CLAYTON UTZ

Governance, Risk and Compliance

What is GRC: What is its impact on compliance practices and where is GRC heading?

2013

Introduction

Well established governance, risk and compliance functions have for many years formed a key part of management practice in both the private and public sectors in Australia. A relatively new concept, "GRC", has emerged, which emphasises on building a closer inter-relationship between governance, risk and compliance, and how these functions can be further integrated to increase their effectiveness.

The purpose of this briefing paper is to examine GRC and to outline its current impact on compliance practices in both the public and private sectors in Australia. It will also sketch where GRC is heading and give an indication of likely future developments.

What is GRC?

Most organisations have functions for overseeing governance, risk and compliance frameworks and policies.

In many organisations these functions or frameworks have a separate operation and focus. Generally, the persons who have oversight of these functions are different officers who may not interact closely. For example, governance is often the province of the company secretary, risk is overseen by the chief risk officer and compliance by the head of compliance or such like.

This model has traditionally been seen as having a distinct advantage of being able to quickly establish controls and policies specific to the organisation relating to the particular governance, risk or compliance failures or key risk areas (eg. Competition and Consumer Act or environmental licence requirements).

A limitation with this approach is that it may create:

- a disconnect between governance, risk and compliance functions themselves and their interaction with their relevant organisational silos;
- inefficiencies or duplication of corporate effort, with multiple approaches to managing the same or similar risks and controls;
- inconsistency within the governance, risk and compliance frameworks themselves;
- lack of transparency and uniformity in approach across the frameworks and organisation; and
- an increased risk of unidentified gaps in these frameworks and controls.

An integrated GRC framework is almost a reversal of this traditional approach. A GRC framework does not simply centralise the GRC functions but seeks to integrate all relevant policies, processes, procedures and controls. Specifically, this approach is designed to identify and standardise common processes, procedures and controls and ensure that they are consistently rolled out throughout the organisation.

The path to integrated GRC

While there does not appear to be one path for successful GRC integration, there are a number of key factors that need to be considered when doing so.

These matters include:

Strategy

There should be a standard approach to implement corporate strategy that take into account organisational performance, goals and objectives, and GRC conformance matters (for example balanced scorecards, complimentary integrated targets and the like).

Reporting and Audit

A key aspect of implementing these initiatives is monitoring and reporting on their effectiveness. Central to this is establishing appropriate goals and targets (perhaps expressed as Key Performance Indictors (KPIs), Key Result Areas (KRAs) or the like) and their related reporting frameworks. A further important step is determining how internal and external audit interacts with these arrangements and leveraging synergies to ensure you can derive maximum benefits for all GRC aspects from these audits.

Legal function

Many organisations ensure that the senior in-house lawyer has a general counsel role which includes, in effect, providing advice on the management of the legal aspects of the reputation of the organisation. The legal section often is also involved in key strategy decisions and implementation of major corporate initiatives (for example mergers and acquisitions, restructuring, adoption of new products and services). The legal group is also responsible for providing detailed advice in delicate and difficult circumstances. As a result, organisations try to ensure that legal professional privilege applies to particular advisings and investigations. It is therefore crucial to ensure that the legal group have a clearly understood role in the GRC frameworks.

Information technology

A further factor is the ease with which information is available and managed across the organisation. In particular, a key issue is whether there are common IT platforms for use throughout the organisation to facilitate the sharing of information. This is often the province of the chief information officer whose role must also be considered with implementation of GRC frameworks.

Ethics and corporate social responsibility

Increasingly, organisations are adopting ethical and corporate social responsibility underpinnings for their organisational goals, values and desired behaviours. If this is the case, these key drivers both for corporate performance and behaviour management models (particularly remuneration and incentive arrangements) will need to be factored into the GRC model.

