Affordable Integrated Governance, Risk and Compliance: Wishful Thinking or Reality?
Alf Esteban
Head of Consulting and Client Services – Asia Pacific

Introduction
The rapidly changing regulatory environment across all industry sectors requires managers and their boards to be more anticipatory to the challenges of strong governance, effective enterprise-wide risk management and the implementation of an efficient and effective compliance regime. Many organisations have sought to create an integrated governance, risk and compliance (GRC) oversight function, but have generally failed in achieving the desired goal. This white paper discusses the issues being faced and provides an approach which can turn the dream of an integrated GRC into an affordable reality.

Regulatory Overload
The conflicting demands of societal needs versus individual freedoms, economic rationalism versus market control, globalisation versus localisation, and unabashed political expediency has resulted in a pendulum swing between regulation, deregulation and re-regulation. Recent global events have seen the pendulum swing further towards regulation, and it is unlikely that the pendulum will swing back in the short to medium term – with indicators showing no deceleration in the rate of new regulations.

The proliferation of rules, regulations, codes of conduct, governance principles, and the need (perceived or actual) to adhere to standards, coupled with an increased focus on risk management has resulted in an explosion in the number of obligations and related controls that organisations, business units and individuals must comply with. This proliferation has resulted in compliance inefficiencies, inaccuracies, and, in many cases, duplicate efforts. Businesses are being stretched and the effort to comply is taking its toll.

The regulatory overload has an impact on the culture of compliance, with anecdotal evidence suggesting that increasing the number of controls has a direct correlation to an attitude of compliance as pure bureaucratic overhead with no benefit to the business. No matter how much expense is applied to increasing the efficiency of compliance processes, effectiveness of the controls diminishes.

Ultimately, regulatory overload increases the risk of non-compliance and leads to a failure of governance systems as a ‘tick the box to comply’ mentality subsumes the desired culture of good governance, risk management and compliance.

Connecting and integrating GRC has become a key issue in many boards and executive ranks looking to reduce the regulatory compliance burden and to establish an efficient integrated approach to managing risks, adhering to compliance obligations, and creating value.
Existing Approaches – Wishful Thinking
A study conducted by AMR Research\(^1\) indicates that the estimated spend on GRC by organisations globally in 2007 was planned to be approximately $30B, an increase of 8.5% from 2006 actuals, with approximately 20% being spent on compliance with the Sarbanes-Oxley (SOX) legislation.

The existing approaches to GRC are inherently flawed in that they typically result in a growing disconnect between governance systems, risk management frameworks, and compliance activities – which are frequently undertaken by different business units using different systems, processes and data. This silo approach cannot cost effectively be sustained.

As a result there is a lack of integration across the business with, at best, multiple independent GRC oversight functions and committees each focused on a specific GRC challenge. More likely, management and staff are being diverted from their core mission of revenue generation as they carry out disparate compliance tasks, and management and board are presented with late, incomplete and often inaccurate reports on the firm’s compliance status.

The key point of failure with existing GRC implementations is that firms often fail to integrate their efforts into a sustainable program of action that will address the issues identified. Coupled with this, many firms have also failed to implement a computerised enterprise wide compliance and risk management database and control management system, relying instead on antiquated paper based or simple spreadsheet based tools that make it difficult and unwieldy to effectively manage and monitor control obligations associated with regulations and individual risks and/or demonstrate robust audit trails for actions and tasks. Compliance departments, when they exist, are failing in their duties with required information being held in multiple systems, filing cabinets, and often in the heads of the compliance officer or business unit managers.

Common sense and a practical approach to the development of an integrated GRC are essential for seizing business opportunities while remaining adaptable to addressing new risks and compliance obligations.

Integrated GRC – Turning Vision into Reality
The AMR Research on GRC, cited previously, shows that budgeted increases for GRC spending in 2008 reflect a realisation that GRC is not a passing fad but a systemic change in how companies manage, monitor, and control business activities. While in 2007 SOX compliance accounted for 20% of the total GRC spend, the remaining 80% was spent on other important programs: information security and data privacy, ethics, business resilience and sustainability, fraud minimisation, and operational risk management in general (estimated at growing by over 5% in 2008).

In most cases, these other programs have real potential to preserve and create shareholder value for organisations – a highly desirable objective.

To ensure that this increased spending is both efficiently and effectively used, a new approach to the development on an integrated GRC needs to occur.

\(^1\) AMR Research Inc, Enterprise Strategies Service, 22 February, 2007
Moving from current silo based GRC, or even where a GRC framework is non-existent, requires a multi-phased approach, with the first phase determining the current situation and identifying opportunities for integration across people, processes, systems and data. Not surprisingly, these are the same elements that need to be assessed in developing a robust operational risk management framework.

