University of Minho

School of Engineering

Melise Ribeiro Cavallare

Information Systems Security Governance Evaluation in the Portuguese Local Public Administration

Master's Thesis
Master Program in Information Systems

Work produced under the supervision of
Professor Filipe de Sá-Soares
Professor Delfina Soares

September 2020

University of Minho

School of Engineering

Melise Ribeiro Cavallare

Information Systems Security Governance Evaluation in the Portuguese Local Public Administration

Master's Thesis
Master Program in Information Systems

Work produced under the supervision of
Professor Filipe de Sá-Soares
Professor Delfina Soares

September 2020

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

Licença concedida aos utilizadores deste trabalho

Thanks

I would like to thank God, for my life and my health. Also for making me a curious person, that embraces changes and is very stubborn and determined. Without it I wouldn't have been able to do half of what I've done in my life so far.

Moreover, I would like to thank my family. Mostly my mom Marcia and dad Marcello for everything they have done for me, from my education, the extracurricular activities, for being able to explore the world; and for their unconditional support and understanding through every step on the road. You guys have always been my inspiration and I admire everything you've done. I couldn't be more proud of the parents I have, for everything you taught me in life. I will always be thankfull and gratefull for all of your love. Know that my love for you is beyond reach.

I also would like to thank my sister Marjorie, eventhough we have very different personalities. I am very happy she found herself, because I always knew she was capable of doing great things. She taught me, even without ever realizing, how to be fearless and to get out of the comfort zone. Therefore, I admire her and she will always be an inspiration. Along with her, my thanks goes to the new additions to our family; my brother-in-law Hugo and their little princess Maria Helena, thank you for the joy you guys brought to our family.

Additionally, I would like to thank my friends. The old ones, that I had to leave behind. Thanks for understanding that this meant that I had to be miles apart and missing out on many things, but you will always be in my thoughts and my heart. And to the new ones, particularly Catarina and Filipa, I am thankful for having in my life. That accompanied and helped me through this journey, and will remain with me also in my thoughts and heart, on my next journey.

Lastly, I would like to thank my advisors Professor Filipe Sá-Soares and Professor Delfina Soares, for being such great human beings, a wonderful team and for demonstrating such work ethics. For helping me whenever I needed help, and guiding me throughout the whole process. Also for pushing me forward, with their strict delivery times and structure, their insight and advice. Eventhough I may have failed to deliver at times, they never gave up on me and kept pushing me forward; I never once felt alone in this journey. Without them I wouldn't be able to produce this work. So, my deepest thank you for believing in me and for all your time and care.

STATEMENT OF INTEGRITY

I hereby declare having conducted this academic work with integrity. I confirm that I have not used plagiarism or any form of undue use of information or falsification of results along the process leading to its elaboration.

I further declare that I have fully acknowledged the Code of Ethical Conduct of the University of Minho.

Title: Information Systems Security Governance Evaluation in the Portuguese Local Public Administration

Abstract:

In the recent years, an increase focus in the area of Information Systems Security Governance (ISSG) can be observed. Largely because of the dependency organizations have on information systems and the risks that may affect those systems. Should a failure occur, in the information security measures for these systems, the organization's reputation can be directly impacted.

Those information security concerns and a rise in regulatory requirements are particularly interesting within the context of these study, which evaluates the ISSG in Portuguese Local Public Administration. This context is derived from a shift in perspective, from previous studies from Lopes and de Sá-Soares [2010] and Lopes and Oliveira [2016], that shown an slow adoption of Information Systems Security policies by the Portuguese City Halls.

The methodology that will be used in this study is the Design Science Research (DSR) strategy, because considers as artifacts, the instrument creation and the methodological guide. The process surrounding the instrument development, from the problem awareness to the conclusion, is included as a subject for this research. The DSR also presents clear cycles, processes and guidelines; and is largely used in the Information System (IS) field, due to the high regard for evaluation.

The propose set of this study is the development of an instrument to evaluate the ISSG in Local Public Administration (more precisely, to evaluate ISSG of all three hundred and eight City Halls across the Portuguese territory, including the autonomous regions of Azores and Madeira). Alongside a secondary artifact will be constructed, which consists of a methodological guide that will help with the implementation of said instrument.

Keywords: Information Systems Security Governance; City Hall; Portugal; Local Public Administration.

Título: Avaliação da Governação da Segurança de Sistemas de Informação na Administração Pública Local Portuguesa

Resumo:

Nos últimos anos, tem vindo a ser observado um crescente interesse na área da Governação da Segurança dos Sistemas de Informação (GSSI) devido, em grande parte, à dependência que as organizações têm sobre os sistemas de informação e os riscos inerentes aos mesmos. Caso ocorra uma falha nas medidas de segurança da informação desses sistemas, a reputação da organização pode ser diretamente afetada.

Estas preocupações com a segurança da informação e o aumento dos requisitos regulatórios são particularmente interessantes no contexto deste estudo uma vez que avaliam o GSSI na Administração Pública Local Portuguesa. Este contexto deriva de uma mudança de perspectiva, verificada em estudos anteriores como o de Lopes e de Sá-Soares [2010] e Lopes e Oliveira [2016], que mostram uma adoção lenta das políticas de Segurança de Sistemas de Informação pelas câmaras municipais portuguesas.

A metodologia que será utilizada neste estudo é a *Design Science Research* (DSR), dado que considera como artefactos, a criação de um instrumento e o guia metodológico. O processo em torno do desenvolvimento do instrumento, desde a consciencialização do problema até à sua conclusão, está incluído como assunto nesta investigação. O DSR também apresenta ciclos, processos e diretrizes claras, que são amplamente utilizados na àrea dos Sistemas da Informação (SI), devido à importância da avaliação.

O objetivo definido para este estudo é a criação de um instrumento para avaliar o GSSI na Administração Pública Local (mais precisamente, para avaliar a GSSI em todas as trezentas e oito Câmaras Municipais do território português, incluindo as Regiões Autónomas dos Açores e da Madeira). Posteriormente será construído um artefato secundário que consiste na elaboração de um guia metodológico, que ajude na implementação do instrumento referido.

Palavras-chave: Governação da Segurança dos Sistemas de Informação; Câmaras Municipais; Portugal; Administração Pública Local.

Index

List of Acronyms

Throughout this document acronyms can be found, their use is common to this knowledge area and due to their high occurrence in the text, thus justifying their substitution. The following list summarizes them alphabetically:

COBIT – Control Objectives for Information and Related Technology

CRP – *Constituição da República Portuguesa* (Constitution of the Portuguese Republic)

DPO – Data Protection Officer

DSI – *Departamento de Sistemas de Informação* (Information Systems Department from University of Minho)

DSR – Design Science Research

EDM – Evaluate, Direct and Monitor processes

GDPR – General Data Protection Regulation

GTAG – Global Technology Audit Guide

ICI – Islands, Coastal and Interior zones

ICT – Information and Communication Technology

IEC – International Electrotechnical Commission

IS – Information System

ISG – Information Security Governance

ISMS – Information Security Management System

ISS – Information Systems Security

ISSG – Information Systems Security Governance

IST – Information Systems and Technology

IT – Information Technology

ITG – Information Technology Governance

NIST – National Institute of Standards and Technology

PA – Public Administration

List of Figures

List of Tables

Information Systems Security Governance Evaluation

in the

Portuguese Local Public Administration

1 Introduction

The present document contains the dissertation report needed as one of the two required deliveries for the conclusion of the Information Systems Masters at University of Minho.

As a starting point for the project, are the difficulties organizations, such as City Halls, face to protect their Information Systems (IS) resources; as does the governance of its security. The city halls Information Systems Security Governance (ISSG) can be considered the central focus for this work, and it will be explained in the next chapter, along with its relevance.

This chapter will provide a brief overview on the subject at hand, the ISSG and its current context in City Halls across the Portuguese territory. After, the objectives for this study will be defined, followed by a quick explanation of the research methodology and ultimately the document structure will be presented.

1.1 Overview

Once the Information Security measures of an organization fails, this failure can directly impact the organization's reputation. Therefore, concerns about information security have become a key issue for the organizations, along with an increasingly amount of regulatory requirements [ISO/IEC 2013].

Furthermore, Dhillon et al. [2007] add that organizations are increasing their dependencies on information systems and so are the risks affecting those systems. Consequently, the organizational members become an extreme important form of defense, similar to a frontline defense. This form of defense is addressed as behavioral security, and can suffer impact from factors such as integrity and structures of responsibility.

Data has shown that many organizations suffered from data breaches such as: use of stolen credentials, backdoor, theft, ransomware, privilege abuse and many others. In Public Administrations from the 21,239 incidents, 239 had data disclosure confirmed, Personal and Secrets both had 41% each of their data compromised [Verizon 2017]. The top three patterns are cyber-espionage, privilege misuse and miscellaneous errors (accounting for more than 80%); those being committed by external (62%) and internal (40%) actors, multiple parties (4%) and partners (2%) and these breaches usually take years to be discovered [Verizon 2017].

Since then, security concerns over the previous problems and the fact that City Halls deals with relevant and sensitive information; and that information is intensively used on a daily basis [Soares et al. 2017]. The government decided to improve the performance of this sector in dealing with information, thus arising the e-governance [Soares 2009].

To Gupta et al. [2017], e-governance is described as the infrastructure and the services that are being offered to the citizens and other institutions through the use of public channels, such as the internet.

As more and more countries develop their e-Governance infrastructure, more issues concerning security and threats of attack emerge. Those issues are related to the e-Governance infrastructure and their services that are being offered via public channels to citizens and other institutions [Gupta et al. 2017]. Their stakeholders face the challenges of loss of government data and breach of privacy and confidentiality of the citizen's data [Gupta et al. 2017].

Since all Portuguese City Halls have websites, and in them, citizens have the ability to retrieve information and request services [Soares et al. 2017]. Therefore the risks for those websites to be susceptible to suffer from a data breach is huge [Verizon 2017, p. 6].

As much as massive cybersecurity breaches have become common, many organizations worldwide still struggle to comprehend and manage those risks and as well as being able to develop resilience to withstand them [PricewaterhouseCoopers 2017].

To safeguard from risks, Information Systems Security Governance has a principle that is to comply with internal and external laws and regulations [ISO/IEC 2013, p. 4; von Solms and von Solms 2009, p. 37].

One of these external directives is the National Institute of Standards and Technology Special Publication (NIST) 800-100, that proposes ways to ensure the implementation of Information Security Governance (ISG) in public bodies. This implementation should be done proactively, in order to apply the appropriate controls at a good cost benefit, while managing the risk. The implementation is also necessary due to the huge dependency on Information Technology (IT) these public bodies have in their daily operations [Bowen et al. 2006].

Another external directive is the ISO/IEC 27014:2013 standard, that focuses on ISG, and their application in an organization. Acting as a guidance, where organizations can assess, direct, monitor and communicate the activities related to information security intrinsic to them. This standard, can also be molded to fit the organization's purpose, objectives, type and size. This tailoring is possible because the standard's principles are written on what the organization should expect (the result), and not by giving specific direction on how it should be implemented [ISO/IEC 2013].

Another framework largely used (because of its best practices) by organizations around the world is COBIT 5 framework. The framework takes a hoslistic view of the organization, which is important while implementing governance. But also, ensures that the needs of the stakeholders are met; determine a balance between options and conditions; certifies that the agreed objectives are achieved; defines a direction according prioritization and decision making; and monitors the conformity and performance against the agreed objectives and directions. It also separates the processes that are specific for Governance from those that are related to Management [ISACA 2012b].[5]

Lastly for internal laws and regulations, some studies have been carried out for a better understanding on how they are being implemented in Portuguese Local Administration.

Lopes and Oliveira [2016] compared the data about the adoption of ISS policies in Portuguese city council's with a study previously carried out in 2010. They realized only an 8% increase during that period, a relatively low number; because only 20% of Portuguese City Council's said to have this measure. These results generated questions about the continuous low adoption of ISS by the Portuguese city council's and emphasized the need for future works to be carried out.

Within the scope of this document and taking into consideration the findings from Lopes and Oliveira [2016] previously mentioned, the premise used in the development of this study is that the slow institutionalization of security policy controls is related to a deficient or inexistent Information Systems Security Governance (ISSG) in city halls across Portugal.

Governance in Information Systems in the Local Public Administration has suffered from various motives such as small IT departments and government plans such as PGETIC that had difficulties achieving their goals [Querido 2014].

Another new regulation they must follow, that started in May twenty-fifth 2018, from the European Parliament, is the General Data Protection Regulation (GDPR) [European Union 2016].

[5] This paragrafh, eventhough is taken from COBIT® 5 and this document was modified in order to use the latest version of COBIT® (COBIT® 2019). The ideas behind it are still relevant, and COBIT® continues to be used as a reference within the governance field. Also, the latest version of COBIT® was created with COBIT® 5 as a base.

1.2 Objectives

The study aims to answer the following research question: “How to evaluate the Information Systems Security Governance of Local Public Administration bodies?”. Derived after an analysis of Lopes and Oliveira [2016] study, which set a premise that a slow institutionalization of security policy controls could be the result of a deficient or inexistent Information Systems Security Governance (ISSG) in city halls across Portugal.

To help answer this research question, is the purpose of this study: where an instrument is set to be developed and validated, which will allow the evaluation of Information Systems Security Governance in the Local Public Administration of Portugal.

Considering the study purpose and the research question, the three main objectives of this dissertation are as follows:

- Characterize the Information Systems Security Governance activity;
- Create an Information Systems Security Governance assessment tool for the Local Public Administration context;
- Create a Methodological Guide for the application of the assessment tool for the Information Systems Security Governance in the Local Public Administration context.

To achieve these objectives, it is the up most importance a rigorous literature review, that is presented in the following chapter, and the research strategy. A brief description of the methods and techniques used in this work is presented in the following section.

1.3 Study Methodology

The last section described the study’s objectives, and their fulfillment leads to the main goal of this investigation. In order to better understand the process, the strategy used to accomplish these objectives, also needed to be explained. Therefore, an approach was defined and is explained in the next paragraphs. Also, the remaining work was established and based upon this approach.

The followed approach used a two-scope strategy that converged; one referred to the research and analysis of the bibliography, the other was about the research strategy of the study.

The first strategy aimed to give context and cover the subject of the study, justifying and contributing to the relevance of the research question.

For the second strategy, in this case the research strategy, the Design Science Research (DSR) was proposed. Vaishnavi and Kuechler [2004] note that this research strategy has a particular interest for the IS field, since there is an extreme concern for a rigorous evaluation.

This strategy results in the creation of a main artifact, an instrument to evaluate the Information Systems Security Governance of Local Public Administration; and a secondary artifact, that is a methodological guide, on how to apply such an instrument. The strategy is composed of three cycles, Rigor, Relevance and Design, that are constituted, respectively by guidelines, process steps and results.

According to Hevner [2007], the Relevance cycle initiates the DSR by giving a context to the study (for instance the problem to be addressed); the Rigor cycle will extract the knowledge from theories and methods serving as a basis for the research, ensuring its innovation; and lastly, the Design cycle is the heart of the project, where the artifact will be constructed, evaluated (creating feedback), then refined for further design, until the desired satisfactory design is achieved.

1.4 Document Structure

Since the aim of this document is to present information, as well as to demonstrate the knowledge that resulted from the investigation carried out to evaluate the ISSG in Local Public Administration, this section describes in short the structure by which the document is composed, and as a short summary of the five corresponding chapters.

Starting out by the present chapter, that gives an introduction about the project's focus, the relevance of ISSG in the actual context of the Local Public Administration and internal to the field of IS, the objectives the study plans to achieve, and a brief description of the methodology used to realize it. While in chapter two the Literature Review is then presented; the main concepts are defined, afterwards Governance is explained and so are their related areas, culminating into Information System Security Governance, that is the focus of the research.

The third chapter presents the problem within the context studied in this project, followed by the methodology that is being used and their corresponding instantiations. Later, the fourth and fifth chapters follows the steps used in DSR, for the creation of the artifacts, from their inception through their conclusion. These DSR steps are separated between these two chapters, where the first one has the steps of Problem awareness, Suggestion and Development up to the concept tree.

While Chapter five has the final part of the Development step (which is the instrument and the methodological guide construction), the Evaluation and the Conclusion steps. Lastly, the sixth chapter synthesizes the deductions obtained from the entirety of the work, such as the contributions, the limitations and the conclusion.

The document is then followed by the appendices, whereas the first one, Appendix A – Literature and Concept Matrices is comprised of four tables; Table 36 represents some of the literature used in this document, where it was researched, and gathered. It also includes the amount of citations, as well as the order number for the concept tables. This table is then succeeded by other three tables, Table 37, Table 38 and Table 39, which represent the concept matrices, separated by scope, derived from the reading process of documents used in the creation of this document.

The next appendix is Appendix B – COBIT® 2019 COBIT Core Model, with an illustration of the forty processes found in the Process Reference Model, which is separated by Governance and Management objectives. Afterwards, in

Appendix C – Portuguese Population by City Hall, the City Halls are characterized by dimension (Small, Medium and Large, depending on their population size), their population, by Island, Coastal and Interior zones and by district and by NUTs.

Then in Appendix D – Portuguese City Hall Election, Political Parties Results, the results from the past City Hall Election[6] is displayed, separated by Political Parties and how many City Hall such parties have. Followed by

Appendix E – Evolution of e-Governance Initiatives in Portugal, that uses a table to depict the initiatives for e-governance in Portugal over the years.

The next appendix, Appendix F – *Estratégia TIC 2020*, is composed of three tables that summarize the structure of the "Estratégia TIC 2020", the first table presents the strategy's axels, measures and actions, while the second and third tables[7] displays, respectively, the governmental areas, its strategic projects and the sectorial plans; and the general activities for each governmental actions specific to measure 01[8] of the axel.

Subsequently, Appendix G – Artifact Construction: Instantiations of Relevant ISSG Documents presents the summary tables of the relevant documents used in this study, detailed on Chapter 2, separated in seven categories. Whereas, Appendix H – COBIT 5 Summary, exhibits the summary table for the older version of COBIT® (COBIT® 5).

[6] The city council's mayoral information was extracted from the portal *"Associação Nacional de Municípios Portugueses*" [Associação Nacional Municípios Portugueses 2017] and verified against the information from the MAI portal "*Eleições Autárquicas 2017*" [Secretaria Geral Ministério da Administração Interna 2017], due to the recent voting (October 1st).

[7] The second and third tables of "*Estratégia TIC 2020*" are presented in Portuguese, since they had no official English versions.

[8] This measure represents the governance measures of this strategy, therefore relevant for this work.

Next, Appendix I – Artifact Construction: Concept Tree versions presents the evolution and finetuning of the concept tree[9], where each version of concept tree is displayed, along with a table that displays the number of their corresponding concept. Additionally, a matrix to clarify the changes between version 1 and version 2, and another table, that compares the changes of version 2 thru 5, is displayed.

In a similar structure, Appendix J – Artifact Construction: Instrument, is presented. Each version of the instrument, from version 0 to version 5, is displayed, along with a matrix crossing the instrument questions with the concept tree version used. To complement, there is a matrix crossing the questions from version 0 with GTAG questions. Ultimately, there is a table comparing the evolution of version 2 thru version 5.

In the subsequent appendix, Appendix K – Instrument Accessory – Translated Version, a translated version of the instrument is presented. This version was created in order to fit the instrument within the environment in which it would be applicable.

Afterwards, Appendix L – Artifact Construction: Methodological Guide presents the methodological guide of the instrument. Which is followed by Appendix M – Methodological Guide Accessory – Instrument V5 Cheat Sheet, that presents an accessory created, a cheat sheet of the instrument version 5, that indicates the value for the answer right next to it, thus, helping in the first part of the global index calculation.

Lastly, Appendix N – Instrument Evaluation: Pretest, shows the pretest created to represent each version of the scenarios, that can be used when calculating the global indicator. Then, in the final part of the document, the references cited in this work are listed.

[9] A clear leveled structure used to display the refined concepts found within the literature review.

2 Literature Review

As previously mentioned, this part of the document is where the review of relevant literature, that underlies this research work, happens. The first step was to conduct a bibliographic research, using the specific services provided by University of Minho library, which contains the most recognized electronic platforms currently in the academic and scientific environment (B-ON, Scopus and Web of Knowledge), the University's Online repository (*RespositoriUM*); for further research Google Scholar was used, and additionally other means were used (such as the help from the supervisors to attain some documents and contacting the authors of articles).

The following expressions were applied for the thematic indexing of the research: "information security governance", "public administration Portugal", "ISO 27014", "COBIT 5 governance", "COBIT 5 security governance"[10], "ISO 27014:2013", and other specific article searches; the articles compelled from these expressions and their respective search engines can be verified in Table 36 of Appendix A – Literature and Concept Matrices.

Following, on section 2.1, the main concepts for this study (such as IT, IS and ISS) are explained, evidencing the context in which the study is inserted. Subsection 2.2 displays the contents related to Governance, in subsections 2.2.1, 2.2.2, 2.2.3 , and are analyzed and thoroughly reviewed. Also, in subsection 2.2.3.2 the relevant documents for ISSG are revealed. While subsection 2.3 presents the study's research opportunity.

2.1 Main Concepts

In this part the concepts of IT, IS and Information Systems Security (ISS) are defined; because they are the foundation for this research. This vocabulary is specific to this knowledge area and its ambiguity must be minimized in order to maximize the reader's understanding.

Some of these concepts may encounter some disagreement within the scientific community about their definition, but due to their high importance in this work, their different interpretations will be explained. The following definitions will be adopted for the entireness of this document and do not intend

[10] At the beginning of these work the current version of COBIT was COBIT 5, therefore the initial literature review was conducted using the terms COBIT 5. In 2018 the new version of COBIT was introduced so the corrections were made to be aligned with COBIT 2019.

to be exhaustively researched, this was created essentially for a better understanding of these concepts before this document.

2.1.1 Information Technology

Ward and Peppard [2002, p. 3] describe IT as “technology, essentially hardware, software and telecommunications networks. It is thus both tangible (e.g. with servers, PCs[11], routers and network cables) and intangible (e.g. with software off all types). IT facilitates the acquisition, processing storing, delivery and sharing of information and other digital content.”

Another author complements by declaring that IT is comprised in the IS Technical dimension [de Sá-Soares 2005, p. 27].

2.1.2 Information Systems

For the UK Academy of Information Systems (UKAIS), IS is defined as “the means by which people and organizations, utilizing technology, gather, process, store, use and disseminate information” [Ward and Peppard 2002, p. 3].

But according to de Sá-Soares’s [2005, p. 27] interpretation, “information systems is a social system whose purpose is to support organizational meaning and action through the organized synthesis of information." He also states that this definition was chosen because is implicit that the organization’s employees are an integral part of the IS. Moreover, this definition lets IS to be perceived in all of the three organizational dimensions (Technical, Formal and Informal).

In line with the previous description, Lopes [2012] goes further and describes IS as “a social system whose purpose is to accomplish a set of procedures designed to capture what happens in the organization and on its environment and present this information in a succinct and organized way, in order to support all informational activity, in a more or less automated manner".

[11] Acronym commonly use to describe personal computers.

2.1.3 Information Systems Security

Dhillon [1997, p. 5] states that “information system security concerns not just the security of the technical edifice but also that of the formal and informal systems within an organisation.” He later goes to add that “Information system security is considered as a state of caution and safety with respect to the information handling activities of an organisation.”

de Sá-Soares [2005, p. 28] emphasizes on the perspective of the organizational activities related to the manipulation of information, taking into account concerns about the technologies that are intrinsic to the technical dimension of organizational information systems, therefore classifying ISS in four meaning groups: state (reflects the level of integrity of an organization regarding to its activities that manipulate information), means (resources, products and procedures that in an organization context become their ISS technical, formal and informal controls), process (the components of an ISS process; such as planning, evaluation, design and implementation) and knowledge area (area of research or body of knowledge that can be taught) [de Sá-Soares 2005, pp. 29–31].

2.2 Governance

The subject of Governance, which in part is the focus of this study, still has a broad range of sub-areas. Therefore, this segment is inclined to give a brief information about the relevant areas (corporate and IT governance), while narrowing the scope to the sub-area that is the focus of this study (ISSG).

Much can be said about the importance of a good governance. For instance ISACA [2012b, p. 13] states that “Over the past decade governance has moved to the forefront of business thinking”.

Governance has taken its place in the forefront of the business, so much so, that according to COBIT® 2019 it is used to ensure “the stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives” [ISACA 2018d, p. 15].

With such a large scope, several areas of governance models (IT governance, Organizational / Corporate / Enterprise governance) can exist inside an organization, all of them being an integral component for the organization’s governance; emphasizing the importance of the business objectives alignment [ISO/IEC 2013].

2.2.1 Corporate Governance

As mentioned, one of governance sub-areas is called corporate governance; and it is described by von Solms and von Solms [2009] as "the way a company is run and managed in order to ensure its well-being" and that the responsibility and accountability begins with the Board of Directors and Senior Management. The authors also remarked that the use of actions such as direct and control are in the heart of corporate governance.

Although, in COBIT® 5[12], corporate governance is explained in a more robust manner as: "A set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly. It could also mean a governance view focusing on the overall enterprise; the highest-level view of governance to which all others must align" [ISACA 2012b].

Whereas, in ISACA[13]'s online glossary, corporate governance is described in a broader aspect as "The system by which enterprises are directed and controlled. The board of directors is responsible for the governance of their enterprise. It consists of the leadership and organizational structures and processes that ensure the enterprise sustains and extends strategies and objectives" [ISACA 2019b].

