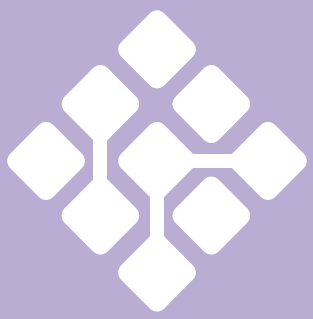


ForRisco

2nd Edition

2nd Edition

Revised and updated version: format change, paging and revision in the diagramming.

ForRisco: risk management in public institutions in practice/Paulo Henrique de Souza Bermejo et al.

Brasília/DF: Editora Evobiz, 2020.

2nd edition

208 p.; 16x23 cm
Contains bibliography

1. Risk Management - Public Institutions. 2. Risk Management in practice. 3. Methodology for risk management. 4. Software platform for Risk management. 5. ForRisco. I. Bermejo, Paulo Henrique de Souza. II. Sant'Ana, Tomás Dias. III. Salgado, Eduardo Gomes. IV. Mendonça, Lucas Cezar. V. Anjos, Fábio Henrique dos. VI. Alves, Gustavo de Freitas. VII. Borges, Guilherme Henrique Alves. VIII. Pagotto, Daniel do Prado. IX. Pagliares, Rodrigo Martins. X. Pinheiro, Iara Ferreira. XI. Salomão, Inessa Laura. XII. Silva, Priscila Daniel de Paiva Gama. e XIII. Neves, Thiago José Galvão das.

ISBN: 978-65-86351-01-9

ForRisco

2nd edition

ForRisco:
risk management in
public institutions in practice

FOR Platform

TECHNICAL DATA

Authors

Paulo Henrique de Souza Bermejo, Dr.
Tomás Dias Sant'Ana, Me.
Eduardo Gomes Salgado, Dr.
Lucas Cezar Mendonça, Me.
Fábio Henrique dos Anjos, Me.
Gustavo de Freitas Alves, Me.
Guilherme Henrique Alves Borges, Me.
Daniel do Prado Pagotto, Me.
Rodrigo Martins Pagliares, Dr.
Iara Ferreira Pinheiro, Me.
Inessa Laura Salomão, Dra.
Priscila Daniel de Paiva Gama e Silva, Esp.
Thiago José Galvão das Neves, Me.
Everton Leonardo de Almeida, Esp.

About the authors

Paulo Henrique de Souza Bermejo

He holds a doctor´s degree in Engineering and Knowledge Management from the Federal University of Santa Catarina (Universidade Federal de Santa Catarina - UFSC), with a post-doctorate degree in Innovation from Bentley University (USA). He is currently an adjunct professor of the Administration Department at the University of Brasília (Universidade de Brasília - UnB). Coordinator of the Research and Development Center for Excellence and Transformation of the Public Sector (NExT) of UnB; a permanent professor of the Postgraduate Program in Administration (academic master's and doctorate degrees) and of the Professional Master's Degree in Public Administration, both from UnB. Contact: paulobermejo@next.unb.br

Tomás Dias Sant'Ana

He is a doctoral candidate in Administration at the University of Brasilia (Universidade de Brasília - UnB) and holds a master´s degree in Computer Science from the University of Sao Paulo (Universidade de São Paulo - USP). He is currently an adjunct professor of the Department of Computer Science at the Federal University of Alfenas (Universidade Federal de Alfenas - UNIFAL-MG). He was Pro-Rector of Planning, Budget and Institutional Development between 2010 and 2018 at UNIFAL-MG. Contact: tomas@bcc.unifal-mg.edu.br.

Eduardo Gomes Salgado

He holds a doctor´s degree in Mechanical Engineering from the Sao Paulo State University (Universidade Estadual Paulista - UNESP), and a postdoctoral degree from the University of Glasgow at the Adam Smith Business School (UK); a master´s degree in Production Engineering and graduated in Industrial Engineering from the Federal University of Itajubá (Universidade Federal de Itajubá - UNIFEI). He is currently a professor and Adjunct Pro-Rector of Planning, Budget and Institutional Development at the Federal University of Alfenas (Universidade Federal de Alfenas - UNIFAL-MG). Contact: eduardosalgado@bcc.unifal-mg.edu.br

Lucas Cezar Mendonça

He holds a Master's degree in Public Administration from the Federal University of Lavras (Universidade Federal de Lavras - UFLA), and a post-graduate degree in Corporate Finance from the University Center of Southern Minas (Centro Universitário do Sul de Minas - UNIS-MG); graduated in Economic Sciences from the Cenecista College of Varginha (Faculdade Cenecista de Varginha - FACECA). He is currently Pro-Rector of Planning, Budget and Institutional Development at the Federal University of Alfenas (Universidade Federal de Alfenas-UNIFAL-MG). Contact: lucas.mendonca@unifal-mg.edu.br

Fábio Henrique dos Anjos

He holds a Master´s degree in Public Management from the Federal University of Alfenas (Universidade Federal de Alfenas - UNIFAL-MG), and a bachelor´s degree in Administration from the Federal University of Lavras (Universidade Federal de Lavras - UFLA). He was substitute professor in the course of Public Administration of the Institute of Applied Social Sciences at UNIFAL-MG - Varginha campus. He is currently a Senior Analyst of Planning and Management for the ForRisco Project and a researcher at the UnB's R&D Center for Excellence and Transformation of the Public Sector (NExT). Contact: fabioanjos@next.unb.br

Gustavo de Freitas Alves

He is a doctoral candidate in Administration at the University of Brasilia (Universidade de Brasília - UnB); holds a Master´s degree in Applied Computing with emphasis in Risk Management also from UnB; earned his Bachelor´s degree in Computer Science with emphasis in Computer Networks from the Catholic University of Brasilia (Universidade Católica de Brasília - UCB). He is currently a consultant in Information Technology and Risk Management. Contact: gustavo.ucb@gmail.com

Guilherme Henrique Alves Borges

He holds a Master´s Degree in Public Administration from the Federal University of Lavras (Universidade Federal de Lavras - UFLA) and graduated in Information Systems from the same institution. He is a specialist in process management and business management systems. He currently is

the manager of a company and software projects. Contact: ghaborges@gmail.com

Daniel do Prado Pagotto

He holds a Master´s degree in Business Administration from the Federal University of Goiás (Universidade Federal de Goiás - UFG), with emphasis on entrepreneurship and innovation; a Bachelor's degree in Business Administration from the University of Brasilia (UnB), with a sandwich period at Kirkwood Community College (USA). He is currently a researcher and project leader at UnB's R & D Center for Excellence and Transformation of the Public Sector (NExT). Contact: danielpagotto@next.unb.br

Rodrigo Martins Pagliares

He holds a Doctor´s degree from the Graduate Program in Electrical Engineering and Computing at the Technological Institute of Aeronautics (Instituto Tecnológico de Aeronáutica - ITA); a Master´s degree in Computer Science from the Federal University of Santa Catarina (Universidade Federal de Santa Catarina - UFSC). He has a Bachelor's Degree in Computer Science from the Federal University of Ouro Preto (Universidade Federal de Ouro Preto - UFOP). He is currently a professor of the Bachelor's Degree Program in Computer Science at the Federal University of Alfenas (Universidade Federal de Alfenas - UNIFAL-MG), and an institutional development coordinator at the same institution. Contact: pagliares@bcc.unifal-mg.edu.br

Iara Ferreira Pinheiro

She holds a Master´s degree in Public Education Management and Evaluation from the Federal University of Juiz de Fora (Universidade Federal de Juiz de Fora - UFJF) and a Post-graduate degree in Controllership and Business Finance from the Federal University of Lavras (Universidade Federal de Lavras - UFLA). She graduated in Accounting Sciences from the University of Brasília (UnB) and is currently an effective servant of the Ministry of Education, serving as undersecretary of Planning and Budget. Contact: iarapinheiro@mec.gov.br

Inessa Laura Salomão

She holds a Ph.D. in Energy Planning from the Federal University of Rio de Janeiro (Universidade Federal do Rio de Janeiro - UFRJ); a Master's degree in Production Engineering from the Alberto Luiz Coimbra Institute of Graduate Studies and Research in Engineering (COPPE); and graduated in Economics from the University of São Paulo (Universidade de São Paulo - USP). She is currently an adjunct professor of the Production Engineering course at the Celso Suckow da Fonseca Federal Center for Technological Education (CEFET/RJ). Contact: inessa.salomao@cefet-rj.br

Priscila Daniel de Paiva Gama e Silva

She holds a postgraduate degree in Public Management from Signorelli International College and a degree in Business Administration from the Celso Suckow da Fonseca Federal Center for Technological Education (CEFET/RJ). She holds a position as an administrator at CEFET/RJ, where she currently serves as head of the Department of Institutional Development. Contact: priscila.paiva@cefet-rj.br

Thiago José Galvão das Neves

He holds a Master's degree in Accounting from the Federal University of Pernambuco (Universidade Federal de Pernambuco - UFPE). He is a specialist in Auditing, Controlling and Accounting Skills by IBPEX; graduated in Accounting Sciences from UFPE. He is currently Pro-Rector of Planning, Budget and Finance at UFPE, a professor of the Specialization Course in Accounting and Government Controllership, and accountant at the same institution. He is the coordinator of the National Forum of Pro-Rectors on Planning and Administration of Federal Institutions of Higher Education (FORPLAD). Contact: thiago.neves@ufpe.br

Everton Leonardo de Almeida

Master in Business Administration from the Federal University of Lavras (UFLA). MBA in Project Management from Anhanguera College. Bachelor of Information Systems from the Federal University of Lavras (UFLA). He is currently manager of the NexT / UnB information technology team. Contact: everton.almeida@next.unb.br

National Association of Directors of Federal Institutions of Higher Education

ANDIFES/BRAZIL

Reinaldo Centoducatte (UFES)
President

João Carlos Salles Pires da Silva (UFBA)
First Vice-President

Margarida de Aquino Cunha (UFAC)
Alternate

Edward Madureira Brasil (UFG)
Second Vice-President

Cleuza Maria Sobral Dias (FURG)
Alternate

Gustavo Henrique de Sousa Balduino (ANDIFES)
Executive Secretary

National Forum of Pro-Rectors on Planning and Administration of Federal Institutions of Higher Education

FORPLAD/IFES/BRASIL

Thiago José Galvão das Neves (UFPE)
National coordinator
(November/2017 - November/2019)

Vilson Ongaratto (UTFPR)
First Vice-coordinator

Tânia Mara Francisco (UNIFESP)
Second Vice-coordinator

Dulce Maria Tristão (UFMS)
First Secretary

Kleomara Gomes Cerquinho (UFAM)
Second Secretary

Administration committee

Inessa Laura Salomão (CEFET/RJ)
Coordinator

Wilma Gomes Silva Monteiro (UNIFAP)
Vice-coordinator

Planning and evaluation committee

Raquel Trindade Borges (UFPA)
Coordinator

Pedro Fiori Arantes (UNIFESP)
Vice-coordinator

Forrisco project working group

Vander Matoso (UFGD)
Coordinator for the Administration Committee

Joeder Campos Soares (UFSM)
Coordinator for the Planning and Evaluation Committee

Members of the working group

Alessandra Dahmer
Federal University of Health Sciences of Porto Alegre
(Universidade Federal de Ciências da Saúde de Porto Alegre - UFCSPA)
Alex Fraga
Federal University of Grande Dourados
(Universidade Federal da Grande Dourados - UFGD)
Álvaro Fabiano Pereira de Macedo
Federal Rural University of the Semi-Arid
(Universidade Federal Rural do Semi-Árido UFERSA)
Aluízio Mário Lins Souto
Federal University of Paraíba *(Universidade Federal da Paraíba - UFPB)*
Anailson Márcio Gomes
Federal University of Rio Grande do Norte
(Universidade Federal do Rio Grande do Norte - UFRN)
André Macedo Santana
Federal University of Piauí *(Universidade Federal do Piauí - UFPI)*
Auton Peres de Farias Filho
Federal University of Acre *(Universidade Federal do Acre - UFCA)*
Carlece Carvalho Duarte
Federal University of Roraima *(Universidade Federal de Roraima - UFRR)*
Carolina Guimarães Raposo
Federal Rural University of Pernambuco *(Universidade Federal Rural de Pernambuco - UFRPE)*
Darizon Alves de Andrade
Federal University of Uberlândia *(Universidade Federal de Uberlândia - UFU)*
Deylon Gomes de Moraes
Federal University of Tocantins *(Universidade Federal do Tocantins - UFT)*
Edson Nascimento
Federal University of Maranhão *(Universidade Federal do Maranhão - UFMA)*
Eunice Alves de Oliveira
Federal University of Roraima *(Universidade Federal de Roraima - UFRR)*
Fernando Costa Archanjo
Federal University of the Jequitinhonha and Mucuri Valleys
(Universidade Federal dos Vales do Jequitinhonha e Mucuri - UFVJM)

Forrisco project implementation team

Bruno Augusto Terra
Cléber Monterani Tavares
Daniel do Prado Pagotto
Débora Silva Barroso de Araújo
Diogo Guilherme Pereira
Edney Pereira Pinto
Eduardo Gomes Salgado
Everton Leonardo de Almeida
Fábio Henrique dos Anjos
Guilherme Henrique Alves Borges
Gustavo de Freitas Alves
Gustavo Soares Melo
Lucas Cezar Mendonça
Maik de Souza
Marcelo Cezar Costa
Marcelo Penha Fernandes
Paulo Henrique de Souza Bermejo
Pedro de Almeida Marques
Rebeca Nonato Domingos
Renato Resende Ribeiro de Oliveira
Romário da Silva Borges
Tomás Dias Sant'Ana
Vinícius Alex da Silva
Vinícius Nogueira da Silva
Wagner Vilas Boas de Souza

2nd Edition

Revised and updated version: format change, paging and revision in the diagramming.

List of illustrations

Figure 1 | Generic risk management process 51

Figure 2 | Risk management methodology proposed by ERM-COSO 55

Figure 3 | Risk management methodology proposed by ISO 31000 60

Figure 4 | Relationship between M_o_R-OGC documents 66

Figure 5 | Risk management methodology proposed by M_o_R-OGC 67

Figure 6 | Comparison between risk management methodologiesv 71

Figure 7 | Methodology of integrity, risk and internal control management 80

Figure 8 | Risk management methodology proposed by MGR-SISP 82

Figure 9 | IBGC Risk Management - Maturity Assessment 88

Figure 10 | Maturity level structure for continuous improvement 94

Figure 11 | Risk map structure between departments 97

Figure 12 | Risk map structure: department's risks 98

Figure 13 | Preparation of summarized report: threats and opportunities 99

Figure 14 | Conception of logic in decision trees 101

Figure 15 | Stages for conducting the case study 130

Figure 16 | Cycle of risk management at UNIFAL-MG 137

Figure 17 | Form for monitoring units and risks 138

Figure 18 | Risk Identification Form 139

Figure 19 | Structure of the Risk Management Plan of UNIFAL-MG 142

Figure 20 | Implementation of the mapping process in CEFET/RJ 147

Figure 21 | Stages of risk management in CEFET/RJ 151

Figure 22 | ForRisco Methodology for Risk Management in Public Administration 157

Figure 23 | Model of risk management stages of the ForRisco methodology 160

Figure 24 | Prerequisites for the risk management stages of the ForRisco methodology 162

Figure 25 | Stages of the risk management process proposed by the ForRisco methodology 164

Figure 26 | Addition of a new Risk Management Policy 181

Figure 27 | New Risk Management Plan 181

Figure 28 | New risk and risk information 182

Figure 29 | Facility in the creation of new risk plans: the duplicate plan feature 183

Figure 30 | Real-time monitoring of risk management with the ForRisco Platform 183

List of tables

Table 1 | Questions to be answered by the stages of the methodologies 52

Table 2 | Risk management components and principles proposed by the ERM-COSO review 57

Table 3 | Tools used for the risk assessment process 62

Table 4 | Approach to risk management - Documents 65

Table 5 | Techniques in Appendix B of the M_o_R 68

Table 6 | M_o_R maturity scale 70

Table 7 | Comparison between the definitions of the main market methodologies 73

Table 8 | Guidance books and methodologies on risk management of the Brazilian Public Administration. 77

Table 9 | Tasks in the MGR-SISP 83

Table 10 | Reflections on the components of GRCorp 89

Table 11 | Measurement of maturity in relation to components 90

Table 12 | Comparison between the definitions of the main methodologies of the Brazilian Public Administration 95

Table 13 | Laws and regulations on risk management in Brazil 104

Table 14 | Software tools included in the research. 110

Table 15 | Softwares evaluated and their main characteristics 113

Table 16 | Risk typology 135

Table 17 | Actors and description of responsibilities 136

Table 18 | Probability and impact 139

Table 19 | Risk Classification Matrix 140

Table 20 | Tool 5W2H 141

Table 21 | Factors considered for probability analysis 148

Table 22 | Risk classification by se ctor/department 149

Table 23 | Risk Matrix Probability vs. Impact 150

Table 24 | Confrontation between the stages of risk management of UNIFAL-MG and CEFET/RJ and the ForRisco methodology 176

Table 25 | Items for the risk recording form 198

Table 26 | Interpretation of the level of maturity of risk management in public organizations 202

List of abbreviations and acronyms

ABNT	Associação Brasileira de Normas Técnicas *(Brazilian Association of Technical Standards)*
ANDIFES	Associação Nacional dos Dirigentes das Instituições Federais de Ensino Superior *(National Association of Leaders of Federal Institutions of Higher Education)*
APF	Administração Pública Federal *(Federal Public Administration)*
AP	Administração Pública *(Public Administration)*
AUDIN	Auditoria Interna *(Internal Audit)*
BPM	Business Process Management
CBOK	Commom Body of Knowledge
CDI	Coordenadoria de Desenvolvimento Institucional *(Institutional Development Coordinating Body)*
CEFET/RJ	Centro Federal de Educação Tecnológica Celso Suckow da Fonseca – Rio de Janeiro *(Celso Suckow da Fonseca Federal Center for Technological Education – Rio de Janeiro)*
CGRC	Comitê de Governança, Riscos e Controle *(Governance, Risk and Control Committee)*
CGU	Controladoria-Geral da União *(Comptroller General of the Union)* Coordenadoria-Geral *(General Coordinating Body)*
CGE	Control Objectives for Information and Related Technologies
COBIT	Conselho Diretor *(Board of Directors)*
CODIR	Conselho Nacional das Instituições da Rede Federal de Educação
CONIF	Profissional, Científica e Tecnológica *(National Council of Institutions of the Federal Network of Professional, Scientific and Technological Education)*
COR	Coordenadoria de Orçamento *(Budget Coordinating body)*
CPO	Coordenadoria de Projetos e Obras *(Projects and Works Coordinating Body)*
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CVM	Comissão de Valores Mobiliários *(Brazilian Securities and Exchange Commission)*
DEDIN	Departamento de Desenvolvimento Institucional *(Department of Institutional Development)*
DIGES	Diretoria de Gestão Estratégica *(Board of Strategic Management)*
DIPPG	Diretoria de Pesquisa e Pós-Graduação *(Board of Research and Graduate Studies)*

DIRAP	Diretoria de Administração e Planejamento *(Board of Management and Planning)*
DIREG	Direção-Geral *(General Direction)*
DIREN	Diretoria de Ensino *(Board of Education)*
DIREX	Diretoria de Extensão *(Board of Extension)*
DSIC	Departamento de Segurança da Informação e Comunicações *(Department of Information and Communications Security)*
ERM	Enterprise Risk Management
ETIR	Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais *(Treatment and Incident Response Teams in Computer Networks)*
FACEPE	Fundação de Apoio à Cultura, Ensino, Pesquisa e Extensão de Alfenas *(Foundation for Support to Culture, Education, Research and Extension of Alfenas)*
FDA	Food and Drug Administration's
FERC	Federal Energy Regulatory Commission
FMI	International Monetary Fund
FORPLAD	Fórum Nacional de Pró-Reitores de Planejamento e Administração *(National Forum of Pro-Rectors on Planning and Administration)*
GIRC	Gestão de Integridade, Riscos e Controle Interno *(Integrity, Risks and Internal Control Management)*
GR	Gesão de Riscos *(Risk management)*
GRCORP	Gerenciamento de Riscos Corporativos *(Corporate Risk Management)*
GRSIC	Gestão de Riscos de Segurança da Informação e Comunicação *(Information and Communication Security Risk Management)*
IBGC	Instituto Brasileiro de Governança Corporativa *(Brazilian Institute of Corporate Governance)*
IFES	Instituição Federal de Ensino Superior *(Federal Institution of Higher Education)*
IFTO	Instituto Federal do Tocantins *(Federal Institute of Tocantins)*
ITIL	Information Technology Infrastructure Library
INC	Instrução Normativa Conjunta MP/CGU nº 01/2016 *(Joint Normative Instruction)*
ISO	International Organization for Standardization
KPI	Key Performance Indicator
KRI	Key Risk Indicators
M_o_R	Management of Risks

MEC	Ministry of Education
MGR-SISP	Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações *(Methodology of Information and Communications Security Risk Management)*
MP	Ministry of Planning, Development and Management
MTP	Passive Technical Means
NEXT/UNB	R & D Center for Excellence and Transformation of the Public Sector/ University of Brasília
NBR	Norma Brasileira *(Brazilian Standard)*
NIST	National Institute of Standards and Technology
OCDE	Organização para Cooperação e Desenvolvimento Econômico *(Organization for Economic Cooperation and Development)*
OGC	Office for Government Commerce
PDI	Plano de Desenvolvimento Institucional *(Institutional Development Plan)*
PE	Plano Estratégico *(Strategic Plan)*
PTRs	Plano de Tratamento de Riscos *(Risk Treatment Plan)*
RACI	Responsible, Accountable, Consulted, Informed
RH	Human Resources
SETEC	Secretaria de Educação Profissional e Tecnológica *(Secretariat of Professional and Technological Education)*
SIC	Segurança da Informação e Comunicação *(Information and Communication Security)*
SIEM	Security Information and Event Management
SISP	System of Administration of Information Technology Resources
SOC	Security Operations Center
SOX	Sarbanes-Oxley
SWOT	Strengths, Weakness, Opportunities, Threats
TCU	Tribunal de Contas da União *(Brazilian Federal Court of Auditors)*
TI	Information Technology
UFLA	Universidade Federal de Lavras *(Federal University of Lavras)*
UNB	Universidade de Brasília *(University of Brasília)*
UNIFAL-MG	Universidade Federal de Alfenas – Minas Gerais *(Federal University of Alfenas - Minas Gerais)*

Contents

1. Preface 37

2. The for platform for public governance 41
2.1. For Platform 42
2.2. ForPDI - Strategic Plan Management/PDI 43
2.2.1. ForPDI Methodology 43
2.2.2. ForPDI Software 44
2.2.3. ForPDI On-line Training 44
2.3. ForRisco - Risk Management 44
2.3.1. ForRisco Methodology 45
2.3.2. ForRisco Software 45
2.3.3. ForRisco On-line Training 45

3. Motivation for risk management 47

4. Main risk management methodologies and tools 51
4.1. Market methodologies 53
4.1.1. Enterprise Risk Management (ERM-COSO) 53
4.1.2. ISO 31000 59
4.1.3. Management of Risks (M_o_R-OGC) 63
4.1.4. Comparison between the main market methodologies 71
4.2. Methodologies of the Brazilian Public Administration 77
4.2.1. Methodology of integrity, risk and internal control management – GIRC 79
4.2.2. SISP- MGR-SISP risk management methodology 81
4.2.3. IBGC Risk Management Methodology 86
4.2.4. Comparison between the main methodologies of Brazilian Public Administration 93
4.3. Tools for monitoring risks 96
4.3.1. Risk map 96
4.3.2. Summarized reports 98
4.3.3. Communications and alert messages 100
4.3.4. Decision trees 100
4.3.5. Brainstorming 101
4.3.6. Scenario analysis 101

5. Laws and rules related to risk management in the public sector: the case of Brazil 103

6. Risk management software tools 109

7. Investigating real cases of risk management in the public sector: the cases of UNIFAL-MG and CEFET/RJ 127
7.1. Context and motivation 127
7.2. Search objects 127
7.2.1. The Federal University of Alfenas – UNIFAL-MG/BRAZIL 127
7.2.2. Celso Suckow da Fonseca Federal Center for Technological Education – CEFET/RJ/BRAZIL 128
7.3. Research procedures 128
7.4. Case Study: The Federal University of Alfenas – UNIFAL-MG/BRAZIL 133
7.5. Case Study: the Celso Suckow da Fonseca Federal Center for Technological Education - CEFET/RJ/BRASIL 143

8. The forrisco methodology: risk management in the public sector 155
8.1. Stages in the implementation of risk management 156
8.2. Example of the ForRisco methodology application 166
8.2.1. Case 1 - Initiating the implementation of risk management with the ForRisco methodology 166
8.2.2. Case 2 - Applying the ForRisco methodology in an organization that has already started risk management 167

9. How to evolve risk management in a public institution? An analysis of the cases of UNIFAL-MG and CEFET/RJ in the light of the ForRisco methodology 169

10. The ForRisco software platform 179

11. Final considerations 185

References 188
Appendix I - Questionnaire 191
Appendix II - Risk Recording Form 198
Appendix III - Questionnaire On Risk Management In Public Sector Organizations 200
Glossary 203

Foreword

With the advent of "new public management", innovative tools need to be developed to support decision-making in public administration to meet today's complex challenges.

It is worth mentioning that the FOR Platform, the focus of this book, comes to collaborate precisely in this sense, to support the decisions of public managers under the risk management perspective, based on organizational priorities.

Therefore, the authors define the FOR Platform as a set of solutions designed to improve public management aimed at stimulating culture for innovation, strategic action, and control of organizational risks.

For this purpose, two tools were developed within the scope of the FOR Platform:

- ForPDI, focused on strategic management, aims to monitor in real time, collaboratively and efficiently, the results considered as priorities by the organization; and

- ForRisco, aimed at risk management, has the purpose of organizing and planning resources minimizing possible negative impacts originated from organizational risks.

The wealth of positive evidence (see the case studies presented in this book) leaves no doubt about the benefits to public administrators by adopting the methods and tools proposed by the FOR Platform to improve organizational results.

Therefore, the work in question is a provocative invitation to theoretical and innovative reflections among scholars on "new public management". Furthermore, it provides added value and technical and managerial knowledge to public administrators to address organizational risks with a strategic focus on the achievement of priority results.

Welles Matias de Abreu
Director DRE/Ministry of Environment

Foreword

Governance, integrity, compliance, risk management ... In recent years, we have been bombarded with these terms that until recently were not usual in Public Administration.

These topics, which were treated as good practices only, included in recommendations of supervisory bodies, started to be requested in infralegal norms and regulations, with emphasis on Joint Normative Instruction MP/CGU nº 01/2016 and, more recently, Decree No. 9.203/17, known as the "Governance Decree".

Faced with all these issues, and now focusing on risk management, the subject of this book, it is inevitable that managers have several doubts, starting with quite a usual one: Do we really need this?

Yes, we do! A lot!

However, to better understand risk management (and especially to be open-minded to practice it), some points need to be demystified. In this preface, I would like to speak only of three.

The first great myth says that risk management will increase work, that is, if I introduce this task into my organization, in my department, I will have to work harder. I have heard several times: "I already work 8, 9 and up to 10 hours a day. Now you want me to do risk management too?" Based on this behavior, it is clear that the manager did not understand what risk management is. One can see that the premise used by them is wrong. Risk management is not "one more activity". It is a culture change, a new way of looking at your own business/process.

A second myth is that risk management will increase the costs of the organization. In a scenario of considerable fiscal constraint, such as what we are experiencing, it is natural and commendable to worry about the cost. However, this cannot be an excuse for not implementing good risk management. The benefits of effective risk management are often far greater than any costs incurred in implementing it. Gains start from the risk

identification phase, which induces managers to rethink their processes, optimizing them to the monitoring phase, when activities can be prioritized or even missed. In this respect, risk management is an ally in the search for cost savings in an organization, through process optimization and prioritization of current demands.

Finally, the third myth is the one that says that risk management will make processes even more difficult, as it will bring more controls. Those who believe in this myth are those who think, "This is a controlling organ thing". Perhaps because it appears for some time now in the recommendations contained in the reports of these bodies, many auditors think that risk management will only bring more controls to the organization, making the process more difficult and bureaucratizing the work too much. Wrong! Good risk management will make managers better aware of their processes and, consequently, the level of risk involved in the activities carried out. This will even allow the withdrawal of controls considered unnecessary, when applicable.

Having clarified some myths, and assuming that the manager was convinced of the need to implement risk management in his organization, another question arises: Okay, but how?

ForRisco!

In a didactic way and with the baggage acquired from ForPDI - Strategic Plan Management/PDI, the book I have the honor of preface addresses everything the manager needs to know to begin improving maturity in risk management of his organization's.

In this work, you will have the opportunity to understand better the motivation for an organization to adopt risk management, to have contact with the conceptual structures on the subject, to know the main legal frameworks in force and, mainly, to "learn to do" based on cases and the ForRisco methodology.

Come and join the world of risk management. Your organization thanks!

Prof. MSc.Rodrigo Fontenelle
CGAP, CRMA, CCS

Foreword

The way of conducting public management has been improved over the years. Since the proposal for an administrative reform that preached an approximation of public and private management, and which culminated in the inclusion of the Principle of Efficiency in the caput of Article 37 of the Magna Carta, we have sought ways to adopt quality in the provision of public services. Precepts such as efficacy, effectiveness, and efficiency have echoed higher and higher in the day to day of the public manager.

There are several tools used by private management to achieve their goals and objectives. Over time, there have been several attempts to bring the concepts already settled in the private sphere into the public sphere, and many of them have been left aside by the actors and relegated to fads. Others ended up being implemented and corroborated an improvement in the fulfillment of administrative aspirations. However, there is still a long way to go in the search for quality public management, and that is within the guiding precepts of the public interest.

Thus, another wave comes up and takes over the technical debates of public administration thinkers. Concepts such as governance, control, risk, transparency, and accountability are dealt with in official documents and discussed in public agendas. Control bodies are the first to address these issues because they understand its complexity as well as its benefits for the performance of the public manager.

Since then, questionnaires, reports, judgments, normative instructions, and decrees have been used to bring such discussion into the administrative sphere. The concern with the result and with the purpose of the actions of the Public Administration, as well as the accountability for conducts that differ from the emphasis imposed by the public interest, are increasingly causing managers to seek instruments to assist them in the difficult process of making decisions.

In this context, risk management is designed to assist the manager in making decisions, as well as to provide means and elements that allow the implementation of tools that contribute to the achievement of institutional goals and objectives. However, this is a culture that must be assimilated and internalized by all management, so that risk management is not seen

as another fad that will soon be overcome. The difference between risk management and other tools presented in the past is that it has been improved in the private sector and inserted in the legal-administrative order through rules that somehow impose its adoption. Although there is this fog of imposition, what is really intended is to demonstrate the relevance of working under a dynamically controlled and structured atmosphere, with a focus on the implementation and optimization of controls that aim to provide reasonable security to the manager to act in a more efficient manner, moving away from behaviors that may negatively affect institutional objectives.

It was then that, after the enactment of Joint Normative Ruling No. 01/2016, the idea of modulating a system that could help the Public Administration organs to carry out their risk management was born. A search was started to establish a methodology based on the different models used for risk management. Thus, market frameworks such as COSO ICIF, COSO ERM and ISO 310000, the British framework Management of Risks M_o_R-OGC, known as "Orange Book", focused on Public Administration, as well as the methodologies of the Brazilian Public Administration GIRC and MGR-SISP of the Ministry of Planning, and the methodology of the IBGC 2017, this one for proposing the evaluation of the maturity of the organization with regard to risk management, were studied to enable the formatting of the ForRisco methodology.

In addition to the methodologies and frameworks mentioned, some tools for identification, evaluation, and prioritization of risks are addressed in this book and also served as a basis for tabulating the ForRisco system and methodology. Among the many tools suggested by international documents, we can find risk map, summarized reports, communications and alert messages, decision tree, brainstorming and scenario analysis through the SWOT matrix.

The establishment of a standard methodology that could be adopted by all would be possible if we were inserted in institutions with the same characteristics. However, what is observed is that the universe of peculiarities and features of each organ is immense. Each institution, within its autonomy, develops its administration in accordance with its local demands and following its characteristics. Thus, any attempt to tabulate a single methodology cannot succeed. The purpose of developing a methodology is to show how it could be adopted if properly adapted to the realities of each institution.

That being said, the presentation of the various integrated structures that are in the market, the tools that can be used by each institution to identify, evaluate and manage their risks, as well as the methodologies adopted by some public agencies and the ForRisco methodology itself, aims at demonstrating that it is possible to format a methodology of its own and the use of risk management to improving management actions in such a way that decisions are made based on a risk concept. This improvement in management acts corroborates the idea of increasingly professionalizing administrative bodies so that all decisions are better grounded on less and less subjective aspects. Of course, it is not intended to eliminate the subjectivity of decision-making, because the one who establishes appetite and tolerance for risk is the manager himself who takes responsibility for the acts. However, the more structured the institution is, and the more mature the risk management structure, the higher the security of management, because with the risks mapped it is possible to see more clearly the consequences of each management act.

In order to confirm the consistency of the techniques and methods developed during the ForRisco Project, the developer team confronted the methodology developed with the practical reality of the organizations. Therefore, case studies were carried out in two Federal Institutions of Higher Education (IFES), which are: the Federal University of Alfenas – Minas Gerais (Universidade Federal de Alfenas - Minas Gerais - UNIFAL-MG); and the Celso Suckow da Fonseca Federal Center for Technological Education - Rio de Janeiro (Centro Federal de Educação Tecnológica Celso Suckow da Fonseca - Rio de Janeiro - CEFET/RJ). From this analysis, it was possible to evaluate what had been established until then and to format some adjustments to help other managers in the adoption and adaptation to their realities of both the methodology and the system.

Thus, by understanding that risk management is a path without a return because its adoption will ultimately add value to management, is that free tools like ForRisco should be encouraged. They will help its users enter their data of risk identification, as well as to enable better management of these data. As risk management is dynamic, each evaluation cycle will provide the manager with a critical view of his processes and routines in order to establish corrections and improvements always under the optics of achieving his objectives in the most efficient way possible. This systemic view of the weaknesses and probable consequences of the acts corroborates

the establishment of control tools increasingly optimized and that end up providing reasonable security to the manager in the act of making decisions.

Thus, strengthening what has already been said, the purpose of adopting risk management is not merely to meet normative demands, but rather a cultural change in the management for the adoption of tools that can serve as a support in the fulfillment of its activities and in achieving its objectives.

Jeferson Alves dos Santos
Chief auditor of UNIFAL-MG and President of the FONAIMEC Association

Introduction

Risk management, the central theme of this book, allows the reader to awaken to a more comprehensive perception of organizational reality and invites him to reflect on the benefits of proper planning and mapping of the processes managed by the institution. Although the issue is relatively new in the Brazilian public sector, I see risk management as an excellent opportunity to transform the management model used by most public bodies.

In this sense, a group of federal public universities, through the National Forum of Pro-Rectors on Planning and Administration of Federal Institutions of Higher Education (FORPLAD) and the Research and Development Center for Excellence and Transformation of the Public Sector (NExT) of the University of Brasilia, decided to contribute so that federal, state and municipal public agencies could provide a public service with more efficiency, efficacy, and effectiveness. The ForRisco tool emerged from the desire to support public managers and transform how the projects and processes in the Public Administration are planned and managed.

Modern, innovative, open source, adaptable to the various organizational realities and fully compatible with the strategic planning system also built by this group (ForPDI), the ForRisco solution is more than a new system of the For Platform. It is part of a dream that it is possible, very shortly, to have public policies that can demonstrate to society how effective government actions can be. Plan, monitor and mitigate the risks of not accomplishing its intended objectives are the challenges that this book and the software of the FOR Platform intend to tackle.

I invite the reader to deepen concepts and foster new transformative ideas that will contribute to an increasingly fair, transparent, inclusive and innovative public management.

Thiago José Galvão das Neves
UFPE | National coordinator

Research and Development Center for Excellence and Transformation of the Public Sector – University of Brasília – **NExT/UnB**

Coordinated by Professor Paulo Henrique de Souza Bermejo, we are an interdisciplinary research and development group linked to the Administration Department of the Faculty of Economics, Administration, Accounting and Public Policy Management (FACE) of the University of Brasília (UnB). Our team has researchers, undergraduate and graduate students that are specialists in Public Administration, and is committed to the application of methodologies and scientific techniques that aim to promote excellence and transformation of the public sector.

It emerged with the visionary ideal of boosting the analysis and effective implementation of innovative and high-impact solutions in public services and of delving deeper into this process. As a purpose of this ideal, we want to respond to changes in the new paradigms highlighted by the Brazilian Public Administration, focused on the client citizen, demanding a greater offer and better services and policies, and also in delivering results to citizens. Know our mission, vision, and values:

Mission:

- Provide innovative solutions that promote excellence and transformation to produce results and generate value in companies and governments.

Vision:

- Be recognized as a national leader in developing solutions for innovation and efficiency in corporate and government management.

Values:

- Dynamism, commitment, and courage
- Respect and simplicity
- Recognition and gratitude.
- Efficiency and effectiveness

We are committed to developing strategies and planning, managing innovation, R & D for specific solutions and organizational restructuring, and to redesigning and automating processes in private and public sector companies. Also, as a research group, we seek to support ourselves in the investigation of techniques and methods for the elaboration of strategic plans, in agile methods for innovation management, in the automation of strategic innovation programs and the optimization of services based on artificial intelligence and knowledge management.

The Ministry of Education, the Ministry of Planning, the Superior Military Court, the Attorney General's Office, the National School of Public Administration, the Department of Public Safety of Minas Gerais, the NOVA University - Portugal and the University of Bentley - USA are some of our customers and partners. However, it is also important to highlight the partnership between NExT/UnB and FORPLAD, UNIFAL-MG, UFLA, and other public institutions for the construction of this book, which, through research and development, believed and believe in the positive transformation of Public Administration in Brazil.

Enjoy your reading!

1. Preface

Individuals have limited perception about reality and, to deal with this fact, they seek to come together in groups and organizations to shape observable behaviors in rational patterns or mental models, contributing to the achievement of organizational goals. An organization is, at the same time, a set of articulated purposes and established mechanisms directed towards the achievement of results. After that, the mechanisms by which their purposes are achieved are constantly modified and refined, reorganizing their structure and processes, roles, and relationships [1].

