Abstract

Corporate failures such as HIH, Enron, WorldCom, Arthur Anderson and, unfortunately, many others have changed today’s business environment. Shareholders, employees, clients and wider community stakeholders are demanding that stricter rules are applied so that when public companies release their financial statements or position to the market, the figures are in fact a true reflection of the company. In recent times a myriad of standards have been formed with which organisations have to comply. Standards such as Sarbanes-Oxley in the United States, Principal 7 in Australia and Turnbull in the United Kingdom are all recent developments to ensure organisations do not falsify their financial position to the public market and ensure that organisations have an understanding of their material business risks.

The global financial crisis revealed that the governance, risk management and compliance lessons of these corporate collapses were not learned by all organisations. According to an OECD review - “The risk management systems have failed in many cases due to corporate governance procedures rather than the inadequacy of computer models alone: information about exposures did not reach the board or even senior levels of management, whilst risk management was often an activity rather than enterprise-based. These are board responsibilities. In other cases, boards approved strategy but then did not establish suitable metrics to monitor its implementation. Company disclosures about foreseeable risk factors and about the systems in place for monitoring and managing risk have left a lot to be desired…”1 A number of financial institutions collapsed and many more were subject to enforced takeovers as governments invested heavily to prevent a crisis of the global financial system. Failures of risk management and governance by these organisations resulted in their very existence being threatened.

---

1 (page 2, Kirkpatrick, G. The Corporate Governance Lessons from the Financial Crisis, OECD, 2009.)
Abstract continued

The terminology of Governance, Risk and Compliance, or GRC, has been bandied around as the latest buzz phrase as a result of these standards. These words however, are not new. Enterprise risk has been around for many years and so has regulatory or financial compliance. Only recently have organisations started to combine these words together in order to provide for better corporate governance. After all, it is the risk reports and compliance reports which are reviewed by the board of directors.

In order for transparency, accountability and integrity to occur, companies should look at adopting one or more of the following enablers:

- Adopt a culture of business integrity and ethical values. Employees must accept being held accountable in the event an issue arises
- Look at GRC as a single entity as opposed to separate activities
- Utilise technology to enable efficiencies and effectiveness

Historically, organisations have treated their risk and compliance initiatives as independent silos that span distributed business operations - be it in a single location, national or around the globe. With the increased focus on corporate governance and enterprise risk management, organisations should start to look towards enabling technologies to drive sustainability, efficiency and consistency in managing enterprise risk and compliance management in an effective manner.

This paper discusses why GRC should be treated as a single entity as opposed to separate ones. It also highlights how technology can be leveraged to maintain, monitor and report in real time the state of compliance for an organisation.

About the Author

Alf Esteban is the General Manager, Compliance Division Asia Pacific at SAI Global. Prior to taking on this role in early 2010, Alf was the Head of Consulting and Client Services where he was 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 in 2007, 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 is a Certified Compliance Professional the Australasian Compliance Institute.
Table of Contents

1. Introduction 1
2. Reward for Good Governance, Risk & Compliance 2
3. Integrated View of Governance, Risk & Compliance 4
4. Integrating GRC into the business 6
4.1. A Framework for Integrated GRC 8
4.2. Organisational Ethics and Culture 9
4.3. Governance Processes 10
4.4. Risk Management Processes 11
4.5. Compliance Processes 13
4.6. GRC - Underpinned by Culture 14
4.7. GRC - Bringing it All Together 15
5. Leveraging Technology 16
5.1. Access to Real Time Data 18
5.2. Assessment of Risks and Compliance Obligations 18
5.3. Issues/Incidents Tracking and Risk Mitigation 18
5.4. Accountability and Reporting 18
6. Why Automated Systems Fail 19
7. Conclusion 20
1. Introduction

With companies trying to outprice, out-manoeuvre, or out-perform their nearest competitors, they are doing more to impress their investors. Public companies are no longer treating financial statements as confidential but are broadcasting this information to the market. Companies are using this opportunity to gain a competitive advantage over rivals by doing more in the way of compliance as opposed to doing just the minimum required by the law.

Recent events surrounding financial markets has also put further pressure on financial services organisations, who not only want to keep regulators appeased, but also want to ensure that no adverse findings are made against them by the regulator – and hence the marketplace.