Furthermore, von Solms and von Solms [2009] also state that "all active employees are considered stakeholders in corporate governance and they are divided in three levels: Board of Directors and Executive Management, Senior and Middle Management, and Lower Management and Administrators".

To Reinert et al. [2010, pp. 227, 230] and von Solms and von Solms [2009], corporate governance is considered dynamic in its nature, due to the Direct/Control cycle; the direction comes from the top level downwards in a document form (Directives, Policies, Procedures); and the control comes from the bottom up, in the form of control measures. These measures are monitored by the executive management (to ensure compliance with the documents).

One of the major responsibilities in corporate governance is Risk Management. A corporate risk should be implemented since it is crucial to meet the company's desired risk profile guideline, and would

[12] The reason COBIT® 5 is used to define the term is due to the lack of definition in COBIT® 2019 document. Also, COBIT 5® is used as a base for COBIT® 2019, therefore the relevance pertains.

[13] ISACA is the organization behind COBIT® 5 and 2019.

need to specify the type (IT, financial, human resources) and degree of the risk the company is willing to accept, in order to meet the company's goal. Consequently, the Board of Directors and Executive Management are responsible and accountable for understanding and managing IT- related risks, since IT risks are viewed as the most important type of risk [von Solms and von Solms 2009].

von Solms and von Solms [2009] also reiterates that corporate governance consists of a large number of 'sub-governance' such as: Financial Governance, Human Resource Governance and IT Governance, each of them managing their own environment and related risks.

In line with the thought of risk management, Dhillon [2007, p. 216], also states that "Corporate Governance is necessary for enterprise risk management, for defensible management practices, and to establish a control position such that prudence can be demonstrated when held accountable to shareholders, stakeholders, and regulators."

The same author also divulges into IS security corporate governance declaring that "Information and systems that acquire, assimilate, convey, retain, and process that information are vital corporate assets without which the survival of the corporation is doubtful. Hence information systems must be secured to a level appropriate for the execution of the corporation's profitable enterprise" [Dhillon 2007, p. 216].

2.2.2 Information Technology Governance

Another governance sub-area is Information Technology Governance (ITG); which Querido [2014], in his work, gives an overall description as being: "The subject concerned with the alignment of IT with business, to achieve maximum business value".

ISACA [2012b][14] develops this description by stating: "A governance view that ensures that information and related technology support and enable the enterprise strategy and the achievement of enterprise objectives. It also includes the functional governance of IT, i.e., ensuring that IT capabilities are provided efficiently and effectively."

von Solms and von Solms [2009] use the previous statement to add that ITG is an integral part of Corporate Governance, consisting of organizational leadership, structures and processes to ensure that

[14] Though in its new version, COBIT® 2019, incorporates enterprise as part of its IT governance efforts, and treats it as a whole, this is then called Enterprise Governance of Information and Technology (EGIT). ITG couldn't be found within the document for this new version, but as it was previously mentioned, this version uses COBIT® 5 as a basis, therefore this description remains accurate to a certain extent.

their IT sustains and extends the strategy and objectives of the organization. Those responsible for ITG are the board of Directors and Executive Management.

Successful enterprises have recognized that they need to embrace IT like any other significant part of doing business and both managers and the board (in business and IT functions) must collaborate and work together to include IT in their governance and management approach; moreover, the need to implement and address legislation and regulations are being passed [ISACA 2012b].[15]

Since the need to implement and address these legislations and regulations, one must focus on Risk Management; that is stated in corporate governance as a core idea, thus the responsibility of managing the risks caused by the use of IT should also be core in ITG; and effectively managed and assured by the Board, being the most important IT-related risks reviewed at least once a year [von Solms and von Solms 2009].

von Solms and von Solms [2009] state that when a company uses their IT system electronic assets (such as data, information, system and applications) they will be able to store, process and, in the case of system and applications, transmit data and information.

These assets suffer from many threats (such as internal, external and physical attacks), the most important ones threatens the CIA (confidentiality, integrity and availability) of those electronic resources, thus the need to always ensure their CIA; meaning only people authorized may read or access (ensuring confidentiality and privacy) and make changes (ensuring integrity) of those electronic assets; and they must be available to authorized users when required (thus ensuring availability). Therefore, in order for a good ITG one must put in place countermeasures or asset protection mechanisms, to prevent attacks from happening or at least limit their impact. In that case, a relevant knowledge of international best practices and guidelines (such as COBIT) is prudent to have [von Solms and von Solms 2009].

2.2.3 Information Systems Security Governance

In accordance with the preceding part, this subsection is intended to further narrow the target of study and explain the governance area used as the main focus of this study. Since this study is focused on the governance of Information Systems Security, the subject is broken down into two parts for a richer understanding. The first part intends to define ISSG based on the literature researched. Then, the second part summarizes the relevant documents used in ISSG.

[15] This paragraph remains pertinent in the new version of COBIT® [ISACA 2018c, p. 11], the ideas behind it can still be found within EGIT.

2.2.3.1 Definition

In the literature reviewed, a common thread was noticed, where Information Systems Security Governance is often portrait as Information Security Governance. Even in articles that have ISSG in its title, such as "Information system security governance: Technology Intelligence perspective" by Zaydi and Nasserddine [2016], the authors referred to ISSG as ISG. Even though, authors who use the term ISG are often referring to ISSG, in some sort; either by referring to a system in their own definitions or implicitly by referring to employees, which are considered an integral part of an organization's IS (as explained in the IS section).

One of the first and broader definitions found within this literature review was used by Moulton and Coles [2003], in 2003, in which the authors defined ISG as "the establishment and maintenance of the control environment to manage the risks relating to confidentiality, integrity and availability of information and its supporting processes and systems".

Then, three years later, Bowen et al. [2006] defined ISG as "the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk".

Aftwards, Veiga and Eloff [2007] noticed three distinct phases for Information Security Governance, wich evolved through the years. In the first phase ISG was characterized through a very technical approach (securing the IT environment), the second phase information security was incorporated to the organizational structures (with the involvement of top management), finally the third phase incorporated information security into the employee everyday practices (information security culture). The definition, which Veiga and Eloff [2007] notice these phases, is the one used by ISO/IEC 27014 [2013], that still continues to be used in 2013, which defines ISG as a "system by which an organization's information security activities are directed and controlled" [ISO/IEC 2013].

Though, authors such as von Solms and von Solms [2009], explain ISG in short, by saying that it is "the system by which the confidentiality, integrity and availability of the company's electronic assets are maintained"; later they improve this definition by writing that ISG "consists of the management commitment and leadership, organizational structures, user awareness and commitment, policies, procedures, processes, technologies and compliance enforcement mechanisms, all working together to ensure that the confidentiality, integrity and availability (CIA) of the company's electronic assets (data, information, software, hardware, people etc.) are maintained at all times".

While, Abu-Musa [2010] went to describe ISG as "could be regarded as implementing governance concepts and principles on information security issues".

Whereas in a more recent definition of ISG, which comes from Zaydi and Nasserddine [2016], states that ISG "consists of leadership, organizational structures and processes that safeguard information".

This study chose to follow the definition used by Moulton and Coles [2003], which is straight forward, simple and embraces a general overview of ISSG. Such aspects described in the definition can be found within the relevant documents of ISSG as explained in the following subsection.

2.2.3.2 Relevant Documents

The following documents are some of the frameworks currently used in ISSG. These documents are also customarily mentioned in the literature for this subject, so much so, that Veiga and Eloff [2007] proposed a new government framework (cf. Figure 13), and added that "the first step in developing an information security culture and empowering the workforce to be aware of their responsibilities towards protecting information assets would be to implement a comprehensive Information Security Governance framework".

The documents reviewed are COBIT® 2019, NIST SP 800-100, ISO/IEC 27014:2013, GTAG® 15, and Veiga and Eloff Framework. The first one is a customizable framework that provides a foundation for information and technology governance, aimed at the whole enterprise. As for the second document, it was created by the American Federal Government to manage and govern information security, focused on directing managers to establish and implement ISG in their organizations.

The third document, ISO/IEC 27014:2013, is an international standard, used to provide guidance for ISG in all types of organizations. Whereas GTAG® 15 is a practical guide for conducting internal audit activities, such as an ISG audit plan. The last document, Veiga and Eloff Framework, is a framework developed to serve as a starting point for ISG.

- COBIT® 2019

COBIT (formerly known as Control Objectives for Information and Related Technology) [ISACA 2012b] is a framework designed for the governance and management of the enterprise information and technology, it is aimed at the whole enterprise and its last version was released on November[16] and December[17] of 2018 [ISACA 2018c, p. 13, 2019a].

The intended audience for this framework are the stakeholders for Enterprise Governance of Information and Technology (EGIT), extending to the stakeholders for corporate governance. The document group them by internal and external stakeholders, whereas for internal stakeholders are included the board, executive management, business management, IT managers, assurance providers and risk management. The second group, external stakeholders, includes regulators, business partners and IT vendors [ISACA 2018c, p. 15].

COBIT also introduces the concept of EGIT, starting by acknowledging the crutial role information and technology (I&T) has gotten in the support, sustainability and growth of enterprises; and the correlation it has on the stakeholders value creation[18] due to a high degree of digitalization in new business models. EGIT is an integral part of corporate governance and gives a special focus in the governance of I&T. The focus on EGIT arose in the past three decades, due to the centrality I&T have in enterprise risk management and value generation [ISACA 2018c, p. 11].

EGIT consists of the board overseeing the definition and implementation of processes, structures and relational mechanisms, that will enable both the business and IT people to execute their resposabilities to support business/IT aligment and to create business value driven from I&T-enabled business investiments. This kind of governance is complex and multifaceted, as such its measures and implementations are required to be tailored for each specific context and needs. Also, enterprises must be willing to have both a different mindset and culture, and accept more accountability for I&T [ISACA 2018c].

The document specifies the three main outcomes to be expected from a successful adoption of EGIT: Benefits realization (creation of value that is aligned with the business focus, on time and within budget); Risk optimization (preserving the value by addressing the business risks that could pontentially impact the business; alignment with the enterprise risk management approach); and Resource

[16] Release of COBIT publications Introduction and Methodology; and Governance and Management Objectives.

[17] Release of COBIT publications Design Guide; and Implementation Guide.

[18] Stakeholders value creation is said to be the realization of benefits at an optimal resource cost while optimizing risk [ISACA 2018c]

optimization (ensuring that the appropriate capabilities are in place to effectively execute and support the strategic plan) [ISACA 2018c].

In a break from previous versions, this version of COBIT uses the concept of enterprise I&T which means: all the efforts puts in place to achieve the enterprise's goals in technology and information processing, regardless where it happens on the enterprise. These efforts of the enterprise I&T include, but are not limited to, the organization's IT department [ISACA 2018c, p. 13].

COBIT's key concepts are Principles, Govenance and Management objectives, Goals Cascade, Components of a Governance System, Focus Areas and Design Factors [ISACA 2018e].

The framework was built upon two sets of principles, one that describes the core requirements of a governance system and another that can be used to build a governance system, refered as governance framework principles. Figure 1 represents both the six core principles of COBIT's Governance System and the three principles for Governane Framework, while Table 1 gives a more in depth definition of these principles [ISACA 2018c].

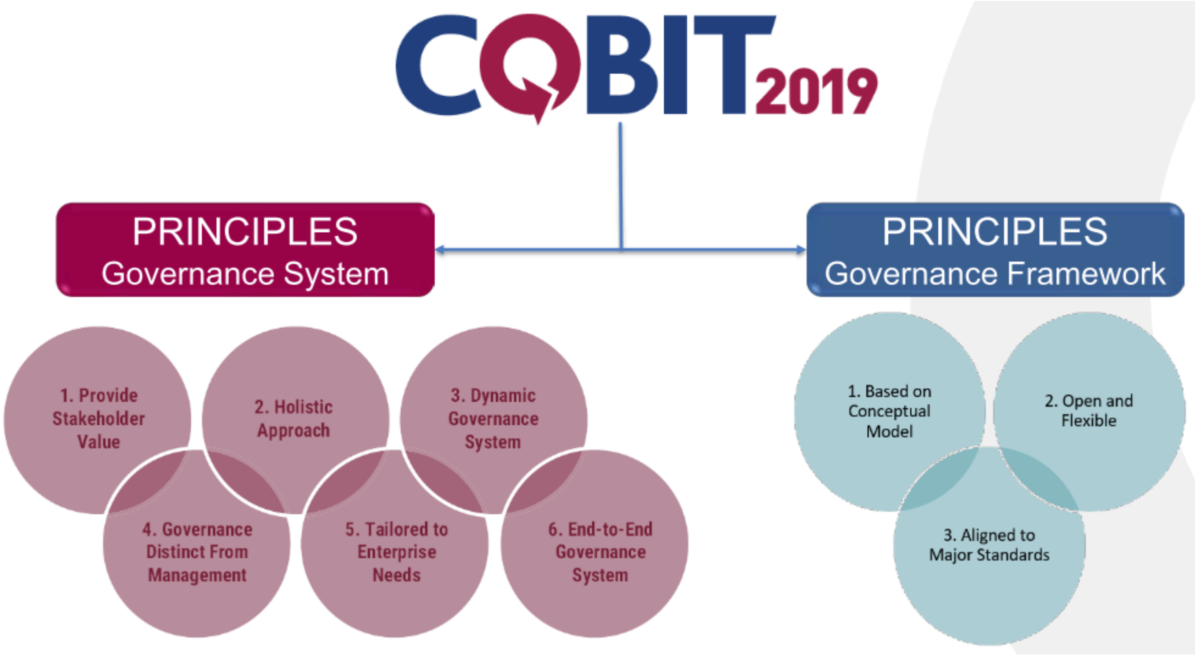

COBIT 2019
PRINCIPLES
Governance System
PRINCIPLES
Governance Framework
1. Provide Stakeholder Value
2. Holistic Approach
3. Dynamic Governance System
4. Governance Distinct From Management
5. Tailored to Enterprise Needs
6. End-to-End Governance System
1. Based on Conceptual Model
2. Open and Flexible
3. Aligned to Major Standards

Figure 1 – COBIT Principles

Source: ISACA [2018e]

Table 1 – COBIT Principle Definition

Source: ISACA [2018c, pp. 17, 18]

Governance System Principles		
Number	**Name**	**Definition**
1	Provide Stakeholder Value	Each enterprise needs a governance system to satisfy stakeholder needs and to generate value from the use of I&T. Value reflects a balance among benefits, risk and resources, and enterprises need an actionable strategy and governance system to realize this value.
2	Holistic Approach	A governance system for enterprise I&T is built from a number of components that can be of different types and that work together in a holistic way.
3	Dynamic Governance System	A governance system should be dynamic. This means that each time one or more of the design factors are changed (e.g., a change in strategy or technology), the impact of these changes on the EGIT system must be considered. A dynamic view of EGIT will lead toward a viable and future-proof EGIT system.
4	Governance Distinct from Management	A governance system should clearly distinguish between governance and management activities and structures.
5	Tailored to Enterprise Needs	A governance system should be tailored to the enterprise's needs, using a set of design factors as parameters to customize and prioritize the governance system components.
6	End-to-End Governance System	A governance system should cover the enterprise end to end, focusing not only on the IT function but on all technology and information processing the enterprise puts in place to achieve its goals, regardless where the processing is located in the enterprise.
Governance Framework Principles		
Number	**Name**	**Definition**
1	Based on a Conceptual Model	A governance framework should be based on a conceptual model, identifying the key components and relationships among components, to maximize consistency and allow automation.
2	Open and Flexible	A governance framework should be open and flexible. It should allow the addition of new content and the ability to address new issues in the most flexible way, while maintaining integrity and consistency.
3	Aligned to Major Standards	A governance framework should align to relevant major related standards, frameworks and regulations.

The first principle, from Governance Systems, states that the value created is driven from the stakeholders need. Which means, that to achieve this objective, the governance should balance the needs of the enterprise into an actionable strategy and governance system; by realizing benefits at an optimal resource cost while optimizing the risks [ISACA 2018c].

Principle 2 (Holistic Approach) refers to a number of components (factors, of different types, that individually or collectively contributes to the good operation of the enterprise's governance systems over I&T). Their interactions with each other result on a holistic governance sytem for I&T. Components are also established, tailored and used to sustain the governance system, that was build upon the needs of the enterprise. Their goal is to satisfy the governance and management objectives. They are divided into seven categories as show in Figure 2 [ISACA 2018c].

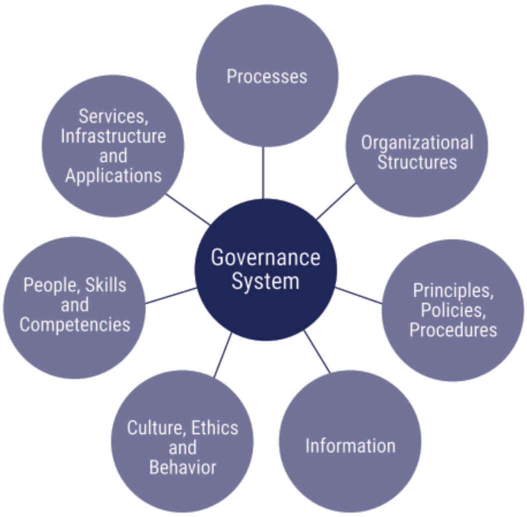

Processes
Services, Infrastructure and Applications
Organizational Structures
Governance System
People, Skills and Competencies
Principles, Policies, Procedures
Culture, Ethics and Behavior
Information

Figure 2 – COBIT Components of a Governance System

Source: ISACA [2018b]

The most common type of components is Processes (organized set of practices and activities to achieve objectives and produce outputs for IT-related goals), but there are also others like: organizational structures; policies and procedures; information items; culture and behavior; skills and competencies; and services, infrastructure and applications. These components can also be generic, described in the COBIT core model and in need of customization; or they can be variants, based on a generic component but tailored to a specific purpose or context within a focus area [ISACA 2018c].

In the third principle, Dynamic Governance System, each time a change occurs in one or more design factors, its impact on the EGIT system, is something that should be considered. These design factors can influence in the design of an enterprise's governance system and position it for the successful use of I&T. The design factors listed in Figure 3 can be used in any combination [ISACA 2018c].

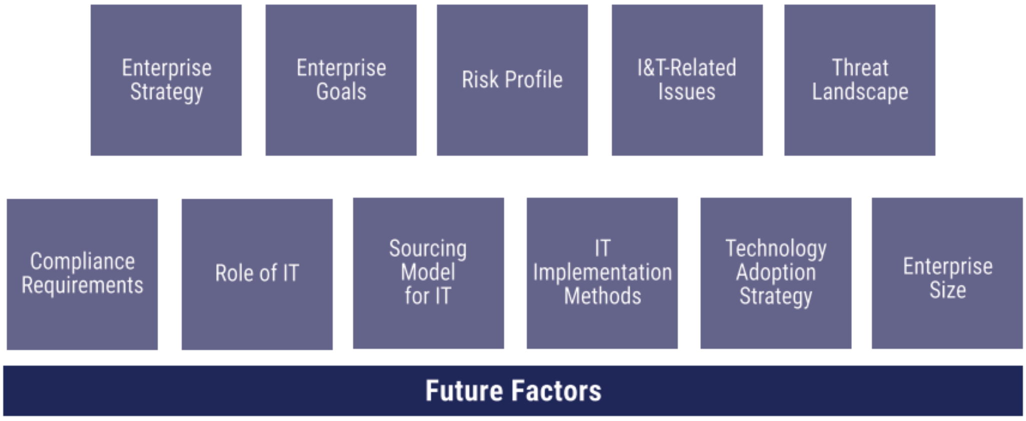


Figure 3 – COBIT Design Factors

Source: ISACA [ISACA 2018c]

For the impact the Design Factors have on the governance system of an enterprise, COBIT distinguishes it in three different types: Management Objective Priority and Target Capability Levels, Component Variations and Specific Focus Areas. The first one influences on the equivalence of the governance and management objectives, rendering sometimes one objective more important than the other, which translates into setting a higher target capability level for the more important objectives. While the second type, which is Component variations, represents how design factors can mandate specific variations of components, or influence the importance of components in order for them to achieve governance and management objectives. Lastly, the third type, represents how some design factors (such as threat landscape, specific risk, target development methods, infrastructure set-up) will determine the need for a variation in the COBIT core model to fit into a specific context [ISACA 2018a].

The fourth principle, is where the governance system makes a clear distinction of governance and management. These are two different disciplines that embrace different types of activities, need distinctive organizational structures and have different purposes. The responsibility of governance lays upon the board of directors under the leadership of the chairperson, while for management that responsibility is entrusted to the executive management under the leadership of the CEO [ISACA 2018b].

Though COBIT is not a prescriptive framework, it encourages, by defining all components, which decision should be taken, how and by whom. One of these components are processes, that can be organized by the enterprise in the manner that best fit the enterprise; as long as all necessary objectives for governance and management are covered. The framework includes a reference model (Appendix B – COBIT® 2019 COBIT Core Model Figure 17),which defines and describes in detail the forty core governance and management objectives. Each objective always relates to a process and a series of related components. They are divided in two main domains (Governance and Management). The first contains five objectives referred as EDM01 (Ensure Governance Framework Setting and Maintenance), EDM02 (Ensure Benefits Delivery), EDM03 (Ensure Risk Optimization), EDM04 (Ensure Resource Optimisation) and EDM05 (Ensure Stakeholder Engagement). Their description and purpose are presented in Table 2 [ISACA 2018b].

Table 2 – EDM Objectives Description

Source: ISACA [2018b]

Number	Name	Description	Purpose Statement
EDM01	Ensure governance framework setting and maintenance	Analyse and articulate the requirements for the governance of enterprise IT. Put in place and maintain governance components with clarity of authority and responsibilities to achieve the enterprise's mission, goals and objectives.	Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions must be made in line with the enterprise's strategies and objectives, and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.
EDM02	Ensure benefits delivery	Optimize the value to the business from investment in business processes, I&T services and I&T assets.	Secure optimal value from I&T-enabled initiatives, services and assets; cost-effective delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.
EDM03	Ensure risk optimization	Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed.	Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.
EDM04	Ensure resource optimisation	Ensure that adequate and sufficient business and IT-related resources (people, process and technology) are available to support enterprise objectives effectively and, at optimal cost.	Ensure that the resource needs of the enterprise are met in the optimal manner, I&T costs are optimized, and there is an increased likelihood of benefit realization and readiness for future change.
EDM05	Ensure stakeholder engagement	Ensure that stakeholders are identified and engaged in the I&T governance system and that enterprise I&T performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and the necessary remedial actions.	Ensure that the stakeholders are supportive of I&T strategy and roamap, communication to stakeholders is effective and timely and the basis for reporting is established to increase performance. Identify areas for improvement, and confirm that I&T-related objectives and strategies are in line with the enterprise's strategy.

For the principle Tailored to Enterprise Needs, design factors are used as parameters to customize and prioritize components in the govenance system, in order for the system to be tailored for the enterprise's needs. This tailoring process shoud follow the proposed four stage design workflow, presented in Figure 4 [ISACA 2018a].

The results for this process are recommendations for prioritizing (in terms of target capability levels or adopting specific variant of components) governance and management objectives or related components of the governance system. Also during this process, some conflicting guidance may occur as a result for the substeps, which are not mandatory. To manage this conflicted guidance, COBIT recommends putting all guidance obtained during the different steps onto a design canvas, and in the last stage of the process, resolve them to a possible degree, and them conclude the process. COBIT also notes that the final design will be decide case-by-case [ISACA 2018a].

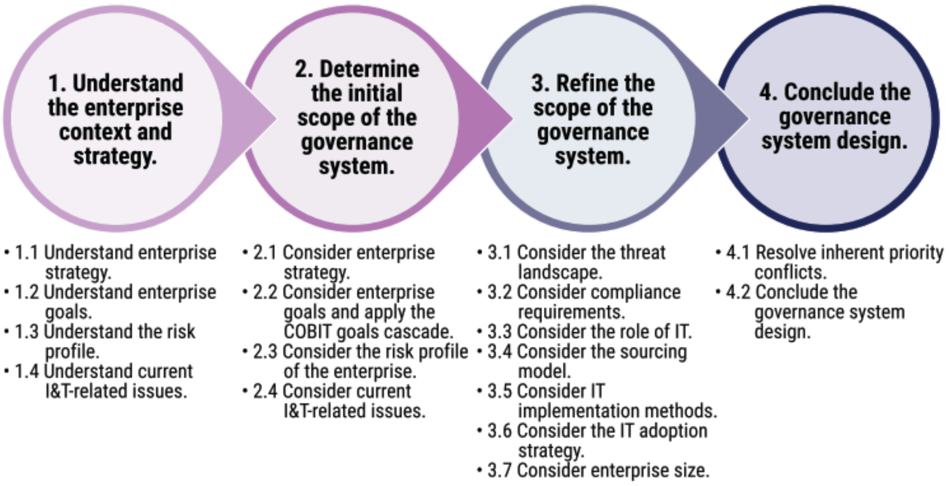

1. Understand the enterprise context and strategy.
2. Determine the initial scope of the governance system.
3. Refine the scope of the governance system.
4. Conclude the governance system design.
• 1.1 Understand enterprise strategy.
• 1.2 Understand enterprise goals.
• 1.3 Understand the risk profile.
• 1.4 Understand current I&T-related issues.
• 2.1 Consider enterprise strategy.
• 2.2 Consider enterprise goals and apply the COBIT goals cascade.
• 2.3 Consider the risk profile of the enterprise.
• 2.4 Consider current I&T-related issues.
• 3.1 Consider the threat landscape.
• 3.2 Consider compliance requirements.
• 3.3 Consider the role of IT.
• 3.4 Consider the sourcing model.
• 3.5 Consider IT implementation methods.
• 3.6 Consider the IT adoption strategy.
• 3.7 Consider enterprise size.
• 4.1 Resolve inherent priority conflicts.
• 4.2 Conclude the governance system design.