Over time, several areas of knowledge, especially those of the Social Sciences, have sought to substantiate what proves effective for achieving the goals in organizations. It was expected that the lessons learned in one sector could be transferred to another, forming a unique theory of organizations. However, in addition to this not easy adaptation, scholars suggest that differences between sectors - public or private, for example - require their management methods and practices [2–4]. This means that, while these organizations have fundamentally similar structures, there are clear distinctions between them.

In the paradigm of "new public management", the adoption of managerial practices from private administration is increasing. Both the public and private sectors benefit from management models that contribute to a set of new knowledge. Notably, it is valid that management practices, such as the management of projects, processes, services or risks, have a body of knowledge that can be applied in both sectors [3, 6]. By highlighting risk management, similar behavior is observed in these management practices, although they have peculiarities due to the nature of their activity. The practice of risk management has at its core the identification and treatment of uncertainties, so as not to affect the objectives of the organization [5].

In Public Administration, risk management techniques are incorporated to increase internal control and governance. The Joint Normative Instruction (INC) 01/2016, dated May 10, 2016, of the Ministry of Planning (MP) and the Office of the Comptroller General of the Union (CGU), provides for internal controls, risk management, and governance within the Federal Executive Branch [7]. The INC should be adopted so that these bodies implement systemic and practical measures of risk management, and is also aligned

with the best market practices related to risk management, namely: COSO II, GRCorp and ISO 31000 [5, 8]. The MP also developed its risk management guide, through the Integrity Management Manual, Risks and Internal Control of Management (GIRC) [22], and the Methodology of Risk Management of Information Security and Communications of the Administration System of Information Technology Resources of the Federal Executive Branch - MGR-SISP [9].

What we want to highlight is the importance of adopting risk management as a complementary management method for public organizations. Risk management can contribute to a better organizational performance by allowing systemic controls and monitoring of risks [10–12]. Nonetheless, societies and citizens urge for more effectiveness in the provision of services by the Public Administration. In addition, PA spending needs to be more satisfactorily applied and managed, and the demand for greater efficiency and management of public resources brings accountability to society in an active and participatory position.

Thus, with the argument that there is a relatively low level of maturity in the discussions about risk management in public sector organizations, especially in Brazilian public institutions and, conversely, high demand for public bodies to be more efficient, effective and transparent in their practices, this work aims to promote and motivate the best practices of risk management in the public sector. The book presents a methodology of risk management - the ForRisco methodology - and ensures to have grounded its research on the methodologies most appreciated in the market and on those also adopted by Public Administration organizations.

This book goes from this preface to Chapter 2, which proposes a brief presentation of the For Platform for public governance. Chapter 3 aims to contextualize the motivation for managing organizational risks. Chapter 4 then discusses the risk management methodologies adopted in both the private and public sectors and the tools for risk monitoring. Chapter 5 presents the laws and regulations related to risk management in the public sector, and for this purpose, the study focuses on the laws and regulations that affect the Brazilian public sector. Chapter 6 discusses the most common software tools for conducting risk management. In Chapter 7, two case studies on risk management are carried out at two Federal Institutions of Higher Education (IFES) - UNIFAL-MG and CEFET/RJ - and the procedures

that made the research possible are presented. Chapter 8 deals with the ForRisco methodology, presenting important concepts about the methodology developed as well as the stages for implementation of risk management. Chapter 9 discusses how to evolve risk management through the ForRisco methodology. For this purpose, in this chapter, a comparison is made between what is done at UNIFAL-MG and CEFET/RJ, and what is recommended by the ForRisco methodology. Chapter 10 gives a brief presentation of the ForRisco Platform, that is, the software developed to manage, control and monitor risks in a systemic way. Finally, Chapter 11 sets out the final considerations, which highlight the main achievements of the ForRisco Project published in this book, and infers suggestions for further research and projects.

2. The for platform for public governance

In the last decades, the globalization process is leading extraordinary world transformations for markets and societies. In this set of transformations, more and more ways of maintaining transparency, strategy, and innovation are needed. In order to do so, the strategic management of processes and businesses has become an important ally of managers to boost development and competitiveness in organizations.

Administration or strategic management is seen as the art of exploring favorable conditions and/or applying available means to achieve specific objectives [32]. In this understanding, strategically managing an organization refers to a rational-creative process that permeates the actions of the teams aiming at competitive advantages. The strategy, in this case, serves to determine short- and long-term goals, preparing organizations for decision-making and action.

In response to these significant changes, in the context of public and private organizations what we see is more attentive institutions, concerned with improving the allocation of resources and expenditures, and focused on providing reliable results. Moreover, when it comes especially to the public sector, governance has become the main dialectic capable of fostering mechanisms to direct and evaluate management when considering the set of public policies and the provision of services to society.

Following this line of reasoning, over the years, governance structures have been created in several countries to improve performance, reduce conflicts, align actions, and bring greater security to owners and States. [33] As described in the book on public governance of the Tribunal de Contas da União ("The Brazilian Federal Court of Auditors"), Brazil and countries such as the United States, England and all other countries that make up the G8 (United States, Japan, Germany, United Kingdom, France, Italy and Canada (former G7, plus Russia), are focused on governance issues.

In addition, several organizations have begun to address this issue and to foster a range of codes that unveil and recommend practices related to governance. The World Bank, the International Monetary Fund (IMF) and the Organization for Economic Co-operation and Development (OECD) are some of

these organizations. The Brazilian Securities and Exchange Commission (CVM), the Brazilian Institute of Corporate Governance (IBGC) and the Brazilian Federal Court of Auditors (TCU) have published their governance proposals [33].

Notably, we can infer the constant transformations in the paradigms of organizations, which are progressively more focused on the gains of all those who relate, directly or indirectly, to the circumstances brought about by their institutions, that is, all citizens in society. Whether they are private organizations, public organizations or governments themselves, their actions should be mindful of ensuring the purpose of direction to seize opportunities and avoid threats. From this point of view, the For Platform is presented as an innovative segment of planning, strategy and risk management.

2.1. For Platform

The successful experience of an open solution for the management of strategic plans, such as ForPDI, motivated the development of new methods and aggregated technologies, which culminated in the construction of the For Platform for public governance. This platform was designed and built by a team of professors, researchers and specialists in strategic management, innovation, and risk management to foster the improvement of methods, processes, and software for planning and management in organizations.

Therefore, the For Platform is presented as a set of solutions that has the mission of motivating the best practices of innovation and strategic planning for management in organizations, provoking thought and generating added value and knowledge. Among its main products are: the ForPDI solution, including its set of artifacts, composed of the ForPDI methodology, online and software training for the management of Strategic Plans (PE) and Institutional Development Plans (PDI); and the ForRisco solution, which is completed through the ForRisco methodology (PE/PDI integration), online training and software for risk management in organizations.

The following is a brief description of the solutions and products offered by the For Platform.

2.2 ForPDI - Strategic Plan Management/PDI

The strategic actions in Federal Institutions of Higher Education and other public institutions have gained support through Strategic Plans/Plans of Institutional Development, a kind of instrument that aims at the foundation of systemic diagnoses and provides a support structure for reflection, formulation, implementation and management of the objectives, core tasks to the organizational development.

ForPDI is an open system for management and monitoring of federal universities and other public institutions PE/PDI. It emerged from the need for a real-time PE/PDI monitoring tool in a collaborative, efficient, fast and secure way. With ForPDI, it is possible to register all the strategic planning of PDI, to enter the values of the goals reached, to monitor the performance of the goals, to elaborate the document of PDI and much more.

The ForPDI project was designed to provide managers with support for the development, implementation, and execution up to the PE/PDI evaluation. Thus, ForPDI aims to support the strategic planning of educational institutions and other institutions in an integrated and interactive way. The ForPDI methodology, the ForPDI software, and the online training were developed for this purpose.

2.2.1 ForPDI Methodology

After conducting a diagnosis with 63 Brazilian federal universities to gather information about the Institutional Development Plan (IDP) of these universities, it was identified the need to create a reference book on IDP management. For this purpose, the ForPDI methodology was developed to be used by all Federal Institutions of Higher Education (IFES) in the development of the IDPs. The methodology is based on several normative ordinances, resolutions, and decrees that deal with the IDP. Based on this methodology, a structure for the documentation of the IDP is proposed.

2.2.2 ForPDI Software

Given its own methodology to support the structuring of strategic plans and IDPs in public organizations, the need to create the ForPDI software was recognized. It is an IDP computerization tool to optimize the monitoring of the results of indicators and targets. Among the main features of this software, it stands out its flexibility and the capacity to support different structures of plans. It is also worth noting the alignment between the methodology and the ForPDI software.

2.2.3 ForPDI On-line Training

Online training is a complementary resource aimed at integrating the principles and objectives of the ForPDI methodology and software. The training, as well as all other featured products, are available free of charge in the For Platform portal. This training consists of four modules: (1) methodological presentation; (2) fundamentals on the strategy applied to the public sector; (3) Institutional Development Plan: the ForPDI method; and (4) the ForPDI software platform.

2.3 ForRisco - Risk Management

Risks and uncertainties are part of the development of projects at different levels and local or global scales. Therefore, risk management becomes, over time, an effective mechanism in the search for results and positive impacts. This is because managing risks has come to be recognized by institutions as a concrete way of more satisfactorily planning material, human and administrative resources.

Following this line of reasoning, the ForRisco solution is the sum of efforts to guarantee excellence and commitment in performing important tasks that aim to manage processes of identification, analysis, planning, monitoring and control of risks. With this solution, it is possible to organize and plan resources in order to reduce the impacts of the risk on the institution. For this purpose, a set of techniques is used to minimize the effects of accidental damage, directing the appropriate treatment to the risks that can cause damage to the project, the people, the environment and the image of the organization.

The ForRisco project is, therefore, a set of free and open solutions composed of the ForRisco methodology, the online training, and the software ForRisco. Thus, the project aims to provide theoretical and practical artifacts for monitoring and managing risks arising from the processes developed by the institutions.

2.3.1 ForRisco Methodology

In order to motivate risk management practices in the public sector, this reference document was prepared to present and support the implementation of the ForRisco methodology. The book presents a series of information on the motivation for risk management as well as other methodologies heavily used in the market and Public Administration. Also, it provides a set of tools to manage and control risks as well as examples of case studies on risk management, also pointing out its methodology, that is, the stages and processes of the ForRisco methodology.

2.3.2 ForRisco Software

The ForRisco software is an integrated risk management module that allows changes and adaptations of risks by members of institutions and teams, facilitating the prevention of disasters arising from such risks. The tool has features to capture the occurrence of risks, management of monitoring processes, analysis of the aspects aligned to the organizational reality, elaboration of several realistic scenarios and planning of future management strategies, assisting in decision making by managers.

2.3.3 ForRisco On-line Training

In order to establish support for the ForRisco methodology and software, online training brings a set of resources available to users. The tool is seen as a complementary step to the other ForRisco products, allowing the integration of objectives and techniques of risk management in institutions. The training consists of courses related to the ForRisco methodology for using the software.

3. Motivation for risk management

At the organizational level, uncertainties occur at all times. Uncertainty refers to situations where there is not enough information to understand the scenario or knowledge about the consequences of a particular event. Risk, in turn, is related to the effect of uncertainty on the achievement of organizational goals [5]. Thus, when talking about risk management, there is a quest for practices recommended by corporate governance and the Board of Directors to identify and list, in a preventive manner, the main risks to which the organization is exposed, indicating the probability, the impact and the path to treatment, based on systematic practices [13].

Failures in the banking system, natural disasters, mismanagement of resources, and lack of knowledge of the organization resulted in the development of risk management prepared by auditors, insurers, accountants and other practitioners of various private sector organizations. Over time, these management practices have converged to generic corporate risk management models - frameworks - that emphasize the hierarchical structure of management, quantify exposure to risk and provide control systems for risk management [14]. With the development of these frameworks, corporate risk management has attracted the attention of public and private sector managers as a means to identify and manage comprehensively and strategically the risks to which they would be exposed.

In the public sphere, risk management has already been adopted by various government agencies around the world. In the international scenario, the British Treasury Department developed a Risk Management Assessment Framework (a tool for departments) between 2004 and 2009 to assist in collecting and evaluating evidence on departmental performance, and also to assist in setting priorities for improvement actions [15]. Other less generic initiatives have been developed in the United States by the Government Accountability Office, which includes various frameworks related to security, military, and terrorism, fraud, and finance, among others [16]. In Canada, the Treasury Board of Canada Secretariat has developed mechanisms for financial risk, internal audit, procurement of services, Information Technology (IT) and others [17]. These examples illustrate the relevance and adoption of the theme in some countries.

In Brazil, the Joint Normative Instruction MP/CGU 01/2016, was developed by the Ministry of Planning (MP) and the Office of the Comptroller General of the Union (CGU), which provides for internal controls, risk management, and governance within the Federal Executive Branch [7]. Other initiatives on information security risk management were developed by the Presidency of the Republic, through the Department of Information and Communications Security(DSIC), in Complementary Norm 04/13 [18].

The Brazilian Institute of Corporate Governance (IBGC) has developed a methodology for implementing risk management in organizations [13]. This framework differs from what has been adopted by the normative ruling (IN) nº 01/2016 on the process of risk management but can be used in a complementary way to other methodologies. Also, the IBGC methodology contributes to different reflections on the subject of risk management, and it should be emphasized that analyzing different methodologies can enrich and add value in the conduction of risk management.

All these initiatives, both international and Brazilian, allow bodies to consider their processes and their search for efficiency, identifying gaps and creating plans and actions to fill deficiencies. By achieving these results, these organizations can deliver greater satisfaction and better services to society and citizens. This search for more meaningful answers to the development of risk management was the motivating condition to leverage research on organizational risks in public institutions in Brazil.

Notoriously, this book brings a significant contribution to Brazilian organizations, especially those of a public nature, by establishing a range of information on current legislation, most used software and practical cases of risk management processes in agencies linked to the Federal Government of Brazil. However, it is important to emphasize the relevance of the topic addressed which, in general, encompasses a set of key references, methodologies, and tools for any organizations that have an interest in ensuring success in effective risk management.

Namely, this work is revealed as a result of a project entitled "Risk management in federal universities: elaboration of the reference model and implementation of the system. "For the development of the research, the project had the resources of the Foundation for Support to Culture, Education, Research and Extension of Alfenas (FACEPE), an organ linked to the Federal

University of Alfenas. It also received support from 63 Federal Institutions of Higher Education (IFES) by the National Forum of Pro-Rectors of Planning and Administration (FORPLAD) and the National Association of Directors of Federal Institutions of Higher Education (ANDIFES) in Brazil.

The following are some risk management methodologies and tools that have been adopted in both private and public organizations.

4. Main risk management methodologies and tools

Risk management methodologies have several similarities among them, especially for identifying and treating uncertainties systematically so that there is proper communication throughout the risk assessment process. It is also worth noting that, in general, any risk management process will provide a secure basis for decision making, logical planning, clarification of objectives and, lastly, the minimal risk from an economic point of view.

Therefore, during the implementation of a risk management process, there is a set of linked issues where one question naturally leads to the next, forming a generic process of risk management [19]. These issues are presented in Figure 1.

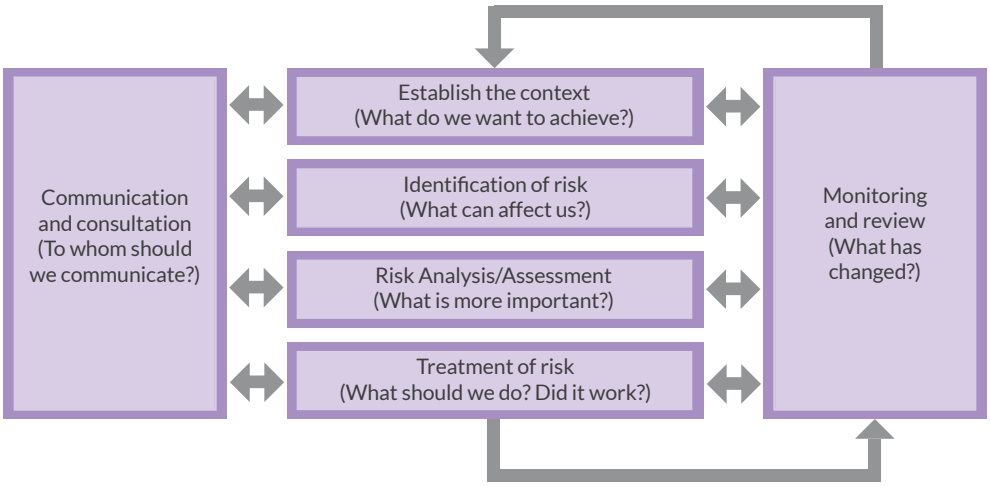


Figure 1 - Generic risk management process
Source: Hillson (2 017, p.9), with adaptations

According to Hillson [19], all these issues are present during the implementation of the stages contained in the main methodologies on risk management or evaluation, such as ISO 31000 and M_o_R-OGC. These are guiding questions that help the development team in the stages of risk

management and tend to ensure its development feasibility, without losing sight of the focus and other objectives proposed in the formulation of the process. Table 1 relate these issues to the stages in each methodology.

Table 1 - Questions to be answered by the stages of the methodologies

Questions	ISO 31000 (2018)	M_o_R-OGC (2010)
What do we want to achieve?	Establishment of context	Identify the context
What can affect us?	Identification of risk	Identify risks
What is more important?	Risk analysis Risk assessment	Estimate Evaluate
What should we do? Did it work?	Treatment of risk	Plan Implement
To whom should we communicate?	Communication and consultation	Communicate
What has changed?	Monitoring and critical analysis	Incorporate and revise
What have we learned?	Recording and reporting	-

Source: Hillson (2017, p8), with adaptations

Each guiding question can be treated in different ways, depending on the methodology or the purpose for which it is intended, but its merit stands out here. As for the question "What do we learn?", Hillson [19] suggests that this stage is little explored in the methodologies and that the lessons learned are rarely conducted at the end of projects or key decisions of the organization, so they have been left blank. It turns out, however, that the non-implementation of the lessons learned usually is caused by long-term benefits due to the complexity of the goals or lack of clarity, lack of employee altruism in helping colleagues with experiences or because employees need to start a new challenge before they have time to capture the lessons from the previous challenge. Failure to capture and disseminate these lessons causes the organization to make the same mistake repeatedly, spending scarce resources and not delivering the results it needs.

Below, we discuss the most recurring risk management methodologies in the market as well as a comparison between these methodologies. Next, it is worth mentioning that some methodologies developed and adopted by the Brazilian Public Administration will also be detailed.

4.1 Market methodologies

The following are the main market methodologies used for enterprise risk management: ERM-COSO - widely adopted by the Brazilian Public Administration - and ISO 31000 and M_o_R-OGC - recurrent methodologies in public and private organizations in several countries.

4.1.1. Enterprise Risk Management (ERM-COSO)

ERM-COSO is perhaps the most widely accepted framework on the market for organizing risk management efforts. Developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), its first version, published in 1992 - Internal Control - Integrated Framework, proposed a structure focused on the implementation and conduction of internal control in organizations, and in the evaluation of its effectiveness. Among other versions, in 2004, the Enterprise Risk Management - Integrated Framework (ERM-COSO) project drives the argument that risk management exists in organizations or entities to provide value to stakeholders such as shareholders, customers, employees, among others [8].

In its most recent narrative, ERM-COSO 2017, which is an updated version of Enterprise Risk Management - Integrated Framework, 2004, addresses the evolution of enterprise risk management and the need for organizations to improve their risk management approach to meet the demands of an evolving business environment [34]. According to COSO [34], the complexity of risks has changed, and new risks have emerged, but managers and executives have also improved their awareness and oversight of enterprise risk management while new, improved resources are needed.

In fact, all organizations face uncertainties, and the challenge of management is to determine how much uncertainty to accept, as they can

affect the desired organizational values [8]. Therefore, all organizations need to define their strategies and adjust them periodically, keeping in mind the changing opportunities for value creation and the challenges that will occur in search of these values. In order to do so, they need the best structure possible to optimize strategy and performance. At that point, enterprise risk management comes into play. Risk management is aimed at maximizing value resulting from a clear and precise definition of objectives and strategies to find the ideal balance [34].

According to ERM-COSO [34, pp. 15-16], there are many benefits to organizations that integrate their enterprise risk management strategies, such as:

a. increase the range of opportunities: risk management processes can improve the entity's ability to identify new opportunities and unique challenges associated with these opportunities;

b. identify and manage the entire risk entity: a risk can originate in one part of the entity but affect a different part. Consequently, management identifies and manages these risks across the entity to sustain and improve performance;

c. increase positive results and benefits, and reduce negative surprises: managing risks enables entities to improve their ability to identify new risks and establish appropriate responses, reducing surprises and related costs or losses;

d. reduce the variability of performance: enterprise risk management enables organizations to anticipate the risks that would affect their performance and enables them to take the necessary actions to minimize disruption and maximize opportunities;

e. improve resource allocation: obtaining robust information about the risks allows the management, faced with finite resources, to evaluate and prioritize the implementation of these resources; and

f. strengthen business resilience: the medium and long-term viability of an entity depends on its ability to anticipate and respond to changes not only to survive but also to evolve and thrive. In part, effective enterprise risk management enables this.

These benefits show the need for a holistic view of organizations in an interactive process among their members. In fact, risk should not only be viewed as a potential uncertainty or challenge to establish and execute strategies. Far from this, risk must be understood as a strategic and planned opportunity that can improve the responses, resources, and deliveries in the entity that proceeds it [34].

Through this holistic view, ERM-COSO establishes the importance of integrating enterprise risk management, mainly because of risk influences and aligns the strategy and performance of entities across all departments and functions. To explain this, the document proposes the framework of enterprise risk management, represented in Figure 2:

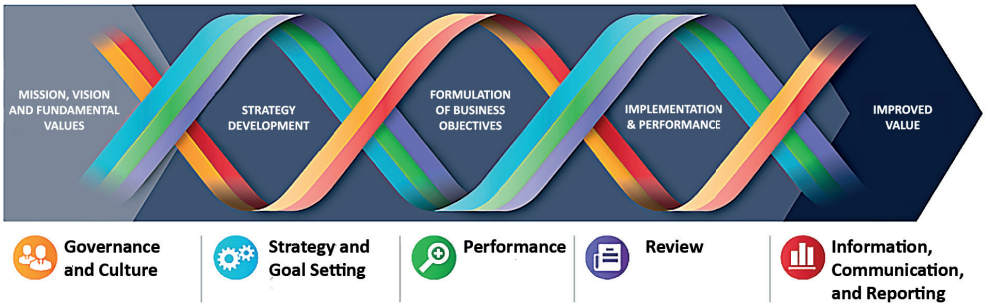


Figure 2 - Risk management methodology proposed by ERM-COSO
Source: ERM-COSO (2017, p. 18).

The framework governs a set of principles organized into five main, interrelated components [34, p. 18]:

1) Governance and culture: governance sets the tone of the organization, reinforcing the importance of mission and vision, and establishing supervisory responsibilities for enterprise risk management. Culture refers to fundamental ethical values, desired behaviors, and understanding of risk in the entity;

2) Strategy and goal setting: in enterprise risk management, strategy and goal setting must be worked together in the strategic planning process. Risk appetite is established and aligned with strategy; and business objectives put the strategy into practice as a basis for identifying, assessing and responding to risks;

3) Performance: risks can affect the scope of the strategy, and business objectives need to be identified and evaluated. Risks are prioritized by gravity in the context of risk appetite. The organization then selects risk responses and obtains a portfolio view of the number of risks it has assumed. The results of this process are reported to the main stakeholders of the entity;

4) Review: when reviewing the entity's performance, an organization can consider how well the risk management components are working, over time, and what changes are needed; and

5) Information, communication, and reporting: Enterprise risk management requires a continuous process of obtaining and sharing the information needed from both internal and external sources, flowing up, down and across the organization.

In addition, the five components of the framework are supported by a set of principles, which seek to meet all the requirements of good risk management in an organization, from governance to monitoring. They are also manageable principles and describe practices that can be applied in different ways, regardless of entity size, type or industry. In Table 2, the principles for each of the components are explained and described, according to ERM-COSO [34, p. 19].

Table 2 - Risk management components and principles proposed by the ERM-COSO review

Components	Principles	Description
1. Governance and culture	a. Supervise risk through the Council.	The board provides supervision to the strategy and performs governance responsibilities to support management in achieving the strategy and business objectives.
	b. Establish operational structures.	The organization establishes operational structures in pursuit of strategic and business objectives.
	c. Define the desired culture.	The organization defines the desired behaviors that characterize the culture desired by the entity.
	d. Demonstrate commitment to fundamental values.	The organization demonstrates a commitment to the entity's core values.
	e. Attract, develop and retain capable people.	The organization is committed to building human capital aligned with business strategy and objectives.
2. Strategy and goal setting	f. Analyze the business context.	The organization considers the potential effects of the business context on the risk profile.
	g. Define risk appetite.	The organization defines risk appetite in the context of creating, preserving and gaining value.
	h. Evaluate alternative strategies.	The organization evaluates alternative strategies and the potential impact on the risk profile.
	i. Formulate business objectives.	The organization considers risk when setting business goals at various levels. These objectives will support the strategy.

3. Performance	j. Identify the risks.	The organization identifies the risk that affects the performance of the strategy and business objectives.
	k. Assess the severity of the risks.	The organization assesses the severity of the risk.
	l. Prioritize risks.	The organization prioritizes risks to select responses to these risks.
	m. Implement risk responses.	The organization identifies and selects responses to risks.
	n. Adopt a portfolio view.	The organization develops and evaluates a risk portfolio view.
4. Review	o. Evaluate important changes.	The organization identifies and evaluates changes that can substantially affect business strategy and objectives.
	p. Analyze risks and organizational performance.	The organization reviews the performance of the entity and considers the risk.
	q. Seek improvement in enterprise risk management.	The organization seeks to improve corporate risk management.
5. Information, communication and reporting	r. Leverage information systems and technology.	The organization uses the entity's information and technology systems to support enterprise risk management.
	s. Communicate risk information.	The organization uses communication channels to support enterprise risk management.
	t. Disclose risk, culture and performance information through reports.	The organization reports on risk, culture, and performance at various levels and throughout the entity.

Source: ERM-COSO (2017, pp. 18-23), with adaptations

It is worth mentioning, based on the components and the principles proposed by the ERM-COSO review [34] for risk management, that adherence to these principles aims to provide the administration, the Council and the managers with a reasonable expectation that the organization that understands and strives to manage risks more effectively meets its business strategy and objectives. The result of this, regardless of the type of entity, should reflect in the integration of enterprise risk management practices with other aspects of the business, increasing the trust of the stakeholders and generating value for the organization.

4.1.2. ISO 31000

ABNT NBR ISO 31000: Risk Management - Guidelines - defines principles and guidelines in risk management, and can be adopted by different organizations in the activities of strategic decision, operation, process, function, project, service, and risk assessment. The methodology can be applied to different types of risks, regardless of their nature, such as qualitative or quantitative objectives and, also, on positive or negative impacts, establishing and achieving objectives and improving performance [5].

The standard suggests that treatments be done according to the specifics of the organization, which, initially, uses the methodology to harmonize the risk management process in existing standards, thus providing a certain support to the actions [5]. Also, ISO 31000 aims to support the standardization of risk management in the organization without leaving aside the understanding of the need to treat specific cases and situations, that is, inherent to each institution.

According to the standard, the risk is the "effect of uncertainty on objectives" [5, p. 1]. Therefore, managing risks corresponds to helping organizations in establishing strategies for decision-making. Risk management integrates governance actions and contributes to improved management [5]. In addition, all organizations manage risks to some degree, and the standard sets forth principles that need to be addressed to make risk management effective, systematic, transparent and reliable.

The standard is divided into three components: a) principles; b) structure and c) processes. In other words, starting from the ISO 31000 risk management proposal and a set of rules and guidelines contained in the principles, a structure

is created to support the implementation of risk management processes in organizations aiming at continuous improvement. From this set of components, the standard process aims to establish the context, identify, analyze, evaluate and treat the risk, and, in the course of the process, to communicate and monitor it [5]. Figure 3 represents the general model of the methodology.

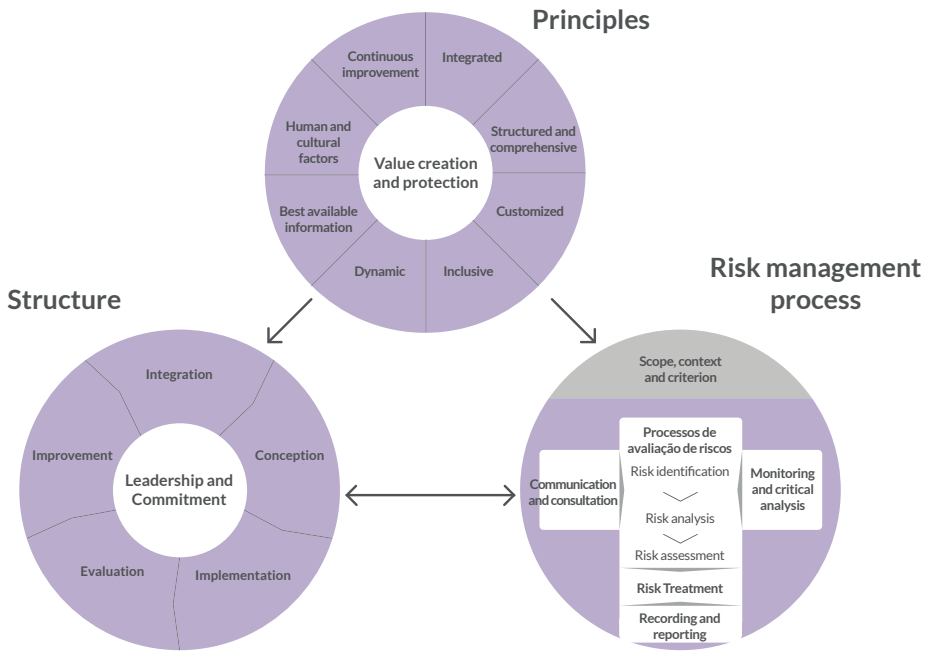


Figure 3 - Risk management methodology proposed by ISO 31000
Source: ABNT NBR ISO 31000 (2018, p. vi)

a) In **Principles**, the purpose corresponds to the creation and preservation of values. Through this value structure, organizations must develop their basis for risk management. To this end, ISO 31000 highlights the following principles: value creation; integration; structure and scope; customization; inclusion; dynamic; best information available; human and cultural factors; and continuous improvement.

b) In **Structure**, ISO 31000 allows the organization to reflect on the integration of risk management into meaningful activities and functions. For this purpose, the institution should evaluate existing practices and

processes, and then identify possible gaps. It is important to consider all stakeholders and top management. The elements of the structure are leadership and commitment; integration; conception; implementation; evaluation; and improvement.

c) In the **Process**, risk management comprises the construction and implementation of policies and practices to control and monitor activities. In summary, the risk management process starts with defining the scope of the organization's activities, the external and internal contexts, and the definition of criteria for risk assessment. It is necessary to identify, analyze and evaluate the risks and then treat them. This process must continuously be communicated and monitored. The risks, their treatments, and all monitoring must be reported and recorded.

When ISO 31000 is implemented and maintained, the risk management proposal contained in this standard enables several objectives to be met to meet the needs of stakeholders. Through this set of structured and proposed controls, and with a clear understanding of the context and the risks, the best tools for the treatment of risks are defined according to their nature. Therefore, it is believed in the quality of the treatment of risks and the greater aggregation of value to the business through the management.

In addition to ABNT NBR ISO 31000 - Guidelines, ABNT NBR ISO 31010: Risk Management - Techniques for the risk assessment process guides the selection and application of systematic techniques for the risk assessment process, contributing with risk management activities. According to the risk assessment process, by using the tools and techniques proposed in the standard, it is possible to understand better the risks, gathering relevant information that helps in decision-making and the establishment of prioritization for the treatment of risks [20]. Table 3 presents these tools.

Table 3 - Tools used for the risk assessment process

Tools and techniques	Risk assessment process				
	Identification of risks	Risk analysis			Risk assessment
		Consequence	Probability	Risk level	
Brainstorming	SA[1]	NA[2]	NA	NA	NA
Structured or semi-structured interviews	SA	NA	NA	NA	NA
Delphi	SA	NA	NA	NA	NA
Checklists	SA	NA	NA	NA	NA
Preliminary hazard analysis (PHA)	SA	NA	NA	NA	NA
Hazard and Operability Study (HAZOP)	SA	SA	A	A	A
Hazard analysis and critical control points (HACCP)	SA	SA	NA	NA	SA
Environmental risk assessment	SA	SA	SA	SA	SA
Structured technique "And if" (SWIFT)	SA	SA	SA	SA	SA
Scenario analysis	SA	SA	A	A	A
Analysis of impacts on the business	A	SA	A	A	A
Root cause analysis	NA	SA	SA	SA	SA
Failure mode and effect analysis	SA	SA	SA	SA	SA
Fault tree analysis	A	NA	SA	A	A
Event tree analysis	A	SA	A	A	NA
Analysis of cause and consequence	A	SA	SA	A	A
Cause and effect analysis	SA	SA	NA	NA	NA
Layers of protection analysis (LOPA)	A	SA	A	A	NA
Decision tree	NA	SA	SA	A	A
Human reliability analysis	SA	SA	SA	SA	A
Bow-Tie Analysis	NA	A	SA	SA	A
Reliability-centered maintenance	SA	SA	SA	SA	SA
Hidden Circuit Analysis	A	NA	NA	NA	NA
Markov Analysis	A	SA	NA	NA	NA
Monte Carlo Simulation	NA	NA	NA	NA	SA
Bayesian Statistics and Bayes Networks	NA	SA	NA	NA	SA

Tools and techniques	Risk assessment process				
	Identification of risks	Risk analysis			Risk assessment
		Consequence	Probability	Risk level	
FN curves	A	SA	SA	A	SA
Risk indices	A	SA	SA	A	SA
Probability/consequence matrix	SA	SA	SA	SA	A
Cost-benefit analysis	A	SA	A	A	A
Multi-criteria Decision Analysis (MCDA)	A	SA	A	SA	A
[1] SA - Strongly applicable, [2] NA - Not applicable, [3] A – Applicable					

Source: ABNT NBR ISO 31010 (2012, p. 21-22), with adaptations

The ABNT NBR ISO 31000 standard presents a set of stages containing the principles, strategy, and processes of risk assessment, and in that process, it lists the tools and techniques to allow a systematic risk assessment to be sought. It is worth reflecting that, just like the ERM-COSO, the concerns fall on the human factor, such as the lack of understanding and other problems arising from the lack of communication and limited rationality. However, through the governance structure proposed by the standard, it is possible to guarantee better organizational performance and the reduction of uncertainties.

4.1.3.Management of Risk (M_o_R-OGC)

The M_o_R (Management of Risk) framework developed by the Office of Government Commerce (OGC) is a guide to assist organizations in making decisions about risks that may affect the achievement of their strategic objectives of programs, projects, or operations.

The methodology encompasses principles, approach, and processes in a set of interrelated stages in these dimensions for risk management in organizations. It is also supported by tools and techniques for identifying, assessing and treating those risks. There are some ISO 31000 references included in the M_o_R-OGC, which makes it complementary in relation to risk management [21].

In M_o_R-OGC, there is a more prescriptive way of conducting risk management in the organization. In this way, eight principles are presented so that risk management can happen practically according to the guidelines of this methodology - the first seven are enabling principles, and the last one is a result principle [21]:

1. Alignment to objectives: risk management must be continually aligned with organizational objectives.
2. Suitability to the context: risk management must be perfectly adequate to the current context.
3. Stakeholders' engagement: risk management should engage stakeholders and deal with different perceptions of risk.
4. Providing a clear process guide: risk management should provide a clear and coherent process guide for stakeholders.
5. Support for decision-making: risk management must properly inform and be linked to decision making throughout the organization.
6. Support for continuous improvement: risk management should use historical data to facilitate learning and continuous improvement.
7. Creating a supportive culture: risk management must create a culture that recognizes uncertainty and considers the organization to be at risk.
8. Scope of measurable values: risk management allows the achievement of measurable values in the organization.

To ensure that risk management is conducted properly and successfully throughout the organization, there are methods and models for achieving results, such as the HealthCheck or the maturity scale based on best market practices.

In order to be able to reach the mentioned principles, M_o_R-OGC suggests an approach through a set of guiding documents (records, plans, and reports, among others) in the definitions of how actions will be conducted, how they will be communicated, managed and improved over time [21]. Table 4 presents some of these documents.

Table 4 - Approach to risk management - Documents

Document	Description
Policy	The purpose of the policy is to communicate "why" and "how" risk management will be implemented throughout the organization (or part of it) to support the achievement of the objectives.
Process Guide	The process guide describes how risk management stages will be conducted, from the identification of these risks to their treatment or implementation. It reflects the core of M_o_R-OGC's risk management methodology.
Strategy	The strategy describes specific activities for the management of risks that must be carried out by an organization, or part of it, in a particular way considering its characteristics.
Recording of Risks	The risk recording should capture and maintain threat and opportunity information related to a specific organizational activity. It is the main component to be evaluated in conjunction with the other risks and allows the allocation of responsibilities and the distribution of tasks.
Recording of Issues	Issues are materialized risks. These records should capture and maintain information in a consistent and structured manner on the issues that are currently occurring and requiring attention.
Improvement Plan for Risk Management	The purpose of the improvement plan is to support the incorporation of risk management into the organizational culture. This document should reflect the improvements planned for the environment and reflect the current health status (HealthCheck - Assessment Questionnaire, Annex C of the standard) compared to the current maturity state to set a course to increased maturity and continuous improvement (Annex D of the standard).
Risk Communication Plan	The risk communication plan describes how the information will be disseminated and assimilated by key people in the organization. Accurate communication is a critical success factor to ensure that the context is understood, risks identified and evaluated, and appropriate responses planned and executed.
Risk Response Plan	The risk response plan is linked to risk recording and should contain specific details for a single risk. In this document, it is stipulated who is the owner of the risk, the executor or agent, how the risk must be monitored and communicated, among other characteristics for its treatment. Thus, if the event of a risk materializes or exceeds its tolerance limit, it is not necessary to develop a plan at runtime, which will save time and effort.
Risk Treatment Progress Plan	The progress plan of risk treatment must provide a report with regular information on the progress of the implementation or the treatment of risks to the managers involved or the stakeholders. This report allows adding value to decision makers so they have the most accurate information and can analyze trends.

Source: M_o_R-OGC (2010, pp. 21-25), with adaptations

Figure 4 shows the relationship of these documents. It is worth pointing out that there are some comprehensive documents, that is, that are valid for the entire organization, and specific documents for activities unique to organizations.

