19

Brazilian Institute of Corporate Governance

Corporate Governance Handbooks

Corporate Risk Management

Evolution in Governance and Strategy

IBGC | Instituto Brasileiro de Governança Corporativa

Corporate Risk Management

Evolution in Governance and Strategy

IBGC | Instituto Brasileiro de Governança Corporativa

2020

Brazilian Institute of Corporate Governance (IBGC)

Founded on November 27, 1995, the Brazilian Institute of Corporate Governance (IBGC), a civil organization, is the Brazilian reference and one among the main reference organizations for corporate governance worldwide. Its purpose is to generate and disseminate knowledge on the best corporate governance practices and influence the most diverse agents in its adoption, contributing to the sustainable development of organizations and, consequently, to a better society.

For further information about the Brazilian Institute of Corporate Governance, visit the website www.ibgc.org.br. To become a member, call +55 11 3185-4200.

Production of the translated publication. Translator: Cintia Isobata Aquino, Fernanda Vitarelli, Gisela Christiano, Mônica Pimentel de Mello Moreira; Proofreading: Camila Cristina da Silva; Back-office support: William Barros A. de Melo; Graphic design, layout and cover: Kato Editorial; Translation costs: IDB Invest.

International Cataloging Data in Publication (CIP) according ISBD

G946 Corporate Risk Management: evolution in governance and strategy / organized by Instituto Brasileiro de Governança Corporativa – IBGC ; translated by Cintia Isobata Aquino … [et al.]. – São Paulo, SP : Instituto Brasileiro de Governança Corporativa – IBGC, 2017.
66 p. ; 18cm x 25,5cm. – (Corporate Governance Handbooks Series, 19)

ISBN: 978-65-86366-28-0

1. Corporate Governance. 2. Board of Directors. 3. Risk. 4. Management. I. Aquino, Cintia Isobata. II. Vitarelli, Fernanda. III. Christiano, Gisela. IV. Moreira, Mônica Pimentel de Mello. V. Title. VI. Series.

CDD – 658.4
2020-2751 CDU 658.114

Prepared by Vagner Rodolfo da Silva – CRB-8/9410

Index for systematic catalog
1. Corporate Governance 658.4
2. Corporate Governance 658.114

Credits

This publication is the result of a project developed and executed by the IBGC's Corporate Risk Management Committee. Its content does not necessarily reflect the individual opinions of those who participated in its preparation, but rather the understanding of the institute. During its preparation, this document went through an intense process of internal discussions and public hearing, having received several contributions and suggestions.

Overall coordination

Mercedes Marina Stinco.

Coordination of Drafting and Review Groups

Alex Lelis Buzato Borges, Érico Torres, Luciana Bacci, Ricardo Lemos, and Roberto Lamb.

Committee Members

Alberto Whitaker, Alberto Yamandú Messano Colucci, Alessandra Silva de Jesus Artifon, Alex Lelis Buzato Borges, André Coutinho, André Echeverria, André Vitoria, Antônio Cocurullo, Antonio Edson Maciel dos Santos, Antônio Lemos, Antonio M. F. Ribeiro, Arnaldo Bonoldi Dutra, Carlos Sá, Clara R. F. Biscar, Clovis Corrêa da Costa, Érico Torres, Erlon Lisboa de Jesus, Fábio Coimbra, Fábio Mendes, Fernando Nicolau Freitas Ferreira, Flavio Abrão, Francisco Carlos Fernandes, Frederico de Campos Ventriglia, Ivana Regina Galvão Leite, Ives Pereira Müller, João Francisco Arcoverde Lopez, Leandro Pavão, Leonardo Machado, Lucia Casasanta, Luciana Bacci, Marcelo Lerch Hoffmann, Marco Antonio Bueno, Marcos Lorençani, Marcus Lanzelotti, Maria Paula Aranha, Marilza Benevides, Mario Augusto Filipini, Mercedes Marina Stinco (coord.), Mirian Paula Ferreira Rodrigues, Paulo Baraldi, Pedro Antônio Maziero, Rainer Lutke, Ricardo Aparecido dos Santos, Ricardo Lemos, Ricardo Roschel, Roberto Lamb, Roberto Sobral Hollander, Sandra Cristina Bernardo, Silvio Valdrighi, and Tatiana Leite.

Contributions and Special Thanks

To the IBGC team, for their support to the committee and for their contributions to the document.

To Lucas Legnare and Luciana Del Caro, for their support in the process of drafting the handbook.

To Carlos Eduardo Lessa Brandão, José Luiz Bichuetti, and Sergio Moreno, for their comments and participation in the board that examined the publication.

To Annibal Ribeiro Lima, Camila Sardenberg, Cida Hess, Clara Regina Ferrão Biscar, Edina Biava, José Martins, José Ricardo De Moraes Pinto, Leila de Oliveira Lopes Rega, Leonardo Viegas, Luiz Alberto de Castro Falleiros, Luiz Athayde, Maurício Loures Rodrigues, Roberta Simonetti, Tatiana de Oliveira Leite, and Thomas Brull, for participating in a restricted forum that discussed the content of the document.

To Alexandre de Oliveira, Carlos Antonio Vergara Cammas, Diego Silveira Maciel, Felipe A. F. Gomes, Isabella Saboya, Sergio Mastrangelo Ferreira, Vladimir Barcellos Bidniuk, and William Borges Lima, for the contributions sent during the public hearing process.

To Francisco Fernandes, João Francisco Arcoverde Lopez, Maria Paula Aranha, Marilza Benevides, and Silvio Valdrighi, for the contributions generated in the production of the texts.

To Ricardo Lemos, for the consolidation and revision of the various versions generated by the drafting groups.

To Roberto Lamb, for his invaluable and relevant contribution throughout all stages of construction of the handbook, making the text as rich and current as possible.

ABOUT IDB INVEST:

IDB Invest, the private sector institution of the Inter-American Development Bank (IDB) Group, is a multilateral development bank committed to supporting the private sector in Latin America and the Caribbean. It finances sustainable enterprises and projects to achieve financial results that maximize economic, social and environmental development for the region. IDB Invest works across sectors to provide innovative financial solutions and advisory services that meet the evolving demands of its clients. For more information visit www.idbinvest.org.

Index

Presentation

Since 1999, with the launch of the first edition of the Code of Best Practice of Corporate Governance, IBGC started to publish specific documents within the scope of good corporate governance practices.

This publication, **Corporate Risk Management**: **Evolution in Governance and Strategy**, is part of a series of publications called Corporate Governance Handbooks, whose objective is to bring practical information to the market that contributes to the corporate governance process.

The IBGC Governance Handbooks are edited, according to their content, in three series: Legal Governance Documents, Documents on Governance Structures and Processes, and Special Governance Themes. They bring contributions, suggestions, and recommendations prepared by IBGC members who are part of its various work committees.

Part of the Special Governance Themes, this handbook addresses how managers, with special emphasis on directors, can develop an efficient implementation model for risk management based on the principles of good corporate governance.

The handbook instructively presents the roles of the main governance agents and some of the main recommended practices, providing support for the implementation of a risk management structure that dialogues with the long-term strategy set by the organization.

With this publication, IBGC expects to contribute to the proper management of the uncertainties that accompany the risks, ensuring that the managers are better prepared for a reflected and balanced decision making.

Foreword

This work aims to bring reflections and guidance to senior management, and, above all, directors interested in implementing or improving the corporate risk management model (GRCorp) of the organizations in which they work. The document is intended to serve organizations at different stages of GRCorp maturity.

If the focus of the first IBGC handbook on risk management[1] was on the risk treatment methodology, this publication highlights GRCorp governance and strategy, that is, the organizational structure through which risk management is designed and operationalized. The purpose of the text, therefore, is not to be exhaustive in relation to risk management techniques. Many manuals addressing this topic can be found on the market, and some are cited in the bibliographic references at the end of this material. We decided to present herein only essential concepts so that senior management and directors can understand the importance of their role in the implementation and coordination, supervision, and inspection of a solid and consistent risk management structure.

Risk management is becoming more important in the daily routine of companies, not only as a way of reacting to corporate failures that could have been avoided by proper management, but because of its strategic importance. The information collected by GRCorp is an integral part of the business decision-making process, the protection of assets, and the value creation process, which highlights the importance of adequate governance of this structure.

IBGC believes that the ponderations and suggestions contained herein will improve corporate governance, since GRCorp is a valuable instrument of management and governance and acts in favor of the sustainable development of organizations, benefiting all stakeholders.

For the design of this handbook, we took into account the discussions and analyses carried out by the IBGC Risk Committee over the years, since its first edition (2007), the experiences of projects and risk management implementations in companies of different sectors,

1. *IBGC, Guia de Orientação para Gerenciamento de Riscos Corporativos, 2007. Please note that the IBGC Risk Committee has already developed other publications on the topic with the series Estudos de Caso, namely: Visão Evolutiva do Modelo de Gestão de Riscos: Vale e Natura Cosméticos, 2008; Gestão Integrada de Riscos: Banco Real e Brasil Telecom, 2008; and Gestão de Riscos como Instrumento para a Tomada de Decisão: Votorantim Celulose e Papel (VCP), 2008.*

and the different stages of maturity in the risk management process, GRCorp good practices used by international or national independent organizations and institutes, associations of manufacturers or professionals, standards organizations and regulatory agencies were also considered.

At the time of the conclusion of this publication, the revision of the standard ISO 31000: General Guidelines for Principles and Implementation of Risk Management was being carried out, as well as that of Coso ERM (Enterprise Risk Management - Aligning Risk with Strategy and Performance). The latter explores how GRCorp should be integrated into the strategic planning of organizations, since the strategy influences their development. A company that integrates GRCorp into its strategic planning provides management with risk information that must be considered in its strategic alternatives and choices.

Like the IBGC, these organizations (ISO and Coso) realized the complexity to which organizations are subject, the changes that have occurred over time, and the appearance of new risks. Therefore, the stress to and awareness of corporate risk management by boards of directors is crucial.

Hoping that the material will be useful and beneficial, we wish you a good reading.

Introduction

In the daily lives of individuals and organizations, the fact that almost all actions and activities involve risks is rarely taken into account. The word risk comes from the Latin word risicum or riscum, whose definition involves the concept of risking - riscare. Thus, every action or undertaking carries some risk. "Living is very dangerous," says the character Riobaldo in the book Grande Sertão: Veredas by Guimarães Rosa.

Organizations are increasingly faced with issues such as sustainability, corruption, fraud, abuse of short-term incentives for executives and investors, business ethics, and reputation. Each of these issues brings with it the notion of risk. And these issues must be managed by organizations in order to obtain profits, achieve important goals (social, environmental, etc.), create value, and, above all, have a long-lived existence.

Risk is customarily understood as the possibility of something failing. But the current concept of risk in the corporate world goes further: it involves the quantification and qualification of uncertainty[2] in terms of losses and gains by individuals or organizations. As risk is inherent to all activities – and impossible to eliminate–, its management is a key element for the survival of companies and other entities.

This is how corporate risk management (GRCorp) activities should be viewed. GRCorp activities need to contribute to the long-lived existence of organizations and the achievement of its corporate purposes and strategic goals. For this to be possible, organizations must have a structure for risk management and corporate governance, albeit minimal in less mature organizations with less financial capacity. This publication aims to guide directors and executives in the implementation of a GRCorp model and the strengthening of existing models. Given the particularities and the different stages of development of each organization, the recommendations and suggestions contained herein must be analyzed in view of the reality and the moment of each organization.

2. *Risk: identified future event to which it is possible to associate a distribution of probabilities of occurrence. Uncertainty: identified future event to which it is not possible to associate a distribution of probabilities of occurrence. Ignorance: Future events that, at the moment of analysis, cannot even be identified, much less quantified (example: events resulting from complex systems such as climate - the consequences of global warming are unpredictable). M. Faber, R. Manstetten and J. Proops, Ecological Economics: Concepts and Methods, 1996, p. 209-211.*

According to the 5th edition of the IBGC Code of Best Practices of Corporate Governance: "The risks to which the organization is subject must be managed to support decision-making [...]. Governance agents have a responsibility to ensure that the entire organization is in compliance with its principles and values, which are reflected in internal policies, procedures, and standards, and with the law and regulations to which the organization is subject "[3].

The IBGC code advises that directors have knowledge about the topic, so that they can effectively identify, prioritize, and ensure the effective management of the organization's exposure to the various risks related to its business. The board of directors must adopt a proactive attitude, requiring information based on the GRCorp model. This will become possible to the extent that the directors are able to evaluate the models, structures, processes, tools, and indicators used.

This handbook is divided into three chapters. The first chapter deals with the basic concepts of GRCorp, its importance, and how risk management is aligned with corporate strategies. Chapter 2 focuses on the duties of the various corporate governance agents, with an emphasis on the role of the board of directors from the perspective of decision-making processes, responsibilities, and risk drivers. Finally, Chapter 3 provides support for the implementation of a GRCorp structure appropriate to the size and complexity of the organization and which respects the stage of business maturity and the long-term strategy of its management, presenting the main recommended practices. The handbook also includes annexes with additional information.

