Reference Information Model for Risk Management in Corruption and Related Offenses

Filipe Miguel da Cunha Semanas

Department of Engineering and Management, Instituto Superior Técnico, 2016

Abstract

In 2009, *Conselho de Prevenção da Corrupção* (**CPC**) requested the conception of a risk management plan for corruption to all organizations somehow involved in the management of public assets. [1]

In the five years that followed such recommendation, **CPC** conducted an analysis about the implementation of those plans over the targeted organizations. It was concluded that those plans are useful tools in preventing corruption. However, it was also noticeable a significant heterogeneity among all those risk management plans; as in only a small percentage of said plans, it was utilized any perceived formal methodology. [2]

Hence, the relevance of a reference model for risk management and, therefore, for this project. In it, it is suggested a reference risk management framework for corruption and, in order to validate the recommended model, said model was applied to real-life cases related to organizations in three distinct fields of work: **INCM**, **IST** and **LNEC**.

It was concluded that the resulting framework can indeed provide added value in preventing corruption. Moreover, as this is intended to be a reference framework, following these recommendations could ensure a greater homogeneity among risk management plans.

Keywords: Risk Management, Corruption, Framework, Inductive Reasoning, Risk Register, ISO 31000

1. Introduction

According to *Conselho de Prevenção da Corrupção* (**CPC**), the activity of managing public assets should follow a set of ethical principles, and corruption is a clear violation of such values. Therefore, on the July 1st 2009, **CPC** approved a recommendation that asked all organizations involved in the aforementioned activity to elaborate risk management plans in order to prevent corruption. [1]

As of 2014, about a thousand organizations had already developed their own risk management plan for corruption and related offenses; however those plans were very heterogeneous and only 41,2% of

those organizations followed any perceived formal risk management methodology. [2]

Therefore, the main goal of this dissertation is to propose a reference information model for risk management in corruption; one that may be used by all organizations inside the domain of said problem.

In **Figure 1,** it is shown the methodology that was used to accomplish said goal, and the structure of this document is based upon it.

Figure 1 – Methodology used

In chapter **2**, it will be shown a literature review over risk management.

Chapter **3** finds itself divided in three parts. It starts by analyzing the case of *Metro Lisboa*, then analyzes the *risk register* tool and, in the end, it is explained the process of validation for the proposed model.

In chapter **4**, it is presented the result of this work and, to top it off, in chapter **5**, this work is concluded with a balance of what has been accomplished, its relevance for organizations, and how this work can be a foundation for other engineering projects n the future.

2. Literature Review

2.1. ISO 31000 Family of Standards

The ISO 31000 standard, as well as the ISO Guide 73 and the ISO 31010 standard, are commonly referred to as the ISO 31000 family of standards.

The **ISO** standard presented in *ISO 31000: Risk Management – Principles and Guidelines* establishes a number of principles and guidelines for a more efficient risk management in an organization. As with most developed countries, Portugal has already adopted this standard as its official national risk management standard. Whether or not a given organization already has implemented risk management, the ISO 31000 standard is still applicable. [3]

In **Figure 2**, it is shown: (1) the eleven principles of risk management according to the ISO 31000 standard; (2) ISO 31000 standard's recommendation for the conception of a risk management framework; (3) ISO 31000's standard's recommendation of a risk management process.

ISO Guide 73: Risk Management – Vocabulary presents definitions and vocabulary for risk management which has become the most commonly accepted by both the scientific and the academic communities. ISO Guide 73's purpose is to provide generic vocabulary for all risk management. [4]