Figure 4 – Governance System Design Workflow

Source: ISACA *[ISACA 2018a]*

In the last principle of the Governance System, End-to-End Governance System, the system in place should cover the whole enterprise, not only the IT function. The system should also cover all the other technology and information processing that is put in place by the enterprise, in order for the enterprise to achieve its goals. These goals come from the needs of the stakeholders and those needs are transformed into an enterprise actionable strategy. The goals are supported by the goals cascade, as seen in Figure 5, which is a key design factor for the governance system. In addition, the thirteen enterprise goals are structured along the balance score card (BSC) dimensions [ISACA 2018c].

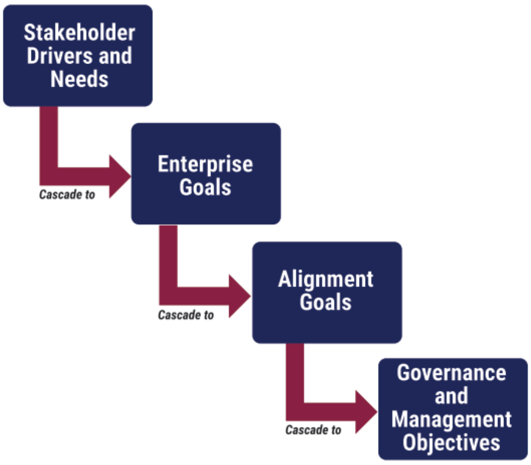

Stakeholder Drivers and Needs
Cascade to
Enterprise Goals
Cascade to
Alignment Goals
Cascade to
Governance and Management Objectives

Figure 5 – Goals Cascade

Source: ISACA [2018c]

The second set of principles consists of three principles, which underlines the Governance Framework and how it can be used to build a governance system for the enterprise [ISACA 2018e]. Those principles are: Based on a Conceptual Model (in which the components and their relationships of the framework are identified, for consistency and automation, and based on the conceptual model); Open and Flexible (in which the framework should allow new content and be able to address new issues, while maintaining integrity and consistency); and Aligned to Major Standards (in which the framework should be aligned with relevant major related standards, frameworks and regulations; such as Information Technology Infrastructure Library (ITIL®), US National Institute of Standards and Technology (NIST), Institute of Internal Auditors® (IIA®), The Open Group Architecture Forum (TOGAF®), Project Management Body of Knowledge (PMBOK®), Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the International Organization for Standardization (ISO) standards) [ISACA 2018c].

Apart from the principles, COBIT's framework also presents the COBIT Performance Management (CPM) and COBIT's Implementation Approach. CPM describes the activities that express how the systems and components of the enterprise work, and how to improve them to reach the required level, in terms of capability and maturity [ISACA 2018c].

CPM should follow these five principles: be simple to understand and to use; be consistent and support the conceptual model of COBIT, besides being able to manage the performance of all types of components of the governance system, processes and other types of components; should provide reliable, repeatable and relevant results; should support different types of assessments; and must be flexible to support different requirements from different organizations with different priorities and needs [ISACA 2018c].

The CPM model is largely aligned to the concepts of CMMI® Development V2.0, and then goes further by having capability levels associated not only to processes, but other governance and management component types (such as organizational structures and information). Alongside, maturity levels are associated with the focus areas[19] and will be achieved once all capability levels are achieved [ISACA 2018c].

In this version of COBIT, the explicit processes outcomes and goals are replaced by the process practices [ISACA 2018c]. To manage the performance, each process operates a capability level, ranging

[19] Description of certain governance topic, domain or issue usually addressed by a collection of governance and management objectives and their components, such as cybersecurity, privacy, security and risk. Their number can be unlimited and may contain a combination of generic and variant governance components. For such reason, COBIT is classified as open-ended, since new focus areas may be added as required or as COBIT model grows [ISACA 2018c].

from 0 to 5, as demonstrated in Figure 6, and is used to measure how the process is implemented and performing. When a capability level is assigned to all process activities, it enables a clear definition of what the process is and which required activities are needed, in order to achieve each capability level [ISACA 2018c].

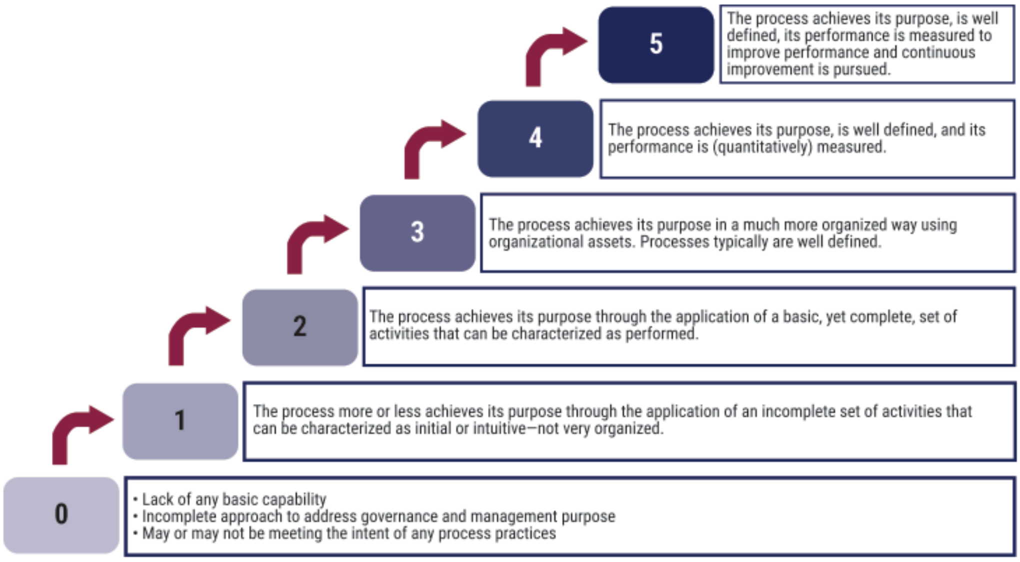

5
The process achieves its purpose, is well defined, its performance is measured to improve performance and continuous improvement is pursued.
4
The process achieves its purpose, is well defined, and its performance is (quantitatively) measured.
3
The process achieves its purpose in a much more organized way using organizational assets. Processes typically are well defined.
2
The process achieves its purpose through the application of a basic, yet complete, set of activities that can be characterized as performed.
1
The process more or less achieves its purpose through the application of an incomplete set of activities that can be characterized as initial or intuitive—not very organized.
0
• Lack of any basic capability
• Incomplete approach to address governance and management purpose
• May or may not be meeting the intent of any process practices

Figure 6 – Capability Levels

Source: ISACA *[ISACA 2018c]*

The governance and management objectives, in the COBIT core model, present an example of metrics, designed to reach those capability levels. These metrics correlates to the goals for alignment, enterprise and processes, though a limited number of example metrics is presented for processes practices. [ISACA 2018b].

Moreover, capability levels can be achieved through various degrees, which are expressed in a form of ratings (this range depends on the context by which the assessment is performed). For instance, a formal method may use a binary pass/fail set of ratings, while less formal methods may work better with a large range of ratings (e.g., in a performance-improvement context) following the set of Fully (>85%), Largely (50-80%), Partially (15-50%) and Not (15%>) achieved [ISACA 2018c].

When a higher level of performance assessment is required, maturity level is used. These maturity levels measure the performance at a higher level, usually from focus areas. To achieve certain maturity level in a focus area, one needs to have achieved all prior capability levels for the processes within that focus area. The maturity level also ranges from 0 to 5, as seen in Figure 7 [ISACA 2018c].

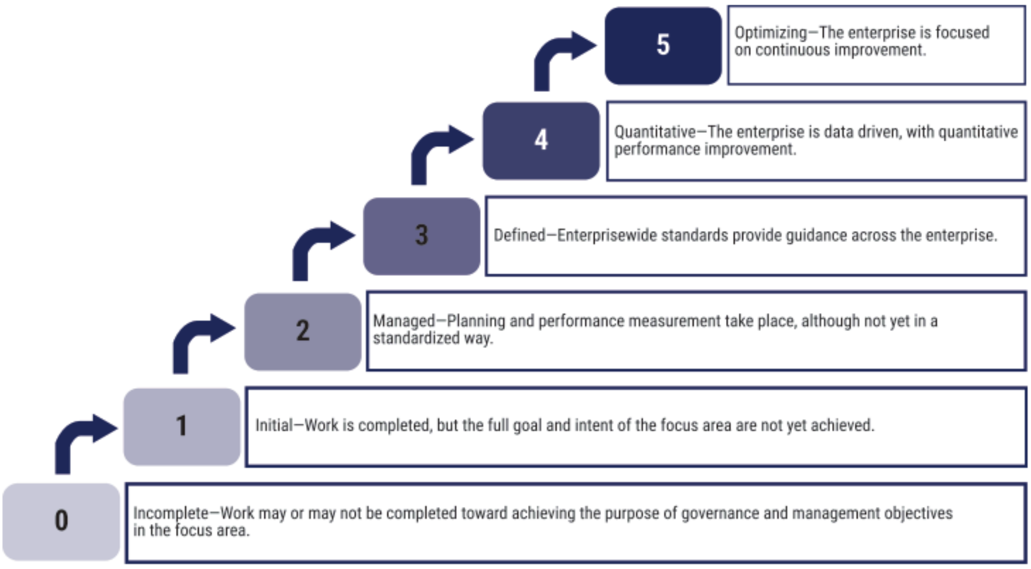

5
Optimizing—The enterprise is focused on continuous improvement.
4
Quantitative—The enterprise is data driven, with quantitative performance improvement.
3
Defined—Enterprisewide standards provide guidance across the enterprise.
2
Managed—Planning and performance measurement take place, although not yet in a standardized way.
1
Initial—Work is completed, but the full goal and intent of the focus area are not yet achieved.
0
Incomplete—Work may or may not be completed toward achieving the purpose of governance and management objectives in the focus area.

Figure 7 – Maturity Levels

Source: ISACA *[ISACA 2018c]*

Aside from process performance, the CPM also manages the performance of other components such as Organizational structures, Information Items and Culture and Behavior. The assessment of these components is done in a less formal manner, which is linked to various capability levels. For instance, organizational structures are assessed by a set of three criteria and twelve subcriteria, while information items have three main criteria and fifteen subcriteria, and culture and behavior is assessed by defined aspects and the conditions by which they are met [ISACA 2018c].

Another part of the framework is the Implementation approach that COBIT uses to emphasizes the enterprisewide view of governance of I&T, where governance and management of the enterprise I&T should be implemented as an integral part of the enterprise governance. This integration enables and facilitates changes in governance programs, that needs to be absorbed at the same pace as the planning of a change. Another integral part of the implementation life cycle is the Program Management [ISACA 2018c].

COBIT 2019 also provides good practices for implementing and optimizing an I&T governance system, these practices are based on a continual improvement life cycle approach and should to be tailored to the enterprise's needs.This approach helps the enterprise address the complexity and challenges encountered during the EGIT implementation [ISACA 2018d].

The continual improvement life cycle approach, represented by Figure 8, displays three interrelated components, in its core (light blue ring) is the EGIT continual improvement life cycle, the (pink) middle ring is for the change enablement (which addresses the cultural and behavior aspects), and the outer ring (dark blue) is for the program management. The most outer ring presents the seven phases of the implementation road map [ISACA 2018d].

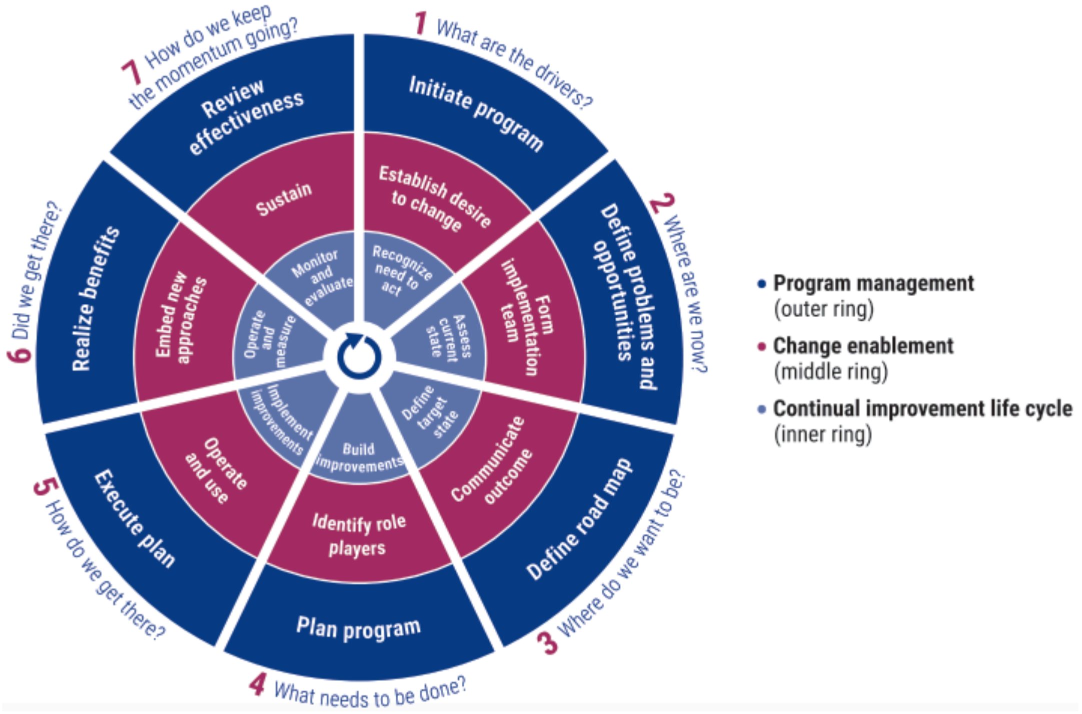


Figure 8 – COBIT Implementation Road Map

Source: ISACA *[ISACA 2018d].*

Each phase of the life cyle is supported by a summarized chart with the responsabilities of each group/role of players in the phase; a table containing the phase objective and description, the tasks for continual improvement, change enablement and program management, examples of inputs likely to be required, suggested framework items to be used, and the outputs needed to be produced; and lastly a responsible, accountable, consulted and informed (RACI) chart for the key activities with corresponding cross references [ISACA 2018d].

- NIST SP 800-100

NIST Special Publication 800-100 was developed by the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST), responsible for developing standards and guidelines, for the cost-effective security and privacy of nonnational-security-related information in federal information systems. The Special Publication 800 series reports on the information system security and its collaborative activities with industry, government, and academic organizations [Bowen et al. 2006].

The document aimes to "provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program" [Bowen et al. 2006, p. 1].

Also, in the document, is stated the purpose of ISG, which is to ensure that appropriate information security controls are being implemented in a proactive manner by the agencies, to support their mission in a cost-effective way, while managing evolving information security risks. ISG has its own set of requirements, activities, challenges and types of structures, and is used to identify key information security roles and responsibilities, influence the development of policies and oversee the ongoing managing activities [Bowen et al. 2006].

The second chapter of the document focuses on the Information Security Governance for the federal agencies in the United States. It relays the requirements for a minimum ISG adoption, while realizes that each agency must tailor this information to their own organizational mission, operation and needs.

The key legislatives acts define the overall governance requirements; and other three legislative documents, are also described in the second chapter of the document. These other legislative documents are the Federal Information Security Management (FISMA), the OMB (Office Management and Budget) Circular A-130 and the Homeland Security Presidential Directive 12 (HSPD-12), that emerge as a foundational source for ISG requirements.

Bowen et al. [2006] state that the agency should integrate their ISG activities with the overall agency structure and activities by ensuring appropriate participation of agency officials in overseeing the implementation of information security controls throughout the agency. To represents the agency's structure and their relationships, Figure 9 was created

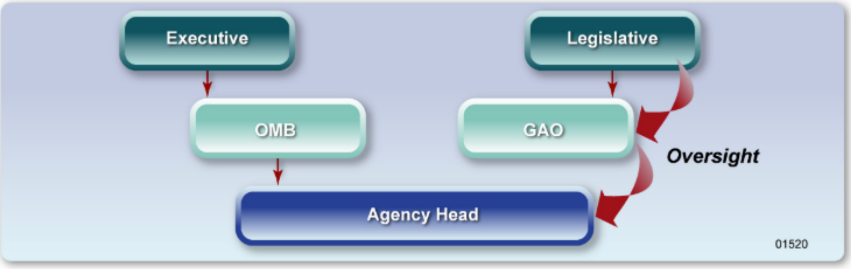


Figure 9 – NIST Key Roles[20]

Source: Bowen et al. [2006]

The key activities (components) mentioned in NIST SP 800-100 to facilitate the ISG integration in the agency are: strategic planning, organizational structure, establishment of roles and responsibilities, integration with the enterprise architecture (Federal Enterprise Architecture – FEA), document the security objectives in policies and guidance, and also to perform ongoing monitoring activities [Bowen et al. 2006]. These components are displayed in Figure 10.

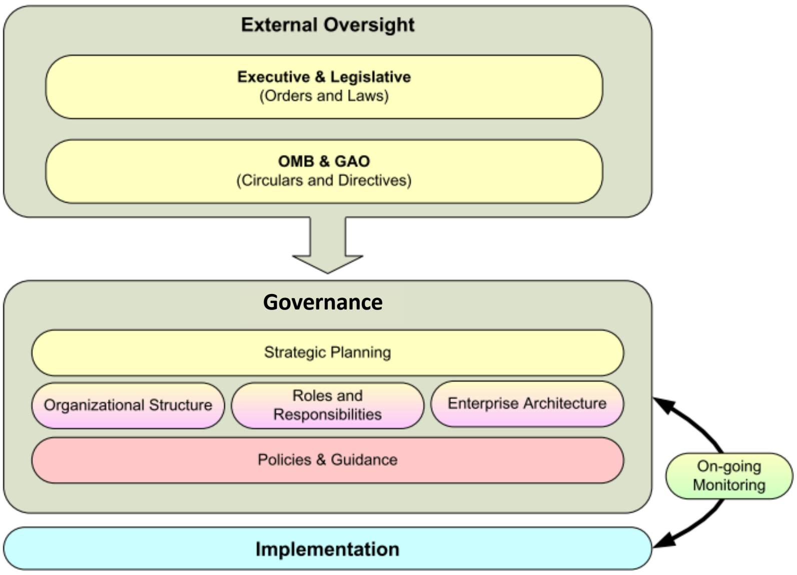


Figure 10 – NIST ISG Components

Source: Bowen et al. [2006]

[20] The roles of OMB and GAO are present within the governmental structure of the United States of America, and they correspond respectively to the Office of Management and Budget, and the Government Accountability Office.

The strategic planning is where the information security should be integrated to the agency's strategic planning processes. These information security strategies need to support the agency's strategy and performance, but also their information security progam [Bowen et al. 2006].

As for the organizational design and development (organizational structure), this can exist as a centralized or decentralized structure model. Where in the centralized model, a departamental CIO (and occasionally the Senior Agency Information Security Officer or SAISO) is responsible for all information security activities. Whereas, in the decentralized model, those activities are separate between the departamental SAISO and the operating unit SAISO. In both cases the agency head is responsible for the management and governance of their agency [Bowen et al. 2006].

The establishment of roles and responsibilities is comprised of several governance stakeholders, that includes senior leadership such as the Agency Head; the CIO; the information security personnel, such as the SAISO; the Chief Enterprise Architect (CEA); and other related roles like an Inspector General (IG); a CFO; a Chief Privacy Officer (CPO); a Physical Security Officer; a Personnel Security Officer; an Acquisitions/Contracting. Each of these roles have specific requirements set out for them [Bowen et al. 2006].

To perform the integration of ISG with the enterprise architecture, the Federal Enterprise Architecture (FEA) is used. FEA is a business-based framework for government-wide improvement. Its purpose is to facilitate the cross-agency analysis and to identify duplicates, gaps or opportunities. This enterprise architecture consists of five reference models: the Performance Reference Model (PRM), the Business Reference Model (BRM), the Service Component Reference Model (SRM), the Data and Information Reference Model (DRM) and the Technical Reference Model (TRM).

Finally, the information security policies and guidance should address the agency's ISG structure and how to effectively implement specific controls across the enterprise. Also, the security policy should be current, have a revision cycle implemented and that the information security policies implement cross-cutting and convergent security objectives.

The ongoing monitoring should have a constant review, in order to produce an effective ISG program. The data for the monitoring can be gathered via activities such as Plans of Actions and Milestones (POA&M), Measurement and Metrics, Continuous Assessment, Configuration Management, Network Monitoring and Incident and Event Statistics. Also, the agency should monitor if the information security activities are supporting the agency's mission; if policies and procedures are aligned with current technologies; and if the controls are accomplishing their purpose [Bowen et al. 2006].

- **ISO/IEC 27014:2013**

Released by both the ISO/IEC[21] and the ITU-T[22] in 2013, this standard is part of the ISO/IEC 27000 series [Mahncke 2013]. Being under review[23], since the WTSA[24] meets every four years to produce new recommendations on these topics [ISO/IEC 2013].

The document is to be used by all types and sizes of organizations, as a guide on the concepts and principles regarding ISG, where they will be able to evaluate, direct, monitor and communicate the activities related to information security within the organization [ISO/IEC 2013].

For ISO/IEC[2013], ISG is important because it provides a link between the organization's top management (executive management and governing body) and those responsible for implementing and operating an Information Security Management System (ISMS); and should be assessed, analyzed and implemented through risk management approach and supported by an internal control system, in order to align the objectives and strategies for both information security and the business, and to comply with laws, regulations and contracts.

The objectives and desired outcome by implementing an ISG are: strategic alignment (when information security and business objectives and strategy are aligned), value delivery (when value is delivered to stakeholders and the governing body) and accountability (when there is guarantee that information risk is being adequately addressed). As for the outcomes expected they are the visibility by the governing body of the information security status; an agile decision-making attitude towards information risks; investments on information security are effective an efficient, and to be in compliance with laws, regulations and contracts (external requirements) [ISO/IEC 2013].

As previously mentioned, the governing body represents one of the two roles that composes the Top Management of an organization. It is also defined as a person or a group who are accountable for the performance and conformity of the organization [ISO/IEC 2013].

One of the governing body responsibilities is to ensure that Information Security and the organization's objectives are achieved; by certifying an effective ISG, through an effective, efficient and acceptable Information Security approach, that meets the stakeholders expectations and guarantees that

[21] ISO (International Organization for Standardization) and IEC (International Electro technical Commission) form a specialized system for worldwide standardization [ISO/IEC 2013].

[22] ITU (International Telecommunication Union) and ITU-T is their Standardization sector [ISO/IEC 2013].

[23] This ISO/IEC will be replaced by ISO/IEC DIS 27014 – Information security, cybersecurity and privacy protection — Governance of information security, in the enquiry phase as of December 7th 2019 [ISO/IEC 2019].

[24] WTSA (World Telecommunications Standardization Assembly) establishes the topic of study by the ITU-T groups [ISO/IEC 2013].

the governing body receives relevant reporting about activities related to information security, enabling them to make pertinent and timely decisions regarding information security issues that may arise and support the organization's strategic objectives. They may benefit from the development of an holistic and integrated view of the governance models, since the scopes sometimes overlap.

The other Top Management role is the Executive Management, also defined as a person or a group that delegates the responsibility given by the governing body to implement strategies and policies that accomplish the purpose of the organization, which may include the organization's CEOs (Chief Executive Officers), CFOs (Chief Financial Officers), COOs (Chief Operating Officers), CIOs (Chief Information Officers), CISOs (Chief Information Security Officers), Heads of Government Organizations and other similar roles [ISO/IEC 2013].

Another role is the stakeholder which is defined as any person or organization that can be affected, affect or perceive themselves to be affected by an activity of the organization (decision makers are included in this role). They also may have different values and needs [ISO/IEC 2013].

The document also exposes the relationships between governance models, and their overlapping scopes. For instance, in Figure 11, where the focus of IT governance is in resources required to acquire, process, store and disseminate information; and for ISG is to cover the confidentiality, integrity and availability of the information; but both of them have to be handle by the EDM (Evaluate, Direct, Monitor) governance process. Still, ISG requires an additional internal process (communicate) [ISO/IEC 2013].

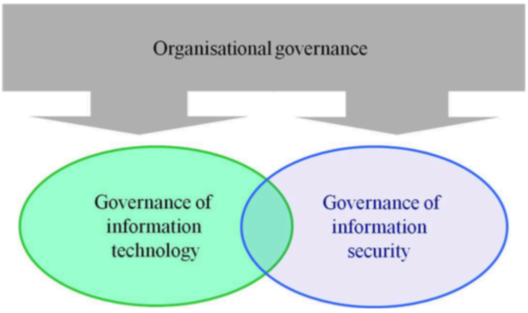

Organisational governance
Governance of information technology
Governance of information security

Figure 11 – Relationship between Governance Models

Source: ISO/IEC *[2013]*

In the first governance model (IT), a set of principles and processes form the ISG. Which are accepted rules for governance action or conduct, acting as a guide for implementing governance. The second governance model (Information Security) describes a series of tasks that enables ISG and their interrelationships (also demonstrates the relationship between governance and management) [ISO/IEC 2013].

ISO/IEC sets out six action-oriented principles, presented in Table 3. In order to achieve two long term goals of the organization (strategic alignment and value delivery); they also are the foundation to implement the governance processes.