3. IBGC, Code of Best Practices of Corporate Governance, 2015, p. 91.

1

Definitions and Bases

1. Definitions and Bases

1.1 Corporate risk management concepts

Given that risk is inherent in any business activity, it is up to companies to manage risk in order to take calculated risks, reduce the volatility of companies' results and increase the predictability of their activities, and become more resilient in extreme situations. The effectiveness of risk management can directly affect corporate purposes and strategic objectives set by management - and, ultimately, it impacts the organization's longevity.

Corporate risk management (GRCorp) can be understood as a system intrinsic to strategic business planning, consisting of continuous and structured processes – designed to identify and respond to events that may affect the organization's objectives – and a corporate governance structure – responsible for keeping this system alive and functioning. Through these processes, the organization can map profit opportunities and reduce the likelihood and impact of losses. GRCorp is, therefore, an integrated system designed to guide the appetite for risk taking in the business environment, in order to achieve set objectives.

There are several GRCorp structures and models – such as those proposed by the Committee of Sponsoring Organizations of the Treadway Commission (Coso II) and the ISO 31.0004 standard[4]. The GRCorp process generally begins with the identification and classification of risks, which can be carried out according to their nature, their origin, or to the company's industry and culture, among other criteria. A possible methodology may establish, for example, that there are internal risks (arising within the organization), external risks (unrelated to the company), and strategic risks (related to the information used by management for decision making). One of the generally accepted tools for classifying or categorizing risks is the risk matrix, which considers the origin of events (internal, external, or strategic) and divides them into several classes. The types of risks will be presented in more detail in Annex 2 of this handbook.

The following stages of the GRCorp process are assessment, which seeks to determine the degree of exposure of the company to risk (given by the probability of occurrence and the impact of the event), measurement (quantification of loss estimates), and the treatment given to risks. This requires that the company make a simple decision between avoiding or accepting the risk. The option to accept risks leads to some alternatives, such as retaining, reducing, sharing, or exploiting the risk. When the company decides to retain the risk, the company assumes such risk at its current level of severity (impact and probability). When the company decides to reduce the degree of severity, it takes measures to minimize or mitigate the

4. *Here we can also mention the standards ISO 22301, ISO 27000-series and NIST, ISO 38500 and Cobit 5, and the draft standard BS 65000 from the British Standard Institute (BSI), which deal with risk management in relation to information systems, IT governance, business continuity, and organizational resilience.*

probability of occurrence of the risk and its impact. Sharing refers to cases in which the risk is partially passed on to or shared with third parties. Exploration means using the organization's skills to obtain results with the current level of exposure to risk, or with an increased level of exposure, to enjoy competitive advantages.

Other stages of the GRCorp process are the communication and monitoring of risks. The first involves the constant follow-up of effectiveness and adequacy of the process by the Board of Directors and Executive Board. The communication, in turn, helps the corporate environment to reflect the values and risk culture the company desires.

One of the key aspects of GRCorp is achieving a balance of the levels of retention, reduction, exploration and transfer of risks suitable to the company's risk appetite.

The risk appetite is connected to the level of risk the company willing to accept in the pursuit and fulfillment of its mission. It should be established by the Board of Directors (CA) (or by the partners, if the company does not have a board), considering the companies' best interests and acts as reference for establishing strategies and choosing the objectives related to those strategies. Based on this appetite, the company's risk profile is outlined. In an analogy with investors in financial markets, companies range from the most conservative to the boldest when it comes to the willingness to take risks and accept potential gains or losses. "Risk tolerance can be seen as the acceptable variation around the limits established. Among the acceptable risks and exposures, the tolerance limits are 'triggers' ´prompting action by the Board of Directors. The Board of Directors should follow-up on risk and hedge effectiveness indicators"[5].

Another important concept is the GRCorp. strategy. It should include issues related to the expectations, purposes, goals, investments and development vis-à-vis the company's GRCorp practices. Both the definition of the GRCrop strategies and the determination of the risk profile are incumbent upon the Board of Directors, as detailed in Chapter 2 of this handbook.

An effective risk management is dictated by the quality of governance, human resources, strategies, culture, perception of risks generated by quality of the business environment, processes, controls and technologies adopted. It is a particular feature of companies in which the risk-return relationships base the taking of decisions by managers with a view to achieving the company's objectives. The risk-return relationship suggests that the higher the expected return, the greater the risks to be undertaken, demanding an assessment of the power to manage and control such risks. Therefore, the reflection on the capacity to manage risks taken is key for well-founded and conscious choices.

Implementation of the GRCorp brings several benefits for companies to manage their risks, be them operating or related to the business environment as a whole. Once the company relies on clear processes to identify, measure, report, monitor and mitigates the risks, internal controls

5. *S. A. Ross, R. W. Westerfield, J. Jaffe and R. Lamb, Corporate Finance, 10th Edition, 2015. p. 924. While the "risk appetite" is associated to the risk level the company may accept in the search for and achievement of its mission/ vision (ex-ante analysis), "risk tolerance" refers to the acceptable level of variation in the accomplishment of defined goals and objectives (mostly related to the ex post monitoring).*

are enhanced, bringing operating gains and reducing the possibility of losses and maximizing entrepreneurial efficiency and effectiveness.

Another benefit of risk management is the deepening of discussions on key aspects of the business, as well as the identification of new opportunities. The information gathered provides a better foundation to make decisions, streamlining the processes of choice and allocation of resources.

The GRCorp foster transparency by explaining the main business risks and how they are treated. Investors count with more subsidies to assess if it is worthwhile to invest in a given company (or what is the expected return). Other stakeholders such as the community, the government and employees also benefit, directly or indirectly, from a robust and well-structured GRCorp system, to the extent the company generates value by taking risks, its results are less volatile and the system contributes to the company's feasibility from the economic-financial, environmental, social, reputation and conformity standpoints.

There is also an improvement in corporate governance resulting from the processes inherent to risk management such as enhanced accountability, corporate liability and involvement of the several internal decision layers such as the Board of Directors. All of this converges to the company's longevity and its appreciation.

1.2 History

Risk management has been part of the routine of businesspersons since the very early days[6]. However, the topic has gained relevance since the end of the 20th century given the increased complexity of the companies, financial institutions and third sector companies, in addition to a tighter connection among the markets (globalization). The outset of the vast literature on the topic was dedicated to the area of insurance[7]. Recently, the matter has evolved as a methodology structured from various aspects among which those of finance, audit, strategy and information technology stand out.

In the financial industry, the incentive to implement risk management surfaced in the 1980' due to the growing concern by the Bank of England and the Federal Reserve Board (United States) with the banks' exposure to unrecorded transactions, coupled with problematic loans to countries then considered as third world.

The Bank of International Settlements (BIS) followed suit by forwarding proposals to the banks and requesting their comments and suggestions. The first results of this process arose in 1988 with the first Basel Agreement (Basel I) and its subsequent amendments since 1996. The first agreement, in 1988, focused on allocating capital to face credit risks.

6. *See P. Bernstein, Desafio aos Deuses: A Fascinante História do Risco, 1996.*
7. *See, for example, E. J. Vaughan and C. M. Elliot, Fundamentals of Risk and Insurance, 2003.*

Since 1993 rules for market risk were put in place adopting JP Morgan's publication Risk Metrics[8] in October 1994 as reference. The document was a reply to the severe financial disasters of the early 1990' (such as the Procter & Gamble, Orange County, Barings cases, etc.) and introduced the concept of Value-at-Risk (VaR). The VaR measures the maximum potential loss of a portfolio based on a determined level of trust, in each time period and in normal market operating conditions.

However, the process of identification and treatment of non-financial risks is more complex. While financial risks are easier to quantify using tools such as VaR, the measurement of other risks - such as operating, environmental or reputation risks - involves a greater degree of subjectivity. Since the publication of RiskMetrics, a passionate debate on how to adapt the VaR concept to non-financial risks ensued. Yet, the sole consensus reached was that the VaR would not be enough and it would be necessary to combine a series of quantitative and qualitative techniques to measure non-financial risks. Also, we should remember that the definition of VaR includes the concept of "normal business environment" which, at the outset, means that VaR models will not operate in crises scenarios (for these cases, there are the "stress-test" models).

In June 1999, the BIS' Basel Committee on Banking Supervision, also known as Basel Committee, proposed a new structure for capital conformity, the Basel II, which publication replaced the 1998 agreement. The Basel Committee proposed a three-pillar structure: the first concerned the suitability of the minimum capital based on market, credit and operating risks; the second reinforced the banking supervisor's authority to assess and adapt the regulatory capital to the conditions of each financial institution; and the third provided to transparency and disclosure of information a key role in fomenting market discipline.

As a result of the financial crisis of 2007-2008, which exposed severe regulatory deficiencies in the worldwide financial system, in 2010 BIS once again proposed a new agreement, Basel III, to promote the increase of the banks' capital reserves to protect from potential crises and their consequent "bank races".

Along these same lines, the Commission for European Insurance and Occupational Pension Supervisors - Ceiops, prepared in 2007 the Solvency II directive[9]. Applicable to the insurance and welfare industry, the Solvency II regime is based on three pillars, each one with its own approach and governing a different aspect: i) calculation of the requirements for solvency capital and minimum capital required, based on the standard or internal model; ii) general principles on risk regulation and internal controls; and iii) directives on disclosure and transparency of information on solvency and financial situation.

8. *See <https://www.msci.com/documents/10199/5915b101-4206-4ba0-aee2-3449d5c7e95a>.*
9. *Solvency II (sic) or Solvency II are, in summary, a risk-based supervision. It is the regime created by the European Parliament (Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of insurance and reinsurance [Solvency II]) for insurance companies to improve their control and risk management practices involving governance practices.*

Parallel to the development in the financial field, auditors, accountants, and legislators have devoted growing attention to internal controls. In non-financial companies, the most used risk management directives originate from recommendations of the Committee of Sponsoring Organizations of the Treadway Commission (Coso). This committee issued recommendations and established an integrated methodology to help organizations in analyzing and improving their internal control systems and business risk management processes (ERM - Enterprise Risk Management). This methodology, broadly disseminated since, has been incorporated into the policies, rules, and regulations by several companies to better control their activities to reach the purposes intended.

The Financial Accounting Standards Board (Fasb) published guides fostering disclosure of more complex financial statements, demonstrating the progress made to mitigate and manage risks based on the governance model in place, among other initiatives A group of regulators and professionals has been publishing important guides on internal controls and risk management. In addition to the Coso Report (1992), other noteworthy efforts are the Cadbury (1992) and the Turnbull (1999) Reports.

Nonetheless, the 21st century would rise to a new wave of corporation scandals (Enron, WorldCom, Adelphia, among others), demanding even more regulations. In reply, the United States enacted in 2002 the Sarbanes-Oxley Act (SOX) emphasizing the fundamental role of internal controls and making good practices of corporate governance a legal requirement in the US. The SOX affected all American and foreign companies and their subsidiaries listed in American exchanges. It also provided the basis for local regulations worldwide, placing a spotlight on the methodology developed to improve internal controls. SOX required that CEOs and financial officers of listed companies expressly certify accuracy of the financial statements published, through the creation of internal controls and corporate risk management, as well as procedures for fraud prevention and detection. The act also set forth stricter (criminal) punishment for CEOs and financial officers and changed the way companies are audited. Along the same lines as the SOX and further to the financial market crisis of 2007-2008, the United States approved the Dodd-Frank Act enhancing regulations and creating relevant restrictions over the country's financial activity.

The UK Bribery Act of 2010 came to strengthen and improve the anti-corruption American act (FCPA) enacted in 1977. Brazil also issued its anti-corruption act (Law n. 12946/2013) which came into force in 2014. Subsequently, a string of executive orders and administrative rules contributed to the anti-corruption regulation in Brazil. The act seeks to attribute liability to the companies, their controllers, controlling companies, consortium associates or affiliates for harmful practices affecting the government. Companies began to answer in the administrative and civil levels for their corrupt and fraudulent acts in bids and contracts with the government.