Corporate culture

Some leading organisations are recognising the importance of planning and mapping their organisational cultures and having planned culture change programs to achieve stated organisational cultural objectives and targets. There is increasing evidence that the organisation's culture can significantly support or hinder achieving corporate objectives. At the very least, organisational culture needs to be closely considered to ensure the smooth implementation of GRC initiatives throughout the organisation. GRC initiatives should also be designed to improve organisational culture.

Business process management

Any integration of frameworks, policies, procedures or processes call for consideration of how the best outcomes can be most easily achieved. Business process management is being used or examined by many as an important tool to achieve the greatest synergies and efficiencies.

Common elements

Organisations that have embraced GRC have found that there are a range of common elements that go right across successfully integrated governance, risk and compliance policies, processes and procedures.

These include:

(a) Objectives: There needs to be a clear understanding of organisational objectives and how GRC targets support achieving them within the mandates of the law and organisational policies. Of vital importance is the breakdown of these objectives into departmental or functional goals that form part of each staff members individual objectives.

(b) Identification of boundaries: An organisation must be able to identify and articulate the boundaries of acceptable organisational conduct to its stakeholders, particularly its staff and contractors. These include specific mandatory boundaries, such as laws and externally imposed codes of conduct, but also extend to voluntary organisational boundaries, for example adopted codes of practice, industry standards, contractual provisions and internal policies and procedures.

(c) Identification and assessment of key risks: The GRC frameworks should seek to identify, analyse and prioritise the organisation's key events and controls. The focus should be upon those events or controls that must be assessed and monitored so the organisation can meet its performance goals and objectives within its established boundaries (mandatory and voluntary).

(d) Detect, check and prevent: Organisations need to specifically develop their GRC mechanisms– the policies, processes and controls to detect and check that the organisation is keeping on track to achieve its goals and objectives. Importantly, this should focus on not only ensuring that there are adequate procedures in place to guide the organisation but also that appropriate conduct and behaviours are being demonstrated and inappropriate conduct prevented. It is therefore necessary to have separate processes to evidence, monitor and check for performance as against targets and ensuring that undesirable conduct is not occurring. Examples include whistleblower hotlines, workforce surveys, control and trigger monitoring and assessment.

(e) Continuous improvement and adjustment: Organisations are constantly changing and therefore the GRC frameworks need also continuously strive and improve and adjust. If weaknesses are discovered, or a scan of emerging issues indicates that a more fundamental change to the organisation objectives or GRC frameworks are required, then an organisation needs to focus on responding and adjusting organisational structures. Examples of this approach include regular health checks, analysis of complaints and queries, routine reviews of emerging risks and opportunities and root cause analysis.

(f) Communication and reporting: Throughout all these processes ongoing communication with all appropriate internal and external stakeholders is required. This includes the establishment of clear reporting lines and reporting frameworks to ensure that both management and the board have a clear line of sight on organisational performance and emerging issues.

Implicit in all of the above is that there is a common vocabulary, approach and organisational appetite for all GRC initiatives. This way, matters identified in one organisational area can be quickly replicated across the entire organisation. The key questions such as "What are the most important risks that we face?" or "Is our organisation compliant?" can then be answered uniformly across the organisation.

Of assistance in this process is the sharing of a common technology infrastructure to facilitate these processes, particularly GRC-friendly software.

What are the benefits of an integrated GRC approach?

Many who adopt an integrated GRC approach cite significant benefits including:

- an improvement in the quality and availability of information;
- fewer breaches and errors;
- lower costs and greater efficiencies;
- a more flexible and externally focused workforce capable of rapid change to meet customer and organisational needs;
- a greater assurance for the organisation and its Board and senior management that GRC issues are being appropriately dealt with and the organisation remains on target with its performance objectives; and
- improved levels of communication across the organisation.

Key challenges

Given these benefits as described above, what then are the key challenges to GRC integration?

