Professional Risk Managers' International Association
(PRMIA)

Principles of good governance

September 2009

I. PURPOSE

As an independent association of professional risk managers from diverse industries in more than 150 countries, PRMIA provides the premier meeting place for financial and non-financial organisations, their stakeholders and their regulators to engage in, and verify the existence of, best practice corporate governance. The tool we use is the *PRMIA Principles of Good Governance.*

This document sets out principles for good governance and risk management using the following definitions:

Governance	The framework of authority for an organisation within which its institutional objectives are pursued and within which risk management operates.
Risk	Unknown future circumstances that alter the value or well-being of an organisation or system.
Risk Event	The realisation of a specific circumstance that decreases (but could unexpectedly increase) the value or well-being of an organisation or system.
Risk Management	The process of evaluating the potential impact of risk events and shaping business decisions in light of this evaluation.
Board of Directors	A body of elected or appointed members who jointly oversee the activities of a company or organisation – also referred to as board of trustees, board of governors, board of managers, executive board, etc. The precise responsibilities invested in the Board may differ from country to country.

The ten principles below have been gleaned from international sources, both commercial and non-commercial, and from various disciplines, all addressing aspects of good governance. They are designed to be cross-cultural norms which provide Boards of Directors, Audit Committees and senior executives with a standard framework for effective governance. They also seek to provide regulators and auditors with an evaluation tool to ensure that effective governance is in place.

Best practice governance and risk management do <u>not</u> attempt to eliminate risk. Rather, they are designed to help organisations maximise the risk-adjusted return on capital whilst, at the same time, transforming uncertainty - which is unmanageable and unmeasurable - into risk, which can be identified, assessed and may be measurable.

Decision-making in business is predicated on a belief in potential rewards, balanced with the knowledge, understanding and appreciation of all of the risks taken to pursue those potential rewards. The key individuals involved in governance and risk management (see section IV of this document) have a responsibility to stakeholders, including the general public, as well as to financial stability. They must ensure that they do not give disproportionate weight to personal gain, or to the benefit of the organisation, to the detriment of public good and of financial stability.

II. THE PRINCIPLES

These ten principles of corporate governance are based on common themes in a variety of sources (see section V of this document):

1. Key Competencies
2. Resources and Processes
3. Ongoing Education and Development
4. Compensation Architecture
5. Independence of Key Parties
6. Risk Appetite
7. External Validation
8. Clear Accountability
9. Disclosure and Transparency
10. Trust, honesty and fairness of key people

N.B. The principles have not been prioritised in any way as they are inextricably interrelated and no one principle is more important than any other.

Key Competencies
The organisation should have at its disposal employees who have adequate knowledge, skills and expertise to perform the tasks assigned to them. These competencies can be gained through professional qualification or by experience in role.

Resources and Processes
Adequate levels of resource shall be in place to enable the organisation to operate effectively. The business and technological processes shall be fit for purpose.

Ongoing Education and Development
The organisation shall encourage all employees to keep abreast of the latest developments in their particular areas of expertise, through courses, conferences, journals and other education channels and shall make adequate resources available to enable this to occur.

Compensation Architecture
Employees should be remunerated adequately for the roles that they perform, where 'adequately' is defined using external references and benchmarks, and in a framework which is consistent with the type of risk-taking behaviour expected of the employee.

Independence of Key Parties
The organisation shall ensure that, at all times, key checks and balances are in place to assure effective governance. Functions such as Audit and Risk Management are to be independent and report directly to through senior management rather than through those for whom they serve as a check and balance.

Risk Appetite
The Board of Directors of an organisation shall determine, and officially record, its appetite for each category of risk within its published risk framework. It shall encourage a cascade of this approach throughout the whole of the organisation. Such appetite must be expressed in a measurable way that can inform decisions at lower levels in the organisation.

External Validation
All aspects of the governance framework of the organisation shall be periodically validated by an independent body or bodies, external to the organisation, to ensure that they are appropriate to the sector and geographies in which the organisation operates and consistent with the stated policies and public representations made by the organisation.

Clear Accountability
At all levels in the organisation, accountabilities should be clearly defined. Individuals should be clearly advised of their own accountabilities and of the consequences of not fulfilling them in a timely and appropriate manner.

Disclosure and Transparency
The Board of Directors and senior management shall adopt an approach of disclosure and transparency consistent with their stated policies and ensure that this approach is followed at all levels throughout the organisation.

Trust, honest and fairness of key people
The key people involved in the application of good governance and risk management must be trustworthy and honest and treat others fairly at all times.

III. APPLICATION OF THE PRINCIPLES

The essence of good corporate governance is a deliberate and sustained effort to adhere to the principles defined above. These principles are applied in the following areas:

- Board of Directors including the Audit and Risk Committees
- Risk Management Infrastructure
- Financial Accounting and Reporting Infrastructure
- The organisation as a whole

The tables below provide an introductory checklist to the ways in which the PRMIA Principles of Good Governance are to be applied in each of these four areas.