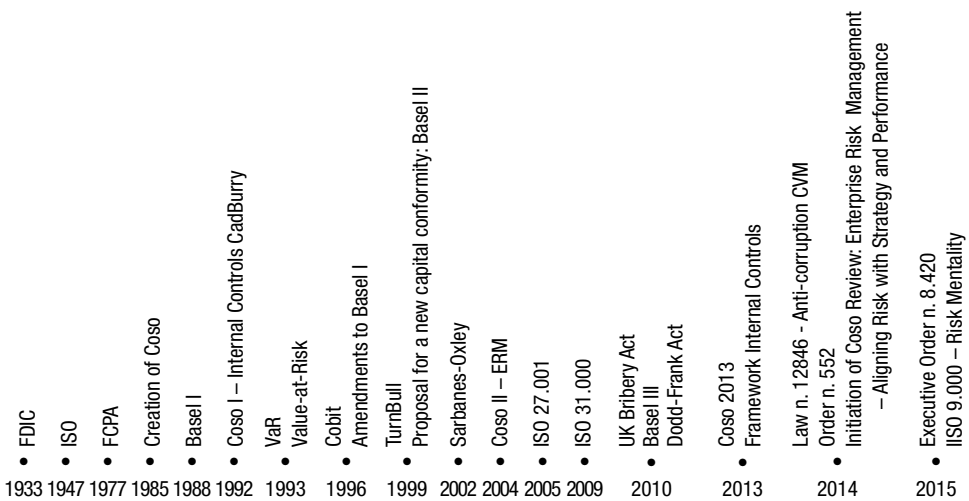
Law n. 12846 was regulated by Federal Executive Order n. 8420/2015 setting forth the criteria for calculation of fines, parameters for assessment of conformity programs

(compliance)[10], the rules for execution of leniency agreements and provisions on the national register of punished companies.

Particularly on the compliance program, the executive order provided the mechanisms and procedures for integrity, audit, application of ethics or conduct codes and incentives to whistleblowing of irregularities to be adopted by the company and monitored by the Ministry of Transparency, Supervision and Control, formerly known as Comptroller General. The integrity program should be structured, applied, and updated according to the current risk characteristics of each legal entity which, in turn, oversees the constant improvement and adaptation of the program.

Despite this recent development, the quest for GRCorp standards remains rather active in Brazil and worldwide. Models aligned with good practices have been developed (some as a crisis-response) with the goal of incorporating new concepts for risk and control assessment and meeting the demands of the market and regulators. The chart below cites the main events contributing to the evolution of GRCorp practices:

Figura 1. Risk management evolution



Key:
FDIC – Federal Deposit Insurance Corporation
ISO – International Organization for
Standardization FCPA – Foreign Corrupt Practices Act
Coso – Committee of Sponsoring Organizations of the Treadway Commission
Basel – Basel Committee on Banking Supervision
Cadbury – Committee on the Financial Aspects of Corporate Governance
Cobit – Control Objectives for Information and related Technology
Sarbanes-Oxley – American law drafted by Paul Sarbanes and Michael Oxley in 2002

10. *Conformity or compliance programs seek to ensure compliance with laws and regulations. They also seek to guarantee conformity, strengthening and operation of the company's internal controls.*

2

GRCorp Governance and Maturity

2. GRCorp Governance and Maturity

2.1 Corporate governance and risk management

IBGC in its Code of Best Practices of Corporate Governance, defines corporate governance as "the system by which companies and other organizations are managed, monitored and encouraged. it involves the relationship between shareholders, the Board of Directors, the Executive Board, supervisory and control bodies and other stakeholders"[11].

Risk management should be associated to the decision-making process and to the process of establishing the strategy, i.e., risk management is the process which should be integrated to the decision-making process. From an operating standpoint, we may say that risk management is part of the company's governance as the risk needs to be identified, measured, treated and monitored - and this information fuels the process of decision-making by several agents such as the partners, the Board of Directors, the Executive Board and the remaining stakeholders (for instance clients, suppliers, the community, regulators, the government, among others). Therefore, GRCorp provides advantages to the organizations' governance structure such as increased transparency and accountability, strengthening of internal controls and stronger commitment to corporate responsibility.

To properly operate, GRCorp needs a previously established and formalized clear governance structure. This structure will define attributions and liabilities of each agent in the several GRCorp levels and practices regarding risk, indicating, for instance, who will identify and assess the risks, take the decision on risk treatment, monitor the risks and supervise the process as a whole.

The main reflections to be discussed by the Board of Directors and Executive Board for building a GRCorp governance model include:

- What may harm achievement of the strategies and goals?
- Where are the largest opportunities, threats, and uncertainties?
- Which are the main risks?
- Which are the risks to explore?
- What is these risk's perception?
- What is these risk's exposure? Is there a difference between risk perception and risk exposure?
- How does the company respond to risks?

11. IBGC, Code of Best Practices of Corporate Governance, op. cit., p 20.

- Is there trustworthy information to make decisions?
- What can be done to ensure an acceptable level of risks according to the risk appetite approved?
- Are the senior management and managers conscious of the relevance of the risk management process?
- Does the company have the necessary skills to manage the risks taken?
- Who actively identifies and monitors the company's risks?
- Which standards, tools and methodologies are used?

This handbook will not analyze in depth the topics related to each of the above questions, which should be understood as a non-exhaustive instrument for reflection by the Board of Directors. The replies to those questions will base evaluation of the current model or create the GRCorp model most suitable for the company.

2.1.1 GRCorp governance and culture

GRCorp governance and culture are the basis for all remaining risk management components. Governance sets the tone, strengthens the relevance, and establishes those in charge of the GRCorp. Culture, in turn, refers to the ethical values, desired behavior and comprehension of risk in the company. Culture is defined in the process of decision-making and assists in fulfilling the company's life and mission. A risk-conscious culture emphasizes relevance of the GRCorp and foments a transparent flow of risk information, with an attitude of knowledge, accountability, and continued improvement.

The risk culture should permeate the entire company and the Board of Directors oversees promoting a broad understanding of the relevance of the matter for the business' longevity. The risk culture of a company is a product of its identity and refers to the body of its ethical standards, values, attitudes and behaviors accepted and practiced, and of the dissemination of risk management as part of the overall decision-making process on all levels. It is established both by the speech and behavior of the Board of Directors, the Executive Board and the company's risk appetite. The risk culture of a company influences how it identifies, accepts, and manages risks.

2.2 Roles and attributions of the GRCorp governance model in the three lines of defense

The GRCorp governance model, represented by roles distributed within the company's structure, helps in managing risks in different company levels.

This model aims to ensure that information originating from the risk management process is effectively communicated and used as basis for decision-making and accountability on all applicable company levels. The model is most effective when risk management purposes are

integrated to performance bonus goals and to following up on key indicators measuring performance and risks taken.

As mentioned in the above topic, the management and consideration of risks in the decision-making process should be integrated to the company's culture. Several agents perform GRCorp roles and responsibilities. It cannot be the attribution of only one area or person, rather it should be performed by all units and persons within the company having the responsibility of integrating and guiding the various risk management efforts, interacting with management.

Processes involving GRCorp should be defined and incorporated as part of the company's culture and structure, leading to a system in which the responsibility for risk management is clearly assigned, activities are formally outlined and communication is streamlined so all those involved reach the company's objectives.

GRCorp duties should be described, formalized, approved, and disclosed in the corporate-wide GRCorp policy. It should represent the group of principles, actions, roles, and responsibilities necessary to identify, assess, respond to and monitor the risks to which the company is exposed.

Three documents may be part of the framework to communicate GRCorp practices:

1) Risk management policy disclosed to the market (such as the disclosure of policies related to securities or related parties' transactions).
2) Risk management rule (or its equivalent), disclosed internally, setting forth the procedures to take risks, liabilities and reporting liabilities, accountability, definition of roles and operating boundaries and the general system for risk management governance; and
3) Code of conduct disclosed in-house and externally, with the purpose of promoting ethical principles and reflecting the company's culture and identity, adding to the legal and regulatory obligations[12].

The processes and activities involving GRCorp and its monitoring should be developed:

i. By the several governance bodies' agents, including the Board of Directors, audit committee and other advisory committees (such as the risk management committee or others discussing specific technical matters), Executive Board and Fiscal Council, if applicable. If the company does not have a Board of Directors, this task will be performed by the partner(s).
ii. By the three lines of defense[13], as detailed below.

12. *Annex 3 of this handbook contains models for the GRCorp policy and rule for reference. The IBGC website contains its code of conduct (see bibliography) to serve as an inspiration for companies, market agents and other types of companies.*
13. *The Three lines of defense, or 3LOD, are a structure for risk exposure governance, also implicit in The Coso ERM reference table, widely used worldwide by financial institutions, but likewise applicably to any company. Encompasses several tasks and corporate teams, including governance structures and agents, enabling control of key-risks identified. Certain approaches are directed to five lines of defense, or 5LOD, in which the insertion of two*

1st Line of defense - performed by unit managers who are directly in charge of processes: covers the tasks they manage and risks for which they are liable.

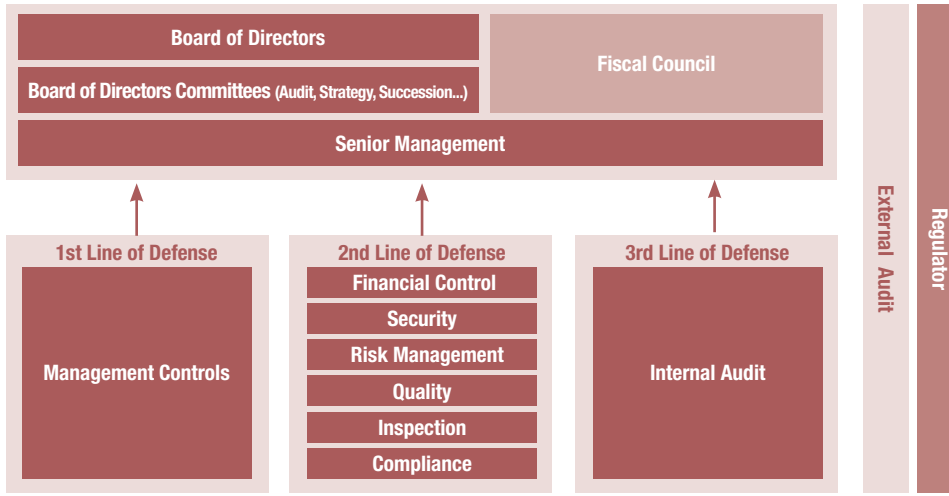
2nd Line of defense - performed by corporate managers of GRCorp, compliance or other control practices, for example, covering the tasks which monitor an integrated view of the risks

3rd Line of defense - performed by internal audit: provides independent assessments through the follow-up of internal controls.

The GRCorp governance model presupposes existence of an interaction among all company levels, including the Board of Directors and its committees, the fiscal council, the Executive Board and the first, second and third line of defense agents.

In this model, each of these three lines of defense fulfills a different role within the broader governance structure of the company.

Figure 2. GRCorp function Lines of Defense



Source: Adapted from IIA, *Declaração de Posicionamento do IIA: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles*, 2013.

more lines defining the liabilities related to risk governance and regulatory compliance stems from the top of the company to the base involved (tone at the top), enabling the three lines of defense to properly operate in a systemic manner. This enables insertion of the fourth line of defense, known as "internal guarantees providers" and of the fifth line of defense, known as "risk supervision and executive management board".

The Executive Board includes the CEO and the remaining members in charge of the operation and of the performance of the several business and support units. The Executive Board may have different responsibilities and manners of accountability in the three lines of defense model, depending on their employer company. For example, a technology executive manager may have the role of second line of defense in a financial company but may act in the first line of defense in a technology company.

There are several alternatives to build GRCorp governance. Each company must adopt what is more suitable to its profile and maturity. Therefore, companies in initial stages must draw their reflections from the above-mentioned outlines to define the best model to be adopted.

2.3 Agents of the GRCorp governance model

2.3.1 Governance bodies

2.3.1.1 Board of Directors

The Board of Directors must oversee the determination of the company's strategic goals, guidelines, and risk profile suitable to its risk appetite, culture, and identity. These responsibilities derive from the concept of "tone at the top", in other words, the ethical principles must emanate from such organ.

Regarding its role in GRCorp, the Board of Directors must monitor the functioning of the risk management process and follow-up on the company's risk profile and action plans defined in response to risks.

The Board of Directors is also in charge of assessing if the performance of the company is aligned with the risk appetite and tolerance established. It is also in charge of monitoring the efficiency and effectiveness of the internal control system, whose capacity must continuously evolve, keeping pace with the developments in the types of risk inherent to the evolution of corporate development and business model, including cyber business models.

In its meetings, the Board of Directors must dedicate time to analyze the risk matrix and internal control system, define adequate exposure levels and routinely follow-up on risk exposures and respective action and mitigation plans.

The Board of Directors' mission is to protect and value the company's heritage. It must be fully aware of the company's values and of the shareholders' purposes and beliefs, watching for their improvement.

The Board of Directors must[14]:

- Seek to comprehend the key elements for the success of the company.
- Assess the company's strategic risks.
- Periodically define and revise the company's risk appetite.

