

INTEGRATED GOVERNANCE, RISK & COMPLIANCE ("GRC")

BOOGEYMAN FEAR MONGERING, POT OF GOLD AT THE END OF THE RAINBOW, OR JUST GOOD BUSINESS?

Tim J. Leech FCA·CIA·IT, CFE

The boogeyman (also called bogeyman) is a legendary ghost-like monster that children often believe is real. Sometimes parents will, as a way of controlling their children, encourage belief in a boogeyman that only preys on children that misbehave. Some say the concept of a boogeyman originated from the Middle English word *bugge*, meaning "a frightening spectre". Although the specific term used varies around the world, the concept of "the boogeyman" is universal. The well known adage "the pot of gold at the end of the rainbow", while not quite as universal as the boogeyman, is also very well known. This expression is rooted in Irish mythology, leprechauns, and people's quest for riches. The term has come to generally mean a promised reward for a long journey.

Promotional claims for "the next big thing" on the corporate scene, integrated governance risk management and compliance or Integrated GRC for short, are a confusing mix of boogeyman scenarios, both real and imaginary; pot of gold at the end of the rainbow promises; and just plain good business. The challenge for companies and executives thinking of embracing the new GRC integration movement is to sort out what is genuine and relevant, what's imaginary, or at best of limited relevance to them (or as the Irish expression goes, blarney), and which parts are irrefutably a better way of doing business in today's world.

WHAT IS GRC?

Before analyzing and dissecting the various elements of the emerging integrated GRC movement, the term "Governance Risk and Compliance" needs to be properly introduced. Like other IT driven movements that have come before such as ERP (Enterprise Resource Planning) and CRM (Customer Relationship Management) the term GRC is evolving and subject to a range of interpretations.

GOVERNANCE

One of the better, albeit fairly long, explanations of the term corporate governance is found in the Preamble of the 2004 OECD (Organization for Economic Co-Operation and Development) **Principles of Corporate Governance**:

Corporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. Good corporate

governance should provide proper incentives for the board and management to pursue objectives that are in the best interests of the company and its shareholders and facilitate effective monitoring. The presence of an effective corporate governance system, within an individual company and across an economy as a whole, helps to provide a degree of confidence that is necessary for the proper functioning of a market economy. As a result, the cost of capital is lower and firms are encouraged to use resources more efficiently, thereby underpinning growth. (page 11)

In a 2004 white paper titled **Integrity Driven Performance**, PricewaterhouseCoopers reduces the concept of governance to a shorter, more succinct set of activities:

Governance activities include setting business strategy and objectives, determining risk appetite, establishing culture and values, developing internal policies and monitoring performance.

SIMPLY PUT

Simply put, governance is fundamentally about how an organization is managed by the people responsible.

RISK MANAGEMENT

Many people believe, quite correctly, that the emerging discipline of structured and formalized risk management is rooted in the **Australian/New Zealand Risk Management Standard 4360**, originally issued in 1995. The 2004 update of that seminal foundation standard defines risk management simply as:

the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects.

The 2004 COSO **Enterprise Risk Management – Integrated Framework**, issued by a U.S. 5 member committee 9 years after the first edition Australia/New Zealand standard, proposes a longer definition for the broader concept of *enterprise* risk management:

“a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives” (page 4)

Expressed as a set of activities the PwC white paper **Integrity Driven Performance** states:

Risk management activities include identifying and assessing risks that may affect the ability to achieve objectives, applying risk management to gain competitive advantage and determining risk response strategies and control activities. (page 7)

A Conference Board report titled **Corporate Governance Best Practices: A Blueprint for the Post-Enron Era** suggests:

Management and boards should give thoughtful consideration to the benefits of implementing a robust and effective risk management system which includes: greater flexibility, less frequent and severe sudden shocks, and greater investor confidence. It is management's responsibility to assess and manage the various risks facing the company while boards must ensure that a system is in place; that the key risks are identified and transparent; that the system is robust, independent and fully aligned with the overall strategy; and the company develops and supports a true risk management culture. (page 57)

SIMPLY PUT

Simply put, risk management is fundamentally about formally identifying and considering events or situations that could impact on the achievement of objectives and asking whether the organization's position, after considering what has been done to manage or "treat" those risks, is tolerable and appropriate given the organization's appetite for risk.