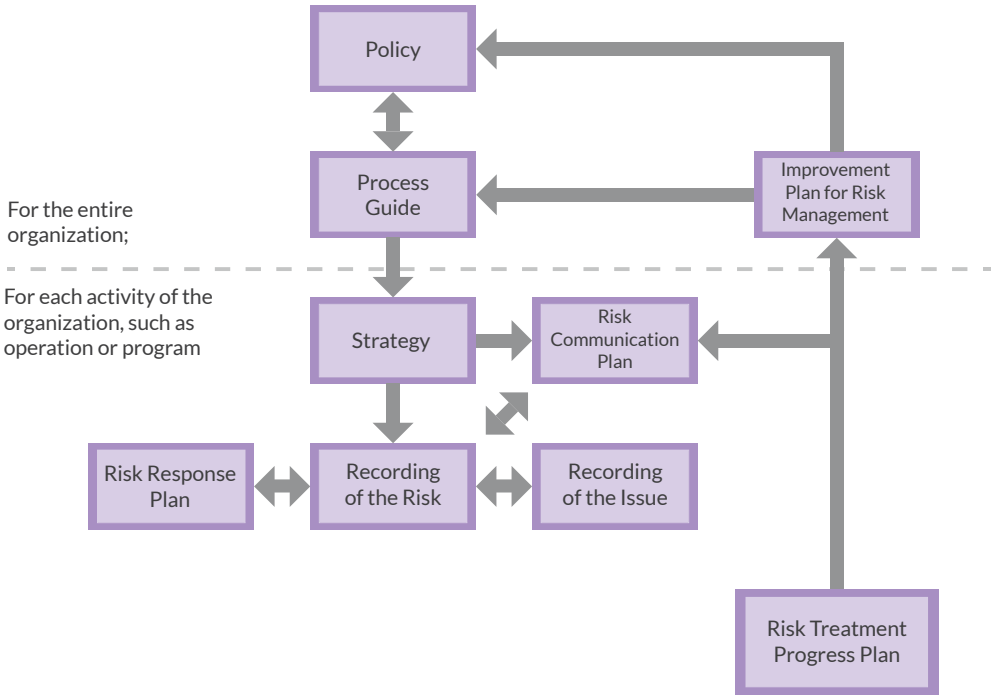


Figure 4 - Relationship between M_o_R-OGC documents
Source: M_o_R-OGC (2010, p. 24), with adaptations

Once the policy is structured, and the approach to risk management at the organizational level is defined, risk processes are started in a more individualized way. The M_o_R-OGC risk management process contains several stages, as shown in Figure 5. The "Communicate" stage is central and must occur several times in order to have a correct alignment between those involved. The stages "Identify", "Estimate/Evaluate", "Plan" and "Implement" represent a logical sequence, and the output of a stage serves as input for the next stage.

Figure 5 - Risk management methodology proposed by M_o_R-OGC
Source: M_o_R-OGC (2010, p. 3), with adaptations

As in ABNT NBR ISO 31010, M_o_R-OGC has a set of tools and techniques to support the implementation of the risk management process. The techniques for risk management are classified according to the framework stages - Table 5. This framework is intended to assist managers in the definition of management techniques and resembles the tools and techniques present in ABNT NBR ISO 31010.

Table 5 - Techniques in Appendix B of the M_o_R

Process stage	The technique primarily associated with the process stage	Another stage in the process in which the technique may be useful
Identify the context	Stakeholder analysis PESTEL analysis SWOT analysis Horizontal scanning Probability and consequence matrix	Identify the risk
Identify the risk	Checklists Response list Cause and Effect Diagram Group Techniques Delphi Questionnaires Interviews Assumptions Analysis Constraint analysis Risk Descriptions	Plan
Estimate	Probability assessment Impact assessment Proximity assessment Expected value as decision criterion	
Evaluate	Risk map Expected value as decision criterion Probabilistic risk models Probability tree Sensitivity analysis	Plan
Plan	Risk response Cost-benefit analysis Decision tree	Evaluate
Implement	Updating the Risk Map Report Risk exposure trends Updating probabilistic risk models	

Source: M_o_R-OGC (2010, p. 86), with adaptations

To support these activities, M_o_R-OGC suggests a set of roles and responsibilities that involve:

- the senior team or Senior Management Committee, with attributions focused on strategic activities, dissemination, and incorporation of risk management;

- the representative of the senior team, with responsibilities to ensure governance and internal controls, and other information that must be reported, among other activities;

- program, operation or project managers who are responsible for ensuring that the record, review, evaluation, tasks and other controls are performed properly;

- the quality team, to ensure that there are accounting controls by internal guidelines, review of the progress of plans and other audit activities;

- risk specialists to ensure that the Risk Management Policy is properly implemented, in addition to facilitating the dissemination of the methodology by the agency; and

- the other teams, which participate in identifying the treatment of risks, implement the rules of the policies and scale the risks when necessary.

The methodology also provides a maturity scale to support managers and senior management in defining the objectives for the evolution of risk management and its maturity in the organization. Table 6 represents this scale with maturity levels.

Table 6 - M_o_R maturity scale

	Level 1 Initial	Level 2 Repetitive	Level 3 Defined	Level 4 Managed	Level 5 Optimized
Aligned to objectives	The objectives are not defined.	Risks associated with defined objectives.	Objectives defined and updated during risk management.	Objectives changed according to risk response.	Objectives defined according to risk management.
Suitable to the context	Context not reflected in the identification.	The context is examined throughout the risk process.	The context is strict.	Managers inform the context in advance.	The context is used to define management actions.
Involves stakeholders	Not all stakeholders are consulted.	Stakeholders are identified and minimally engaged.	The objectives of stakeholders are identified, recorded, aligned, and assigned.	Stakeholders are actively involved.	Stakeholders are encouraged and involved in the investment cycle.
Defined Process	Undocumented and vague policy and processes.	Policy and processes are defined.	Uniform processes are adopted throughout the organization.	Risk management is fully integrated with the activities of managers.	Best practices are identified and shared across the organization.
Decision Making	There is no definition of operational limits, reviews or reports.	Management reports are issued consistently and within defined time frames.	Senior managers report in a consistent format.	There is quality quantitative analysis.	Scenario planning techniques are naturally used.
Continuous improvement	Lack of training and knowledge about risk management.	People are trained throughout the implementation of risk management.	Different levels of training are defined.	Experienced staff analyzing quantitative results.	Constantly updated knowledge and skills.
Collaborative culture	The team acts on its own in independent groups.	Risk owners, managers, and agents are identified.	Teams integrated into the organization with roles and responsibilities.	Risk management attitudes are recognized and honored.	Risks are appended in the organization, present in the job descriptions.
Measurable values	No measurements.	Measurements of processes, but not performance	Performance measures implemented.	Performance measures demonstrate the scope of value.	Scope of measurable value for internal and external stakeholders.

Source: M_o_R-OGC (2010), with adaptations

Compared to ERM-COSO and ISO 31000, M_o_R-OGC presents the largest framework of guidelines for the implementation and operationalization of risk management in organizations. It is inferred that, although it is more prescriptive than the other standards, this standard remains generic enough to be adopted by both public and private sector organizations of greater or smaller size.

4.1.4. Comparison between the main market methodologies

Market methodologies have a common set of guidelines for professionals in the area of risk management. As they were developed at different times, there is an evolution in the focus of management techniques, as well as a comprehensive set of tools and techniques to support managers in conducting organizational risks. Therefore, Table 7 contains information that summarizes the main ideas of the risk management process according to market methodologies. To facilitate the understanding, Figure 6 was elaborated, which exemplifies a comparison between the risk management methodologies with the following specifications: A as a representation of principles; B as the structure of the methodology; and the numbering (from 1 to 10) with the stages of support and implementation of the methodologies.

The stages and processes in Figure 6 are recorded and interpreted in Table 7 to facilitate the understanding of risk management and the individual characteristics of market methodologies. Risk interpretations, corporate risk management, risk assessment process, principles, structure, context/internal environment, the definition of objectives, identification, analysis/evaluation, treatment/response, communication, monitoring, and approach are presented for each of the methodologies mentioned.

Figure 6 - Comparison between risk management methodologies
(continues)

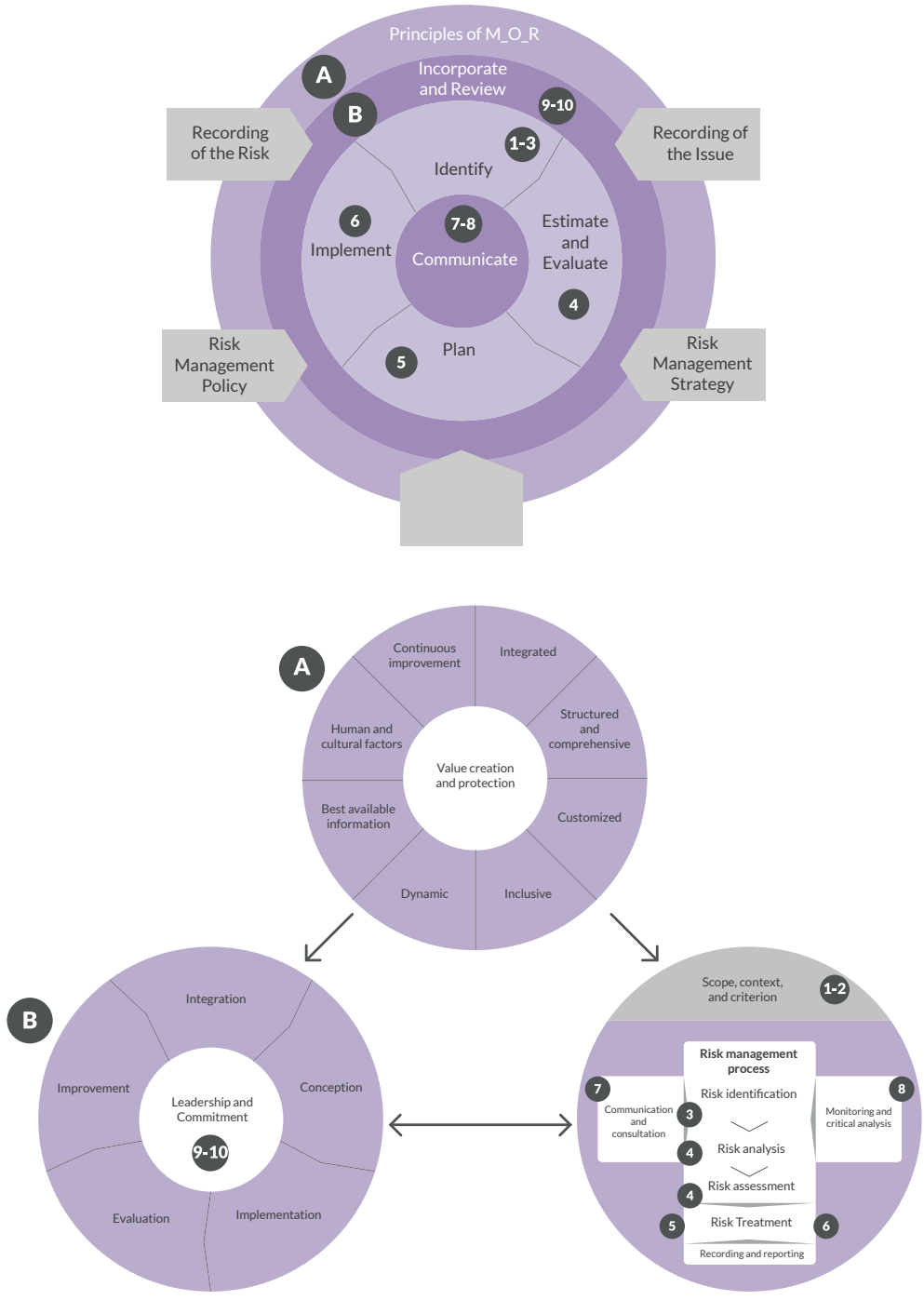


Figure 6 - Comparison between risk management methodologies
Source: ERM-COSO (2017), ISO 31000 (2018), M_o_R-OGC (2010), with adaptations

Table 7 - Comparison between the definitions of the main market methodologies

ERM-COSO (2017)	ISO 31000 (2018)	M_o_R-OGC (2010)	
Risk is the possibility of an event to occur and affect the achievement of objectives (p.16).	The effect of uncertainty on objectives (p.1).	An event or set of uncertain events that, if they occur, will affect the achievement of objectives (p.135).	Risk
It is a process conducted by a committee of directors, managers, and others, applied in the strategic definition and throughout the organization. It is designed to identify potential events that may affect the organization and management of risks (pp.34-35).	Coordinated activities to direct and control an organization about risks (p.2).	Systematic application of principles, approaches, and processes for risk identification and assessment tasks, followed by planning and implementation of risk responses (p.136).	Enterprise risk management
The identified risks are analyzed to form a basis for determining how they should be managed. They are then associated with goals that can be affected. Finally, they are evaluated taking into account both inherited and residual risks, with the evaluation considering probability and impact (p.59).	The risk assessment process is the overall process of risk identification, risk analysis, and risk assessment. It should be conducted in a systematic, iterative and collaborative way (p.12).	Describes how the process stages will be executed, from the identification to the implementation. It involves identifying, analyzing and estimating, planning and implementing the risk management plans developed (p.22).	Risk assessment process

There is a specific definition of principles in the guide, correlated with the five components for enterprise risk management (page 23).	The standard introduces nine principles for effective risk management at all levels of the organization (p.3).	The purpose of the principle is to communicate why and how risk management will be implemented at the organizational level to support the achievement of its objectives. Eight principles are presented for management (p.21).	A - Principles
ERM-COSO proposes a specific structure to connect principles with the entities' processes, as shown in Table 2 of this book.	The success of risk management depends on the effectiveness of the management structure, which provides the fundamentals and components to incorporate it throughout the organization. Its purpose is to support the organization to integrate risk management into meaningful activities and functions (p.4).	The purpose of incorporation and revision is to integrate the principles into the risk management processes, making a change in the organizational culture. It must ensure that risk management is being conducted properly and successfully across the organization, and relies on the use of methods and models to achieve this result (page 51).	B – Structure
Defines the basis on how risks and controls are addressed by people in the organization. The core of any business is its people - its values, including integrity, ethical values and competence - and the environment in which they operate (p.87).	Defining the external and internal parameters to be taken into account in risk management, and establishing the scope and risk criteria for the Risk Management Policy (p.11).	The purpose of context identification is to obtain information about planned activities to see how they fit across the organization in order to serve the market or society (p.32).	1 - Context/Internal Environment
There must be prior objectives for management to identify potential events that affect their reach (p.101).	The Risk Management Policy should clearly state the objectives, criteria for assessing the significance of the risk and the commitment of the organization to risk management (p.11).	Risk management continually aligns with organizational objectives. It is focused on uncertainties, which have the potential to affect the achievement of one or more of the organization's objectives (page 13).	2 - Goal setting

ERM-COSO (2017)	ISO 31000 (2018)	M_o_R-OGC (2010)	
It involves identifying potential events from internal or external sources that affect the achievement of objectives. This includes distinguishing between events that represent risks, those that represent opportunities, and those that can be both (p.109).	Process of finding, recognizing, and describing risks. The organization should identify sources of risk, areas of impact, events (including changes in circumstances) and their causes and potential consequences. The purpose of this stage is to generate a comprehensive list of risks based on these events that can create, increase, prevent, reduce, accelerate or delay achievement of objectives (p.12).	IIdentify risks in activities to reach objectives in order to minimize threats while maximizing opportunities, which includes: • identify opportunities and threats in the activity; • prepare the recording of the risk; • prepare key indicators and other indicators; • understand key people's view of risk (p.36).	3 - Identification
In ERM, analysis and evaluation occur at the same stage, that is, in the review stage. Under the framework, risk assessment allows the organization to consider the scope and proportion in which potential events can affect the achievement of objectives. The management of this evaluation considers the prospects, the impact and the probability related to qualitative and quantitative methods. It also considers the inherited and residual risks (pp. 138-141).	Process of understanding the nature of the risk and determining its level. Risk analysis involves assessing the causes and sources of risk, their positive and negative consequences, and the likelihood that these consequences will occur (p.13).	The purpose of the analysis is to prioritize individual risks to clarify which of them are most important and most urgent. For this, it is necessary to understand their probability, impact, and proximity (p. 38).	4 – Analyze
	The process of comparing the results of the risk analysis with the risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable. The purpose of risk assessment is to assist in making decisions based on the results of risk analysis on which risks need treatment and to prioritize the implementation of such treatment (pp.13-14).	Risk assessment is useful to understand the risk exposure of the activity in the chain of effects of the threats and opportunities of these activities together (p.41).	4 - Evaluation

Staff identifies and evaluate possible risk responses, which include accepting, reducing, sharing or avoiding risk. Management selects a set of actions to align risks with the organization's tolerance and risk appetite (pp.127-129).	The purpose of risk treatment involves selecting one or more options for modifying risk and implementing these options (page 14).	The purpose of the plan is to prepare a specific response to reduce threats and maximize opportunities so that the business and its staff are not surprised if a risk materializes (p.44).	5 and 6 - Treatment/ Response
Relevant information is identified, captured and communicated in a defined format and is regularly performed for people to carry out their responsibilities (page 157).	Continuous and iterative processes that an organization conducts to provide, share or obtain information and engages in stakeholder dialogue, to manage risk by recording and reporting them (page 16).	Communication is conducted throughout the risk management process. Since the organization's exposure to risks is not static, effective communication is a key component for identification, changes in existing risks, or new threats and opportunities (p.31).	7 - Communication
Comprehensively, the organization's risk management is monitored, and modifications are made when necessary. Thus, it is possible to react dynamically (pp.161-164).	The purpose of monitoring and critical analysis is to ensure and improve the quality and effectiveness of management. It is necessary to plan as part of the risk management process and involve regular checking or monitoring (p.16).	Monitoring is necessary to understand whether responses are being implemented effectively. Although monitoring has its value, it is only a process of observation. It should be more comprehensive than a review of action plans (p.47).	8 - Monitoring
As for the approach to conducting risk management, the framework defines five categories: (1) governance and culture; (2) strategy and goal setting; (3) performance; (4) review; and (5) information, communication and reporting. These categories are related to twenty organizational principles (pp.18-19).	The standard presents the mandate and the commitment, which comprise the following factors: definition and approval of the policy; alignment between culture and politics; performance indicators; alignment with objectives and strategies; conformity; attribution of responsibility and allocation of resources; and communication of the benefits and maintenance of the structure (p.9).	The principles provide a basis for the approach to be developed. In this approach, it is described the activities to be performed, the sequence in which they are performed, the roles and responsibilities required for deliveries. These deliveries consist of documents, such as records, plans, and reports (p.52).	9-10 - Approach

It can be said that market methodologies have a common set of guidelines for professionals in the area of risk management, that is, similarities regarding the topics addressed. However, as they were developed at different times, there is an evolution of the focus on management techniques, especially ISO 31000 and M_o_R-OGC, as well as a comprehensive set of tools and techniques to support managers in risk management in the organization in all the methodologies presented. Through this comparison, one can also infer the convergence of the methodologies for an understanding that refers to a generic process of risk management, which highlights the understanding of the context, identification and risk assessment, preparation of plans for treatment and implementation of these plans.

4.2. Methodologies of the Brazilian Public Administration

The following are the main risk management methodologies identified in Brazilian Public Administration bodies. Table 8 lists the bodies in which the methodologies were developed, the title of the document and a brief description.

Table 8 – Guidance books and methodologies on risk management of the Brazilian Public Administration.

Body	Tittle	Description
Escola Nacional de Administração Pública (National School of Public Administration) - (2006)	Guide on Risk Management in the Public Service	This guide is not intended to make a comprehensive assessment of risk management or to address all the details of the issue. It intends to create a common starting point for learning and working on what constitutes good risk management and thus to have a sense of the obstacles that can be faced in the incorporation of risk management into governmental decision-making processes. In order for the greatest possible number of people to benefit from reading this guide, technical jargon was avoided, and an effort was made to keep it succinct. Readers wishing to have more comprehensive information can refer to the list of additional features included at the end of the guide.
Instituto Brasileiro de Governança Corporativa (Brazilian Institute of Corporate Governance) - (2007)	Guidance book for Enterprise Risk Management	The recommendations and suggestions contained in the guidebook should be evaluated according to the reality of each organization. Although it is primarily intended for profit-seeking organizations, concepts and suggestions may also be used by first and third sector entities.

Ministry of Planning, Budget, and Management (2013)	Guidance book for Corporate Risk Management	This guide has as main objectives to support the Excellence Model of the Public Management System with regard to the topic of risk management and to introduce the topic of risk management.
Ministry of Finance (2014)	Risk Management Front	Integrated corporate risk management model for the MF.
Ministry of Planning, Development and Management (2016)	The methodology of Information Security and Communications Risk Management of the Information Technology Resources Management System of the Federal Executive Branch - MGR-SISP v 2.0	The methodology aims to standardize and systematize the Information and Communication Security Risk Management (GRSIC) in the Federal Public Administration (APF). The aim is to achieve satisfactory levels of SIC and, at the same time, to rationalize investments by prioritizing actions and avoiding redundancies in risk management.
Superior Court of Justice (2016)	Risk management	The work processes of the SCJ involves risks. Therefore, the awareness that they exist and the ability to manage them, combined with the willingness to take risks and make decisions, is indispensable. With the implementation of this methodology of risk management based on proven experiences, we are increasingly looking for excellence in the provision of quality public services to jurisdictions with speed and transparency.
Instituto Brasileiro de Governança Corporativa (Brazilian Institute of Corporate Governance) -(2017)	Enterprise Risk Management - Evolution in Governance and Strategy	It integrates the series of publications called Cadernos de Governança Corporativa (Corporate Governance Papers), whose objective is to bring to the market practical information that contributes to the process of corporate governance. It proposes to present reflections and guidelines for executives and, above all, management advisors 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 in different maturity stages of GRCorp.
Ministry of Planning, Development and Management (2017)	Integrity, Risks and Internal Control Management Manual	It seeks to present the integrity, risk and internal control management methodology of the Ministry of Planning, Development, and Management, in the context of the model under development in the MP (policy, supervisory bodies, methodology and technological solution).

The following were considered for analysis:

- The methodologies of the Ministry of Planning, Development and Management, developed by the General Coordination of Information Security - CGSIN/DESIN/STI/MP, the MGR-SISP of August 2016, and the Integrity, Risks and Internal Controls Management Manual, elaborated by the Special Advisory on Internal Control, the GIRC of January 2017, for being in line with Joint Normative Instruction 01/2016; and

- The IBGC 2017 methodology, for proposing the assessment of the organization's maturity in terms of risk management.

Other methodologies were not considered in this analysis because of the similarity with the market methodologies or the specialized scope of the body in which it was developed.

4.2.1. The methodology of integrity, risk and internal control management – GIRC

According to the Ministry of Planning, Development and Management, the Integrity Program aims to mitigate corruption and ethical deviations from the mobilization and active participation of public managers by means of measures that ensure delivery of the expected results by society, the strengthening and improvement of the governance structure, risk and control management, and integrity procedures [22].

In this methodology developed by the MP's Special Advisory on Internal Control, premises, concepts, roles and responsibility, the taxonomy of risk events and list of basic controls for a public organization are described. It consists of four pillars:

- **1st Pillar** - Integrity Environment: provides the basis for the program to be effective; is comprised of commitment actions, senior management support, and alignment with strategic planning;

- **2nd Pillar** - Integrity, Risk and Control Management: definition of a Risk Management Policy; Subcommittee on Integrity, Risks and Controls (SIRC); and implementation of risk management;

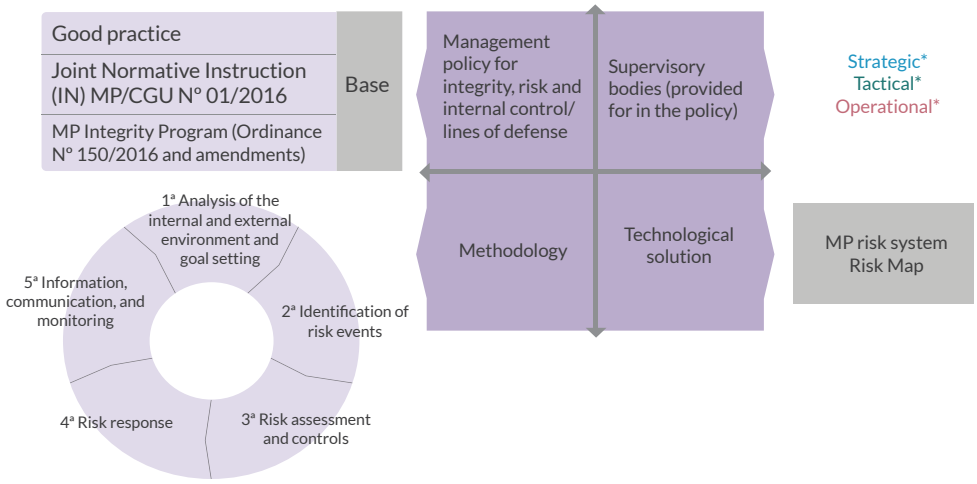
- **3rd Pillar** - Institution and Compliance of Integrity Procedures: integrity involves the development of the code of conduct, reporting channel,

training plan, and internal education; compliance involves actions that foster the declaration of assets, combat conflict of interest and the presence of nepotism and implementation of the Law on Access to Information; and

- **4th Pillar** - Information, Communication and Monitoring: the process of making information available to stakeholders, the relationship between supervisory and monitoring bodies on program actions to assess the quality of the internal control system over time.

These pillars provide a basis for integrity, risk and control management in the organization through the methodological model shown in Figure 7. The following are presented in the methodology:

- the policy, which establishes the principles, guidelines, and responsibilities;
- the supervisory body, which advises the body's highest authority in the definition and implementation of guidelines, policies, standards, and procedures;
- the GIRC methodology, which assumes that the organization's value chain and processes are mapped to apply the "Process Prioritization Method";
- the technological solution, which serves as an instrument to support the application of the GIRC methodology [22].



(continued)

Details on supervisory bodies

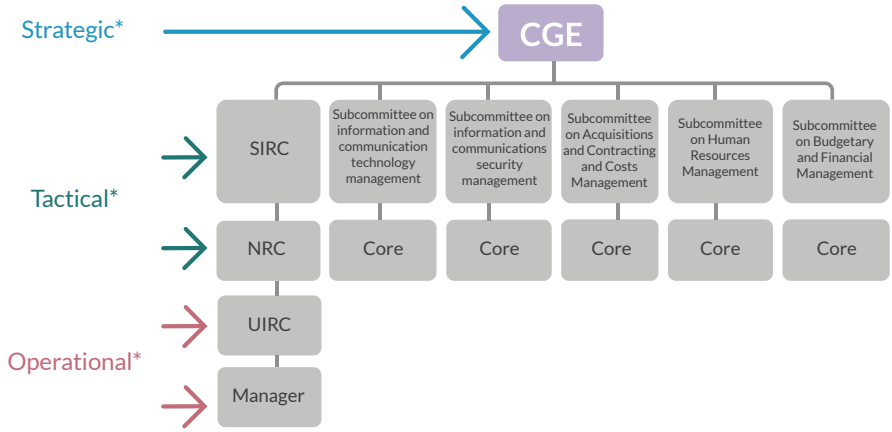


Figure 7 – Methodology of integrity, risk and internal control management
Source: GIRC (2017, p. 16), with adaptations

The methodology emerged from the document "Method of Prioritization of Processes". There, it is possible to identify and evaluate risk processes and events, prioritize those presenting the most critical risks and adopt responses to the risk events of the unit processes. Additionally, this record still provides basic guidelines on good practices to awaken in managers the importance of integrity, risk and internal control management [22].

The major contribution of this methodology corresponds to the structure developed before the application of risk management, which defines a policy to be followed, roles and responsibilities, methods of recording and monitoring risks, and aligning those dimensions with Technology Information (IT) to enable an information system to facilitate risk management in organizations. It also makes an important contribution regarding the availability of internal control tools to enable recording and follow-up through the "Process Prioritization Methodology" and the "Documentation Worksheet", available on the Ministry of Planning website.

4.2.2. SISP- MGR-SISP risk management methodology

The MP, through the General Coordination of Information Security - CGSIN/DESIN/STI/MP, developed a risk management methodology focused

on Information and Communications Security of the System of Administration of Information Technology Resources of the Federal Executive Branch, according to Joint Normative Instruction CGU/MP No. 01/2016. Although it has been developed with a focus on Information and Communication Security Risk Management (GRSIC), the standard can be adapted as a generic process of risk management.

The methodology makes a great contribution in relation to the Brazilian context by understanding references to current norms and laws applied to risk management and by having a set of processes, activities, and tasks in a structured way, as shown in Figure 8. In the process, communication and monitoring are tasks that must happen in parallel with the set of risk management processes. In this way, a strong similarity with the ISO 31000 methodology is inferred in a logical sequence of stages for the resolution of the risks.

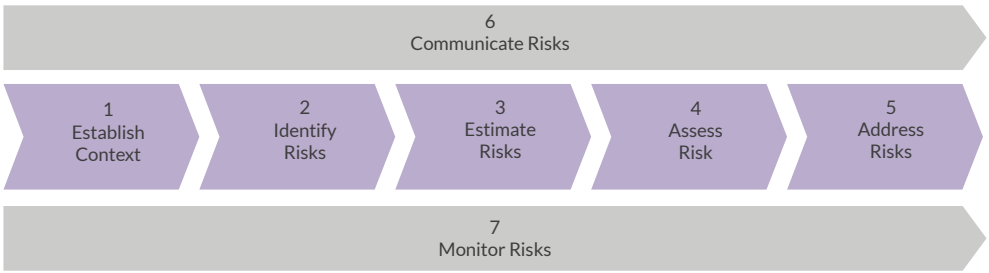


Figure 8 - Risk management methodology proposed by MGR-SISP
Source: MGR-SISP (2016, p. 36)

This methodology has seven processes that contain 16 activities, totaling 65 tasks for the management of risks, as shown in Table 8. The roles for these tasks are also defined, which correspond to:

- Competent authority: responsible for providing the necessary resources for risk management, identifying those responsible, initiating risk management activities and approving important points related to risk management, such as the objective, restrictions, and enhancements of the MGR-SISP;

- Risk manager: responsible for carrying out risk management activities and coordinating efforts to identify and estimate risks, propose improvements needed to mitigate risks, and report the results of analyzes to all stakeholders;

- Responsible for the unit of the organization: accounts for an area of the organization in which the methodology will be implemented or for an area that must provide information for risk management. Has the role of coordinating the provision of the information needed to identify and estimate risks and make necessary improvements when the analyzes indicate;

- Responsible for assets: responds by providing information about the assets that are part of the risk analysis. This information helps decision-making on controls to be implemented.

In Table 9, those responsible and their respective tasks are represented by the following acronyms: CA - Competent authority, in black; RM - Risk Manager, in blue; RA - Responsible for Assets, in orange; and RU - Responsible for the Unity of the Organization, in green. The gray color was used for more than one role [9].

Table 9 - Tasks in the MGR-SISP

Process	Activity	Task	Initials
1. ESTABLISH CONTEXT	1.1 Start GRSIC project	1.1-A: Define Risk Manager	CA
		1.1-B: Identify objectives, premises, constraints, and scope of the GRSIC project	RM
		1.1-C: Validate objectives, premises, constraints, and scope of the GRSIC project	CA
		1.1-D: Define those responsible for the units of the organization	RM
		1.1-E: Define those responsible for assets	RU
	1.2 Perform pre-analysis of the scope of the GRSIC project	1.2-A: Prepare a questionnaire	RM
		1.2-B: Identify professionals to answer the questionnaire	RM
		1.2-C: Get Answers	RM
		1.2-D: Consolidate Results	RM
		1.2-E: Validate results	CA

Process	Activity	Task	Initials
2. IDENTIFY RISKS	2.1 Identify assets	2.1-A: Define the GRSIC approach	RU/RM
		2.1-B: Register assets	RU
		2.1-C: Validate information about assets	RM
	2.2 Identify threats, controls and vulnerabilities	2.2-A: Request identification of threats, controls, and vulnerabilities	RM
		2.2-B: Obtain threats, controls, and vulnerabilities of unit assets	RU
		2.2-C: Report threats, controls, and vulnerabilities of the unit assets	RA
		2.2-D: Validate threats, controls, and vulnerabilities of unit assets	RU
		2.2-E: Validate information about threats, controls, and vulnerabilities	RM
3. ESTIMATE RISKS	3.1 Assess the impacts	3.1-A: Request impact analysis	RM
		3.1-B: Obtain information on the consequences	RU
		3.1-C: Identify consequences	RA
		3.1-D: Define impacts	RU
		3.1-E: Validate impact analysis	RM
	3.2 Evaluate probabilities	3.2-A: Request Probability Assessment	RM
		3.2-B: Request definition of probabilities	RU
		3.2-C: Define Probabilities	RA
		3.2-D: Assess Probabilities	RU
		3.2-E: Validate Probability Assessments	RM
	3.3 Estimate risk level	3.3-A: Request risk estimates from each unit	RM
		3.3-B: Request risk estimates	RU
		3.3-C: Define risk estimates	RA
		3.3-D: Assess unit risk estimates	RU
		3.3-E: Validate risk estimates of the GRSIC project	RM
4. ASSESS RISKS	4.1 Classify the risks	4.1-A: Carry out risk classification	RM
		4.1-B: Record awareness of risk classification	RU
		4.1-C: Request validation of risk classification	RM
		4.1-D: Validate risk classification	CA

5. ADDRESS RISKS	5.1 Estimate resources for the treatment of risks	5.1-A: Request treatment estimates	RM
		5.1-B: Estimate costs, efforts, deadlines, and constraints	RU
		5.1-C: Validate estimates	RM
	5.2 Define response to risks	5.2-A: Define treatment	RM
		5.2-B: Define controls and monitoring	RM
		5.2-C: Analyze risk response	RU
		5.2-D: Request validation of responses to risks	RM
		5.2-E: Validate responses to risks	CA
	5.3 Implement risk responses	5.3-A: Request Risk Treatment Plan (PTRs)	RM
		5.3-B: Prepare Risk Treatment Plan	RU
		5.3-C: Assess Risk Treatment Plan	RM
		5.3-D: Validate Risk Treatment Plan	CA
		5.3-E: Start risk treatment	RU
		5.3-F: Perform Risk Treatment Plan	RA
6. COMMUNICATE RISKS	6.1 Plan risk communication	6.1-A: Prepare Risk Communication Plan	RM
		6.1-B: Validate Risk Communication Plan	CA
	6.2: Implement Risk Communication Plan	6.2-A: Get information on GRSIC	RM
		6.2-B: Send information on GRSIC to stakeholders	GR
	6.3 Validate strategic information	6.3-A: Get strategic information on GRSIC	CA
		6.3-B: Avaliar informações estratégicas sobre a GRSIC	AC
7. MONITOR RISK	7.1 Monitor SIC risk management	7.1-A: Check for changes impacting the GRSIC	All of them
		7.1-B: Communicate changes impacting the GRSIC	All of them
		7.1-C: Request update of GRSIC	RM
		7.1-D: Update GRSIC Information	All of them
	7.2 Monitor risk management	7.2-A: Validate treatments	RU
		7.2-B: Monitor implementation of PTRs	RM
		7.2-C: Monitor strategically	CA
		7.2-D: Verify needs for change in the treatment of risks	RM

Source: MGR-SISP (2016, pp. 31-34), with adaptations

It is understandable that GRSIC has tools to support managers and still is appropriate to the national context. Although it has specific tasks for the Information and Communication Security (SIC) scenario, it is possible to generalize to other cases or other organizations. Also, MP provided tools in electronic format to support managers in recording and identifying these risks, such as the Process Prioritization Worksheet and the Documentation Worksheet. However, these tools present limitations and restrictions on the treatment and monitoring of risks. However, in the MGR-SISP, the explanation of the set of tasks and roles contributes significantly so that the uncertainties are resolved.

4.2.3. IBGC Risk Management Methodology

According to the IBGC (2017) methodology, regarding Corporate Risk Management (GRCorp), the Board of Directors should be responsible for determining the organization's strategic objectives and risk map. This consists of identifying the "degree of appetite" for the risks of the organization and the ranges of tolerance and deviations in relation to acceptable levels of risk. The methodology should also establish the board's policy of responsibility to assess which risks the organization may be exposed to, develop procedures to manage them, and evaluate, discuss and approve the risk policy proposed by the Executive Risk Committee [13].

It is recommended that the members of the Board of Directors know performance indicators to express their opinion on the subject. It is also suggested that the company has a program to bring the risk management culture to new advisors. The role of implementing a structure of risk management and control is assigned to the managers, with the Audit Committee exercising the supervision, assisted, when necessary, by the three lines of defense, respectively:

- 1st Line of defense - carried out by the managers of the units and those directly responsible for the processes: it contemplates the functions that manage and has responsibility for the risks;

- 2nd Line of Defense - performed by corporate managers of GRCorp, compliance managers or other control practices, for example, and includes functions that monitor the integrated view of risks;

- 3rd Line of Defense - conducted by the internal audit: provides independent evaluations by monitoring internal controls.

There are different alternatives for building GRCorp governance and achieving the desired maturity level. Each organization should design the one most appropriate to its business profile, organizational culture, management model and required level of maturity in relation to its GRCorp practices. For measurement of maturity, organizations need to assess their current capacity for risk practices and understand how and why they should be improved. This evaluation will allow organizations to document, communicate, and program improvements in their model [13].

Figure 9 presents an overview of the components of GRCorp integrated with the organization's corporate governance process and its main elements for maturity measurement. In this representation, the Regulation (Compulsory and Optional) supports the definition of external and internal contexts that influence corporate governance. For each component, there should be reflections to identify the current level of maturity. These reflections, separated into components, are recorded in Table 10, and they should complement Figure 9.

The reflections in Table 10 contribute to the identification of the maturity stage according to the GRCorp components. For each context or stage, it is necessary to understand what level of maturity the organization is, for risk management, and what would be the actions to reach the next level. In Table 11, these maturity levels are recorded, which should contribute to the identification of the current state of the organization and later stages.

The methodology of IBGC (2017) proposes the following levels of maturity in relation to the stages of an organization's GRCorp:

- Initial;
- Fragmented;
- Defined;
- Consolidated; and
- Optimized.