“Simply complying with the rules is not enough. If companies view the new laws as opportunities – opportunities to improve internal controls, improve performance of the board, and improve their public reporting – they will ultimately be better run, more transparent, and therefore more attractive to investors” (Donaldson, W 2003).

So what are organisations doing in order to achieve a good governance status? Post the large corporate scandals of recent times in the United States, “WorldCom is mandating that its Board consist of entirely independent directors, and Tyco is encouraging better controls by having the CFO’s of each unit report to a corporate CFO rather than the business unit presidents” (Ernst & Young). So the question is, “What can we tell shareholders that you have done to polish up on your corporate governance?” (Deloitte & Touche LLP and Deloitte Consulting LLP).

The answer to the above question is that organisations are starting to treat the three separate activities of Governance, Risk and Compliance as a single entity instead of separate ones scattered across the organisation, only being used in their entirety in pockets of the organisation. After all, enterprise risk management works hand in hand with compliance. With the inception of standards such as Sarbanes-Oxley in the United States, Principal 7 in Australia and Turnbull in the United Kingdom, which demand transparency and accountability, the penalties for false disclosure of financial statements are so severe that many organisations would struggle to recover. It is this level of scrutiny that companies need in order to maintain investor confidence and attract new investors.

Technology is starting to play a pivotal role in good corporate governance. Software vendors are mapping software development to purpose built frameworks such as COSO and Basel II. Real time reporting on the state of compliance of a division, business unit or company is priceless. However, companies should ensure they have their manual processes in place before investing in a technology solution. After all, the main benefit of technology is automation, if companies have not got the process and information in place, the advantages will be minimal. Technology allows recording of control assessment information, risk mitigation, incident tracking and issue findings by internal and external audit to all be captured into a central repository which can later be reported on. While information technology spending is on the rise, most solutions currently on the market target Sarbanes-Oxley (SOX) specific, risk specific or compliance specific activities. Like the rest of the corporate world, software companies have now seen the requirement to build combined solutions with Governance, Risk and Compliance (GRC) in mind.
2. Reward for Good Governance, Risk & Compliance

Few will publicly admit it, but many companies have come to view compliance standards such as the Financial Services Reform Act 2001, Sarbanes-Oxley 2002, Anti-Money Laundering Act 2006, and other regulatory impositions, as an unwelcome but necessary burden. The cost and effort in complying with these regulations are a result of a select few individuals who went outside the law for personal gain. Most will agree that the laws were required in order to restore investor confidence. “Public markets are rewarding companies that have good governance, transparency, timeliness, accuracy, and reliability and punishing those who do not”. (Deloitte & Touche LLP and Deloitte Consulting LLP).

Smart companies are going beyond what is required by the law, innovating new practices of their own. This sort of behaviour is reaping shareholder rewards. The author believes compliance has a direct correlation with good governance. Although the mandatory requirement in the United States is to comply with the Sarbanes-Oxley Act of 2002, and in Australia, compliance with the ASX Principles of Good Corporate Governance, organisations are using the same principals and techniques in other areas of the business such as Occupational Health and Safety (OHS), environment and general corporate social responsibility.

The cost to organisations in dealing with investigations and prosecutions – let alone reputation damage – is often not considered by boards or governing bodies. However, any organisation that has been involved in a lengthy investigation, administrative inquiry or prosecution will openly admit that the cost was considerable.

While avoiding such actions cannot be guaranteed, minimising the risk and the cost is certainly achievable through the implementation of a robust, integrated GRC framework that is underpinned by an appropriate culture and supported by appropriate enabling technologies.

The diagram below shows the framework used by many organisations and has been adopted by a framework shared with the author by Fosters Group Limited, a major international player in beverages and operation of licensed premises.
Real cost efficiencies can be gained by promoting a culture that aligns the commercial interests of the company (or social / community interests if considering public sector entities) with its regulatory obligations. When a company’s competitors fail to factor in risk, an organisation with an integrated approach to GRC will have contingencies in place, giving it a competitive edge should a problem arise. Used successfully as a risk mitigation tool, GRC encourages communication and transparency at all levels of an organisation, streamlining business processes and improving work practices that would otherwise go unreviewed.

Capital markets, especially since the recent financial markets crises, are paying closer attention to governance systems and how organisations manage risks and demonstrate compliance. Rating agencies have expanded their assessments to include more qualitative factors around governance, risk and compliance; with the belief that better governance and management of risk can lead to more certainty around the achievement of business objectives which in turn can increase business value.

