MANAGING LEGAL RISK IN AN INTEGRATED GRC FRAMEWORK

A BRIEFING PAPER

www.claytonutz.com
Organisations are finding that their stakeholders (particularly Boards) are seeking greater assurance of their legal risks and that governance, risk and compliance (GRC) is dealt with in an integrated manner.

This Briefing Paper explores some of the practical issues that organisations are encountering when dealing with these concerns.

Traditionally in organisations, the governance, risk and compliance functions or frameworks each have a separate operation and focus. The employees who operate or have oversight of these functions may often be located in different departments with different reporting lines. For example, an organisation’s governance arrangements may be overseen by the Company Secretary, while risk is overseen by the Chief Risk Officer and compliance by the Head of Compliance or General Counsel.

In this Briefing Paper, we will refer to this approach to governance, risk and compliance as the silo approach. While the silo approach has its strengths, its limitation 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 (for example, by using different descriptors or metrics);
► lack of transparency and uniformity in approach across the frameworks and organisation; and
► an increased risk of unidentified gaps in these frameworks and controls.
GRC is a relatively new concept which seeks to emphasise a close inter-relationship between governance, risk and compliance and how these functions can be further integrated to increase their effectiveness.

An integrated GRC approach is almost a reversal of the traditional silo approach.

A GRC framework does not seek to simply centralise the GRC functions; rather it seeks (over time) 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 implemented and acted upon throughout the organisation.

For more information on GRC, please refer to our Briefing Paper What is GRC and Where is it Heading?

The goal is a consistent approach to governance risk and compliance – particularly concerning organisational strategy and behavioural management initiatives.

Legal risk management is an integral component of an integrated GRC framework. It seeks to ensure that the organisation pursues its corporate goals and objectives within the boundaries of its legal obligations.

Within a GRC framework, legal risk management is usually the responsibility of the organisation’s legal and/or compliance function – often closely overseen and owned by the General Counsel.

Adopting a GRC approach to management of an organisation’s legal risks could lead to the following benefits:

► an increased perception of value that legal risk management adds to the organisation;
► if properly implemented, the process of developing an organisation’s legal risk management program (LRMP) can foster greater buy-in at the business level by engagement of business stakeholders and senior management to own their legal risks and the associated controls, processes and procedures;
► development of a performance model of legal risk management (ie. ensuring that the organisation is doing the right things having regard to its organisational goals), as opposed to a conformance model (ie. merely ensuring that the organisation is not doing anything wrong);
► legal risk management as documented in an LRMP integrates risk, compliance and legal planning, and thus works towards embedding them into your processes and procedures, so that they are relevant, effective, efficient, robust and sustained;
► an LRMP can also link into and support organisational business continuity, disaster recovery and crisis management plans;
► an improvement in the quality and availability of information to and from the legal and GRC team (and thereby, the wider external stakeholders, particularly senior management and the Board);
► fewer breaches and errors;
► lower costs and greater efficiencies;
► a more flexible and externally focused workforce capable of rapid change to meet stakeholder and organisational needs; and
► a greater assurance for the organisation and its Board and senior management that legal risks are being appropriately dealt with and the organisation remains on target with its performance objectives.

The goal is a consistent approach to governance risk and compliance – particularly concerning organisational strategy and behavioural management initiatives.
While there does not appear to be one approach for managing legal risks within a GRC framework, there are a number of factors that need to be considered, including:

- **Ambit of legal risk**: this is a key threshold issue. How wide is the organisation’s definition of legal risks? Are these just risks arising from legislation? Or will the organisation also consider tortious risks (for example, negligence and nuisance), key contractual obligations, reputational and political risks, as well as risks arising from its codes of conduct, internal processes and procedures?

- **Settling of organisation-wide risk tolerance**: this is another threshold issue. As a first step, the organisation’s governing and leadership bodies must define the acceptable risk levels for the organisation. For instance, what is the organisation’s desired risk tolerance? Is the desired risk tolerance level appropriate for the organisation, having regard to its activities, functions and stakeholders? What level of risk is considered unacceptable? What is the organisation’s current risk level?

- **Required level of assurance**: what level of assurance does the organisation need from the LRMP? To whom is this assurance provided? How can the required level of assurance be measured?

- **Legal function**: many organisations ensure that its senior in-house lawyer (for example, the General Counsel) is responsible for managing the organisation’s legal risks and also has a role in providing advice on the management of the legal aspects of the organisation’s reputation. In an integrated GRC framework, the legal function often is also involved in setting and maintaining the organisation’s legal risk tolerance, advising on key strategy decisions, and the legal risks associated with the implementation of fresh corporate initiatives;

- **Ethics and corporate social responsibility**: increasingly, organisations are adopting ethical and corporate social responsibility underpinnings for their organisational risk tolerances, goals, values and desired behaviours. These will need to be factored into the controls the organisation adopts for managing legal risks; and

- **Corporate culture**: there is increasing evidence that the organisation’s culture is vital in achieving (or hindering) its quest to fulfil its corporate, governance and compliance objectives. Leading organisations are recognising the importance of planning and mapping their organisational cultures and having planned culture change programs to achieve their stated cultural objectives and targets.
An effective LRMP within a GRC framework will often have the following components.

CORPORATE OBJECTIVES

There needs to be a clear understanding of organisational objectives and an ability to demonstrate how GRC targets and the LRMP support these organisational objectives within the mandates of the law and organisational policies.

STATED RISK TOLERANCE AND BOUNDARIES

An organisation must be able to identify and articulate its risk tolerance level and the applicable boundaries of acceptable organisational and legal risk to its stakeholders (particularly its staff and regulators).

LEGAL RISK MANAGEMENT POLICY

There needs to be an overarching legal risk management policy which sets out the purpose of the LRMP in the relevant organisational context, and what the organisation wants to achieve through legal risk management.