COMPLIANCE

Corporate compliance functions on two levels – compliance with externally imposed laws and regulations and compliance with directives from the board and senior management in the form of policies and rules. People in their everyday lives first confront the concept of compliance as young children when parents first attempt to impose the "house rules" of behavior – make your bed, eat your peas, don't wet your bed, don't hit your sister, etc. The total universe of applicable rules and laws expands exponentially as we get older, particularly for people that take on senior executive roles in business and government. Just how big and onerous that universe of laws and regulations is varies widely around the world at the national, state and municipal levels.

A hard-hitting report from the Competitive Enterprise Institute titled **Ten Thousand Commandments: An Annual Snapshot of the Federal Regulatory State** estimates the total cost of regulation in the U.S in 2005 at **\$1.127 trillion**, equivalent to 9% of U.S. gross domestic product that year. A report titled **Government Regulatory Compliance Cost Report** estimates that complying with government regulation consumes \$1.4 Trillion, or the equivalent of \$4,680 per man, woman and child in the U.S. Although the basis of these calculations can be debated, the fundamental point that regulatory compliance is massively expensive is irrefutable.

The number and complexity of the laws and regulations that govern business conduct continues to grow unabated each month. Although high profile regulatory regimes like Sarbanes-Oxley, the Patriot Act, OSHA, HIPPA in the U.S. and Basel II national regimes globally capture disproportionate amount of attention and press, there are literally thousands of laws and regulations that even small companies operating in a single country must obey or risk the consequences. “Regulatory Risk”, and the consequences that can flow from it, is regularly and increasingly being cited by senior executives and board members as one of the most dangerous risks companies face today, especially in the U.S.

In addition to external laws and regulations, boards of directors and senior management often issue “internal laws” via corporate policies and rules. Although just how much formal policy is necessary to meet regulatory expectation is open to debate, what is clear is that the absence of some reasonable level of formal documented direction on how business is to be conducted is increasingly seen, and publicly reported, as a symptom of “bad governance”.

SIMPLY PUT

Simply put, compliance in the business world is about ensuring external laws and regulation and internal policy directives are being complied with at a level consistent with corporate morality and risk tolerance.

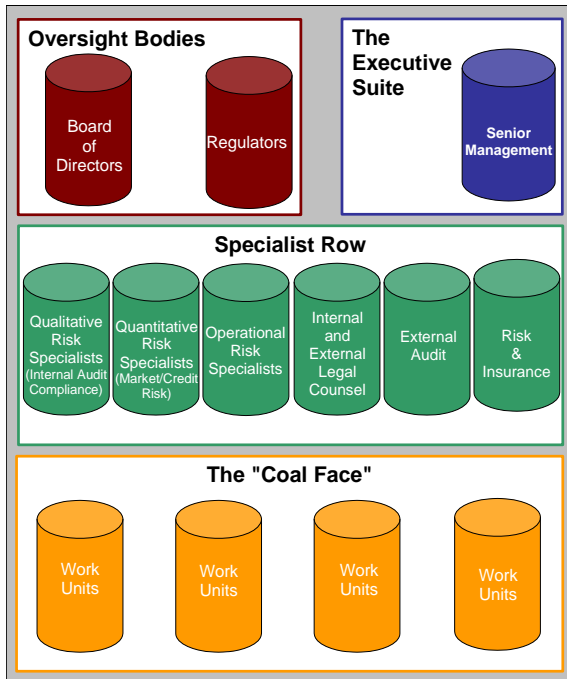
INTEGRATED GOVERNANCE, RISK AND COMPLIANCE

Most readers will have recognized that the three core elements of GRC described above exist in some form in organizations of all sizes and types, and have existed in some form since organized business activities came in to existence. Laws, risks and notions of what constitutes adequate corporate governance have been around for a long time.