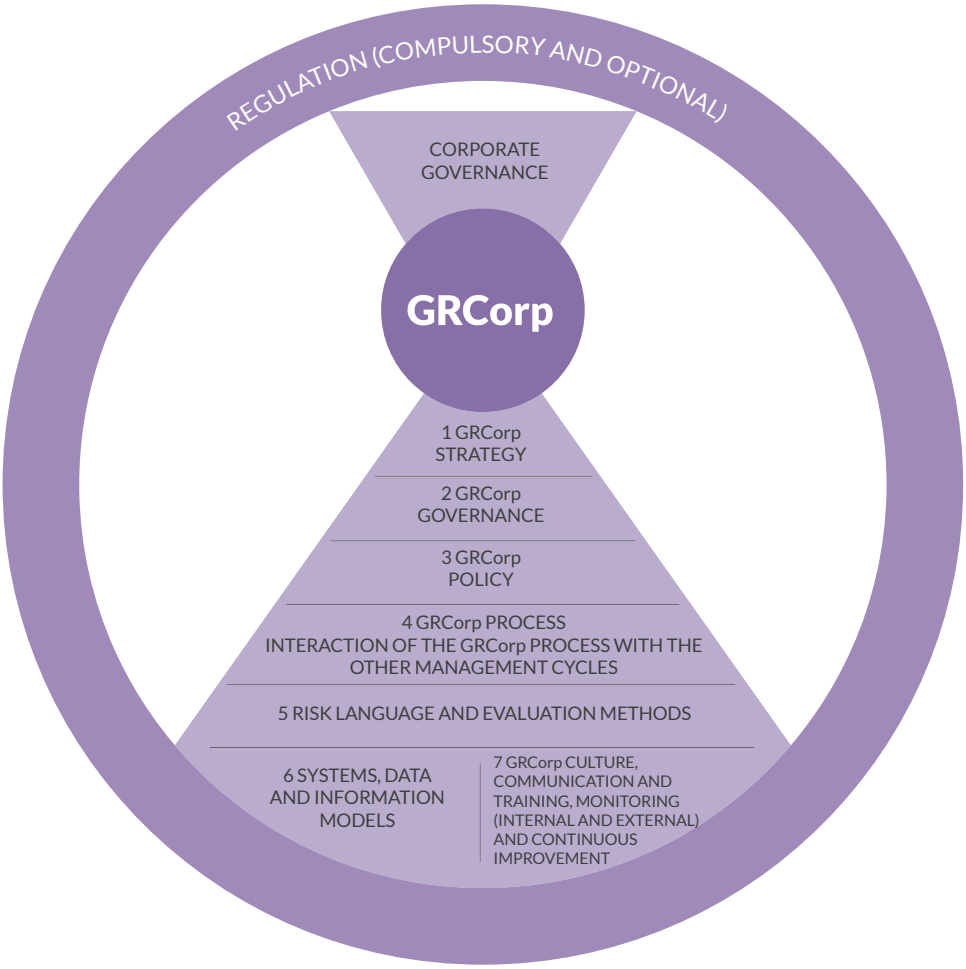


Figure 9 - IBGC Risk Management - Maturity Assessment
Source: IBGC (2017, p. 34), with adaptations

Table 10 - Reflections on the components of GRCorp

GRCorp component	Reflections
1) GRCorp Strategy	• Are there established GRCorp strategies, goals and targets?
(2) GRCorp governance	• Is there an organizational structure with clearly defined roles and responsibilities in GRCorp practices? • Does the structure consider the roles of the Committee and Board and all three lines of defense detailed in GRCorp governance model?
(3) GRCorp Policy	• Are the issues above regimented, approved, and disclosed through a GRCorp policy?
(4) GRCorp process and interaction of this process with the other management cycles	• Is there a GRCorp process defined and implemented with activities of risk identification, risk assessment (including scenarios), evaluation of control, response, monitoring and communication activities? • Is there a risk management standard (or an equivalent document) of internal disclosure that establishes procedures, responsibilities – including reporting–, segregation of functions, frontiers of action and the general governance system of risk management? • Are GRCorp practices in line with other control practices? • Is there a defined model for incorporating GRCorp into decision-making processes and management cycles?
(5) Risk language and assessment methods	• Is there risk taxonomy (categories) and defined assessment methods? • Does the organization use measurement techniques?
(6) Systems, data and information models	• Is information about the organization's risk exposure shared across different organizational levels and captured consistently?
(7) GRCorp Culture of communication and training, monitoring (internal and external) and continuous improvement	• Is GRCorp embedded in decision-making, organizational culture, and day-to-day business management? • Does the organization evaluate employees' understanding of GRCorp culture, practices, and internal control system? • Are GRCorp communication and training actions carried out with the different audiences of the organization? • Do governance bodies and the three lines of defense permanently monitor GRCorp practices? • Is GRCorp carried out continuously?

Table 11 - Measurement of maturity in relation to components

Initial	Fragmented	Defined	Consolidated	Optimized
1) GRCorp Strategy				
The organization does not know how, who, when, where and why to implement risk management. Performance targets exist.	The organization knows where to start, even if it is unclear where it wants to go. Performance targets exist.	Risk management strategy clearly defined and implemented. Performance targets are defined.	Risk management strategy clearly defined and implemented. Performance goals are monitored.	Risk management strategy clearly defined, implemented and integrated with other management cycles. Performance targets are aligned with strategy and risk management.
(2) GRCorp governance				
The functions of the 2nd line of defense are performed individually, not integrated with the strategic vision.	The functions of the 2nd line of defense focus on the historical areas, in response to compliance with regulatory obligations.	The functions of the 2nd line of defense cover business risks and value drivers, and there may be overlaps. The organizational structure is defined.	The functions of the 2nd line of defense comprehensively cover the organization's risks. The organizational structure is well defined and aligned with strategy and objectives.	The objectives are clearly defined and aligned among the various functions of the 2nd line of defense in order to provide value to the organization. The model is a benchmark in the industry.

Initial	Fragmented	Defined	Consolidated	Optimized
(3) GRCorp Policy				
Policies and procedures are not defined, and there is no consistent process for their development and maintenance.	Policies and procedures are limited to key driving areas.	GRCorp policies and procedures are formal and consistently communicated throughout the organization.	Policies and procedures are well developed and applied consistently throughout the organization. They are continually updated according to changes in business strategy.	Third parties and the industry regularly reference policies and procedures. Policies have an impact on the external business environment.
(4) GRCorp process and its interaction with the other management cycles				
Processes and controls that support risk management are poorly developed. Minimal monitoring activities occur.	Risk identification and assessment processes are performed as distinct or separate activities happening on demand.	A risk-based approach is implemented systematically and consistently applied at the corporate level and across the organization.	Risk identification and assessment processes are well defined and structured. Business managers systematically monitor the risks associated with their processes.	Risk identification and assessment processes are well integrated into strategic objectives. Efficient and coordinated monitoring activities.
(5) Risk language and assessment methods				
There is no standard approach to setting the acceptable level of risk. Qualitative and quantitative analyses are performed.	There is no standard approach to setting the acceptable level of risk. Qualitative and quantitative analyses are performed.	There is a standard approach to setting the acceptable level of risk. However, it is not used consistently by all functions.	Uses a standardized and consistent approach to define appetite and risk tolerance. Stress tests and scenario analysis are used at the corporate level.	Uses a standardized and consistent approach to define appetite and risk tolerance. Future scenarios and stress tests are used to explore risk analysis.

(6) Systems, data and information models				
Information and reporting models are driven by external requirements and are not sufficiently defined.	Information and reporting models are defined by top management but are not understood by management or aligned within the organization.	Models of information and reporting are well defined and understood. The reports are prepared with correct, complete information.	Emerging technologies are leveraged to enable risk management objectives to be achieved at the corporate level.	Integrated technologies enable the organization to manage risks; they are considered highly effective and recognized as market-leading practices.
(7) Culture, communication and training, monitoring and continuous improvement				
There is no dissemination plan implemented to formalize the main decisions of the organization regarding risk practices.	There are communications, but they are not formally defined. Specific training is conducted.	Clear communication protocols exist and are open to all employees. Two-way communication with stakeholders is encouraged.	The culture of risks and controls is embedded in the daily activities of the organization, and risks are treated proactively at the process and function levels.	Risk and control culture is effective at all levels of the organization. Dissemination programs are applied for the continuous evolution of risk management.

Source: IBGC (2017), with adaptations

It should be remembered that the components maturity levels are independent of each other. This means that each component (individually) can be positioned at different levels of maturity.

After conducting the maturity level assessment, the Board of Directors should reflect on what stage the organization should be and, subsequently, develop necessary actions to define the expected deadlines in order to reach the next stages. The maturity scale (Figure 10) provides a structured and detailed guide for continuous improvement in search of short-, medium- and long-term results for the GRCorp strategy [13].

Through this tool outlined in Figure 10, the organization can document, communicate, and schedule improvements regarding its internal environment. The methodology also recommends conducting industry standards research to compare the organization with leading companies in these GRCorp practices. In order to measure the maturity level, the dimensions (principles) of the M_o_R (2010) were combined with the form of measurement and presentation contained in the IBGC methodology (2017). This adjustment facilitates understanding and allows the creation of improvement plans and other actions.

4.2.4. Comparison between the main methodologies of the Brazilian Public Administration

The Public Administration methodologies, as well as the market methodologies, were developed to meet the different needs and institutions of this sector. In Brazil, some methodologies have been structured, as of 2006, by different bodies of this scope and to respond to the organizational objectives in these institutions or to support them. The following is a comparison between the main concepts presented by the methodologies highlighted in this study regarding risk management by the Brazilian Public Administration. The results of this comparison are presented in Table 12.

Dimension	Level of Maturity					Current Stage	Desired Stage	Action Plan
	Initial	Fragmented	Defined	Consolidated	Optimized	★	★	
Aligned with the objectives	★	→ ★				2	2	Action Plan A
Appropriate to the context		★	→ ★			3	3	Action Plan B
Involves stakeholders		★	→ ★			3	3	Action Plan C
Defined Process		★	→	→ ★		4	4	Action Plan D
Decision-making		★	→	→	→ ★	5	5	Action Plan E
Continuous improvement	★	→	→	→	→ ★	3	3	Action Plan F
Collaborative culture	★	→ ★				2	2	Action Plan G
Measurable values		★	→ ★			3	3	Action Plan H

Figure 10 - Maturity level structure for continuous improvement
Source: IBGC (2017), M_o_R (2010), with adaptations

Table 12 - Comparison between the definitions of the main methodologies of the Brazilian Public Administration

GIRC (2017)	MGR-SISP (2016)	IBGC (2017)	Item
In this model, the policy is who must establish the principles, the guidelines and the responsibilities of the involved ones and of the whole institution.	It represents the purpose of investments in risk management. This purpose must be associated with the organization's mission and objectives and must also be documented and approved by senior management representatives.	It should be the responsibility of the board of directors of the organization. Its function is to document and create a means to assess the risks to which the institution may be exposed and develop procedures to manage them.	Policy
It aims to mitigate corruption and ethical deviations from the mobilization and active participation of public administrators using measures that ensure the delivery of the results expected by society, by strengthening and improving the governance structure, risk and control management, and integrity procedures.	It seeks to ensure risk management with a focus on Information and Communication Security (SIC). This risk management should enable better communication and better decision-making on the priorities for the allocation of SIC resources.	It believes that the Board of Directors should be responsible for determining the organization's strategic objectives and risk map. This is to identify the "degree of appetite" for the risks of the organization and the ranges of tolerance and deviations in relation to acceptable levels of risk. In summary, it has the purpose of establishing and measuring the maturity of the institution's risk management.	Purpose/Objective
The environment and the integrity, risk and control management; the institution and conformity of its procedures; information, communication, and monitoring.	Rationalization of resource use: avoid redundant protections and protect vital resources.	The operation of strategies, policies, processes, risk languages and methods of evaluation, data system, culture, communication and monitoring for corporate governance.	Pillars
It presupposes the analysis of internal and external environments, the identification of risk events, risk and control assessment, risk responses, information, monitoring, and control.	Existing risks and the likelihood of their occurrence, as well as the extent and severity of the negative effects produced, should be identified. This is determined by a set of 65 tasks grouped into 16 activities, which are organized into seven processes.	It aims at establishing policy, dividing responsibilities (in lines of defense), identifying and assessing risks, attaining maturity level (initial, fragmented, defined, consolidated, optimized), communication, training, monitoring, and continuous process improvement.	Methodology

Notably, each one of the evaluated methodologies presents structured thinking in what corresponds to its policies, purpose and objectives, pillars, and the own methodological structuring. Therefore, the main difference between them is the practical application, since GIRC (2017) focuses on maintaining the integrity of the processes by public administrators that must correspond to the expectations of the society. MGR-SISP (2016) intends to improve communication and decision-making aimed at information security; and the IBGC (2017) methodology intends to establish the maturity level of institutions. In short, we do not emphasize that one methodology is better than the other is, but in fact, one methodology may be more appropriate than the other is, depending on the interest of each organization.

4.3. Tools for monitoring risks

Since risk recording is occurring in the environment, a set of actions is required to enable these risks to be communicated and effectively reported to decision makers. Some tools for this purpose are presented below.

4.3.1. Risk map

Risk map is a tool for assessing the risks according to the criteria or parameters provided by the specialists, technicians or those responsible for the identification of the risk. In this case, the map should reflect the risk analysis to allow a holistic view, that is, to indicate the risk prior to treatment and its current situation. These risks can be filtered to the organization or department as well as the opportunities or threats and other grouping mechanisms that facilitate the visualization of the decision maker.

The technique suggests the production of a probability and impact matrix capable of indicating the prioritization of activities and current actions. In this way, the risk map assists the specialist in identifying the risks that must be analyzed or addressed more urgently, in addition to allowing the monitoring and evolution of each risk identified. Figure 11 corroborates the understanding of what a risk map is:

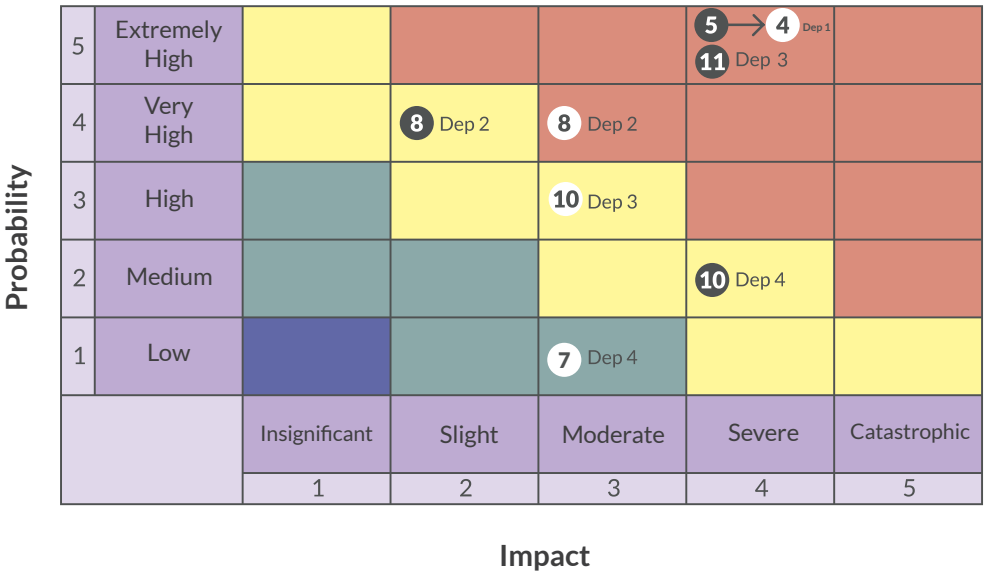


Figure 11 - Risk map structure between departments

In the example of the risk map, the dark circles (filled) represent the previous moment of the identification of the risks, and the clear ones the current moment. The numbers within the circles represent the amount of risk related to the department. Note that, for department 1 (Dep1), there were five risks previously and that at present there are only four risks, that is, a risk has already been dealt with. Department 2 (Dep2) maintained the amount of risks of the previous moment, but its risks had a high impact level, which caused a repositioning of the graph, going from slight to moderate impact. Note also that department 3 (Dep3) was added risk and, also, its risks increased significantly the probability of events, which went from high to elevated, and the probability of impact that went from moderate to severe. Finally, department 4 (Dep4) had three risks solved, with the remaining risks decreasing in the level of probability and impact.

The second example proposed refers to the visualization of the risks of a single department. The illustration in Figure 12 reflects this scenario.

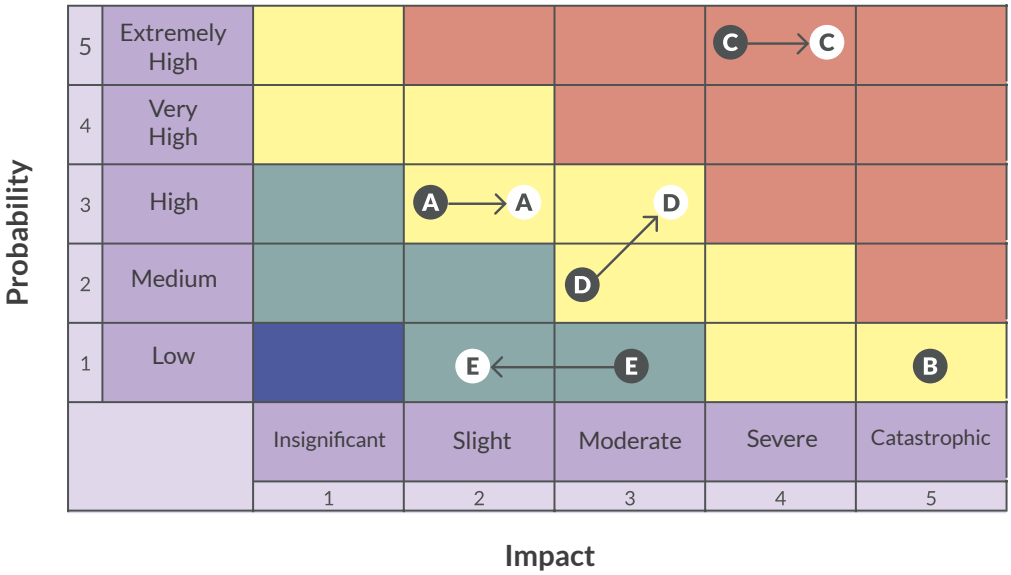


Figure 12 - Risk map structure: department's risks

When viewing the risks of a single department, such as department 1 - Figure 12, one can see the risks that affect it. There is a letter (A, B, C, D, E) in each circle to identify the risk uniquely. We can see in this case that Risk A maintained the levels of the previous moment and that it remains unresolved at present. Meanwhile, Risk B has been resolved. Risk C also remained the same and still without a solution. Risk D, in turn, was aggravated, and the probability of occurrence increased. Finally, Risk E has been slowed down at present, and its impact level has been reclassified to slight. It is inferred that these maps should allow a visualization based on the criteria that the risk specialist wishes to visualize. In this way, it is possible to prioritize and distribute the tasks to the agents and specialists, besides allowing traceability and monitoring of the risks. The colors, in both examples, help to understand the urgency of the cases visually. Blue indicates the normality of risk, green, minimal urgency, yellow requires attention and, finally, red characterizes the most urgent risks.

4.3.2. Summarized reports

The purpose of summarized reports is to provide information to decision-makers with a summary view of the amount of risks at the time of their identification (previous time) and at present, as well as a comparison between these two moments. This technique presents the sum of threats and

opportunities through a filter. Figure 13 exemplifies this set of information in four departments of any organization in a given period.

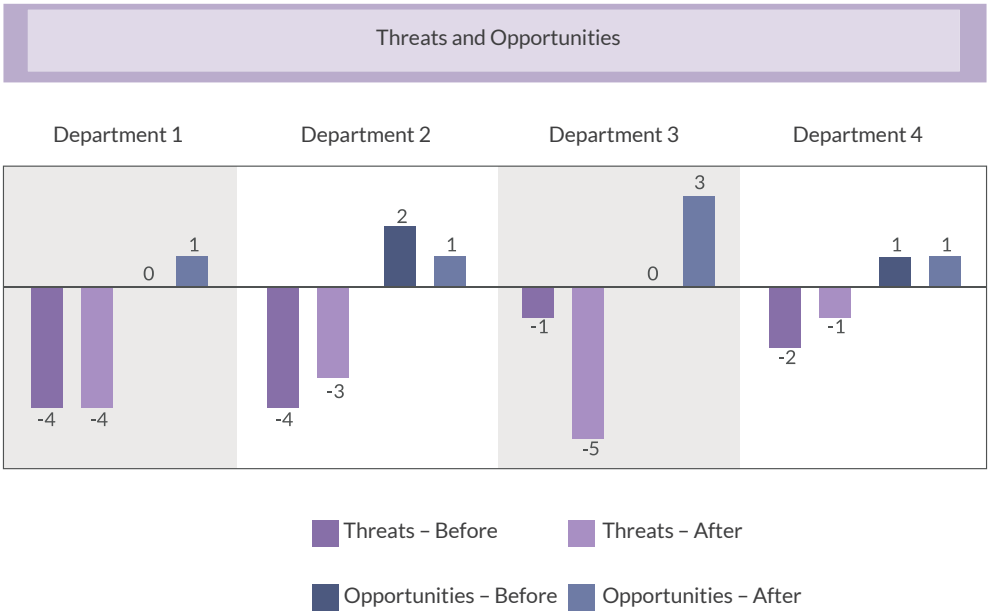


Figure 13 - Preparation of summarized report: threats and opportunities

In this scenario, it is observed that department 1 (Dep1) maintained the amount of threats of the previous moment, but identified an opportunity at the moment. Department 2 (Dep2) solved a threat and completed an opportunity. Department 3 (Dep3) identified four new threats and three new opportunities. Finally, department 4 (Dep4) solved a threat but did not complete the previously recognized opportunity.

The summarized report does not contain the severity of the risks but the amount of risks and opportunities to which the departments are exposed. It allows a quick and expanded view of which departments are facing the most problems and require more attention. In conjunction with this type of report, succinct and explanatory texts should be developed regarding identified risks and opportunities.

4.3.3. Communications and alert messages

After the quantitative recording of risks, a set of information such as survey date, proximity and last update may contribute to systematic reviews to occur. For example, a severe case that has not been updated for more than 15 days may lead to a problem. In this case, it is recommended that the risks be often revisited to update the information in the record.

A second example corresponds to the risks that are close to the solution deadline. Through alert messages, decision-makers can stay tuned. It is worth highlighting the use of information systems that can be created for specific alerts by e-mail or another communication channel, notifying the risk specialists in the conduct of their activities. A simple attitude that results in safer and more efficient risk management.

4.3.4. Decision trees

Among the more practical models that contribute to organizational decision making, there is the decision tree. The method is characterized by systematizing a series of facts, risks, probabilities, and opportunities - related to a situation, objective, and goals or, on a larger scale, programs and projects - whose effects must be recognized, manipulated and compared. Visually, decision trees take the form of diagrams and structure a map with possible choices for the best action. The tool, even in its simple form, can provide logic for choosing alternative courses of action/decision. According to Keeling [29], decision trees help in various situations, from risk assessment in an organization, or comparison between alternative proposals, to the discussion of the results of a brainstorming session. According to Keeling [29, p. 217], the method ensures that the quality of all decisions is influenced by the accuracy of information; quality of judgments and evaluations; probability factors; and the attitude of the decision-maker about risk management. Figure 14 exemplifies the logic in decision trees.

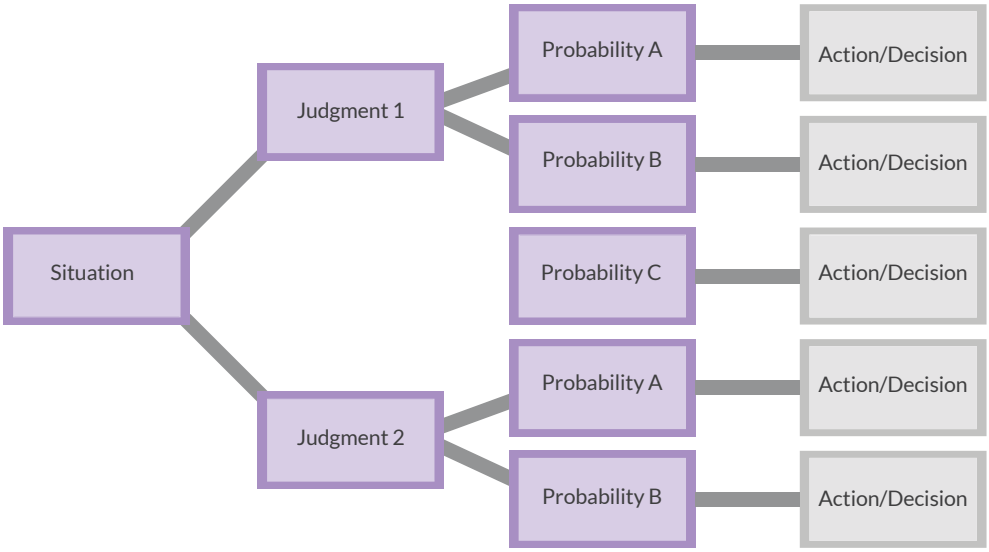


Figure 14 - Conception of logic in decision trees
Source: Keeling (2002, p. 220), with adaptations

4.3.5. Brainstorming

Technique focused on solving problems or expanding ideas so that these problems are solved. The first and perhaps most important stage in the technique is to ensure the definition and/or recognition of the problem, since only then will it be possible to plan corrective actions. When dealing with "problems" or specific situations, the method encourages the gathering of a group of people so that they can reflect and generate innovative thoughts that seek a solution. Among other advantages of brainstorming, it is possible to highlight its ability to sprout the causes for problems, help decide a step by step in developing a project and recognize opportunities, as well as encouraging the participation of all members of a team or organization.

4.3.6. Scenario analysis

Extremely widespread in consulting and management studies, scenario analysis aims at strategic organizational action by considering information from the present in a context of the future. As described in the Policy and Integration Secretariat's Strategy Portal [30], the ability to analyze scenarios underlies the importance of designing strategic planning and, therefore, drives

action. In summary, the main function of scenario analysis is the recognition of the context (internal and external) in which the organization is inserted, in order to identify future factors that are likely to occur. Simple attitudes such as these ensure a clearer view of the current scenario and allow for more informed and accurate decision making. To assist in the development of this methodology, it is recommended to jointly use the SWOT Analysis procedures - Strengths, Weaknesses, Opportunities and Threats -, which strengthen the organizational strategies.

5. Laws and rules related to risk management in the public sector: the case of brazil

In the world's democracies, the Public Administration has increasingly felt the presence of citizens, demanding public policies that long for the provision of quality services. Social control, through the requirement of greater transparency and accountability, makes us feel the regulation of laws and norms that govern a better performance of the public management towards its institutions and its servants.

Due to these pressures, there was also an almost automatic need for the Public Administration to reinvent itself. Notably, the models of Public Administration have assumed, over time, peculiar ways of presenting and organizing itself in the face of globalization and economic, environmental, political and social changes. Risk management is an excellent example of transformation in Public Administration and has been practiced in several countries recently.

In Brazil, what is perceived is a paradigmatic change on the part of public bodies in trying to manage their budgetary, human and administrative resources better. However, this change, in large part, comes from the interest of the Brazilian Public Administration, through the Ministry of Planning, Budget and Management, and the Office of the Comptroller General of the Union, to try to provide laws and regulations that encourage the adoption of systematized measures for risk management, internal controls and governance.

It is the peoples, in their established territories, who define the laws and regulations to be applied in explicit cases to discipline, limit and organize their societies. Laws, as a rule, are guidelines established by the constituent power to be respected by all members of society. Clearly, every law should be in line with the Federal Constitution of the country. Regulations are, in this case, instructions; administrative acts characterized in kind, nature, and purpose to satisfy principles and determinations contained in the laws.

This chapter contains the laws and regulations (Table 13) related to risk management and valid in Brazil. The surveys were conducted on Public Administration sites to support managers regarding legal recommendations

and obligations. It is worth remembering that the consultation of this material is indispensable for managers since it should provide a legal basis for the development of regulations and internal policies of each organization.

Table 13 - Laws and regulations on risk management in Brazil

Legislation	Year	Main object/subject
COMPLEMENTARY LAW nº 101	2000	Established that the Annual Budget Guidelines Law (LDO) should determine the primary surplus target and contain an annex of fiscal risks with the evaluation of contingent liabilities and other risks capable of affecting the public accounts.
COMPLEMENTARY REGULATION nº 02/ IN01/DSIC/GSIPR	2008	Methodology of Information and Communication Security management (SIC).
NORMATIVE INSTRUCTION GSI Nº 1	2008	Regulates the management of SIC and communications in the Federal Public Administration (APF), direct and indirect, and gives other provisions.
COMPLEMENTARY REGULATION nº 03/ IN01/DSIC/GSIPR	2009	Guidelines for the elaboration of SIC policy and communications in APF bodies and entities.
COMPLEMENTARY REGULATION nº 05/ IN01/DSIC/GSIPR	2009	Regulates the creation of Treatment and Incident Response Teams in Computer Networks (ETIR) in APF bodies and entities.
COMPLEMENTARY REGULATION nº 06/ IN01/DSIC/GSIPR	2009	Establishes guidelines for business continuity management, in aspects related to SIC and communications, in APF organs and entities, direct and indirect.
COMPLEMENTARY REGULATION nº 08/ IN01/DSIC/GSIPR	2010	Establishes guidelines for the management of incidents in computational networks in APF organs and entities.
COMPLEMENTARY REGULATION nº 10/ IN01/DSIC/GSIPR	2012	Establishes guidelines for the inventory process and mapping of information assets to support SIC and communications of APF organs and entities, direct and indirect.
COMPLEMENTARY REGULATION nº 11/ IN01/DSIC/GSIPR	2012	Establishes guidelines for conformity assessment in aspects related to SIC and communications in APF organs and entities, direct and indirect.
COMPLEMENTARY REGULATION nº 12/ IN01/DSIC/GSIPR	2012	Establishes guidelines and basic guidelines for the use of mobile devices in aspects related to SIC and communications in APF organs and entities, direct and indirect.

Legislation	Year	Main object/subject
COMPLEMENTARY REGULATION nº 13/ IN01/DSIC/GSIPR	2012	Establishes guidelines for the management of changes in aspects related to SIC and communications in APF organs and entities, direct and indirect.
COMPLEMENTARY REGULATION nº 14/ IN01/DSIC/GSIPR	2012	Establishes guidelines for the use of cloud computing technologies, in aspects related to SIC and communications, in APF organs and entities, direct and indirect.
COMPLEMENTARY REGULATION nº 15/ IN01/DSIC/GSIPR	2012	Establishes SIC and communications guidelines for the use of social networks, in APF organs and entities, direct and indirect.
COMPLEMENTARY REGULATION nº 16/ IN01/DSIC/GSIPR	2012	It establishes guidelines for the development and acquisition of secure software in APF organs and entities, direct and indirect.
COMPLEMENTARY STANDARD nº 04/IN01/DSIC/GSIPR and its annex	2013	Establishes guidelines for the SIC and Communications risk management process (GRSICC) in APF bodies and entities.
COMPLEMENTARY REGULATION nº 17/ IN01/DSCI/GSIPR	2013	Establishes guidelines in the contexts of action and adjustments for professionals in the area of SIC and communications.
COMPLEMENTARY REGULATION nº 18/ IN01/DSIC/GSIPR	2013	It establishes guidelines for SIC and communications teaching activities in APF bodies and entities.
GSI NORMATIVE INSTRUCTION Nº 2	2013	Provides on the security accreditation for the treatment of classified information, in any degree of secrecy, within the scope of the Federal Executive Power.
GSI NORMATIVE INSTRUCTION Nº 3	2013	It deals with the minimum parameters and standards of cryptographic resources based on state algorithms for encryption of classified information within the scope of the Federal Executive Branch.
DECREE Nº 8.135	2013	Provides for data communications of the direct, autarchic and foundational Federal Public Administration, and on the waiver of bidding on contracting that could compromise national security.
COMPLEMENTARY REGULATION nº 07/ IN01/DSIC/GSIPR	2014	Establishes guidelines for the implementation of access controls related to SIC and communications, in the organs and entities of APF, direct and indirect.
COMPLEMENTARY REGULATION nº 09/ IN01/DSIC/GSIPR	2014	Establishes specific guidelines for the use of cryptographic resources in SIC and communications, in the organs or entities of APF, direct and indirect.
COMPLEMENTARY REGULATION nº 19/ IN01/DSIC/GSIPR	2014	Establishes minimum SIC and communications standards for APF structuring systems, direct and indirect.

COMPLEMENTARY REGULATION nº 20/ IN01/DSIC/GSIPR	2014	Establishes guidelines for information and communications security to establish the process of information processing in the organs and entities of APF.
NORMATIVE INSTRUCTION SLTI/ MP Nº 4	2014	It deals with the process of contracting Information Technology (IT) solutions by the member bodies of the System for Administration of Information Technology Resources (SISP) of the Federal Executive Branch.
INTERMINISTERIAL ORDINANCE MP/MC/ MD Nº 141	2014	Provides that data communications of direct, autarchic and foundational APF shall be carried out by telecommunication networks and Information Technology (IT) services provided by APF bodies or entities, including public companies and mixed-capital companies of the Union and its subsidiaries, observing the provisions of this ordinance.
JUDGMENT TCU Nº 4.330	2014	Provides on risk management in hiring.
FEDERAL DECREE Nº 8.420	2015	It regulates various aspects of the Anti-Corruption Law, such as criteria for calculating the fine, parameters for evaluating compliance programs, rules for the conclusion of leniency agreements, and provisions on national registrations of punished companies.
JUDGMENT TCU Nº 2.110	2015	Deals with managing risks of the organization.
JOINT NORMATIVE INSTRUCTION CGU/ MP Nº 1	2016	Provides for internal controls, risk management, and governance within the Federal Executive Branch.
DECREE Nº 8.945	2016	Regulates, within the scope of the Union, Law 13.303, of June 30, 2016, which provides for the legal status of public companies, mixed-capital companies, and their subsidiaries, within the Union, States, Federal District, and Municipalities.
Law No. 13303	2016	It provides for the legal status of public companies, mixed-capital companies, and its subsidiaries, within the Union, States, Federal District, and Municipalities.

Source: MGR-SISP (2016), with adaptations

Table 13 is an updated list of current laws and regulations in Brazil, affecting and modifying the execution and role of risk management. It should be remembered, however, that risk management processes are subject to change and particularities according to each public body, and it is recommended that, for each context, the current laws and regulations to be applied in managing these risks are identified for each context.

For this work, we highlight the Joint Normative Instruction MP/CGU No. 1/2016-IN, published in the Official Gazette of the Union on May 11, 2016, which establishes to the organs and entities of the Federal Executive Branch a series of measures to the systematization of practices related to risk management [35]. In short, bodies and entities of the Federal Executive Branch should enable the implementation, maintenance, monitoring and review of internal management controls and the management of risks that could derail the achievement of objectives of these organizations [35].

The implementation of the risk management process must occur "in a systematic, structured and timely manner, subordinated to the public interest" [35, p. 77], and risk mapping should be used to support "decision-making and strategic planning and continuous process improvement" [35, p. 77]. Finally, as suggested by IN [7], risk management should be competent in identifying the level of risk that the organization is willing to accept, i.e., its risk appetite, and reasonable certainty about the achievement of the organization´s objectives.

6. Risk management software tools

The planning and alignment between the theoretical foundation and the design of technological tools have over the years shown fundamental importance to support management initiatives at any organizational level, considering the nature of their processes and products, as well as the reality and the specificity of the most diverse performance scenarios of the institutions. In the current reality, good planning, capable of successfully conducting projects, is based on principles, techniques, skills, and tools that can increase management effectiveness, achieve better results and optimize opportunities.

In this sense, for organizations to be able to include risk management actions in their tasks, it is fundamentally necessary that control and record centralizations tools be willing to assist such efforts in order to enable proper communication, monitoring, and mastery of risks. For this purpose, Information Technology (IT) plays an important role by allowing this set of business rules to be operated in the best possible way, automating tasks and providing an interface to support risk managers in their assignments.

The risk management scenario in the public sector is still under development in Brazil, so research was carried out using the benchmarking strategy for the evaluation of 33 software tools on the market that are committed to creating processes and management strategies consistent with the reality of organizations that use them. We chose to display specific information - albeit in a synthesized form - on the module for risk management in each software examined, as well as information on procedures and strategies that aim to complement the management process initially quoted.

At first, in order to be able to know these tools, an information frame was developed containing the name of the evaluated software, its website and if there is any cost for its acquisition. All these references are systematized in Table 14 below:

Table 14 - Software tools included in the research.

Name	Website	Acquisition cost
Eramba	http://www.eramba.org	No
Open Risk	https://www.openriskmanagement.com	No
OpenSource Risk	http://www.opensourcerisk.org	No
Simple Risk	https://www.simplerisk.com	No
Ágatha	https://softwarepublico.gov.br/social/agatha	No
ACL GRC	https://www.acl.com	Yes
ACCELUS	https://www.thomsonreuters.com	Yes
Active Risk Manager	http://www.sword-activerisk.com	Yes
Adaptive GRC	https://candf.com	Yes
Aris GRC	http://www2.softwareag.com	Yes
IntelligenceBank GRC	http://www.intelligencebank.com	Yes
BPS Resolver	http://www.resolver.com	Yes
BRINQA	https://brinqa.com	Yes
BWISE	http://www.bwise.com/solutions	Yes
Convercent	https://www.convercent.com	Yes
Datalyzer FMEA	https://www.datalyzer.com/products/fmea-software	Yes
TruComply	http://anxebiz.anx.com	Yes
Enablon	https://enablon.com	Yes
IBM OpenPages GRC	https://www.ibm.com	Yes
INTERISK – Risk Intelligence	https://www.brasiliano.com.br/software-interisk	Yes
I Touch Vision Governance & Risk	https://www.itouchvision.com	Yes
MasterControl	https://www.mastercontrol.com	Yes
MetricStream	https://www.metricstream.com	Yes
Optimal Risk Management	http://www.optimalrisk.com	Yes
Oracle Fusion Governance Risk	http://www.oracle.com	Yes

ORACLE GRC	http://www.oracle.com	Yes
ProcessGene GRC	http://processgene.com	Yes
RiskGAP	http://riskgap.com	Yes
RIVO	https://rivosoftware.com	Yes
RSA Archer	https://www.rsa.com	Yes
SAP GRC	https://www.sap.com	Yes
SE Risk	https://www.softexpert.com/pt-br/produto/gestao-riscos-controles	Yes
360factor	http://www.360factors.com	Yes

Analysis of the software tools available on the market may enable, if necessary, the development of specificities and adjustments of the scenario in the Brazilian public sector. In addition, this research shows its importance in contributing to the development of the risk management software itself and in supporting communities in general, creating reflection processes for new, more efficient, effective actions aimed at improving results and transparency, so that they can complement the actions of public and private organizations, mainly when they reflect directly in life in society.