The purpose of integration is to combine processes and information while preserving variations in how principles are applied when it makes sense to do so. Integration should occur at sensible points designed to move the organisation towards an integrated GRC framework that allows for a balance between growth, risk and return.

Subsequent phases are determined by the level of existing integration, but need to revolve around a principles-based GRC framework that clearly defines responsibility, authority and accountability across the organisation.

For compliance departments, the first step in this multi-phased approach is usually the establishment of an enterprise-wide management dashboard on compliance activity that supports better business decisions while directing risk mitigation. Often this will require working with the risk management department (where one exists) in developing a methodology for establishing and setting risk appetite. Secondly, the dashboard must be kept up to date and present the risks derived systematically from compliance work in real time, not haphazardly as a monthly exercise.

The compliance department must allow compliance work to be redirected to risk mitigation rather than ‘tick-in-the-box’. To do this, the different processes and data that represent compliance work must be mapped and captured electronically using a dedicated compliance software program linked to regulatory update alerts and on-going education. Control tasks need to be clearly understood by the end user, along with education to ensure that end users appreciate the importance to the business as well as benefits to themselves in honestly completing the control tasks.

The importance of communications to all stakeholders, including end users tasked with undertaking the control processes, cannot be overlooked. The compliance department needs to actively engage each business unit as well as marketing to develop and implement communication plans for each stakeholder group.

Finally, the compliance department needs to organise their presentation of risk and underlying compliance obligations to reflect the unique nature of their organisation – a one size fits all approach is not workable.

The crucial issue in gaining buy-in from senior management and boards is to identify benefits from the very outset of the integrated GRC project, assign responsibility for achieving these benefits, and ensure that appropriate measurement systems are in place to track the achievement of these benefits throughout the life of the project.
Summary
GRC is no longer solely an esoteric discussion, but one that has captured the minds of business executives looking to identify, categorise, assess, and mitigate potential problems before they adversely affect performance.

Existing methodologies to implement an integrated GRC are inherently flawed and require a new principles-based approach that focuses on what needs to be done rather than on who provides reports or where GRC occurs. The result is a more efficient allocation of resources, allowing management and front line staff to focus on revenue generating activities.

By integrating compliance, governance and risk management, organisations will be armed with the information needed to better direct compliance activity. Compliance departments can be made to be more effective and agile allowing the organisation to demonstrate its capacity to manage risk. With the shift to a more principles based regulatory regime, regulators are more likely to allow organisations to take greater risks if they can clearly demonstrate that they are able to effectively manage those risks in an integrated GRC framework.

It is no secret that organisations with efficient governance, compliance and risk systems tend to score highly in terms of business performance and business sustainability. They are generally characterised by their capability to invest to create value rather than to scrimp to save expense.

Where to Now
Successful implementation of an integrated GRC is not something that can be achieved easily. It is also not wishful thinking but a reality that requires careful planning, buy-in across divisions, and strong leadership.

Highly integrated organisations with a strong GRC champion will be able to implement an integrated GRC framework with little external assistance. Most firms, however, do not possess the multifaceted skills required to bring together the disparate elements of governance, risk and compliance, coupled with project management, change management, communications management, and more!

Successful integrated GRC implementations are not easy to achieve, with many organisations requiring external assistance. However, the benefits to be gained from achieving the reality of an efficient and effective integrated GRC are clear and demonstrable.

Integrated GRC, when done properly, is more than wishful thinking, it is an affordable – and essential – reality.

For information on the capabilities of SAI Global and how to turn the wishful thinking of an integrated GRC into reality, please contact:

- Sonya King, Senior Business Development Manager, Southern Region
  Tel: (03) 9278 1127
  Email: Sonya.King@saiglobal.com

- Ross Millar, Senior Business Development Manager, Northern Region
  Tel: (02) 8206 6364
  Email: Ross.Millar@saiglobal.com
Author Biography:

Alf Esteban is the Head of Consulting and Client Services – Asia Pacific at SAI Global, where he is responsible for leading a team of consultants and implementation services professionals assisting clients in achieving the reality of integrated GRC. Prior to joining SAI Global, Alf provided risk and compliance management consulting services to a wide range of firms in Australia and internationally. He was also the Global Head, Strategy and Operations for IBM’s Financial Markets division based in London. Alf holds several post graduate degrees in business management and is a member of the Global Association of Risk Professionals and the Australasian Compliance Institute.

© 2008 SAI Global Ltd. All rights reserved.
SAI Global accepts no responsibility for advice or information contained in this article although every effort is made to ensure its accuracy.