Organisations that are able to actively demonstrate an effective governance, risk and compliance framework can potentially create for themselves a competitive edge. These qualities have been shown to be of value to investors who are willing to pay a premium and to penalise those who cannot meet the standards of GRC that they require (Ernst & Young).
3. Integrated View of Governance, Risk & Compliance

Up until recently, management and the board of directors have treated GRC as separate activities, managed separately in various business units and divisions across the organisation, which has led to accountability and communication breakdowns as well as a myriad of confusion. In the worse case scenario, this has led to large corporate collapses which are the result of certain individuals falsifying financial statements in order to create the illusion of profit to the public market. New definitions, requirements and standards have been created to stop this sort of behaviour, forcing executive management and the board of directors to rethink the responsibilities and relationships of GRC activities. The actual definitions of Governance, Risk and Compliance are:

- Governance is the set of processes, customs, policies, laws and institutions affecting the way in which a corporation is directed, administered or controlled. The principal players are the shareholders, management and the board of directors (Wikipedia)

- Risk management is a systematic process of making a realistic evaluation of the true level of risks to your business. Before risks can be properly managed they need to be identified (Australian Government)

- Compliance activities include operating in accordance with objectives and ensuring adherence with laws and regulations, internal policies and procedures, and stakeholder commitments (PricewaterhouseCoopers)

A 2006 study (AMR Research) 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. Recent studies indicate that these estimates are likely to be accurate, if not conservative.

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 be sustained cost effectively.

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 organisations often fail to integrate their efforts into a sustainable program of action that will address the issues identified. Coupled with this, many organisations 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 integrated GRC are essential for seizing business opportunities while remaining adaptable to addressing new risks and compliance obligations.

The starting point in an integrated GRC model is the development of a model that takes into consideration the regulatory, commercial and philosophical drivers that impact an organisation. These drivers feed directly into the governance approach of the organisation; which in turn is supported by the risk management system and compliance controls, practices and procedures – including the management of control incidents and risk management failures. Underlying this is access to real time internal data and regulatory updates, supported by a robust document management system. Control tasks are accomplished through a set of consistent and meaningful questionnaires, with knowledgeable staff able to understand the implications of their answers. The information gained from these tasks, regulatory alerts, and organisational learning, needs to be presented to the board or governing body in a meaningful way.

The following diagram illustrates this model of integrated GRC.

![Diagram](image-url)

**Figure 2:** Integrated GRC Model  
© 2009 SAI Global Limited
4. Integrating GRC into the Business

Trusting your staff is not good enough these days. It was this level of trust which led to the collapse of Enron, WorldCom, Arthur Anderson and, unfortunately, a host of others. It is imperative to establish a culture of business integrity within the workforce. Without it a company can quickly lose control.

The following table, using figures obtained in 2003, depicts the level of integrity in a common workplace:

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21%</td>
<td>Abusive or intimidating behaviour toward employees</td>
</tr>
<tr>
<td>20%</td>
<td>Misreporting actual time or hours worked</td>
</tr>
<tr>
<td>19%</td>
<td>Lying to employees, customers, vendors, or the public</td>
</tr>
<tr>
<td>18%</td>
<td>Withholding needed information from employees, customers, vendors, or the public</td>
</tr>
<tr>
<td>13%</td>
<td>Discriminating on the basis of race, colour, gender, age, or similar categories</td>
</tr>
<tr>
<td>12%</td>
<td>Stealing, theft or fraud</td>
</tr>
<tr>
<td>11%</td>
<td>Sexual harassment</td>
</tr>
<tr>
<td>5%</td>
<td>Falsifying financial reports</td>
</tr>
<tr>
<td>4%</td>
<td>Giving or accepting bribes, kickbacks or inappropriate gifts</td>
</tr>
</tbody>
</table>

**Table 1:** Ethics Resource Centre National Business Ethics Survey 2003

The worrying aspect of this data is that the latest survey (2007) shows that ethical misconduct is back at pre-Enron levels, with over 50% of employees seeing ethical misconduct of some kind. Of those employees who reported ethical misconduct, 16% experienced some form of retaliation for reporting the matter.