Thus, in order to summarize the main information that shapes the evaluated software, Table 15 summarizes the risk management modules and process information and/or modules that complement the process mentioned above. This list of issues - listed below - corresponds to the items in the column "Information about risk management modules" in Table 15, which deals with the software and their main features.

1. The software allows the complete management of a certain risk, from its first detection to its proper solution and/or use. 3. Does it allow management aligned with the pre-established objectives of each unit/department or the organization itself as a whole?

2. Does the software allow an in-depth analysis of the causes of a given risk by combining data mining techniques to allow managers to use these causes as a basis for decision-making?

3. Does the software allow the centralization of all information about risk management measures in a single repository of information (includes all actions that will be taken to address a risk, e.g., actions, occurrence information, and so forth.)?

4. Does the software allow the customization of evaluation metrics, evaluation functionalities, and data presentation screens according to the demand of a particular organization?

5. Does the software allow the delegation of responsibilities and/or the organization of work groups for the construction of processes, aiming at the treatment of a certain risk?

6. Does the software allow the standardization of control mechanisms, through the construction of control processes, to ensure the continuity of risk management initiatives?

7. Does the software have a significant variety of qualitative and quantitative measures to situate managers on the maturity of risk control processes? Example: KPI, KRI.

8. Does the platform use audit procedures management as a complementary feature to risk management?

9. Does it allow the integration of a communication module to risk management aiming to manage the flow of information and procedures to be disseminated throughout the organization?

10. Does it allow the use of questionnaires for situational assessment and/or to link functionality to communication management?

11. Does it allow the management of laws and regulations in force to adjust the organizational reality to market and government requirements?

12. Does it have a module for public management?

13. Does it allow the connection of multiple devices, such as cell phones, tablets, and computers?

Table 15 - Softwares evaluated and their main characteristics

	Information on risk management modules												
	1	2	3	4	5	6	7	8	9	10	11	12	13
360factor	•		•	•		•	•	•			•		
ACCELUS	•		•	•	•	•		•	•		•		
ACL GRC	•	•	•	•	•	•	•	•	•	•	•	•	
Active Risk Manager	•	•	•	•		•	•	•	•		•		•
Adaptive GRC	•	•	•	•		•	•	•	•		•		
Ágatha	•	•	•		•								
Aris GRC	•	•	•	•	•	•	•	•	•	•	•	•	
BPS Resolver	•		•	•	•			•					•
BRINQA	•	•	•	•			•				•		
BWISE	•	•	•	•		•	•	•	•		•		
Convercent	•				•				•				
Datalyzer FMEA	•	•	•	•									
Enablon	•	•		•		•	•		•	•			
Eramba	•		•					•	•		•		
ITouchVision Governance & Risk	•	•	•		•			•	•	•		•	•
IBM OpenPages GRC	•	•	•	•	•	•	•	•	•	•			•
IntelligenceBank GRC	•	•		•		•		•	•	•			
INTERISK – Inteligência em Riscos	•	•	•	•	•	•		•	•		•		
MasterControl	•		•	•		•		•	•	•			
MetricStream	•	•	•	•			•	•	•		•		
Open Risk	•		•			•		•					
OpenSource Risk	•		•	•		•							
Optial Risk Management	•	•	•	•	•			•					
Oracle Fusion Governance Risk	•	•	•	•		•		•	•		•		
ORACLE GRC	•	•	•	•	•	•		•	•		•		
ProcessGene GRC	•	•	•	•		•		•			•		
RiskGAP	•		•	•	•						•		
RIVO	•	•	•	•		•							
RSA Archer	•		•	•	•	•		•			•		
SAP GRC	•	•	•	•	•		•	•	•		•		
SE Risk	•	•	•	•	•	•		•	•		•		
Simple Risk	•	•		•	•	•		•					
TruComply	•	•	•	•		•					•		

Taking advantage of the interest of ensuring a more complete analysis of the tools evaluated, in addition to the questions to which "an attempt has been made to respond" by means of Table 15, a series of information was developed on the main functionalities of each of the softwares that are contemplated in tables 14 and 15 of this study, through access to the official sites cited and official videos of the tools, as well as trial with the software available on the World Wide Web – especially on YouTube. The analysis is outlined and documented below:

i. 360factor: this software provides an audit module that understands and tracks any audit process. It allows the view of risks in the entire organization, implementing integrable modules in all departments. It offers a module that aims to develop, manage and control agreements, contracts with suppliers and third parties, which aim, in general, to minimize costs and exposure to risk as well as to direct excellence in service. The software provides the policy and procedures management service, and the management of regulatory and control frameworks to keep the organization in line with best market practices. For more accurate control of risks and incidents, the tool allows the creation of periodic and manageable reports in order to highlight the main processes of the evaluated organization. As an advantage, the tool has an evaluation performance module, continuous feedback, goal achievement, and development coaching to improve the organization.

ii. Accelus: the Accelus tool allows the establishment and analysis of rules, regulations, and policies in the scenario in which the organization is inserted. It provides users with an action tracking mechanism that allows the organization to check compliance with current regulations. It also allows the management of a certain risk, from its initial identification to the application of corrective measures. In particular, this software guarantees the distribution of responsibilities to the employees involved in verification procedures and risk analysis and offers a complete system of notifications to inform the organization's employees about changes in legal regulations and internal changes in processes. Finally, it allows the automatic generation of reports, with periodic sending via e-mail already defined, and centralizes a library of actions and processes already executed for future consultations and adjustments.

iii. ACL GRC: allows the creation of a macro view of all the possible risks of a situation, with the possibility of categorizing them. It provides off-line activities - which are automatically synchronized in the existence of a

connection (with cloud data storage services and security) and allows you to manage incidents and possible failures through data analysis. About modeling, it facilitates the organization of one or several structures or work processes based on models/frameworks such as COBIT, ITIL, SIEM, NIST, SOC, and COSO. In addition, it offers functionality dedicated to the public sector in order to manage projects from conception to completion.

iv. Active Risk Manager: offers a contribution to risk management from an IT project to the management of risks of strategic business planning. It allows the creation of automated alerts and the presentation of data in simple dashboards, besides the update of data through any device, be it a computer, mobile phone or others. Among its strengths, the tool offers functionality that allows finding opportunities through cost savings, improvements through ideas, processes or new products. Finally, it facilitates the control of goals and the monitoring of actions making use of quantitative and qualitative measures.

v. Adaptive GRC: with this tool, one can create reports that present information about a particular project, which enables and facilitates audit procedures. The tool also allows the filtering of information, allowing the visualization of workflows and life cycles of processes related to a certain risk. The tool easily tracks its identified risks, whether they are resolved or not. Also, Adaptive GRC makes it possible to generate real-time reports to determine the characteristics of key processes. Application hosting is done in the cloud.

vi. Ágatha: the Ágatha tool allows the mapping of macro processes and processes with information from organizational units, information about the internal environment, goal setting and SWOT analysis. This solution identifies risk events, capturing their main causes, consequences, categories, and natures and, in addition, allows the planning of responses to the risks related to the causes and consequences of the risk event. All actions on the risk control plan are recorded, which corresponds to the responses to risk events, as well as validation and the decision to refuse or accept. About risk assessment processes, the tool evaluates risks and controls with inherent risks and residual risks, which are recorded in risk maps for probability and impact. Finally, the tool allows creating a repository of risk events, risk event causes, risk event consequences, risk category, risk controls, control drawings, control operations, taxonomies and glossary of terms, facilitating reuse.

vii. Aris GRC: the Aris GRC system performs the main regulatory adjustments following the specifications of the European Union, in order to ensure best practices for data storage and processing. It allows the use of a system dedicated to the detection, analysis, and correction of risks, which guarantees the ease in the control and adequacy of processes and workflows and analyzes by internal audits. The tool includes the evaluation of periodic risks and risks related to financial and information security and allows the division of responsibilities around activities to assess the main characteristics and influences of a risk. It is worth mentioning that this system has a module for public management.

viii. BPS Resolver: allows the visualization of risks from their identification to their response, analysis, and possible solution. Its structure is intended to document and store information on controls and procedures, which simplifies the conduct of internal audits. The system supports multiple devices, such as computers, mobile phones, and tablets. In advantage, the tool enables the creation of evaluation groups and coordinates the creation of polls of the discussion groups in order to categorize and classify the analyzed risks. In groups, it is possible to delegate performance roles to solve or evaluate a certain risk as well as to create reports in order to check in graphs the evolution and analysis of risks.

ix. BRINQA: proposes to be a risk management platform for the storage of business data. Its structure allows the joining of several sources of information and analysis to verify the existence of risks, which also includes the categorization and classification of the main and most obvious risks in which the organization may be inserted. The tool allows the creation and display of data models and processes that represent the relationships of risk agents, allowing a critical analysis of the categorization and order of the actions to be performed. Finally, it is possible to create and use several metrics and their presentation in customizable dashboards in different scenarios.

x. Bwise: to adapt the organizations to the regulatory frameworks in force, the Bwise solution allows the connection and analysis of the main regulatory agents as well as the use of their practices to align the company. With this tool, the monitoring and analysis of the organizational profile are guaranteed, adapting them to the most current models and market standards such as COBIT, FERC, FDA. Also, it enables the creation of metrics and the use of data panels for the

analysis of top management, the performance of the scope analysis based on the main risks and the implementation of flexible evaluations through the application of specific filters. It should be noted, finally, its ability to tailor information from applications and external data sources.

xi. Convercent: the Convercent system brings the suitability of processes and workflows as a mandatory practice for establishing compliance policies. With this, the tool offers and builds efficient and safe policies for the storage and availability of data. As a rule, it allows the preparation of reports and customizable and comprehensive analyzes, as well as the export of these reports.

xii. Datalyzer FMEA: streamlines the creation of processes and workflows appropriate to the organizational reality. Through this tool, it is possible to record and map all aspects around designing a new flow of work, risks, alternatives and centralizing them in one place for future reference. Its dashboards and metrics can track all actions related to a risk or a process, which allows the business audit to look for failures and execution problems. Finally, the tool verifies the creation and classification of users, assigning levels of execution and performance according to the process of risk management.

xiii. Enablon: aims the control and evaluation of practices and work processes used within organizations. Through its analyzes, it is possible to verify if the processes are in line with the best practices widespread in the market or if they can be aligned to them. This tool is concerned with intensifying the communication and dissemination of internal organizational issues through the generation of customizable reports applicable to the various business sectors. It is worth highlighting the possibility of creating specific tasks for a given process to reach an adequate level of regulation, and to create controls and flows in processes that are in the implementation phase or that have already been implemented.

xiv. Eramba: focuses on the internal environment to carry out risk management, allowing the setting of goals and objectives at all levels of the organization. Its process offers steps for identification of risks, the criticality of risks and impacts. Among other points, the Eramba tool allows the creation of risk policy, information flows and procedures for coping with risks. It is possible to distribute responsibilities and create a real-time database for consultation of risk management processes. This tool is also used to carry out audit procedures, from design to evaluation of results.

xv. ITouchVision Governance & Risk: offers consultations through questionnaires that can be easily structured within the application. Also, it is possible to determine the performance of each user of the application, and how this employee may act in certain scenarios where the risk exists. The solution provides tools for audit in processes, departments, and individuals, and it is possible to create a communication tool between a common user and the administrator. It allows the connection of multiple devices, such as microcomputers, mobile phones, tablets, and smartphones. Finally, its structure has a module directed to public management, presenting information mining tools and functionalities to manage and guarantee compliance with legal processes, as well as creating and exploring several channels of contact between citizens and public management.

xvi. IBM OpenPages GRC: allows the identification, analysis, and management of operational risks in a single platform, ensuring and evidencing the visualization of risks with the possibility of acting or mitigating actions on one or more identified risks. It is a quick tool to find possible hidden data and identify the main relationships about risk and, also, allows the use of scenario analysis, with the opportunity to monitor and evaluate the impacts related to the risks verified. Thus, it is possible to perform data processing through its storage and its high availability.

xvii. IntelligenceBANK GRC: offers the recording of risk and its management, which corresponds from the identification of a risk to its proper solution. In practice, it guarantees the use of customizable metrics and dashboards and allows the visualization and recording of the risks using as a source of information the most widespread compliance practices such as ISO, COBIT, and SOX. The system has received almost real-time feedback, through queries and questionnaires distributed throughout the organization, also allowing the export of files in various formats. The tool also includes a calendar for recording the activities and offers to host services in the cloud.

xviii. INTERISK – Inteligência em Riscos: has three integrated modules: (1) Enterprise Risk Management, (2) Risk-Based Audit, and (3) Business Continuity Management. This integration makes it possible to define the criteria for measuring Probability and Impact of the Risk Matrix in line with Risk Appetite, according to the strategy of the company, and allows integrating numerous risk disciplines, enabling the manager to have a holistic view and

agility during the work. Its operation aims at secure storage, transparency, and standard language.

xix. MasterControl – Risk Analysis Software Systems: allows the control of risks in a separate module, in which it is possible to follow the life cycle of a certain risk, from its initial analysis to its final resolution. This software implements a series of controls, metrics, and ways of evaluating the data in order to base and support high management decisions, as well as to enable mechanisms for control and evaluation of standardized risks. It provides periodic submission of forms and questionnaires related to best practices and makes it possible to create customizable reports addressing the specific demands of certain scenarios.

xx. MetricStream: the MetricStream solution has its infrastructure laid out in the cloud, a factor that favors data security, and centralizes them in a single data environment. It provides consumers with a robust database and the verification of best practices/work processes. In particular, the tool allows the creation of metrics and dashboards with customizable information, and the automation and control of workflows to reduce risk. Finally, it ensures the management of risks by adapting them in processes that can or cannot be studied and modified according to regulatory frameworks and good practices such as ISO and frameworks such as COBIT, ITIL, among others.

xxi. Open Risk: is an open source tool aimed at analyzing financial risks in an institution. It aims the management of risks, in order to enable their identification, criticality, and impacts. Also, one can create information flows and procedures to address risks. It allows the development of the risk policy and the distribution of responsibilities and, finally, considers the control and monitoring of risks as key to make it possible to face them.

xxii. OpenSource Risk: with a focus on risk management, the tool allows the setting of objectives at all levels of the organization. It is focused on the identification/mapping of processes and the coping/treatment of risks. It allows creating information flows and information panels to update the risk checks and for the distribution of responsibility. It is also possible to create a database and use methodologies that are consistent with the reality of each organization.

xxiii. Optial Risk Management: this tool has the ability to adapt to a wide range of organizational structures, as well as being compatible with current regulatory frameworks, such as SOX, ISO, and COSO. A solution that allows monitoring of all processes and actions through an internal audit module, enabling the export of data, creation of metrics and custom reports. Also, the roles and responsibilities of the users can be assigned, which allows the management of the actions of risk since its initial identification until the resolution of the demand. In particular, it is possible to automate the risk assessment by choosing content pillars, in addition to being able to define the periodicity of these actions and to record pertinent information about a certain risk, among them: values of impact, probability, and exposure at an inherent risk level.

xxiv. Oracle Fusion Governance Risk: through this tool, it is possible to control the execution and the activities related to a process, being possible to explore risks, points of improvement and problems in search of the best actions and more efficient processes. This solution has a wide range of reports and pre-configured evaluation metrics but allows customization. It is possible to evaluate the particular status of each activity, including corrective measures and adjustments. It enables the organization to design its action scenario, as well as specific characteristics to verify and analyze the influence of risks. An advantage, this tool has a library of policies already applied by other organizations in order to support changes and adjustments in processes and, in addition, can evaluate business models and suggest anomalies in processes or workflows. Analyzes can be carried out through multi-criteria.

xxv. Oracle GRC: this software is a risk management module that seeks to address the risks identified in the organization at all levels. It aims to consider the risks differently and to allow different forms of control and approaches for each of them. It is possible to carry out the distribution of responsibilities within the tool, as well as to establish internal and external audit procedures, a step understood as complementary to risk management. The tool also allows the adequacy of processes to the rules and regulations by which the organization is governed.

xxvi. ProcessGene GRC: acts on a wide range of risks, regulations and auditing systems to ensure the user a centralized location of information. It has customizable panels and metrics to direct the presentation of results and offers a module that aims to serve as a history to map and store as

much information as possible. The tool allows the distribution of roles of access and action, as well as the automation and analysis of workflows, as well as related activities in order to make each process efficient and effective. The application infrastructure is available in the cloud.

xxvii. RiskGAP: aims at the use of workgroups in the identification and classification of risks. It provides managers with a knowledge base in legal processes and regulations to align actions and processes more appropriate to the objectives of the organization, intensifying the action of users by allowing the analysis and verification of risks. It also allows the user to be offered a report on the best practices according to the information mining and guarantees to its users the integration of this information in different corporate systems.

xxviii. RIVO: allows a complete view of the organization in search of the main risks to which it may be subject. A tool that seeks to facilitate the standardization of risk assessments for future analyzes and to base decisions on corrective measures, allowing the use of several metrics and visualization frameworks to situate managers, directly influencing them in real-time decision-making. Its structure makes it possible to create a "library of risks" in order to catalog the main risks and allow future consultations. It also enables creating a risk map that aims to map the organization and demonstrate the sectors with the highest trends and the highest incident rates as well as the classification and categorization of risks. Its information is made available in cloud architecture.

xxix. RSA Archer: this tool allows the adjustment in the organization's policies on existing internal processes and new processes, quickly reconfiguring applications, workflows, reports, and dashboards. Its language allows the adjustment of processes to the most updated best practice guides available on the market today. It is possible to distribute and list responsibilities by managers or departments so that they act in order to minimize the effects of a certain organizational risk. It allows the use of customizable metrics and dashboards as well as additional controls against fraud, financial damage, among others.

xxx. SAP GRC: with this solution, it is possible to automate provisioning and certify that only those who have responsibilities over them make access to processes and data. This tool has an internal audit module that aims to

verify the integrity of processes, antifraud alignments, process control, among other resources. It allows the visualization of risks, classifying their influence as well as their impact on organizational processes. Moreover, it allows the management of risks, from the moment they are initially verified until corrective measures are taken to resolve the demand.

xxxi. SE Risk: establishes a risk infrastructure that produces accurate regulatory reports and enables the management and monitoring of risks in real time. As main features, this tool enables the creation of a repository of risks, controls, mitigation activities, and standard operating procedures, facilitating reuse and, also, allows identifying, capturing and managing the most critical risk processes. Risks are assessed taking into account their various dimensions and impact criteria as well as probability and workflows to ensure the correct use of the data and, to this end, allows the application of quantitative and qualitative risk assessment models, regardless of type. It also allows automatic risk assessment and provides assessments and comparisons between residual risk and inherent risk, with proactive alerts when limits are exceeded. As advantages, the tool monitors the effectiveness of mitigation activities, controls, and policies, as well as changes in risks and requirements through the management of tests, indicators, and incidents, and provides heat maps for analysis and monitoring of risks.

xxxii. Simple Risk: Simple Risk software is a module designed to perform audits, allowing the creation of audit flows and process management, which may be processed by department or branches of business. It also allows the implementation of methodologies and the adequacy of scenarios for the application of the audit stages, be it internal or external. The tool considers risks at the departmental and organizational levels and offers the possibility of creating databases for future reference.

xxxiii. TruComply: enables the identification and screening of regulations and standards that can be applied in an organization with regard to risk control, processes, and so forth. This solution allows the creation of control frameworks with metrics and customizable data panels. This attests that it can develop, document and communicate to the whole organization practices, procedures, and standards aligned with the objectives and the organizational mission. In short, the tool manages all activities related to risk, and this can be done from its identification to its due correction.

Given the systematized analysis and in line with the aspects already mentioned in this study, it is possible to observe that, in general, the software tools are committed to carrying out and supporting risk management processes and initiatives. All the tools presented showed the ability to perform actions and tasks at different stages of risk management, from the moment of identification of risks, through its analysis, categorization, control, and monitoring, and response stages until arriving at action plans. In a way, it is possible to infer many similarities among the featured tools, acting comprehensively in the various situations that correlate the management of institutional risks.

As can be seen from the data presented in Table 15, the approach used by most risk management applications differs only in the extent to which risk analysis and risk management can occur. For some applications, such as Accelus, SE Risk, RIVO, among others, the organization is considered as a single entity, with specific management objectives that are aligned throughout the company. In others - SAP GRC, ProcessGene GRC, 360factor, among others - we choose to observe the organizational levels and departments respecting specific objectives for the realization/implementation of this initiative.

It is also observed the existence of complementary procedures to the process of risk management. As an example, we mention:

- the use of evaluation metrics to locate and present relevant data in the form of reports or presentation screens - Oracle Fusion Governance Risk, TruComply, RSA Archer, Optimal Risk Management, MetricStream, among others;

- the centralization of information, which consists of an impactful property in software development or initiatives related to risk management - Active Risk Manager, BRINQA, Eramba, I Touch Vision Governance & Risk, among others; and

- the ease of data mining to find relevant information and knowledge - ORACLE GRC, Simple Risk, ACL GRL, BWISE, among others.

Later, it was possible to notice that, in almost all applications, there is at least one specific module for communication or process management that allows the flow of information indispensable for the success of management actions, such as targeted notifications, news delivery through emails, daily reports,

among others. Examples include the Accelus, Adaptive GRC, BPS Resolver, Convercent, Enablon, MasterControl - Risk Analysis Software Systems, Optimal Risk Management, Oracle Fusion Governance Risk and other tools.

Ensuring the availability of organizational information to managers and employees included in any management initiative is of vital importance for the correct alignment of actions towards a control objective. Thus, functionalities such as questionnaires and other evaluations aim to guarantee the involvement of all and feedback from various organizational levels. They are, also, elements that guarantee the multidisciplinarity for the management and its effective adaptation to specific realities and scenarios. In this sense, the software that stood out the most were the I Touch Vision Governance & Risk, IntelligenceBANK GRC and MasterControl - Risk Analysis Software Systems.

Another element that stands out in the presented software tools is the use of specific modules for audits, which are configured as methodical processes of verification and adequacy of procedures. This element is of utmost importance in estimating the success in the employability of management initiatives, since it allows critically evaluating a scenario in search of procedures that impel continuous improvements, the suitability of conduct, among other factors that prevail for the continuity of processes. The Optimal Risk Management, ProcessGene GRC, SAP GRC, 360factor, Adaptive GRC, and Aris GRC tools are the best examples of this configuration.

Finally, it is possible to observe the massive use of extra components to carry out the verification of current regulations, as well as legislative requirements that must be taken into account during the activities of an organization. Enablon, ProcessGene GRC, and SE Risk are tools that have demonstrated this concern. It should be noted, however, that for the applicability of these processes of legislative follow-up and regulations, the module aimed at this activity must be adequately studied and planned so that it adapts to the different realities that may influence the processes and products of organizations.

Finally, for anyone interested in the tools described, it is recommended a deeper analysis more appropriate to its applicability in organizational practices and objectives. In fact, there was no pretension to establish the best, but to make full disclosure of the most common tools available in

the market, with their characteristics and functionalities. Therefore, it is understood the need of each institution to recognize, according to its context and interest, which of these tools should better serve its purpose. As a suggestion, if the organizational purpose is the automation of the risk management process - for private or public institutions – we see greater viability in the software SE Risk, INTERISK - Risk Intelligence, Active Risk Manager, Adaptive GRC and IBM OpenPages GRC.

7. Investigating real cases of risk management in the public sector: the cases of UNIFAL-MG and CEFET/RJ

7.1. Context and motivation

Carrying out case studies, when it comes to some real-life context of people, has proven its value to empirical-scientific investigations to understand social phenomena holistically. The analysis of these phenomena, observed in their natural environment, provides researchers with a set of prevailing variables of true and concrete facts and ensures the reach of conclusions relevant to those conducting research and to other interested parties.

In order to corroborate the development of research in risk management, to confront and confirm the coherence of the techniques and methods developed during the course of the ForRisco Project with the practical reality of the organizations, it was decided to carry out case studies in two Federal Institutions of Higher Education (IFES), autarchies linked to the Brazilian Ministry of Education (MEC). They are: (1) The Federal University of Alfenas – Minas Gerais (UNIFAL-MG) and (2) the Celso Suckow da Fonseca Federal Center for Technological Education - Rio de Janeiro (CEFET/RJ).

7.2. Objects of research

The following are the two IFES evaluated with regard to their current risk management processes.

7.2.1 The Federal University of Alfenas – UNIFAL-MG/BRAZIL

UNIFAL-MG, originally Escola de Farmácia e Odontologia de Alfenas – EFOA (Alfenas School of Pharmacy and Dentistry), was founded in April 1914 and 2005 was transformed into a university. Besides the headquarters, in the city of Alfenas-MG, it was expanded using two campuses that are more advanced: the Varginha - MG campus and the Poços de Caldas - MG campus. UNIFAL-MG has been responsible for

training several generations of professionals through its undergraduate and postgraduate courses, consolidating extension activities, occupying a prominent position in providing services to the local and regional community and for the expressive growth of its scientific and technological production. As a mission, the institution aims to promote the full education of the human being, generating, systematizing and disseminating knowledge, committing itself to excellence in teaching, research and extension, based on the principles of critical reflection, ethics, freedom of expression, solidarity, justice, social inclusion, democracy, innovation and sustainability.

7.2.2. The Celso Suckow da Fonseca Federal Center for Technological Education – CEFET/RJ/BRAZIL

CEFET/RJ has its origin in 1917 as the Escola Normal de Artes e Ofícios Wenceslau Braz (Normal School of Arts and Crafts Wenceslau Braz). Currently, it is a federal educational institution that sees itself as a public space of human, scientific and technological training, offering technical courses integrated to secondary, post-secondary, technological, undergraduate, and lato sensu and stricto sensu post-graduate courses (masters and doctorate), in the face-to-face and distance modalities. Since 2010, and from the Professional Education Expansion Program (PROEP), the institution has the Maracanã campus and seven other campuses throughout the State of Rio de Janeiro, which are Angra dos Reis, Itaguaí, Maria da Graça, Nova Friburgo, Nova Iguaçu, Petrópolis and Valença. CEFET/RJ operates in the teaching, research and extension triad and aims to contribute to the training of well-prepared professionals for the economic and social development of mesoregions in the State of Rio de Janeiro.

7.3. Research procedures

This research is defined by the qualitative research method, with deep inferences in case studies. Qualitative research considers that there is a dynamic, contextual and temporal relationship between the research and the object of study, so it demands too much interpretation of the phenomena in light of context and facts [24]. In qualitative research, the researcher participates, understands and interprets events consciously and coherently, with precision and objectivity, and must guarantee the logical argumentation of ideas.

In addition to qualitative research, a case study is a scientific basis that supports the collection and analysis of the data [25]. In 1994, researcher Creswell [26, p. 12] emphasized a definition very close to what is accepted today, understanding case study as the process in which "the researcher explores a simple entity or phenomenon limited by time and activity, and collects information in detail using a variety of procedures".

In this logic, a case study should be considered as a material design in which several data collection methods or techniques are used, such as observation, interviewing and document analysis [25]. Promptly, it is proposed that a case study should be understood as an empirical investigation that examines a contemporary phenomenon in its context, especially when the boundaries between phenomenon and context are not clearly defined [27].

Based on the definitions presented, it is important to understand that a case study presents essential characteristics that surround it at a strategic level and that were taken into account for the development of this content, namely:

1. the unitary nature of the phenomenon investigated, i.e., the risk management in IFES;

2. investigation of a contemporary phenomenon: although considered as historical conjunctions, the risk management processes of these institutions occur simultaneously with the research;

3. the use of multiple data collection procedures: risk management is being examined taking into account different means of data collection, such as interview, participant observation, and document analysis;

4. being a study of depth: the interview applied to IFES is semi-structured, which allows for a greater depth of the researched topics and, consequently, an increase in the level of interiority in organizations.

From the point of view of the operational level, or rather, considering a proposal of content and sequence for the conduct of the case study, an argument was adapted according to the studies of Cauchick Miguel [28, p. 221] that provides the framework for conducting the case study as detailed in Figure 15 below:

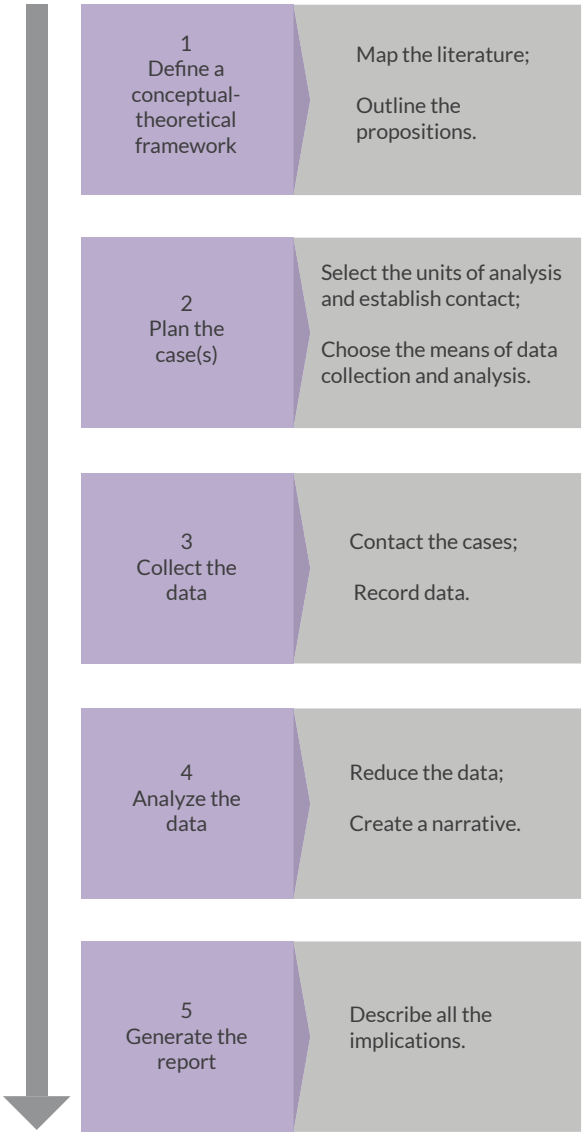


Figure 15 - Stages for conducting the case study
Source: Cauchick Miguel (2007, page 221), with adaptations

At first, a mapping of relevant literature on risk management in public and private organizations was carried out, as well as the methodologies and tools for the implementation of this management. All this survey is presented in the course of the book. Given the study on risk management, it was necessary to propose a case study in institutions that present their processes already structured, delimiting the propositions of this chapter. To that end, two higher education institutions in Brazil have been chosen, which are developing their processes of formulation, implementation, monitoring and control of risks, which is in other words, risk management. The selection of UNIFAL-MG and CEFET/RJ to compose the research took place through the participation of these institutions in the National Forum of Pro-Rectors on Planning and Administration, an event in which both publicized their projects for risk management.

The methods of data collection selected were interview with a member responsible or co-responsible for the implementation of the institutional risk management; participant observation, through the evaluation of presentations in congresses of their respective management processes, of both organizations; and, finally, the provision of documents relating to risk management, such as the Risk Management Policy. The institutions were then contacted, and the commitments of each one was adjusted so that they could be integrated into the study. All data obtained through interviews, presentations, and documents were collected within a maximum period of 30 days. For the analysis, we chose the descriptive narrative of the facts and the implications encountered during the research process.

The research carried out at UNIFAL-MG was supported by the Pro-Rector's Office for Planning, Budget and Institutional Development (Proplan), in the position of Adjunct Pro-Rector who works directly with the Institutional Development Coordination (CDI). The Pro-rector supported the application of the interview questionnaire, which was completed in full on March 6, 7 and 8, 2018 via Skype. The semi-structured interview has 25 questions - APPENDIX III - about the different stages to implement risk management in an institution. The stages are: (1) policy definition [four questions]; (2) establishment of the external context [three questions]; (3) definition of risk management strategies [four questions]; (4) establishment of the internal context [three questions]; (5) effective implementation of risk management in the activities [four questions]; (6) reassessment of policy [two questions]; and (7) maturity assessment of risk management in the organization [five questions].

Documentation on its risk management processes was also made available by UNIFAL-MG. The university offered the following documents: the Risk Management Policy, effective on May 4, 2017, and used by the current management; the Draft Risk Management Plan of UNIFAL-MG, which is defined as a practical plan for the development of risk management procedures and actions in 2018; and a prior presentation made by the coordinators of the university risk management at FORPLAD. This Forum was held on March 14, 15 and 16, 2018, in the city of Natal, Rio Grande do Norte, and where the procedures and progress of UNIFAL-MG's risk management were presented in detail. The dashboard, titled "ForRisco System Development Project", developed by the university and accompanied by the researchers, was also an important object of this study.

Prior to the interview at CEFET/RJ, a preliminary meeting was held between the junior planning and management analyst - a member of the ForRisco Project - and the head of the Institutional Development Department (DEDIN) of the institution CEFET/RJ, on the morning of February 23, 2018 in the city of Brasília/DF. This meeting had the purpose of enabling us to know a little more about the risk management of CEFET/RJ and formalize the invitation to carry out the case study, which was promptly accepted. The application of the interview questionnaire happened on April 11, 12 and 13, 2018 via Skype. It should be noted that the same questions applied to UNIFAL-MG were also applied to CEFET/RJ, so the questionnaire follows the same implementation structure of risk management presented previously.

In addition to the interview, the researchers had access to the Risk Management Policy of CEFET/RJ, to a presentation developed by the Board of Strategic Management (DIGES) of this institution and to two worksheets detailing the mapping steps (identified critical processes, definition of risks, probability analysis and risk impacts) and management of risk processes. It is noteworthy that CEFET/RJ also made a presentation at the National Forum of Pro-Rectors on Planning and Administration, in Natal, Rio Grande do Norte, on March 14, 15 and 16, 2018, entitled "Risk Management: the experience of CEFET/RJ ", and that served as a basis for the realization of the case study.

Therefore, the emphasis is placed on the search for totality and depth in the studied research objects, and in this case, it intends to understand the reality of the processes of formulation, implementation and execution of risk management in public educational institutions. It is important to understand

the case studies carried out, aiming the understanding of different techniques for risk management. It is also worth noting the standardization of the data collection procedures carried out in both institutions, through document analysis, interviews and participant observation. Finally, the analysis of the cases of risk management at UNIFAL-MG and CEFET/RJ is presented below, and then a comparison between the institutions and a proposal for the implementation of risk management by the ForRisco methodology is presented below.

7.4. Case Study: The Federal University of Alfenas – UNIFAL-MG/BRAZIL

The Risk Management Policy of UNIFAL-MG is recent, but from the outset, it was established as a reference within this institution. The development of a Risk Management Policy at UNIFAL-MG was thought based on what is prescribed in article 17 of Joint Normative Instruction MPOG/CGU No. 1, dated May 10, 2016. The university, in establishing compliance with Ordinance no. 888, art. 3rd paragraph VII, determines its policy on July 7, 2017.

The development of the Risk Management Policy of UNIFAL-MG took place initially through the performance of the Pro-Rector of Planning, Budget and Institutional Development. In this sense, Proplan is the advisory body of the Rectory responsible for preparing the institution's budget proposals, for institutional information, for technical support to all organs of UNIFAL-MG in the preparation of plans, projects, and proposals for agreements, as well as sustainable administrative modernization initiatives.

Currently, Proplan is composed of: pro-rector; adjunct pro-rector; coordinators (General Coordination (CGE); Institutional Development Coordination (CDI); Budget Coordination (COR); Projects and Works Coordination (CPO)); managers of managements (Management of Information and Institutional Marketing, Management of Strategic Planning, Management of Environment and Sustainable Development, Management of Budget Planning, Management of Execution and Budget Control, Architecture Management, Engineering Management); and other servants.

After being drafted, the policy was presented to the Governance, Risk and Control Committee (CGRC), an internal entity of UNIFAL-MG responsible for analyzing, approving, treating and monitoring the institution's risks. CGRC has its composition established by the presence of the rector of UNIFAL-

MG, in the figure of president; the Pro-rector of Administration and Finance; Pro-Rector of Planning, Budget and Institutional Development; Pro-Rector of Graduation; Pro-Rector of Research and Post-Graduation; Pro-rector of Extension; Pro-Rector of Community and Student Affairs; Pro-Rector of People Management; and the Coordinator of Institutional Development, as secretary.

After approval of the policy by the Committee, it becomes the main promoter of the practices and principles outlined in the document, as well as providing and institutionalizing appropriate structures for governance, risk management, and internal controls. Thus, it is worth mentioning that the general objective of the policy is to provide elements for UNIFAL-MG to institute risk management and promote the identification, evaluation, treatment strategy and monitoring of the risks to which it is subject.

In this sense, the institution understands that risk management is designed to ensure that managers have access to information about the risks to which the organization is exposed, improving the decision-making process and increasing the possibility of achieving objectives. The Governance, Risk and Control Committee is aimed at preparing, approving and implementing the Risk Management Policy of UNIFAL-MG, which will be reviewed annually, beginning a new cycle of preparation, approval, and implementation.

In addition, for the implementation of the Risk Management Policy, UNIFAL-MG takes into account, in principle, the Institutional Development Plan (IDP) as well as the objectives, targets, and indicators outlined in that document. Subsequently, the organizational strategic objectives (macro processes) of the institution, that is, of the units that form it, are retaken: Rectory, Vice-Rectory, Pro-Rectories and Board of Directors. Then, the managerial and support processes, and the sub-processes in two organizational levels are detailed: Pro-Rectories and Board of Directors. It is from this mapping of macro processes, processes, and sub-processes that one understands to what risks each organizational unit may be subject.

Therefore, the main actions to be performed are mapped, in their different levels of responsibility. The mapping considers the following types of risk, as shown in Table 16, below:

Table 16 - Risk typology

Risk typology	Interpretation
Operational	Events that may compromise the activities of the organ or institution, usually associated with failures, deficiencies or inadequacies of internal processes, people, infrastructure and systems.
Legal	Events derived from legislative or normative changes that may compromise the activities of the body or institution.
Financial/Budgetary	Events that may compromise the capacity of the body or institution to have the necessary budgetary and financial resources to carry out its activities or events that may jeopardize its own budget execution, such as delays in the bidding schedule.
Image/Reputation of the Organ or Institution	Events that may compromise the trust of society (or partners, customers or suppliers) in relation to the capacity of the body or institution to fulfill its institutional mission.
Other Risks	Other risks, such as cultural, technological, management, human resources risks, among others that may jeopardize the progress of the institution's activities.

