Legal risk — what, why and how?

By Duncan Ramsay, Lawyer and Consultant

- The meaning of legal risk is often assumed.
- Effectively dealing with legal risk increases an organisation's ability to achieve its goals by way of greater efficiencies.
- The risk management process involves establishing the context; conducting a risk assessment; identifying the risks; analysing the risks; evaluates the risks; and then treating the risks.

People talk about legal risk. But what is it really? And why is it important? How do you minimise it?

What

References to legal risk often assume its meaning is obvious. The joint judgment of the New South Wales Court of Appeal in *Morley & Ors v ASIC* [2010] NSWCA 331 mentions legal risk eleven times without definition when stating it was the duty of James Hardie's general counsel and company secretary to protect it from legal risk. Sheryl Sandberg, chief operating officer of Facebook, in her 2013 book *Lean In* writes about legal risk ('The first time I asked a prospective employee if she was considering having children soon, I knew that doing so could expose me and my company to legal risk' p 151).

My description of legal risk is:

> 'the extent to which the law will adversely affect the organisation from achieving its objectives, where the organisation did not consider the law, wrongly believed the law to be different, is subject to an adverse judgment that is contrary to advice received or is uncertain as to the law.

Legal risk can be from either mandatory or voluntary sources (examples of the former are case law and statutes and instances of the latter are contracts and the organisation's code of conduct).

Legal risk can involve a claim, change in law, defective transaction (including bad due diligence, an unconsidered exposure in a contract and poor structuring) or inadequate asset protection (such as not registering a security interest or trademark).

Legal risk can result in civil and criminal sanctions for the company and individuals as well as loss of reputation (including losing customers, a lower share price and write downs of goodwill).

Legal risk management in turn involves the organisation providing goods or services that maximise its opportunities while minimising failure to comply with the requirements of the law, including of a court or a regulator.

Very importantly, legal risk management does not mean avoiding legal risk altogether. Rather it involves identifying legal risk, facing risks deliberately, not taking unnecessary risks and carefully managing the risks that the organisation decides to accept.

The Basel Committee on Banking Supervision sees legal risk as part of operational risk, namely the risk of financial loss resulting from inadequate or failed internal processes, people and systems or from external events. This view has influenced the Australian Prudential Regulation Authority (APRA) and other regulators.

Operational risk is seen as different from other risks such as strategic, credit, market, investment or liquidity risks.

Legal work by its nature involves operational risk, whereas other risks are more for others (such as strategic risk and management consultants).

However, risk categories are somewhat arbitrary. The main point is to be thinking afresh and contributing to the organisation's business by identifying a risk, be it legal or not, and then agreeing on steps to manage the risk.

Why

Risk management is topical, especially to regulators.

ASIC published regulatory guide 247 on effective disclosure in an operating and financial review (OFR) of a listed entity on 27 March 2013. Its paragraph 61 defines material business risks as the most significant areas of uncertainty or exposure at a whole of entity level that could have an adverse impact on the achievement of financial performance or outcomes referred to in the OFR.

This comment is in reference to section 299A(1) of the *Corporations Act 2001* which provides for a listed entity's annual directors' report to include information that its members would reasonably require to make an informed assessment of the business strategies and prospects for future financial years.

As a result, listed companies' annual reports last year expanded their commentary on material business risks. Three examples are BHP Billiton, Commonwealth Bank of Australia and Caltex Australia.

Secondly, APRA revised its prudential standard CPS 220 on risk management during 2014 and its accompanying prudential practice guide (both are effective from 1 January 2015).

In particular, paragraph 13 of CPS 220 requires the board to ensure that:

a) it sets the institution's risk appetite within which it expects management to operate and approves a risk management strategy (RMS)

b) it forms a view of the institution's risk culture and the extent to which that culture supports the risk appetite

c) senior management monitors all material risks consistent with the strategic objectives, risk appetite statement and policies approved by the board

The main point is to be thinking afresh and contributing to the organisation's business by identifying a risk, be it legal or not, and then agreeing on steps to manage the risk.

d) the operational structure of the institution facilitates effective risk management

e) policies and processes are developed for risk-taking that are consistent with the RMS and the established risk appetite

f) sufficient resources are dedicated to risk management

g) it recognises uncertainties, limitations and assumptions attached to the measurement of each material risk.

Paragraph 20 of CPG 220 defines material risks as those that could have a material impact, both financial and non-financial, on the institution or the interests of depositors or policyholders. Like ASIC, APRA refers to 'could', not a higher threshold of 'would' in determining materiality.