The research also shows that the number of companies that are successfully incorporating strong enterprise-wide ethical culture into their business has declined since 2005, with only 9% of organisations reporting that they have a strong ethical culture. The key issue appears to be that the majority of organisations implementing ethics and compliance programs focus on ‘what employees must avoid’ instead of providing principles of what employees ‘should do’.

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 of an integrated GRC framework needs to occur.
Moving from current silo based GRC, or 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.
4.1. A Framework for Integrated GRC

Integrating GRC into a business requires an organisation to have a starting framework from which they can tailor their policies and control procedures. It is essential that this framework takes into consideration a recognition that the ethics, culture and training of the organisation plays a significant role in the success of integrated GRC; the ability for the organisation to problem solve and continuously improve its controls, procedures and policies; and that the responsibility for an effective integrated GRC program starts with the board or governing body of the organisation.

The following framework has been developed by the author as a starting point in the development of an integrated GRC framework. It has been successfully implemented – with appropriate customisation to meet the idiosyncrasies of each organisation – in public, private, government and not-for-profit organisations.

![Figure 3: Elements of an Integrated GRC Framework](image)

This framework builds upon the model shown in Figure 1 and shows the logical linkages and dependencies between each of the components.
4.2. Organisational Ethics and Culture

Enron had all of the elements usually found in comprehensive ethics and compliance programs - a Code of Ethics and a reporting system, as well as a training video on Vision and Values led by Ken Lay and Jeff Skilling. Also, while there was criminal activity, Enron did not set out to hire felons. Rather, it was the mindset and culture of the company that brought out the worst in some top executives and inaction and passivity on the part of many others.

Culture is the leading risk factor for compromising integrity and compliance in companies today. Yet many organisations are unable to implement a truly effective ethics and compliance program because they lack sufficient knowledge of how their culture can create vulnerabilities and risks. And without that knowledge, companies cannot measure progress towards meeting ethics and integrity goals.

Moreover, many companies only focus their ethics program assessment and measurement on elements that do not directly determine the outcomes they need. Ethics officers need to be certain that the data they obtain, such as code certifications and compliance course completion, correlates to the compliance behaviour and the ethical culture they are seeking.

An ethical culture is a reflection of the collective ethical values and behaviours of all employees, managers and leaders. A Culture Risk Assessment is a useful tool, providing a measurable overview that can direct an organisation to specific behavioural problem areas that increase the likelihood of both unethical conduct taking place, and if it does take place, of not being reported.

The benefits of a positive ethical culture include:

- Employees feel a sense of responsibility and accountability for their actions and for the actions of others
- Employees freely raise issues and concerns without fear of retaliation
- Managers model the behaviours they demand of others
- Managers communicate the importance of integrity when making difficult decisions
- Leadership understands the pressure points that drive unethical behaviour
- Leadership develops processes to identify and remedy those areas where pressure points occur

In an ethical culture, employees and managers understand why doing the right thing is important for the organisation’s long-term viability, and they have the determination, courage and freedom to see that the right thing gets done. An ethical culture supports independent thinking employees and managers who make decisions consistent with the organisation’s values.

The challenge is determining how to get to this state and whether the tools in place to measure and monitor the performance of the ethics program are sufficient to gauge whether adequate progress is being made.

Many organisations have set expectations for ethical conduct and are working towards maintaining a strong ‘tone from the top’. However, many of these same organisations really don’t know whether their employees and managers will demonstrate integrity in their actions when they are under pressure and immediate business objectives loom large in front of them. As the former director of accounting at WorldCom, Buford Yates, Jr. said as he was sentenced to a year in prison for his role in the fraud: “When faced with a decision that required strong moral courage, I took the easy way out”.

Corporate culture is made up of the collective values of employees and managers that are reflected in their collective actions. Companies must therefore be aware of the range of values held by its employees if it is to be able to shape and guide its culture towards supporting the kinds of ethical behaviours needed to reduce the risk of ethics scandals and criminal prosecution.
4.3. Governance Processes

Governance is the framework of rules, relationships, systems and processes within and by which authority is exercised and controlled in organisations. It encompasses the mechanisms by which the organisation and those in control are held to account. Governance influences how the objectives of the organisation are set and achieved, how risk is monitored and assessed, and how performance is optimised (ASX).

Corporate governance is a new term for an issue which has been discussed and debated for several centuries. Adam Smith, writing in 1766, said that “the directors of such companies, however, being the managers rather of other people’s money than of their own, it cannot well be expected that they should watch over it with the same anxious vigilance [as owners]... Negligence and profusion, therefore, must always prevail, more or less in the management of the affairs of such as company” (Adam Smith 1766).