It is worth noting that the process of identification and mapping guarantees the understanding of which procedures might pose risks to a specific organizational unit since the units are also responsible for the identification step. The risks identified should be attributed to the so-called "risk owner", who is responsible for ensuring that the risk is monitored, managed and adequately handled. It is also worth mentioning that the analysis should cover all the activities considered relevant for the achievement of the institutional objectives of UNIFAL-MG.

We notice, therefore, that responsibilities are not concentrated only on the members of the CGRC, but on all those who are part of the organization. This was the way found by UNIFAL-MG to ensure full execution of the processes of monitoring and control of risks: accountability. Table 17 summarizes the actors and their responsibilities towards risks.

Table 17 - Actors and description of responsibilities

Actor	Responsibility
Committee	Prepare the Risk Management Plan. Carry out the management of the Risk Management Plan. Determine mitigating measures, monitor actions and communicate situations.
Rector	Ensure the continuity and improvement of the Risk Management Policy.
Pro-Rectors	Monitor, in the respective scope, the mapped risks. Communicate about situations involving risk and apply necessary mitigation measures.
Coordinators	Monitor, in the respective scope, the mapped risks. Communicate about situations involving risk and apply necessary mitigation measures.
Servants	Monitor, in the respective scope, the mapped risks. Communicate about situations involving risk and apply necessary mitigation measures.

In order to ensure excellence in the development of the Risk Management Plan, CGU's auditors, who, from June 27 to 29, 2017, provided a training course on risk management and internal controls in the public sector, supported UNIFAL-MG. The course was offered to all managers, pro-rectors, institute leaders, campus directors, and technicians, in order to ensure the same understanding of risk management at the institution. It is up to the pro-rectors to disseminate risk management within each unit for which they are responsible. In addition, the CDI of UNIFAL-MG, ensuring cohesion in understanding the subject, intensified CGU course.

Thus, in general, UNIFAL-MG established the structure of its risk management process in five stages: (1) identification of risks; (2) risk analysis; (3) planning; (4) tracking and monitoring; and (5) control of risks. Figure 16 shows this structure:

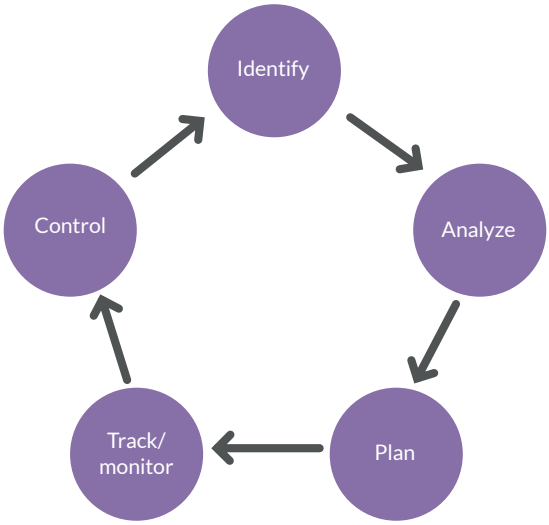


Figure 16 - Cycle of risk management at UNIFAL-MG

For the identification process, it is suggested that the mapping of the processes of the units be carried out in loco, i.e., by the servants involved, through the collection of historical data, information, interviews, and meetings with leaders and technicians in their activities. The identification of processes and risks is inherent to each area or unit and can occur through two contexts: external and internal.

In the case of establishing the external context, UNIFAL-MG has the support of the Legal Department. It is through this legitimate unity that the university responds to major external changes, which notably refer to changes in legislation. Regarding the internal context, each unit should take into account its abilities, strategies, activities developed and internal regiment or policy of the institution. In addition to the units, which are responsible for the identification and monitoring of processes, it is the responsibility of the CGRC to ensure continuous action on identified risks.

With regard to the tools used to establish the external and internal factors that may affect the institution, the units are oriented to use SWOT Analysis, brainstorming, Ishikawa Diagram, Bow-Tie, and risk identification form. At first, the SWOT Analysis is a strategic management tool used for the generation of environmental diagnoses, which aims to increase the positive aspects of the organization and eliminate negative aspects. SWOT Analysis allows learning

from the present and reflecting on what can be done from it through the global assessment of strengths and weaknesses (internal environment) and opportunities and threats (external environment).

Brainstorming is a methodology that proposes to stimulate participation and integration of the participants openly and spontaneously, aiming to stimulate creativity in order to solve a problem. Meanwhile, the Ishikawa Diagram maintains its focus as a facilitator in the risk identification process. The Ishikawa methodology makes it possible to identify and analyze the causes of risks and to develop actions to mitigate, accept or even share the risk according to the risk tolerance level of the institution.

To complement, the Bow-Tie technique allows visualizing the relationship between the causes and consequences of the risk evidenced, to minimize possible failures during the process. This technique establishes, respectively, the risk, the causes and their consequences, and the control measures related to each cause and each consequence. Finally, UNIFAL-MG uses and recommends a risk identification form (Figure 18), which establishes the risk concept described as follows: the risk; the causes of risk; the likelihood of risk; the impacts of the risk; and the owner of the risk.

It is worth mentioning that all the techniques and methodologies mentioned are part of the training conducted by the CGU (external training) and the internal training carried out by the Institutional Development Coordination (CDI). In addition, CDI monitors risk management in institutional units using completed forms, as exemplified in Figure 17. Direct monitoring is also carried out with the Pro-Rectories and, at the end of each Risk Management Plan proposed by the developer unit, the plan should be evaluated, validated and approved by the CGRC.

MACROPROCESSO/PROCESS/SUBPROCESS										
Date										
Sector										
No	Event	Risk	Cause	Degree of Risk	(*) Controls/ Existing Procedure	Improvement required	Deadline	Person Responsible	Status	Observation
1										
* Implement/develop actions that act on the causes of risks. Justify why a certain measure should be adopted.										

Figure 17 - Form for monitoring units and risks

The risk analysis and assessment stage aim to standardize and clarify the risks identified. For this purpose, a Form for Risk Identification was developed - as previously mentioned. The form is based on the qualitative methodology and has the purpose of facilitating the tabulation of information. At the end of each descriptive form, it will be possible to ascertain the likelihood of the occurrence of the risk and the level of impact of that risk concerning the risk planning and classification stage. Figure 18 represents the form.

MACROPROCESSO/PROCESS/SUBPROCESS									
Date									
Sector									
No	Event	Risk	Cause of Risk	Impact of Risk	Risk Owner	Degree of Risk	Probability of risk	Mitigating measures	People Responsible
1									

Figure 18 - Risk Identification Form

When it comes to planning and classifying risks, probability and impact interfere with these actions. UNIFAL-MG, through its management policy, proposes the following interpretation, as shown in Table 18.

Table 18 - Probability and impact

Probability	Low	Medium	High
Descriptors	Likely to occur, likely to mitigate the already planned strategies.	Likely to occur, likely to mitigate with additional costs and actions.	High possibility to occur; difficulties in mitigating even with additional resources and actions.
Impact	**Low**	**Medium**	**High**
Descriptors	Losses (although reduced) to goals, requires new projects or actions.	Loss of management capacity; additional demands on time and resources.	Serious damage to the objectives and fulfillment of the institutional mission.

Thus, risks are thought and monitored according to the results of the classification stage. In order to evaluate the probability of occurrence of risks and their impacts on the unit/institution, a Risk Classification Matrix is proposed, as shown in Table 19.

Quadro 19 – Risk Classification Matrix

Probability		Low	Medium	High
Impact	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	High

A partir desta matriz, a UNIFAL-MG define os riscos que serão constantemente monitBased on this matrix, UNIFAL-MG defines the risks that will be constantly monitored and the strategies to treat each one of them. It should be noted that, in general, risks are classified as follows:

(1) Low risk - tolerable risk, no immediate action is necessary, but the risk should be monitored; the risks in this class should be treated only if the constraints (such as cost and treatment effort) are not significant;

(2) Medium risk - attention situation; if possible, the risk should be addressed in the medium term; the risk should be monitored frequently; restrictions (such as cost and treatment effort) can be considered to prioritize the treatment of risks in this class;

(3) High risk - intolerable risk, the situation of great concern; actions need to be taken quickly, and results need to be monitored frequently to assess whether the situation has changed with actions. Risks should be treated regardless of constraints (such as cost and treatment effort).

Ahead, the monitoring phase will take place over one year from the date of approval of the Risk Management Plan. Each responsible person should follow the behavior of the scoring risks, suggesting interventions when necessary. For the materialization of this process, the university object of the study proposes the use of the tool 5W2H, previously established by the 11th IN nº 1, of 2016 [31], according to Table 20 below:

Table 20 - Tool 5W2H

Tool 5W2H	
Risk	Definition
What	What will be done? (Action)
Why	Why will it be done?
Who	Name of the person involved
When	Period/Term
Where	Place
How	Procedure/Way
How Much	Financial Value/Time

Free translation of the authors (2018)

Monitoring is an ongoing process, and it should be carried out in the day-to-day operations of the organization. It includes management and other supervisory activities as well as other actions that the servants perform in fulfilling their responsibilities. Finally, the control stage should occur through participation among Pro-Rectories, Support Units, Legal Unit, CDI and CGRC. It is also through these different units that all forms of communication and/or disclosure of new policies and procedures in the verified institution are achieved.

Finally, UNIFAL-MG has developed an organizational chart structure that represents and summarizes its entire process of risk management. Figure 19 depicts the risk management process from the outset, with the creation of CGRC. It involves the training of public servants through training provided by CGU (external training) and by CDI (internal training) and also establishes the scenario between process monitoring, risk identification, management tool choices and classification of risks with regard to probability and impacts. It is worth adding that in the stages of monitoring and controlling risks UNIFAL-MG understands the possibilities between accepting the risk, mitigating it or even sharing it.

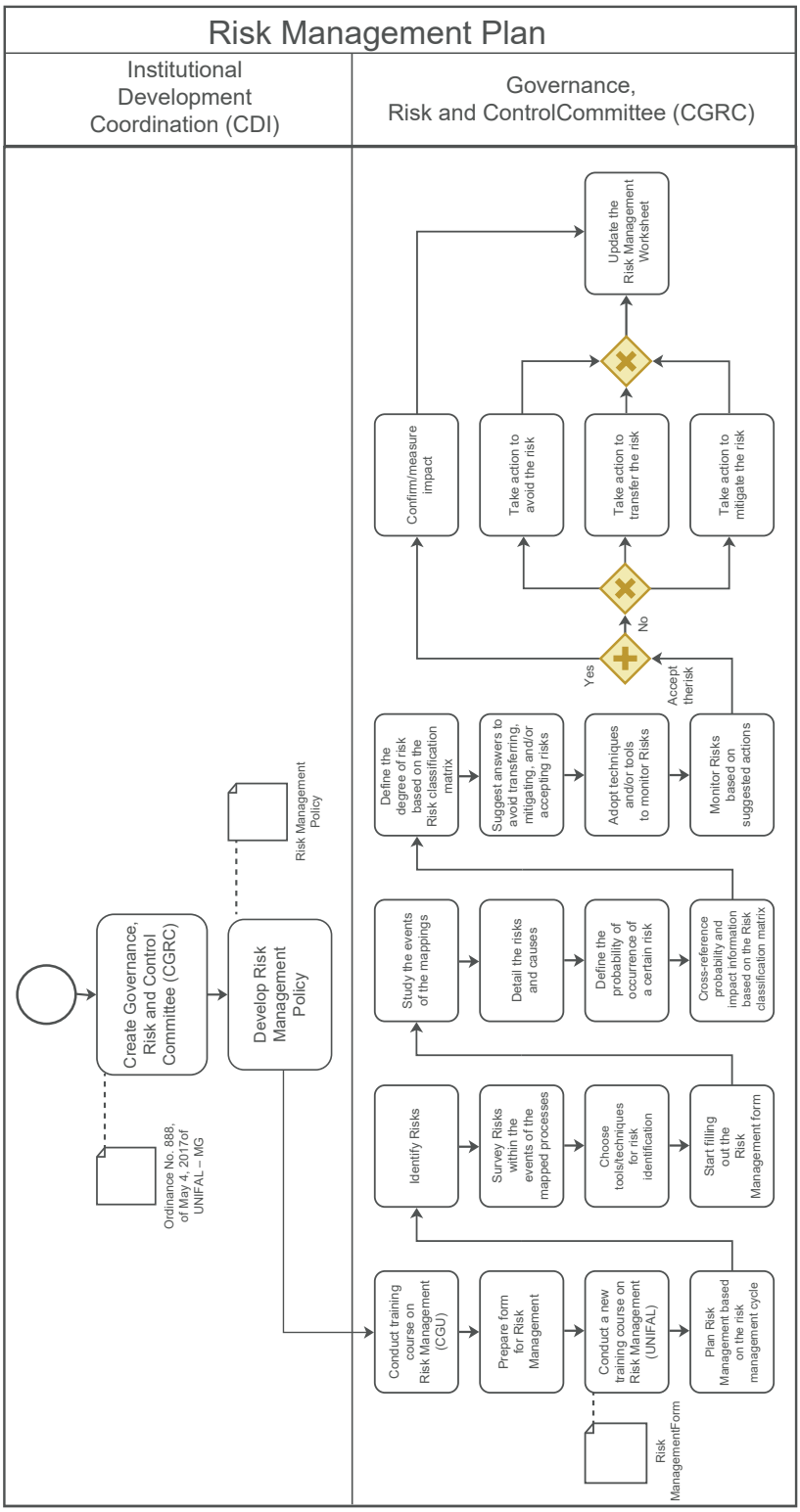


Figure 19 - Structure of the Risk Management Plan of UNIFAL-MG

It is important to state that UNIFAL-MG has not yet defined a process for reassessing the Risk Management Policy, which is justified by the fact that its policy is still recent and in the process of being implemented. Thus, considering that the Risk Management Policy of UNIFAL- MG still identifies itself with status "under implementation"; it is also not possible to assess the maturity of this policy. However, this infers that the institution's risk management provides for procedures, rules, and routines that enable its managers to evaluate the effectiveness of their actions and their execution plans. Finally, UNIFAL-MG's risk management is an updated process, structured and developed according to the needs of preventive responses expected from a risk management process, especially since it is a public educational institution.

7.5. Case Study: the Celso Suckow da Fonseca Federal Center for Technological Education - CEFET/RJ/BRASIL

Under Resolution No. 44/2017, the Risk Management Policy of this institution was approved on December 8, 2017, by the Governance, Risk and Control Committee, and promulgated by the Board of Directors (CODIR) of the Celso Suckow da Fonseca Federal Center for Technological Education. The policy was elaborated by the Department of Institutional Development, under the coordination of the Board of Strategic Management, considering the Joint Normative Instruction [31] MP/CGU nº 01/2016, which is in force in accordance with the Standard ABNT NBR ISO 31000:2018 and establishes the principles and the guidelines for risk management, internal controls and related actions.

Still, at an early stage of implementation, the CEFET/RJ policy aims to develop and ensure the existence of a structured risk management process that guarantees the adoption of best practices to its processes, technologies, and people. It is worth noting, among other things, that this institution has the premise of aligning its risk management with the current PDI strategies, taking into account the systematization and integration of organizational processes, and the commitment and decision making by managers. They are, therefore, objectives of the Risk Management Policy of CEFET/RJ:

I. establish concepts, guidelines, attributions and responsibilities of the risk management implementation process;

II. guide the identification, evaluation, monitoring, and reporting of institutional risks;

III. increase the likelihood of reaching organizational objectives by reducing risks to acceptable levels; and

IV. add value to the organization by improving decision-making processes.

CEFET/RJ understands that the Risk Management Policy is its responsibility and, therefore, the implementation of this policy must be exercised in a shared way by managers, servants, systemic units, councils, sectorial committees, and commissions. However, for policy formulation purposes, the institution specifically has the Department of Institutional Development, and the Governance, Risk and Control Committee. The latter composed of the Directorate General (DIREG), represented by its director, and the other systemic directors of the following boards: Board of Education (DIREN), Board of Research and Graduate Studies (DIPPG), Board of Extension (DIREX), Board of Management and Planning (DIRAP) and Board of Strategic Management (DIGES).

For the formulation and implementation of the Risk Management Policy, the educational institution prioritized, in principle, the qualification of the teams in all its units and sectors. For this training, a risk management course was conducted in partnership with the Federal Institute of Tocantins (IFTO), as well as benchmarking strategies to understand risk management in that institution deeply. Given the knowledge acquired during the training phase, the institution's policy was elaborated by DEDIN, a department of the Board of Strategic Management of CEFET/RJ. Once formulated, the policy goes through a system of approval and validation composed of three stages: (1) validation by the organization's internal audit department; (2) approval by the Governance, Risks and Control Committee; and (3) approval of the policy by the Board of Directors.

The next stage concerns the implementation of the Risk Management Policy. To do so, the first stage involves the disclosure of the policy through the institution's website and the holding of workshops on risk management by DEDIN on all campuses. It should be noted that CEFET/RJ is a multi-campus institution, which means that its structure is decentralized in eight campuses in the State of Rio de Janeiro. They are the Maracanã Campus – head office

- and the other campuses of Angra dos Reis, Itaguaí, Maria da Graça, Nova Friburgo, Nova Iguaçu, Petrópolis, and Valença.

Given the disclosure, an ancillary worksheet was developed to define risk management in each institutional unit. Also, the Institutional Development Committee was created, responsible for preparing the Worksheet Fill-in Manual and conducting a workshop with the different sectors and institutional units to ensure the correct performance of the action. It is also the Committee´s responsibility to study the weaknesses of the completed worksheets in each unit and approve the worksheet. After approval by the Committee, the worksheets are sent for approval by the CGRC, and then the treatment and control of identified risks is started.

In general, it is possible to establish that the main duties, with regard to the formulation and implementation of the Risk Management Policy of CEFET/RJ, are the responsibility of the Governance, Risk and Control Committee. They are: a) institutionalize appropriate risk management structures; b) promote the continuous development of public agents and the adoption of good risk management practices; c) ensure adherence to regulations, laws, codes, norms, and standards; d) approve guidelines, methodologies and mechanisms to communicate and institutionalize risk management; and, e) to issue recommendations for the improvement of risk management.

However, in this process of formulating and implementing the policy, there are still two other key actors:

- the maximum director of CEFET/RJ, who is primarily responsible for establishing the organization's strategy and also for sponsoring the implementation of risk management; and

- the Institutional Development Committee, which became the main proposer of the necessary updates to the Risk Management Policy of CEFET/RJ and who performs periodic critical analyses of the risk management process through DIGES, submitting it to Internal Audit (AUDIN), to the Governance, Risk and Control Committee (CGRC) and to the Board of Directors (CODIR).

The establishment of the external context analysis comes from the control carried out by the Governance, Risks and Control Committee, which, as previously mentioned, aims to ensure adherence to regulations, laws,

codes, norms, and standards. To identify opportunities and threats, the main methodology described by the institution was the brainstorming technique, performed by the servants that act directly in the processes and recorded in the ancillary risk management worksheet. The purpose of the worksheet is to detect, monitor, and address all organizational risks identified.

The brainstorming methodology is understood by the institution as a group tool for exposing a problem in order to get ideas and reflections to solve it. It is also an important tool for defining organizational risk management strategies. In addition to this, the processes of risk mapping, risk simulation, and vulnerability identification are performed. Only after the development of these activities will it be possible to structure the action plan, that is, the strategic actions.

Therefore, process mapping is an activity occurring in each of the units, coordination boards, departments, divisions and sectors, and not exclusively performed by a single team. The mapping begins exactly with the identification of processes performed in an area, followed by a prioritization stage of these processes to detect the most important or critical. The entire team undergoes training in Bizagi, a tool used for modeling, monitoring and controlling the identified processes.

Given the training, the servants are able to structure the process mapping, which will need to be validated. Validation is carried out by the sector head responsible for the process and, subsequently, the mapped processes are sent to DEDIN, which, after the analysis, suggests a team recycling in the Bizagi tool or discloses the processes mapped to the institutional departments. This process is described in Figure 20 below:

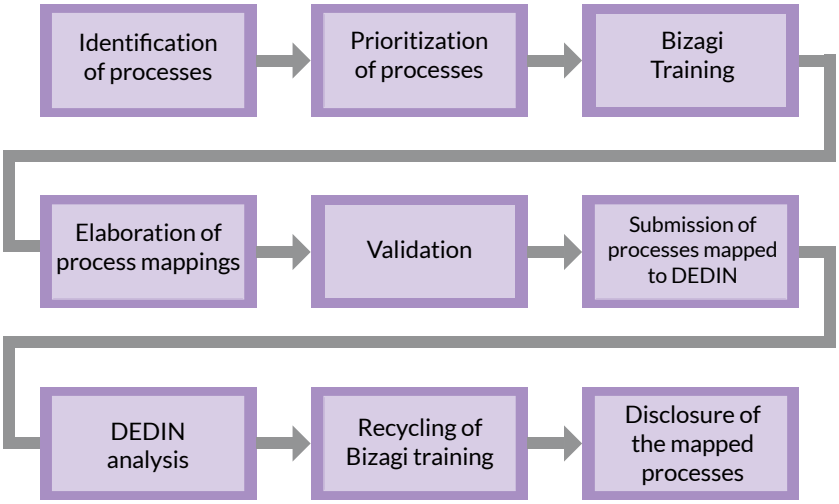


Figure 20 - Implementation of the mapping process in CEFET/RJ
Source: CEFET/RJ

In the review stage of the mapping forwarded, all those understood as "non-processes", that is, that were only activities, were removed from the risk management analysis. CEFET/RJ understands vulnerabilities as the root cause (critical node) or the causes that increase the likelihood of the risk happening. Notably, risks are not addressed directly, but the vulnerabilities (the causes and critical nodes) that can lead to their occurrence are addressed. The final stage corresponds to a plan of action that is triggered in the individual treatment by the area of each critical node.

For the realization of the internal context, other methodologies are used. In addition to the technique of brainstorming and process mapping, the methodology of the five whys and the 5W2H are applied. The first is a technique for finding the root cause of a defect or problem. A technique of analysis that starts from the premise that, after asking five times why a problem is happening, always related to the previous cause, the root cause of the problem would be determined. The second, 5W2H, seen in the previous case study, is intended to understand who, when, where and how an action will be performed, and how much it costs to perform this action.

It is important to highlight the use of the ancillary worksheet during the entire process mapping and risk management. In fact, the spreadsheet has

been the basis of the identification of processes from the beginning. All macro processes are identified and plotted in the worksheet, defining their sector of activity, that is, the area in which the process fits, which can be administration, teaching, research, extension or management. Subsequently, it is understood which processes are critical, and only these processes will be deepened in their root cause (vulnerabilities). To classify the risks, four groups of processes are proposed: operational, financial, legal or image of the institution - in which it will be necessary to determine to which of these groups the process belongs. Thus, the next stage is the definition of risks, in which one can ask: What is the risk in that process?

Continuously, CEFET/RJ analyzes the risks from two perspectives: (1) risk probability analysis and (2) risk impact analysis. In the first perspective, seven factors are taken into account, as detailed in Table 21 below:

Table 21 - Factors considered for probability analysis

Factors	Interpretation
External Environment	Survey of prospective scenarios that influence the realization of hazards (crime, parallel markets, judicial structure, corruption, trade union movement, among others).
Internal Environment	Survey of the level of relationship between employees and senior management, compensation, organizational climate, organizational culture, HR policy, and ethics.
Infrastructure	Survey of Passive Technical Means (MTP) and physical resources.
Organizational Means	Verify whether the organization has routine and emergency standards, risk treatment policies, and enterprise risk management.
Human Resources	Survey of the qualification level, quantity and tactical position of the team.
Information Technology (IT)	Survey of the nonexistence of electronic/computerized systems.
Frequency/Exposure	Degree of occurrence of the "risk factor" in each area or sector studied. The frequency/exposure can be classified as very low, low, medium, high and very high.

Source: CEFET/RJ

The second risk impact analysis considers the four groups of processes previously defined - operational, financial, and legal or image of the institution - and the degree of influence on them. In order to maintain the significance proposed by CEFET/RJ, Table 22 characterizes this classification.

Table 22 - Risk classification by sector/department

Sector/Department	Interpretation
Operational	1- Very slight disturbances; 2- Light; 3- Limited; 4- Serious; 5. Very serious disturbances.
Financial	1- Negligible; 2- Light; 3- Moderate; 4- Severe; 5- Massive.
Legal	1- Very slight disturbances; 2- Light; 3- Limited; 4- Serious; 5. Very serious disturbances.
Institution Image	1- Individual character; 2- Local; 3- Regional; 4- National character; 5 - International character.

Source: CEFET/RJ

The results found in the probability and impact analyses are expressed in a risk matrix (Table 23) that should result in the level of risk. This level corresponds to a result between the probability of the risk occurring in the department and the degree of impact of that risk on the activities carried out in that sector. The level of risk can be classified as low, medium, high and extreme. From this definition, the measures for the treatment of risks are formulated and adjusted through the action plans. At this stage, the recording will be done by completing the Action Plan in the Risk Management Worksheet and seeks to increase the probability of reaching organizational results through the treatment of risks.

The action plans aim to accept, mitigate, avoid or share the risks. Accepting risk means tolerating it; mitigate (reduce or modify) the risk is to reduce its likelihood and/or impact by bringing it to an acceptable level; avoiding risk corresponds to eliminating the activity that gave rise to it; and, finally, sharing the risk with third parties means seeking cooperation to solve the problem. Moreover, this is the moment in which the responses to the risks are defined through the execution of actions devised by the sector's team (risk owners - i.e., systemic boards and campus management), in partnership with its responsible person to carry out risk-treatment actions (read risk agent). The deadlines for responses to the risks and the total investment foreseen in each strategic action are also defined.

Table 23 - Risk Matrix Probability vs. Impact

RISK ANALYSIS		Probability				
		Very low	Low	Medium	High	Very high
Impact	Very high	High	High	High	Extreme	Extreme
	High	Medium	Medium	High	High	Extreme
	Medium	Medium	Medium	Medium	High	High
	Low	Low	Medium	Medium	Medium	High
	Very low	Low	Low	Low	Medium	Medium

Source: CEFET/RJJ

The strategies for risk mapping and treatment in the institution are always defined by the CGRC, which reveals that there is not yet a strongly decentralized or fragmented process in definitions of objectives, targets, and indicators by other areas of CEFET/RJ. It is worth mentioning, however, that all strategic actions defined are disseminated in the various areas through meetings, workshops, institutional e-mails and on the institution's website. It should also be pointed out that, throughout the decision-making process for risk management, five areas and their respective responsibilities are summarized as fundamental. They are:

1. CGRC: Committee created by Ordinance No. 803, dated July 6, 2016, and it has as main attribution to institutionalize, promote, guarantee and supervise the implementation and development of risk management in the institution. It is formed by the director general and by the systemic directors, being presided over by the director general.

2. CODIR: a permanent and advisory committee in support of the management of the Board of Strategic Management, with one of its functions supporting the implementation of institutional risk management. It consists of representatives of the systemic directors and the campuses, and the head of the Department of Institutional Development currently chairs it.

3. DIREG: responsible for chairing the Governance, Risk and Control Committee and for ensuring all necessary support for the implementation of institutional risk management.

4. DIGES: responsible for the implementation of process mapping and institutional risk management; and

5. DEDIN: responsible for supporting the Board of Strategic Management in the implementation of process mapping and institutional risk management.

Similarly, it is possible to establish the risk management of CEFET/RJ in seven main stages, as shown in Figure 21 below.

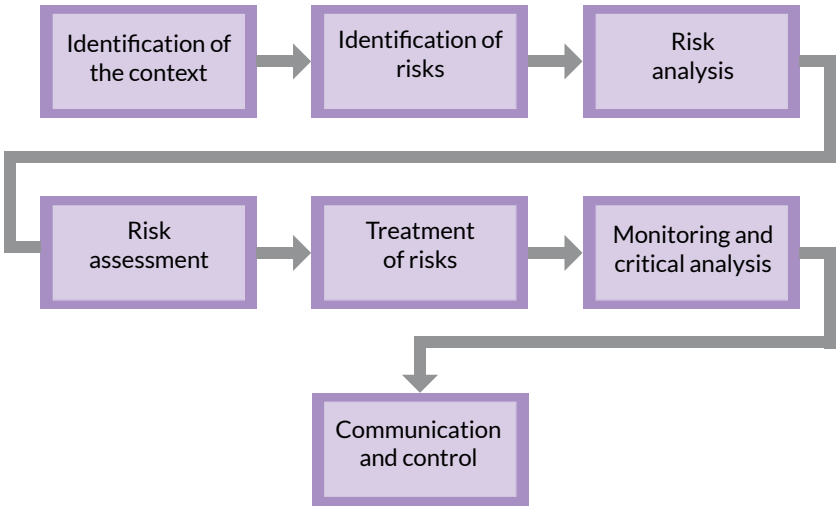


Figure 21 - Stages of risk management in CEFET/RJ
Source: CEFET/RJ

Thus, it is understood that the establishment of the context in the Risk Management Policy provides for the definition of external and internal parameters essential to the achievement of its objectives. All levels of the organization must have objectives set and communicated. There should then be clear objectives, aligned with the organizational mission and vision, and that is necessary to enable the detection of events. Risk identification involves the

recognition and description of critical events that may affect the achievement of the objectives. Risk analysis refers to the determination of the likelihood and impact of critical events that may have effects on pre-established objectives.

The purpose of the risk assessment is the quantitative and qualitative analysis, which will define the risks to be addressed and their order of prioritization through the level of risk identified by the risk matrix. The treatment of risks consists of the identification and selection of means (actions) intended to offer new controls or improve existing ones. The Monitoring and critical analysis deal with the review and the periodic analysis of the risk management, aiming at the continuous improvement of the institution. In the monitoring process, the performance of the risk indicators should be monitored, the implementation and maintenance of the action plans supervised, and the achievement of the goals established verified. Finally, communication and control constitute the flow of information between the parties involved in the risk management process in order to ensure the necessary understanding to decision-making involving risks and the control of the implementation of planned actions.

It is interesting to describe that the monitoring process occurs in three dimensions. In the first line of defense, there are the departments, coordination, sections and public agents whose task is to implement preventive actions to solve deficiencies in processes and controls. In the second line of defense, the director general, the systemic directors and the directors of the decentralized units of CEFET/RJ are present, whose duties are to determine directions and support the first line. Lastly, the third line of defense is the internal audit, which should promote independent assessments of internal controls.

In addition, a relevant aspect worth mentioning is the motivation for risk management. As presented at the FORPLAD conference in Natal, Rio Grande do Norte, risk management, before being conceived in this way, arising from the initiative of DIRAP to map all the processes in force in the institution, ensuring greater control and efficiency over them. Subsequently, through the Ordinance/Cefet/RJ nº 803, dated July 6, 2016, and amendments, this project was extended to the entire institution, under the coordination of the Board of Strategic Management (DIGES). During the process-mapping phase, 700 (seven hundred) processes were identified, grouped into two sets: (1) campus processes and (2) processes by boards. In the same period, legislation about risk management came into force, which ensured the mapping processes to fit into the context of this new legislation.

It is likely that CEFET/RJ has not yet undergone a reassessment of its Risk Management Policy, which is justified by the fact that the establishment of its first policy is recent. However, the institution affirms that the revaluation stages of its policy will be implemented after one year of the current policy and/or the implementation of a new Institutional Development Plan, as well as in the implementation of an Improvement Plan. The Improvement Plan refers to the processes of maturity evaluation since the risk management policy is still in the implementation phase, which prevents actions that measure the degree of maturity. As a recommendation, CEFET/RJ suggests mapping processes to provide appropriate and effective risk identification.

8. The forrisco methodology: risk management in the public sector

Developed to complement the ForPDI methodology - Institutional Development Plan [23], the ForRisco methodology has been supported by the Federal Institutions of Higher Education (IFES), by the National Forum of Pro-Rectors on Planning and Administration (FORPLAD) and by the National Association of Leaders of Federal Institutions of Higher Education (ANDIFES) of Brazil.

The ForRisco methodology is the result of a research project titled "Risk Management at Federal Universities: development of reference model and system implementation ", which was divided into the following five stages:

1. evaluation of market risk management methodologies adopted by the Brazilian Public Administration;

2. preparation of a questionnaire to assess the maturity of methodologies;

3. construction of a risk management methodology appropriate to public and private organizations, to be published in book format;

4. development of software to support managers in the conduct of risk management; and

5. Online and face-to-face training on the methodology and software tool ForRisco.

The first stage is described in the fourth chapter of this book. For the second stage, a chapter was published in the book Lecture Notes in Business Information Processing, Springer publishing house, entitled Perception of Enterprise Risk Management in Brazilian Higher Education Institutions, containing relevant information on the application of the questionnaire. The third stage corresponds to the creation and publication of this book. The fourth stage refers to free software to perform risk management in organizations, presented in Chapter 10. The fifth stage is related to face-to-face and online training, with courses that include the methodology and the ForRisco software.

In its origin, the project for risk management in federal universities seeks, in addition to the development and dissemination of the reference model by its own methodology, the development of the software ForRisco, a risk management tool that should support, in view of the proposed methodology, all the processes for implementing, managing, controlling, and monitoring organizational risks.

The ForRisco proposal is one of the most current and promising resources for efficient risk management in private and public organizations. Firstly, based on renowned international and national studies, the methodology shows itself capable of serving different institutions and sectors. Moreover, for its conception, some of the main structures of the market and the Public Administration were taken into account, which reinforces the methodology's ability to respond to the demands of different areas and natures.

Another differential is the ability to integrate the methodology and the ForRisco tool in support of the organizations' objectives. In fact, this integration allows aligning the stages to conduct the risk management following the structural logic designed by the software. It is also relevant to mention that the ForRisco methodology is the only one that argues the correlation between the developments of risk management policies aligned with the institutional development plans.

The following will present an outline of the stages for the implementation of risk management proposed by the ForRisco methodology and a description of each.

8.1. Stages in the implementation of risk management

In establishing what is understood by stages in the implementation of risk management, the ForRisco methodology brings, within the scope of management, a process composed of seven fundamental stages. They are: (1) policy definition; (2) establishment of the external context; (3) definition of risk management strategies; (4) establishment of the internal context; (5) implementing risk management for activities; (6) reassessment of the policy and the establishment of the level of maturity; and (7) assessing the maturity of the organization. The ForRisco methodology is described in Figure 22.

For these stages, it is suggested that it is interesting to think about which activities are generic and which are specific to the risk management of the organization, and which are macro level and micro level. Figure 22 contains a diagram of this logic:

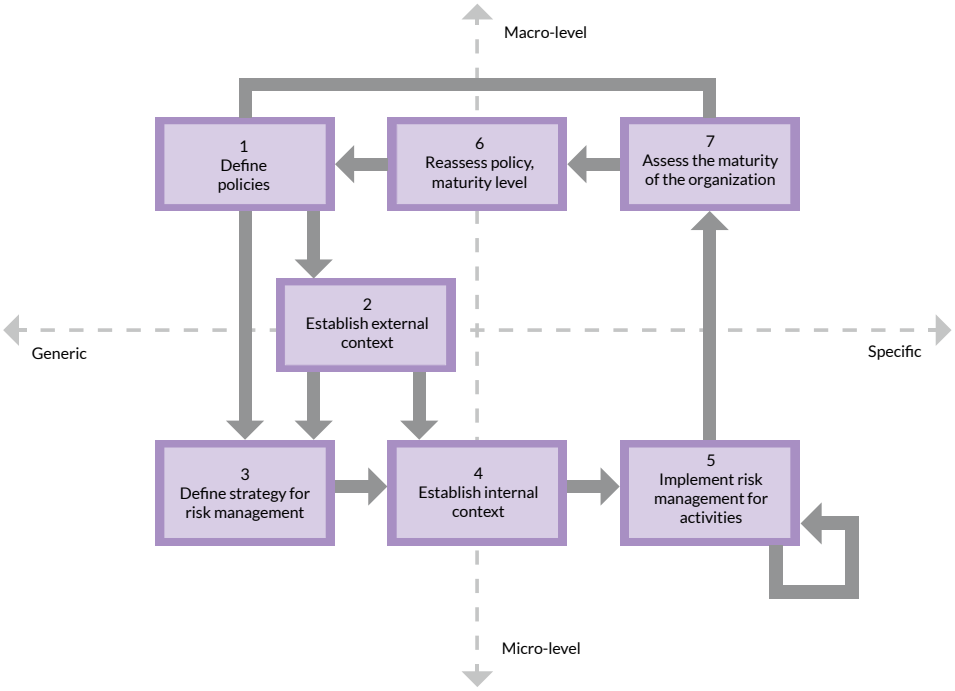


Figure 22 - ForRisco Methodology for Risk Management in Public Administration

At first, to structure each of the stages in an organization, one has to think about the generic and specific activities, as well as the macro and micro levels of this institution. Generic means a set of activities, processes, concepts, resources, and decisions that are analogous (similar) in the areas in a particular body. Specific means the same set of activities, processes, concepts, resources, and decisions that refer exclusively to a specific area in the body or to the whole body itself.

Next, it is important to consider how activities, processes, concepts, resources, and decisions can affect the organization. For this purpose, it is necessary to be sure about the levels of the organization. The macro level indicates that the entire organization is propitious to receive or to feel the repercussion of the executions established by these activities, processes, concepts, resources, and decisions made. On the contrary, the micro level indicates that the repercussion of activities, processes, concepts, resources, and decisions will be perceived only by the executing area.

It is worth mentioning that, over time, all activities reflect in the organizational context, in the short, medium or long term. In this way, it is up to the risk management to reduce the negative impacts of the areas, in the entire organization, especially in the medium and short term.

For the ForRisco methodology, the following scenarios apply:

- First quadrant - stages 1, 2 and 7 are activities that can (or should) be understood as generic and macro-level. This is because they are actions that involve the organization as a whole and can also affect the entire organization, even in the medium or short term;

- Second quadrant - stages 2, 3 and 4 are activities that can (or should) be understood as generic and micro-level. That is, they are activities that are common throughout the organization, but are also carried out in the organizational areas, reflecting their different contexts;

- Third quadrant - stages 4 and 5 are activities that can (or should) be understood as generic and micro-level. In fact, it is inferred that each specific area is able to understand its context and, in addition, to perform all the risk management actions for the activities that are convenient to them; and

- Fourth quadrant - stages 6 and 7 are activities that can (or should) be understood as specific and macro-level. In short, they must be carried out by the areas or by the organization as a whole, with a general impact on the organizational context.