14. *Adapted from NACD,* Report of the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward*, 2009.*

- Define its role and the roles of consulting committees in supervising risks.
- Assess whether the company's GRCorp (including persons and processes) is adequate and has sufficient resources.
- Discuss with the Executive Board the effectiveness of the company's internal control system and provide guidelines to its constant improvement.
- Ensure that management implements effective controls to mitigate business disruption risks (continuity of business) and to mitigate the risk of loss of or unauthorized access to information (information security).
- Define, jointly with the executives, the types, formats, and frequency of information on risks and internal controls subject to its follow-up.
- Foment a dynamic and constructive dialogue between the management and the Board of Directors about risks and controls, including the willingness of the Board of Directors' members to question assumptions.
- Continuously monitor risks potentially impacting the company's goals.
- Monitor critical alignments: strategy, risks, controls, conformity (compliance), incentives and personnel.
- Periodically evaluate whether the GRCorp processes allow the Board of Directors to achieve its risk supervising goals.
- Be the party formally liable for the strategic orientation and monitoring of the company's risk management activities and internal control system.

Further, the Board of Directors is in charge of considering the level of GRCorp maturity of the company in each dimension and develop, jointly with the Executive Board, a future vision of the expected stage where the company must by then and an action plan to achieve it. Assessment of the level of maturity will be analyzed below in item 2.4.

2.3.1.2 Fiscal council

As a governance agent, the fiscal council oversees checking if the company is complying with its principles and values reflected in internal policies, procedures, and rules, as well as laws and regulatory provisions.

In its supervisory work, members of the fiscal council must abstain from orienting or directing any company activities. They may contribute on risk management topics, issuing written opinions on the ancillary information deemed necessary or useful to the risk management process or to the shareholders' meeting. Comprehension of the risk management structure throughout the fiscal year is a key part of the process of formation of the opinions of fiscal council members about the results and the management report to be discussed at the shareholders' meeting.

Some of the main activities performed by the fiscal council related to risk management are:

- being aware of the processes, risk map, key-risk indicators, and those in charge of the GRCorp process and its alignment with the business purposes, as well as of

the internal control structure, risks monitored, key controls, monitoring system and budget and personnel suitability.

- Discussing with other agents playing a role in defining, supervising and monitoring risk management: audit committee, risk management committee, internal audit, accounting, legal, compliance, ethics and conduct areas with a view to gathering information about risk management to substantiate its opinion on management acts.
- Defining, jointly with the executives, the types, formats, and frequency of the information on risks necessary for the fiscal council to perform its supervision role.

2.3.1.3 Audit committee

Companies have different approaches to this committee. It is "a relevant organ to assist the Board of Directors, helping it with the quality control of financial statements and internal controls for purposes of achieving reliability and completeness of information and protecting the company and all stakeholders"[15].

The audit committee has the following goals:

- Supervising quality and completeness of financial reports.
- Supervising adherence to legal and regulatory rules and bylaws provisions.
- Supervising conformity of processes related to the risk management and internal control system aligned with the guidelines established by the Board of Directors.
- Supervising the activities of external and independent auditors.

The audit committee must perform the role of supervising risk management as defined by the Board of Directors The supervising of execution of policies, compliance with risk management rules and following-up on key-risk indicators must be reported to the Board of Directors. These reports, in turn, must include warnings and topics for discussion of risk-related issues for deliberation by the Board of Directors. This includes frequent assessments of the risk culture permeating the company.

2.3.1.4 Corporate risk management executive committee[16]

On the existence of a specific GRCorp executive committee, we highlight that this is not a regulatory requirement[17] but is otherwise aligned with best practices of risk management and internal controls. Existence of this committee relates to the level of maturity of the compa-

15. *IBGC, Code of Best Practices of Corporate Governance, op. cit., p 79.*
16. *IBGC considers committees must be advisory bodies assisting the Board of Directors formed by such Board's members. However, in the case of the corporate risk management executive committee, the usual market nomenclature was adopted. This is, therefore, a body subordinated to the Executive Board with daily activities at the company.*
17. *The Federal Government bodies and entities must create a governance, risk, and control committee. Federal government companies must create compliance and risk management policies suitable to their size and consistent with the nature, complexity, and risk of the operations they conduct. Article 23 of Joint Normative Instruction CGU/MP n. 001 of 10/May/2016.*

ny in terms of corporate governance practices and its GRCorp maturity. The risk management executive committee is a collegiate body of the Executive Board, former by persons directly in charge of risks and other executives and professionals able to contribute to the company's decision-making process. This committee may be created as part of the company's risk management learning process or in those companies daily involved with risk taking and/or hedge transactions. The body may issue collegiate recommendations on risk matters to be decided by the Executive Board and propose, jointly with other governance bodies, guidelines, and directions for deliberation by the Board of Directors. The committee may monitor performance of policies and compliance with risk management rules and follow-up on key-risk indicators, orientating decisions when indicators demonstrate the need for decision-making. The committee may also prepare information letters and follow-up reports for the Board of Directors. When the risk management process is ready, the committee activities may be absorbed as part of the agenda in Executive Board meetings.

We suggest the risk executive committee be coordinated by the CEO of the organization, having as members the financial officer, operating officers, internal audit, advisers, and others in charge of risk-involved areas. Its formation depends on the level of complexity of the company's activities, and on the maturity of its risk management process, but must in all cases be composed by persons having suitable skills and abilities and who are able to provide an effective, independent and objective supervision at all times. The committee may further hire qualified professionals to act as specialists.

The main responsibilities of this executive committee are:

- Applying and executing actions related to risk according to the company's GRCorp principles, policies, and strategies.
- Evaluating at the management level, and suggesting changes to GRCorp, as GRCorp, necessary, for deliberation of the Board of Directors
- Monitoring and developing actions related to:
    a. The main risks to which the company is exposed (per type of risk and/or business) and their impacts in the company's risk profile.
    b. Developing and perfecting key-risk indicators and internal controls for monitoring and risk management.
    c. Discussing and choosing risk mitigation alternatives evaluating alternatives recommended
    d. Calculating impacts and probabilities.
    e. Assisting the decision-making process of the Executive Board, mainly in more difficult and complex cases, being part of the process of analysis and risk calculation at collegiate or units' decisions.

2.3.1.5 Executive Board

The Executive Board is directly in charge of all activities of a company, including GRCorp and control activities.

In any company, the CEO is the final depositary of liability for the GRCorp model and internal control system. One of the main aspects of this responsibility is providing the resources necessary to ensure effectiveness of the GRCorp model. More than any other person or function, the CEO is person who must put in place the tone and level of maturity expected by the Board of Directors regarding the GRCorp model, as well as the effectiveness of the internal control system. Naturally, executives of different areas will have different GRCorp and internal control system responsibilities. These responsibilities may largely vary depending on the characteristics of the organization.

The CEO responsibilities include ensuring that all GRCorp components are implemented. The CEO normally complies with their roles by:

- Providing leadership and direction to the Senior Management. Jointly with them, the CEO establishes the values, principles, and main policies (approved by the Board of Directors) forming the foundation of the GRCorp model and internal control system part of such model.
- Meeting with the Executive Board in charge of the several operating areas - sales, marketing, production, finances, human resources - to review their responsibilities as to how they manage risks. The CEO acquires knowledge of the risks inherent to the operations, risk responses and control improvements necessary, and of the stage of initiatives in course. To effectively develop the leadership role, the CEO must clearly define the information needed, particularly for the taking of strategic risks.

Once possessing this information, the CEO will be able to take decisions based on calculated risks and monitor activities and risks related to the company's risk appetite. In the event of a change of circumstances, emergence of new risks, early implementation of strategies or actions indicating a potential mismatch with the company's profile and risk appetite, the CEO will adopt the measures necessary to reinstate alignment and discuss with the Board of Directors the measures to be adopted or else if the company's risk profile must be adjusted.

2.3.2 Defense agents

2.3.2.1 First line of defense - unit managers and persons directly in charge of processes

Unit managers and those directly in charge of processes are entrusted with management of risks related to their units' goals and/or processes, as well as control activities inserted

in such (see Figure 2). These persons understand the strategic goals and align operating and strategic goals. Also, they direct application of GRCorp components and control activities in their spheres of authority, ensuring their application is consistent with the risk profile and appetite. In this sense, responsibility flows downwards, and each executive effectively presides over their acting area. it is important to stress that responsibility for GRCorp must be attributed to all company levels, and not only to the Board of Directors.

2.3.2.2 Second line of defense – GRCorp

This group oversees setting the policies and methodology for the GRCorp model, in addition to playing a relevant role in its development monitoring. The roles and responsibilities of this agent include, among others:

- Being the defender "supporter" of GRCorp within the company (from the strategic to the operating levels).
- Providing the policy, structure, and methodology to identify, analyze and effectively manage its risks aiming to comply with the goals.
- Facilitating the challenge and directing GRCorp activities. However, this will not attribute liability for corporate risk management.
- Ensuring the GRCorp policy and strategy defined by the Board of Directors are effectively operating to achieve the company's purposes.
- Identifying current and emerging issues.
- Identifying changes in the company's implicit risk appetite.
- Assisting the management in developing processes and controls to manage risks.
- Directing the problems identified to those in charge of solving them.
- Being accountable before the Board of Directors or consulting committees to discuss any existing risk issues.

In certain companies, the responsibility for putting in place the internal control system practices' is also shared by this manager.

2.3.2.3 Third line of defense - internal audit[18]

Internal audit plays a key role in assessing effectiveness and determining improvements in GRCorp and internal control systems. In fact, it is part of the GRCorp and internal control monitoring systems. Internal audit is not primarily in charge of establishing and maintaining the GRCorp struc-

18. *Definitions from the IIA which conducted studies, discussed with specialists, and defined the role of internal auditors vis-à-vis risks.*

ture. This task is incumbent upon the CEO and the professionals they appoint but is essential to attest effectiveness of the rules and policies established.

All activities within a company - not merely internal controls and the GRCorp system - are potentially under the scope of authority of internal auditors.

The internal audit is in charge of:

- Assessing reliability of the information, revising effectiveness and efficiency of the transactions, safeguarding compliance with laws, rules, and contracts.
- Examining the internal control system to provide senior management with an assessment of its effectiveness.
- Assisting the CEO and the Board of Directors, via the audit committee, monitoring, examining, evaluating, informing, and recommending improvements to enhance suitability of the internal environment and effectiveness of the GRCorp process.

Internal auditors must be objective while examining the company's activities. This objectiveness is based on the position they hold at the company, directly reporting to the board, audit committee and providing reports to the fiscal council. The main audit executive must be selected and dismissed upon consent of the Board of Directors or audit committee. The internal auditor has access to the Executive Board, audit committee and fiscal council. Internal auditors also play a key role in assisting operating areas in their understanding of internal controls, rules and policies established.

2.3.3 External agents

2.3.3.1 Independent audit

External auditors enable the Executive Board and Board of Directors to have a singular, independent, and objective view potentially contributing to the achievement of the company's goals for outside communication of financial information.

They are in charge of forming an opinion on accounting statements based on the evaluation of the conclusions gathered from audit evidence and expressing this opinion by means of reports drafted in accordance with Brazilian Accounting Rules (see NBC TA 700). External auditors also contribute to the fulfillment of the purposes related to communication of financial information and risk management, conveying useful information to the management so that the latter can comply with its responsibilities regarding the GRCorp and internal control systems.

2.3.3.2 Regulatory bodies

Regulatory bodies directly influence economic freedom and the company's sphere of operations by imposing rules and conducts and sanctions for their breach. In other words, they regulate the business environment surrounding the company.

2.4 Maturity level

This handbook proposes the following maturity levels regarding a company's GRCorp stage: i) initial, ii) fragmented, iii) defined, iv) consolidated and v) optimized. There are different alternatives to build GRCorp governance and reach the desired maturity level. Each company must develop the alternative most suitable to its business profile, company culture, management model and desired maturity level vis-à-vis its GRCorp practices.

Thus, the GRCorp maturity level at an organization is defined by the following aspects:

- Actions adopted to reach the goals and purposes related to GRCorp and internal control system.
- Level of effort (time and investment) deployed to reach such goals and purposes.
- Results obtained, as well as the effectiveness and efficiency of the practices implemented.
- Level of involvement of the professionals with such practices.
- Level of understanding of the company's maturity and of improvement opportunities.

Ultimately, maturity represents comprehension of the current company's position and must determine its goals, in addition to the methods and means adopted to achieve those.