Requirement	Principles									
	Key Competencies	Resources and Processes	Ongoing Education and Discernment	Compensation Architecture	Independence of Key parties	Risk appetite	External Validation	Clear Accountability	Disclosure and Transparency	Trust, honesty and fairness of key people
Boards of Directors, including Audit and Risk Committees, must:										
• be aware of the business structure and environment in which the organisation operates and understand how the Risk Management Infrastructure has been designed to address the risks encountered in that environment	✓	✓	✓		✓		✓	✓		✓
• be composed in a manner such that sufficient independence and expertise exist to evaluate competently the business structure and environment in which the organisation operates	✓		✓		✓		✓	✓	✓	
• define the risk appetite of the organisation and articulate this clearly to senior management			✓			✓		✓	✓	
• set a policy for compensation and targets which supports the Board of Directors' commercial strategy and which encourages employees to operate within its risk appetite				✓		✓				✓
• review thoroughly compensation plans of potentially "highly compensated positions" for consistency with corporate risk appetite, competitive market conditions and fiduciary responsibility to shareholders			✓		✓	✓			✓	
• delegate – to one of their number – formal responsibility for understanding, in detail, the Risk Management Infrastructure of the organisation and for reporting regularly, to the Board of Directors / Committee on the effectiveness of that Infrastructure	✓	✓						✓	✓	
• review continually the application of the Principles of Good Governance to the Risk Management Infrastructure, financial accounting and reporting infrastructure and the organisation as a whole			✓		✓		✓	✓		
• be fully accountable to shareholders and work to the benefit of public good and of financial stability		✓						✓		✓

Requirement	Principles									
	Key Competencies	Resources and Processes	Ongoing Education and Discernment	Compensation Architecture	Independence of Key parties	Risk appetite	External Validation	Clear Accountability	Disclosure and Transparency	Trust, honesty and fairness of key people
The Risk Management Infrastructure must:										
• be independently staffed and report to an employee who is on the Executive Committee (Operating Committee), but who is not a business unit leader					✓			✓		✓
• possess sufficient funding, intellectual and technological capacity to understand and communicate the risks presented by the business structure and environment	✓	✓	✓	✓					✓	
• avoid silos of control and oversight		✓						✓		
• include financial risk management, compliance and external reporting and, to the extent that resources allow, should exclude legal or accounting					✓			✓		
• define the organisation's definition of risk management as articulated by the Board in clear and uncertain terms			✓			✓		✓	✓	
• implement and maintain an approval and implementation process which ensures that the organisation's compensation and targets policy does not compromise the risk management framework and risk appetite policies				✓		✓				
• have a budget that is established by a subset of the Executive Committee or Board, excluding the influence of individual business-unit leaders		✓			✓					
• provide a clear Escalation Policy, for the employees of the organisation as a Whole, to escalate matters of concern without the threat of inappropriately adverse impact		✓			✓					✓
• actively provide ongoing professional development for risk management staff and require them to be committed to standards of best practice, conduct and ethics in their work	✓	✓	✓							
• provide general risk management and related corporate governance training for employees of the organisation as a Whole – responsibility for the implementation of a risk culture rests with the risk management infrastructure		✓	✓							
• provide, in the organisation's Annual Report to Shareholders, a detailed description of the Risk Management Infrastructure			✓						✓	

Requirement	Principles									
	Key Competencies	Resources and Processes	Ongoing Education and Discernment	Compensation Architecture	Independence of Key parties	Risk appetite	External Validation	Clear Accountability	Disclosure and Transparency	Trust, honesty and fairness of key people
The Financial Accounting and Reporting Infrastructure must:										
• represent accurately, and in a timely manner, the current financial condition of the organisation									✓	✓
• only use those off-balance sheet transactions which have a legitimate economic, tax, risk transfer or risk mitigating purpose. All such transactions must be reported completely, equally, clearly and visibly (i.e. not be buried in the footnotes)								✓	✓	
• provide to the Board and Audit Committee an auditable Annual Statement of Compliance with the Board's publicly stated Standards of Corporate Governance			✓				✓		✓	

The organisation as a whole must:										
• provide ongoing education and training to all employees on the role of risk management and corporate governance in the organisation			✓							
• provide an environment in which a Risk Escalation Policy can be effective									✓	
• enforce corporate governance polices								✓		
• comply fully with local laws and regulations, and should comply with local customs, to the extent that such customs do not conflict with local laws and regulations			✓							
• publish an external auditor's opinion that the organisation is in compliance with the Board's publicly stated Standards of Corporate Governance							✓		✓	
• work within a policy for compensation and targets which supports the Board of Directors' commercial strategy and its risk appetite policies				✓						
• ensure that there is a good flow of employees between business functions and governance and risk management functions			✓							
• ensure that the organisation establishes and maintains a risk culture throughout the organisation			✓			✓		✓		

IV. DUTIES OF KEY PARTIES

The following defines the roles and the expectations of key parties as they relate to risk-taking, risk management and governance. It is recommended that the risk function is directly represented at the most senior committee within the organisation.