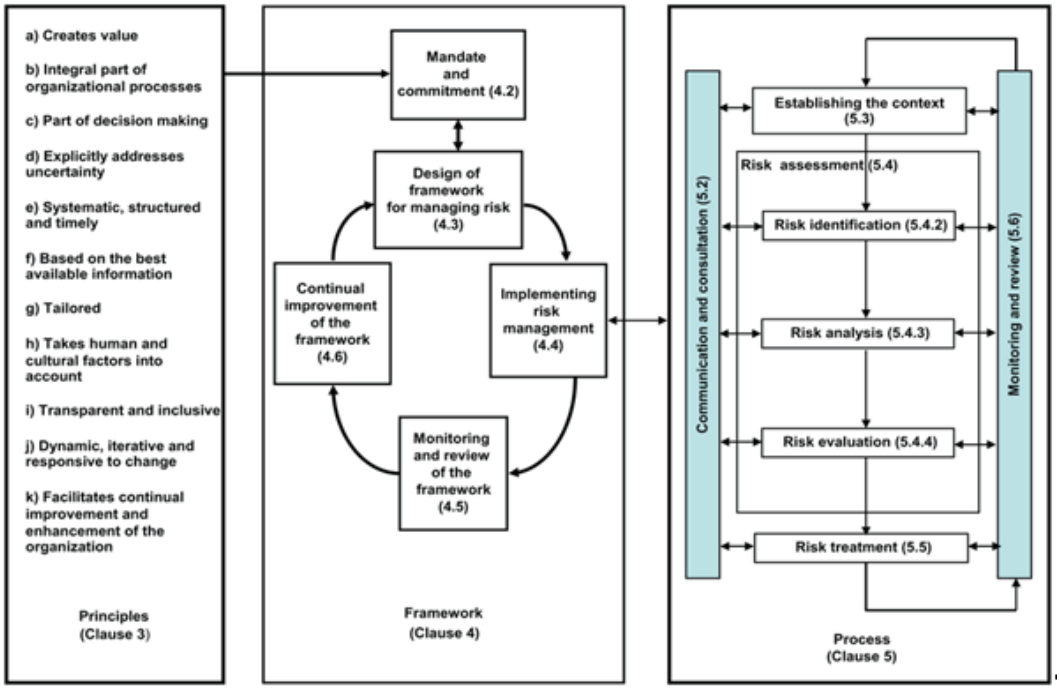

Figure 2 – Relation between the principles of ISO 31000 standard, and recommended risk management framework and process (Source: [3])

The standard shown in the *ISO 31010: Risk Management – Risk Assessment Techniques* document has the goal of assisting organizations in their risk assessment processes. The ISO 31010 standard includes a list of all tools and techniques relevant for risk management, as well as a comparison between them. [5].

2.2. Definitions in the Domain of Risk

According to [4], *risks* are the "effect of uncertainty on objectives", wherein *uncertainty* is considered "the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood".

Risk is usually characterized as an association of an *event* and a *consequence*. Therefore, the *level of risk* is usually determined by combining in some way the *impact* of an event's possible consequence with the *likelihood* of said event occurring.

Another relevant definition in risk management is *risk owner*, which is the person or organization that is held accountable for a given risk. There is also the term *control*¸ that refers to risk-modifying measure. [3] [4]

Finally, in [4], *risk management* itself is also defined. It is considered as a set of "coordinated activities to direct and control an organization with regard to risk ".

3. Analysis and Solution of the Problem

3.1. *Metro Lisboa's* Case Analysis

This case is meant to showcase two main points of interest. First, that *Metro Lisboa* was able to add quality to its risk management plan by following a formal methodology. Second, how by not following the recommendations of the ISO 31000 standard, it becomes difficult or downright impossible to take certain conclusions that

would further benefit the prevention of corruption in that organization.

Starting with the positives, in this risk management plan, it was followed a methodology based on the **ACFE** *Fraud Risk Manual*, classifying fraud risks according to: (1) corruption; (2) conflicts of interest; (3) asset misappropriation; (4) information manipulation. In turn, said categories are split amongst subcategories befitting the organization's context. This adjustment ensures the plan's compliance with Portuguese legislation. In spite of not mentioning the ISO 31000 standard in its risk management plan, *Metro Lisboa* ends up by following a recommendation of the standard by adapting a formal methodology to the organization's own context. [6]

Nevertheless, it can be seen that there are some ISO 31000 recommendations that *Metro Lisboa* does not follow; this leads to a risk register that is useful but still has some flaws worth mentioning (see **Figure 3**). However, the most relevant is related with a risk being an association of an event and a consequence, according to the ISO 31000 standard. But there is no mention of the terms *event* or *consequence* anywhere in *Metro Lisboa's* plan (nor of terms that could be used with a similar purpose). Moreover, most times the organization refers to *risks* in their risk register, it just so happens those *risks* are actually *consequences*.