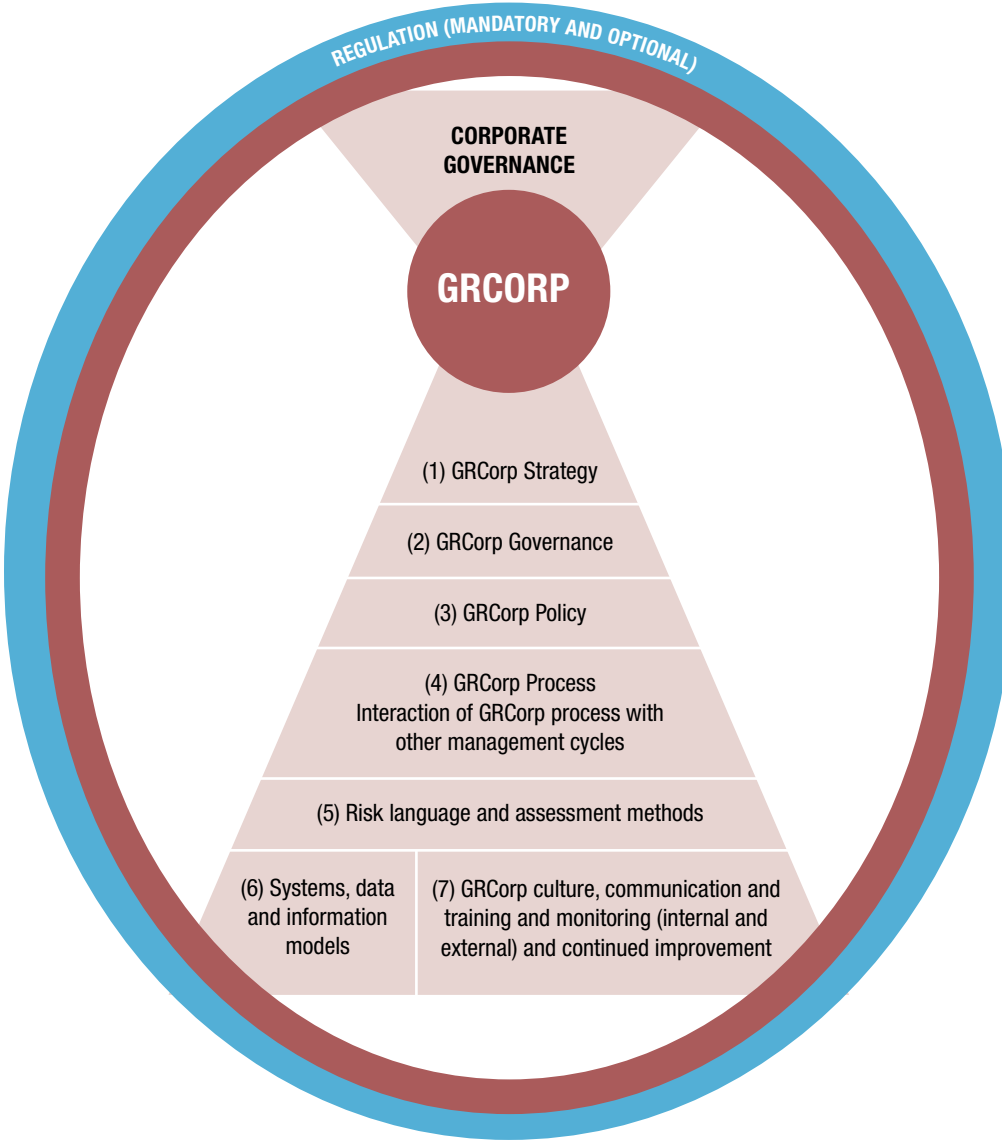
2.4.1 Measuring Maturity

Measurement of the GRCorp maturity status is a key tool for the company's planning, indicating where it currently is, where it intends to go and which actions it must take to reach the desired GRCorp stage.

For such measurement, companies must evaluate the actual capacity of GRCorp practices and understand how and why they need to improve those practices. This assessment will permit companies to document, communicate and schedule improvements to their model.

Figure 3 presents a general view of the GRCorp components integrated to a company´s corporate governance process, considering the main elements necessary to guarantee implementation of GRCorp.

Figure 3 – GRCorp components



As such, the current maturity level of a company may be measured by the responses to the following reflections associated to GRCorp components:

	GRCORP COMPONENT	REFLECTIONS
(1)	GRCorp Strategy	• Are there established GRCorp strategies, objectives, and goals?
(2)	GRCorp Governance*	• Is there an organizational structure with roles and responsibilities clearly defined in GRCorp practices? • Does the structure consider the role of the Board of Directors and Executive Board and of all the three lines of defense detailed in the GRCorp governance model?
(3)	GRCorp Policy	• Are the issues raised above regulated, approved, and disclosed by means of a GRCorp policy?
(4)	GRCorp process and its interaction with the remaining management cycles	• Is there a defined and implemented GRCorp process, with activities of risk identification and assessment (including scenarios), evaluation of control activities, reply, monitoring and communication? • Is there a risk management rule (or its equivalent), internally disclosed, establishing procedures, responsibilities - including reporting responsibilities - segregation of duties, operating boundaries, and the general risk management governance system? • Are GRCorp practices aligned with the remaining control practices? • Is there a defined model to incorporate GRCorp in decision-making processes and management cycles?
(5)	Risk language and assessment methods	• Are there defined risk taxonomy (categories) evaluation methods? • Does the organization employ measurement techniques?
(6)	Systems, data, and information models	• Is the information on the company's risk exposure shared with its different levels and captured in a conscious manner?
(7)	GRCorp culture, communication and training and Monitoring (internal and external) and continued improvement	• Is the GRCorp incorporated into the decision-making process, the organization culture and the daily business management? • Does the company evaluate the understanding of employees about the culture, GRCorp practices and internal control system? • Are the activities of GRCorp communication and culture training performed with the different publics within the company? • Do the governance bodies and three lines of defense permanently monitor GRCorp practices? • Is the GRCorp conducted in a continued manner?

* Here GRCorp governance refers to how the general risk management process, defined in the GRCorp strategy, is incorporated into the company's overall governance process, to ensure the GRCorp strategy is effective and aligned with the company's strategic purposes.

By replying to each of these reflections, the company may self-evaluate and identify the level of maturity and where it stands regarding GRCorp practices, considering the seven dimensions of GRCorp components. Figure 4 indicates the characteristics of the maturity stages proposed in this paper:

Figure 4. Measuring maturity in terms of GRCorp components

	(1) GRCorp Strategy	(2) GRCorp Governance	(3) GRCorp Policy	(4) GRCorp process and its Interaction with the remaining management cycles	(5) Risk language and Assessment methods	(6) Systems, data and information models	(7) Culture, communication and training, monitoring and continued improvement
OPTIMIZED	• Clearly defined risk management strategy, implemented and integrated to the remaining management cycles • Performance goals are aligned with the strategy and risk management	•Goals are clearly defined and aligned between the various activities of the 2nd line of defense, promoting value to the company • The model is a reference in the sector	• Policies and procedures are routinely influenced by third parties and by the sector Policies have an impact over the external business environment	• Risk identification and assessment processes are well integrated into strategic goals • Efficient and coordinated monitoring activities	• Uses consistent and standard approach to define appetite and risk tolerance • Future scenarios and stress tests are used to explore risk analysis	• Integrated technologies enable the company to manage risks and are considered highly effective and recognized as leading practices by the market	• The risk and control culture are effective throughout all levels of the company • Dissemination programs are applied for continued evolution of risk management
CONSOLIDATED	• Risk management strategy clearly defined and implemented • Performance goals are monitored	• Duties of the 2nd line of defense widely encompass company's risks • Company's organizational structure is well defined and aligned with the strategy and objectives	• Policies and procedures are well developed and applied consistently throughout the company • Are continuously updated according to changes in business strategy	• Risk identification and assessment processes are well defined and structured • Business' managers routinely monitor risks associated to their processes	• Uses consistent and standard approach to define appetite and risk tolerance • Stress tests and case analyses are used corporate-wide	• Emerging technologies are used to enable achievement of risk management goals corporate-wide	• The risk and control culture are inserted in the company's daily activities and risks are pro-actively addressed on the levels of process and duties
DEFINED	• Risk management strategy clearly defined and implemented • Performance goals are defined	• Duties of the 2nd line of defense cover business' risks and value-drivers; overlapping may occur • The organizational structure is defined	• GRCorp policies and procedures are formal and consistently communicated company-wide	• A risk-based approach is systematically performed and consistently applied on a corporate level and throughout the company	• There is a standard approach to define the acceptable risk level. However, it is not used by all functions in a consistent manner	• Information and report models are well defined and understood. Reports are prepared with correct and complete information	• Clear communications protocols exist and are open to all employees. Two-way communications with interested parties are encouraged.
FRAGMENTED	• The organization knows where to begin, even if it does not have its destination clear • Performance goals exist	• Duties of the 2nd line of defense focus on historic areas to respond to compliance with regulatory obligations	• Policies and procedures are limited to key-driver areas	• Risk identification and assessment processes are performed as different or separate activities, on demand	• There is no standard approach to define the acceptable risk level • Qualitative and quantitative analyses are performed	•Information and report models are defined by senior management, but are not understood by management or aligned at the organization	• Communications exist but are not formally defined. • Occasional training is conducted
INITIAL	• The organization does not know how, who, when, where and why to implement risk management • Performance goals exist	• 2nd line of defense duties are performed individually, not integrated to strategic vision.	• Policies and procedures are not defined and there is no consistent procedure for their development and maintenance	•Processes and controls supporting risk management are poorly developed • Minimal monitoring activities occur	•There is no standard approach to define the acceptable risk level • Qualitative and quantitative analyses are conducted	• Information and report models are driven by external demands and are not sufficiently defined	• There is no dissemination plan implemented to formalize the main decisions of the company regarding risk practices

In this context, the GRCorp maturity model now proposed derives from the company's governance model.

This handbook proposes defining and implementing all written components, considering companies' particulars, with the decisive participation of the Board of Directors and Executive Board in the definition and monitoring of GRCorp strategy, its governance and policy of GRCorp.

Agents on the second line of defense play the role of operating and monitoring of the functioning of these components, to be performed by the entire company, including the Executive Board and the first line of defense, represented by units' managers and those directly in charge of processes.

Given each company is inserted in an external and internal context determined by its sector, level of operation and regulation and its stakeholders and business model, to position itself and obtain the results of its maturity measurement, it is advisable to assess its stage at each dimension and, subsequently, self-classify in the maturity levels proposed.

It is worth stressing that generally organizations present different maturities for each dimension analyzed. This is part of the process. The entity itself must evaluate its level of maturity on each dimension/stage, based on its reality and future expectations regarding GRCorp practices.

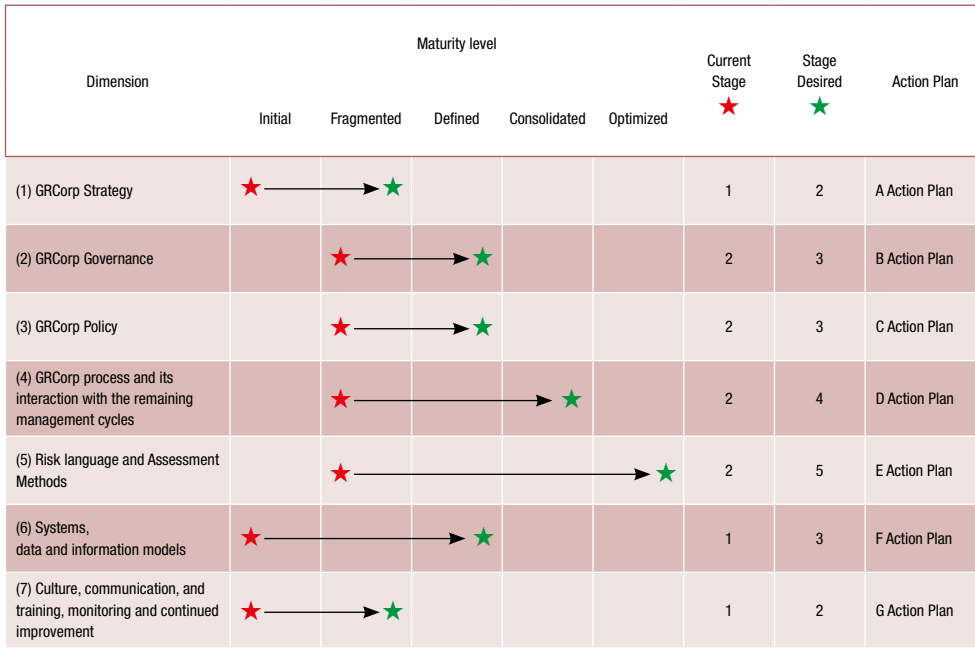
2.4.2 Consolidating the results of the maturity assessment

Once the organization has assessed its GRCorp maturity level on each dimension, the Board of Directors must reflect in which state the organization must be. Subsequently, the Executive Board must develop the necessary actions and define the expected timeframe to reach next stages.

It is relevant to note that the purpose of using the maturity model is to provide the organization with a structured and detailed guide facilitating its incremental improvement in management capacity, enabling definition of a short, medium and long term realistic approach for the GRCorp strategy. Assessment of the maturity model permits the organization to document, communicate and schedule improvements in its GRCorp model.

The final product of this assessment is comprehending the current situation in each dimension, defining the stage desired and actions required to reach the stage desired, which must be subject to action plans. It is also advisable to conduct a research on industry patterns and compare the organization with leading companies in GRCorp practices. Figure 5 presents an example of consolidation of the GRCorp maturity resources.

