Risk management

Role of the board

Risk management is the culture, processes and structures that are directed towards taking advantage of potential opportunities while managing potential adverse effects. Risk management begins with understanding the risk appetite. The board's role is to set the risk appetite of the organisation and then to ensure it has a risk management framework to identify and manage risk on an ongoing basis.

All organisations must take risks to create value. The question is how much and what types of risk should they take? Risk appetite is the mutual understanding between management and the board regarding the drivers of, and parameters around, opportunity-seeking behaviour. A balanced approach to value creation means the organisation accepts those risks that are prudent to undertake and which it can reasonably expect to manage successfully or handle the consequences of the occurrence.

The board is ultimately responsible for an organisation's risk management framework. Management are responsible for designing and implementing the framework. The board's role is to ensure the framework is sound and to oversee the effective operation of the framework. Since the global financial crisis, there is a greater focus by boards, their auditors and regulators on risk management.

Corporate Governance Principles

The ASX Corporate Governance Council *Corporate Governance Principles and Recommendations 3e* (2014) ('ASX Recommendations') in most respects are not mandatory, rather operating on an if not, why not basis. However, they do provide the benchmark against which all companies should measure and evaluate the effectiveness of their corporate governance policies, procedures and practices. The ASX Recommendations contain a number of recommendations concerning risk and the board.

Principle 7 of the ASX Recommendations provides that:

> *"The board of a listed entity is ultimately responsible for deciding the nature and extent of the risks it is prepared to take to meet its objectives.*
>
> *To enable the board to do this, the entity must have an appropriate framework to identify and manage risk on an ongoing basis. It is the role of the management to design and implement that framework and to ensure that the entity operates within the risk appetite set by the board. It is the role of the board to set the risk appetite for the entity, to oversee its risk management framework and to satisfy itself that the framework is sound."*

" The ASX Recommendations suggest that a risk committee can be an efficient and effective mechanism to bring the transparency, focus and independent judgement needed to oversee the entity's risk management framework."

Risk management committee

For larger companies, one way for the board to focus on risk management is to establish a risk management committee. The ASX Recommendations suggest that a risk committee can be an efficient and effective mechanism to bring the transparency, focus and independent judgement needed to oversee the entity's risk management framework.

The role of the risk committee is to report to the board on risk management activities, including making recommendations to improve the framework and to bring any issues to its attention. The committee would, in practice, work closely with management to ensure that the board and/or the committee receive adequate reporting on the organisation's risks.

What are the key design elements of an effective risk management framework?

The board establishes the organisation's risk appetite. The board (or the board's risk management committee) should establish a risk management framework that provides mechanisms for:

- identifying risks including any emerging risks;
- the regular review of the risks facing the organisation and the updating of the organisation's risk registers;
- determining the materiality of those risks and the development of a plan to minimise the impact of such risk on the organisation;
- formulation and updating of the organisation's risk management processes and procedures to address the significant risks;
- monitoring that the risk culture of the organisation is consistent with the board's risk appetite and risk priorities;
- monitoring the extent to which the organisation's risk management processes and procedures have been implemented and operating effectively; and
- monitoring and evaluation of the personnel within the organisation responsible for risk management.

What are the types of risks to be considered?

The types of risk which have to be considered will vary enormously from business to business and industry to industry. Common sense indicates that the risks faced by an organisation should be categorised in relation to what the organisation does. By definition, they include things that are not easy to predict. For example, until recently, few members of the travel industry would have worried about ash from volcanoes in Iceland. The best way to approach this is to classify the categories of risk.

The following list of frequently used risk categories.

- **Financial** – includes cash flow, budgetary requirements, tax obligations, creditor and debtor management, remuneration and other general account management concerns.
- **Equipment** – extends to equipment used to conduct the business and includes everyday use, maintenance, depreciation, theft, safety and upgrades.
- **Organisational** – relates to the internal requirements of a business, extending to the cultural, structural and human resources of the business.
- **Security** – includes the business premises, assets and people. Also extends to security of company information, intellectual property, and technology.
- **Legal and regulatory compliance** – includes legislation, regulations, standards, codes of practice and contractual requirements. Also extends to compliance with additional 'rules' such as policies, procedures or expectations, which may be set by contracts, customers or the social environment.
- **Reputation** – entails the threat to the reputation of the business due to the conduct of the entity as a whole, the viability of products/services, or the conduct of employees or others associated with the business.
- **Operational** – covers the planning, daily operational activities, resources (including people) and support required within the a business that results in the successful development and delivery of products/services.
- **Contractual** – meeting obligations required in a contract including delivery, product/service quality, guarantees/ warranties, insurance and other statutory requirements, non-performance.
- **Service delivery** – relates to the delivery of services, including the quality of service provided or the manner in which a product is delivered. Includes customer interaction and after-sales service.
- **Commercial** – includes risks associated with market placement, business growth, product development, diversification and commercial success. Also to the commercial viability of products/services, extending through establishment, retention, growth of a customer base and return.
- **Project** – includes the management of equipment, finances, resources, technology, time frames and people involved in the management of projects. Extends to internal operational projects, business development and external projects such as those undertaken for clients.
- **Workplace safety** – Every business has a duty of care underpinned by State and Federal legislation. This means that all reasonable steps must be taken to protect the health and safety of everyone at the workplace. Workplace health and safety is integrated with the overall risk management strategy to ensure that risks and hazards are always identified and reported. Measures must also be taken to reduce exposure to the risks as far as possible.
- **Stakeholder management** – includes identifying, establishing and maintaining the right relationships with both internal and external stakeholders.
- **Client** - customer relationship – potential loss of clients due to internal and external factors.
- **Strategic** – includes the planning, scoping, resourcing and growth of the business.
- **Technology** – includes the implementation, management, maintenance and upgrades associated with technology. Extends to recognising critical IT infrastructure and loss of a particular service/function for an extended period of time. It further takes into account the need and cost benefit associated with technology as part of a business development strategy.

What are some choices for dealing with risk?

Determining the most appropriate method to deal with the risks facing an organisation will depend on the nature of those risks. In general terms, an organisation will have a choice between:

- Avoiding the risk by discontinuing the activity that generates it;
- Preventative control that reduces the likelihood of the risk occurring (for example, only allowing new business initiatives to proceed if they have been assessed and approved from a business risk perspective);
- Corrective controls that reduce the consequences of the risk if it occurs (for example, contingency planning, back-up systems, business continuity plans);
- Transferring the risk to another party (for example, by contract, insurance, outsourcing, joint ventures or partnerships);
- Accepting the risk and having plans in place in case the risk eventuates.

Other important considerations

Establishing an internal audit function is another important consideration in designing an effective risk management framework. An internal audit function can assist the board in overseeing the effective implementation and operation of the organisation's risk management framework. In particular, an internal audit function can provide a board with valuable assurance that key risk mitigating strategies including internal controls are operating effectively. A proactive internal audit function can also provide valuable benchmarks and insights into how to improve the effectiveness of the organisation's risk management framework.

About us

The Australian Institute of Company Directors is committed to excellence in governance. We make a positive impact on society and the economy through governance education, director development and advocacy. Our membership includes directors and senior leaders from business, government and the not-for-profit sectors.

For more information **t:** 1300 739 119 **w:** companydirectors.com.au

05446-5-12_16