It can be concluded from this case study that *Metro Lisboa's* risk register is useful and is well organized given the organization's context, which is a plus for their risk management and corruption prevention. However, by not following some key recommendations of the ISO 31000 standard, their plan shows some flaws that end up diminishing the overall quality of risk management in the organization. It is worth stressing that those *flaws* mentioned are common to most anti-corruption risk management plans.

Plano de Prevenção de Riscos de Corrupção e Infrações Conexas no ML			
Identificação dos Riscos	**CR**	**Função ou Atividade**	**Medidas de Prevenção**
1 – Corrupção			
A) Corrupção ativa/suborno, exercida sobre:			
1) Exterior (empresas e indivíduos)	1B	Relacionamento com entidades externas	**(a)** Conforme previsto no Código de Ética e de Conduta os colaboradores do ML têm o dever de observar e de fazer observar os princípios e compromissos do "*Global Compact*" e de denunciar qualquer situação que viole esses princípios. **(a)** As auditorias de certificação são sempre acompanhadas por mais de um elemento do ML e o IPAC pode vir verificar in loco sem aviso a atuação da entidade certificadora. **(a)** Periodicamente existe mudança de empresa para a auditoria às contas anuais. **(a)** Valores comunicados de vendas de títulos são confrontados com os valores registados no sistema de venda. As diferenças são objeto de análise sistemática. **(a)** A generalidade da faturação dos fornecedores é confrontada com os pedidos de compra (contratos e notas de encomenda). **(b)** Auditoria ao sistema de recolha de receitas tarifárias.
2) Colaboradores (incluindo remunerações e compensações não justificadas)	1A	Gestão de recursos humanos	**(a)** As remunerações / compensações estão previstas nos Acordos de Empresa e são processadas pela RHC com base na informação que resulta do registo e controlo de assiduidade. **(a)** Os colaboradores do ML devem promover a salvaguarda dos princípios estruturantes e valores centrais da empresa (Código de Ética e de Conduta). **(b)** Auditoria ao processamento de remunerações e complementos de reforma.

CR - Classificação do Risco: Combinação de Probabilidade (1 = Baixa; 2 = Média e 3 = Alta) e Impacto (A = Baixo; B = Médio e C = Alto).

Medida preventiva do Risco: (a) Implementada; (b) A implementar.

Figure 3 – *Metro Lisboa's risk register*

3.2. Risk Register Models

Nearly all studied organizations used the *risk register* tool in their respective risk management plans for corruption. According to [4], a *risk register* is a "record of information about identified risks". Even though *risk registers* are not mentioned in the ISO 31000 standard, that document still stresses the importance of risk documentation. [3]

Hence, it is tested the possibility of utilizing a risk register as a solution for this problem. The risk register model will depend on the problem's context. A risk register may contain as much information as an organization wishes; however, too many items in a register may lead to an overly complex model for the organization.

Therefore, the design of a risk register may become a challenge where the goal will be the optimization of the register to the point where adding one more item will not make up for the increase in complexity of its model.

By analyzing the ISO 31000 standard and its main concepts, it is proposed a model conceptually similar to the one presented in **Figure 4**.

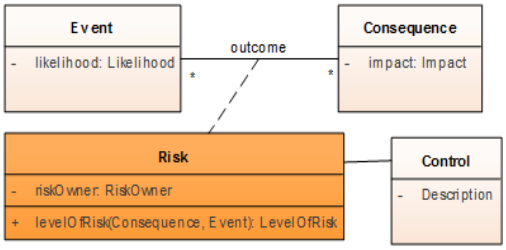

Figure 4 – Initial proposal for a reference risk register model

In said model, a given *risk* is associated to a single *event* and a single *consequence*. There is a *likelihood* of the *event* occurring; and, depending of what the *consequence* is, there will be an associated *impact* on an organization's objectives. A *risk* should also be associated to a *control*. At last, the concept of *risk owner* can be considered as an entity of its own, rather than an attribute of *risk,* as shown in **Figure 4**.

This risk register model is simple as it only contains the fundamental concepts of risk management as recommended by the ISO 31000 standard. Moreover, returning to the example of *Metro Lisboa*'s risk register, it can be observed that said model follows a similar framework, and, in spite of some shortcomings common to most organizations, it is one of the most useful risk registers among Portuguese organizations. Besides, given the context of the problem, it is not justifiable the use of a more complex model.

