Risk Management Framework

Adopted by the Board on 19 May 2017

Risk Management Framework Purpose

In order to achieve its strategic objectives, an organisation needs to identify and manage a range of risks that it faces both on a day-to-day basis and over the longer term.

The International Standard for Risk Management ISO 31000:2009: Risk Management – Principles and Guidelines defines risk as:

> *"…the effect of uncertainty on objectives."*

It further defines a risk management framework as:

> *"…a set of components that support and sustain risk management throughout an organisation"*

The risk management framework characterises an entity's processes for managing risk as including the organisations policy, objectives, implementation, monitoring, reviewing and improvement of risk management.

Bapcor's key elements of the Risk Management process aligns with ISO 31000:2009 Clause 5:

A. Communication & Consultation (5.2)

B. Establishing the Context (5.3)

C. Risk Assessment (5.4)

- Risk Identification
- Risk Analysis
- Risk Evaluation

D. Risk Treatment (5.5)

E. Monitoring & Review (5.6)

Accordingly, risk management is a critical area of responsibility for the Board and core component of a good governance framework.

Risk Governance

Governance is defined in the ASX Corporate Governance Councils *Corporate Governance Principles and Recommendations* as:

> "…..*the framework of rules, relationships, systems and processes within and by which authority is exercised and controlled in corporations'. It encompasses the mechanisms by which companies, and those in control, are held to account."*

The primary objective of risk governance is to provide assurance to the Board that risks are being effectively managed throughout the organisation.

This encompasses:

- Identification of emerging risks
- A risk-aware culture
- Effective communication of risks; and
- Alignment of risks to strategy

Governance Structure

Board: The Board's role is to set the risk appetite for the Bapcor group, oversee its risk management framework and to satisfy itself that the framework is sound.

Audit & Risk Committee: provides oversight and advice to the Board in relation to current and potential future risks and risk management strategies; provides recommendations about risk appetite and tolerance; monitors the management of risk and identifies to the Board any matter where it considers that action or improvement is needed and recommends steps to be taken.

Group Leadership Team: It is the role of management to design and implement the risk management framework and to ensure that Bapcor operates within the risk appetite set by the Board.

Audit: Audit reviews the effectiveness of controls. It brings a systematic, disciplined and independent approach to recommending improvements of the control framework operating within an organisation.

Employees: Employees have the responsibility to raise matters of risk with management or the Group Leadership Team as identified in the Bapcor working environment.

The utilisation of external professionals in conjunction with the Board, Audit & Risk Committee**,** Group Leadership Team and employees enables a comprehensive process of identification, treatment, monitoring and review of risks associated with Bapcor and its strategic objectives.

Risk Responsibilities

While all the employees of Bapcor have the responsibility to be involved in the identification, evaluation and treatment of risks and opportunities that could impact or influence Bapcor as an organisation, the ultimate responsibility for risk management oversight lies with the Board.

The Bapcor **Board of Directors** ("Board") is responsible for the informed oversight of risk management within the organisation, and reviewing and approving the risk management framework, and monitoring the activities under the framework.

The Board have constituted the **Audit & Risk committee** ("ARC") to oversee the effective management of financial, strategic and operational risks. The ARC's role isn't to eliminate risks but to ensure that Bapcor is responding to risks in a way that creates value for the company and its shareholders.

The Bapcor **Group Leadership Team** ("GLT) is responsible for developing and implementing a sound system of risk management and internal control. Accordingly, the GLT has the responsibility to report on the progress of achieving the strategic objectives of Bapcor in line with the Boards risk appetite.

Audits responsibility as part of the Bapcor's risk management framework is to understand the key risks of the company and to examine and evaluate the adequacy and effectiveness of the system of risk management and internal controls used by management and raise any deficiencies or suggested improvements

Risk Management Methodology

Bapcor Ltd recognises that risks, benefits and opportunities accompany change and uncertainty in all aspects of its business operating environment.

The risks faced by Bapcor are diverse and vary significantly in terms of likelihood of the event occurring and the consequence of such an event. These risks can result from factors both externally and internally driven and can be interdependent in nature.

Bapcor's risk management methodology parallels the ISO 31000 risk management process by systematically applying management policies, procedures, and practices to a set of activities with the intent to establish the context, communicate and consult with stakeholders, and identify, analyse, evaluate, treat, monitor, and review risk.