The overall steps or stages for conducting risk management under the ForRisco methodology are presented below:

1. Define the Risk Management Policy at the organizational level.

2. Establish the external context following the guidelines of the GIRC to identify and understand the laws and standards that form the basis for implementing an agency's Risk Management Policy.

3. Based on the policy and external context, define the strategy for risk management containing the roles that will form the lines of defense,

train people and disseminate risk management. Defining strategies is key to ensuring the cohesive delineation between objectives and expected results for business processes and the organization's projects.

4. Establishing the internal context means considering the institution's skills, capacity, strategy, external context, and policy. It is recommended to complete the tasks of MGR-SISP about step "1. Establish context" and define people and roles in order to perform the tasks recommended by MGR-SISP.

5. Perform risk management for the activities and actions of the organization following the process steps presented in this chapter, contained in Figure 25 - Stages in the process of risk management proposed by the ForRisco methodology.

6. Re-evaluate each year, or when necessary, the policy and legislation in order to establish the level of maturity about the stages of risk management according to IBGC maturity measurement and realign actions regarding risk management in the organization.

7. Evaluate the maturity of the organization according to IBGC guidelines and use the questionnaire presented in Appendix I.

From a general understanding of the implementation of risk management, the essential components of this action will be detailed. The stages of risk management processes have four components: (1) Inputs; (2) Techniques; (2) Objectives, processes and tasks; and (4) Outputs. During the implementation of the process, the output from an earlier stage becomes the input to the next stage. Such techniques provide the necessary support to the steps and tasks of the stage in achieving the outputs. It should be noted that project/process mapping activities must be performed before the stages of risk management are initiated. For this purpose, it is recommended that information from the GIRC methodology be used. Figure 23 represents the model described above.

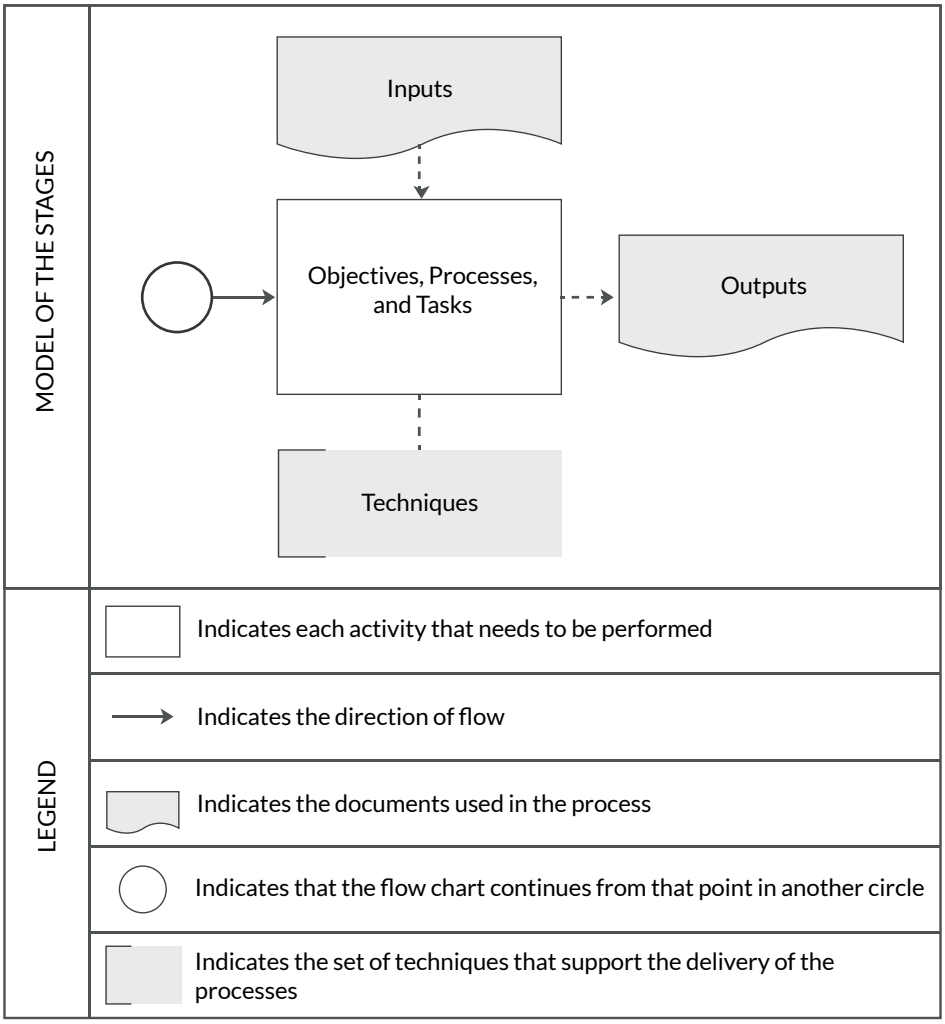


Figure 23 – Model of risk management stages of the ForRisco methodology

In risk management, the policy establishes the principles, guidelines, and responsibilities. Based on the development of this policy in order to understand and identify the objectives, processes and organizational tasks, it will be feasible to use a set of techniques to gather important information to the business and to carry out the activities of the organization. In the process of Figure 24, some techniques are suggested, but it will always be necessary to evaluate what best applies to the identification of the external context. For this stage, information about regulations in laws and rules, lessons learned on other occasions and questions that apply to the scenario will be used as input. As output, a strategy will be defined to guide the activities of the organization,

here separated between projects and processes, but not limited to these components.

Then, to identify the internal context, it will be taken into account the previously defined risk management strategy. Emphasis is placed on the use of guiding documents, such as organizational plans and policies, to ensure a better understanding of the internal context. It is also worth mentioning the use of the RACI matrix (acronym for Responsible, Accountable, Consulted and Informed) to recognize the assignments, tasks, and responsibilities in a given process, project, service or in the context of department and organization. Without detail, Responsible is who develops the activity; Accountable approves products and activities delivered, and also bears responsibility for them; Consulted means checking, with a kind of consultant, the progress of the process to add value; and Informed is the action of notifying all those involved/interested.

As mentioned, the ForRisco methodology understands projects and processes as different. As for the projects, it is recommended a methodology for their management, but it is understood that, at the end of the projects, products or services will be delivered and, if they become an internal service, they will be included in the business processes. For these cases, one should have another suitable control set. Risk management in projects occurs throughout the entire process, involving initiation, planning, execution, monitoring and control, and closure. Risk management is expected to contribute to changes in project scope, time, cost, resources, and quality, allowing for accurate communication and monitoring of project constraints. Since projects are understood as unique and complex, forms of control and monitoring must be ensured so that they can be tackled at first, avoiding rework and additional costs.

For business processes, it is necessary for understanding and control. Processes are all the routine activities of a department, division, or organization. In fact, processes do not necessarily have deadlines for closure, and yet need to be monitored. Process mapping contributes to the dissemination of information in a clear way, so that process participants know what to do when to do, how to do, and what the expected outcome is for a given process. However, because all processes are not always mapped, it is critical to think in the least about which deliveries a department or division is making, what is required for delivery, and what requirements these deliveries need to offer.

It is recommended to use the SIPOC technique (Supplier, Input, Process, Output, and Customer) to gain a better understanding of these processes. It is important to state that process risks must have their strategy for the outcome of these processes. Finally, as the processes are continuous, it is necessary to seek their improvement over time.

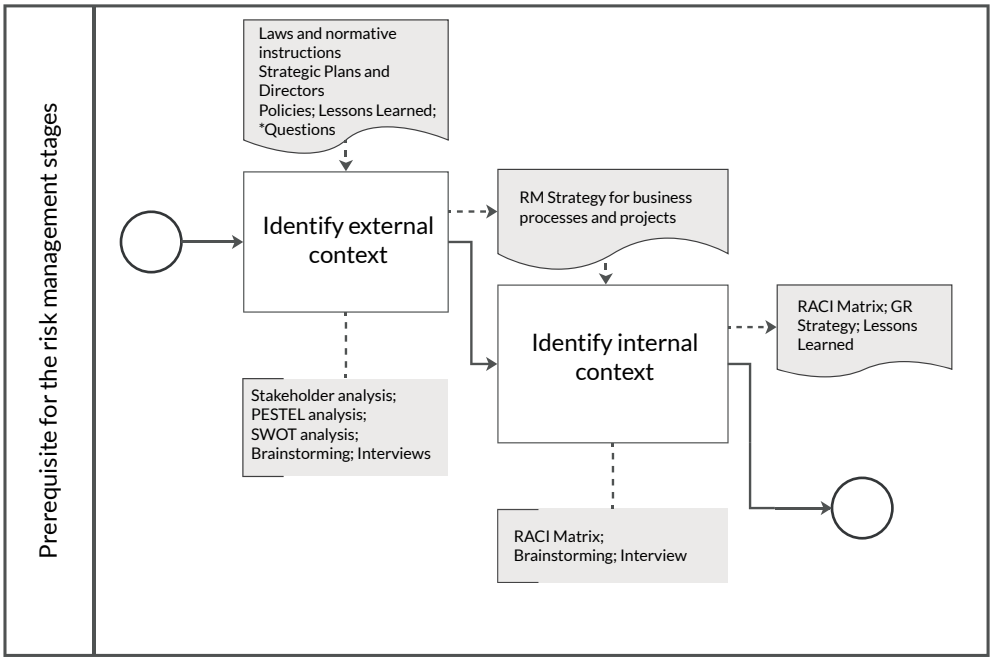


Figure 24 - Prerequisites for the risk management stages of the ForRisco methodology

Once the strategies are defined, and the external and internal contexts are recognized, the stages of the risk management process will be initiated, as shown in Figure 25. It is recommended at this stage that information from the activities present in the MGR-SISP be used. The first stage in this process is to identify and assess risk and to do so, it is suggested as input the rules of the body, policy, and strategy of GR processes, responsibilities of participants in the form of RACI matrix, lessons learned, among other information that aid in this identification and evaluation. As techniques to perform this stage, it is proposed the Probability and Impact matrix, brainstorming, impact assessment, probability and proximity, evaluation of expected value for treatment, among others. For this stage, the main output is the risk record, which will accumulate information throughout the process. A risk map and lessons learned as ancillary results can also be created.

Once the risk is identified and evaluated, the risk record information will be used for planning, but nothing prevents the risk from being revisited and reassessed according to the organization's need. Once this is done, there will be a guarantee that monitoring and control are occurring. In the same line, there may be changes in planning for the due treatment of risk. The risk map, presented in section 4.3.1. Of this book, can be used to monitor risks. Note that the map should reflect the risk analysis to enable a holistic view, i.e., indicate the risk at the moment prior to treatment and their current situation.

The "Plan" stage uses as input the risk record already identified and evaluated, the risk map, and the lessons learned. As a technique for this stage, risk response planning should take place, which will result in the definition of the people (RACI matrix) and the activities that must be performed. As output, this stage should contain, minimally, the owner of the risk, responsible for controlling and monitoring it, the risk agent, responsible for executing the treatment plan, the risk record, so that it can continue accumulating information about the risk, and the response plan, which should contain the actions necessary to address the risk.

The "Implement" stage will be executed when the risk tolerance level reaches an unacceptable level or when the risk materializes. In this case, the information of the risk record, containing the risk owner, the risk agent and the execution of the response plan are used as inputs. As a backup technique, it is inferred that the risk map is updated, and the control and monitoring of risks must be kept up to date. As output, progress reports on risk treatment and other summarized reports should be prepared. These reports reaffirm the organization's interest in maintaining monitoring and control by stakeholders.

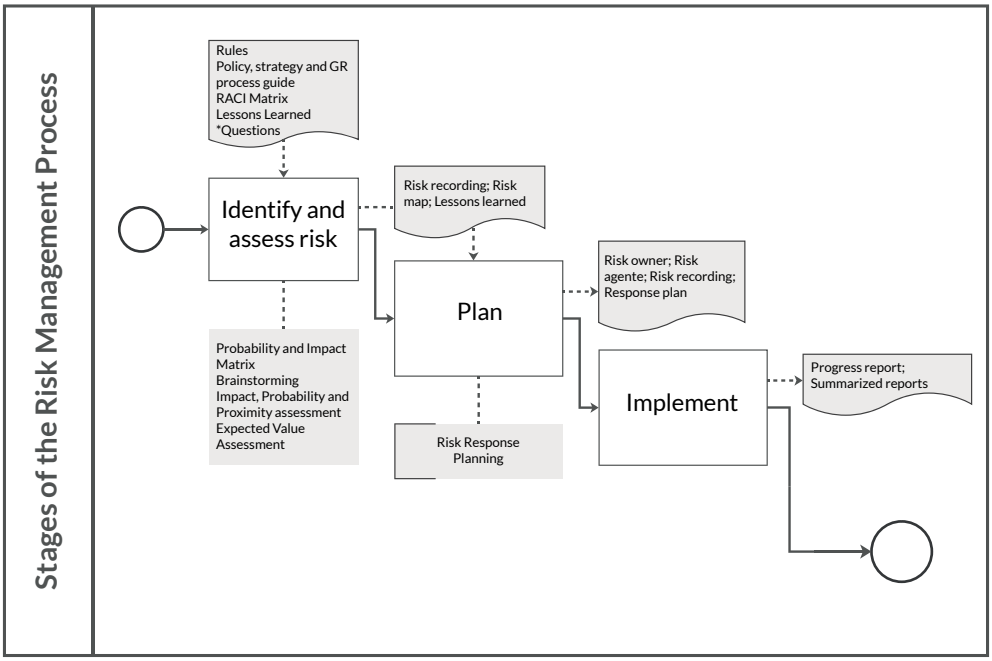


Figure 25 - Stages of the risk management process proposed by the ForRisco methodology

Ahead, in the stages for risk management of the ForRisco methodology, it is necessary to recognize the level of maturity. In this sense, it was decided to recommend the measurement of maturity in relation to the components defined in the IBGC methodology: (1) strategies; (2) governance; (3) policy; (4) processes, process interaction and management cycles; (5) language and assessment methods; (6) systems, data and evaluation models; and (7) culture, communication and training, monitoring and continuous improvement. Among the maturity levels defined by the IBGC methodology, the following classifications are presented:

(1) Initial - an organization that does not know how, where and why to implement risk management;

(2) fragmented - the organization knows where to start but does not know where it wants to go;

(3) defined - the organization has defined objectives, goals and strategies;

(4) consolidated - the organization has objectives, goals, and strategies

defined, implemented and monitored;

(5) optimized - the risk management strategy was revisited and clearly defined, implemented and integrated with other management cycles.

Thus, based on the evaluation of the level of maturity of the components in the organization, it will be possible to recognize and establish the need to re-evaluate the Risk Management Policy. As seen, the policy is one of the components that should be considered at this stage, and it will be relevant to determine the fundamental procedures for it to be effective to organizational and stakeholder aspirations. In consideration, time is a significant and conditioning factor for the reassessment of the policy. That way, the ForRisco methodology prescribes the need to reassess the organization's policy, legislation and maturity level every year, or when necessary, and realign actions and practices regarding risk management.

As a final stage in risk management, the ForRisco methodology encourages, once again, the use of the IBGC proposal, in addition to the questionnaire presented in Appendix I. In summary, the questionnaire seeks to develop organizational self-knowledge by admitting specific questions for risk management and those responsible, as well as collecting information about the work execution and perceptions about risk management by employees. The application of the questionnaire, together with the evaluation strategies and measurement of maturity through the IBGC methodology, foreshadows an organization with effective results in its risk management.

Finally, through the stages described above, we defend the adequacy when conducting risk management. It is emphasized that the monitoring and control stages must occur throughout the entire process, but since they do not have specific input and a defined result, it was chosen not to describe these processes. Monitoring and control, risk recording and progress reporting are essential components for adequate monitoring of identified risks. Regarding the control stage, from time to time - every six months or annually, or depending on the interests of each organization - should be undertaken to define process review activities, updates on policies and guidelines, as well as a reevaluation of maturity to define improvement actions about risk management.

In order not to make the risk management process time-consuming, it is necessary to ensure that, the registration tool provides an uncomplicated

interface, with information that is crucial to the conduct of risk management, but at the same time complete and effective in ensuring visibility of the current risk state, its magnitude and a history of risks. In this sense, a set of variables was considered to compose a form that allows the recording of risks, as presented in Appendix II of this book.

8.2. Example of the ForRisco methodology application

Two practical cases of the ForRisco methodology application are presented below.

8.2.1. Case 1 - Initiating the implementation of risk management with the ForRisco methodology

In case 1, the members of an organization are initiating the implementation of risk management, but no action has been taken so far. Probably, the level of risk management maturity is still low, and it is possible that the main stakeholders are not yet involved in these initiatives.

In this scenario, it is necessary to gain the sponsorship of the top management, which can be supported by the obligations regarding the legislation in chapter 5, which addresses Brazilian laws and regulations related to risk management.

Then, the organization's risk management policy must be formalized through an ordinance or equivalent document. After this formalization, it is important to measure the maturity of the organization even though implementation has not yet begun. This helps to form a baseline to allow future monitoring of the whole process.

For the identification of the external context, it is necessary to survey the laws, rules, and obligations that the institution should follow. Some cases follow higher public authorities or the guidelines of international organisms. These definitions of external context vary from organ to organ, or according to the rules of the Brazilian states, or according to other definitions. With this set of information, it is possible to outline a strategy for risk management that will depend on this context and the type of risk to be faced. For example, health risks will be treated differently from financial risks, or from information security, or from urban mobility, and each case requires its regulation.

Once a risk management strategy is already in place, projects and processes will undergo constant analysis. These analyzes can occur spontaneously or scheduled, keeping the purpose of interaction between people so that they can perceive the events. Once the events that cause uncertainties are identified, it is necessary to record them, and in order to do so, the suggested techniques can be used. Once the risk is identified, it is suggested that it be written in the form Cause → Risk → Consequence or Event → Risk → Effect. This facilitates reflection and understanding of the scenario. At that moment, the risk record begins to be filled with the information present so far.

With the risk recorded, an analysis will be carried out that will detail the nature of this risk for better understanding, profoundly and individually. In this case, the information on impact, probability, proximity and, if any, the expected value for the treatment is filled in. Such information helps to define this risk - identified - and allow comparisons with other risks in order to address, in the first place, the most urgent ones. This briefly described process occurs in the risk assessment stage. In exception, risk assessment considers several risks together, although individually evaluating each one of them.

Once the risks are assessed, the most serious ones should have a treatment plan. The more serious the risk, the better and more detailed the plan should be. The milder risks do not necessarily require treatment plans, but for the more serious risks, it is mandatory that such plans exist.

At any time that the risk materializes (becomes an issue), or exceeds the tolerance limit, the risk plan must be implemented, and the control and monitoring of these risks is necessary. Risks should be continually reevaluated in order to allow their last state to be represented in the tool and to have accurate communication regarding those risks. This reassessment is part of the monitoring stage. These cycles are interactive and continuous, as events occur at unknown intervals. However, after a period of 6 months to 1 year, policy and legislation should be reviewed, and the maturity of that period should be reassessed for future improvements.

8.2.2. Case 2 - Applying the ForRisco methodology in an organization that has already started risk management

In case 2, the organization has already begun to implement risk management, but its processes have not yet been mapped. To make the scenario worse,

the servants and employees are overloaded with assignments, and there is a shortage of human and material resources in the organization.

There are knowledge and willingness on the part of top management to apply risk management, but the workforce for conducting risk activities is scarce. One possible solution to this scenario is the time optimization of those involved so that risk management is not a hindrance to teams.

The Risk management software will be of vital importance in automating notifications, remembering deadlines and dates, centralizing information about risks and saving time for those involved.

In this case, managers must monitor these risks more frequently, accessing the tool daily to give them the necessary development. One should avoid meetings with many participants, calling only those responsible or representatives. There is a need for accountability directed to the stakeholders and a request for the issue of risks to proceed.

Even without the mapped processes, the stages of risk identification and assessment can occur. These stages will help in planning and treating risks, as well as assisting with monitoring and control.

In this scenario, it is better to have a minimum of control and record than no control at all. By giving more visibility to the control of events and allowing more effective communication, one can better understand the performance of teams and request support in the definitions of people relocation and financial resources, since the volume of work is known.

Risk management is not the solution to all organizational problems, but it allows a record and monitoring structure to be created in order to measure and communicate these risks more accurately. It also contributes to the internal culture as to the proper handling of important business issues. Also, it should be remembered that audit and control bodies will request the development of these actions and that complying with these guidelines is of utmost importance to the organization.

9. How to evolve risk management in a public institution? An analysis of the cases of UNIFAL-MG and CEFET/RJ in the light of the forrisco methodology

In order to establish an appreciation of risk management currently developed in the researched IFES, this chapter intends to conduct a comparison, that is, a comparison between the reality of the organizations studied and the principles and stages of the ForRisco methodology. As evidenced, the ForRisco methodology emerged from a project whose purpose is to influence risk management in the public sector, especially in the field of education, where it has gained support from IFES in Brazil. Proof of this is the possibility of carrying out the case studies at UNIFAL-MG and CEFET/RJ, institutions recognized by MEC and acting in the scope of education, research, and extension.

It is worth mentioning that the ForRisco methodology aims to become the main reference model for public or private institutions wishing to formulate and implement or optimize their risk management processes. Taking as support, therefore, real cases articulated in consolidated public organizations, a detailed investigation is admitted between what the ForRisco proposal suggests and how the risk management processes were developed and implemented in practice.

To give greater visibility to what is established in the stages of risk management in the ForRisco methodology, it is important to remember that the methodology designates seven key stages. The stages are: (1) policy definition; (2) establishment of the external context; (3) definition of strategies for risk management; (4) establishment of the internal context; (5) implementing risk management for activities; (6) reassessment of policy and maturity level; and (7) assessment of the organization's maturity. It should be noted that risk management is, in itself, a continuous cycle, and it is recommended after stages 6 and 7, respectively, a reassessment of the policy and maturity level and assessment of the maturity of the organization, so that the cycle restarts.

The policy is understood by the ForRisco Project as the direction of the course of the risk management to be implemented. It ensures the determination of parameters - external and internal - for the full execution of management tasks. Only an established policy may be able to assist and integrate risk management into the overall agenda of any institution, so its merit. Notably, both UNIFAL-MG and CEFET/RJ have a Risk Management

Policy already formulated and implemented (or under implementation). Both policies are recent – dating from 2017 - and were institutionalized after the Normative Instruction proposed by the Federal Government that incited the management of risks in public organizations.

Initially, what is worth highlighting are the different scopes in which these policies were formulated, including meeting different objectives. The risk management policy at UNIFAL-MG comes from the active role of the Pro-Rector's Office for Planning, Budget and Institutional Development in improving the budget proposals at the institution, as well as the initiative of a more modern and sustainable administration. In CEFET/RJ, before the policy was conceived, the Department of Administration and Planning needed to map all the processes in force in the institution to guarantee greater control and efficiency. With the validity of risk legislation, the process was appropriate and proved to be efficient in the implementation of risk management.

Regarding the establishment of the external context, the present methodology highlights the need to identify and understand the legislation and regulations related to the implementation of a Risk Management Policy. The book itself contains a series of laws, regulations, and decrees governing risk management, governance, and internal controls in federal bodies. The fact is that at UNIFAL-MG, this support is provided by the Legal Department of the institution, which allows us to infer the proper position of the university regarding legislative changes and its deadlines. It should be noted that, because it has a specific sector that deals with legislative changes and proposes modifications in the organization's internal policies, UNIFAL-MG does not seem to depend on a system or tool for this identification process.

For the realization of the external context, CEFET/RJ has as its governing body the Governance, Risk and Control Committee, and the technique of brainstorming as the main tool used, which, according to the institution, is effective for ensuring the participation of servants from different areas of the organization. It should be noted, however, that this is not the only function of the Governance Committee, which should be primarily responsible for institutionalizing, promoting, guaranteeing and supervising the implementation of the Risk Management Policy in the institution. For both institutions, it is inferred the possibility of inserting a risk management software as a guarantee of greater effectiveness in the development of contexts.

The third stage provided for in the ForRisco methodology describes the concern to determine, based on the policy and external context, the strategies for the management of risks, containing the roles that will form the defense lines of this policy that will soon be focused on the answers and the compliance with regulatory obligations and organizational planning. In addition, strategic actions aimed at training people and disseminating risk management in order to have a common and uniform understanding among institutional bodies. These strategies ensure, finally, the delineation of the objectives and expected results for the business processes and projects.

The strategic management of the processes for formulating and implementing the policy, and for monitoring and controlling risks at UNIFAL-MG is the sole responsibility of CGRC. The strategy begins, inclusive, with the very formation of the Committee, which ensures the participation of both the High Public Administration, in the figure of the Rector of the University and the Pro-Rectors, as well as coordinators of institutional matters. It is possible to understand that being strategic in this institution depends previously on establishing a Risk Management Policy and knowing the relevant legislation, which corresponds to the very establishment of the external context.

It is worth ensuring that "being strategic" is not the only function of CGRC, yet all the strategic actions that ensure the effectiveness of management come from it. For example, the Committee, in addition to approving and implementing the risk policy, aims to ensure access to information on the risks to which the organization is exposed, aiming, strategically, for improvements in the decision-making process and expansion in the range of possibilities for achieving objectives. Also, for the implementation of risk management, all the objectives, goals and indicators outlined in the Institutional Development Plan of UNIFAL-MG are taken into account, which stimulates reflexive action in all areas.

Regarding CEFET/RJ, the important role of DIGES is highlighted through an Institutional Development Committee. Although it also has a Governance, Risk and Control Committee, DIGES is primarily responsible in the institution, for example, for conducting periodic critical analyses of risk management processes. Brainstorming is the most common methodology to define strategies; however, it is valid to recognize that decision-making on risk mapping and treatment strategies is centralized in the hands of the Governance, Risk and Control Committee.

It is also noted that the context-setting process of CEFET/RJ does not occur in two stages, as proposed by the ForRisco methodology. Perhaps because it presents a Board of Strategic Management, the institution does not distinguish, in practice, between the moment of realization of the external and internal context, even ensuring that there are different parameters for each of them. In agreement with what was presented in the CEFET/RJ case study, the establishment of context is the initial stage of risk management, which has in its policy all the objectives to be set and communicated in the organization.

By understanding the establishment of the internal context, the ForRisco methodology intends to identify all the skills, the strategic capacity and the activities developed in the organizations. The recommendation is, at first, to define clearly the internal stages of risk management, identifying the objectives, premises, constraints, and scope of the projects developed. It is also necessary to define those responsible for the units of the organization or the projects and activities developed, in this case, the owners of the risk and agents of the risk. Such actions are important to ensure the feasibility of context actions.

UNIFAL-MG understands that the realization of the internal context must occur only after the Risk Management Policy is established and disclosed institutionally. For this university, it will only be possible to identify fully the processes and their risks when the whole institution has a thorough knowledge of what is involved in risk management and the possibilities of monitoring, controlling and treating them. In addition, several methodologies and/or tools are used to carry out context activities, both internal and external, such as SWOT Analysis, brainstorming, Ishikawa Diagram, Bow-Tie and Risk Identification Form. It should be noted that this is a decentralized process carried out by each institutional unit, with accountability by the owner and the risk agent.

For the realization of the internal context, CEFET/RJ uses other methodologies besides brainstorming. It is important to remember that the external and internal contexts are carried out in the same stage, that is, the first; what differs are the methodologies and tools used in each process. Thus, it is common to perform internal context, in this institution, through the methodology of 5 whys and the 5W2H methodology. The use of the ancillary worksheet, which covers all aspects relevant to risk management in the institution, is added to the use of the presented methodologies. The realization of the internal context of CEFET/RJ also occurs in a decentralized manner, but this entire process is supported by the Governance, Risks and Control Committee.

The fifth stage provided for in the reference model of the ForRisco methodology is the implementation of risk management in the activities. The practical stage of risk management, at which point all activities and actions taken in the organizations are identified, analyzed, monitored and addressed, when necessary. It can be understood as a permanent cycle that monitors the tasks, the business, and the performances to avoid problems or situations that prevent the achievement of the objectives pre-established in the policies, plans, and institutional programs.

According to what was presented in the case study of UNIFAL-MG, its empirical process of risk management occurs through five stages/phases: (1) identification of risks; (2) risk analysis and assessment; (3) risk planning and classification; (4) monitoring; and (5) control. In short, identifying risks is the act of mapping all processes and possible risks that may negatively affect their flow in the institution. The analysis phase aims to bring clarity and standardization to the identified risks according to the university´s policy. Planning is the action of classifying the risks as to their probability of occurrence and its impacts. Monitoring means that risks are continually observed throughout the operations. Risk control is the final phase and represents the action plan established for risk treatment through joint decision-making between the Pro-Rectories, the Support Units, the Legal Unit, the Institutional Development Coordination and CGRC.

In practice, risk management at CEFET/RJ presents a process described in seven stages/phases: (1) identification of the context; (2) identification of risks; (3) risk analysis; (4) risk assessment; (5) treatment of risks; (6) monitoring and critical analysis; and (7) communication and control. In summary, the first stage is to identify external and internal issues that affect, directly or indirectly, the activities of the institution, followed by stage 2, which recognizes the risks. The third stage deals with the determination of probability and the impacts caused by risks; and risk assessment - stage four - tends to verify, quantitatively and qualitatively, the level of these risks. The fifth stage is the one that will treat the risks according to their degree of need and, later, the risks are monitored in order to maintain the continuous improvement of the institution, being finally communicated and controlled to guarantee the transparency of the management (stages 6 and 7).

Once the cycle of a risk management process is understood, the ForRisco methodology presents as the sixth stage the need to reassess the policy and to identify its level of maturity. It should be stressed that the policy must be reviewed at least once a year, or when the institutions deem it necessary. In addition, identifying the level of maturity means understanding where the organization is in its management process, going through the initial, fragmented, defined, consolidated or optimized level. It should be noted that all of these definitions are described in Table 10 of this book as guided by the risk management strategies of IBGC/GRCorp.

It is valid to infer that, at the date of this study, none of the analyzed institutions had completed one year in their Risk Management Policy, and both did not understand the need to re-evaluate the policy before the recommended deadline. UNIFAL-MG established its policy on 05/04/2017 and anticipated in its process of risk management, control and monitoring the stages of reassessment of policy and identification of the level of maturity. The situation is repeated in CEFET/RJ, which instituted its policy on 12/08/2017, an even more recent date, and ensures the stages of reassessing the policy and measuring management maturity in its institution. Thus, the two institutions analyzed are in the process of implementing their risk management and are in the "fragmented" status in the measurement of the level of maturity according to GRCorp strategies.

The seventh and final stage of the process of risk management in organizations, proposed by the ForRisco methodology, aims at the self-knowledge of the organization. It is essential that all public or private institutions, newly established or already consolidated, know their processes and objectives, as well as their mission. In fact, assessing the organization's maturity translates into understanding its human resources, aligning its strategic objectives and ordering it so that it is clear "where the institution wants to go" and "how the institution wants to be recognized". At the same time, understanding the maturity of organizations allows them to recognize their weaknesses and, consequently, their risks. Moreover, the clarity of risks drives its treatment, more efficient management and a precise reach of the opportunities, goals and organizational goals. In time, neither UNIFAL-MG nor CEFET/RJ presented an assessment of the maturity of their organization.

Notably, it is possible to recognize the good work carried out by UNIFAL-MG and CEFET/RJ in its risk management processes. Both institutions have thought, stepped up their efforts to identify, assess, monitor, control risks, and have therefore demonstrated their high ability to deal with adverse situations, problems, and vulnerabilities in their day-to-day processes. Thus, although risk management has been designed to trace different interests, missions, and objectives, it is possible to recognize similarities in its management processes. Table 24 presents a general context of the stages presented in the organizations surveyed and the ForRisco proposal.

Table 24 - Confrontation between the stages of risk management of UNIFAL-MG and CEFET/RJ and the ForRisco methodology

Stages	UNIFAL-MG	CEFET/RJ	FORRISCO
Policy	Formulated as a more modern and sustainable management initiative.	Formulated from the need to map all the processes in force in the institution to ensure greater control and efficiency.	Understood as the direction of the course of risk management to be implemented by an institution. It ensures the determination of parameters - external and internal - for the full execution of management tasks.
External Context	The support is given by the institution's Legal Department, which deals with legislative changes and proposes changes in the organization's policy.	Its governing body is the Governance, Risk and Control Committee, and it uses the brainstorming technique to realize the context and update the policy.	It highlights the need to identify and understand the legislation and rules related to the implementation of a Risk Management Policy.
Strategies for risk management	Exclusive activity of the Governance, Risk and Control Committee. Being strategic depends on establishing a Risk Management Policy and knowing the relevant legislation.	DIGES is responsible for the implementation of process mapping and risk management strategies.	Define the roles or those responsible that will form the lines of defense to manage risks, train people and disseminate risk management in the organization.
Internal Context	The realization of the internal context must occur only after the Risk Management Policy is established and disclosed institutionally. It uses certain methodologies and tools to implement the internal context, among them: SWOT Analysis, brainstorming, Ishikawa Diagram, Bow-Tie and Risk Identification Form.	It does not differentiate between the external and internal contexts, executing them as a single stage.	The recommendation is to define clearly the internal stages of risk management, identifying the objectives, premises, constraints, scope and those responsible for the areas or projects developed. It also promotes the identification of the skills, the strategic capacity and the activities developed in the organization.

Stages	UNIFAL-MG	CEFET/RJ	FORRISCO
Risk management for activities	It occurs through five stages/phases: (1) identification of risks; (2) risk analysis and assessment; (3) risk planning and classification; (4) monitoring; and (5) control.	Process described in seven stages/ phases: (1) identification of the context; (2) identification of risks; (3) risk analysis; (4) risk assessment; (5) treatment of risks; (6) monitoring and critical analysis; and (7) communication and control.	Suggests risk identification and assessment based on rules and procedures set out in the policy and management tools; planning stage, with risk record, risk map and lessons learned; implementation of risk responses by owners and risk agents. The monitoring and control stages must occur throughout the entire process, establishing itself as an explicit phase in the process. Finally, it is recommended the preparation of progress reports and summary reports.
Reassessment of policy and definition of maturity level	The institution did not conduct a reassessment of policy and did not present the defined maturity level.	The institution did not conduct a reassessment of policy and did not present the defined maturity level.	Emphasizes that the policy should be revisited at least once a year, or when necessary. On identifying the level of maturity, it means understanding where the organization is in its management process, going through the initial, fragmented, defined, consolidated or optimized level.
Assessment of organizational maturity	The institution did not present an assessment of the maturity level.	The institution did not present an assessment of the maturity level.	Assessing the organization's maturity means understanding human resources, aligning strategic objectives and perspectives that involve "where the institution wants to go" and "how the institution wants to be recognized".

In this way, both UNIFAL-MG and CEFET/RJ recognize the need to establish a Risk Management Policy that represents the agenda of all actions and strategies that have been put into practice. Despite presenting relatively new policies and management plans, the two institutions make clear the need to establish the external and internal context, even if their processes are applied differently. They are organizations that know each other, perceive their resources and make use of them to work peculiarly, their own. It also reveals the proximity of their risk management cycles, which, in the manner of each institution, cover the same stages of process identification, risk analysis and assessment, risk planning and treatment, and monitoring and control.

Finally, it is understood the importance and relevance of the ForRisco methodology to propose a structured, updated and complete thought for full effectiveness of the risk management processes in public organizations. The methodology is presented as an innovative instrument that aims at consistency with what is prescribed by the current legislation on risk management, governance and internal controls in Brazil, and motivates organizations in the evolution of their risk management processes. In addition, it is essential to demonstrate, following this work, the development of free software, offered by the ForRisco Project, which translates the alignment between the theoretical foundation presented in this book and the technological tool that allows integrating and operationalizing all the probable actions for the effective management of risks.

10. THE FORRISCO SOFTWARE PLATFORM

One of the main objectives of the ForRisco Project was to establish, in addition to its methodology that would support and foster risk management, a tool capable of linking knowledge, innovation, and practicality to dealing with possible risks in an organization. Therefore, the ForRisco Platform is an open source database for monitoring and managing risks arising from the processes developed by the institutions.

The ForRisco Platform arose from the need to align theoretical and practical principles for the management of risks that interfered in the strategic planning of the Brazilian federal teaching authorities. Risk management was a recognized deficiency in the research developed by a working group of the National Forum of Pro-Rectors on Planning and Administration (FORPLAD), composed of the Federal University of Alfenas (UNIFAL-MG), the Federal University of Lavras (UFLA), the University of Brasilia (UnB) and other participating universities that assisted in the discussions and definition of the software.

The main purpose of the ForRisco software is to enable the application of risk management techniques to private and public entities, seeking to increase the internal control and governance of these institutions. With this software, it is possible to organize and plan resources in a way that minimizes the impacts of the risks in the institution, using a set of techniques to minimize the effects of accidental damages and direct appropriate treatment to risks that may damage the project, the people, the environment and the image of the organization.

Through the ForRisco Platform, the user will have access to a set of features to ensure the management and monitoring of the risks. Here are some possibilities provided by the software:

- **create Risk Management Policy:** a concrete dimension of the mechanisms for guiding the decision-making and action of risk management activities and processes;

- **create Risk Management Plan:** refers to the project or set of measures established as a practical guide to identifying, managing and monitoring risks;

- **assess and classify the risk typology:** the classification is organized in operational, legal, image/reputation of the organ and financial/budgetary;

- **define the degree of risk:** refers to a classification by the user of the position or level of risk at a given time. The risk can be classified as critical, high, moderate and small;

- **establish corrective actions:** are activities and practices aimed at implementing decision-making to correct incidents;

- **allow different levels of access:** the tool makes it possible to hierarchize and control the access of users by their managers;

- **recognize risk-related threats or opportunities:** threats are situations of uncertainty, external and/or internal to organizations, that can hinder or prevent the achievement of defined objectives; opportunities are favorable, external and/or internal circumstances or circumstances that can be harnessed and positively affect the achievement of objectives;

- **define the periodicity of the analysis:** refers to the regular intervals at which the risk should be analyzed. The platform offers the following intervals: daily, weekly, biweekly, monthly, bimonthly, quarterly, semi-annual and annual;

- **identify causes and consequences of risks:** the cause is considered the principle, the reason, the reason or the origin for the risk to happen; the consequence is all that has been produced (or can be produced) in the face of the identified risks. Effects or results of risks; and

- **develop risk matrix:** mechanism to indicate, in an orderly manner, the risk classification proposed by the user based on the degree of risk.