The governing body should require a person with responsibility, authority and accountability to implement these principles, since they refer to what should happen in the organization and does not prescribe how, when or by whom they should be implemented, because these aspects may vary from one organization to another [ISO/IEC 2013].

Table 3 – ISG Principles

Adapted from: ISO/IEC [2013]

Principle		ISG	Action
1	Establish organization-wide information security	Should ensure information security activities are comprehensive and integrated. Handled at organizational level and considering all relevant aspects for the decision-making. Activities related to physical and logical security should be closely coordinated.	Establish an organization-wide security, responsibility and accountability across the full span of the organization's activities for information security; including external parties.
2	Adopt a risk-based approach	Based on risk-based decisions. Risk appetite should determine how much security is acceptable for the organization.	Adopt an information risk management appropriate with the organization and integrated with the organization's overall risk management approach. Acceptable levels of information security should be based upon the organization's risk appetite. Appropriate resources should be allocated by the governing body to implement the information risk management.
3	Set the direction of investment decisions	Establish an information security investment strategy based on business outcome achieved. Short and long term harmony between business and information security requirements. Meet the current and evolving needs of the stakeholders.	Optimize information security investments to support organizational objectives. Governing body should ensure that information security is integrated with existing organization processes.
4	Ensure conformance with internal and external requirements	Ensure that information security policies and practices conform with relevant and mandatory legislation, regulations, business commitment, contractual and other requirements.	Address conformance and compliance issues. Governing body should obtain assurance of the satisfaction of their information security activities by commissioning independent security audits.
5	Foster a security-positive environment	Built upon human behavior (fundamental element to support appropriate level of information security). Include the evolving needs of the stakeholders. Harmony and concerted orientation between various stakeholders.	Establish a positive information security culture. Governing body should require, promote and support coordination of stakeholders activities to achieve a coherent direction for information security.
6	Review performance in relation to business outcomes	Ensure the approach taken to protect the information is fit for purpose in supporting the organization, providing agreed levels of information security. Maintain security performance at all levels that meets current and future requirements.	Review the information security performance from a governance perspective. Governing body should evaluate the performance relating it to the business impact.

The EDM and communicate processes are performed by the governing body to govern information security, in addition the assure process provides and independent and objective opinion about the level attained for ISG. The relationship between these processes are showed in Figure 12, followed by an overview of each process and in Table 4 a compact view of the tasks each role performs [ISO/IEC 2013].

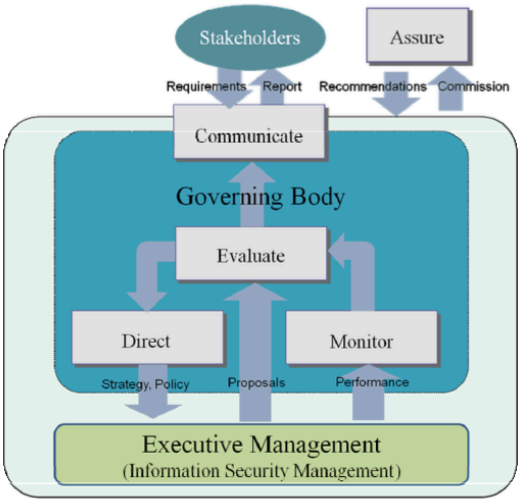


Figure 12 – Implementation of the Governance Model for Information Security

Source: ISO/IEC [2013]

The Evaluate process will consider the current security objectives and forecast them based on the current processes and planed changes, to determine if any adjustments are required to optimize the achievement of strategic objectives in the future.

The governing body will give directions (changes in resource level, allocation of resources, activity prioritization and approval for policies, risk management plan and material risk acceptance) about the information security objectives and strategies that needs implementation; in the process entitled Direct.

Monitor is the process that enables the governing body to assess the achievement of strategic objectives.

For the Communicate process, which is a bi-directional process, where the information about information security is exchanged by the governing body and the stakeholders, according to their needs. One of the methods is to communicate the information security status (information security activities and issues are explained to stakeholders).

Lastly, the Assure process is where the governing body commissions independent and objective audits, reviews or certifications to identify and validate the objectives and actions related to information security (governance activities and conduct operations to attain the desired level).

In order for these relationships to come to fruition tasks need to be performed by either the Governing Body or the Executive Management role, therefore Table 4 presents a compact view of the tasks each of these roles are responsible for.

Table 4 – Processes relationship

Adapted from: ISO/IEC [2013] and Mahncke [2013]

Process	Governing Body (Performs)	Executive Management (Enables)
Evaluate	Ensures business initiative considers information security issues. Prioritize and initiate the required actions in response of information security performance results.	Ensure information security adequately support and sustains the business objective. Submit new information security projects with significant impact on the governing body.
Direct	Determine organization's risk appetite. Approve information security strategy and policy. Allocate adequate investments and resources.	Develop and implement the information security strategy and policy. Align information security and business objectives. Promote a positive information security culture.
Monitor	Assess the effectiveness of information security management activities. Ensure conformance with requirements (internal and external). Consider the changing environment (business, legal and regulatory) and their potential impact on information risk.	Select from a business perspective the appropriate performance metrics. Provide feedback to the governing body on information security performance results, including the performance of actions previously identified by them and their impacts on the organization. Alert the governing body of new developments affecting information security and risks.
Communicate	Report to external stakeholders that the organization practices a level of information security commensurate with their business nature. Notify executive management of results of any external reviews and request for corrective actions for those identified information security issues. Recognize regulatory obligations, stakeholders expectations and business needs regarding information security.	Advise the governing body of any matter requiring their attention and possibly their decision. Instruct relevant stakeholders on detailed actions to be taken in order to support the governing body's decisions and directives.
Assure	Commission independent and objective opinions on compliance and accountability for the desired level of information security.	Support audits, reviews and certifications commissioned by the governing body.

- **Global Technology Audit Guide (GTAG®) 15 – Information Security Governance**

GTAG is short for Global Technology Audit Guide, in this case, a guide for Information Security Governance, which is also, a practice guide, under the International Professional Practices Framework (IPPF), created by the Institute of Internal Auditors (IIA) [Love et al. 2010].

The document starts by presenting its objectives, which are to define ISG; help internal auditors understand the right questions to ask and know what documentation is required; and describe the internal audit activity (IAA) role in ISG.

In the second part, the document attempts to define ISG. Thought the guide doesn't give a formal definition to ISG, since it states there are different definitions across different organizations and standards, the guide does believe there are three common themes amongst them. Those include a promotion of good IS practices with a clear direction and understanding at all levels (top down); a control of IS risks associated with the business; and a creation of an overall IS activity that reflects the organization's needs and risk appetite levels.

It also states that an organization should develop a framework and reporting structure to address ISG; but notes that while formal documentation may exist (such as policies and reporting lines), the use informal reporting line for the governance body shouldn't be underestimated.

Next, the document uses the IS practical guidance on how to prepare for successful audits (IT compliance institute) to clarify ISG roles and responsibilities of the board of directors, executive management, line managers and internal auditors. The document describes the board responsibilities as provide oversight; communicate business imperative; establish and oversee security policy; and define corporate security culture.

Afterwards, the document lists the bases of an effective ISG program, an efficient ISG activity; and reasons why the Chief Audit Executive (CAE) should be concerned about ISG. To have an effective ISG program, one should involve the appropriate organizational personnel; define a governance framework or methodology; enable a uniform risk measurement across the organization; produce quantifiable, meaningful deliverables; and reflect the business priorities, organizational risk appetite, and changing levels of risk.

For an efficient ISG activity, the document says that this measure will reflect the concept of proporcionality by encouraging a tiered structure of internal control; adjusting reporting based on the level of management involved; and allowing for properly approved deviations to policies and standards.

As for the reasons the CAE should be concerned about ISG, those are listed in the document as such: regulatory actions; reputational damage; competitive advantage; contractual noncompliance; innacurate or incomplete data; and fraud.

The third part of the document explains the role the IAA has on ISG. The document divides this part into three, the first explains the IAA's responsibilities, while the second explains the background and experience level of an auditor should have, and the third explains the forms to perform an ISG activity audit (could be several).

The subsequent part of the document is designed to help audit ISG, where internal auditors could understand the right questions to ask and know which documentation is required. This part is split into Planning, Testing and Analyzing. Each part is also divided and within each division of the planning part, a set of questions to be asked can be found.

The Planning part covers the understanding of the ISG organizational structure; the purpose and objectives of each component of the environment; the documented communication that occurs among reporting lines; the organization's risk appetite; the integration of ISG whitin the organization; and the external influences that could affect the ISG structure.

As for the Testing part, the audit should confirm and validate the understanding of: the stakeholders concerns; reporting and communication lines; Key Performance Indicators (KPIs) and their use; the aligment of supporting documentation with governance structure; and the alignment of risk appetite.

Lastly, in the Analyzing portion of the audit, the internal auditor should perform an analysis of each theme and draw its conclusions about the effectiveness of the program. These themes are accountability, design effectiveness, IS program effectiveness, efficiency, resource levels, value added, and continuous improvement.

- **Veiga & Eloff Framework**

Veiga and Eloff [2007] in their document intended to evaluate four current approaches for ISG frameworks, so they could construct a new and more comprehensive ISG framework. The new framework would encompass three components (technical, procedural and human behavioral), and would serve as a single point of reference for ISG.

The authors start their document presenting the historical evolution of ISG, with four distinct phases. In the first phase, information security was viewed as a technical approach in securing the IT environment.

As time went by and with the involvement of management and top management, ISG was incorporated to the organizational structure. This shift characterized the second phase in the ISG evolution.

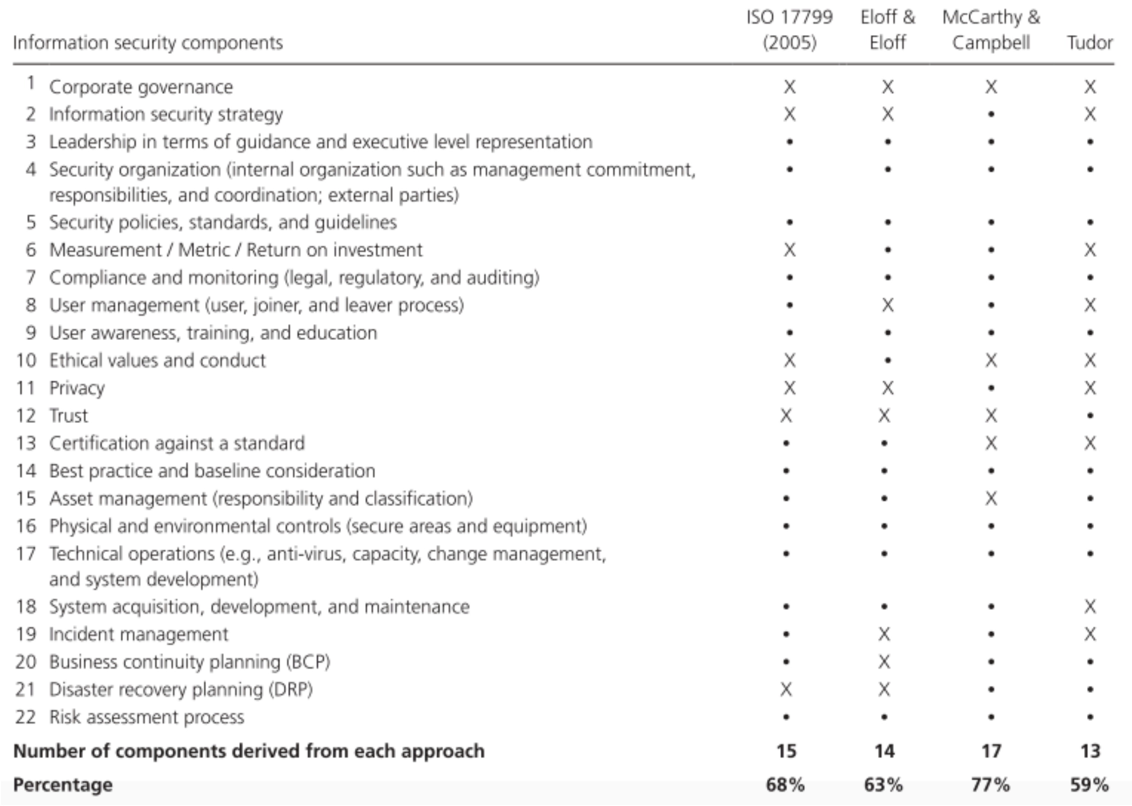
The third phase was characterized by information security being incorporated in the everyday practices accomplished by the employees. That created a sense of information security culture.

Finally, the fourth phase was where the ISG role was developed. One of the key drivers for this phase was risk prevention. ISG is described as "the overall manner in which information security is deployed to mitigate risks" [Veiga and Eloff 2007].

Afterwards, the authors set to analyse four current frameworks for ISG (ISO/IEC 177995, PROTECT, Capability Maturity Model, and Information Security Architecture), for each of them a table with a summary of ideas is displayed. And at the end, a new table is created, Table 5, comparing the information security components the authors found throughout their research of these four frameworks, links them to the respective document which they were discovered, and gives a percentage for the number of components derived from each approach.

Table 5 – ISG Approach Component Table

Source: Veiga and Eloff [2007]



	Information security components	ISO 17799 (2005)	Eloff & Eloff	McCarthy & Campbell	Tudor
1	Corporate governance	X	X	X	X
2	Information security strategy	X	X	•	X
3	Leadership in terms of guidance and executive level representation	•	•	•	•
4	Security organization (internal organization such as management commitment, responsibilities, and coordination; external parties)	•	•	•	•
5	Security policies, standards, and guidelines	•	•	•	•
6	Measurement / Metric / Return on investment	X	•	•	X
7	Compliance and monitoring (legal, regulatory, and auditing)	•	•	•	•
8	User management (user, joiner, and leaver process)	•	X	•	X
9	User awareness, training, and education	•	•	•	•
10	Ethical values and conduct	X	•	X	X
11	Privacy	X	X	•	X
12	Trust	X	X	X	•
13	Certification against a standard	•	•	X	X
14	Best practice and baseline consideration	•	•	•	•
15	Asset management (responsibility and classification)	•	•	X	•
16	Physical and environmental controls (secure areas and equipment)	•	•	•	•
17	Technical operations (e.g., anti-virus, capacity, change management, and system development)	•	•	•	•
18	System acquisition, development, and maintenance	•	•	•	X
19	Incident management	•	X	•	X
20	Business continuity planning (BCP)	•	X	•	•
21	Disaster recovery planning (DRP)	X	X	•	•
22	Risk assessment process	•	•	•	•
	Number of components derived from each approach	**15**	**14**	**17**	**13**
	Percentage	**68%**	**63%**	**77%**	**59%**

Ultimately, Veiga and Eloff [2007] consolidate all these analysis into a single comprehensive ISG framework, as seen in Figure 13. The authors also aimed for this framework to be used in organizations, so it could ensure a holistic perspective to the governing information security.

This new framework contains four levels, where Level A is composed of three ISG components (strategic, managerial and operational, and Technical). The strategic component will provide direction to the managerial and operational component, and so on.

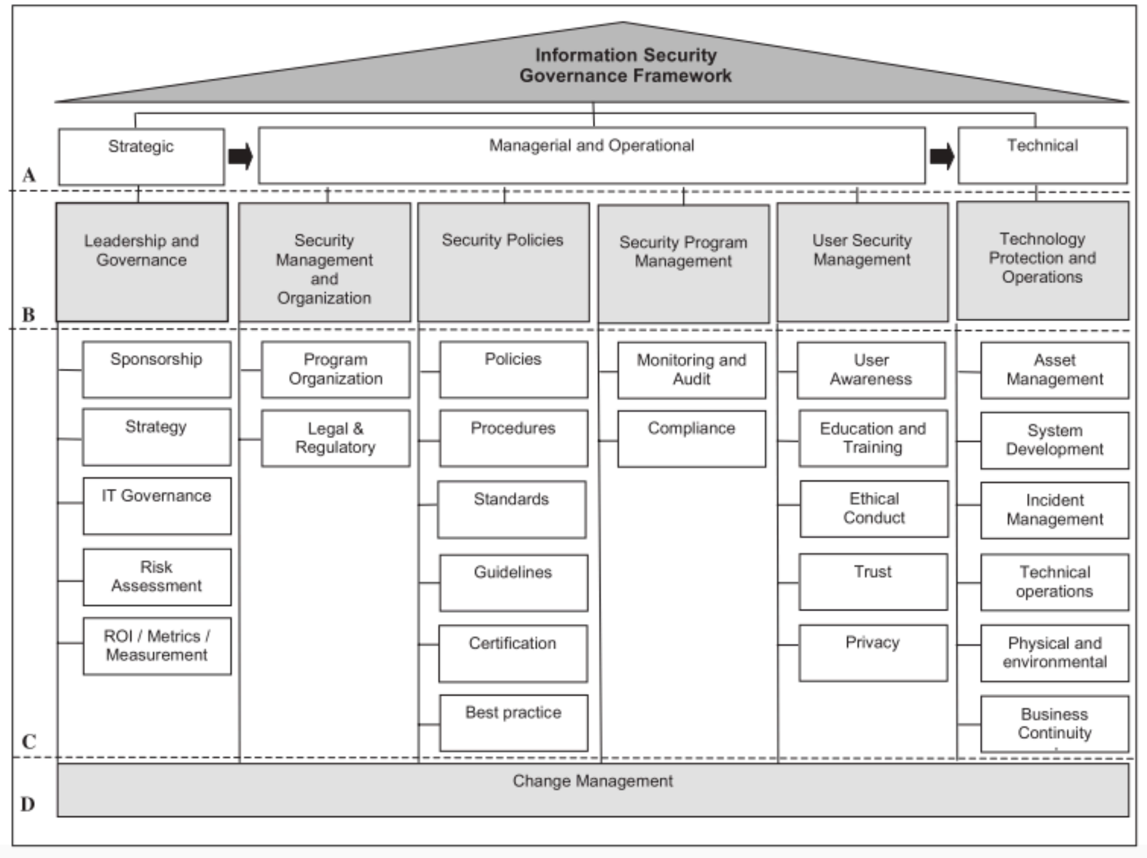


Figure 13 – ISG Framework

Source: Veiga and Eloff [2007]

While, Level B consists of six categories (Leadership and governance, Security management and organization, Security policies, Security program management, User security management, and Technology protection and operation) grouped according to the Level A categories. In Figure 13 the Level B categories are nested under their Level A counterparts.

In Level C, a comprehensive list of information security components is displayed, and they follow the same logic as the previous level (B). The components in this level nest under the previous level categories, in this case the six main categories of level B.

For Level D, represents the changes that can influence the six main categories of level B. Therefore, level D is depicted at the bottom of Figure 13 and as a single box, because of its influence in all of the level B categories.

2.3 Research Opportunity

After the review of the relevant documents in ISSG, similarities can be observed. One of those similiarities is the approach of governance in organizations, that seems to be intertwined at every level of the organization.

This bond between ISSG and the organization appears to be at a fault, when looking at the context in which this study is situated. Previous studies from Lopes [2012] and Lopes and Oliveira [2016] demonstrates a slow adoption of ISS policies by the Portuguese City Halls. Therefore by changing the focus from a single aspect (ISS policies) to a broader aspect (ISSG), this could help find and clarify the streghts and weaknesses that City Hall faces in what concerns ISS.

Hence, a research opportunity was identified, which gives attention to the Governance aspect of the Information Systems Security within the Portuguese local public administration.

3 Study Characterization

This chapter was created as a complement to the previous chapter, in which the literature review was used to characterize ISSG. The subsections of this chapter, are used to clarify the other components of the research question. The first step to answer the other components of the research question, which is "How to evaluate the ISSG of Local Public Administration bodies?", consists on elucidating what is a Local Public Administration body. Then, the second part consist on clarifying how to evaluate such body.

Therefore, in order to explain the last portion of the research question, one must contextualize the problem. Considering that the question focuses on a specific area and on a specific entity inside the portuguese public administration. Hence the description of the local public administration (City Halls), in part 3.1. Followed by a brief description of e-governance and the initiatives in Portugal, with studies that already had been carried out within the context of IS and governance, as well as the laws relevant to the ISSG.

Then, the second subsection 3.2, gives a more in-depth description of the methodology used in this study, afterwards a correlation with the study subject is established.

3.1 Local Public Administration in Portugal

Sousa and Matos [2004, pp. 43, 46] describe Public Administration as having two meanings: organic (bodies, services and State agents) and material/functional (set of actions as operations). These bodies are defined as public institutes, public associations, municipalities and autonomous regions. This public administration can be divided in three: central (operates within all the national territory), local (comprised of a territorial public entity – municipal administration) and state administrational services.

A further refinement on the Local Public Administration, are the Municipalities, and their divisions are described in the Constitution (Articles 235 and 236) [Assembleia Constituinte 2005] as "a collective of territorial people endowed with representative bodies, aimed at the pursuit of their population's own interest"; "In the continent the municipalities are parishes, cities and administrative regions. The autonomous regions of Açores and Madeira consists in parishes and cities". Also in Article 239 of the Constitution [Assembleia Constituinte 2005], the city representative bodies are comprised by a City Council and a City Hall". Throughout all these refinements of the public administration a hierarchy is shaped and its representation is demonstrated in Table 6.

Table 6 – Public Administration Hierarchy

Adapted from: Lopes [2012]

Public Administration	• Central			
	• Local	• Municipalities	• Municipal Boroughs / Parishes • Administrative Regions • Cities	• City Council • City Hall

In line with the structure presented in Table 6, the Portuguese territory is divided into continent (with eighteen districts) and two autonomous regions (Açores and Madeira), within these two divisions, they are also divided into 308 cities, where 278 are located in the continental territory and 30 are located on the islands [Instituto Nacional de Estatística 2018].

Appendix C – Portuguese Population by City Hall separates the city halls by district, territory (ICI zones) and dimension (related to the size of the population).

3.1.1 e-Governance

Initially, the term e-governance, was described as electronic government (in the US[25] the term used was digital goverment) and it was used to describe the government's use of IT to provide public services to its citizens. It was only after 2010, that the term came to be called e-governance, with a broader concept, that involves not only the electronic government but also other kinds of transformations (consequences of an evolution in the interoperability of IS in the public administration, in the global politics and in society) such as: e-services, e-public administration, e-administrative-politic relationships, e-politics, e-democracy and e-society [Soares 2009].

The term for electronic government originated in the 1970s, when a new ideology emerged, in which the reform/revitalization of the public sector was essential. This process of change/reform within these organizations (public administration) aimed to improve the performance of the sector (public sector) [Soares 2009].

[25] The acronym used to describe the United States of America.

In the 80's, a new society emerged; the information society, characterized by a strong and intense use of IT. Which was consolidated, in the 1990s, by an "explosion" in the use of the Internet. IT began to have more recognition, until this stage, their potential was only used to automate the internal functioning of government at the departmental level; that is, replacement of manual procedures by digital data processing systems [Soares 2009].

This view began to change when Al Gore, in 1993, highlighted the role of the information society in the renewal of society; and with it the importance of improving the performance of the public sector. In light of the speech given by Al Gore, the European Commission decided to outline a strategy, and in addition decided to create a group for its implementation, which culminated in the development of the Bangemann Report in 1994 [Soares 2009].

However, this report was not much "assimilated" or used by the EU[26], as it focused on the more private sector aspects of the economy. Again, stimulated by external examples, in 1999, the European Commission launched the "eEurope – An Information Society for All" initiative, which sought to accelerate the adoption of IT; in which one of the priority areas of action was online governance. Therefore, the importance of online goverment was once again reinforced at the European summits of Lisbon and Feira in 2000, where all EU members turned their attention to the development and implementation of e-government strategies and policies [Soares 2009].

In the purpose of demonstating these initial key marks for the term electronic government, Figure 14 was created. In it, the marks are inside the blue bloxes, while being distributed along the timeline, with the decade on top and on a coloured background.

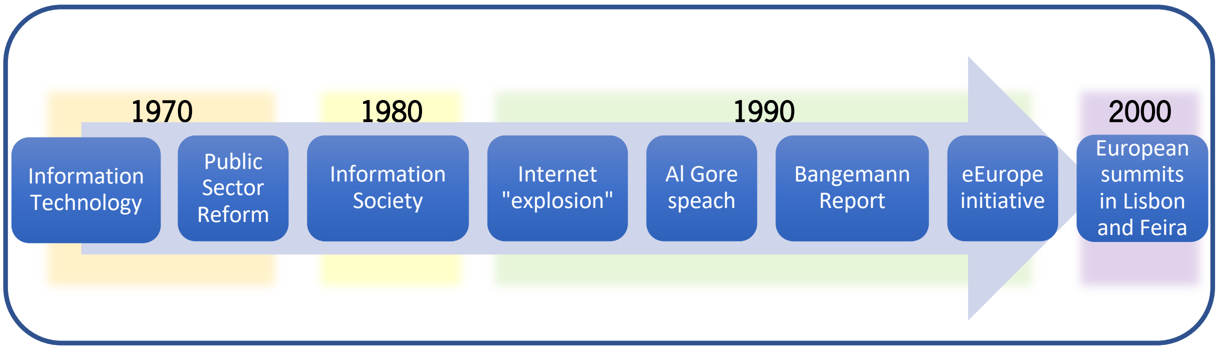


Figure 14 – Key marks for the Electronic Government term.

Adapted from: Soares [2009]

[26] Acronym used to describe the European Union

To present the next stages of the evolution, another table was create, Table 42 in

Appendix E – Evolution of e-Governance Initiatives in Portugal, that describes the key initiatives the Portuguese government has taken throughout the years focused towards the electronic government later turning into e-governance.