Identification

Risk categories (as identified in the table below) are specific to Bapcor and consider the external and internal parameters and factors that influence how Bapcor manages risk in order to achieve its strategic objectives.

1.	Compliance	Compliance Risk is the current and prospective risk to an organisations financial performance arising from breaches or contraventions of, laws, rules, regulations, prescribed practices, internal policies and procedures, or ethical standards. Compliance risk may also arise in situations where ambiguous or untested laws or rules govern products or activities of Bapcor. Compliance risk exposes Bapcor to fines, penalties, payment of damages, and the voiding of contracts. Compliance risk can lead to a diminished reputation, limited opportunities, and lack of contract enforceability. Compliance risk goes beyond a failure to comply with consumer protection laws. It encompasses all laws as well as prudent ethical standards, contractual obligations and exposure to litigation. Compliance risk can blend into operational risk and legal risk.
2.	Strategic	Strategic Risk is the current and prospective risk to an organisations financial performance transpiring from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry or regulatory changes. This risk is a function of the compatibility of Bapcor's strategic goals, the business strategies developed to achieve those goals, the resources deployed to accomplish these goals, and the quality of implementation. The tangible and intangible resources needed to carry out business strategies include communication channels, operating systems, delivery networks, monitoring systems, and managerial capacities and capabilities.
3.	Financial	Financial Risk is the current and prospective risk to an organisations financial performance arising from financing arrangements, transactions, instability and losses in financial markets caused by movements in share prices, currencies, interest rate and debt defaults. Financial Risk is one of the highest priority risk types of every company. Further classification and possible overlap with other categories of financial risk could fall into the following categories: Market Risk (i.e. Volatility risk), Credit Risk (settlement risk), Liquidity Risk (asset/funding liquidity) and Operational risk (Fraud, people, legal risk)
4.	Operational	Operational Risk is the prospect of loss resulting from inadequate or failed internal policies and procedures, people and systems or external events. Operational risk encapsulates business continuity plans, environmental risk, crisis management, process systems, Human Capital (including OH&S), and information technology.
5.	Human Capital	Human Capital refers to the ability of employees of a business to produce economic value through the performance of labour by applying relevant skills, know-how and expertise (in a safety cognisant environment). The combination of policies, processes, training, reputation of the business and the effective use of resources will affect the Human Capital Bapcor attracts and associated economic benefits. Human Capital risks is likely to overlap with legal and operational aspects of risk such as Occupational Health & Safety (OH&S).

6.	Legal	Legal risk is associated with the impact of a defect in the application or erroneous administration of financial, operational, strategic, IT, Human Capital or cultural operations in relation to the contravention of legislative, regulatory, statutory, governance or industrial obligations and requirements.
7.	Information Technology (IT)	IT risk is associated with: • General (hardware, software failure, malware, viruses, spam, human error), • Criminal (hackers, cybercrime, fraud, password theft, security breaches, staff dishonesty); and • environmental threats (fire, storm, flood, other natural disasters) to Bapcor's IT systems. IT risk management is the ability to ensure that various events or incidents do not compromise Bapcor's business processes, ability to generate economic benefit and avert breaches of laws and regulations and protect privacy, security, storage and access to data. IT risk is likely to overlap with legal and operational aspects of risk.
8.	Cultural	Culture is a key determinant in the performance of an organisation and its capability to achieve its objectives. It goes to the heart of the openness and transparency needed for effective stewardship and informed decision-making. An organisation's culture is the sum of its shared values and behaviours. It includes the values and behaviours of its people as they relate to various dimensions, such as risk, safety and compliance. The risk culture of an organisation is the shared attitudes (values) and behaviours of individuals about the management of risk in an organisation. Bapcor's culture will be a key determinant in its ability to respond and adapt to changes in the environment in which it operates.

Communication

Principle 7 of the ASX Corporate Governance Principles and Recommendations guidelines (2nd edition) requires the disclosure and communication to stakeholders on matters of risk and the effective corporate management of material business risk.

Regular discussions in regards to the culture and attitude towards risk amongst the GLT and the Board reinforces the process of developing a risk aware culture. Communicating the resulting expectations set by the Board to management and employees is an important foundation of risk management.

The Risk Register is the key tool that the GLT utilises to identify and communicate the principle risks and mitigation strategies pertinent to Bapcor. The GLT compiles the Risk Register via consultant lead workshops on at least an annual basis. In addition the risk framework is periodically updated for changes in circumstances and utilises upward feedback from employees throughout the organisation.