In order to execute effective governance, the board of directors and executive management must effectively oversee a number of key business processes:

- Strategy and operation planning
- Risk management
- Ethics and compliance
- Performance measurement and monitoring
- Mergers, acquisitions and other transformational transactions
- Management evaluation, compensation and succession planning
- Communication and reporting

The starting point in the governance process is the determination of levels of accountability and responsibility. While the board is ultimately responsible for the achievement of objectives and satisfying stakeholder criteria, delegation of decision making and accountability to the CEO (and ultimately to all levels of the organisation) needs to be defined and documented.

The governance process needs to ensure that there are defined and documented policies and procedures relating to areas which may materially impact upon the achievement of objectives. The ASX’s Principles of Good Corporate Governance provides a set of recommendations which can assist in the development of a solid governance foundation.

Australian Standards AS 8000 Good Governance Principles, AS 8001 Fraud and Corruption Control, AS 8002 Organisational Codes of Conduct, AS 8003 Corporate Social Responsibility and AS 8004 Whistleblower Protection Programs are also good reference tools for organisations wanting to implement good governance across all levels of management.

AS 8000 breaks governance principles down into the three broad elements of structure, operational, and maintenance. The table below shows the components of each element and will be used again later in this paper to show the linkage between governance and compliance.

<table>
<thead>
<tr>
<th>Structure</th>
<th>Operational Elements</th>
<th>Maintenance Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commitment</td>
<td>Identification of issues</td>
<td>Education and Training</td>
</tr>
<tr>
<td>Governance Policy</td>
<td>Operating procedures</td>
<td>Visibility &amp; Communication</td>
</tr>
<tr>
<td>Board Responsibility</td>
<td>Dealing with breaches &amp; complaints</td>
<td>Monitoring &amp; assessment</td>
</tr>
<tr>
<td>Continuous Improvement</td>
<td>Record keeping</td>
<td>Review</td>
</tr>
<tr>
<td></td>
<td>Internal reporting</td>
<td>Liaison</td>
</tr>
</tbody>
</table>

Table 2: AS 8000 Good Governance Principles
4.4. Risk Management Processes

The word ‘risk’ is derived from the early Italian ‘risicare’ which means ‘to dare’. Risk is a choice rather than a fate and the actions that all individuals, groups, organisations and countries take are based on an assessment – either consciously or not – of the risks involved in taking that particular choice (Bernstein 1996).

The various risk management standards (AS 4360, COSO enterprise risk management framework, ISO 31000) identify key elements of an effective enterprise risk management framework designed to help an organisation achieve strategic, operational, compliance and reporting objectives. In general, these elements are:

- Risk identification
- Risk assessment
- Risk response
- Risk mitigation
- Incident tracking and remediation
- Control activities
- Monitoring and reporting

The diagram on the next page, adapted from the draft ISO 31000 Standard, shows the linkages between each of these elements.

Risk governance is a process which is often overlooked in the implementation of risk management frameworks in organisations. The author has often seen well documented risk management frameworks that fail to take into consideration that risk management is the responsibility of all employees and not just the senior management and risk manager.

In implementing risk governance, policies and procedures should be in place which will allow for:

- The education across all levels of staff of the risk management process
- The identification of the sources of risks
- How the level of risk is determined
- The comparison of the levels of risks with either pre-determined thresholds or risk appetite to prioritise mitigation actions
- Management of risk treatment action plans
- Ongoing monitoring of the risk management process to ensure continual effectiveness of risk treatments
- Linkage with overall governance reporting needs
Risk governance can only be successfully applied if there is an appropriate risk management culture in place. Staff need to know what is expected of them in their specific roles, receive appropriate training based on the role, and be held accountable for all aspects of their performance – including the management of risk.

A good risk management culture is one where there is an environment in which staff are encouraged to speak up and report risks, including control failures and near misses, and management welcomes and acts on this information.

Figure 4. ISO 31000 Risk Management Framework
4.5. Compliance Processes

Compliance is a set of actions that ensures that activities undertaken by an organisation agree with both the letter and spirit of the standard, law and/or regulations that govern a business of activity and the internal policies and procedures set down by that business for its own activities (Standards Australia, AS 3806). Enforcing compliance means ensuring that the business adheres to its external (legislation, regulations, rules, standards etc.) and internal (policies and procedures) obligations and risk control mechanisms.