Figure 5. Example of consolidated GRCorp maturity results



2.4.3 Transforming maturity assessment results in plans or projects

Once the current maturity level is analyzed and the desired level is defined, the company must establish the actions necessary to develop GRCorp practices, appointing a working group to act on each front described, as set forth in the maturity model. Having implemented the actions, improvement plans must be structured, and new evaluations must be conducted.

During the company's development process, the following questions must be asked:

- Is there a person or team in charge of GRCorp improvement?
- Is there an existing improvement plan to guide progression of GRCorp practices from the current to the next maturity level?
- Prior to implementing the improvement plan, were the benefits potentially reachable once the next maturity level is achieved?

The improvement plan is managed with clear objectives and resources. This continuous improvement process must be revised from time to time considering the GRCorp expectations and strategy, tone-at-the-top, identity and culture established by the company. Every company must evaluate the cost/benefit analysis to determine the ideal level to be reached. In certain cases, for example, the search for an optimized level of maturity may not be justified.

3

Conceptual Model for GRCorp Implementation

3. Conceptual GRCorp Implementation Model

Despite the company's trend to indicate a specific risk management model adopted (such as ISO 31.000 and ERM [Coso] Model), there is no single manner to implement the GRCorp nor one single adequate structure for this. The model adopted depends on the company's culture and the business' nature and complexity.

Thus, it is important that, when considering adoption or creation of a GRCorp model, companies analyze their market environment and their own understanding of risk management and corporate culture. They may address the following topics:

- Perception of the value proposal: particularly via the Board of Directors, the company must be sure GRCorp practices are understood as relevant to strengthen corporate governance and reach strategic objectives.
- Dissemination of uniform culture: the Board of Directors, Executives and other officers must exercise their leadership and authority to disseminate GRCorp in all company levels, set expectations, define responsibilities, engage internal public, foster changes and create a culture of risk identification and management in a coordinated and integrated manner.
- Context analysis: the company must evaluate the external context in its cultural, social-economic, political, legal, regulatory, financial, and technological aspects. It must also evaluate the internal context, considering its resource and knowledge resources and possibilities for practical application of company's resources and knowledge to deploy a GRCorp model.

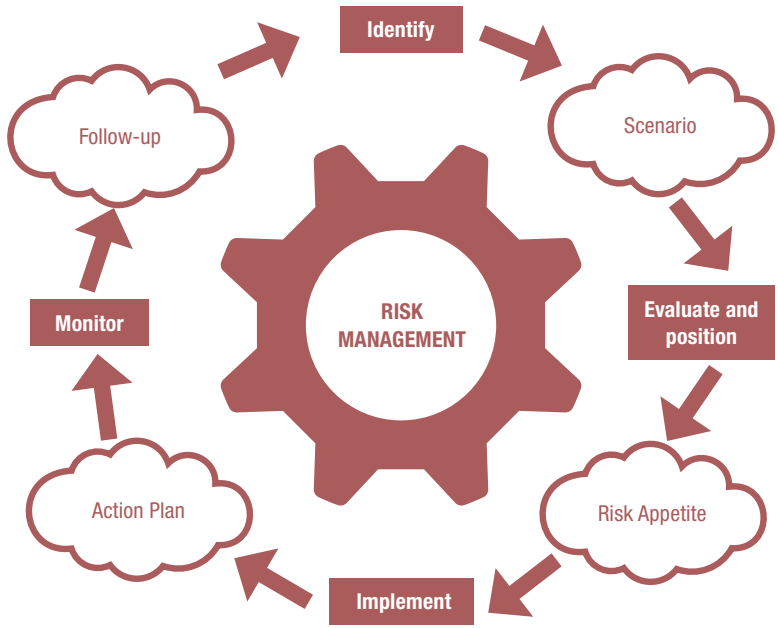
Companies have different objectives, values, principles, and strategies, as well as several organizational structures, diversified operating philosophies and specific capacities to manage risks based on their profiles. But, despite these singularities, there is a common ground when it comes to GRCorp: the company must introduce the practice of considering risks from a structured perspective as part of the decision-making process, and address such risks identifying, assessing and responding consistently with the model adopted. Deployment of the GRCorp model is a process demanding continuous improvement and alignment with the company's strategic planning and identity.

GRCorp governance is formed by the processes of decision-making, supervision, monitoring and ensuring effective operation of the risk management structure. These processes, coupled with managers and executives' knowledge of the business, enable development of mechanisms for decision-making and control of risk exposure. In innovative companies, risk assumption is fomented. Creativity, flexibility and, mostly, fast creative responses raise the need for an innovative risk management culture and a singular GRCorp suitable for a highly modern environ-

ment. This may be a manner to address disruptive risks - those threatening existing technologies, products, or processes by destructing incremental processes - due to presenting solutions in a completely revolutionary manner.

To implement the model proposed in this handbook, we present below the main steps a company must take:

Figure 6. Steps to implement GRCorp



3.1 Step 1 - Identify and classify risks

This concerns defining the external or internal events potentially impacting (from a positive or negative standpoint) the company's strategic objectives, including those related to intangible assets. The process of identification and general risk analysis must be monitored and continuously improved to identify potentially unknown risks, either due to ignorance or lack of attribution of probability (uncertainty), vulnerability or speed. This process must enhance knowledge of risk exposure.

Strategic objectives guide how the organization must work to create and preserve value, which crucially depends on the corporate risk profile. Definition of the risk profile is incumbent upon the executive team, and the Board of Directors must discuss and evaluate (supervision role).

There is no single type of risk classification at the same time consensual, mutual or definitive and applicable to all companies. Classification must be developed according to each company's characteristics, contemplating particularities of the industry, market, and operation segment. For example: consumer goods inventories are less relevant to a bank than to an industry, for which they may represent one of the main risk factors. Likewise, the variables relating to "market risk" are crucial for a bank and may not be so relevant to a determined manufacturing company. Also, the appetite and willingness to accept risk bear subjective components. Thus, companies operating in the same sector and business may have different risk profiles and appetites. Despite the analysis of probabilities and impacts of risks affecting a business field may be general, the appetite and willingness to take risks have subjective components such that companies operating in the same sector and business have different risk profiles and appetites.

One of the manners to classify risks is by developing a risk matrix considering the origins of internal and external events foreign to the company and the nature and types of risks. Further details on risk categories may be found in Annex 2 of this handbook (Examples of risk categories).

3.2 Step 2 - Assess the Risks

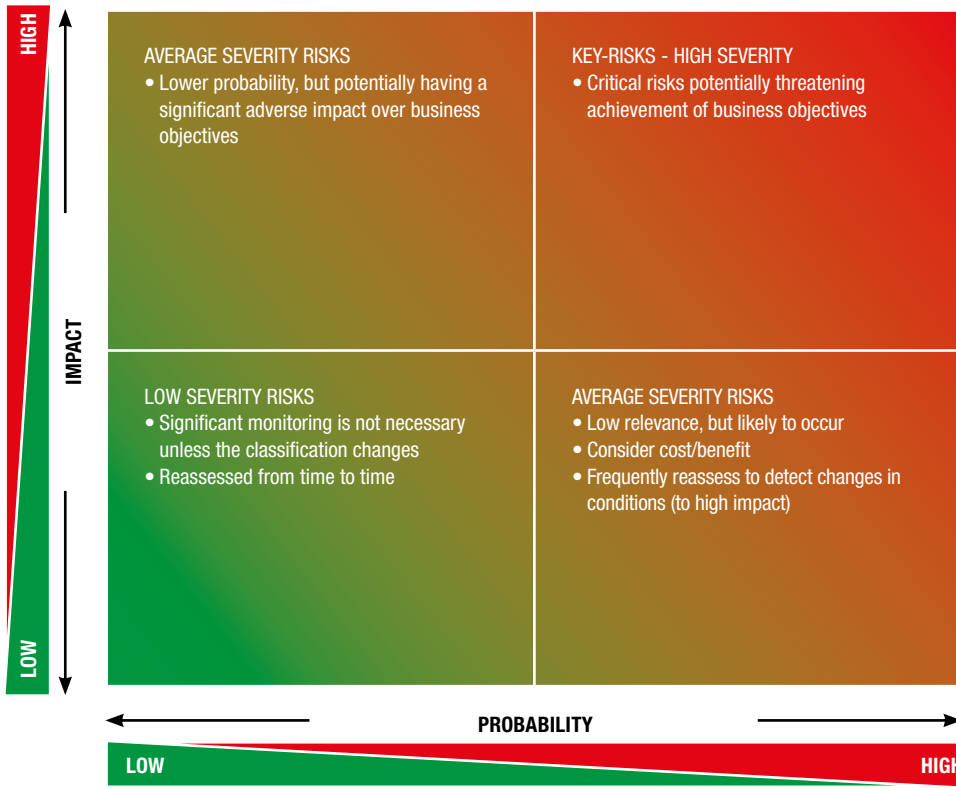
To define which treatment to give a determined risk, the first steps is to determine its potential effect, i.e., the degree of exposure of the company to such risk and capacity and skills to manage it. This degree considers at least three aspects: probability; vulnerability and impact (generally measured by impacts on economic-financial development, corporate image and social, environmental, compliance and strategic factors). Analysis must also consider intangible impacts.

Quantification of the exposure level is not always easy and there may be correlation between risks on two levels: i) events may not be independent; ii) a determined event may generate "multiple impacts", i.e., different effects over different types of risks in different areas. In this case, the degree of exposure will depend on the consolidated financial impact, probability, speed, or joint vulnerability of all events, and must be measured quantitatively and according to the methodology of each company. For cases where independent events affect only a certain area - such as most operational risks - the degree of financial exposure will be calculated based on techniques to adequate to the objectives and risk appetites of each company.

The most common manner to document the impact, probability or vulnerability regarding the risks identified is via a risk map. Figure 7 contains an example of such a risk map (or matrix). Responses to risks must be developed starting from risks located in the upper right corner (key-risks), concentrating high probability and impact events, i.e., high severity. To the extent the level of severity decreases, risks may be monitored and treated in longer terms, as illustrated. But, in no way the so-called medium (those of a low probability and high impact or high probability and low impact) or low severity risks must be ignored, especially the former.

Respecting the characteristics of each company, key-risks must be monitored by management and secondary risks must be monitored by managers at the company's lower risks. It is also necessary to consider the volume of risks at hand so that their management is not too costly or difficult for the company, while also addressing the effects of aggregating many low impact or probability risks. The company must, based on its field of operation and profile, conduct a detailed analysis of how to manage such risks, considering their impact for the company and society at large, being permanently attentive to the externalities[19] generated by its operations.

Figure 7. Risk Matrix



19. *Effects of a transaction impacting third parties who have not consented with or participated in it, not entirely reflected in prices. Externalities may be positive or negative.*

3.3 Step 3 - Implement the risk management and internal control function

To implement the model and promote GRCorp, it is necessary to prepare an architecture to facilitate implementation of GRCorp governance.

Management of risks of a certain process is an activity incumbent upon this process' managers and includes application of market models. The GRCorp management must integrate and drive the several efforts in line with the objectives set forth by management and evaluate the need to establish a risk management executive committee.

3.4 Step 4 - Monitor

3.4.1 Define performance measures

The process of defining performance measurements must include risk management and permanent analysis of effectiveness of the measures defined for performance measurement adjusted to risk and risk taking adjusted to appetite.

The main purpose of defining risk and performance measures must be to evaluate if action plans and respective controls implemented are effective for performance evaluation considering the risks taken.

Once reaching the conclusion the action plans and controls adopted are not sufficient to control risks taken in seeking performance or mitigating company risks, the risk management itself must be revised. Likewise, it is possible that risk taking is below necessary for the desired objectives according to the appetite defined in the strategy. This also indicates the need for reviewing risk management associated to the decision process.

The following issues must be considered at this stage:

- How are the strategic objectives and performance goals defined and managed?
- How is management of strategic objectives and goals conducted, guiding identification of risks, their respective controls and remaining risk architecture components.
- How is early management of changes in business environment conducted, in terms of objectives, goals, risks and controls.

3.4.2 Prepare periodic risk and control reports

The combination of strategic objectives, performance measures, critical success factors, risks and controls must be emphasized. It is also important to note that the number of indicators is limited to those necessary for decision-making, to avoid harming their monitoring.

It is essential to prepare frequent risk reports ensuring their results reach the Executive Board and Board of Directors. Their frequency depends on the type of company and risk reported. For a financial company, it may be key to have a daily report to the management. For another company in which the relevant risk is litigation or long-term strategy, a report may be necessary only when new information justifying its preparation arises.