3.1.2 Relevant Studies

In the next subsections (3.1.2.1, 3.1.2.2, 3.1.2.3 and 3.1.2.4), data gathered from studies with relevant information about the Portuguese City Halls are going to be displayed, for a better contextualization and a broader approach of the study subject.

The first study to be reviewed is the "*Presença na Internet das Câmaras Municipais Portuguesas em 2016 : Estudo sobre Local e-Government em Portugal*" [Soares et al. 2017], a study conducted biannually by *GÁVEA – Observatório da Sociedade da Informação* from Minho University, that evaluates the modernization of the Portuguese City Halls. Then, a thesis "*Caracterização Infraestrutural, Aplicacional e Funcional das Tecnologias e Sistemas de Informação nas Câmaras Municipais Portuguesas*" [Almeida 2017], where the Information Systems and Technology of the City Halls is studied. Afterwards, data is gathered from the works of Lopes and de Sá-Soares [2010], Lopes [2012] and Lopes and Oliveira [2016], all of them surrounding the same main topic, the adoption of information system security policies by Portuguese city council's. Followed by a study from Querido [2014], that evaluates the IT governance in the Portuguese Public Administration.

3.1.2.1 Portuguese City Halls Internet Presence

This study, which evaluates the internet presence of city halls in Portugal, is conducted biannualy and it is currently in its ninth edition [Soares et al. 2017]. Its purpose is to depict the modernization status of the city council websites and their level of electronic relationship with their citizens. This study also performs an assessment of the evolution for each city council compared with previous editions. The study is in accordance with Minister Council Resolution number 22/2001, which states that the Public Administration Internet webpages should be subjected to a periodic evaluation by a mechanism that would assess their compatibility with basic quality criteria [Presidência do Conselho de Ministros 2001; Soares et al. 2017].

In the first study, conducted in 1999, only 153 websites were analyzed; that number matched with the city halls that had websites at that time. This number gradually evolved, culminating in 2009 when all of the 308 Portuguese city halls had websites [Soares et al. 2017].

The current study uses a two-phase information gathering process, where the first phase would verify the existence of a webpage for each City Hall and other data related to the website, then the second phase would focus on the assessment of each of the four evaluation criteria (Content; Accessibility, Navigation and Ease of Use; Online Services; and Participation); with a number between 0 and 1 attributed to each criteria, being 1 the highest.

The first and second phases of the current study occurred between November 2016 and January seven 2017, and the processes they used was the direct observation of the websites, and emails sent to all city halls (to the President, Vice President and First opposition Councilor) to assess their answering time and response relevance.

The data was than validated and treated similarly to the previous studies. Afterwards, different analysis perspectives were derived. For instance, a segmented analysis which city halls were separated by dimension (by the size of the population), and grouped in three categories: Large (population bigger than 100.000 residents), Medium (population bigger than 20.000 residents but equal or less than 100.000 residents) and Small (population inferior or equal than 20.000 residents); by zones (Islands – Coastal - Interior) (ICI); by NUTs II, divided by seven units (Alentejo, Algarve, Centro, Área Metropolitana de Lisboa, Norte, Região Autónoma dos Açores e Região Autónoma da Madeira); by districts (20 in total) and by political parties.

According to the 2017 study, from the top ten City Halls that had the most Internet Presence, sorted by their NUTs II classification, five were from the Centro, four were from the Norte and one from Açores and one from Algarve, the fifth and tenth place were ties. They were also sorted by population dimension, where five of them were from medium city halls, four were from the small and two were from the large city halls.

When analyzing each of the criteria, the best city hall for the first criteria was Bragança with a score of 0,900. For the second criteria, the best score was Alfândega da Fé, from the Bragança district. And the top from the third and fourth criteria were city hall's from Faro and Leiria district, respectively.

Other analysis, that evaluated the response time and quality were conducted. The analysis for the response quality, showed that only the Councilor's response, was behind the other responses verified, in comparison with the previous studies. And the response time analysis, revealed that the City Council president took a little bit longer to answer.

For the Dimension Analysis, from the total of 308 city halls, 24 (8%) were categorized as large, 99 (32%) were medium, and 185 (60%) were categorized as small. That being said, the best in the overall score by dimension were respectively from the Braga, Bragança and Vila Real district. The study also considers a regional analysis (zones and NUTs) on chapter seven.

The authors conclude the study verifying that the city halls have been evolving at a distinct level depending of the city council. The improvement level is relatively low considering the desired level, due to discrepancies from one city council to another. The criteria analysis shows the best scores being achieved in the first criterion. Lastly, as future work they note that there is still a lot of room for improvement and more online services can be provided to the citizens and with that growth a greater level of maturity should be achieved [Soares et al. 2017].

On another note, but relevant to this study, the first and third criteria respectively, Content and Online Services, possess inidicators that are relevant to governance, in which their existence is assessed. These indicator are C1.I6, that assesses the existence of a relevant legislation, copyright policy, content responsibility, privacy and security policy; and indicator C3, that assessed six services the City Halls provided and crossed examined them with itens such as the existence of the use of authentication to perform a service, which is also relevant to the study.

The mean value for indicator C1.I6 was 0,830, higher than the values for the 2014 (0,800) and 2012 (0,820) assessments. Also, in regards to indicator C3, the City Hall that possessed the highest value, for the overall services assessed, was CM Vila do Bispo, with a value of 0,431, whereas the other city halls had values from 0,350 and below.

3.1.2.2 Information Systems and Technology at the City Halls

In her study, Almeida [2017] creates a framework to characterize the infrastructure, application and organization of Information Systems and Technology (IST) in Portuguese City Halls. This framework is composed of five dimensions (Human and Financial Resources, Infrastructures, System and Application Software, IS Organizational Function, and Innovative Capability of the IS Function) along with their indicators and metrics.

For the first dimension, Human and Financial Resources, a number of four indicators and 14 possible metrics are presented. The second dimension, Infrastructure, also has four indicators but 21 possible metrics. Next for the System and Application Software dimension, there are seven indicators and 43 possible metrics. Then comes the seven indicators for IS Organizational Function and their 26 possible metrics. Lastly, the dimension for Innovative Capability of the IS Function has eight indicators and 33 possible metrics.

Building on this framework, the author creates a questionnaire in order to gather information related to the dimensions, allowing her to characterize the City Council IST. In addition, the author described the phases and activities used to design the questionnaire and its application in the Portuguese reality. Then, the results are analyzed by answering rate and by all of the items that characterizes the IST in the city halls (this one is summarized in Table 7).

Table 7 – Framework findings summary

Adapted from: Almeida [2017]

Framework Dimension	Results
Human and Financial Resources	Low percentage of workers to perform IST functions (1,6%). Academic Qualification – most have bachelor's degree. City budget for IST of 1,1% . Only 0,7% of available hours for training in IST area.
Infrastructures	Average of 212 PCs, 15 workstations and 12 servers. Used all data processing forms (real-time, online and multiprocessing). 89% use virtualization resources, hardware largely in this case. Cloud computing implemented in half of the City Halls, mostly for email and file storage.
System and Application Software	100% of the Operating Systems use Windows. 92% use open source software. 58% use helpdesk software. AIRC and Medidata use for different kinds of software solutions. Most used security applications are antivirus, antispam and access control software (sandbox and cryptography software not much implemented).
IS Organizational Function	IST managed by a third-degree unit (department) inside the City Halls in 66% of the cases. 41% of the reusability of the IST goes to the unit head and 43% to the computer technicians. 90% doesn't have a committee board. IS security management one of the most performed functions.
Innovative Capability of the IS Function	57% still use paper. 58% doesn't have smart cities project. 69% doesn't have a futuristic view. 83% doesn't have a portal or open data initiatives. 65% use IST for cooperation with other public bodies. 52% have some level of interoperability with other systems.

It is possible to observe from Table 7 that a low budget was destined to IST (1,1%) and that can be correlated with a small number of people working on IST functions (1,6%); also the low percentage of training in the are, that is below 1%. Besides, only half of the City Hall uses a cloud computing structure, and this structure is mainly used for email and file storage. In addition, the totality of City Halls use windows as their main operating system, and a high percentage (92%) also use an opens source software.

As for ISS management, which is one of the most performed functions in City Halls, though performed through the help of tools such as: antivirus, anti-spam and access control software.

3.1.2.3 Information Systems Security Policies in City Halls

Lopes and de Sá-Soares [2010] study was produced to find out about the reality of Portuguese City Council in adopting ISS policies (by quantifying it); because at the time they found few studies about the ISS area. Consequently, they conducted a survey directly to the 308 Portuguese municipal entities.

A survey was used because it enabled a clear, direct and objective answer to the question, by the respondents (the IS responsible in the municipalities). The contact was made by phone (in 299 City Councils) and six of them via email, after a previous phone call.

The authors structured the survey in four groups of questions (the characterization of the City council and respondent; followed by the question "Does the City Council have an ISS policy?", then they proceeded to questions concerning ISS policy features). The results discovered that only 38 (12%) of the city councils had adopted an ISS policy while 270 (88%) had not. When separated by electoral dimension, from those 38, 20 (52,6%) were medium sized municipalities, 9 (23,7%) were small, 6 (15,8%) were large and 3 (7,9%) were very large municipalities.

In 2016 the same model for the survey was conducted and compared with the previous one. The authors noticed a slight increase of 8% in the ISS policy adoption in the Portuguese City Council's; were 59 (20%) had an ISS policy [Lopes and Oliveira 2016].

3.1.2.4 Information Technology Governance in Portugal

In his study, Querido [2014] aimed to tackle the difficulty of implementing Information Technology Governance (ITG) in the Portuguese Public Administration. He believes that the plan created in 2011 for global strategic planning of rationalization and expense reduction called PGETIC (3.1.3.1) was a good start, however problems still persisted due to a slow evolution of this plan and its lack of a clear methodology that could be adapted to the department's specific needs and goals, although he points out that this plan could benefit from an existing method to implement its measures.

After analyzing the ITG frameworks available, COBIT 5 was decided as the most fit to be used when comparing with PGETIC. As for the strategic plan used in Portuguese Public Administration, he adds that is an overlong and verbose document, with almost 150 pages and has no clear and synthesized measures, thus being hard for an organization to implement it. Another remark he noticed was that the entity responsible for the measure is the organization itself, therefore being difficult to make someone responsible.

The author uses the Situational Method Engineering to create a new method, from existing methods (PGETIC and COBIT 5). This was used because of their uniform terminology and the ability to achieve four important qualities (Flexibility, Experience accumulation, Integration and communication, and Quality).

The artifact, which was a situational method to implement ITG in public administration, needed to achieve goals such as: ITG ease of implementation, along with alignment with goals and needs, PGETIC, and COBIT® 5 good practices. This method had to focus on the current situation of the organism and proposed improviments thru a Process Advice report. These improvements could be proposed incrementally in each cycle and feedback would be collected.

This study was also conducted using the DSR approach. For the evaluation process, the artifact was evaluated in a field study, in the IT Department of the Portuguese Air Force (part of the Defense Ministry of the Portuguese Public Administration). A total of eight people were interviewed. These interviews were performed during three phases and followed two different path of analysis, one using PEGTIC and the other using COBIT 5 Cascade.

Within the first path, there were some concerns about information security, the second also had similar results, with concerns about IT compliance, as well as information security and availability. The artifact developed was considered successful by the IT department of the Portuguese Air Force, and resulted in a document called Process Advice.

The author notes as a big advantage in this method, the fact that the insertions (method increments) could be performed without changing the method itself, therefore reducing the risk in complex projects. Though, within the organization viewed in the study, DCSI (*Direção de Comunicações e Sistemas de Informação*), their focus was on the full implementation of ITG, as well as rationalization of the IT sector, and some concern about information security.

3.1.3 Directives Applicable to Information Systems Security in Portuguese City Halls

There is a vast range of normative documents by which the City Halls need to be aware of and should adopt, in order to provide information security to their employees and citizens. Some of these normatives are grouped by categories and presented bellow. Those perceived to be the most important ones are described separate and in detail, shortly thereafter.

- Cybercrime
    - *Lei 109/2009, de 15 de Setembro*, that approves the cybercrime law;
    - European Union Council Recommendation of 25 June 2001 - on contact points maintaining a 24-hour service for combating high-tech crime.
- Personal data protection
    - *Lei 41/2004, de 18 de Agosto*, personal data protection and privacy in telecommunications;
    - Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000, on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;
    - Regulation (EU) 2016/679 General Data Protection Regulation (GDPR);
    - *Lei 58/2019, de 08 de Agosto*, protection of personal data and the free data movement (which executed the GDPR at a national level).
    - Resolução do Conselho de Ministros n°41/2018 – technical guidelines for the Public Administration regarding the security architecture of networks and information systems relating to personal data;
- Network Security
    - *Lei 5/2004, de 10 de Fevereiro*, electronic communications;
    - Opinion of the Committee of the Regions on the "Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions Network and Information Security: Proposal for a European Policy Approach" (2002/C 107/27);
    - Council Resolution of 22 March 2007, on a Strategy for a Secure Information Society in Europe (2007/C 68/01).
- Computer Security
    - *SEGNAC's 1, 2, 3 e 4*, respectively for classified matters, industrial security, communications security and computer security.

3.1.3.1 PGETIC

PGETIC stands for "*Plano Global Estratégico de Racionalização e Redução de custos nas TIC*" and was created by the Ministry Council Resolution 12/2012 [Agência para Modernização Administrativa 2015].

This strategic plan proposes 25 measures, structured in five strategic axes:

- I – Improve Governance Mechanisms: definition and implementation of ICT governance in Public Administration; architecture, standards and guidelines for information technology and systems; definition and implementation of a national information security strategy;
- II – Reduce Costs: evaluation of ICT projects and expenditures; communications rationalization and unified communications platform; cross-cutting measures fostered by ICT;
- III – Enhancing Administrative Change and Modernization: interoperability in public administration; electronic authentication and signing in administration;
- IV – Adopting Common Solutions: cataloging, sharing and standardization of state software; directory of good ICT practices;
- V – Stimulating Economic Growth: adoption of open software in state information systems; internationalization of methodologies, ICT solutions and public knowledge.

Since the implementation of the plan, only an overall of 56% of the plan was executed.[27] One of the activities of the plan to be implemented, was the measure "Definition and implementation of ICT governance in Public Administration". This activity proposed the development of a proposal for an ICT Governance model, which was then concluded [Agência para Modernização Administrativa 2015].

In one of the documents presented for the PGETIC strategy, an outlined table with the functions that are transversal in the support of the ICT governance were compared to the implementation level amongst countries such as Denmark, Canada, United Kingdom, France and Germany [Agência para Modernização Administrativa 2015].

[27] Shortly after retrieving this data, on the 29 of December of 2017, the website in which showed the progress of the plan was discontinued and changed for the website for "Estratégia TIC 2020", which was the plan that replaced the PGETIC. Therefore, no additional data was able to be found concerning this subject.

3.1.3.2 Estratégia TIC 2020

In July 26th of 2017, the Ministry Council Resolution n° 108/2017 was approved, where a new governance model for the Public Administration ICT, called *Estratégia TIC 2020*, focused on the digital transformation of the Public Administration, in order to enhance the quality of public services provided to citizens and businesses [Agência para a Modernização Administrativa 2018b].

Estratégia TIC 2020 follows some guiding principles, those are: governance, security, reliability and data privacy; digital transformation of the Public Administration focused on efficiency, usability and inclusion; and reinforcement of skills and resource sharing [Agência para a Modernização Administrativa 2017].

This new strategy has three main axels: integration and interoperability; innovation and competitiveness; and resource sharing and investment in digital competences. In total, these axels have twelve measures with thirty-seven actions, including activities that can be implemented in a cross-sectional and distributed way through different areas of the government.

Within the first axel, a governance model was created to allow the coordination of ICT investments and make the most of its transforming potential. The Measure1 (M01) is designed for ICT governance, its actions are to define and implement a cross-sectional governance model for the ICT; and to consolidate the ICT governance model for each governmental area.

Also, these actions have general activities that will be performed in accordance with each of the seventeen governmental areas in this strategy. These areas are presented in Appendix F – *Estratégia TIC 2020*, together with each individual area strategic project and the general activities best fit for each area.

The general activities for the first action are: Define and implement a cross-sectional governance of the ICT in the Public Administration(PA) (*Definição e Implementação de Governação transversal das TIC na AP*), and Establish a Project group for the ICT in Local PA and elaborate the ICT strategic plan in Local PA (*Constituir o Grupo de Projeto para as TIC na AP Local e elaborar o Plano Estratégico para as TIC na AP Local*).

The general activities for the second action are: ICT governance at a global and intraministerial level (CIO identification in the PA) (*Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP)*); Propose and implement a model to rationalize the ICT function in the Central PA (*Propor e implementar Modelo para a Racionalização da Função TIC na AP Central*); and Publish service catalogs, pricing and service levels of governmental areas (*Publicar catálogos de serviços, pricing e níveis de serviço das áreas governamentais*).

Along with this strategy, a council called CTIC (*Conselho para as Tecnologias de Informação e Comunicação na Administração Pública*) was created thru the Ministry Council Resolution nº 33/2016. This council was to ensure the development of a global planning and optimization strategy for the ICT in Public Administration [Agência para a Modernização Administrativa 2017].

3.1.3.3 General Data Protection Regulation (GDPR)

The objectives of this regulation is the "protection of natural persons with regard to the processing of personal data and on the free movement of such data", to protect the "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" and the free movement of personal data within the Union without restrictions [European Union 2016].

Therefore, to fulfill these objectives, a new type of role was introduced by this regulation, inside the fourth section of the document (article thirty-seven through thirty-nine), there is a description for the Data Protection Officer (DPO). These articles cover from the designation of such DPO, to their position and the tasks expected for such role.

A DPO should be designated when the process is carried out by a public authority or body, and the core activities consists of processing or monitoring in a regular and systematic basis a large scale of data subjects; or processing a large scale of special categories data pursuant and personal data, relating to criminal convictions and offences.

Also, a public authority or body may designate a single DPO for several authorities or bodies, depending on the organizational structure and size. The DPO should be a staff member or fulfill the tasks based on a service contract. Furthermore, it should be designated based on their professional qualities, such as knowledge of data protection law and practices and the ability to fulfil those tasks; also, it needs to be easily accessible from each establishment. Their contact details should be published by the controller or the processor and communicated to the supervisory authority.

The DPO should be involved in all issues that relates to the protection of personal data. The role also needs to perform tasks related to the previous context, provided that the controller and processor supports them, by giving the necessary resources for the DPO to carry out those tasks; and provide access to personal data and processing operations, in order for them to maintain their expert knowledge.

Yet, the DPO should not receive any instructions regarding the exercise of those tasks, and should not be dismissed or penalized for performing them. The DPO must also report directly to the highest management level of the controller or the processor.

The DPO may fulfil other tasks and duties, as long as it doesn't result in a conflict of interest. He must also be bound by secrecy or confidentiality concerning the performance of his tasks. And can be contacted by any data subject, regarding all issues related to processing of such subjects personal data and to the exercise of their rights [European Union 2016].

The tasks that a DPO shall perform are as follows: inform and advise the controller, processor or any other employee that carries out this type of processing, about the GDPR or other data protection provision; monitor the compliance of such relating to the protection of personal data (including assign responsibilities, raise awareness, training and related audits); provide advice when requested regarding data protection impact assessment and monitor its performance; cooperate with the supervisory authority; act as a contact point to the supervisory authority on issues related to processing and to be consulted regarding any other matter, when appropriate; finally the DPO should perform its task while regarding the risks associated with the processing operations.

3.2 Research Methodology

Enclosed within this part, is the clarification of the methodology used in this study, which is the Design Science Research (DSR). The reason behind this choice was that the methodology uses the method (in this case the development of an artifact) as an output. Another important factor considered when choosing this approach was the methodology's rigor, which is highly used in the IS field.

Both, Hevner et al. [2004] and Helms et al. [2010] described the DSR methodology as an "approach has gained popularity in the Information System (IS) domain as a research method, where the Information System development method itself or their outcome is the subject of study".

Other authors, such as Vaishnavi and Kuechler [2004], explains the popularity of this methodology in the IS field, with the fact of the community being a multi-pragmatic community. This type of community overlaps its research in sets of phenomena[28] of interest, and/or in methods of investigation[29].

The methodology also uses the design activity of the science of the artificial (aka design science) to create something new that doesn't exist in nature. Design Science is described as a body of knowledge

[28] "a set of behaviors os some entity(ies) that is found interesting by the researcher or a group" [Vaishnavi and Kuechler 2004].

[29] A set of activities that produces understanding (which is knowledge that allows for a prediction, of the behavior, of some aspect of the phenomenon) [Vaishnavi and Kuechler 2004].

about the artificial (man made) objects or phenomenon, designed to meet certain desired goals [Vaishnavi and Kuechler 2004].

Hevner et al. [2004, p. 82] goes to add that "Design Science is inherently a problem solving process". Design Science possess an inner environment (a set of *components*, that is comprised by the artifact and its relationships) and an outer environment (a set of *external forces* and effects that act on the artifact, the artifact's organization), and the *interface between* them is what meets certain desired goals [Vaishnavi and Kuechler 2004].

By using an analogous perspective to consider design as an interface between the two environments and that can be thought as a mapping from a function space (functional requirement) to an attribute space (artifact satisfaction), Takeda et al. [1990] state that "design is not a simple mapping process but rather a stepwise refinement process where the designer seeks the solution that satisfies the constrains", therefore design is knowledge in the form of techniques and methods for performing this mapping [Vaishnavi and Kuechler 2004].

March and Smith [1995, p. 253] state that design science produces four types of outputs or artifacts: constructs (concepts from the domain vocabulary), models (set of prepositions or statements expressing the relationships among constructs), methods (set of steps used to perform a task) and implementations (realization of an artifact in its environment). Vaishnavi and Kuechler [2004] consider yet another form of output or artifact, called better theories (artifact construction analogous to experimental natural science, coupled with reflection and abstraction; where a resulting artifact could be quite similar to different research communities, but their stages of development and the measures used to evaluate them would be different for each community, thus differing in perspective).

However, Iivari [2007] does not share the same vision, stating that "In a way, this is a very general classification that can be applied to any IT systems. Unfortunately, its application is not always straightforward, since the classification so strongly reflects data/information modelling". In contrast with Iivari, and going along with the others, Hevner et al. [2004, p. 82] add that "The result of design-science research in IS is, by definition, a purposeful IT artifact created to address an important organizational problem. It must be described effectively, enabling its implementation and application in an appropriate domain".

Also, a multi-pragmatic community such as IS, is forced to considered the most fundamental bases of socially constructed realities. This community operates under the assumption created by DSR, where the methodology can interactively determine the reality, and knowledge emerges from the research effort. This meta-level approach used by DSR contrasts with earlier works of a more traditional type of research, such as positivist and interpretative [Vaishnavi and Kuechler 2004].

For Vaishnavi and Kuechler [2004], DRS is a combination of an analytical technique and perspectives used to perform research in IS. It involves the design of novel or innovative artifacts; their usage and performance are going to be analyzed to improve and understand the behavioral aspects of Information Systems (IS). These artifacts may include algorithms, human/computer interfaces and languages or system design methodologies. DSR can be found in a broad spectrum of disciplines and fields (such as Engineering and Computer Science), using various approaches, methods and techniques.

Also in their work, Vaishnavi and Kuechler [2004] present a method for DSR while specifying all the phases. Those phases include artifact design, construction, analysis and evaluation. The authors continue the document by focusing on the process through their outputs Figure 15.

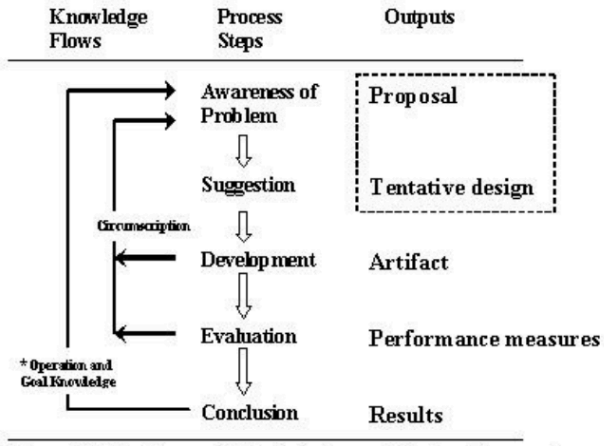


Figure 5. The General Methodology of Design Research

Figure 15 – General Methodology of Design Research

Source: Vaishnavi and Kuechler [2004]

Vaishnavi and Kuechler [2004] outline that the typical DSR effort proceeds as follows. It starts with Problem Awareness, which according to Hevner et al. [2004], happens to be based on the problem relevance and its importance for resolving the various issues affecting the organization. In the end, a Proposal (that can be formal or informal) is created for a new research effort.

This Proposal is then, almost immediately, followed by the Suggestion phase. That is essentially a creative step in which a new functionality is imagined based on the innovative configuration of existing elements or new and existing elements, in some cases a prototype. The output for this phase is entitled Tentative Design.

Right after the suggestion phase is the Development phase, where the Tentative Design is implemented. The implementation techniques may vary, depending on the artifact to be constructed. The output for this phase considers the novelty the design of the artifact brings. Therefore the output for this phase is called Artifact design.

The Evaluation phase comes after the artifact is constructed, in the development phase. In this phase, the artifact needs to be evaluated according to the criteria that are always implicit and often explicit in the Proposal. Deviations from expectations, either quantitative or qualitative, are carefully noted and must be tentatively explained. This phase outputs are the Performance Measures.