LEGAL RISK MANAGEMENT STRUCTURE

This structure will typically consist of key definitions, risk assessment criteria and a commonly agreed set of protocols to address legal breaches or incidents, or risks which are rated in excess of the organisation’s legal risk tolerance. It is crucial that the legal risk management structure is in accordance with the outputs from paragraphs (a) to (c) above.

IDENTIFIED LEGAL REQUIREMENTS

These include the identification of specific mandatory legal requirements that apply to the organisation, such as laws and externally imposed codes of conduct. For an organisation’s LRMP to be truly effective and meaningful, this should also extend to voluntary organisational requirements, for example adopted codes of practice, industry standards, contractual provisions and internal policies and procedures. These legal requirements are usually documented in a “Legal Obligations List” or “Obligations Register”.

IDENTIFICATION AND ASSESSMENT OF KEY LEGAL RISKS

The LRMP should seek to identify, analyse and prioritise the management of the organisation’s key legal risks and controls. The focus should be upon those legal risks that must be assessed and monitored so that the organisation can meet its performance goals and objectives within the established boundaries of its legal obligations (mandatory and voluntary). The key legal risks are usually documented in a “Legal Risk Register”.

DETECT, CHECK AND PREVENT

Part of managing an organisation’s legal risks is putting in place policies, processes and controls to detect and check that the organisation is effectively discharging its legal requirements. The identification of any control gaps is also important in this step. Importantly, legal risk management focuses not only on ensuring that there are adequate controls to address legal risks, but also that appropriate conduct and behaviours are being evidenced 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. The policies, processes and controls can be documented in the Legal Risk Register, or organisations may choose to document these in “Legal Risk Management Treatment Plans”.

CONTINUOUS IMPROVEMENT AND ADJUSTMENT

LRMPs need to continuously strive to improve and adjust. If incidents or breaches are discovered, a new corporate initiative or project is to be launched, or there is a fundamental change to the organisation’s objectives or legal obligations, the LRMP needs to be able to respond and adjust. This can accomplished by health checks, analysis of legal issues and incidents, routine reviews of emerging legal risks, projects and opportunities and root cause analysis of any legal breaches.

COMMUNICATION AND REPORTING

Throughout all of the above processes, ongoing communication with all appropriate internal and external stakeholders is crucial. This includes establishing reporting lines and reporting arrangements to ensure that both management and the board have a clear line of sight on the organisation’s legal risks and emerging concerns. Decisions made by the organisations in the above processes (and the underlying reasons for these decisions) and current versions of any documents and registers produced should be kept in a legal due diligence file.
While there is no one correct implementation method, we have noted that GRC leaders who have reported sound results tended to have included at least the following nine steps in their implementation program.

**STEP 1: Internal briefings**
Conduct internal briefings with key executives and other stakeholders upfront to appropriately position and raise awareness of your LRMP implementation initiatives.

**STEP 2: Identification of key business representatives and other internal stakeholders**
Identify key representatives and other internal stakeholders which could potentially form part of the LRMP project.

**STEP 3: Appointment of a senior business sponsor**
Appoint a senior business sponsor to the project who possesses sufficient clout and can invest in seeing the LRMP project through to conclusion.

**STEP 4: Development of the LRMP**
Conduct an audit of the organisation’s activities, structure, emerging and over-the-horizon legal issues and changes in the business, review of existing compliance, legislation and complaints matrices.

**STEP 5: Validation and testing**
Develop the first cut of the LRMP for feedback and testing with the LRMP project working group and other key stakeholders (otherwise known as the "straw man" approach).

**STEP 7: Develop an implementation plan**
This includes allocating business and control owners to Risk Treatment Plans, training, monitoring and ongoing reporting structures.

**STEP 8: Rollout of implementation plan**
Rollout the implementation plan with ongoing monitoring, reporting and adjustment as required.

**STEP 9: Post-implementation review**
Set a date and plan for a post-implementation review to test the effectiveness of the LRMP. This may consist of checking that appropriate controls are in place, reviewing reporting and any incidents identified during the implementation period. Following the post-implementation review, the LRMP would need to be adjusted in the light of any outcomes of the review and feedback from the business.

**HOW IS IT IMPLEMENTED?**

Specifically, we suggest this step would consist of meeting with key business representatives and other internal stakeholders identified under Step 2 to workshop the LRMP for brainstorming, critiquing and validation.

Organisations should adopt a measured approach to implementation and resist quick fixes, as this ensures sound change management methodologies, the changes stick, and they will have wide business buy-in and acceptance.
CONCLUSION

This paper provides a high-level discussion of how we see legal risk management operating within an integrated GRC framework and some associated practical issues.

We have had the privilege of assisting many organisations in both the public and private sectors with their development implementation review and upgrading of these projects and wider GRC initiatives.

While like any significant change management program there are always challenges to be overcome, in our view GRC leaders have found the journey worthwhile. Significantly they have formed this view from their discovery that these projects have also delivered significant organisational efficiencies and performance benefits.

In economically uncertain times they have found a greater business resilience when dealing with their legal risks.

We trust that this Briefing Paper also points the way for your organisation to reap these rewards.

KEY CONTACTS

For further information, please contact:

Randal Dennings
Head Partner
T +61 7 3292 7017 (Brisbane)
T +61 2 9353 5155 (Sydney)
M 0408 878 711
rdennings@claytonutz.com

Samantha Carroll
Special Counsel, Brisbane
T +61 7 3292 7333
M 0434 564 563
scarroll@claytonutz.com

Wei-Loong Chen
Special Counsel, Brisbane
T +61 7 3292 7252
M 0413 835 365
wchen@claytonutz.com