Periodical risk and control reports are relevant parts of the GRCorp model and may be used in different forms and for different purposes, listed below in a non-exhaustive manner:

- Measure progress and monitor key-goals related to contribution of diverse areas for performance of the company's strategy.
- Issue warnings when corrective actions are necessary.
- Highlight to the Executive Board and Board of Directors the need to evaluate progress of reaching corporate goals.
- Warn the Executive Board and Board of Directors of risk areas demanding attention.
- Share best practices.
- Warn the internal audit department about risk areas in need of a review in internal controls.

Management oversees continuous assessment of suitability and effectiveness of the GRCorp model which must be constantly monitored with the objective of ensuring presence and functioning of all its components over time. Regular monitoring occurs in the normal course of management activities. The scope and frequency of evaluations or specific reviews usually depend on an evaluation of the risk profile and effectiveness of regular monitoring procedures.

The continuous monitoring by GRCorp must include:

- Formal documentation related to risks, evaluation results and tests conducted.
- The report, internal and external (when applicable) documents of deficiencies found and the respective level of threat or exposure noted, actual or potential, and opportunities identified for exploration or reinforcement and review of controls adopted.
- The content of reports on risks and level of strategic information: meaning of problems or abnormalities, culture principles, practical and behavioral implications, information to higher levels, laterals, Executive Board, Board of Directors, audit committee, auditors and other external entities.

Alternatively, the company may adopt key-risk indicators built based on loss tolerance intervals. Whenever the indicator is outside the interval, a warning light will go off in the control panel of the monitoring areas in charge of the second line of defense and/or internal audit indicating the need for intervention.

3.4.3 Record and quantify the losses caused by the occurrence of risk events

The GRCorp management must prepare a knowledge basis for business-related losses to help orienting decisions associated to risks. The process of formation of the operating losses database covers from implementation of capture controls to classification and storage of losses, modeling, and subsequent reporting of operating losses.

The following issues must be considered at this stage:

- How are the data capture and classification controls defined?
- How is database implementation done?
- How is the process of continued validation conducted?
- How is financial/accounting conciliation performed?
- How should the database be structured to provide organized information, including to support treatment of future events not yet identified?

Final Considerations

The Board of Directors must oversee the determination of the strategic objectives and the company's risk profile. Defining such profile consists of identifying the degree of the company's risk appetite and the tolerance to deviations from acceptable levels determined. The Board of Directors must also establish the liability policy for the Executive Board to: i) evaluate the risks to which the company may be exposed; ii) develop procedures for their management; iii) analyze, discuss and approve the risk policy proposed by the risk executive committee.

It is advisable that members of the Board of Directors are knowledgeable about performance indicators to opine on the matters discussed since, without this basic knowledge on corporate finances, corporate risk management will not reach the objectives proposed. It is also advisable that the company maintains a program to communicate the risk management culture to new members of the Board of Directors.

The main role of implementing a solid risk management and control structure is delegated to managers with the audit committee (or instance performing the same role) supervision with the assistance, as needed, from the other lines of defense.

As a starting point to analyze the GRCorp model adopted by the company or to create is, we suggest the Board of Directors discusses with the Executive Board to define:

- The risks affecting the business and how they are integrated to strategic planning.
- How are strategic risks considered and controlled in decision-making processes?
- How are the risk management elements linked to the executives' goals and compensation?
- How does the GRCorp integrate the agenda of the Board of Directors, committees, and managers?

- Who are the risk managers of each process and to whom do they report?
- How is the risk management culture disseminated?
- What are the GRCorp reports, who prepares them and who receives them?
- Which are the controls in place to identify, follow-up and mitigate risks.

The members of the Board of Directors must jointly reflect on the GRCorp process most suitable to the company, answering the following questions:

- Which risks must be brought to the Board of Directors and to the audit committee?
- Which topics merit a deeper discussion?
- Is the relationship between risk and opportunity evaluated?
- Which must be the company's risk appetite?
- Which are the tolerance levels for each risk taken and how does aggregation of risks affect tolerance?
- Does the Board of Director expressly reflect about risks in its decision-making processes?
- Does the Board of Directors routinely test effectiveness of the environment and integrity and compliance culture on all company levels?

These reflections are necessary so the members of the Board of Directors are attentive to the risks such organ must analyze and the role of this organ within the GRCorp structure of the company. Such reflections help avoid penalties and harmful consequences to the company and board members. The concern with risks is key "to foster the Board of Directors in the performance of its role as guardian of the company´s principles, values, corporate purpose and governance system", according to the 5th edition of the IBGC Code of Best Practices of Corporate Governance, item 2.1.

References

ABNT (Associação Brasileira de Normas Técnicas). NBR ISO 31.000: 2009, Gestão de Riscos – Princípios e Diretrizes.

Anbima (Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais). *Perspectivas: A Reforma Financeira Norte-Americana – A Lei Dodd/Frank*. Available on: <http://www.anbima.com.br/data/files/B2/24/B5/51/742D7510E7FCF875262C16A8/Perspectivas_20ANBIMA_20Reforma_20Americana_1_.pdf>. Accessed on: 15 Dec. 2016.

Baraldi, Paulo A. "Apetite e Tolerância aos Riscos". 2013. Available on: <www.riskatrisk.com.br/APETITE_E_TOLERANCIA_AOS_RISCOS1.pdf>. Accessed on: 9 Dec. 2016.

_____. "Como Alinhar Estratégias a Objetivos e Metas e ao Processo de Decisão". 2013. Available on: <www.riskatrisk.com.br/imagens-para-site/Alinhar.Estratégias.Metas.pdf>. Accessed on: 9 Dec. 2016.

_____. *Gerenciamento de Riscos Empresariais*. 2. ed. revista e ampliada. Rio de Janeiro, Elsevier (Editora Campus), 2005.

Bernstein, P. *Desafio aos Deuses: A Fascinante História do Risco*. 3. ed. Campus, Rio de Janeiro, 1996.

BIS (Bank for International Settlements). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework (Basel II [Basileia II])*. 2005. Available on: <http://www.bis.org>.

Brealey, R. & Myers, S. *Financiamento e Gestão de Risco*. Porto Alegre, Bookman, 2005.

Brigham, E. F.; Gapenski, L. C. & Ehrardt, M. C. *Administração Financeira: Teoria e Prática*. São Paulo, Atlas, 2001.

Burnaby, Priscilla & Hass, Susan. "Ten Steps to Enterprise-wide Risk Management". *Corporate Governance*, vol 9, n. 5, 2009.

Coso. *Gerenciamento de Riscos Corporativos – Estrutura Integrada – Sumário Executivo Estrutura*. PriceWaterhouse-Coopers, São Paulo, 2007.

Coso Report. *Internal Control: Integrated Framework*. 1997. Available on: <http://www.coso.org>.

Coso II. *ERM – Enterprise Risk Management*, 2004. Available on: <erm.coso.org>.

Crouhy M.; Galai, D. & Mark, R. *Gerenciamento de Risco: Abordagem Conceitual e Prática – Uma Visão Integrada dos Riscos de Crédito e de Mercado*. Rio de Janeiro/São Paulo, Qualitymark/Serasa, 2004.

Doherty, Neil A. *Integrated Risk Management: Techniques and Strategies for Managing Corporate Risk*. Nova York, McGraw-Hill, 2000.

Faber, M.; Manstetten, R. & Proops, J. *Ecological Economics: Concepts and Methods*. Cheltenham, Edward Elgar Publishing Ltd., 1996.

Galesne, A; Fensterseifer, J. E. & Lamb, R. *Decisões de Investimentos da Empresa*. São Paulo, Atlas, 1999.

Grinblat, M. & Titman, S. *Mercados Financeiros e Estratégia Corporativa*. Porto Alegre, Bookman, 2005.

IBGC (Instituto Brasileiro de Governança Corporativa). *Código das Melhores Práticas de Governança Corporativa*. 5. ed. São Paulo, 2015. Available on: <http://www.ibgc.org.br/index.php/publicacoes/codigo-das-melhores-praticas>. Accessed on: 9 Dec. 2016.

_____. *Guia de Orientação para Gerenciamento de Riscos Corporativos*. São Paulo, IBGC, 2007 (Série Cadernos de Governança Corporativa, n. 3). Available on: <http://www.ibgc.org.br/index.php/publicacoescadernos-de-governanca>. Accessed on: 9 Dec. 2016.

_____. *Visão Evolutiva do Modelo de Gestão de Riscos: Vale e Natura Cosméticos*. São Paulo, IBGC, 2008 (Série Estudos de Caso, n. 1). Available on: <http://www.ibgc.org.br/index.php/publicacoes/estudos-de-casos>. Accessed on: 9 Dec. 2016.

_____. *Gestão Integrada de Riscos: Banco Real e Brasil Telecom*. São Paulo, IBGC, 2008 (Série Estudos de Caso, n. 2). Available on: <http://www.ibgc.org.br/index.php/publicacoes/estudos-de-casos>. Accessed on: 9 Dec. 2016.

_____. *Gestão de Riscos como Instrumento para a Tomada de Decisão: Votorantim Ceculose e Papel (VCP)*. São Paulo, IBGC, 2008 (Série Estudos de Caso, n. 3). Available on: <http://www.ibgc.org.br/index.php/publicacoes/estudos-de-casos>. Accessed on: 9 Dec. 2016.

_____. *Código de Conduta do IBGC*. São Paulo, IBGC, 2013. Available on: <http://www.ibgc.org.br/index.php/publicacoescodigo-de-conduta>. Accessed on: 9 Dec. 2016.

IIA (The Institute of Internal Auditors). *Declaração de Posicionamento do IIA: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles*. Jan. 2013. Available on: <http://www.iiabrasil.org.br/new/2013/downs/As_tres_linhas_de_defesa_Declaracao_de_Posicionamento2_opt.pdf>. Accessed on: 12 Sept. 2016.

Jorion, P. *Value-at-Risk: A Nova Fonte de Referência para a Gestão do Risco Financeiro*. São Paulo, BM&F, 2003.

Kaplan, Robert S. & Mikes, A. "Gestão de Riscos: Um Novo Modelo". *Harvard Business Review*, jun. 2012.

NACD (National Association of Corporate Directors). *Report of the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward*. Washington (DC), NACD, 2009.

Ross, S. A.; Westerfield, R. W.; Jaffe, J. & Lamb, R. *Administração Financeira*. Porto Alegre, Grupo AMGH, 2015.

Sarbanes-Oxley Act. Public Company Accounting Reform and Investor Protection Act of 2002, EUA, 2002.

Scott, H. *Risk Management and Insurance*. 2. ed. Boston, Mc Graw Hill, 2010.

Vaughan, E. J. & Elliot, C. M. *Fundamentals of Risk and Insurance*. 9. ed. Nova York, Wiley, 2003.

World Bank. *Governance and Development*. 1992.

Annexes

ANNEX 1 - Rules and regulations involving risk management

Due to undergoing continuous evolution, the rules cited herein must be directly consulted at their sources. They must also not be considered the sole source for taking decisions.

ISO 9.000: 2015 - Creates the risk mentality at companies seeking ISO certification, which must ensure they have a GRCorp process.

ISO 31.000:2009 - This ISO contains the principles, guidelines, models, and processes for risk management.

ISO Guide 73: 2009 - Supplements ISO 31.000 and presents a collection of the terms and definitions related to risk management.

See both (31.000:2009 and Guide 73:2009) at <http://www.iso.org/iso/iso31000>.

Executive Order n. 8420/2015 - regulates several aspects of the Anti-corruption Act such as criteria for calculation of fines, parameters for evaluation of compliance programs, rules for execution of leniency agreements and provisions on national registers of companies punished. Procedures under the authority of the former Comptroller General (CGU) now Ministry of Transparency, Supervision and Control.

Certain other regulatory instruments are:

- Administrative Rule n. 909 CGU (evaluation of integrity programs)
- Administrative Rule n. 910 CGU (procedure for administrative cases and leniency agreements)
- Normative Instructions GCU n. 01/2015 and 02/2015 (regulating the input of information in the National Register of Inapt and Suspended Companies [Ceis] and in the National Register of Punished Companies [CNEP])
- Joint Administrative Rule n. 2279/2015 CGU and Small and Micro-business Secretariat (anti-corruption rules for small and micro-business companies)
- CGPAR Resolution n. 18 of May 10, 2016
- Normative Instruction MP/CGU n. 1 of 10 May 2016
- Law n. 13303 (State-owned companies Act) of 30 June 2016

ANNEX 2 - Examples of risk categorization

Generally, almost all risks derive from[20]:

- External sources (facts alien to the company)
- Internal sources (arisen within the company)
- Strategy or information for decision-making (in search for its longevity)

External sources

External or environmental risk arises when there are external forces suitable to significantly affect the pillars of the company's objectives and strategies and, in an extreme case, put it out of business.

