ORGANISATION

Risk management

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 of the company. 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.[1]

All organisations must take risks to create value. The question is how much risk and what kind of risk will the company decide to 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 those 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 is 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. This focus has increased more recently with the release of the Final Report of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (Banking Royal Commission).

Corporate governance principles

The ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations*[2] (ASX Principles), in most respects are not mandatory but rather operate on an if not, why not basis. However, they do provide the benchmark that companies can measure and evaluate the effectiveness of their corporate governance policies, procedures and practices against. The ASX Principles contain recommendations concerning risk and the board.

---

1. For a more comprehensive examination of how a board might review its risk governance, refer to the Australian Institute of Company Directors, *Improve your board's effectiveness: Governance Analysis Tool*, 2016, **https://aicd.companydirectors.com.au/-/media/cd2/ resources/advisory/pdf/05637-1-part-gat-promo-brochure-gat-standard-a4-4pp-web.ashx**, (accessed 18 February 2019).
2. ASX Corporate Governance Council, 2019, *Corporate Governance Principles and Recommendations*, 4th edition, February, **https://www.asx.com.au/documents/asx-compliance/cgc-principles-and-recommendations-fourth-edn.pdf**, (accessed 8 May 2019).

Principle 7 states that a listed entity should establish a sound risk management framework and periodically review the effectiveness of that framework. It makes four specific recommendations:

1. That the board of an entity has a risk committee and discloses same (or the reasons why there is no such committee);

2. That the risk committee or the board review, at least annually, the entity's risk management framework to ensure that is sound and within the risk appetite set by the board and to make a disclosure whether or not that review has taken place;

3. A listed entity is to disclose whether or not it has an internal audit function, and if so, its structure and role. If not, the entity ought to disclose that fact and its alternative governance processes regarding risk management and internal control purposes; and

4. A listed entity is to disclose whether it has any material exposure to environmental or social risks and if so, how those risks are managed or intended to be managed.

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 Principles 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 will, 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, with the guidance of the board's risk management committee if one exists, will 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.

> 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 six steps for effective enterprise risk management[3] can be summarised as follows:

1. Identify the company's risks: the specific risks that the particular enterprise of your company is exposed to;

2. Create a risk library: map the risks and set out their characteristics within a common repository for all directors, executives and employees to access and to enable an understanding of the company's risk approach and awareness;

3. Identify the persons responsible for each risk within the risk library;

4. Identify the controls to mitigate and reduce risks;

5. Assess the risk impact:

   a. is it significant and, if so, what is the measure of that significance? For example, this will almost always include a quantification of the likely financial cost; and

   b. measure the risk by the best means possible and assess the likely residual after implementation of the risk strategy. This may include modelling the risk or seeking expert assistance for particular risks;

6. Treat the risk management framework as a living, responsive institution within the company and reassess it regularly, and at least annually, to ensure that:

   a. the risk assessment is an accurate reflection of the company's actual activities;

   b. the risks and controls are accurate and that those responsible are managing the risks as anticipated and in accordance with the company's governance framework;

   c. the risk reporting process is accountable and transparent; and

   d. testing of risks and conflicts occurs regularly for those risks with the most exposure.

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.[4] Common sense dictates that the risks faced by an organisation will be categorised in relation to the organisation' activities and product. By definition, they include things that are not easy to predict. For example, it is probably fair to suggest that, until relatively recent times, the possibility of ash from volcanoes in Iceland affecting travel plans were not high on the agenda (or even present on the risk horizon) for those assessing risk in that industry. The best way to approach this is to classify the categories of risk.

The following is a 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.

3. M Corbett, 2015, *6 steps to a good risk assessment process*, Gen Re Enterprise Risk Management, 23 November, **http://www.genre.com/knowledge/blog/steps-to-a-good-risk-assessment-en.html**, (accessed 18 February 2019).

4. D Stuart, "Evolving risk", 2017, *Company Director*, 1 May, AICD, **https://aicd.companydirectors.com.au/membership/company-director-magazine/2017-back-editions/may/evolving-risk**, (accessed 18 February 2019).

- **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 business that results in the successful development and delivery of products/services.

- **Market** – (note "operational" above) includes public perception risk and place in market factors.

- **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 health and 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.

- **Environmental** – includes the exposure to potential environmental hazards and possible changes that might impact on the company.

Companies that are larger tend to have more exposure. One strategy for dealing with the many risks that are identified following a review is to consider grouping the risks into fewer categories as a function of the company's operations and current information systems and then to drill down into the specifics. This will also assist with staff allocation to manage risks and with reporting back to committees where it is necessary to establish sub-committees.

"

Common sense dictates that the risks faced by an organisation will be categorised in relation to the organisation's activities and product.

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.

Consider the use of graphics and spreadsheets to summarise the risk management plan, as well as the elements making up the plan. Some plans will lend themselves to graphic representation: for example, for an international organisation seeking to set out country risk, a geographic map will assist. However, even a moderately sized business will benefit from a spreadsheet identifying and explaining the risks and assigning responsibilities as well as setting agendas and dates for responses that gives the information in a relatively concise format for ease of distribution and comprehension.

About us

The Australian Institute of Company Directors (AICD) is committed to strengthening society through world-class governance. We aim to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. Our membership includes directors and senior leaders from business, government and the not-for-profit (NFP) sectors.

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