Since the inception of legislation, but driven more recently in the last decade by industry specific regulations such as the Financial Services Reform Act, Sarbanes-Oxley in the USA and others, organisations such as Standards Australia and the Open Compliance & Ethics Group (OCEG) have detailed the key elements of an effective compliance framework. These include:

- Standards and procedures
- High-level oversight
- Due care in the delegation of authority and responsibility
- Effective communication and training
- Monitoring, auditing and reporting processes
- Ongoing process improvement

AS 3806 Compliance Programs provide for twelve principles to achieve good compliance management. These are summarised within four key elements:

1. Commitment
2. Implementation
3. Monitoring and measuring
4. Continual improvement

Table 2 summarised the elements of AS 8000. This table is replicated below to also include the elements of AS 3806 and clearly demonstrates the overlap and linkage between the two standards.

<table>
<thead>
<tr>
<th>Commitment</th>
<th>Implementation</th>
<th>Monitoring &amp; Measuring</th>
<th>Continual Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commitment</td>
<td>Responsibility articulated and assigned</td>
<td>Program performance is monitored, measured and reported</td>
<td>Reviewed and continually improved</td>
</tr>
<tr>
<td>Compliance Policy</td>
<td>Competency and training needs assessed and addressed</td>
<td>Demonstrated through documentation and practice</td>
<td></td>
</tr>
<tr>
<td>Appropriate Resources</td>
<td>Encouragement of behaviours that support compliance/ no-tolerance of behaviours that compromise compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endorsement by governing body/ senior management</td>
<td>Controls in place to manage obligations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obligations identified and assessed</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3. Role of Compliance in Governance, AS 3806 vs AS 8000

Compliance alone does not guarantee sound corporate governance. However, a robust AS 3806 compliance program can assist organisations in demonstrating good corporate governance.
4.6. **GRC – Underpinned by Culture**

It is clear from the above that organisational culture is critical to the success of an integrated GRC framework. In 2007, the OCEG, released a paper on the integration of GRC and put culture as the central component, as shown in the diagram below.

A culture that encourages compliance among employees has been referred to as a ‘culture of compliance’ in popular management literature and by industry commentators. The basic proposition is that in a specific type of culture, employees are more likely to engage in compliance behaviours which collectively will contribute to organisational compliance (Interligi, 2008).

Industry has embraced the idea of a ‘compliance culture’ as central to the success of contemporary compliance management. But the notion of a single ‘compliance culture’ is overly simplistic, with organisations balancing multiple and sometimes competing or conflicting regulatory goals. Conflict arises from competition between ideological approaches, values and ideals regarding conception and management of risk in organisations (SAI Global, 2007).

Recent research conducted by Monash University, sponsored by SAI Global, has found that there is no generic compliance culture but culture with multiple dimensions. The research found three ‘types’ of compliance culture:

- Enforcement culture
- Agreement culture
- Alignment culture
An enforcement compliance culture is defined by an underlying objective of employee obedience, is
governed by formal structure (such as hierarchy, rules and processes) and seeks procedural consistency
through compliance. It is often found in highly regulated industries such as financial services where failure
to comply can result in loss of licence to operate, or in mining and processing where failure to comply can
result in death or serious injury.

In contrast, an agreement compliance culture seeks employee responsibility for compliance outcomes
either through processes of organisational-employee exchange that result in compliance co-operation, or
shared commitment to values and principles resulting in compliance co-activity (Interligi, 2008).

An alignment culture is often found in charitable or socially focused organisations where employees share
a common belief system which is reinforced through the GRC process.

The Monash research also found that there is no correct compliance culture, with each organisation
embedding a culture that was aligned to its business objectives, industry type and leadership.

4.7. GRC - Bringing it All Together

The OCEG, working in conjunction with XPLANE.com, have developed a diagram which attempts to bring
all of the above pieces together to show how an integrated GRC system can work in reality. This is available
at http://www.oceg.org/view/IllustratedBigPic and leads to the use of technology to act as an enabler
across the GRC elements.