May derive from a faulty comprehension of client's needs, failure to anticipate or react to competitors' actions, excessive dependence from suppliers, clients, etc. As competitive advantage and ability to support it are more and more temporary, the administration's assumptions about the corporate environment provide a critical breakpoint to prepare and evaluate corporate strategies. These assumptions include strategic profile of the main competitors, social and demographic trends, new technologies bringing opportunities for competitive advantage, political, economic, and regulatory developments. If a company's management does not uniformly comprehend environment risks, its strategic objectives will have no focus. Consequences may be harsh: loss of market share and competitive advantage. In view of the serious consequences deriving from strategic mistakes, management must ensure that business environment premises over which their strategy is based are consistent with reality.

Examples:

- Competition Risk
- Sustainability Risk
- Shareholders' relations Risk
- Capital availability Risk

20. *It is also worth stressing another type of risk we may consider having internal and external natures, currently expanding worldwide and closely related to the disruption caused by the new era of massive information of collective power generate, which has been radically changing business and company models. The risk lies in the so-called worldwide emergence and growth of exponential companies, holders of a massive transforming purpose, transforming and impacting industries and economies, and in the fact that traditional and linear companies, their cultures, people and decisions have the vision and ability to understand and adopt the practices of this trend.*

- Natural disaster
- Political or sovereignty risk
- Legal and regulatory risk
- Financial market risk
- Natural resources risk
- Cyber risk
- Disruptive risk

Internal sources

Risk originated from internal sources normally arise from the risk that companies' business processes:

- Are not clearly defined.
- Are not properly aligned with corporate strategies.
- Are not performed in an effective and efficient manner to meet clients' needs.
- Do not aggregate value to the company.
- Expose financial, physical, and intellectual resources to substantial or unacceptable losses, misappropriation or misuse.

Process risks include:

- Operational Risk
- Cash flow Risk
- Official Risk
- Information Processing/Technology Risk
- Integrity Risk
- Client Satisfaction Risk
- Human Resources Risk
- Product development Risk
- Efficiency and effectiveness risk
- Production capacity risk
- Performance gap risk
- Cycle risk
- Raw materials source and supplies risk
- Obsolescence risk
- Adherence risk
- Commercial disruption risk
- Product/service failure risk
- Social-environmental risk
- Residue - effluents and emissions risk
- Health and safety risks

- Trademark/patent erosion risk

Within company's processes, we may detail financial risks:

- Price risk
- Derivative risk
- Modeling risk
- Interest rate risk
- Exchange risk
- Commodities risk
- Financial instrument risk
- Liquidity risk
- Credit risk
- Concentration risk
- Offsetting risk
- Guarantee risk

Currently, the focus is related to behavior risks of an unexpected and undesired behavior by the employees and compliance faults leading to adverse consequences of bribery, fraudulent financial reports, and other illegal and unethical behaviors.

Another topic refers to the management of risk from uncontrollable external events or integrated and complex systems, with identification of the risks the company must insure or protect with an estimate of the chances of sudden events and case analyses to anticipate and plan external risks, such as risks associated to macroeconomic or political global factors.

Strategy or information for decision-making

Strategy risk or risk of information for decision-making is the risk that information used to support strategic, operational, and financial decisions is not pertinent or accurate.

Several decisions are taken based on performance measures or results from industry analyses or analyses of similar industrial or financial processes. If the indications of such measures are not aligned with corporate strategies or are not realistic, comprehensible and feasible, they will not enable adequate focus and may foster decisions not compatible with the strategies. In this context, procedures and technologies enabling preservation of characteristics known as Cida (confidentiality, integrity, availability and authenticity of information and information systems) are relevant.

Examples:

- Risk of situational assessment
- Corporate activities risk

- Assessment risk
- Company structure risk
- Resource allocations risk
- Planning risk
- Life cycle risk
- Planning and budget risk
- Accounting information risk
- Risk of evaluation of financial reports
- Risk of investment evaluation
- Risk of regulated reports
- Pricing risk
- Contractual commitment risk
- Alignment risk
- Regulated information risk

ANNEX 3 - Policy models and internal risk management standard

3.1 GRCorp policy model

Items potentially forming a GRCorp policy:

Objective

Scope and guidelines of the risk policy

Appetite and acceptable risk limits

Considerations on alignment between risk profile and appetite and corporate strategies.

Considerations on risk limits and those in charge of establishing and monitoring such limits.

Risks and events subject to the risk policy

Considerations on the types of risks affecting the company from internal and external sources.

Considerations on the company's evaluation and treatment of risks.

Comments on risks prioritized by the company.

Company structure for risk management and governance levels

Brief description of the company's management structure.

Brief description of roles attributed to governance levels.

- Board of Directors
- Fiscal Council
- Risk management executive committee
- Executive generally in charge of risk management
- Executive Boards
- In charge of risk management
- Risk management in areas
- Internal Audit

Monitoring Structure

Considerations on risk indicators, their follow-up and assessment.

Considerations on routine follow-up by the Risk Management Executive Committee, Board of Directors and Fiscal Council.

Communication

Considerations on communications processes and guidelines for the communication and sharing of risk-related information within the company.

3.2 3 GRCorp internal rule model

PURPOSES OF THE INTERNAL RISK MANAGEMENT RULE

1. Purposes
2. Scope
3. Approvals
4. Responsibility for updates
5. Responsibility for disclosure and distribution
6. Frequency of updates
7. Target audience and attributions
8. Compliance and Sanctions
9. Validity

APPROACH AND OBJECTIVES OF THE CORPORATE RISK MANAGEMENT

1. Approach of the corporate risk management
2. Objectives of the corporate risk management
3. Life cycle of the corporate risk management

PRINCIPLES OF CORPORATE RISK MANAGEMENT

1. Company's risk appetite
2. Philosophies, principles, policy, guidelines, and procedures
3. Organization model for the function of corporate risk management
4. Risk measurement methodology
5. Risk profile
6. Control environment
7. Limits and compliance
8. Measure of performance of corporate risk
9. Reporting Structure
10. System and Infrastructure

CORPORATE RISK MANAGEMENT MODEL

1. Definition of corporate risk management
2. Establishing the corporate risk management governance
3. Organization model for the function of corporate risk management
4. Common risk language
5. Process and procedures for corporate risk management
6. Priority criteria
7. Update cycle frequency

TOOLS USED IN CORPORATE RISK MANAGEMENT

1. Software
2. Additional Documents

STRENGTHENING OF THE RISK AND CONTROL CULTURE

1. Risk and control culture
2. Training Plan

GLOSSARY OF TERMS

1. Glossary of terms
2. Bibliography

ANNEX 4 - Glossary

Risk aggregation: Process analyzing the joint effects resulting from different risks or the effects of the same risk over various systems, business areas or different processes at the company.

Risk appetite: Represents the level of risk the company may take as established by its vision and mission, indicating the level of exposure acceptable in its search for value.

Risk capacity: Is defined by the maximum impact resulting from a risk that the company is capable of bearing without threatening its continuity.

Risk culture: The risk culture of a company is a product of its identity and refers to the body of its ethical standards, values, attitudes and behaviors accepted and practiced, and of the dissemination of risk management as part of the overall decision-making process on all levels. It is set by the speech and behavior of the Board of Directors and Executive Board and the company's risk appetite.

Risk owner: Is designated by the Executive Board as the person in charge of identifying and effectively managing the risks in their area of operations. Must have defined roles and responsibilities to select and apply risk responses and sufficient authority to prioritize actions related to management risk at their area and be integrated to the general risk governance process of the company.

GRCorp strategy: the definition of expectations, objectives, goals, investments, and performance related to the company's GRCorp practices. It defines where the company intends to be in terms of GRCorp and the means used to reach the objectives.

Risk exposure: refers to the possibility of the company being affected by a given risk. Examining if there is exposure to a certain risk is important as a company operating in a given sector may not be exposed to determined risks affecting other companies of the same sector.

GRCorp Governance: refers to the roles and responsibilities of each of the company's governance agents, from the employees involved in management who must be in charge of controlling direct risks of their activities up to the members of the Board of Officers and Executive Board. The flow of information related to control of risks and transparency of this data is also part of the company's GRCorp governance, concerning the proper decision forums, which is their jurisdiction, roles and responsibilities and how are they composed. Directs and must be inserted in the risk policy and internal rule of risk management.

Key-risk indicators: the indicators discussed and defined by the Board of Directors and Executive Board to follow-up on the performance goals associated to the risk profile accepted by the company. Key-indicators show warning levels for action by the Board in revising the strategy.

Risk map (matrix): tool graphically depicting risks of low probability and impact, low probability and high impact, high probability and low impact, and high probability and impact. See an example of risk map in item 3.2 of this handbook.

Maturity of the risk management model: model for comprehension of the current stage of the company's risk management and governance processes. To assess maturity, the following must be analyzed: actions adopted to reach GRCorp goals and objectives, time and investment efforts, effectiveness and efficiency of the practices adopted, involvement of professionals, understanding of the risk management process as part of the culture, company structures involved with GRCorp, consideration of how the risks are integrated in the decision-making process on all levels and the governance process as a whole.

Internal risk management rule: it is an internal document of the company containing its orientations regarding GRCorp. Must be known by all employees involved in decision-making processes. The internal rule details the company's view of its risk appetite and profile and provides the basis for tolerance of each risk based on parameters of key-risk indicators. It must address GRCorp objectives, contain guidelines, the organization model of the GRCorp activity designating those directly in charge of the risks, their reporting structures and integration of internal control system with GRCorp governance. The rule establishes procedures, responsibilities, segregation of activities, operating boundaries, and operation of the general system of risk management governance. Annex 3 of this handbook contains a model of internal GRCorp rule.

Risk profile: shows the level of risk for a determined performance and its behavior trend when the company acts to explore opportunities or minimize potential impacts.

Risk policy: a formal declaration by the company describing to the market its main understandings and view on risks, generally describing how it conducts risk management and the objectives and strategies of the risk management policy. Brings considerations on the company's risk appetite and profile including, as the case may be, general thoughts on risks for which protection is sought, instruments for protection, the company's risk management and internal control structures to check effectiveness of the risk management policy and overall risk governance process. The risk policy is disclosed to the market such as the remaining policies declared by the company and must be the subject of discussion for knowledge of all company's employees. Annex 3 of this handbook contains a model of GRCorp policy.

Risk: the possibility of occurrence of events affecting the ability of a company to reach its objectives.

Risk sensitivity: refers to how the company is affected by a given risk. It is determined based on the size of the or relevance of its impact, possibility of its occurrence and the company's capacity and promptness to react and respond to this risk.

Risk tolerance: establishes the acceptable variations of the limits set for a company's acceptable risks.

Maximum risk tolerance: it is determined by the point where the risk profile reaches acceptable exposure determined by risk appetite.

Master Sponsor

Deloitte.

Deloitte offers services in the Audit, Corporate Consulting, Tax Consulting, Risk Management Consulting, Financial Advisory and Outsourcing areas for a broad range of clients. With a global network of member firms in more than 150 countries, Deloitte gathers exceptional skills and deep local knowledge to assist clients in reaching the best performance, whichever is their segment or region of operation.

In Brazil since 1911, Deloitte is one of the market leaders and its more than 5,500 professionals are recognized by integrity, expertise, and ability to transform their knowledge in client solutions. Its activities cover the entire domestic territory, with offices in São Paulo, Belo Horizonte, Brasília, Campinas, Curitiba, Fortaleza, Joinville, Porto Alegre, Rio de Janeiro, Recife, Ribeirão Preto and Salvador.

In the corporate risk management area, Deloitte benefits from the largest professional structure exclusively dedicated to this activity in Brazil, helping clients to address all challenges of this kind. Our multidisciplinary vision has also provided a singular position to contribute to the improvement of companies' corporate governance. Go to our website for an array of contents and solutions on risk management and corporate governance, among other business topics.

www.deloitte.com.br

Co-sponsor

Parker Randall Brasil

sabesp

Support

- Carlos Sá
- CIP – Câmara Interbancária de Pagamentos
- Erlon Lisboa de Jesus
- Fernando Nicolau Freitas Ferreira
- Mario Filipini
- Mercedes Stinco
- Muller & Sinergy Consulting
- PFM Consultoria e Sistemas

Corporate Governance Handbooks

Founded on November 27, 1995, the Brazilian Institute of Corporate Governance (IBGC), a civil organization, is the Brazilian reference and one among the main reference organizations for corporate governance worldwide. Its purpose is to generate and disseminate knowledge on the best corporate governance practices and influence the most diverse agents in its adoption, contributing to the sustainable development of organizations and, consequently, to a better society.

Corporate Governance Handbooks

Master Sponsor:

Deloitte.

Co-sponsor:

Parker Randall Brasil

sabesp

Partnership

IDB | Invest

IBGC | Instituto Brasileiro de Governança Corporativa

Av. das Nações Unidas, 12.551
21º andar - Brooklin Novo
04578-903 - São Paulo - SP
Tel.: 55 11 3185.4200

ISBN: 978-65-86366-28-0
9 786586 366280