Lastly, the Conclusion phase is the finale of a specific research effort. Usually, it is the result of the satisfaction of the artifact. The Results, the output for this phase are either categorized as "firm" or "loose ends".

In addition, Hevner et al.[2004] created a conceptual framework for IS research, with seven guidelines (displayed in Table 8) that were derived from the fundamental principle of the DSR. This principle takes knowledge and understanding of the design problem and its solution to attain the development and application of an artifact [Hevner et al. 2004].

The guidelines intent is to assist researchers to understand the requirements for an effective DSR. Although researchers are cautioned to use their creative skills and judgment to determine to which extend they should apply each of the guidelines. Nonetheless, all of them should be addressed in some manner, in order for the research to be deemed complete.

Table 8 – Design Science Research Guidelines

Adapted from: Hevner et al. [2004]

Guideline	Description
1 – Design as an Artifact	DSR must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
2 – Problem Relevance	The objective of DSR is to develop technology-based solutions to important and relevant business problems.
3 – Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
4 – Research Contributions	Effective DSR must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
5 – Research Rigor	DSR relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
6 – Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
7 – Communication of Research	DSR must be presented effectively both to technology-oriented as well as management-oriented audiences.

Hevner et al. [2004] summarize the guidelines as: 1 – the creation of an innovative purposeful artifact; 2 – specify the problem domain; 3 – must yield utility to a specific problem and be thoroughly evaluated; 4 – novelty working with the artifact (to solve an unsolvable problem; or better solve, in a more effective and efficient manner, a known problem); 5 – an artifact rigorously defined, formally represented, coherent and internally consistent; 6 – the artifact creation processes incorporate or enable a search process, where a problem space is constructed and a mechanism is posed or enacted to find an effective solution; and 7 – the results are communicated effectively to a technical and managerial audience.

In their work, Helms et al. [2010] add Hevner et al. [2004] guidelines on top of the five process steps mentioned in Vaishnavi and Kuechler [2004] Figure 15. For the Problem Awareness step, guidelines 1 and 2 are used, the need to develop a new and innovative artifact; and the need the artifact has to respond to a clear and relevant business problem, that was identified by researchers.

The second step, Suggestion, is comprised of guidelines 3 and 4, the definition of proper evaluation measures and methods to verify utility, quality and efficacy of the design artifact; and need of the outcome of the research to have a clear contribution and not be limited to the usefulness for the practitioners. This step is followed by the third step (Development), that encompasses the application of the proper research methods in developing the artifact (guideline 5) and the need of several interactions in order to fine-tune the artifact to the initial requirements (guideline 6).

The Evaluation step (4) uses the third guideline, where the artifact needs to be evaluated using previously defined evaluation measures and methods. Which is then followed by the Conclusion step, that uses guideline 7, to communicate to practitioners and researches the results.

From this conceptual framework for IS research created by Hevner et al.[2004], Hevner [2007, p. 88] later borrowed it to overlay his three cycle view for DSR, as seen on Figure 16.

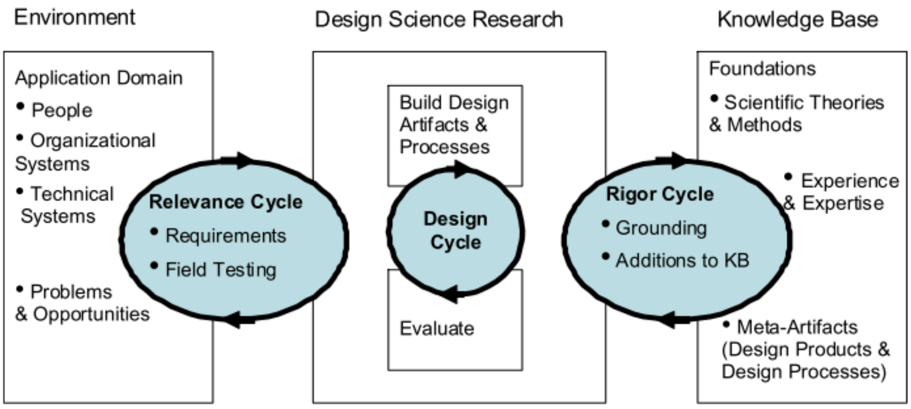


Figure 16 – DSR Cycles

Source: Hevner [2007]

As represented in Figure 16, the Relevance Cycle inputs the requirements from the contextual environment into the research and introduces the artifacts into environmental field testing. Thus, acting as a bridge for the contextual environment of the research project with the design science activities.

Followed by the Rigor Cycle, which provides grounding theories and methods along with domain experience and expertise from the foundations knowledge base into the research and adds the new knowledge generated by the research to the growing knowledge base. Consequently, connecting the design activities with the knowledge base of scientific foundations, experience, and expertise that informs the research project.

Lastly, the Design Cycle, that supports a tighter loop of research activity for the construction and evaluation of design artifacts and processes. Therefore iterates between the core activities of building and evaluating the design artifacts and processes of research.

By using DSR, Helms et al.[2010] observed that even though is useful, but generic, the approach had greatly facilitated the development of the artifact. Since the approach possesses a clear structure, thus, being able to critically evaluate the problem. The evaluation used the guidelines as an structure.

The use of these guidelines encouraged the authors to review various bodies of literature. Which lead the development of their artifact to be based on proper research methods, and enabled it to have continuous improvement between interactions. This also encouraged the authors to disseminate their findings. In a manner of which the approach exerts more rigor and relevance to the research. Therefore, the continuous improvement between interactions is considered essential in improving the design [Helms et al. 2010].

3.3 Instantiations

The DSR methodology was chosen because it uses the development of the artifact, in this case, both the evaluation instrument and the methodological guide, as the subjects of the study. The methodology also presents a clear structure, with process steps, outcomes and guidelines, to guide in the artifact development. Also, being a widely used methodology in the field of IS, since DSR requires a rigorous evaluation.

Particularly to this research work, the problem awareness step happened based upon the understanding urgency that came from a problem with the information systems security in the local public administration (thru the analysis of the relevant literature) and the need for a new perspective. Through a shift in perspective, of the analysis for the security of the information systems in local public administration; which led to a new perspective, one where the governance of the security of the information systems in local public administration was the main focus, and the need to build an instrument that could evaluate it.

It is expected of the artifacts and their future implementations, that they help in answering the question of how to evaluate the governance of information systems security in the local public administration, which is the main research focus of this perspective.

The next process step is entitled Suggestion, which corresponds to the Design Cycle and guidelines 5 and 6. This step appears immediately after the Proposal; in order to give substantial support to the construction of the artifacts, that is based upon an instrument to evaluate the ISSG of the local public administration. A literature review (Chapter 2 and 3) was carried out.

As part of the Literature review conducted, two parallel investigations were conducted. The first (Chapter 2) focused on the main concepts and characteristics for governance. The construction of the evaluation instrument also required a verification of the possible frameworks used so far; with the purpose of obtaining firm approaches for the evaluation instrument and compare those with the instrument created to evaluate ISSG in local public administration. The second investigation (Chapter 3) focused on the Portuguese Local Public Administration.

Another part of the creative process is based upon the innovative configuration of existing elements, or new and existing elements an instrument is planned. In this case, these elements were the concepts of ISSG applied to local public administration, more concretely the Portuguese City Halls. Therefore, being the primary contribution of this research, the conception of an evaluation instrument in order to evaluate the ISSG in the Portuguese public administration fulfills this part. In addition, and a secondary contribution of this research is the creation of a methodological guide, to be used to implement such evaluation instrument. Those two are the result of the Suggestion step, being called Tentative Design.

The Development step (corresponds to the Design Cycle and guideline 1) results in the implementation of the Tentative Design. Vaishnavi and Kuechler [2004] considers as an output, the novelty the design of the artifact brings; which in this case is the creation of an evaluation instrument for ISSG of the local public administration. The outputs for this phase were the design of two artifacts, an evaluation instrument and a methodological guide. Which could be used together in the future, to evaluate the ISSG in the Portuguese Local Public Administration.

The step entitled Evaluation, that also correspond to the Design Cycle and the third guideline, states that once built, the artifact needs to be evaluated according to the (implicit and explicit) criteria of the Proposal (Problem Awareness step). This stage, presented in 5.3, it will not be carried out in full in this research work. Therefore, the artifact will not be fully evaluated against the criteria of validity and reliability.

Ultimately, the final step, Conclusion (where it consists of the knowledge acquired in the Cycles of Rigor, Relevance and Design and corresponds to guideline 4) mentions the clear and verifiable contributions provided by the design of the artefact. This last step of the work will be carried out in Chapter 6.

4 Artifact Creation Process

After the description of the methodology used in this thesis, chapters 4 and 5 were created to explain the artifact creation process. Within this chapter, the initial steps produced according to the methodology are explained, these steps serve as a base for the creation of the outputs or final artifacts of this study. In part 4.1, the first three steps of the methodology are presented, from the problem awareness to the initial part of the development of the artifact. As a complement of this chapter, Chapter 5, will present the final product (the evaluation instrument) along with the secondary artifact the methodological guide.

4.1 ISSG Evaluation Instrument

In virtue of the DSR methodology used by this study, the artifact created had to go through a series of steps in order for its completion. Inside this part, and the following parts in the next chapter of the document, the creation of such artifact is broken down by the DSR steps. The steps are explained in the following sections (4.1.1 - Problem Awareness / Proposal, 4.1.2 - Suggestion / Tentative Design, 4.1.3 - Development / Artifact also present in 5.1 and 5.2, 5.3 - Evaluation and Performance Measures, 5.4 - Conclusion). Each section title, in this chapter, is named after a DSR step and their correspondent outcome (after the slash symbol). The same naming structure is used in the next chapter for sections 5.3 and 5.4. Below the section title, the corresponding DSR guidelines are displayed, and in the lines beneath them the information is presented accordingly.

4.1.1 Problem Awareness / Proposal

Guidelines 1(Design as an Artifact) and 2 (Problem Relevance)

During section 3.1, no evidence of a ISSG plan was found, even though the government had a strategic plan in place called PGETIC[30] that would focus on the information systems of the public administration and would implement an information security strategy for them, but the percentage of the results were low.

[30] Initially was the PGETIC, as of 2018 the strategic plan changed to *Estratégia 2020*.

Another information to complement that strategy plan was the study that aimed to portrait the ITC in the City Halls that observed a low allocation of investment of the City budget for IST resources, in addition a low percentage of human resources to perform IST functions, and only 0,7% allocated to training. But it also revealed that most of their human resources have a bachelor's degree and that IS security-related measurements is one of the most performed function.

These measurements in IS security come to support the studies which evaluated the ISS policies in the City Halls that observed a slight increase (8%) in the amount of City Halls that had implemented these types of policies.

Nonetheless the governance of ISS also has to be in compliance of laws and regulations, and all of the City Halls face a new regulation (GDPR) surrounding data privacy that became effective in May 25th of 2018.

To understand the reasoning behind these low numbers in the adoption of ISS policies by the Portuguese City halls, a shift in perspective was needed. This would broader the investigation from a single aspect (aka. ISS policies) to a greater aspect, in this case the ISSG of Portuguese Local Public Administration (City Halls). The investigation of the ISSG aspect comes at a time new laws put in place and set to change the City Halls environment. Also, no other ISSG study for the Portuguese Public Administration was found. Thus, no evaluation of their initial efficiency was able to be analyzed.

This reason became the main focus for this research; and a proposal to create an instrument to evaluate the ISSG in the Portuguese Public Administration was prepared and sent, in the form of an official admission request for a thesis, to the academic board for approval on October 2nd 2017, along with a work plan. Consequently fulfilling the problem awareness process step.

4.1.2 Suggestion / Tentative Design

Guidelines 3 (Design Evaluation) and 4 (Research Contributions)

After perceiving the problem in hand and suggestion made, in the official admission request along with the work plan on October 2nd 2017, to recommend this subject of study to the academic board. Once the proposal was approved, the first draft containing the idea for the evaluation instrument, with the defined objectives, literature review and research strategy, was submitted in the form of a Dissertation Project on January 22nd 2018.

4.1.3 Development / Artifact

Guidelines 5 (Research Rigor) and 6 (Design as a Search Process)

When it was time to address the development of the instrument, some factors (such as population size and information retrieval) had to be considered. Therefore, given the population size of this study (which are the 308 City Halls across Portugal), the most adequate method would be a mail questionnaire. Even though, personal interview is the most powerful, it wouldn't be practical in this context since they are time-consuming and relatively costly [Kerlinger 1986].

The features provided by using a questionnaire fit the instrument intentions. Since it can support the study of a large amount of population (or universe) from the selection and the study of samples (chosen from the population) to uncover the relative incidence, distribution, and interrelations of the sociological and psychological variables. The questionnaire also help to accurately assess the characteristics of a whole population of people [Kerlinger 1986].

Once chosen the type of instrument, the subsequent step was to follow the 5th guideline which focuses on the research rigor, to extract (from the relevant documents in the literature review) the most relevant aspects of ISSG, to construct the instrument. To accomplish this guideline, first a comparison of the relevant documents was produced (cf. 4.1.3.1) that led to an extraction of some relevant elements of ISSG.

Then, the following step, was the creation of the concept tree (cf. 4.1.3.3), where those relevant aspects would be arranged in a structure, for easy understanding and being able to be easily converted in questions for the questionnaire.

Afterwards, these structurated aspects were used as the basis for the questions of the instrument. The construction of the instrument and their respective methodological guide are presented respectively in parts 5.1 and 5.2.

4.1.3.1 Documents Comparison

To begin constructing the instrument, a singular notion of what ISSG had to be achieved. So, in order for that to succeed, a comparison of the relevant documents of ISSG (that were presented in part 2.2.3.2 of the Literature Review) had to be produced. It started out by creating a summary table for each document, separated by their key aspects. These summary tables are available on Appendix G – Artifact Construction: Instantiations of Relevant ISSG Documents. Once ready, the key aspect tables were created, which grouped the key aspects, found throughout each relevant document in question, onto a single table for each key aspect.

Those key aspects include a document overview, with a brief description of the reason that document was developed, what is the use of said document and so on. Next, the governance definition, with how the documents interpret ISSG. Then, the objectives of the document are exposed. Subsequently the dimensions, attributes, metrics and analysis found within the various document are displayed.

Once each aspect is analyzed separately, a structure with the key topics gathered from these key aspects summary tables, is portrayed side-by-side for a better comprehension of ISSG.

- **Document Overview**

The analysis starts with key aspect for the Document overview. The results for this key aspect from each document summary table is grouped and then presented in Table 9.

Table 9 – Comparison of Relevant Documents – Document overview aspect

Document	Document Overview
COBIT® 2019	COBIT is described as "a framework for the governance and management of enterprise information and technology, aimed at the whole enterprise" [ISACA 2018c, p. 13]. Comprised of four publications (Introduction and Methodology; Governance and Management Objectives; Designing an Information and Technology Governance Solution; and Implementing and Optimizing an Information Technology Governance Solution) that provides a foundation to create a customized governance program for Information and Technology (I&T), that is the right-size for the needs of the enterprise.
NIST SP 800-100	The document was created by the American Federal Government to manage and govern Information Security. Designed to direct managers so they can establish and implement ISG in their organizations.
ISO/IEC 27014:2013	This document is an International Standard that provides guidance on Information Security Governance; and is applicable to all types and sizes of organizations. This version of the document was created in 2013 by a joint technical committee of ISO and IEC participants, that meets every 4 years.
GTAG® 15	The document consists of a practice guide which provides detailed guidance for conducting internal audit activities. A thought process to determine what matters to the organization and to assist the Chief Audit Executive (CAE) incorporate into the audit plan an audit of ISG, are some of the document's approaches. The audit plan will focus on the organization's ISG activities and if those activities delivers correct behaviors, practices and IS execution.
Veiga & Eloff Framework	Created with the intention to serve as a starting point for ISG. Derived from an analysis of four existing ISG approaches, to create a new more comprehensive ISG framework.

Some considerations can be drawn from these findings, for instance most of these documents are meant to be used as a guide for governance, only NIST SP 800-100 and the Veiga & Eloff framework differ from this purpose. The first is used to direct the managers, while the latter is used as a starting point for ISG.

Also, COBIT® 2019, ISO/IEC 27014 and Veiga & Eloff framework focuses on a broad audience, whereas NIST SP 800-100 focuses on the American Government and the GTAG® 15 focuses on the Chief Audit Executive.

Another detail that can be pointed out is that only ISO/IEC 27014 has a timeframe for review of the document, which seems to be relevant since the majority of the documents express concerns about the ever changing environment and technology.

Even though NIST SP 800-100 is focused to direct managers of the American Government on how to establish and implement ISG in their organization, some of its content can be tailored to fit the context of this study, since the study focus is to evaluate the governance of the ISS in the local public administration.

From these considerations, three points are exposed: the type/purpose of the document itself, the focused audience and the review timeframe for the document.

- **Governance Definition**

The next aspect to be analyzed is the Governance definition each document portraits. Likewise, each of the results are displayed in Table 10.

Table 10 – Comparison of Relevant Documents – Governance definition aspect

Document	Governance Definition
COBIT® 2019	The document describes the governance discipline as: "ensures that the stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives" [ISACA 2018d, p. 15].
NIST SP 800-100	ISG is defined in this document as: "the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk" [Bowen et al. 2006, p. 2].
ISO/IEC 27014:2013	The document describes ISG as "system by which an organisation's information security activities are directed and controlled" [ISO/IEC 2013, p. 1].
GTAG® 15	The document doesn't define ISG, since it states that multiple definitions can be found across organization and standard setting bodies [Love et al. 2010, p. 1]. Although it presents three common themes: Promote good IS practices with clear direction and understanding at all levels. Controlling IS risks associated with business. Create overall IS activity that reflects organization's needs and risk appetite levels.
Veiga & Eloff Framework	The document describes ISG as: "the overall manner in which information security is deployed to mitigate risks" [Veiga and Eloff 2007, p. 362].

From the results presented in Table 10, the definition is written at a higher level in ISO/IEC 27014 and Veiga & Eloff framework. The former describes ISG as a system, while the latter calls it an "overall manner". NIST SP 800-100 uses a more granular definition on what ISG is supposed to be about, describing it as a process.

Even though COBIT® 2019 describes the governance discipline, that ISG is a part of. The document also makes it in a granular manner, presenting the tasks in which the EDM processes are included. Though, in Table 11 of the next key aspect (objectives), a more granular detailed explanation (regarding ISG's definition) is given for both COBIT® 2019 and NIST SP 800-100.

The only document that doesn't give a definition to ISG is GTAG® 15, but it does present some common themes extracted from multiples definitions. Also, these themes should be better considered in the following key aspect, as mentioned in the above paragraph, since it refers to a more granular view of ISG and it is in line with some of the EDM process.

In addition to the points pondered above, some other considerations are in order. For instance, both COBIT® 2019 and NIST SP 800-100 discuss objectives. While COBIT® 2019 credits the achievement and compliance of agreed upon objectives, NIST SP 800-100 believes that information security strategies should be aligned and support business objectives.

Following the same line of thoughts, COBIT® 2019 and GTAG® 15 also discuss about needs. COBIT® considers the needs of the stakeholders, whereas GTAG® 15 contemplates the needs of the organization.

Another discussed subject in GTAG® 15, that can also be encountered in NIST SP 800-100 and Veiga & Eloff's framework, is risk. The risk has a different application in each of these documents. GTAG® 15 refers to it as information security risks associated with the business and risk appetite levels. However, NIST SP 800-100 deems it as risk management, and Veiga & Eloff deems it as risk mitigation.

Lastly, yet another matter encountered in these results table surrounds the EDM processes. The majority of the documents, such as COBIT® 2019, ISO/IEC 27014 and GTAG® 15, all contemplate the Direct and Monitor process, although their perspective shifts for each document.

In the Direct process, COBIT® 2019 addresses it as direct through prioritization and decision making, while ISO/IEC 27014 refers to the manner which the information security activities are directed, and GTAG® 15 uses the information security practices to have a clear direction.

As for the Monitoring process, it is only referred like this in COBIT® 2019. In the others documents (ISO/IEC 27014 and GTAG® 15) is referred as Control. COBIT® 2019 focuses on performance monitoring, whereas ISO/IEC 27014 focuses on information security activities being controlled; and GTAG® 15 uses control as one of the themes for controlling information security risks.

The only document that explicitly refers to all of EDM is COBIT® 2019, since is the only one that references the evaluate component in its governance definition, expressing that conditions and options are evaluated to determine balance.

- **Objectives**

Continuing with the analysis of the results, Table 11 presents the results for the Objectives aspect. Again, each row represents the result for each document.

Table 11 – Comparison of Relevant Documents – Objectives aspect

Document	Objectives
COBIT® 2019	To make a clear distinction between governance and management Types of activities. Organizational structure. Purpose.
NIST SP 800-100	Ensure agencies are proactively implementing appropriate information security controls to support their mission at a cost-effective manner, while managing evolving risks. Ensure appropriate level of support of agency's mission. Properly implement current and future information security requirements. Establish in each agency a formal ISG structure.
ISO/IEC 27014:2013	Strategic alignment Align the information security objectives and strategy with business objectives and strategy Value delivery Deliver value to the governing body and to stakeholders Accountability Ensure that information risk is being adequately addressed
GTAG® 15	Define ISG. Help internal auditors understand the right questions to ask and know what documentation is required. Describe the IAA's role in ISG.
Veiga & Eloff Framework	Evaluate the four current approaches of ISG frameworks to construct a new comprehensive ISG framework, that considers the technical, procedural and behavioral components. To provide an all-encompassing (single point of reference) for ISG.

During the analysis of Table 11, some similarities with the first result Table 9 were encountered. The description of the objectives differs, from document to document, in relation to what the document focus was in Table 9. For instance, NIST SP 800-100 and ISO/IEC 27014 focus on the tasks or principles of ISG. Whereas in COBIT® 2019 a broader approach is described, focused on the full spectrum of the governance. Another shift in focus happens in the GTAG® 15, where the main focus is to help the CAE.

Lastly, the focus on Veiga & Eloff's framework is directed to the framework creation, and the aspects of ISG itself.

Apart from these differences in focus, a few links between rows and between tables can be perceived. First the mention of a structure by both COBIT® 2019 and NIST SP 800-100. For the first this structure comes from an organizational point of view, while for the second, is a more formal ISG structure in each agency.

Also, the GTAG® 15 and Veiga & Eloff makes references to ISG, the former tries to define ISG and tries to describe the IAA's role in ISG. As for the latter, tries to create a comprehensive ISG framework, to be used as a single point of reference.

Aside from these reflections, the subsequent ones are either mentioned in both Table 10 and Table 11 (e.g., risk, controls, support and strategy), or are mentioned more than once in this results table (e.g. support).

The risks are mentioned in both NIST SP 800-100 and ISO/IEC 27014, as well as in the governance definition results Table 10. In Table 11, NIST SP 800-100 portrays them as managing evolving risks, while ISO/IEC 27014 emphasizes on the risks being addressed.

Next up on the reflections are the controls, they appear inside NIST SP 800-100 results table for both governance definition and objectives. The initial focuses on the adherence to internal controls, while the succeeding focuses in the appropriate implementation of information security controls.

The same goes for support, that is mentioned twice in NIST SP 800-100. Once in their governance definition, where its attention is to support management structure and processes, also support business objectives; and in the objectives table is also cited, related to support the agency's mission.

Strategy is also mentioned in NIST SP 800-100 for the information security strategy. And is mentioned in ISO/IEC 27014 as strategic alignment, alongside the others objectives of value delivery and accountability.

Another topic, that appears for the first time in this table in NIST SP 800-100, and is considered important in the scope of these study, is the cost-effective manner.

- **Dimensions**

For the subsequent results table studied, the Dimensions aspects are to be presented and explored in Table 12.

Table 12 – Comparison of Relevant Documents – Dimensions aspect

Document	Dimensions
COBIT® 2019	1. COBIT Principles 2. Governance System and Components 3. Governance and Management Objectives 4. Performance Management 5. Design and Tailored Governance System 6. Implement Enterprise Governance of I&T
NIST SP 800-100	1. Requirements 2. Components 3. Challenges and Keys to Success
ISO/IEC 27014:2013	1. Roles and Responsibilities (Definition) 2. Principles 3. Processes
GTAG® 15	1. Information Security Governance 2. Effective Information Security Governance 3. Efficient Information Security Governance 4. Chief Audit Executive (CAE) concerns about ISG 5. Internal Audit Activity (IAA) role in ISG 6. Auditing ISG 7. Samples (questions/topics)
Veiga & Eloff Framework	1. Information Security Phases 2. ISG framework – existing approaches 3. New approach to ISG framework Technical components Procedural components Human Behavioral components

Similar to the previous Table 11, this table also has content adjusted according to the document overall focus. Nonetheless, some common ground between documents could be found. For example, the mention of processes in both ISO/IEC 27014 and COBIT® 2019, even though in COBIT® those processes come within the governance objectives. These same processes are also mentioned in Table 9 as EDM processes. In this table, both documents don't go into details of these processes, only mentioning them as processes like in ISO/IEC 27014 and within the COBIT® 2019 Reference Model of Governance and Management Objectives, part of COBIT® 2019 Core Model.

Another common ground surrounds the element of roles and responsibilities. In ISO/IEC 27014, roles and responsibilities are only mentioned, similar to processes for this table, unlike in GTAG® 15, where roles and responsibilities are intrinsic to the CAE's concerns and the IAA's role in ISG.