Members of the Board

Act as sponsors for risk throughout the organisation and ensure that a risk culture is implemented, and maintained, from the top down. Are responsible for setting the risk appetite for the organisation and for ensuring that this is cascaded throughout the organisation.

The Board member responsible for risk management reporting

Ensures that risk reporting is produced in an accurate and timely manner and, where the intended readership is external to the organisation, that the reporting is accompanied by adequate interpretation which gives a complete picture of the risk landscape of the organisation.

Chief Executive Officer

Is responsible for ensuring that all of the operations of the organisation are carried out with due consideration of the risk appetite of the organisation and that the accompanying risks are understood and taken into account when doing business.

Chief Financial Officer

Must ensure that all of the risks associated with the key processes that contribute to the financial reporting of the organisation have been identified and that effective controls are in place to mitigate these risks to an acceptable level.

Chief Risk Officer

Responsible for the management of the Risk Management Infrastructure. Helps the Board to determine the risk appetite of the organisation and then implements this, throughout the organisation, through the Risk Management Infrastructure. Ensures that reporting of risk and governance-related matters is produced in a timely and accurate manner.

The tenure and independence of the Chief Risk Officer should be underpinned by a provision that removal from office would require the prior agreement of the board. The remuneration of the Chief Risk Officer should be subject to approval by the chairman or chairman of the board remuneration committee.

Internal Audit management

Must maintain appropriate assurance measures to ensure that the Governance and Risk Framework of the organisation is effective and, if any shortcomings are discovered, to escalate these so that remedial action can be taken in an appropriate and timely manner.

Compliance management

Must ensure that all employees understand the rules and regulations (both internal and external) with which they must comply and the implications, for them and for the organisation, of non-compliance. Management of the compliance function must ensure that the organisation does comply with all relevant regulation and that adequate governance is in place to facilitate this.

Other senior management within the organisation

Has a responsibility to ensure that the governance and Risk Framework are embedded within their business area and, by rolling out a risk culture, that all employees understand their roles and responsibilities with regard to risk.

V. SOURCE DOCUMENTS

- COSO Framework (Committee of Sponsoring Organizations of the Treadway Commission)
- O'Malley Panel on Audit Effectiveness
- OECD (Organisation for Economic Co-operation and Development) Principles of Corporate Governance
- International Corporate Governance Network - Statement on Global Corporate Governance Principles
- Commonwealth Association for Corporate Governance Principles of Corporate Governance
- Blue Ribbon Panel on Audit Committee Effectiveness
- Greenbury Recommendations on Board Compensation
- Basel Committee - Risk Concentration Principles
- Basel Committee - Enhancing Corporate Governance for Banking organisation
- PAIB/IFAC Enterprise Governance Principles
- External Environmental Factor Considerations for Boards and Audit Committees - Ernst and Young
- Sarbanes-Oxley Act
- Securities and Exchange Commission
- Group of 30 Reports
- The Turner Review: A regulatory response to the global banking crisis – Financial Services Authority
- CFA Institute Code of Ethics and Standards of Professional Conduct
- The Walker Review: A review of corporate governance in UK banks and other financial Industry entities – Financial Services Authority

VI. REVIEW COMMITTEE

Dr. John Paul Broussard	Associate Professor, Rutgers University
Frank Hayden	Managing Director - Market Risk, Fortis Bank
Kruskal Hewitt	Vice President, Union Bank of California
David Koenig	Chief Executive Officer the Governance Fund LLC Past Chair and Executive Director of PRMIA
Robert W. Kolb	Professor of Finance and Frank W. Considine Chair of Applied Ethics, Loyola University, Chicago
Colin Lawrence	Director of Risk, Financial Services Authority
Steven Lindo	Executive Director, PRMIA
Renato Maino	Professor of Credit Risk Management, Milan L. Bocconi and Turin Universities
Robert Mark	Chief Executive Office of Black Diamond Risk Deputy Chair of the PRMIA Executive Board
Colin Stringer	Director of Parascosa Consulting
Kalyan Sunderam	Chief Risk Officer and Deputy Chief Executive Officer - Bahraini Saudi Bank
Desheng Dash Wu	Affiliate Professor, Toronto University Chief Executive Officer of RiskLabs China in Shanghai

Version 4.2
15th September 2009