3.3. Validation of Solution

In the next paragraphs, it is presented the process for validating said solution by applying real-life data into the designed framework.

First, the risks are identified and their correspondent information is presented. That identification is assisted by the use of an attribute that will allow for an easier traceability of each risk in the remainder of this process. An example of such is shown in **Figure 5** by using data from **INCM**'s risk management plan.

Second, those risks are analyzed in order to determine the best way to structure them. The key point in this step of the process is to determine whether there are really *risks* as defined in the ISO 31000 standard or just an *event* or just a

consequence. And, if it really is a *risk*, it still needs to be determined whether it is just one risk (the combination of a single event with a single consequence) or multiple risks (for example, an event with distinct consequences). Also, it is of the utmost importance to determine if the risk belongs or not to the domain of corruption and related offenses. In the absence of explicit information, interpretations of the data must be registered. Again, an example of such is presented in **Figure 6**, by using the same **INCM** data.

Third, taking as reference the results obtained in the previous step, risks are structured in a risk register based on the proposed reference model. It will also be of added quality the addition of *flags* to each risk, event, consequence or control, as that will make for a more accessible risk classification.

The data used for validating the model in chapter **4** came from three organizations with three distinct backgrounds: **INCM** (production of goods/services for the State), **IST** (academic education and research) and **LNEC** (I&D in civil engineering).

4. Proposed Model and Data Structuring

After explaining how the proposed solution was validated, it will be described said reference information model, as seen in **Figure 7**.

That model is conceptually similar to the one presented in **Figure 4**; as a matter of fact, in said figure, it is visible four out of the five entities of the proposed model: *risk*, *event*, *consequence*, *control*. The only meaningful difference between those two models is the positioning of the concept *risk owner.* In the proposed model of **Figure 7**, that concept is considered as an entity of its own (possibility such that had been discussed already in chapter **3.2**).

	A	B	C	D	E	F	G
1	Risco_ID	Risco_Nome	Nível de Risco	Unidade de Negócio	Atividade	Controlos	Responsável_Controlo
2	RR1	Favorecimento de terceiros	Moderado	Compras	Geral	Regulamento de Aquisições.	Todas as áreas DCP
3	RR2	Quebra de sigilo profissional, revelando informações com intenção de obter benefícios	Fraco	Compras	Geral	Regulamento de Aquisições. Plano de Atividades e Orçamento (PAO).	Todas as áreas DCP

Figure 5 – Example of the process' first step

	A	B	H	I	J	K	L
1	Risco_ID	Risco_Nome	Possível evento?	Possível consequência?	Relevante para o contexto?	Análise/Interpretação	Acção Recomendada
2	RR1	Favorecimento de terceiros	Não	Sim	Sim	A existência de favorecimento de terceiros é já por si uma...	Não constitui um risco
3	RR2	Quebra de sigilo profissional,...	Sim	Sim	Sim		Manter/Estruturar

Figure 6 – Example of the process' second step

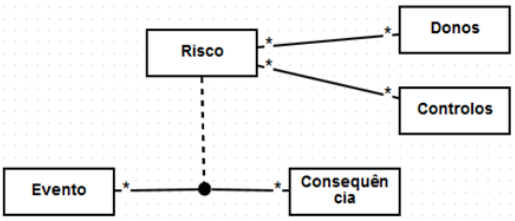

Figure 7 – Proposed reference risk management framework

In **Figure 8**, **Figure 9**, **Figure 10**, **Figure 11** e **Figure 12**, it can be seen the attributes correspondent to each entity in this reference risk register model via the application of said framework to data of **INCM**'s risk management plan.

Risco					
Risco_ID	Risco_Nome	Nível de Risco	Rastreio	Risco_Flags	Legenda de Risco_Flags
R8	Insatisfação das áreas requisitantes por fraca qualidade dos materiais	Fraco	RR7	RD	Risco que se conseguiu estruturar (especifica ou genericamente); não se conseguiu deduzir se pertence ou não à área da corrupção e infrações conexas
R9	Favorecimento próprio via processo de aquisição incompleto	Moderado	RR8	RC	Risco que se conseguiu estruturar de um modo específico; área da corrupção e infrações conexas
R10	Apropriação indevida de bens via processo de aquisição incompleto	Moderado	RR8	RC-Gen	Risco que só se conseguiu deduzir com base na informação disponível e, consequentemente, está estruturado de um modo genérico; área da corrupção e infrações conexas
R11		Moderado	RR9	N-Cq	Nestes casos, não temos um risco já que não foi possível a sua estrutração por indeterminação da consequência do evento respetivo