The results of these risk identification workshops are presented to the ARC for their assessment, review and management inquiry on a semi-annual basis.

Mitigating strategies identified in the Risk Register are rolled out by the identified risk owners and monitored and reviewed on an ongoing basis.

Any new risks that are identified in the normal course of business are considered by the GLT on an ongoing basis, and where considered a high risk or above, are conferred and discussed with further action taken as appropriate.

Management and the Board consider risk on continual basis through the operational management and oversight of the business. By performing this on an ongoing basis the quality and timeliness of communication is enhanced and cultural awareness engrained.

The identification, flow of risk reporting and communication are encapsulated in following activities.

Management

- Continuous assessment of risk in allocated area of responsibility
- Monthly reporting on performance of operations
- Monthly business segment reviews by CEO and CFO
- Monthly Group Leadership Team meetings
- Semi-Annual review and update of Risk Register and allocation of risk owners
- Annual update of risk management framework

Board / ARC

- Monthly Board meetings and quarterly ARC meetings
- Semi-annual review of Risk Register (including risk tolerance ratings)
- Periodic meetings with external auditors
- Review of outcome of audit reports and other documentation and processes as prepared.
- Periodic meetings with the Group Leadership Team

Risk Assessment

Bapcor's risk assessment process evaluates the likelihood and consequence of each risk identified under each risk category. Bapcor details this process via a comprehensive risk register using both qualitative and quantitative measures. The risks identified are classified on a scale of 1-5. (refer table below).

The multiple combination of the two ratings will ascribe a relative inherent risk rating if there weren't any controls in place relevant specifically to the Bapcor entity.

Consequence					
Rating		**Financial Rating ***	**Human Capital**	**Regulatory**	**Reputational / Brand**
1.	Insignificant	<$5k	First Aid	Miss lodgement date	Nil
2.	Minor	$500k to $2m	Medical Treatment	Interest & Penalties	Nil
3.	Moderate	$2m to $10m	Injuries	Breach of regulations	Some Media
4.	Major	$10m to $25m	Single Death or Disability	Trading Halt	Adverse Media
5.	Catastrophic	$>$25m	Multiple Deaths	Deregistration	Adverse Media

**Note: Reviewed as part of the 2017 risk register update post Hellaby acquisition.*

Rating		**Likelihood**
1.	Rare	Once every 100+ years
2.	Unlikely	Less than once every 100 years
3.	Possible	Once every 10 years
4.	Likely	Probably occur once every (1) year
5.	Highly Likely	Expect to occur more than once a year

(i.e. 4 - Major consequence x 3 - Possible Likelihood ascribes an inherent risk rating of 12)

Risk Evaluation and Treatment

The Risk Register identifies the relevant GLT member who is responsible for each risk.

By developing an understanding of the risks. Management can determine whether risks need to be reduced, transferred or accepted when compared to managements risk tolerance and risk appetite set by the Board.

All identified risks in the register are then reassessed for their residual risk after taking into consideration the mitigating risk strategies already in place.

Potential risk strategies that could be further employed are also documented to gauge the impact on the risk and are utilised as a guide to cost benefit of reviewing existing strategies, investigating or deploying further mitigation strategies.

For any risks with a residual risk of 12 or higher, investigation is undertaken to ascertain alignment with the Boards risk appetite and ability for Bapcor to mitigate risk any further. Risks that remain above 12 are agenda points of discussion for the GLT, ARC and the Board while risks with residual ratings of 6-10 are monitored on an ongoing basis.

The following table represents the risk rating table for evaluating risk

(Residual) Risk Rating Table		
Risk Rating	**Description**	**Action**
12-25	High - Critical	Risks are deliberated by management, the GLT, ARC and the Board to assess potential mitigation strategies and consequent actions to be implemented.
6-10	Moderate	Monitor for the potential need of corrective action
1-6	Low	Does not currently require corrective action

The updated Risk Register is presented to the ARC for further review and assessment with the express purpose of reporting to the Board as to the soundness of the current framework and controls in place.

Monitoring & Review

By capturing, analysing, and monitoring Bapcor's risk register on a methodical basis, vital identification of new or evolving risks, and effectiveness of current risk management systems are swiftly identified.

The risk register is a dynamic tool and subject to ongoing review by the GLT. The Risk Register undergoes a detailed update process annually and an interim review of the key risks after six months. Those updates are then provided to the ARC to ensure it reflects the risks of Bapcor in real time.