- A perception by staff that the initiative may have an ulterior motive, for example a cost recovery drive or head count reduction.
- Business unit managers or middle management are fearful of losing control of their decision-making or loss of power generally.
- They also fear being marginalised as GRC responsibilities are devolved to those in lower levels of the hierarchy.
- Organisations are sometimes sceptical of the proposed targeting and measurement systems and are concerned that there will not ultimately be an appropriate return on investment, given the establishment and maintenance costs involved.
- Corporate cynicism and scepticism around the outcomes and results achieved from past planned organisational change (and management fads generally).

These are key challenges indeed, especially as successfully integrated GRC initiatives are still fairly isolated and few have occurred in Australia.

This being said, overseas experience is indicating that an increasing number of organisations are considering GRC initiatives and those that have embraced GRC report positive benefits (See "A pathway to principled performance®: The OCEG Framework Approach to Integrated GRC" (Mitchell, S., 2008. Available at http://www.oceg.org/View/20055) and the 2007 OCEG GRC Strategy Study Findings Report).

It is therefore vitally important that the GRC integration process is carefully scoped and benchmarked to ensure that the return on investment is targeted and achieved, and that the underlying implementation strategy is carefully thought through.

What are the GRC impacts upon current compliance practices?

There are a number of current significant GRC impacts upon existing compliance practices in the Australian context, including:

- Re-evaluation of functional boundaries: Many organisations are now closely reviewing what their governance, risk and compliance functions are actually doing and examining the interaction between those functions. Many are concluding that there is unnecessary duplication and effort and are looking at ways of implementing further integration in order to reduce costs and the number of invasive activities of GRC on the organisation (eg. audit, monitoring, reporting and use of a single incident escalation system). Business process management methodologies are increasingly being used as a driver for these outcomes in GRC integration.

- Corporate culture: There appears to be an increasing appreciation of the importance of corporate culture and the role that governance, risk and compliance plays in ensuring that there is a healthy corporate culture. Some organisations are now mapping their corporate culture to identify hotspots for potential problems. Leading organisations appear to be also looking at establishing corporate culture targets and planned corporate change mechanisms to achieve those targets. Most of these targets are operationalised within the GRC frameworks.

- Productivity, gains and dissatisfaction: There are currently a number of common drivers for organisations' GRC frameworks, including the need to control costs and achieve greater performance and productivity from their GRC efforts and GRC integration.

Our discussions with a number of key directors, middle management and compliance professionals across a range of our public and private sector clients indicate a rise in dissatisfaction with their non-integrated GRC efforts, in part because they cannot measure the impact of their GRC efforts or whether they achieve the results intended in the most cost-efficient manner.

As a result of this, and challenging economic times and the need for cost management, many organisations are now reviewing their GRC framework to , at best, reduce costs but ideally to identify greater efficiencies and business improvement outcomes.

Where is GRC heading?

The above OCEG research supported by the latest SAI Global research (Practitioner Issues & Trends - Risk & Compliance in Australia 2008) seems to be generally consistent with the results that we are observing amongst our clients and GRC colleagues, namely:

- More organisations are investigating or adopting a GRC model or at least seeking to combine elements of governance, risk and compliance.
- Few have indicated that they have completed this task – many have indicated that they are only just beginning to identify how they can extract the greatest value out of their GRC efforts.
- Those who have started only recently are generally finding the challenges much greater, and resistance to change far more deeply ingrained than they initially expected. In particular, many of those who sat at the head of the governance, risk and compliance silos who supported a GRC approach subsequently raised previously unidentified issues and challenges that proved to be major obstacles.
- GRC leaders have adopted a number of approaches to maximise benefits achieved, including:
- Upfront identification and ongoing measurement of detailed targets and metrics from the GRC project.
- Very clear cultural measurements and milestones as to how these targets and metrics were to be achieved. These GRC and cultural milestones were of vital importance to keep momentum. There appears to be a general acceptance that organisation culture for larger organisations will only be changed over a long term (3 to 5 year) timeframe, so it was important to renew focus on the long-term goals during incremental challenges so as to not lose commitment just as the planned benefits were delivered.
- Incremental change based around enterprise-wide projects appears to deliver greater immediate results than a single larger GRC big bang enterprise-wide project. Business process management initiatives are often also being used to drive quick wins in key processes that require updating.
- A focus on ensuring there were performance measurements rather than merely conformance measurement. This approach reportedly appears to have achieved a greater perception of value for the organisation at all levels.
- What this means is that organisations were measuring their performance as against corporate targets as well as ensuring they met their conformance boundaries (eg. your business rates 3 out of a possible 5 across a balanced scorecard, where 3-5 is a pass on a compliance scale and 5 represents best practice). Middle management in particular reported that this was a much more motivating metric since it provided feedback on how their area of responsibility was performing having to regard to organisational objectives rather than simply being told that they met a minimum compliance standard. Of course it was necessary that the performance targets included within them an appreciation of these conformance requirements, such that the minimum targeted outcome must by definition be compliant.
- Greater use of organisational Codes of Practice. These codes appear to be used to focus attention on principled compliance whereby staff are encouraged to use their codes of practice to guide their decision making in circumstances where existing process and procedures are not of assistance. Increasingly, there is greater use of principles to guide staff rather than detailed checklists.
- Codes need to be carefully drafted to assist with this process and business process management techniques are also adopted to ensure that staff obtain guidance and assistance with their decision making.

Conclusion

While GRC initiatives appear to have become more widespread, in our view, for most Australian public and private sector organisations, they are still in the early stages of their development. It is encouraging therefore that many of the GRC leading organisations report that the further that they journey down GRC implementation the greater the value that they receive.

A further query is what this convergence of governance, risk and compliance will mean to the relevant professional bodies such as the Institute of Chartered Secretaries, the Risk Management Institute of Australasia and the Australasian Compliance Institute.

However, one thing that can be said with some degree of certainty is that while GRC is new it is not a passing management fad and appears to be here to stay.

Contacts

Randal Dennings - Partner - Governance & Compliance Division

Brisbane:
Level 28 Riparian Plaza, 71 Eagle Street
Phone: (07) 3292 7017
Central fax no. (07) 3221 9669
Email: rdennings@claytonutz.com
Mob: 0408 878 711

Sydney:
Level 15, 1 Bligh Street
Sydney NSW 2000
Phone: (02) 9353 5155
Central fax no. (02) 8220 6700

Wei-Loong Chen - Special Counsel - Governance & Compliance Division

Brisbane:
Level 28, Riparian Plaza, 71 Eagle Street
Phone: (07) 3292 7252
Central fax no. (07) 3221 9669
Email: wchen@claytonutz.com
Mob: 0413 835 365

Samantha Carroll - Special Counsel - Governance & Compliance Division

Brisbane:
Level 28, Riparian Plaza, 71 Eagle Street
Phone: (07) 3292 7333
Central fax no. (07) 3221 9669
Email: scarroll@claytonutz.com
Mob: 0434 564 563

Sydney

Level 15
1 Bligh Street
Sydney NSW 2000
T +61 2 9353 4000
F +61 2 8220 6700

Melbourne

Level 18
333 Collins Street
Melbourne VIC 3000
T +61 3 9286 6000
F +61 3 9629 8488

Brisbane

Level 28
Riparian Plaza
71 Eagle Street
Brisbane QLD 4000
T +61 7 3292 7000
F +61 7 3221 9669

Hong Kong

703 - 704
The Hong Kong Club Building
3A Chater Road
Central Hong Kong
T +852 3980 6868
F +852 3980 6820

Perth

Level 27
QV1 Building
250 St. Georges Terrace
Perth WA 6000
T +61 8 9426 8000
F +61 8 9481 3095

Canberra

Level 10
2 Phillip Law Street
Canberra ACT 2601
T +61 2 6279 4000
F +61 2 6279 4099

Darwin

17–19 Lindsay Street
Darwin NT 0800
T +61 8 8943 2555
F +61 8 8943 2500

www.claytonutz.com