The use of technology as an enabler is discussed in the next section.
5. Leveraging Technology

“Historically, businesses have not made GRC technology investments a high priority relative to other technology objectives. However in the current business environment, where access to real-time information can be critical in nature and the burden of regulatory compliance continues to trend upward at an accelerated pace, technology must be viewed as a key enabler for addressing the rising demands of stakeholders” (PricewaterhouseCoopers).

Prior to organisations using technology to aid in their corporate compliance obligations, they need to have all their processes documented, as well as a clear idea of the ongoing process they want to create, before investing in a tool (Ernst & Young 2004). Technology is useful if tasks need to be repeated over and over. Complying with financial standards is a repeatable process. It is this level of duplication or repetition where technology can pay dividends. “To get the most value out of a GRC software platform requires that existing risk and compliance organisational structure and processes are in place so that the software can support and enhance through technology enablement” (Rasmussen 2006).

Up until now, companies have used external service providers such as Deloitte, KPMG and Ernst & Young to assist in the assessment of controls and effective risk management. “Going forward, many companies are recognising the need to make compliance repeatable and sustainable to reduce compliance cost and their reliance on external service providers. Research has found that Sarbanes-Oxley ranks as one of the top three IT spending priorities for 2005” (Markham Hamerman 2005). “The Sarbanes-Oxley Act is giving Chief Information Officers the opportunity to load up IT budgets with special interest line items” (Deloitte & Touche LLP and Deloitte Consulting LLP).

Implementing a GRC software solution can provide a single system of record for identifying, monitoring and maintaining governance, risk and compliance. GRC software solutions create centralised systems of record in the following areas:

- Control monitoring, assessment and remediation
- Risk monitoring, assessment and mitigation
- Process, risk and control reporting by organisation, business unit or division
- Incident and issue tracking and reporting

“The Treadway Commissions Committee of Sponsoring Organisations (COSO) developed a framework which identifies key elements of an effective enterprise risk management approach for achieving financial, operational, compliance and reporting objectives” (PricewaterhouseCoopers). Many software vendors are using this framework as a foundation of their software development. Technology benefits include:

- Access to real time data
- Assessment of risks and compliance obligations
- Automated tracking of issues and incidents as well as risk mitigation controls
- Automated reporting and ease of allocation of accountability
These benefits are expanded on in the following subsections, and shown diagrammatically in Figure 7 below.

Good Corporate Governance

- Board information management
- Audit, assurance & certification
- Risk Management
- Compliance management / questionnaires
- Incident Management

Document management (secure & dynamic)

Training, awareness and employee engagement

Regulatory, risk and market intelligence (alerts, databases & newsfeeds)

Regulatory:
- Corporate law
- Privacy
- Audit & certification
- Financial crime
- OH&S
- Exchange rules
- Local & overseas rules

Commercial:
- Competition
- Evolution/R&D
- Capital/profit
- Security
- Resilience/sustainability
- Efficiency
- Brand/reputation

Social:
- Ethics/integrity
- Culture
- Environmental
- CSR
- Human rights
- Community
- Employees

*Figure 7. SAI Global © 2008*
5.1. Access to Real Time Data

Real time data can include regulatory, risk and market intelligence (alerts, newsfeeds, knowledge databases etc.) which can be used by management and the board in the decision making process.

Processes, risks and associated controls can all be loaded into a technology database. The status of these items can then be reported on instantaneously using a built in reporting engine. Non compliance of controls can therefore be flagged and rectified immediately, as opposed to a manual system whereby non compliance may only be identified moments before the report is due for the board and the market.

5.2. Assessment of Risks and Compliance Obligations

The process of identifying, assigning and addressing/assessing risk and compliance obligations are key elements to establishing overall compliance. An organisation is likely to have a series of controls which treat a number of risks. These controls are assigned to an owner who will assess each item based on the assessment schedule assigned to them. Some controls may need to be assessed weekly or monthly but in most circumstances the state of compliance for an organisation is quarterly. In the event a control is marked as not compliant it is mandatory to create an action plan to ensure the necessary steps are taken to address the failing control and ultimately assess the control as compliant.

5.3. Issues/Incidents Tracking and Risk Mitigation

Issues or incidents can come about in a number of ways. Incidents can be logged anonymously by way of a whistle-blowing policy. Alternatively, an owner of a risk could raise an incident as a form of risk mitigation based on an ineffective control. Prior to technology, issues would be contained within in an audit report under a section called audit findings. Issues would then be itemised, prioritised and assigned to owners who then manage the issue to completion. With the inception of technology, issues and incidents can be logged, escalated electronically and dealt with in real time prior to the audit committee meeting. If issues are dealt with prior to the audit report being drafted, the chances of any red flags will be minimised which in turn provides the board with a transparent view of the organisation’s state of compliance.