In addition to the highlighted commands, the system also allows to establish prevention actions, record the date and time of editing information, duplicate plans and risk management policies to facilitate editing, create or be based on the indicators of the ForPDI Platform, create planning per unit, add and edit risk information and perform advanced search, among other actions. Next, Figures 26, 27, 28, 29 and 30 correspond to a prior presentation of the ForRisco Platform.

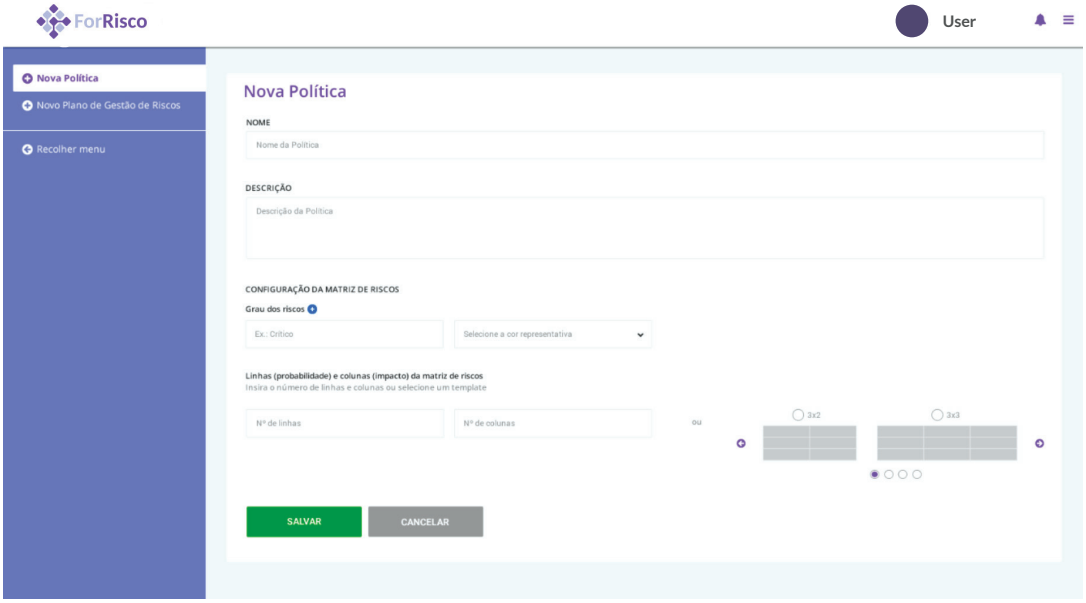


Figure 26 - Addition of a new Risk Management Policy

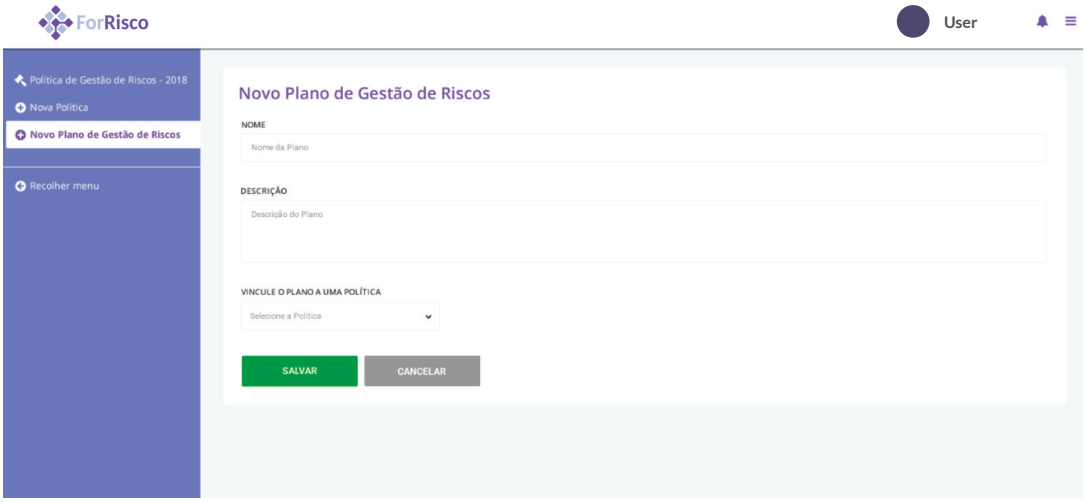


Figure 27 - New Risk Management Plan

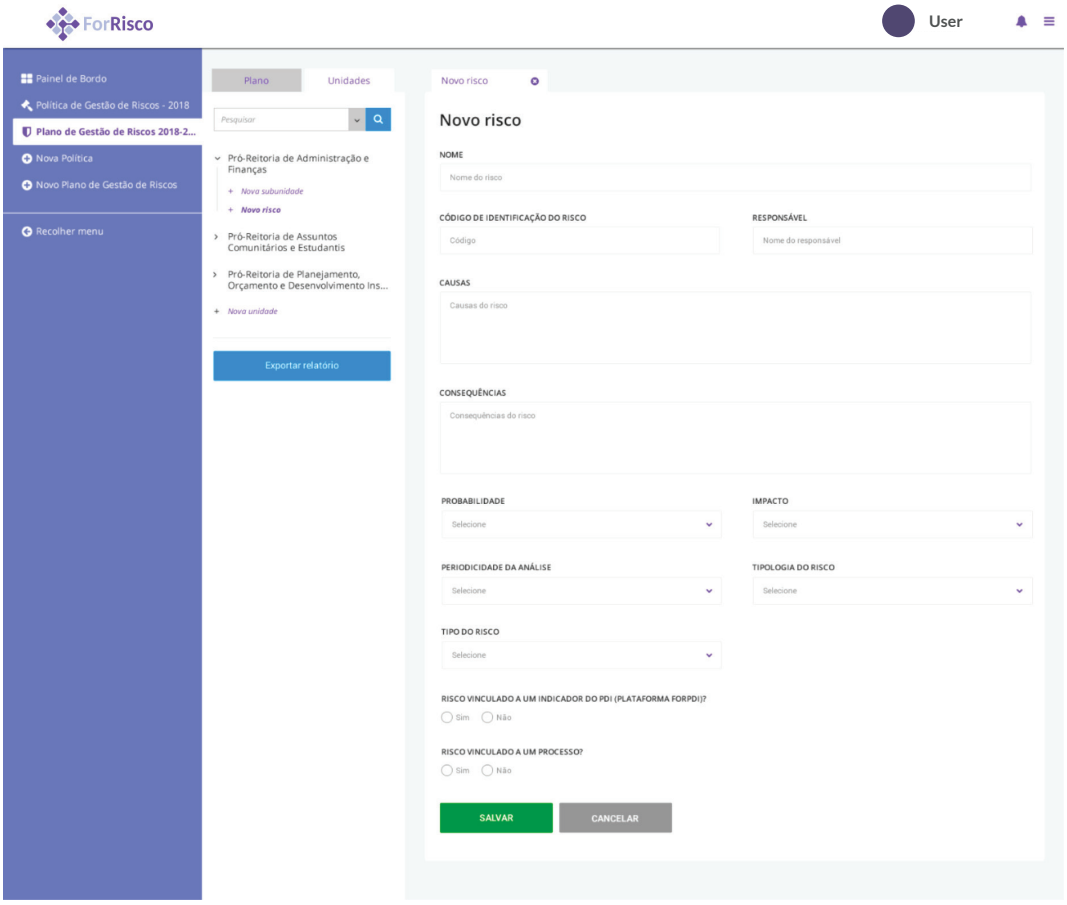


Figure 28 - New risk and risk information

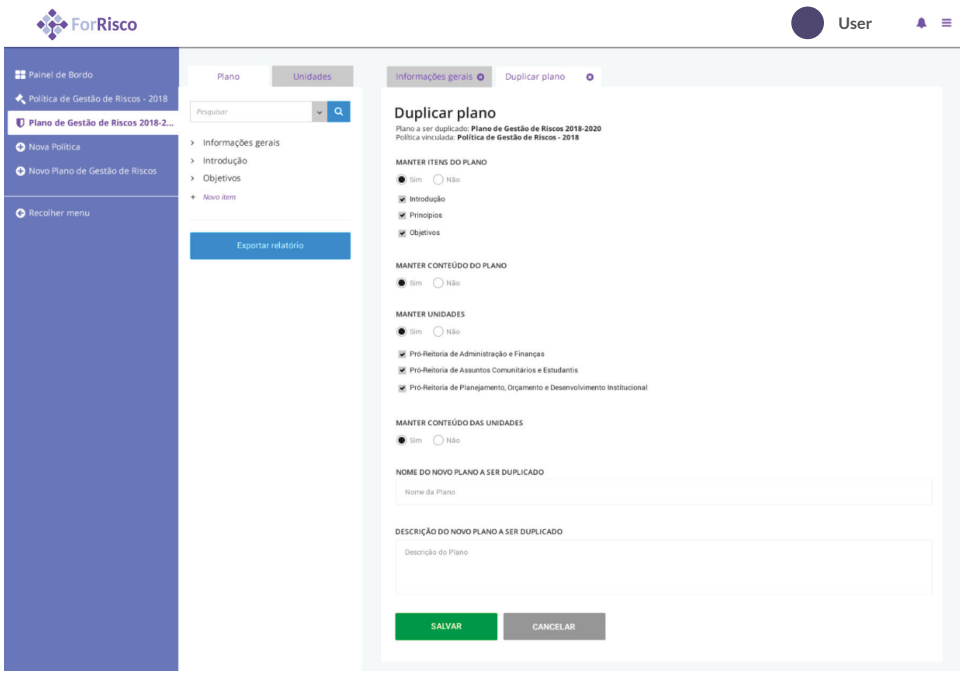


Figure 29 - Facility in the creation of new risk plans: the duplicate plan feature

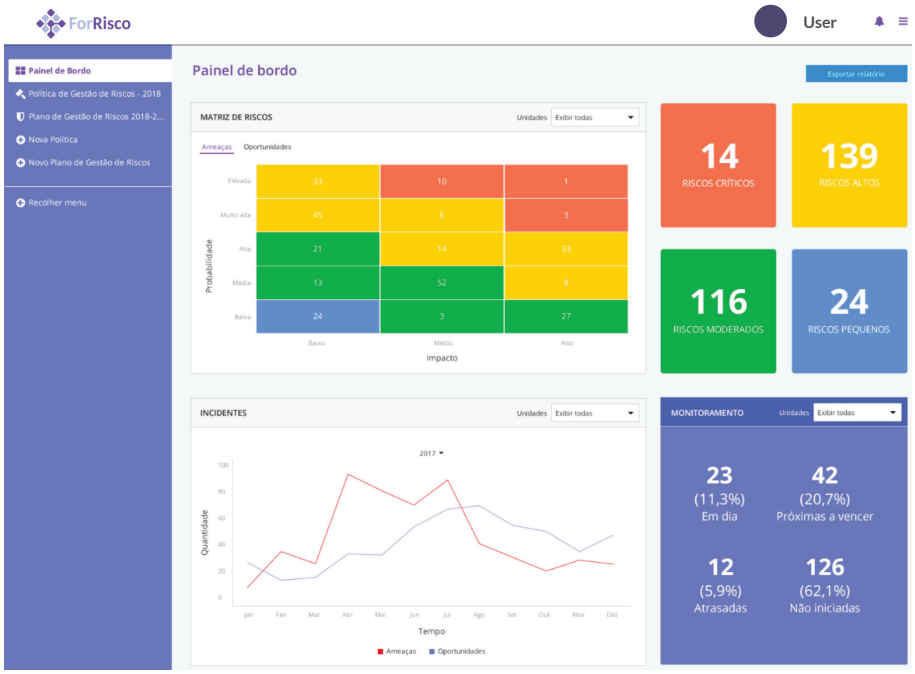


Figure 30 - Real-time monitoring of risk management with the ForRisco Platform

In short, the figures represent the following processes: create and describe an institutional risk policy (Figure 26); create and describe a Risk Management Plan, with the possibility of linking it to an already established policy (Figure 27); define the recognition of a new risk as well as codify it, hold a user responsible, indicate the causes and consequences of the risk, provide probability of occurrence of the risk and the impact of that risk, indicate periodicity of the analysis and classification as to the type and typology of risk (Figure 28); duplicate the plan previously created, either entirely or according to the user's interest (Figure 29); and view the dashboard, which allows monitoring the progress of the plan in real time as well as monitoring of processes, incidents and risk control (Figure 30).

By the way, it is worth highlighting the alignment between the platform and the ForRisco methodology, which, in theory, complement each other. As shown in the figures above, it is possible to recognize this alignment, since the platform enables the creation of risk policy and the detailed structuring of the risk plan through the establishment of internal and external contexts, causes and consequences of risks, definition, and description of activities and processes. In addition, as the ForRisco methodology proposes, the platform makes it possible to establish probability and impact matrix (risk matrix), plan risk responses and corrective and preventive actions by the institution or unit that owns the risk, among other functionalities.

In light of what has been presented, the ForRisco Platform is assumed as the appropriate tool to support risk management actions in organizations, whether private or public. It is worth noting, besides the compliance of the tool with the best systems offered in the Brazilian and international markets, and the various features offered by the platform, the free character of the tool, which has its source code open as well as the user manual of the platform and the training course, available on the ForRisco Project website.

11. Final considerations

Risk management is a practice constantly recommended by Boards of Directors and corporate governance around the world, the fact that stems from the set of uncertainties faced daily by private and public organizations. Risk management corroborates the construction of reflective moments regarding the uncertainties that influence the organization and sometimes provokes continuous processes of action. Managing uncertainties is a need for managers to deliver the necessary objectives and results to organizations, and risk management must efficiently support opportunities for reflection on the uncertainties that influence organizational functioning.

The current moment is very rich and promising in the development of risk management in both the private and public sectors. In countries such as England, the United States and Canada, for example, risk management is already a reality in Public Administration. In Brazil, as from 2016, with the Joint Normative Instruction CGU/MP No. 1 (2016) [31] - which provides for internal controls, risk management, and governance within the Federal Executive Branch - among other laws and regulations, risk management has gained emphasis in institutions. Certainly, much of this exaltation of the theme stems from pertinent legislation, which has come to concern themselves with the regulation of risk management processes, especially of organizations that participate in the public sphere, which brings generality to such processes.

It is important to mention that contemporary studies on risk management methodologies, tools and software, as well as other publications on the subject, have sought to meet this new need to change the culture of risk in organizations involving all levels of the organizational structure, so as to reflect on the obstacles and difficulties in carrying out activities and on the possible consequences thereof. Within the scope of Public Administration, it is possible to infer that risk management techniques incorporated in these organizations are increasingly common in order to increase internal control, governance and the effective achievement of the objectives and expected results.

Among the main objectives proposed and achieved, one can infer the research effort in evaluating the most current methodologies available on risk management both in the market and those adopted in the public sector. For didactic purposes, the main methodologies found were distinguished in two groups: market methodologies: ERM-COSO - widely adopted by the

Brazilian Public Administration - and ISO 31000 and M_o_R-OGC - recurrent methodologies in public and private organizations in several countries; and (2) Public Administration methodologies: GIRC, SISP – MGR-SISP and IBGC. Also, the evaluation of the risk management software contributed to the perception of the main attributes in information systems that support risk management.

Other important points include a chapter devoted to establishing the laws and regulations governing risk management procedures; the identification of a significant number of tools and techniques used for the implementation and execution of risk management in organizations; and the ForRisco methodology itself, which aims to disseminate the importance of the cohesive construction of the stages of risk management. In addition, the ForRisco Platform distinguishes itself, which allows the application of risk management techniques and the administration and planning of resources, in order to reduce the impacts of risks on organizations.

Regarding the carrying out of the case studies, UNIFAL-MG and CEFET/RJ showed, through their risk management processes, the need and the importance of establishing risk management in a rational way, intended to understand the objectives and the peculiarities of its institutions. At the same time, it was possible to perceive similar processes in the execution of risk management in the researched institutions, which raises the pertinence of the ForRisco methodology when proposing a structured reflection in stages to fulfill the requirements and legal devices of risk management.

Knowing the risks means identifying threats to which the organization is exposed, but in addition, it means perceiving opportunities. As a result, risk management aims to contribute to improving organizational performance by allowing systemic controls and monitoring of these risks. It should be noted that this is also one of the objectives of the ForRisco methodology and Platform, which were elaborated based on the project "Risk Management at Federal Universities: elaboration of the reference model and implementation of the system ", have the mission of supporting organizations in the implementation of risk management processes.

For future work, it is recommended that the performance of organizations is evaluated before and after the application of the ForRisco methodology and/or Platform, as well as an evaluation among organizations that have adopted different methodologies to measure their respective performances. The key

success factors identified in these assessments will enable both ForRisco products and the organizations themselves to evolve by ensuring stages of reflection and learning in the organizational context and, consequently, greater assertiveness in future implementations. Finally, what is expected through risk management is more added value to organizations, resulting in improvements in the delivery of their final products and services.

REFERENCES

1. Miles RE, Snow CC, Meyer AD, Coleman HJ (1978) Organizational Strategy, Structure, and Process. Acad Manag Rev 3:546–562. doi: 10.5465/AMR.1978.4305755.

2. Rainey HG, Backoff RW, Levine CH (1976) Comparing Public and Private Organizations. Public Adm Rev 36:233–244. doi: 10.2307/975145.

3. Boyne GA (2002) Public and private management: what's the difference? J Manag Stud 39:97–122. doi: 10.1111/1467-6486.00284.

4. Hvidman U, Andersen SC (2014) Impact of performance management in public and private organizations. J Public Adm Res Theory 24:35–58. doi: 10.1093/jopart/mut019.

5. Murray MA (1975) Comparing Public and Private Management: An Exploratory Essay. Public Adm Rev 35:364–371.

6. ABNT (2018) ABNT NBR ISO 31000: 2018. Gestão de Riscos - Diretrizes. Associação Brasileira de Normas Técnicas, segunda edição, p. 17.

7. Brasil (2016) Instrução Normativa nº 01/2016. Ministério do Planejamento Orçamento e Gestão, Controladoria Geral da União, Brasília, DF.

8. COSO (2004) Enterprise Risk Management: Integrated Framework. 136.

9. Brasil (2017) Manual de gestão de integridade, riscos e controles internos da gestão - GIRC, 1.2. Ministério do Planejamento, Desenvolvimento e Gestão, Brasília, DF.

10. Brasil (2016) Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - MGR-SISP, 2a. ed. Ministério do Planejamento, Desenvolvimento e Gestão, Brasília, DF.

11. Power M (2009) The risk management of nothing. Accounting, Organ Soc 34:849–855. doi: 10.1016/j.aos.2009.06.001.

12. Power M (2004) The risk management of everything. J Risk Financ 5:58–65. doi: 10.1108/eb023001.

13. Schiller F, Prpich G (2014) Learning to organise risk management in organisations: what future for enterprise risk management? J Risk Res 17:999–1017. doi: 10.1080/13669877.2013.841725.

14. Ferreira ABH (1986) Novo dicionário da língua portuguesa. 2a. ed. Rio de Janeiro: Nova Fronteira, p. 726.

15. Brasil (2014) Governança Pública: referencial básico de governança aplicável a órgãos e entidades da administração pública e ações indutoras de melhoria. Tribunal de Contas da União – Brasília: TCU, Secretaria de Planejamento, Governança e Gestão, p. 96.

16. IBGC (2017) Gerenciamento de Riscos Corporativos: Evolução em Governança e Estratégia. IBGC, São Paulo.

17. Andersen TJ (2010) Combining central planning and decentralization to enhance effective risk management outcomes. Risk Manag 12:101–115. doi: 10.1057/rm.2009.13.

18. HM Treasury (2009) Risk Management assessment framework: a tool for departments. 38.

19. U.S. (2016) Risk Management. United States - Government Accountability Office. Homeland Security. on-line.

20. Canada (2010) Framework for the Management of Risk. Treasury Board of Canada Secretariat. 10.

21. Brasil (2013) Gestão de riscos de segurança da informação e comunicações - GRSIC, 1a. ed. Presidência da República - Gabinete de Segurança Institucional - Departamento de Segurança da Informação e Comunicações, Brasília, DF.

22. Hillson D (2016) The Risk Management Handbook: A practical guide to managing the multiple dimensions of risk. KoganPage, London.

23. COSO (2017) Enterprise Risk Management. Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission: p. 202.

24. ABNT (2012) ABNT NBR ISO 31010 Gestão de Riscos - Técnicas para o processo de avaliação de riscos. Associação Brasileira de Normas Técnicas.

25. OGC (2010) Management of Risk : Guidance for Practitioners. Office of Government Commerce - Axelos, London.

26. Brasil (2017) Manual de gestão de integridade, riscos e controles internos da gestão - GIRC, 1.2. Ministério do Planejamento, Desenvolvimento e Gestão, Brasília, DF.

27. Keeling R (2002) Gestão de projetos: uma abordagem global. São Paulo: Saraiva.

28. Brasil (2016) A análise de cenários e o planejamento estratégico. Portal da estratégia - Secretaria de Política e Integração. Ministério dos Transportes, Portos e Aviação Civil.

29. Miranda RFA (2017) Implementando a gestão de riscos no setor público. Belo Horizonte: Fórum, p. 181.

30. Michel MH (2009) Metodologia e pesquisa científica em ciências sociais. São Paulo: Atlas.

31. Gil AC (2009) Estudo de caso. São Paulo: Atlas.

32. Creswell JW (2010) Projeto de pesquisa: métodos qualitativo, quantitativo e misto. Porto Alegre: Bookman: Artmed.

33. Yin RK (2016) Pesquisa qualitativa do início ao fim. Porto Alegre: Penso.

34. Cauchick Miguel PA (2007) Estudo de caso na engenharia de produção: estruturação e recomendações para sua condução. Production, 17(1), 216-229.

35. Sant'Ana TD et al. (2017) Plano de desenvolvimento institucional – PDI: um guia de conhecimentos para as Instituições Federais de Ensino. Livro Eletrônico - E-BOOK.

Appendix I - Questionnaire

A questionnaire was developed to measure the level of maturity and adherence to risk management practices in organizations, which was divided into four stages:

1. Identification of the respondent - the person in charge of risk management, in which case it was desired to collect information regarding risk management; or a participant who was not responsible for risk management in the organization, in which case it was desired to collect the perception regarding risk management;

2. Application of the specific questions on risk management - answered by those responsible for risk management;

3. Collection of organizational information - regarding the execution of the work and perceptions of all employees on risk management;

4. Collection of information from respondents - such as the contact (email, phone) to receive the analysis results.

Prezado(a) Sr.(a),

Dear Sir/Madam,

Organizational risk management is a way/process to assist managers in achieving the goals of an organization. For the Public Administration, practices related to risk management are defined in Joint Normative Instruction MP/CGU nº 01/2016, which completed one year of validity on 05/10/2017.

This questionnaire is part of the project developed by the R & D Center for Excellence and Transformation of the Public Sector (NExT/UnB) at the request of the National Forum of Pro-Rectors on Planning and Administration of Federal Institutions of Higher Education (FORPLAD/IFES), and supported by the National Association of Leaders of Federal Institutions of Higher Education (ANDIFES), the National Council of Institutions of the Federal Network of Professional, Scientific and Technological Education (CONIF) and the Secretariat of Professional and Technological Education (SETEC/MEC). Therefore, this research aims to carry out an independent evaluation of organizational risk management in federal educational institutions and other public administration bodies.

We kindly ask you to respond to the following questionnaire. Please register your answers with the utmost rigor and truthfulness. The estimated response time is 20 minutes.

Your participation will be of great importance for the construction and dissemination of knowledge about levels of effectiveness of risk management practices in the public service.

The questionnaires completed and submitted by 6/20/2017 will be considered part of the project analysis, and they will receive a response regarding the maturity level of the organization's risk management compared to the average of the other participants.

To receive the results of this survey, please enter your e-mail address at the end of the questionnaire. The results will be released without identifying the respondents.

Sincerely,

Coordination of the ForRisco Project (NExT/UnB)

1. Preliminary questions
This section contains questions to define the respondent profile.

Question	Response options
1. Has your institution already defined a committee and/or those responsible for risk management?	Yes, No, I do not know the answer.
2. Are you a member of this committee and/or are you responsible for risk management at your institution?	Yes, No.

2. Questions about corporate risk management
This section contains questions about corporate risk management.

For these questions, please inform your organization's current situation, ranging from "Yes, totally", "Yes, partially", "Yes, minimally" and "No, absent". If the item is not applicable to your environment or you do not want to respond to the item, check the "N/A (Not applicable)/I do not wish to respond" option.

Principles	Item
Alignment of your institution's risk management with its strategic objectives	Have the objectives of the organization or activities in question been clearly documented prior to the identification of risks?
	Has the risk analysis been conducted taking into account the organization's objectives and the objectives of the activity?
	Are the organization's objectives revised when new risks are identified?
	Are changes in objectives considered and reflected in changes in risk policy and strategy?
Adequacy of risk management to the context of the institution	Have analyzes, external to the organization's environment, projects, program or operation (e.g., using PESTEL, stakeholder analysis, brainstorming technique, scenario planning, SWOT) been carried out?
	Is there a clearly defined process for monitoring and reassessing the context of risk?
	Is there a preliminary definition of who (department/unit) will be the owner of certain categories of risk at first?
	Is there a risk management policy that explicitly describes how risk intervenes in the organizational context (comprehensive, pertinent, feasible, and followed)?
Engagement of your institution's stakeholders in risk management	Are the stakeholders' perceptions, attitudes, and behavior considered in the risk identification process?
	Is the acceptance of risk levels discussed or negotiated with stakeholders appropriately?
	Is there currently a (financial) reserve fund mechanism for agreed risk levels?
	Does the organization formally establish a record on how to avoid the mitigation (understatement) of high impact/ probability risks or overstatement of low impact/probability risks?
Existence of a well-defined risk management process	Is a risk management policy used for the organization in question?
	Are there tools and techniques available and appropriate for risk management?
	Is a formal channel used to assign responsibility to senior management for risks that exceed tolerance?
	Is formal communication used, by senior management, to all key stakeholders of the institution about their risk management responsibilities?

Decision-making based on information resulting from risk management	Are indicators regularly reviewed by decision makers for corrective action?
	Is a defined routine used to generate periodic reports on how risk management is being carried out in your institution?
	Does senior management regularly evaluate the risk map and financial implications in your institution, programs, projects or operational units?
	Is the level of risk response commensurate (proportional, appropriate) with the level of risk (e.g., high risks have better-elaborated actions)?
Facilitation for achieving continuous improvements	Is there a responsible person or team to improve risk management in your institution, programs, projects, or operations?
	Are the practices reviewed based on maturity models to determine the level reached (current/present) and the corresponding benefits that can be expected (future)?
	Is the effectiveness of risk responses monitored and reviewed?
	Is a defined format, structure and content used to present review actions regarding risk treatment?
Creating a Collaborative Culture in Risk Management	Is good risk management stimulated by top management and acknowledged with some kind of stimulus/reward?
	Is there a process of orientation, induction, and training on risk management for its employees, including senior management?
	Are good risk management practices shared at the institution regularly?
	Does senior management encourage a climate of trust so that risks can be openly discussed and shared without fear?
Obtaining measurable values associated with risk management	Are measurements associated with risk management performance used?
	Is a trend analysis developed based on risk management?
	Is there management evidence using trend analysis data to drive future improvements?
	Can the institution demonstrate the return on investment obtained from the development of risk management?

This section has open-ended questions about the risk management methodologies adopted and a scale from 1 (Lowest) to 5 (Highest) containing the frequency with which the external workforce is contracted.

Question	Response type
Indicate the methodologies, techniques or risk management artifacts used by your institution.	Open answer
How often do external auditors and/or external consultants contribute to managing the risks of your institution?	Scale from 1 to 5

3. Questions about the organization and employees
This section contains questions about your institution and employees.

Affirmative/ Question	Item	Response type
Indicate your degree of agreement with the following sentences:	The mission, vision, and values of my institution are formulated clearly, without ambiguity.	Strongly disagree; Partially disagree; Neither agree nor disagree; I agree partially; I totally agree; N/A/Do not wish to respond
	The mission, vision, and values of my institution are formalized and communicated internally and externally.	
	The sum of the goals to be achieved reflects the results that the organization wishes to achieve.	
	Performance measures for my institution are clearly related to its objectives.	
Indicate the level of your influence on the decisions of the senior management of your institution.	Strategic decisions (e.g., development of new products or services, disinvestment of specific products and/or services, strategies of your unit).	I have every influence; I have partial influence; neither I nor my superior have influence; my superior has partial influence; my superior has every influence; N/A/Do not wish to respond
	Investment decisions (for example, moving to a new building, renovating buildings, roads or other property, buying and implementing new information systems).	
	Decisions on internal processes (determination of project budgets, definition of priorities, contracts with external suppliers).	
	Decisions relating to organizational structures (change in information structures, hiring/firing of staff, compensation, skills and career profiles, change in committee structures).	

To what extent do you agree with the following statements about your institution's performance measures?	My institution has performance measures that indicate the quantity of products or services provided.	Strongly disagree; Partially disagree; Neither agree nor disagree; I agree partially; I totally agree; N/A/Do not wish to respond
	My institution has performance measures that indicate how operationally efficient it is.	
	My institution has performance measures that indicate the satisfaction of the public served.	
	My institution has performance measures that indicate the effectiveness of its results.	
What is the importance of the following performance metrics for your total compensation (e.g., career, salary, etc.)?	The importance of "quantity metrics" in my institution is ...	Completely irrelevant; Slightly relevant; Moderately relevant; Important; Very important; N/A/Do not wish to respond
	The importance of "efficiency metrics" in my institution is ...	
	The importance of "metrics of attended public satisfaction" in my institution is ...	
	The importance of "outcome metrics" in my institution is ...	
Compare your institution's performance with similar ones (or compatible) in the following items:	In the quantity or amount of work produced.	Very below average; Below average; Average; Above average; Very above average; N/A/Do not wish to respond
	In achieving the goals of production and service.	
	In the quality or precision of the work produced.	
	In the number of innovations or new ideas generated by the units.	
	In operation efficiency.	
	In reputation with regard to excellence in work.	
	In the moral conduct of employees.	

This section contains open questions about respondents' risk perception.

Question	Response type
Justify the importance of risk management for achieving results for your institution.	Open response
In your perception, what are the main challenges, difficulties, and limitations for effective implementation and realization of risk management in the institution?	Open response

4. Identification of the respondent

Questão	Tipo de resposta
Genre	Male; Female; Other (please specify)
What is your age (years)?	From 1 to 100
What is the highest level of education you have completed?	Response
In what Brazilian state were you born?	List with the 27 States and an option Other.
In what Brazilian state do you work?	List with the 27 States and an option Other.
Profile of your current position	Manager (e.g., secretary of state, director, coordinator, rector, pro-rector, advisor, etc.); Technical (e.g., analyst, auditor, professor, etc.)
Institution/body (Place of origin)	Open response
Institution/body (Place of performance - work)	Open response
Time of professional experience (years)	1 to 5; 6 to 10; 11 to 15; 16 to 20; 21 to 25; 26-30; above 30
Approximately how many people work in your institution?	Open response
After completion of the project involving this research, the results of this questionnaire will be disclosed to identified respondents. If you wish to receive it, please inform us your email.	Open response
If you have any suggestions, comments or criticisms about this survey, use the following comment field:	Open response

Appendix II - Risk recording form

Risk recording is the main component of risk management and should contain a set of information to enable monitoring and management. Records have a characteristic of accumulating the best information over time, allowing them to be updated to convey accurate communication. The plans shall be drawn up taking into account the set of information present in the risk record. In the implementation of the plan, risk recording should allow the control and monitoring of these risks individually. The following is a brief description of its main components:

Table 25 - Items for the risk recording form

Item	Detailing
Risk Identifier	Text identifier of the risk associated with a single sequential number. It is suggested the definition of the title according to the suggestion Cause-Risk-Consequence.
Type of risk	Risks should be classified as "Threat" when they negatively affect the environment, or "Opportunity" when they provide positive chances for the institution.
Risk category	Risks should have the following classification: - Strategic, when there is the possibility of affecting the entire organization; - Operational, when they affect only part of the organization; - Budget, when they are related to financial aspects; Reputation, when they influence the image of the organization; - Integrity, when they affect honesty and ethics; - Fiscal Risk, when they influence fiscal and accounting issues; and - Compliance when they are related to compliance with laws and regulations.
Risk Description	Details of the risk containing information such as Event/Cause - Risk - Effect/Consequence and other relevant information.
Department/Unit/Sector	Department most affected by the risk. Usually, the manager of this department/unit/ sector will be the owner of the risk.
Risk status	In short, the risk may be active - being monitored and/or treated - or closed.
Survey date	Date information that represents the day the risk was identified.
Surveyed by	Person responsible for identifying the risk.
Proximity	Time interval in which the risk can be materialized.

Expected value of treatment for each risk	Calculation that represents an estimate of the financial value for the treatment of a risk.
Risk response option	Different risk responses to be adopted by the organization. For the negative risks (Threats), the following responses were proposed: • avoid the threat; • reduce the threat; • transfer the risk, and • accept the risk. For the opportunities, the following responses were proposed: • share the risk; • explore the opportunity; • improve the opportunity; and • accept the risk.
Stage	Current status of the treatment, according to the process guide. For simplification, the stages "Context identification", "Risk identification", "Risk estimation" and "Risk assessment" were consolidated in a single stage called "Identify and evaluate risk". The stages "Plan treatment" and "Implement plan" were maintained.
Risk owner	The main responsible for coordinating all risk actions.
Risk agent	Responsible for carrying out risk actions.
Probability	Chance of occurrence of the risk. This scale ranges from 1 (least likely) to 5 (most likely).
Impact	Represents the result of a particular threat or opportunity actually occurs. This scale ranges from 1 (Lighter) to 5 (Most severe).
Closure date	Date the risk was closed.
Annexes and external links	These functionalities have been added to enable (1) the consolidation of information into a single record and (2) the relationship with other components such as Risk Treatment Plans and other information.

Source: M_o_R (2010), MGP-SISP (2016), with adaptations

Appendix III - Questionnaire on risk management in public sector organizations

1. Does this institution have a defined Risk Management Policy? If yes, present the historical context of the policy.

2. Who participates in the process of formulating and implementing this policy?

3. What are the stages of policy formulation and implementation? Describe all of them.

4. Point out the responsibilities and tasks of each participant in the stages of policy formulation and implementation.

5. How does this organization set the external context for risk management?

6. Who is responsible for performing this task (s)?

7. Is one or more tools (software, methods, etc.) used to identify external threats or opportunities to the organization? If so, which ones? If not, how does this process work?

8. How does the process of defining strategies for risk management take place?

9. Is there a fragmentation of this process of defining strategies through objectives, targets, and indicators? Could you exemplify?

10. Who is responsible for the strategy-setting process?

11. How are these strategies disseminated throughout the organization?

12. Has the organization established the internal context of risk management? How is it done?

13. Who is responsible for the internal context? Describe your duties.

14. Is there validation of the objectives proposed in the internal context stage?

15. Describe the stages or activities for effective risk management in this organization.

16. Point out topics and explain the methods used to identify and assess risks.

17. In the planning stage for risk treatment, how are the identified risks recorded?

18. In the stage of implementing risk treatment, point out the "risk owner" and the "risk agent". Then explain how the organization establishes the Risk Response Plan.

19. How long does the risk management policy take to be re-evaluated in this institution?

20. Describe how the reassessment process of this policy works.

21. Does the institution conduct a maturity assessment? How does it work?

22. Is there an improvement plan for risk management in the organization? Describe it.

23. Describe how communication and/or disclosure of new policies within the institution works.

24. Does the organization use methods or techniques to measure the risk assessment process?

25. How do risk monitoring and control process take place in this organization?

Table 26 - Interpretation of the level of maturity of risk management in public organizations

Stages of the implementation of risk management	Guiding Questions
1. Define policies	1 – 2 – 3 – 4
2. Establish the external context	5 – 6 – 7
3. Define the strategies for risk management	8 – 9 – 10 – 11
4. Establish the internal context	12 – 13 – 14
5. Conduct risk management for activities	15 – 16 – 17 – 18
6. Reassess the policy - maturity level	19 – 20
7. Assess the maturity of the organization	21 – 22 – 23 – 24 – 25

GLOSSARY

Acceptance
A risk response. That means that the organization accepts the chance that the risk will occur with all its impact on the objectives if it happens. Thus, a contingency budget will be required if the risk materializes.

Amplify, enhance
Type of response to positive risks (opportunities) that seeks to increase the probability and/or impact on making the situation more feasible.

Benefit
The measurable improvement of a result that has been perceived as an advantage for one or more stakeholders.

Avoid
Type of risk response that seeks to eliminate the threat by making the situation right. Example: do not collect credit card information on a system to prevent data leakage. Thus, the user will always have to inform their data, and nothing will be retained, avoiding this leakage.

Explore
Type of positive risk response (opportunity) that seeks to transform an uncertain situation into certain.

Risk Management
Systematic application of policies, procedures, methods, and practices in identification and evaluation tasks, and consequently in the planning and implementation of risk responses. Provides a disciplined environment for proactive decision-making.

Impact
Effects produced by events (threats and/or opportunities) or identified risks.

Key Performance Indicator (KPI)
A performance measure that is used to help the organization define and assess how successful it is as it moves toward its organizational goals.

Early Warning Indicators (EWI)
A leading indicator for an organizational goal that is measured by a KPI.

Maturity level
An evolutionary stage defined towards the achievement of a mature process. Five levels are usually cited: initial, repetitive, defined, managed, and optimized.

Opportunity
An uncertain event that could cause a favorable impact on goals or benefits.

Proximity
The temporality of the risk (e.g., the occurrence of the risk) will occur at a specific time, and the severity of its impact will vary depending on when it occurs.

Result
The result of the change, usually affecting behavior or real-world circumstances. The results are desired when the changes are designed. They are reached when activities reach the outcome in the effect of the change.

Risk - MOF
An uncertain event or set of events that, if they occur, will affect the achievement of the objectives. Risk is measured by a combination of the probability of the occurrence of a threat or opportunity and by the magnitude of its impact on the objectives.

Expected treatment value
The approximate monetary value for the treatment of a given risk.

Credits

Coordination and content
R&D Center for Excellence and Public Sector Transformation

Design
Sofia Ruiz Zapata
Gustavo Tognetti Oliveira Lima
Ana Clara Sousa de Matos
Jéssica Caixeta Maranhão

Revision
Sandra Regina Martins

This book was printed with a drawing of 500 Copies
in March 2020, in the city of Brasília, DF.

Get to know our other projects

next
Universidade de Brasília

www.next.unb.br

ForRisco

2nd edition

ForRisco:
risk management in
public institutions in practice

FOR Platform