LexisNexis

Australian
Banking & Finance Law Bulletin

2014 . Vol 30 No 10

Contents

General Editor
Karen Lee
Principal and Consultant, Legal Know-How

Editorial Board
Mark Hilton
Partner, Henry Davis York, Sydney
David Richardson
Partner, HWL Ebsworth Lawyers, Sydney
David Turner
Barrister, Owen Dixon West Chambers, Melbourne
Nicholas Mirzai
Barrister, Level 22 Chambers
John Mosley
Partner, Minter Ellison, Sydney
David Carter
Partner, DibbsBarker, Sydney
Samantha Carroll
Special Counsel, Clayton Utz, Brisbane
John Naughton
Partner, King & Wood Mallesons, Perth
Leonie Chapman
Principal Lawyer and Director, LAWYAL Solicitors

Information contained in this newsletter is current as at December 2014

LexisNexis Butterworths

Australian
Banking & Finance
Law Bulletin

Enterprise risk management for banking lawyers

Graeme Willis *HSW CAPITAL*

Lawyers play a pivotal role in the risk management arena. This is especially true for banking lawyers operating in an in-house environment, such as those employed by investment banks, home loan lenders, credit unions and trustee corporations. So many of the risks organisations face are associated with the legal framework, regulatory requirements and compliance in general, or have implications in these areas. What makes it even more relevant is the speed of change both within the organisation's own operations and in the external environment. This can crystallise new and significant risk with profound implications if not quickly indentified and acted upon. New and disruptive technologies are emerging regularly, regulatory change seems endless, and the fragility of the global economic environment remains present. In this environment, it is important to take time out from the day-to-day operations of the business to reflect on the identified and emerging risks. A sound enterprise risk management approach is not only beneficial, but can be essential.

The development of enterprise risk management over the last 10 years has been significant. The events of the global financial crisis in the late 2000s bought home with devastating consequences the need to fully understand and manage risks inherent in the operations of any organisation, including law firms, leaving a legacy of case studies and lessons from the numerous inquiries, investigations and subsequent reports.

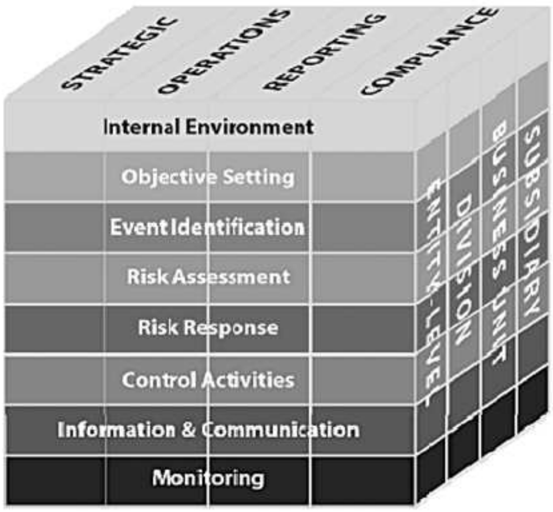
One of the lessons from this period is that the risks of an event were often understated by not recognising the correlated risks associated with the event. An example could be a breach of data security (and all banking lawyers would be familiar with how this relates to legislation such as the Privacy Act 1988 (Cth), with new changes commenced in March 2014), which, when assessed as an operational risk matter, takes into account the cost of rectification of data systems, control frameworks, customer notifications, and possible liability or compensation. What had the propensity to be missed in this environment was the loss of revenue from a disaffected customer base, or the loss of revenue from management being distracted from the operations of the organisation while managing a crisis. The reasons why the correlated risks and impacts are not always recognised is that organisations often manage risks in silos (operational, credit, legal and so on) and, due to the limitations of the management structure, have an inability to recognise or to evaluate the total impact on the organisation.