Lastly, GTAG® 15, Veiga & Eloff and COBIT® 2019 cite components, but only Veiga & Eloff and COBIT® 2019 describe them. Veiga & Eloff separates the components into groups/categories (Technical, Procedural and Human Behavioral), while in COBIT® 2019 these components are into seven types, seen in Table 13 number 2.2 - Components of a Governance System.

Also, something worth mentioning is the effective and efficient ISG, that appears in the GTAG® 15 results. The importance of this reference is connected to the cost-effective objectives, mentioned in NIST SP 800-100 results in Table 11.

The same goes for another topic, Principles, usually described as a set, but in this aspect is only mentioned as principles. For both COBIT® 2019 and ISO/IEC 27014, their principles are later described in the attributes aspect table (Table 13). However, these principles are focused on their respective documents; for this reason this topic won't be included in Table 16 for the key topics, but their similarities will be discussed in the attributes aspect.

Another worthy mention for this aspect concerns NIST SP 800-100, which has a dimension exclusive to Challenges and Keys to Success. The same content is placed differently in COBIT® 2019, where it becomes a part of the Implementation Enterprise Governance of I&T.

- **Attributes**

Next on the analysis of the results tables, is the key aspect for Attributes. Continuing with the format used in previous tables, the results for each document summary table is presented in Table 13. Also, the numbering format that appears in this table is connected to the one presented in Table 12, hence the attributes presented in this table are incorporated in the dimensions presented in the table that has the same name.

Table 13 – Comparison of Relevant Documents – Attributes aspect

Document	Attributes
COBIT® 2019	1.1 Governance System Principles Provide Stakeholder value Holistic Approach Dynamic Governance System Governance Distinct from Management Tailored to Enterprise Needs End to End Governance System 1.2 Governance Framework Principles Based on a Conceptual Model Open and Flexible Aligned to Major Standards 2.1 Governance and Management Objectives (EDM Processes) 2.2 Components of a Governance System Processes Organizational Structure Principles, Policies and Frameworks Information Culture, Ethics and Behavior People, Skills and Competences Services, Infrastructure application

	2.3 Focus Areas 2.4 Design Factors Enterprise Strategy Enterprise Goals Risk Profile I&T-Related Issues Threat Landscape Compliance Requirements Role of IT Sourcing Model of IT IT Implementation Methods Technology Adoption Strategy Enterprise Size Future Factors 2.5 Goals Cascade 3.1 EDM01 – Ensure governance framework setting and maintenance 3.2 EDM02 – Ensure benefits delivery 3.3 EDM03 – Ensure risk optimization 3.4 EDM04 – Ensure resource optimization 3.5 EDM05 – Ensure stakeholder engagement 4.1 Principles Simple to understand and to use Consistent and support the COBIT Conceptual Model Provide reliable, repeatable and relevant results Flexible Support different types of assessment 4.2 Process Capability Levels Rating Process Activities 4.3 Focus Area Maturity Level 4.4 Manage Performance of Other Governance System Components Organizational structures Information Items Culture and Behavior 5.1 Impact of Design Factors Management objectives priority/selection Component variation Need for specific focus area 5.2 Stages and Steps in the Design Process Understand the enterprise context and strategy Determine the initial scope of governance system Refine the scope of governance system Conclude the governance system design 6.1 COBIT Implementation Guide Purpose 6.2 COBIT Implementation Approach What are the drivers Where are we now Where do we want to be What needs to be done How do we get there Did we get there How do we keep the momentum going
NIST SP 800-100	1.1 U.S. Congress 1.2 Office of Management and Budget (OMB) 1.3 Government Accountability Office (GAO) 1.4 Agencies 1.5 Key Legislative Acts and Documents 2.1 Strategic Planning 2.2 Organizational Structure 2.3 Roles and Responsibilities

	2.4 Enterprise Architecture 2.5 Policies and Guidance 2.6 Ongoing Monitoring 3.1 Balancing requirements 3.2 Balancing laws and regulations 3.3 Maintaining currency 3.4 Prioritize funding
ISO/IEC 27014:2013	1.1. Governing body 1.2. Executive management 1.3. Stakeholders 2.1 Organization-wide information security 2.2 Risk-based approach 2.3 Direction of investment decisions 2.4 Conformance of internal and external requirements 2.5 Security-positive environment 2.6 Review performance of business outcomes 3.1 Evaluate 3.2 Direct 3.3 Monitor 3.4 Communicate 3.5 Assure
GTAG® 15	1.1 Information Security Roles and Responsibilities Board of Directors Executive Management Staff and Line-of-Business Managers Internal Auditors. 2.1 Needs to involve appropriate organizational personnel 2.2 Defines an appropriate framework or methodology to guide its activities 2.3 Uniform IS risk evaluations 2.4 Yield quantifiable and measurable deliverables 2.5 Adapt its priorities based on legal, regulatory, and business changes 2.6 Deploy policies and standards that reflect the organization's risk appetite and are practical, reasonable, and enforceable. 3.1 Encorages proportional control 3.2 Observe proportional control in the design of reporting 3.3 Adaptable enough to handle systems that cannot cost-effectively or technically conform to policies and standards. 4.1 Regulatory actions 4.2 Reputational damage 4.3 Competitive advantage 4.4 Contractual noncompliance 4.5 Inaccurate or incomplete data 4.6 Fraud. 5.1 IAA's responsibilities related to ISG 5.2 Auditor background and experience level 5.3 Audits of ISG benchmark the ISG activity against independent standards. 6.1 Planning Organizational structure Purpose/objectives of each component of the environment Documented communication that occurs among reporting lines Risk appetite Integration of ISG within the organization External influences that could affect ISG structure. 6.2 Testing Stakeholder Concerns

	Reporting and Communication lines Key Performance Indicators (KPI) and their use Alignment of supporting documentation with governance structure Alignment with risk appetite. 6.3 Analyzing Accountability Design Effectiveness Information Security Program Effectiveness Efficiency Resource Levels Value added Continuous Improvement. 7.1 Is the organization's risk appetite well defined and understood? 7.2 Is there a defined, effective information security process? 7.3 Is there effective organizational support for the information security governance activity? 7.4 Does the organization monitor the ongoing health of the information security governance activity? 7.5 Has the organization taken steps to improve its governance over time?
Veiga & Eloff Framework	1.1 Information Security phase I Securing IT environment 1.2 Information Security phase II Information security incorporated to organizational structure 1.3 Information Security phase III Information security incorporated to everyday practices performed by employees (information security culture) 1.4 Information Security phase IV Development and role of ISG (risk prevention was a key driver) 2.1 ISO 177995 & 27001 2.2 PROTECT 2.3 Capability Maturity Model 2.4 Information Security Architecture (ISA) 3.1 Leadership and governance 3.2 Security Management and Organization 3.3 Security Policies 3.4 Security Program Management 3.5 User Security Management 3.6 Technology Protection and Operations

For Table 13 some recurring topics from previous tables are presented and matched with the results from this table. Those topics are processes, principles, components, roles, structure, delivery, risk, accountability and effectiveness and efficiency. Subsequently, new topics arise from this results table and they are also displayed. These new topics correspond to policies, stakeholders, compliance, security culture, and document communication and reporting lines.

The processes topic much to what was seen in previous tables, in this table also has references to the EDM processes. All of these processes are encountered in both COBIT® 2019 (inside governance objectives, 6.1 to 6.5) and ISO/IEC 27014, although the monitoring process is cited in NIST SP 800-100 as ongoing monitoring, and is deep-rooted to GTAG® 15 in the continuous improvement.

Other differences regarding the EDM process are seen in COBIT® 2019 and ISO/IEC 27014, where in the first goes to a more granular level by describing each of the five processes for the EDM. In comparison, ISO/IEC 27014 uses the Direct process in one of its principles (Direction of investment decisions), but also adds to the EDM two more nuclear processes, the communicate and the assurance process.

The Principles topic, which is also a recurring topic, is described in different levels according to the focus of each documents. This difference in description, for a topic, was previously mentioned on the dimensions aspect. In this table, their content is presented, where it can be visualized the two sets of principles of COBIT® 2019 and the six principles for ISO/IEC 27014. The last document principles are presented as: organization-wide information security; risk-based approach; direction of investment decisions; conformance of internal and external requirements; security-positive environment; and review performance of business outcomes.

COBIT® 2019 separates the principles into Governance System Principles (that describes the core requirements of a governance system) and Governance Framework Principles (that can be used to build a governance system). The first has six principles such as: provide stakeholder value; holistic approach; dynamic governance system; governance distinct from management; tailored to enterprise needs; and end to end governance system, while the latter possesses three principles (Based on a Conceptual Model; Open and Flexible; Aligned to Major Standards).

Similar to what happens with principles, Components are described in a granular level on the table for this aspect. On Table 13 , COBIT® 2019 and NIST SP 800-100 presents their components, in part 2.2 for the first and from 2.1 thru 2.6 for the second. While Veiga & Eloff presents the components of their three groups/categories (3.1 thru 3.6), and GTAG® 15 describes components as a part of Planning an ISG Audit as purpose/objectives of each component of the environment.

Another recurring topic evident in the results is roles COBIT® 2019 addresses it in this aspect at a higher level, inside the components part of the governance system (2.2) as people, skills and competences, in other parts of the framework it describes in a deeper level as board of directors. ISO/IEC 27014 and GTAG® 15 address roles as a group. The first cites the governing body, executive management and stakeholders, whereas the latter cites the board of directors, executive management, staff on line-of-business manager and internal auditor. Others like NIST SP 800-100 and Veiga & Eloff do it so in a more subtle approach. NIST SP 800-100 uses agencies, that has the core fundamentals of a role, unlike the approach used in Veiga and Eloff, that cites the development and role of ISG in the fourth phase of Information Security.

The next topic that appears to be recurring is structure. The organizational structure cited in Table 11 for COBIT® 2019, also appears in COBIT® 2019, NIST SP 800-100 and GTAG® 15. For COBIT® 2019, these is a component part of the Governance System, as it is seen in number 2.2 of the table for this aspect. The remaining documents also mention other matters which structure is inherited, such as enterprise architecture in NIST SP 800-100 and for GTAG® 15 how external influences could affect ISG structure. Following with fundamental relations the structure topic has in the documents, ISO/IEC 27014 indicates an organization-wide information security and Veiga & Eloff says that information security was incorporated into the organizational structure on the second phase.

Delivery was first presented in Table 11, when ISO/IEC 27014 cited them in its objectives as value delivery. In this table, COBIT® 2019 has the principle of providing stakeholders value and the governance objective of ensuring benefit delivery as a form of delivery. In the other hand, GTAG® 15 uses value added to demonstrate another verge for delivery.

It appears that risk is yet again represented in a table. This being the third time it appears on a table, only maintaining the same notion as exhibited in GTAG® 15 for their governance definition, that of risk appetite. Here ISO/IEC 27014 has a boarder approach as it mentions a risk-based approach, separate from what is demonstrated in COBIT® 2019 and Veiga & Eloff. COBIT® 2019 uses risk as a component part of the governance system as risk profile and as part of the governance objectives thru risk optimization, and Veiga & Eloff focuses on risk prevention as a key driver.

Though Accountability only appears in this table for GTAG, it is the second time it appears in a result table, the first time was cited in ISO/IEC 27014 on its objectives results table. Even though it isn't present in this table for COBIT® 2019, it is an integral part of the framework; which focus on EGIT and for that to be effective, accountability is a key factor.

Once again GTAG® 15 allusions to the effectiveness and efficiency topic, that was first observed in Table 12. This time it does so by bringing up the design effectiveness, and once again brings back the topic efficiency.

The first new topic observed was policies. This topic appears in three of the five documents. Those documents are: COBIT® 2019 in principles, policies and frameworks as part of the components of a governance system; inside NIST SP800-100 components as policies and guidance; and also as part of the components for Veiga & Eloff as security policies.

Even though stakeholders already appeared correlated to needs in the governance definition, this time around, and for this aspect, it appears in many and different variations. For this reason, it was best to be placed on its own topic. Thus, the topic is contemplated in COBIT® 2019 as part of their governance system principles, in provide stakeholders value; and as part of the governance and management objectives, in EDM05 which ensures stakeholder engagement. It also appears on its intrinsic form within NIST SP 800-100 as part of the U.S. Congress, OMB and GAO. In ISO/IEC 27014, the topic appears as a role, and in GTAG® 15 as stakeholder concerns during an ISG audit.

Compliance emerges for the first time in this table; and is cited by ISO/IEC 27014 and COBIT® 2019. For the first, compliance can be found as conformance of internal and external requirements, while the second describes compliance requirements as part of the design factors when designing and tailoring a governance system. Though this topic can be found in other forms inside previous tables, such as controls; laws and regulations; documentation required; and as compliance against agreed-on direction and objectives.

The mention of security culture is innate to COBIT® 2019, ISO/IEC 27014 and Veiga & Eloff. This is visible when COBIT® 2019 references it as security awareness, which is part of one of their governance system component (culture, ethics and behavior). For ISO/IEC 27014, the topic is represented as a security-positive environment, part of one of their principles. Finally, Veiga & Eloff uses it inside their user security management component.

Lastly, document communication and reporting lines are the final new topic presented in this results table. They appear twice in GTAG® 15 in this table, first in the ISG audit planning and latter in testing. And they are incorporated in COBIT® 2019 governance and management objectives, within EDM05 in the form of reporting transparency, which ensures stakeholders engagement; in NIST SP 800-100 as maintaining currency; and in ISO/IEC 27014 in the process of communicate and assurance.

- **Metrics**

Afterwards, the next table to be explored, is the one with the results for the Metrics aspect which are presented in Table 14.

Table 14 – Comparison of Relevant Documents – Metrics aspect

Document	Metrics
COBIT® 2019	COBIT Performance Management (CPM) model Principles Simple to understand and to use Consistent and support the COBIT Conceptual Model Provide reliable, repeatable and relevant results Flexible Support different types of assessment Manage Performance of Processes Process Capability Levels Rating Process Activities Focus Area Maturity Level Manage Performance of Other Governance System Components Organizational structures Information Items Culture and Behavior

NIST SP 800-100	Performance Reference Model (PRM) Plans of Actions and Milestones (POAM) Performance measurements and metrics Incident statistics
ISO/IEC 27014:2013	The executive manager selects the appropriate (from a business perspective) performance metrics in the Monitor process
GTAG® 15	Key Performance Indicators (KPIs)
Veiga & Eloff Framework	Number of security incidentes Empirical results of awareness surveys

The deliberations perceived from this table is that the majority of the documents (four out of five) use performance as a metric element. COBIT® 2019 uses it in the COBIT Performance Management (CPM) model, whereas NIST SP 800-100 uses it in the Performance Reference Model.

COBIT's model is integrated into the conceptual model and expresses how well the governance and management system and all the components of an enterprise work. By managing the performance of processes and other system components, the first is managed thru Process Capability levels, rating Process Activities and focus area maturity[31] levels. While the second is managed thru the performance management of Organizational Structures, Performance management of Information Items and Performance management of Culture and Behavior.

The other documents that use performance as a metric element are ISO/IEC 27014 that uses it in their Monitor process, and GTAG® 15 that uses performance in the forms of KPIs.

As for Veiga & Eloff's document, the authors present a granular approach, by offering examples of metrics.

- **Analysis**

Lastly, the final key aspect results table to be explore is the Analysis, the results for the documents are evident in Table 15.

Table 15 – Comparison of Relevant Documents – Analysis aspect

Document	Analysis
COBIT® 2019	CPM used to: analyze how they can improve achieve the required level for processes and other components COBIT Implementation Approach (continual improvement) phases: What are the drivers Where are we now Where do we want to be What needs to be done How do we get there Did we get there

[31] Note that the introduction of the maturity and capability concepts stands for a better alignment with the CMMI Development 2.0.

	How do we keep the momentum going
NIST SP 800-100	Periodic assessments and reports Annual report on the effectiveness of agency's information security program Refreshed strategic plan every three years Information security performance measures reported to FISMA (quarterly and annually) Incident and events statistics Network Monitoring Continuous assessment Configuration management and control
ISO/IEC 27014:2013	The governing body performs mandated reviews of a performance measurement program. Also, in the Assure process, the governing body also commissions independent and objective security audits
GTAG® 15	Benchmark the ISG activity against independent standards Periodic reviews Multiyear audit plan Reviews of management reporting, approval and documentation of exceptions, consistency of risk assessments, effective use of metrics
Veiga & Eloff Framework	Risk assessments

The results table reveals four new topics: reports, assessments, reviews, and audits. The first one (reports) appears three times in the same document. NIST SP 800-100 describes the uses of periodic reports, reports on information security measurements that are sent to FISMA both quarterly and annually, and the agency information security program effectiveness annual report.

For assessments, there is an association in three documents. NIST SP 800-100 has a periodic assessment and a continuous assessment, while Veiga & Eloff has a risk assessment. Though COBIT® 2019 uses the CPM to perform an assessment to verify the achievement of required levels, in order to analyze how they can improve thru their implementation approach (continual improvement life cycle).

The reviews are conducted in NIST SP 800-100, ISO/IEC 27014 and GTAG® 15. The first refreshes its strategic plan every three years, whereas the second has a mandated review of the performance measurement program; different from the third which uses periodic reviews.

Finally, the audit topic is present in ISO/IEC 27014 and is commission by the governing body. Therefore, it needs to be an independent and objective security audit.

4.1.3.2 Key Topics

Once analyzed each aspect, some key topics prevailed. To sum them up, a table was created. The key topics were then displayed in the Table 16 for a clearer view.

Table 16 – Document comparison – Key topics.

Aspect	Key Topic				
Document overview	• Document type or purpose	• Targeted audience	• Document Review period		
Governance definition	• EDM process ○ Evaluate ○ Direct ○ Monitor/Control	• Risk ○ Risk management ○ Risk mitigation ○ Risk appetite level	• Needs ○ Stakeholders ○ Organization	• Objectives ○ Achieved and in compliance ○ Aligned and supported	
Objectives	• Strategic alignment • Value delivery • Accountability	• Structure	• Support	• Cost-effective	• Controls
Dimensions	• Roles and Responsibilities	• Components	• Effective and efficient ISG		
Attributes	• Policies	• Compliance	• Stakeholders	• Security culture	• Document communication • Reporting lines
Metrics	• Performance				
Analysis	• Reports	• Assessments	• Review	• Audit	

The topics are presented in the row of the aspect table they first appeared. As it was noticed during the documents table analysis, one topic may reoccur in one or more aspect tables.

Aside from the topics displayed on the first row (document overview aspect), only five other topics (Support, Controls, Compliance, Reports and Audits) are observed for only one of the documents. Though, these five topics, seem to be specific to their respective document (such as Compliance as a design factor in COBIT® 2019, or the use of periodic Reports in NIST SP 800-100).

As for other topics on this table, only three (Risk, Structure, Roles and Responsibilities), appear in all five documents. Though, the majority is present in four out of the five documents. Other five topics (Objectives, Policies, Security Culture, Assessments and Review) appear in three documents. Finally, the remaining two topics (Cost-effective, Effective and Efficient ISG) though similar in content, the first is mentioned in NIST SP 800-100, while the second is present in GTAG® 15 Dimensions and Attribute's tables.

In addition, the development of this table helps with the creation of the concept tree. These key topics will serve as an input for the next step, that is presented in part 4.1.3.3 of this document.

4.1.3.3 Concept Tree construction

Once executed the comparison of the relevant documents, and the creation of the table containing the key topics of ISG, it was time to move to the next step, which was the creation of a concept tree, that uses the topics from Table 16 as a guide and arranges them into a structure, that could be clearly understood and later easily transformed into questions.

The first attempt of a concept tree was very rough and needed to be refined. The process of refinement took some attempts, until the concept tree was ready (with the concepts expanded to the point of being able to cover the topic without becoming redundant) for the next step, the creation of the questionnaire questions. All the versions of the concept tree can be found in Appendix I – Artifact Construction: Concept Tree versions, along with the numbered definitions and the concept tree changes comparison of versions 2 to 5.

Throughout the process of creating this thesis, one of the documents used as reference, in the literature review, was updated. Therefore, this document had to be updated, since versions 1 to 5 of the concept tree were based on the previous version of said document; the summary of such document, in this case version 5 of COBIT, can be found in Appendix H – COBIT 5 Summary.

Even with this change of COBIT's versions, Version 5 of the concept tree was reviewed against COBIT® 2019; and no other alteration was needed, since the concepts remained relevant and accurate, mostly due to COBIT® 2019 use of COBIT® 5 as a base its version.

- **Version 1**

In the first version of the concept tree, the layout main division, used the three components (Human behavioral, Procedural and Technical) presented in Veiga and Eloff [2007] ISG framework document and change management, a process used in COBIT® 5 as part of the life cycle approach [ISACA 2013]. Since ISSG is placed in between technical and organizational governance, and also has a human component; this first main separation seemed adequate.

Within the first separation, Human Behavioral components, another division was created between Roles and Responsibilities, both of them are present in the dimension aspect of the document comparison part 4.1.3.1. The concept of roles, observed in COBIT® 5 [ISACA 2012b], as a part of the enablers people, skills and competences, in NIST SP 800-100 [Bowen et al. 2006] the document had a dedicated section, in ISO/IEC 27014 [2013] this concept was presented amongst the definitions and in

GTAG® 15 [Love et al. 2010] the concept was brought up during the organizational structure. As for the concept responsibilities, the same was interconnected with the roles concept.

The refinement of the roles concept went a bit further, and was divided into five roles (governing body, stakeholders, executive management, auditors, and DPO). The roles were arranged according to their importance to ISSG. Note that the DPO is placed in this category, but it relates to the relevant law, GDPR, that Public Administration must conform to.

Next was the Procedural component, that involves the organizational aspect of ISSG. Once again, the main component was divided into concepts, with half of them presenting a further refinement. For this part, nine concepts prevailed, they were divided as:

- Processes – which was present in the governance definition aspect, and presented a refinement into Evaluate, Direct, Monitor/Control (or commonly known as EDM). These processes are core concepts of the Governance activities and are exhibited in COBIT® 5, NIST SP 80-100 and ISO/IEC 27014.
- Objectives (or purpose) – present in ISO/IEC 27014, is separated in three concepts: Strategic alignment, Value delivery (referred in COBIT® 5 process EDM02 and in GTAG® 15 as value added), and Accountability (yet another Governance core concept, appearing in GTAG as accountability a primary focus when implementing ISG in the organization, in NIST as a requirement of an organization's ISG, in ISO/IEC 27014 as an ISG objective when ensuring the information risks are properly addressed, and as a part of COBIT® 5 generic maturity model attributes). This concept is present inside the aspect with the same name in part 4.1.3.1.
- Needs – first appears in the governance definition aspect of the document comparison part and takes into account the stakeholders needs and the necessity for them to be balanced (also considered one of the main principles of COBIT® 5).
- Organizational structure – was observed in the objective aspect of part 4.1.3.1, and present amongst COBIT® 5, NIST SP 800-100, ISO/IEC 27014, and GTAG® 15. This concept is further divided into Reporting lines, Document communication, and ISG integration within the organization. The first two can be seen present in part 4.1.3.1 inside the attributes aspect, while the latter is present in the objectives aspect.
- Security culture – shown in the attributes aspect of the document comparison, is referred in ISO/IEC 27014 as security positive environment, and is also ingrained into COBIT® 5 as part of the enabler culture, ethics and behavior. Additionally, Veiga and Eloff [2007]

use security culture in their user security management component, which is also broken down into Trust and Privacy.

- Risk program – which belongs to the governance definition aspect in 4.1.3.1, is present in COBIT® 5 as part of value creation within risk optimization, in ISO/IEC 27014 as part of a risk base approach, and in GTAG® 15 described as risk management. This concept is also divided into Risk management, Risk appetite, and Risk mitigation. The first refinement is used in COBIT 5, in ISO/IEC 27014 and in GTAG® 15 , in the first document is used as an ongoing alignment with the processes; in ISO/IEC 27014 it is present within the risk based approach as where it should be consistent and integrated with the organization; while in GTAG® 15 it is said to be a focus of the Board. The second refinement in COBIT® 5 is part of the internal factors of the cascade goals, while in GTAG® 15 is part of the ISG activity. This refinement can also be found in the Governance definition aspect of the document comparison for GTAG® 15. The third, risk mitigation, is used in GTAG® 15 as a form of decision making within the organization and in Veiga and Eloff as part of the risk assessment.

The final three concepts: Cost-effective, Effective ISG, and Efficient ISG; which appear in the document comparison inside aspects Objectives (the first concept) and Dimension (the remaining two concepts), are interconnected and mentioned in GTAG®15. Sometimes they are described as Design effectiveness or at times only as effectiveness and efficiency.

The component division is followed with the Technical component, which was divided into eight concepts (Controls, Policies, Performance, Support, Compliance, Documentation, Audits, and Physical Document). These concepts appear in the Objective (Control and Support), Attributes (Policies and Compliance), Metrics (Performance), Analysis (Documentation and Audits) and Document overview (Physical Document) aspects of the document comparison in part 4.1.3.1.

Another breakdown was created for the concepts of Controls, Documentation and Physical Document. The first was refined into KPI's, the second into reports, assessments and reviews; and the third into document type/purpose, target audience and review period.

In the first sub-component of the technical division, Controls is used as process controls and also as internal controls in the EMD05 process in COBIT® 5; used as a component of the ISG described as information security controls and internal controls in NIST SP 800-100; as part of the sixth principle (performance review in relation to business outcomes) in ISO/IEC 27014 for evaluating the performance of security controls; and in Veiga and Eloff [2007] when considering technical and procedural controls for their framework of ISG.

This sub-component has a refinement, KPI's, which are present in GTAG® 15, where are used to monitor IS thru performance measurement. However, this refinement can be found within the Metrics aspect in the previous part 4.1.3.1.