Figure 8 – Example of information structuring for *Risk*

Evento						
Evento_ID	Evento_Nome	Evento_Descrição	Unidade de Negócio	Atividade	Evento_Flags	Legenda de Evento_Flags
EV7	Fraca qualidade dos materiais		Compras	Compra	DC	Não se conseguiu apurar o contexto do evento (se se encontra ou não dentro do contexto da corrupção e infrações conexas)
EV8	Processo de aquisição incompleto	Processo de aquisição incompleto (escolha fornecedor, solicitação de cotação, análise de propostas, justificação da seleção da proposta aceite, nota de encomenda, guia de remessa, receção do bem, fatura)	Compras	Compra	EC	Evento encontra-se dentro do contexto da corrupção e infrações conexas
EV8	Processo de aquisição incompleto	Processo de aquisição incompleto (escolha fornecedor, solicitação de cotação, análise de propostas, justificação da seleção da proposta aceite, nota de encomenda, guia de remessa, receção do bem, fatura)	Compras	Compra	EC	Evento encontra-se dentro do contexto da corrupção e infrações conexas
EV9	Inexistência de formalização atempada de contratos	Inexistência de formalização atempada de contratos entre as partes detalhando as condições de fornecimento dos bens/serviços	Compras	Compra	DC	Não se conseguiu apurar o contexto do evento (se se encontra ou não dentro do contexto da corrupção e infrações conexas)

Figure 9 – Example of information structuring for *Event*

Consequência				
Consequência_ID	Consequência_Nome	Consequência_Descrição	Consequência_Tipo	ConqEstruturada_Flags
CQ6	Insatisfação das áreas requisitantes			Não
CQ3	Favorecimento próprio		Recebimento indevido de vantagem	Sim
CQ7	Apropriação indevida de bens		Peculato	Sim
CQ8				Não

Figure 10 – Example of information structuring for *Consequence*

Controlo_ID	Controlo_Nome	Controlo_Descrição	Controlo_Tipo	*Notas dos Controlos*
CONT1	Regulamento de Aquisições		Conformidade	
CONT2	C.C.P. - Código dos Contratos Públicos		Conformidade	
CONT3	Plano Económico e Financeiro (PEF)		??	
CONT4	Processo de apoio definido no âmbito da qualidade - Compras		Acesso a informação	

Figure 11 – Example of information structuring for *Control*

Dono_ID	Dono_Nome	Dono_Descrição	*Notas dos Donos*
DONO1	DCP	Direção de Compras	
DONO2	DFI	Direção Financeira	
DONO15	ARH		Surge no Risk Register original mas não é mencionado no plano de gestão de riscos
DONO28	??	Comissão de trabalhadores	Não é mencionado como sendo departamentos específicos no plano de gestão de riscos

Figure 12 – Example of information structuring for *Risk Owner*

Figure 8 shows the attributes of the entity *Risk*. **Risco_ID** is the identifying attribute for each risk, **Risco_Nome** is the name given to said risk, and **Nível de Risco** corresponds to the risk score given to it. The attribute **Rastreio** works as a means to retrace the newly-structured risk to its original case according to the initial plan of the organization that provided said risks.

As previously seen in **Figure 7**, a risk is associated with a single event, a single consequence, controls and risk owners. Therefore, for each risk, it is shown the corresponding entities via theirs' own identification attributes (**Evento_ID**, **Consequência_ID**, **Controlo_ID** and **Dono_ID**). However in the case of **Figure 8**, those camps are hidden. The final attribute left to mention is **Risco_Flags**; each risk presented is associated to one of six possible *flags*: (1) **RC** – risk that was specifically structured; it belongs to the domain of corruption and related offenses; (2) **RC-Gen** – risk that was deduced according to available information (generic structuring); it belongs to the domain of corruption and related offenses; (3) **RD** – risk that was structured (specifically or generically); it was not possible to determine whether it belongs to the domain of corruption and related offenses; (4) **OR** – risk that was structured (specifically or generically); does not belong to the domain of corruption and related offenses; (5) **N-Cq** – there is not an actual risk as it was not determined the consequence of said event; (6) **N-Ev** – there is not an actual risk as it was not determined the event that leads to said consequence.