Thirdly, the ASX Corporate Governance Council issued the third edition of its *Corporate Governance Principles and Recommendations* on 27 March 2014. These include 'if not, why not' recommendations on risk management:

- 7.1 (in summary) the board of a listed entity should (a) have a committee or committees to oversee risk and disclose its charter and (b) if it does not have a risk committee, disclose that fact and the processes that it employs for overseeing the entity's risk management framework
- 7.2 the board or a committee of the board should (a) review the entity's risk management framework at least annually to satisfy itself that it continues to be sound and (b) disclose, in relation to each reporting period, whether such a review has taken place
- 7.3 a listed entity should disclose (a) if it has an internal audit function, how that function is structured and what role it performs and (b) if it does not have an internal audit function, that fact and the processes it employs for evaluating and continually improving the effectiveness of its risk management and internal control processes and
- 7.4 a listed entity should disclose whether it has any material exposure to economic, environmental and social sustainability risks and, if it does, how it manages or intends to manage those risks.

The recommendations apply to financial years from 1 July 2014.

These developments provide a framework for boards to establish, support and monitor risk management practices across a broad spectrum and make management responsible for their effective functioning. These steps include drafting board and committee charters, updating compliance programs as well as other policies and procedures, together with providing general comments on corporate governance, especially the responsibilities of non — executive directors compared with management.

Governance practitioners are already familiar with risk. Its allocation is a common issue in contracts, through indemnities, limitation of liability clauses and otherwise. Being involved in disputes includes assessing prospects of success.

Governance practitioners should be able to demonstrate that sensibly dealing with legal risk increases an organisation's ability of meeting (if not exceeding) its goals by way of greater efficiencies,

through lower costs, less errors, fewer surprises, improved decision — making and better customer, employee and supplier relationships.

How

The general risk management process under AS/NZS ISO 31000: 2009 is to establish the context; conduct a risk assessment; identify the risks; analyse the risks; evaluate the risks; and then treat the risks. This will involve communication and consultation together with monitoring and review.

In terms of legal risk, this process includes a legal risk audit, a legal risk plan and reporting.

As for a legal risk audit, this looks at the current state of an organisation's legal risk. Areas to consider include relevant statutes, current contracts (standard form and otherwise), litigation (present and pending) and regulatory proposals. Items to review include the jurisdictions where the organisation operates, potential legal exposures and the litigation culture of the jurisdiction, always bearing in mind the organisation's particular business and customer base.

A legal risk audit will usually produce a legal risk register. This could comprise a spreadsheet with columns for the relevant risk, its source, its likelihood and consequence, its inherent risk (pre control), its control, the residual risk (post control) and monitoring (how, when and by whom).

Two crucial concepts are likelihood and consequence. These can be rated on a scale (one to five is common) in a grid diagram with likelihood on the left axis and consequence on the bottom axis. Often the consequence of legal risk is relatively fixed, especially if its source is statutory (for example, fines). This means the emphasis should be on likelihood, through the organisation's or its competitors' experience or even legal precedent.

The spreadsheet can also be sub-divided into which business units of the organisation are say high, medium or low in terms of the particular legal risk.

A legal risk plan follows from the outcome of the legal risk audit. It can involve either accepting the risk entirely or transferring the risk in whole or in part through insurance and outsourcing after a cost/benefit analysis. Materiality and priority will need to be decided. Avoiding a legal risk is usually not possible (clearly not for mandatory obligations).

Compliance programs are a common feature of a legal risk plan. The courts and regulators will give credit to such programs in the event of a breach (some statutes may provide for the organisation to take reasonable steps to comply or for a due diligence defence).

For organisations which are financial institutions, APRA's CPS 220 requires they have a RMS management strategy. The legal risk plan can be incorporated within this strategy.

Reporting may be either ad hoc or regular and can be divided into information from a governance professional alone or as part of another's report. One example is a quarterly memorandum to say the risk committee on what risks have occurred and what happened from them.

Another example is to focus on emerging risks by writing on material recent legal developments applicable to the organisation. Apart from new case law and legislation, legal actions by or against competitors could affect the organisation directly by way of copycat claims or the industry indirectly through regulatory change.

A third example is a management report on a contractual, employee or other dispute having an appendix from a lawyer subject to client legal privilege of any investigation as to the merits of the complaint or an update of any court action.

Governance practitioners should be able to demonstrate that sensibly dealing with legal risk increases an organisation's ability of meeting if not exceeding its goals by way of greater efficiencies…

In each example, changes may follow to the legal risk plan.

Conclusion

Governance practitioners by their training are well suited to advising on risk management. They can contribute by giving their perspective — the end result does not have to be a separate category for legal risk.

Duncan Ramsay can be contacted on (02) 9437 5595 or by email at damr1962@icloud.com.