compliance management framework for today.

### **Enterprise Risk Management: The most efficient, effective and proactive approach to increasing shareholder value**

As identified above, ERM is both the foundation of any functional system of internal control and governance and the most cost-effective platform for continued and long-term compliance within a business. However, the most compelling reason for implementing an enterprise risk management system is that it is undeniably the most efficient, effective and proactive approach to increasing shareholder value.

*The most compelling reason for implementing an enterprise risk management system is that it is undeniably the most efficient, effective and proactive approach to increasing shareholder value.*

Arguably, the underlying premise of every business entity is to provide value for its stakeholders. Value is created through the process of calculated decision-making about risk and reward. Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks<sup>3</sup>.

Clearly, risk and reward are the very essence of business, and effective risk management is therefore the primary vehicle to deliver maximum shareholder value while simultaneously reducing the potential for share value loss.

This premise is based on the fact that an enterprise risk management system:

- increases the ability of an organisation to identify uncertainty (risk and opportunity) and provides visibility on all risks facing all business units, departments and divisions of an organisation;
- provides a complete picture of the risks in an organisation’s landscape, which enables an organisation to effectively and expeditiously select risk responses (avoid, reduce, share or accept) that best fit its strategic objectives and risk appetite;
- provides significant competitive advantage as it enables an organisation to both respond to risks as fast as practically possible and to seize opportunities as they present themselves;
- can provide an ‘early warning and response’ system for risks, which decreases operational surprises and losses, and increases the capacity of executives to forecast potential events that erode shareholder value;
- improves the effectiveness of resource allocation and capital deployment. By providing visibility of all risks that face an entity and as the significance of risks across the business can be assessed

*Risk and reward are the very essence of business and effective risk management is the primary vehicle to deliver maximum shareholder value while simultaneously reducing the potential for share value loss.*

consistently, ERM ensures that risks can be compared based on their relative significance and impact. This means a business can allocate resource to the most significant risks first and similarly capitalise first on the most significant opportunities; and

- increases the ability of a business to make a comprehensive response to interrelated risks. This provides a greater chance of multiplying the effectiveness of risk responses while simultaneously reducing the cost of and potential for counter-productive risk responses.

## Using technology to improve the efficiency and cost-effectiveness of ERM

If one accepts that enterprise risk management is the core of effective governance and compliance and the key to sustained growth in shareholder value, it stands to reason that in our never-ending pursuit of cost reduction and increased efficiency; improving the efficiency, repeatability and cost-effectiveness of risk management activities is and will forever be essential.

To that end, and as most analysts and experienced practitioners admit, the best solutions for long-term, cost effective and repeatable risk management involve the use of information technology, highlighting that ‘software tools can help businesses steer through the minefield of meeting compliance regulations and offer real cost savings’<sup>19</sup>.

In addition to the benefits attributable to an effective enterprise risk management system, IT-based ERM solutions add value in the following key areas. ERM software solutions:

- increase the possibilities for system automation and streamlining, thus reducing the cost and burden of on-going risk management while continuously increasing the efficiency of the risk management process. Immediate considerations for automation and cost reduction are document management and control, corrective and preventative action management, and risk assessment and control management;
- provide Corporate Risk Officers (CROs) with tools to quickly gather and report enterprise-wide risk information. This reduces lag times in risk identification and response, thus improving the overall effectiveness of risk avoidance and increasing the return from capitalising on opportunities immediately they present themselves;
- provide instant ‘dashboard’ and ‘drill through/drill down’ visibility of crucial risk information across the entire organisation. This means there is a single source of ‘the truth’ with which all risk professionals need to operate and it ensures that risk information is transparent, auditable and actionable from anywhere in your organisation;
- ensure consistency, repeatability and comparability across your organisation. Whether it is being able to provide standard risk assessment methodologies and control protocols or being confident that significant risks are being compared on a consistent basis, software-based ERM solutions provide consistency, repeatability and comparability across a business unit, a division or an entire organisation;
- provide a scalable solution whose implementation and expansion can be phased over time commensurate with an organisation’s capability. This means that a solution will be extensible and future-proofed, enabling an organisation to manage new risk areas as they emerge in the constantly changing business environment;
- increase the potential for present and future systems integration with other applications such as ERP as the need increases for a business’ IT systems to communicate with each other; and
- enable on-going knowledge retention and sharing. This steadily increases the capability for and value of knowledge-sharing throughout the organisation and ensures your system and ERM process are continuously improving while retaining the experiences, lessons and expertise of all previous risk management efforts in your organisation.