Figure 9 shows the attributes of entity *Event*. After the aforementioned **Evento_ID**, it is shown **Evento_Nome** which provides

with the name given to said event; **Evento_Descrição** provides a more detailed explanation of what the event is about, if it is believed that **Evento_Nome** doesn't provide enough information. **Likelihood** corresponds to the likelihood of occurrence of said event according to the analyzed organization (in **INCM**, no likelihood was determined), and the attributes **Unidade de Negócio** and **Atividade** give information about the area of the organization where that event is expected to occur. At last, just like for the entity *Risk,* an event is also associated with certain *flags*; in this case, there are three possibilities: (1) **EC** – event belongs to the domain of corruption and related offenses; (2) **DC** – it was not possible to determine the context of the event (that is, whether or not it belongs to the domain of corruption and related offenses); (3) **Outro** – event does not belong to the domain of corruption and related offenses.

Figure 10 shows the attributes for the entity *Consequence*. Conceptually, **Consequência_ID**, **Consequência_Nome** and **Consequência_Descrição** serve the same functions of their corresponding attributes in *Event*. The same happens for the corresponding attributes for *Control* and *Risk Owner*, as seen in **Figure 11** and **Figure 12**. Back to *Consequence,* **Impacto** is meant to show the impact of a given consequence on the organization's objectives (in **INCM**, no impact was determined).

The attribute **Consequência_Tipo** has the goal of inform what were the crimes from the Portuguese Criminal Code that are related to a given consequence. However, in some cases, there may not be a consequence, or there may be a consequence associated to an undetermined crime. The attribute **ConqEstruturada_Flags** allows for a classification of consequences depending on whether or not it was identified any crime in the Criminal Code associated to said consequence.

To conclude, in **Figure 11**, it is shown as well the attribute **Controlo_Tipo** for *Control*; the goal of said attribute is to typify each control according to the information available in *Transparency International*'s anti-corruption glossary (which is available in https://www.transparency.org/glossary).

5. Conclusions

After verifying the differences between the multiple risk management plans requested by **CPC**, and their shortcomings, it was concluded that there was the need to design a reference risk management framework for Portuguese organizations.

After analyzing several risk management plans, it was concluded that applying a formal risk management methodology and ensuring its compliance with the ISO 31000 standard can help prevent corruption. Therefore, given the context of the problem, it was proposed a model conceptually similar to the one in **Figure 4**. Through a three-step process, it was possible to apply said model to real-life data from three distinct organizations (**INCM**, **IST** e **LNEC**), and therefore validate the problem's solution.

Even though that model is this work's main output, it is worth stressing the process that was utilized to validate it, as said

process allowed for the transfer of data from multiple organizations into a reference model. By validating it, it was concluded this process can be used by an organization, alongside the proposed model.

Finally, the *flags* that were designed for this reference model are meant to add value to risk management in an organization, but they are not considered as being essential to said model. Therefore, even though their use comes as recommended for a better organization of the information, these *flags* can be adapted according the context of the organization. The *flags* shown in this work should work as guidelines for conceptually similar attributes that can add value to risk management without increasing too much the complexity of the organization's risk management framework.

6. References

[1] Recomendação do CPC de 1 de Julho de 2009 sobre *planos de gestão de riscos de corrupção e infrações conexas*. Conselho de Prevenção da Corrupção. Lisboa.

[2] Conselho de Prevenção da Corrupção. (2015). *Prevenir a corrupção no Setor Público: Uma experiência de 5 anos.* Maia, A.J. Lisboa.

[3] ISO 31000:2009. *Risk management – Principles and guidelines.* International Organization for Standardization. Genève.

[4] ISO Guide 73:2009. *Risk management – Vocabulary.* International Organization for Standardization. Genève.

[5] ISO 31010:2009. *Risk management – Risk assessment techniques.* International Organization for Standardization. Genève.

[6] Metro Lisboa. (2014). *Plano de Prevenção de Riscos de Corrupção e Infrações Conexas.* ML. Lisboa.