SO WHAT’S DIFFERENT?

The number one difference that distinguishes integrated GRC is just what the words imply – the degree of integration of the GRC effort of all assurance providers. Assurance players include the Board of Directors, senior executives, a range of assurance specialists and, perhaps most importantly, the work units that execute an organization’s mission and objectives. Law makers and regulators around the world are increasingly recognizing that traditional silo-based GRC with limited integration of efforts hasn’t worked well enough and new more integrated GRC approaches are necessary.

Figure 1 below illustrates the range of “assurance silos” that exist in large corporations. Although the number of silos is usually less in smaller organizations, the basic premise is that integrating the efforts of all of these silos is key to reducing the incidence of major GRC failures and containing costs.



Specific key differentiators of INTEGRATED GRC from silo-based traditional GRC include:

1. **INTEGRATED REPORTING.** Boards and senior executives increasingly want and expect integrated and timely reports on the organization's "RESIDUAL RISK STATUS" ("RRS"). Residual risk is defined as the level of risk remaining after considering the "risk treatments" in place. These reports should be sorted by "level of executive/board attention required" and include easy to understand summary RRS ratings. The coverage in terms of the specific areas/topics being formally assessed and reported on should be defined by the Audit Committee and senior management. A sample of RRS rating definitions is shown in Attachment 2. The consolidated RRS reporting system should cover all areas critical to the organization's long term success, especially areas considered particularly critical and/or dangerous to the organization.
2. **INTEGRATED METHODOLOGY/TERMINOLOGY.** To accomplish point 1 business units, assurance specialist groups and senior management must embrace the use of IT systems that pull together the full range of relevant information necessary to produce reliable enterprise level RRS reports. Residual risk status is what senior executives and boards should focus on. Gross risks and the controls in place must be identified and assessed to accomplish this task, but the real end game should be producing a picture of the current residual risk situation after considering management decisions and actions to avoid, share, mitigate or accept various risks. Attachment 3 to this paper includes a simplified illustration of an approach that is rooted in the principles AS/NZ 4360 and the COSO ERM integrated framework that can be used to determine RRS. The key

goal is to agree a common assessment methodology/terminology that is used across the full range of areas that require formal assurance. This simple assessment approach can be applied at all levels of an organization and be used to assess whole entities, subsidiaries, processes, business objectives and sub-business objectives.

3. **INTEGRATED GRC DATA PLATFORM.** To accomplish points 1 and 2 cost effectively organizations must work towards the goal of identifying, accumulating and quality assuring the information necessary to produce reliable and timely reports on enterprise wide residual risk status. An overview that illustrates the range of data sets necessary to do this activity at a fairly high level of sophistication is included as Attachment 4 to this paper. The goal is not to require the use of all the data sets shown in this illustration but to require the use of as few of these data sets as is necessary to obtain the level of formal assurance that the true residual risk status is being identified and managed.

Once organizations understand the difference between traditional silo-based GRC and integrated GRC the next key question to be addressed has to be WHY CHANGE? The changes required to move from traditional GRC to integrated GRC are both significant and painful on many fronts and should not be underestimated. Getting disparate GRC silo groups like internal audit, external audit, IT security, compliance, safety, environment, insurance, legal and others to give up turf and adopt common assessment methodology, terminology and technology is daunting.

WHY ADOPT INTEGRATED GRC?

BOOGEYMAN FEAR /PAIN AVOIDANCE ARGUMENTS – REAL AND IMAGINERY

The dominant fear/pain avoidance based justifications being advanced for a new and better approach to GRC include:

1. **TRADITIONAL SILO-BASED GRC HAS DEMONSTRATED AN UNACCEPTABLY HIGH FAILURE RATE.** We all make mistakes from time to time in our lives, both big and small. Few, if any, companies consistently produce 100% fault free products and/or service offerings. Some level of failure and danger exists in virtually all facets of human life including national security, operation of nuclear plants, commercial air transport, playing sports in everyday life, as well as operating publicly listed companies. The key question is not whether there will be failures but rather how many failures are too many? The

public's verdict after the Enron era "perfect storm" was the failure rate was too high leading to the enactment of Sarbanes-Oxley.