*Analysts and experience practitioners admit, the best solutions for long-term, cost effective and repeatable risk management involve the use of information technology.*

## Conclusion

In recent years, shareholders, pension holders, investors and society at large have suffered enormous loss as a result of numerous and catastrophic corporate failures. As the means of reducing the potential for such loss, improved corporate governance has become an inescapable must for businesses around the globe. Irrefutably, effective governance is only possible through a functional system of internal control which itself is wholly dependent on a culture of sustained and proactive enterprise risk management (ERM).

As one of the most effective means of managing compliance and avoiding the risk of non-compliance, ERM is also increasingly recognised by forward-thinking organisations as the best long-term, sustainable and cost-effective solution to meeting the compliance mandates as required by the Sarbanes-Oxley Act and the ever increasing compliance requirements companies face today.

While ERM is both the foundation of any functional system of internal control and governance, and the most cost-effective platform for continued and long-term compliance, ERM is also the most efficient, effective and proactive approach to increasing shareholder value.

Therefore, and as most analysts and leading businesses thinkers agree, the most effective long-term solution for compliance, governance and sustained growth in shareholder value is to integrate a formal technology-based system of sustained, repeatable and continuously improving enterprise risk management into the heart of all business processes, practices, control and governance activities.

## Endnotes

<sup>1</sup>The Institute of Chartered Accountants of England and Wales (1999). Internal Control: Guidance for Directors on the Combined Code. [www.icaew.co.uk](http://www.icaew.co.uk).

<sup>2</sup>Demb, A., Neubauer, F. (1992). *The Corporate Board: Confronting the Paradoxes*, Oxford University Press, Oxford, p. 187, cited in Cadbury, A. (2002). *Corporate Governance and Chairmanship: A Personal View*, Oxford University Press, Oxford.

<sup>3</sup>COSO - The Committee of Sponsoring Organizations of the Treadway Commission, (2004). *Enterprise Risk Management – Integrated Framework: Executive Summary*, COSO.

<sup>4</sup>The Institute of Internal Auditors (2003). *Tone at the Top: Managing Risk from the Mailroom to the Boardroom*. [www.theiia.org](http://www.theiia.org).

<sup>5</sup>© Entropy International.

<sup>6</sup>Dionysia, A et al (2005). *SOXA: The why's, when's and how's*, Brunel University PG Info Systems Computing & Mathematics Department.

<sup>7</sup>Hoffman, T. (2003). *Rapid-reporting mandate adds to compliance woes*, Computerworld, July 14, 2003. [www.computerworld.com](http://www.computerworld.com).

<sup>8</sup>Hagerty, J and Scott, F. (2005). *Spending in the Age of Compliance*, AMR Research, [www.amrresearch.com](http://www.amrresearch.com).

<sup>9</sup>Hagerty, John and Scott, Fennella. (2005). *Regulatory Compliance: An \$80B Opportunity*, AMR Research. [www.amrresearch.com](http://www.amrresearch.com).

<sup>10</sup>107<sup>th</sup> Congress of the United States of America (2002). *An Act To Protect Investors by Improving the Accuracy and Reliability of Corporate Disclosures made Pursuant to the Securities Laws, and for Other Purposes (The Sarbanes-Oxley Act)*, [www.findlaw.com](http://www.findlaw.com).

<sup>11</sup>[www.kpmg.co.uk/services/ras/mas/ofr/index.cfm](http://www.kpmg.co.uk/services/ras/mas/ofr/index.cfm).

<sup>12</sup>[www.ftc.gov/privacy/glbact/](http://www.ftc.gov/privacy/glbact/).

<sup>13</sup>[www.hmsa.gov.uk/acts/acts1998/80029--a.htm#1](http://www.hmsa.gov.uk/acts/acts1998/80029--a.htm#1).

<sup>14</sup>[www.hhs.gov/ocr/hipaa/](http://www.hhs.gov/ocr/hipaa/).

<sup>15</sup>[www.dti.gov.uk/sustainability/weee](http://www.dti.gov.uk/sustainability/weee).

<sup>16</sup>[www.environment-agency.gov.uk](http://www.environment-agency.gov.uk).

<sup>17</sup>Church, T. (2004). *Taking the Long View on Sarbanes-Oxley*. Deloitte. [www.deloitte.com](http://www.deloitte.com).

<sup>18</sup>BearingPoint (2004). *Taking Sarbanes-Oxley Beyond Compliance*. [www.bearingpoint.com](http://www.bearingpoint.com).

<sup>19</sup>Goodwin, B. (2005). *Software Can Ease the Pain and Cut the Cost of Compliance*. Computer Weekly, 15 March, 2005. [www.computerweekly.com](http://www.computerweekly.com).

# software for sustainability



1 Waterview • White Cross  
Lancaster • LA1 4XS • UK

T: +44 (0)1524 389 385

F: +44 (0)1524 389 386

[info@entropy-international.com](mailto:info@entropy-international.com)

[www.entropy-international.com](http://www.entropy-international.com)