In its most simplistic form, what started out as a credit issue (subprime debt) for the financial services sector developed into a liquidity risk, which was substantially more severe for many institutions than the credit risk of the subprime debt exposure. Organisations that were able to foresee and duly consider these correlated risks were able to take pre-emptive action to mitigate the position. A lawyer advising a financial institution could help anticipate and contemplate these risks, and could play a key role in alleviating a potential disaster. As the global financial crisis unfolded, mitigating strategic options were closed down or substantially repriced, which provided the early adopters with a financial and strategic advantage.

For enterprise risk management, there are different approaches and models developed by various organisations. While I believe that there is no single model for all entities and all situations, the COSO model[1] shown in fig 1 has been well developed and is a comprehensive framework for considering the topic.

The four categories of objectives — strategic, operations, reporting and compliance — are represented by the vertical columns, the eight components by horizontal rows, and an entity's units by the third dimension. This depiction portrays the ability to focus on the entirety of an entity's enterprise risk management, or by objectives category, component, entity unit or any subset thereof.

Figure 1: Critical components of COSO model



The COSO model defines and reflects certain fundamental concepts. Enterprise risk management is:

- a process, ongoing and flowing through an entity, be it a bank, a professional services firm such as a law firm, or some other entity;
- effected by people at every level of an organisation — for example, in the case of a law firm, this would include not only lawyers at partnership level, but also lawyers at relatively more junior levels; in the case of a bank, it would include not only senior management, but also the in-house legal team;
- applied in a strategy setting;
- applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk;
- designed to identify potential events (such as a change in the regulatory landscape, famously represented by the introduction of the new personal property securities regime in Australia) that, if they occur, will affect the entity, and to manage risk within the entity's risk appetite;
- able to provide reasonable assurance to an entity's management and board of directors; and
- geared to achieve objectives in one or more separate but overlapping categories, including but not limited to legal objectives.

While the framework is an important component of enterprise risk management, the most significant value added is provided by organisational culture and management execution. The framework will facilitate the considerations and conclusions. However, what matters most is the quality of the management's knowledge of the firm's operations and activities and the ability to fully understand the primary, secondary and tertiary impacts of the risks inherent in the operations. The secondary and tertiary impacts may occur in separate divisions, business units or subsidiaries, where the different objectives, incentives and management structures may inhibit transparency of the total impact at the entity level.

My observations also lead me to believe that the effectiveness of the enterprise risk management framework can be enhanced or diminished by the following. In many cases, what a lawyer has to offer in terms of knowledge and skill could enhance the effectiveness of enterprise risk management of the firm or organisation he or she works for:

- the quality of the governance framework within the organisation;
- the degree of articulation and understanding of risk appetite agreed by the board;
- a culture that allows risk decisions to be taken at the appropriate level within the organisation, having consideration for the trade-off between risk and return — this can be impacted by management structures, objective setting and incentive arrangements;
- a culture that allows and encourages open collaboration across management structures;
- the clear identification of the causality of each risk and the ability to monitor that causality and take available action to mitigate the risk if it threatens to exceed the risk appetite of the organisation; and
- the ability to quantify the impact of inherent risks within the organisation.

The use of well-framed scenarios is one method to assist in the quantification of the impact of inherent risks that any entity faces. What is important in determining the assumptions for the scenario is that it has the input from management across all areas of operations, and the partnership (in the case of law firms) and board (in the case of an organisation such as a bank) agrees with them. It is also beneficial to adopt for each scenario a different level of severity and likelihood to provide a sense of impact. The output for each scenario is shared with other areas of the entity to test and establish the levels of correlations across the entity.

Graeme Willis
Managing Partner
HSW Capital
Banking and Insolvency Industry Advisor,
Encompass Corporation
graemew@encompasscorporation.com
www.encompasscorporation.com

About the author
Graeme Willis has *over 40 years of experience in the banking sector, including multiple board and group executive positions within major European and Australian banks. Graeme is currently the Managing Partner at HSW Capital Pty Ltd. He sits on the Industry Advisor Panel for Encompass Corporation.*

Footnotes

1. Committee of Sponsoring Organizations of the Treadway Commission *Enterprise Risk Management — Integrated Framework: Executive Summary* September 2004 p 5, available at www.coso.org.