2. **INCREASINGLY TANGIBLE PENALTIES FOR GRC FAILURES.** The consequences for not effectively managing the GRC dimension of business are escalating. Weak and ineffective GRC systems are increasingly at the root of executive jail sentences, corporate fines and settlements, civil lawsuit decisions, stock price devaluation, credit rating downgrades, and, in extreme cases like Enron and Arthur Anderson, cancellation of the very right to be in business at all. In the U.S. under the Federal Sentencing Guidelines jail time and fines can be as much as 400% of the base penalty for executives and/or companies unable to demonstrate a serious effort was made to avoid breaking the law they have been convicted of violating.
3. **REAL-TIME GLOBAL EXPOSURE OF TRANSGRESSIONS.** Global communications capabilities have advanced exponentially. Public exposes of serious corporate transgressions now travel at what is close to light speed. The conviction of people like Andrew Fastow, Ken Lay and Jeff Skillings from Enron, Bernie Ebbers, ex-CEO at scandal plagued WorldCom, and other high profile executives were broadcast literally around the world within minutes of the judgments.
4. **SEVERE SANCTIONS FOR WHAT WERE COMMON PRACTICES.** Society's view of corporate social responsibility continues to grow and evolve and standards can change literally over night. What was OK yesterday may bring jail time today. Very common and widespread practices in the insurance and mutual fund sectors that had been an everyday way of life for decades were exposed and criminalized by Elliot Spitzer. His work exposing "bad corporate governance" that had been a way of life for decades in those sectors got him elected governor of the state of New York. Labor practices in China and third world countries can now impact on sales in Chicago literally overnight. Reports on corporate illegality can influence the choices of high caliber candidates deciding which company to join, especially CFOs, CEOs and boards of director candidates looking for "safe havens".
5. **WASTING MONEY.** Few of us like to hear that we carelessly wasted money, especially when that money has been entrusted to management to manage on behalf of shareholders. There is increasing evidence that traditional silo-based approaches not only have high failure rates but they are also needlessly expensive because of the proliferation of demands from silo based assurance groups.
6. **STIGMA ATTACHED TO "HAVING BAD CORPORATE GOVERNANCE".** Points 1-4 above can be aggregated in to the general stigma, and the very real tangible adverse impacts that come with being labeled by some combination of regulators, investors, credit agencies, customers, suppliers, unions,

current employees, perspective employees and others, as “a bad corporate citizen” or having “bad corporate governance”.

INTEGRATED GOVERNANCE, RISK AND COMPLIANCE: THE POT OF GOLD AT THE END OF THE RAINBOW CLAIMS – REAL AND IMAGINERY

Turning from the dark or “half-empty” view, a sample of the many positive benefits and rewards proponents claim are in store for organizations that embrace integrated GRC include:

1. **LOWER GRC FAILURE RATE.** Major corporate scandals like the current stock option back dating charges impacting hundreds of U.S. listed public companies; corporate frauds at Enron, WorldCom, HealthSouth, Nortel, Hollinger, Parmalat, and scores of others; SEC investigations; massive entity-crippling civil decisions linked to negligence related to safety, environment, human rights and other similar situations are all linked in some way to a failure of national and corporate GRC systems. Proponents of integrated GRC claim that, properly applied, integrated GRC will significantly out perform silo-based systems.
2. **INVERSE OF BOOGEYMAN FEARS.** It stands to reason that at least some of the fear-based GRC demand drivers can also be seen in the inverse as positive inducements to adopt GRC. This group includes promises that successful adoption of a robust GRC regime will lead to fewer instances of executives going to jail, less corporate fines and out-of-court settlements, a lower overall cost of capital, better credit rating, higher share prices and lower earnings volatility, increased ability to attract senior executives and board members and other similar good things. Even a small change in a firm’s cost of capital or share price that is linked to improved GRC can provide rapid payback for a GRC change initiative.
3. **IMPROVED RESOURCE ALLOCATION DECISIONS.** A key benefit of succeeding with the R or risk management dimension of GRC regularly cited by its proponents is that it produces radically better information to make resource allocation decisions. The key notion is that the integration of efforts of both work units and specialist assurance units will produce better and more balanced information on where the really important risks and risk exploitation opportunities are in an organization. Integration of GRC information and efforts leads to integration and use of the GRC information in the planning, budgeting, performance management and remuneration systems. Silo-based GRC approaches come with the very real risk that by putting a spotlight on only one dimension of an organization and identifying unmitigated risks (also known as control deficiencies) that it will cause managers who may be punished if they are not seen as responsive to audit deficiency reports to sub-optimally allocate human and monetary resources.

4. **LOWER OVERALL COST OF ASSURANCE.** The traditional approach to GRC utilizes a range of silo-based assurance functions including internal audit, external audit, Sarbanes-Oxley units, compliance, insurance/risk management, operational risk management, financial risk management, legal, regulatory affairs, human resources, safety, environment, IT security and more. Each of these groups apply their own unique assessment methodology, technology, terminology, and reporting conventions. Over time the collective cost of assurance rises. In some large organizations the cost of these fragmented, and often un-coordinated, assurance activities is often in the billions of dollars annually. Even in smaller public companies total GRC spending is often in the millions of dollars. Proponents claim that the use of an integrated GRC approach with a common assessment and reporting methodology and reporting system has the potential to lead to significant annual savings - but only if silo-based assurance groups are prepared to change and work units are prepared to participate.
5. **IMPROVED AVOID/MITIGATE/SHARE/ACCEPT RISK DECISIONS.** By improving the overall quality of information on the true state of GRC across an enterprise senior executives and boards are better equipped to make wise decisions on how to deal with risks to the organization's objectives and exploit risk opportunities. One of the most important roles senior oversights play is deciding which risks to accept and manage through mitigation using internal controls; which risks to share with partners, insurers, and others; which risks to avoid by exiting the business line, country, business sector or other avoidance techniques; and, most importantly, which risks to just accept.

BOOGEYMAN, POT OF GOLD OR JUST GOOD BUSINESS?

Different things motivate different people in different ways. What it takes to cause people in their personal lives and organizations of all sizes in the business world to embark on major changes is both complex and simple. A simplified premise is that if the combination of pain avoided and/or pleasure provided by a new state of being is great enough it will cause a significant number of people and organizations to make the change. The speed of change will vary from rapid to glacial. Some people and some companies will never change. They will cling to old ways of doing things even in the face of irrefutable evidence that the new way of doing business is a better one, even to the point of death. This is a fact of life.

This paper sets out some of the "Boogeyman/pain avoidance" claims for integrated GRC, together with a sample of more significant "Pot-of-gold/pleasure/reward at the end of the journey" benefits. At this point in time most companies either aren't even aware of the integrated versus silo-based GRC debate, are still at the "contemplate the claims of consultants and vendors" stage. A small but growing number have taken a few tentative steps to test the integrated GRC value proposition. As is often the case a small number of pioneer/early adopters have already accepted that integrated GRC is better than silo-

based GRC and embarked on the journey, at least in part, on faith that it is the right think to do.

One last thought for you to contemplate:

In my many years in the risk and assurance sector I have not seen a single article or paper anywhere in the world that supports the position that silo-based GRC is preferable to integrated GRC. I have similarly not seen a paper that outlines why flossing ones teeth on a regular basis is a bad thing. To me this simple truth suggests that perhaps the only thing slowing the movement from silo-based GRC to integrated GRC is the human resistance to change.