5.4. Accountability and Reporting

An instantaneous report of the state of compliance for an organisation is priceless. The COSO framework is designed in a way which provides for roll up reporting and monitoring. At first each control is assessed individually. In the event of a non compliant control, an action is created and assigned to an owner. Based on a summary and status of controls, a risk owner can effectively assess the residual risk and overall effectiveness of the controls. If the controls are effective, the residual risk rating should be lower than the inherent risk rating. Once the risks have been assessed, the process owner can certify their process which will then be rolled up to the business unit or division owner. This control self assessment process can be reported on at any time during the assessment period using technology. If the same process was being done manually, the necessary actions will not be put in place and dealt with fast enough which could ultimately lead to a business unit being not compliant. This could be detrimental to an organisation when it is time to collate each business unit’s risk and compliance reports for board reporting purposes.
6. Why Automated Systems Fail

The author has found that applying technology to GRC does not always result in the desired outcomes envisaged when being first introduced. Often, the technology solution merely makes worse an already ineffective system – albeit now being more effective!

Applying technology to GRC without due consideration of the desired outcomes and impact of technology will only automate what is already in place. If the manual system is ineffective, no manner of efficiency improvement will generate improved effectiveness. Often, systems are implemented without regard to the root cause of lack of effectiveness.

An example known to the author was the attempt by the OH&S department of a NSW utilities entity to automate compliance to OH&S legislation. Rather than change the culture of the organisation, driven by the methods to ensure compliance, the department merely automated an ineffective paper-based system. After a number of months using the new system, the OH&S Manager complained that the system had not improved compliance and that OH&S incidents were trending negatively. On inspection, the author found that the organisation had not considered the root cause of issues (lack of communication between the remote depots and head office) and the automation of an existing ineffective paper-based system had no benefit to the organisations outcomes. The organisation, after careful consideration and review, implemented a completely new system and approach to compliance and has since seen a substantial improvement in compliance.

Additionally, the introduction of technology to enhance efficiency – and preferably effectiveness – tends to address the needs at a point in time and requires constant review and monitoring to ensure that the system continues to meet current needs. The author, having implemented a variety of automated GRC systems, has found that typically these systems need to be refreshed (in terms of design, if not overall approach) at least every 3 to 5 years. The author has worked with several large organisations in the financial services sector who have embarked on refresh programs to address changing business circumstances as well as changed governance needs.
7. Conclusion

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 framework 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.

It is essential for a company to adopt a culture of accountability and transparency if they want to portray good governance to stakeholders and investors. Since the inception of corporate standards, the business world is becoming more and more transparent. Leading organisations are reporting additional information to stakeholders in order to meet increasing requirements and to secure competitive advantage over competitors. Companies are looking to technology to flag issues in advance, so that the board and executive management can deal with the problems before a crisis occurs. “Corporations have no choice but to rethink their values and behaviours – for the better. If you’re going to be naked, you better be buff” (Tapscott, Ticoll 2003).
References

1. Rasmussen, M 2006, Overcoming Risk and Compliance Myopia
3. Ernst & Young, Investors on Risk, 2007
4. Deloitte & Touche LLP and Deloitte Consulting LLP, Straight Talk Book No.5
7. PricewaterhouseCoopers, Integrity-Driven Performance
13. Standards Australia – AS 8000: Good Governance Principles
16. The Treadway Commissions Committee of Sponsoring Organisations (COSO)
17. Standards Australia – AS 3806-2006: Compliance Programs
18. Open Compliance and Ethics Group (OCEG) 2007
20. SAI Global with Monash University 2007, The Compliance Imperative: Sustainable Compliance through Culture
21. OCEG and XPLANE.com 2007
22. Ernst & Young, 2004, Section 404 Post implementation

©2009 SAI Global Limited

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate information, there can be no guarantee that the information provided is accurate as of the date received or that it will continue to be accurate in the future. No one should act upon the information contained in this report without appropriate professional advice or examination of their particular circumstance. The views and opinions expressed herein represent judgments at the time and are subject to change.