The Role of the Lawyer in Enterprise Risk Management and Risk Assessments

The identification and mitigation of risks have become, in the last several years, critical functions for boards of directors, executives and the professionals advising them. “Risk” has, of course, always existed and is not necessarily a “bad thing”. The mitigation of risk is also not new. The identification of risk in a systemic manner and its mitigation is something, though, that has developed substantially as a basic management and governance tool in recent years.

The use of an enterprise risk management approach has become mandatory in a number of sectors in the 21st century. The financial services sector in Canada has become accustomed to risk management, including enterprise risk management. The ability of the Canadian banking sector to withstand the economic difficulties post-2008 has been attributed in large measure to (i) a comprehensive risk management approach adopted by the sector in the late 20th century in response to its regulators, and (ii) a comprehensive risk assessment by federal regulators that resulted in measures that were to be taken by the sector in response to the financial situation.

The use of a risk-based approach to regulation is becoming much more common in gaming – whether it involves FINTRAC’s guidance for anti-money laundering purposes, the recommendations of the British Columbia auditor in its review of the British Columbia Lottery Corporation and the BC Gaming Policy and Enforcement Branch, or the more comprehensive approach in Ontario’s Registrar’s Standards and Requirements. Gaming operators and gaming suppliers are being pulled towards a risk-based approach, including enterprise risk management, by regulators and pushed in a complementary direction through modern governance measures and securities law obligations, institutional investors, internal and external auditors and others.

Lawyers are, of course, professionals who provide advice on risk and are recognized as having skills, training and experience that are relevant to risk assessments. But this experience is very often transactional in nature, such as the risks of litigation arising from a potential breach of contract. Nevertheless, lawyers have a potentially strong role to play in risk identification and mitigation, including in an enterprise risk management model.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has had a substantial influence in highlighting the importance of risk management.1 The COSO framework, which is used not only in the United States but also in Canada and elsewhere, involves five components – a control environment, risk assessment, control activities, information and communication, and monitoring. An integrated framework for Enterprise Risk Management (ERM) is a foundational function to allow management to evaluate and improve risk management. The underlying purpose of the ERM framework is to achieve the strategic, operational, reporting, and compliance objectives of the entity.

Risk assessment, in this context, has been described as:

… a systematic process for identifying and evaluating events (i.e., possible risks and opportunities) that could affect the achievement of objectives, positively or negatively. Such events can be identified in the external environment
(e.g., economic trends, regulatory landscape, and competition) and within an organization’s internal environment (e.g., people, process, and infrastructure). When these events intersect with an organization’s objectives—or can be predicted to do so—they become risks. Risk is therefore defined as “the possibility that an event will occur and adversely affect the achievement of objectives.”

ERM is an initial and essential step in risk management. COSO describes ERM as “a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and 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 achievement of entity objectives.”

A key intention of the ERM Integrated Framework is to achieve the business objectives of the entity — including those related to compliance with the law, regulation and standards. A role for the lawyer is perhaps obvious in this context — the identification of what those legal and regulatory requirements are for which the entity must be able to demonstrate compliance. Legal advice and communication are both ensuring legal compliance and achieving business objectives. But to do so in an effective way, the lawyer needs to understand enterprise risk management and the integrated framework, which will build on the lawyer’s existing skills, training and experiences.

A lawyer, in the context of an enterprise risk management approach, is able to articulate for the client what is a reasonable and defensible mitigation strategy in light of the possible in the sector or sectors in which the entity operates. Clients in highly-regulated sectors, such as gaming, will have a lower risk appetite — in particular with compliance with gaming laws — than in other sectors. The approach, though, recognizes that the client has defined through a rigorous process its risk appetite and that it recognizes the business and legal consequences of its decisions.

Donald Bourgeois is a lawyer practising in gaming law and a principal of Gaming & Regulation Group Inc. He was General Counsel for the Alcohol and Gaming Commission of Ontario for 10 years and can now be reached at DonBourgeois@gmail.com.