Next is Policies, which is present in all documents; as an enabler in COBIT® 5; as part of ISG components policies and guidance for NIST SP 800-100; as part of the fourth principle in ISO/IEC 27014; as an ISG practice in GTAG® 15, and as an information security component for Veiga and Eloff.

Followed by Performance, which is used by ISO/IEC 27014 as part of review performance of business outcomes in the attributes aspect of the document comparison, and also as performance metrics in the metrics aspect. Still in the metrics aspect, NIST SP 800-100 uses performance in its performance reference model. And both documents also use performance measurements in the analysis aspect, NIST SP 800-100 uses it as an information security report, and ISO/IEC 27014 uses it as a review of the performance measurement program.

Another sub-component is Support, which is mentioned in NIST SP 800-100 and in GTAG® 15. The first uses support in the governance definition aspect focused on structures, processes and business objectives, and also mentions in the objectives aspect when referring to the agency's mission. In GTAG® 15 is mentioned for measuring the effectiveness of the organization's support for the ISG activity.

After Support, comes the sub-component Compliance. This sub-component, even though displayed in the Attributes aspect of the document comparison, is described for the first time inside COBIT® 5 governance definition as a mention of compliance against agreed-on direction and objectives. Later, the document cites compliance regarding internal policies and external requirements (laws and regulations). Next, NIST SP 800-100 references compliance as part of the ISG requirements and part of some roles (such as Agency Head, CIO and SAISO). In ISO/IEC 27014 it is similar to COBIT® 5, as conformance with internal/external requirements (like contracts), also present within principles two, three and four. For GTAG® 15, compliance is related to IS policies, audits and external influences; and is also a concern for the CAE (in case of noncompliance). Lastly, Veiga and Eloff [2007] use compliance as part of security program management within their ISG framework.

Followed by Documentation, which is a general category and present in the Attributes aspect in 4.1.3.1, that was created to represent the documents used in ISG (such as reports, assessments and reviews). These documents are displayed as a refinement of this sub-component. Though, documentation is mentioned as a good practice for the enabler organizational structure in COBIT® 5, and for guidance and policies of the security objectives in NIST SP 800-100, and as part of an effective ISG activity in GTAG® 15.

The first refinement of the documentation concept is Reports, which is also present in the Analysis aspect. This sub-concept is displayed in NIST SP 800-100 when mentioned as periodic reports as an ISG requirement, usually comprised of the annual program performance report. In ISO/IEC 27014, reports are associated with audit reports and part of the Communicate process. GTAG® 15 uses reports as an element, such as the financial report of an organization, in the audit process.

Assessments, the second refinement of the documentation concept, is also found in the analysis aspect of part 4.1.3.1. This sub-concept is present in COBIT® 5 as part of the PCM, their assessment program approach. It is also present in NIST SP 800-100, where assessments are used in periodic and continuous manners, while for ISO/IEC 27014 e GTAG® 15 assessments are associated with risk assessment.

The final refinement is Reviews. This sub-concept differs from the previous ones, because it is first mentioned in the attributes aspect for ISO/IEC 27014. In COBIT® 5 review is used in the lifecycle approach, where there is a review of the overall success of the initiative. Similarly, NIST SP 800-100 uses review as part of the ongoing monitoring. ISO/IEC 27014 uses review within the sixth principle, as review performance. In GTAG® 15 review is used in the audit to assure management commitment to ISG, also as periodic reviews.

Next comes the concept of Audits, which is present in the Analysis aspect of part 4.1.3.1. This concept first appears in the fourth principle of ISO/IEC 27014, when mentioned that the governing body should commission an independent security audit. Also as part of the sixth principle from the same document, related to performance review. Lastly, in ISO/IEC 27014 audits appear in the "Assure" process, which brings back the fourth principle. In GTAG® 15 audits focus on an audit plan and a formal audit. Also, Veiga and Eloff [2007] use audit inside their framework as part of the security program management.

The final sub-concept is Physical Document, which is a generic category comprised of elements from the documents used in the document comparison. This sub-concept is refined into document type and purpose, target audience and review period. These refinements differs from one document to another. In case of the first refinement, document type/purpose, the majority of the documents their purpose to be used as a governance guide, while for NIST SP 800-100 case it is used to direct managers, and for Veiga and Eloff [2007] is to be the starting point for ISG.

The second refinement is target audience. For NIST SP 800-100 the audience is the American government, while for GTAG® 15 is the CAE role, and for Veiga and Eloff [2007] is destined to a broader audience. The last refinement, review period, is only mentioned in ISO/IEC 27014, which refers to a timeframe of four years until the next version is released.

The last division is change management, found as a part of the life cycle approach in COBIT® 5 (often portrayed as Enabling Change) or to some extent used in the continuous assessment in NIST SP 800-100. This concept was also split into two sub-division, business continuity plan (present in Veiga & Eloff [2007] framework inside Technology Protection and Operations; and in GTAG® 15 within the ISG integration in the organization) and Capability Maturity Model (integral part of COBIT® 5 and one of the documents used in Veiga & Eloff's [2007] framework). Both refinements can be found within the Attributes aspect of the document comparison part 4.1.3.1.

- **Versions 2 to 5**

The next refinement of the Concept tree, version 2, had concepts that were similar to the previous version (some were incorporated under concepts and the introduction of resource optimization); but they were displayed in a different structure. Changes occurred on the 1st level concepts of version 1, which were modified in version 2; these concepts produced a lot of ambiguity, thus resulting in concepts from different categories at the lower levels.

These new 1st level concepts, correspond to more common concepts, making them easier to assimilate because they are more direct. This change also led to a restructuring of the lower levels in version 2. In order to clarify this change, a matrix was produced and is visible within Table 56 and Table 57, inside Appendix I – Artifact Construction: Concept Tree versions.

This time, the core structure was split into: Goals, Agents, Processes and Controls (which in later versions was changed to Artifacts). This structure, which is present in version 2, was carried out in the next versions of the concept tree. Also, in version 5, the context (words) was changed from what was written in the literature, to a version that best reflected the document context. For instance, where once was referred the word ISG in literature, was change to ISSG, the focus of this work. To improve the understanding of the changes made between versions, Table 58 also from Appendix I – Artifact Construction: Concept Tree versions was created.

The first division, Goals, was further refined into strategic alignment, value delivery and accountability, from version 3 onward, compliance was added as another sub-component. The first refinement, Strategic alignment, was also divided in two: balance stakeholders needs; and ISG integration within the organization, representing the Holistic approach. The second was later changed, in version 5, to ISSG integration within the organization.

Followed by the Value delivery refinement, with another three divisions: cost-effective ISG, efficient ISG and the introduction of resource optimization. The first two changed to ISG cost-effectiveness and ISG efficiency, and in version 5 were once again changed to adapt to the study context, becoming ISSG cost-effectiveness and ISSG efficiency. Resource optimization became in version 4 resource, assets and capabilities optimization; which in version 5, was incorporated under ISSG efficiency.

This new concept is present within COBIT® 5 under the EDM04 process; while in NIST SP 800-100 is under ISG structure, as ensure the best use of information security resources; also, in ISO/IEC 27014 is under the second principle and on the direct process. However, is present in GTAG® 15 under effective ISG; and in Veiga and Eloff [2007] within security management and organization.

Another change that happened within the Value delivery refinement thru versions 3 to 5 regards the concept of IT-agility, which appears in COBIT® 5 within the internal IT-related goals, part of the cascade goals. It was first demonstrated in version 3 appearing under the direct sub-component of the process division, then in version 4 it became a refinement of the ISG efficiency and in version 5 it became incorporated under ISSG efficiency.

The next refinement, Accountability, was used in its broader aspect within all versions, since this was an ISSG objective, which was first included in version 1. The final refinement of the Goals division was brought back from version 1 technical components to version 3 onward, and it pertains to the concept of Compliance, which is used in its broader aspect. This concept was put under accountability in version 2, but due to is importance it was separated once again. The compliance concept is found within COBIT® 5, as part of the governance purpose; while in NIST SP 800-100 is part of the ISG requirements; also it is part of the desired outcome and part of principles 2, 3 and 4 of ISO/IEC 27014; however, in GTAG® 15, compliance is part of the ISG activity; and in Veiga and Eloff [2007] is part of the security program management.

For the next division, Agents, since it was a complex subject, it was displayed in the form of a table within the concept tree. This concept is arranged in rows according to the importance the role has within the ISSG context; and in columns were the first column represents the name of the role, and the following columns represent their functions or tasks (versions 4 and 5), their responsibilities and to whom the roles report to (reporting lines). The responsibilities column switched places, in versions 4 and 5, with the tasks column.

The roles were not only arranged according to importance but also grouped over their importance in the ISSG context. Therefore, in version 2, two groups are displayed, one containing the most important roles from a governance point of view (governing body and other stakeholders) and another group for the secondary roles (executive management, auditors, and DPO). The following version added the roles of employees and SAISO, also there was a change within the group division. The first group pertained to the governance main role (governing body), while the second focused on the support roles (executive management, auditors, DPO, Employees, and SAISO) and the last group that pertained to the role of other stakeholders. In version 4 and 5, SAISO was changed for CISO, and employees was downgraded.

These two new roles, SAISO, which later became CISO and employees, are found in documents COBIT® 5, ISO/IEC 27014 and GTAG® 15 for CISO; for SAISO in NIST SP 800-100; and for employees in GTAG® 15, Veiga and Eloff [2007], though in version 3 employees did not have a description, due to the analysis of which focus the role would have.

The third division represents Processes and is divided into the EDM processes which are core to ISSG. These processes are Evaluate, Direct and Monitor and within each another set of refinement is present for a more granular approach.

The first sub-component, Evaluate, has two divisions, which in version 2 are represented as assess the support of business objectives and assess the change management. This second division also had another refinement, namely, estimate the capability maturity model, though both, change management and capability maturity model, were incorporated under other concepts (respectively P.3.3 - Consider the changing business, legal and regulatory environment and their potential of information risk, and P.3.4 - Select appropriate information security performance metrics from business perspective) in the next versions of the instrument.

From version 3 onward, the Evaluate sub-component was split into assess the alignment of ISS to business strategy and realize benefits/value from information security investments (which changed in version 4 to assess benefits/value from information security investments and transformed in version 5 to assess benefits/value from ISS investments). The first division is found in COBIT® 5 within the cascade goals; in NIST SP 800-100 referred to as ISG aligned with business objectives; as part of the objectives in ISO/IEC 27014; and in GTAG® 15 as alignment of organization's risk appetite. The second can be found in COBIT® 5 part of the cascade goals as value of business investments; in NIST SP 800-100 part of the ISG challenges and keys to success; and in ISO/IEC 27014 part of the desired outcomes and the third principle.

"Assess the alignment of ISS to business strategy" was further refined into three: ensure business initiatives takes into account information security issues; ensure that information security adequately supports and sustains the business objectives (which the concept was modified from the first sub-component P.1.1 - Assess the support of business objectives, of the evaluate concept of version 2); and respond to information security performance results, prioritize and initiate required actions. The first two divisions suffered a transformation in version 4, where once was written ensure became verify. Also, all three divisions, in version 5, suffered a change where once was information security to become ISS.

These concepts can be encountered in NIST SP 800-100 and ISO/IEC 27014. Whereas the first is found inside both NIST SP 800-100 under their information security strategic planning and in ISO/IEC 27014 also part of their evaluate process; while the second concept comes from the ISG definition in NIST SP 800-100; and the last is observed in within ISO/IEC 27014 also in their evaluate process.

The next process is Direct, which was divided into three sub-components in version 2 and into five sub-components from version 3 onwards. These sub-components for version 2 are: supervise the risk management plan; oversee the security culture; and supervise the business continuity plan. The first two were also further refined respectively into risk appetite and risk mitigation; and into information security policies, trust concerns, and privacy. The concepts for risk mitigation, information security policies and supervise the business continuity were incorporated under other concepts, respectively AR.5.4 - Risk mitigation, AR.3 - Develop an Information Systems Security policy and guidelines, and P.3.3 - Consider the changing business, legal and regulatory environment and their potential of information risk, within version 3. The rest remained in under the direct process, only trust concerns and privacy concerns were integrated to the concept P.2.5.4 - Promote a positive information security culture in version 3.

In version 3, the sub-components division presented itself as: ensure commitment of executive management to protect information assets and make information security related decisions; develop and approve the information security strategy and policy; allocate adequate investments and resources; direct organization's risk management (derived from the version 2 concept of supervise the risk management plan); and direct resource management and stakeholders communication and reporting. From these six sub-components, only three suffered transformation in the following versions.

The first sub-component suffered two changes, the initial was in version 4, to become oversee where once was ensure, and the second was in version 5 where information security turned into ISS. The second sub-component suffered the same change as the first sub-component in version 5, while the fourth sub-component, in version 5, was changed to risk management program.

In literature the first refinement is referred in GTAG® 15 when it explains ISG, and in Veiga and Eloff [2007] nested under leadership and governance. The second, third and fourth refinement can be found within the direct process of ISO/IEC 27014. The fifth refinement, of the Direct process, is encountered in COBIT® 5 under the processes EDM04.02 - Direct resource management and EDM05.02 - Direct stakeholder communication and reporting.

Though, aside from the first refinement, the last three concepts presented another division. Allocate adequate investments and resources was further divided into ensure IT-agility and ensure optimization of IT assets, resources and capabilities. Although these concepts, in the following versions, were either re-ordered or incorporated; the first concept in version 4 was a sub-component of value delivery, which in version 5 got incorporated within the same concept; while the second in version 4 was incorporated into resource optimization and became resource, assets and capabilities optimization.

The second concept to further refined was the fourth concept (direct organization's risk management) into determine organization's risk appetite (also derived from version 2 concept of risk appetite) and develop risk management policies. The last concept can be found in COBIT® 5 as part of the process EDM03.02 - Direct risk management.

The last concept to be refined was direct resource management and stakeholders communication and reporting. This concept was divided into six sub-concepts: assign responsibilities for resource management; ensure competent and motivated business and IT personnel; develop escalation guidelines; promote a positive information security culture (resultant from the version 2 concept of oversee the security culture; and which incorporated version 2 concepts of trust and privacy concerns); develop reporting and communication principles and guidelines; and develop principles for safeguarding resources. Only two of these concepts suffered alterations in following version, those are respectively the second and fourth concepts. The first alteration occurred in version 4 to P.2.5.2 (Require competent and motivated business and IT personnel), where once was written ensure became require; the second occurred in version 5 to P.2.5.4 (Promote a positive ISS culture) where once was information security to become ISS.

These sub-concepts can also be found in literature, starting with assign responsibilities for resource management, which can be observed in COBIT® 5 process direct resource management (EDM04.02 - Direct resource management). Then the next concept, ensure competent and motivated business and IT personnel, is also referred in COBIT® 5 as part of IT related goals from the goals cascade, while the third concept is mentioned in the process of direct stakeholder communication and reporting, also from COBIT® 5.

The fourth concept, promote a positive information security culture, can be seen within ISO/IEC 27014 and Veiga and Eloff [2007], in the first document it appears as part of the fifth principle and within the direct process; while in the second document it is mentioned as cultivating an acceptable information security culture. Though the concept for develop reporting and communication principles and guidelines is referred in the EDM05.01- Evaluate stakeholder reporting requirements process from COBIT® 5, is also part of the strategic planning in NIST SP 800-100, is also referred in GTAG® 15 as part of the IS activity, and as part of the Leadership and Governance category of Veiga and Eloff framework. Finally, the last concept is commonly observed inside COBIT® 5 EDM04.02 - Direct resource management process.

The last division, which represents the Monitor/Control process is divided within version 2 into three sub-components, while in version 3 onward, is divided into six sub-components. The first division displays the concepts of: compliance with internal and external requirements; apply performance metrics (KPI's); and revise the physical document. This last concept and its refinements (purpose, intended audience and review period) was removed for the next concept tree version, because it was too specific and changed depending on the document revised. The refinements for the second concept (apply performance metrics), which were reports, assessments, and reviews, were incorporated respectively under P.3.2.1 - Report to external stakeholders that the organization practices a level of information security commensurate with the nature of its business; P.1.1 - Assess the alignment of ISS to business strategy, P.3.1 - Assess the effectiveness of information security management activities and AR.5.1 - Risk assessment; and P.3.2 - Check the compliance with legislation, regulations, contractual obligations and statutory requirements in version 3.

The division of the sub-components displayed for version 3 was: assess the effectiveness of information security management activities; check the compliance with legislation, regulations, contractual obligations and statutory requirements; consider the changing business, legal and regulatory environment and their potential of information risk; select appropriate information security performance metrics from business perspective; feedback on transparency of IT costs, benefits and risks; and commission independent and object opinion (audits) of how it is complying with its accountability for the desired level of information security. The majority of these concepts suffered changes throughout the following versions, only the second and third concepts remained the same on the following versions.

Both the first concept and its refinement were introduced in version 3 and were modified from information security to ISS in version 5. The second-tier refinement is displayed as provide feedback on information security performance results and their impacts on the organization. Also, both of these refinements are present in the monitor process of ISO/IEC 27014.

The second concept, check the compliance with legislation, regulations, contractual obligations and statutory requirements, derives from the version 2 concept P.3.1 - Compliance with internal and external requirements, and also incorporates concept P.3.2.3 - Reviews from the same version; and is found in COBIT® 5 as part of the enterprise goals within the goals cascade; in NIST SP 800-100 part of the responsibilities of some roles; in ISO/IEC 27014 part of the desired outcomes; in GTAG® 15 part of ISG; and within Veiga and Eloff [2007] framework for ISG. In version 3, this sub-component had a further refinement (report to external stakeholders that the organization practices a level of information security commensurate with the nature of its business). This refinement also suffered changes in version 4 and 5, in the first version it changed to report to stakeholders the organization's practices for information security are aligned with the nature of its business, and in version 5 information security changed to ISS. Also, this refinement incorporates the concept of reports from version 2. This new concept is referred in the communicate process of ISO/IEC 27014.

The next two concepts, P.3.3 and P.3.4, respectively, consider the changing business, legal and regulatory environment and their potential of information risk; and select appropriate information security performance metrics from business perspective, each have incorporated two concepts from version 2. The first incorporated the concepts of assess the change management and supervise the business continuity plan, while the second incorporated the concepts of estimate the capability maturity model and apply performance metrics (KPI's). Only the second concept suffered changes in the following versions, whereas in version 4, instead of select appropriate information security metrics, became select the metrics for the information security; and in version 5, information security became ISS. These new concepts (P.3.3 and P.3.4) can be found in the monitor process of ISO/IEC 27014.

The last two concepts, feedback on transparency of IT costs, benefits and risks; and commission independent and objective opinion (audits) of how it is complying with its accountability for the desired level of information security, were introduced in version 3. They have also undergone some transformations within versions 4 and 5. The first concept was change in version 4 to became provide feedback, and in version 5 suffered two changes: instead of "on transparency" was switched to "and transparency"; and "on IT costs", it became "over ISS costs". The second concept suffered a major transformation in version 4, it became commission audits to verify compliance with the level of accountability desired (agreed/determined) for information security; which in version 5 was changed to ISS.

Both of these new concepts are alluded in literature, the first can be found in COBIT® 5 IT related goals from the goals cascade, while the second can be found in ISO/IEC 27014 assure process.

Finally, the last core division, was named Controls in version 2, which changed on the succeeding versions to Artifacts. Also, in version 2, this division possessed one refinement, Audits, which was incorporated under the concept P.3.6 - Commission independent and objective opinion (audits) of how it is complying with its accountability for the desired level of information security in version 3. Different from refinement presented in version 3 onward, which has five. The refined concepts of version 3 were: produce the information systems security strategy; create an information systems security program; develop an information systems security policy and guidelines (incorporating concept P.2.2.1 - Information security Policies from version 2); create an information systems security performance program; and create a risk management program. This concept was altered, in version 5, to only display the name of the artifact in question, becoming: ISS strategy; ISS program; ISS policy and guidelines; ISS performance program; and Risk management program.

These sub-concepts are reference in documents such as: NIST SP 800-100, ISO/IEC 27014 and Veiga and Eloff [2007] for ISS strategy; in NIST SP 800-100, GTAG® 15 and Veiga and Eloff [2007] for ISS program; in all of the relevant documents (COBIT® 5, NIST SP 800-100, ISO/IEC 27014, GTAG® 15 and Veiga and Eloff [2007]) for ISS policy and guidelines; in COBIT® 5, NIST SP 800-100, ISO/IEC 27014, and GTAG® 15 for ISS performance program; and in COBIT® 5, ISO/IEC 27014, and GTAG® 15 for Risk management program.

All of these five artifacts concepts, mentioned in the previous paragraph, needed further refinement. The first displayed decision making model as their refinement. While the second was split into investment distribution; resource allocation; and responsibility assignment. The third sub-concept was further refined into authority levels; escalation guidelines; and reporting and communicating structure. The fourth concept was split into reporting and communicating; recommended actions to address resource management deviations; and audit reports. Lastly, the fifth concept, was divided in four parts: risk assessment; risk policies; risk appetite; and risk mitigation (incorporated P.2.1.2 - Risk mitigation concept from version 2).

Only the concept AR.4.2 (Recommended actions to address resource management deviations) from version 3, didn't suffered any transformation in the following versions. The other sub-concepts in version 4 received a verb at their beginning, such as elaborate, contemplate, cover, and regard; which was removed in version 5 to maintain with only the name of the artifact. Other changes happened in version 4, in concept AR.4.1 (Contemplate the Reporting and communicating actions), which became reporting and communicating actions; and in version 5 were concept AR.5.2 (Regarding Risk policies) became risk management policies.

As for the reference of these sub-components in the relevant literature, AR.1.1 (Decision making model) is an output of the EDM process EDM01.01 - Evaluate the governance system from COBIT® 5. The subcomponents (Investment distribution, Resource allocation, and Responsibility assignment) of the second division (AR.2 - Information Systems Security program) are all found in COBIT® 5, respectively the first in EDM02(Ensure Benefits Delivery), while the last two in EDM04(Ensure Resource Optimisation); the first two can also be found in ISO/IEC 27014, while the third can be found in NIST SP 800-100. Authority levels is referred in COBIT® 5 EDM01.01 process (Evaluate the governance system), also escalation guidelines, and reporting and communication structure are mentioned within COBIT® 5 EDM05.02 process (Direct stakeholder communication and reporting).

The sub-components of the fourth division are mentioned in literature in documents such as COBIT® 5 EDM05.01 process (Evaluate stakeholder reporting requirements) and GTAG® 15 for the first sub-concept; or in COBIT® 5 EDM04.03 process (Monitor resource management) for the second sub-concept; or in COBIT® 5 EDM01.03 process (Monitor the governance system), ISO/IEC 27014, and GTAG® 15 for the last sub-concept. While those concepts of the fifth division are usually found in documents COBIT® 5 EDM03 process (Ensure Risk Optimisation), only the last one (risk mitigation) is mentioned in COBIT® 5 EDM02.03 process (Monitor value optimisation).

Aside from the previous sub-component refinement (AR.1.1 through AR.5.4 – decision making model through risk mitigation), sub-components AR.4.1 and AR.5.2 respectively reporting communicating and risk policies, were further refined. The first suffered a two-tier refinement, the first level was stakeholder’s feedback, and the second level was split into two: governance effectiveness and risk management issues. Both of these second level refinement were incorporated in version 4 under other concepts, the first went to P.3.1 (Assess the effectiveness of information security management activities) and G.2.1 (ISG cost-effectiveness), while the second went to P.3.5 (Provide feedback on transparency of IT costs, benefits and risks). The refinement for concept AR.5.2 (Regarding Risk policies, in version 4) was risk tolerance level. These new concepts, stakeholder’s feedback and risk tolerance level can be found respectively within COBIT® 5 processes EDM01.03 (Monitor the governance system) and EDM03.01 (Evaluate risk management) of relevant literature.

After all the changes mentioned above, that occurred to the concept tree during its development, the final version (aka version 5) ended up with a total of 71 concepts. The final numbered version of the concept tree is display in Table 17, while the complete final version (with the Agents Responsibilities and Tasks) are displayed in Figure 22 of Appendix I – Artifact Construction: Concept Tree versions.

Table 17 – Concept Tree Version 5 Numbered Concepts

CT number	CT definition
G	Goals
G.1	Strategic alignment
G.1.1	Balancing stakeholders needs
G.1.2	ISSG integration within the organization (Holistic approach)
G.2	Value delivery
G.2.1	ISSG cost-effectiveness
G.2.2	ISSG efficiency
G.3	Accountability
G.4	Compliance
Ag	Agents
Ag.1	Governing Body
Ag.2	Executive Management
Ag.3	Auditors
Ag.4	Data Protection Officer (DPO)
Ag.5	Chief Information Security Officer (CISO)
Ag.6	Employees
Ag.7	Other Stakeholders (Customers, user, suppliers, partners)
P	Processes
P.1	Evaluate
P.1.1	Assess the alignment of ISS to business strategy
P.1.1.1	Verify that business initiatives takes into account ISS issues
P.1.1.2	Verify that ISS supports and sustains the business objectives
P.1.1.3	Respond to ISS performance results, prioritize and initiate required actions
P.1.2	Assess benefits/value from ISS investments
P.2	Direct
P.2.1	Oversee the commitment of executive management to protect information assets and make ISS related decisions
P.2.2	Develop and approve the ISS strategy and policy
P.2.3	Allocate investments and resources
P.2.4	Direct organization's risk management program
P.2.4.1	Determine organization's risk appetite
P.2.4.2	Develop risk management policies
P.2.5	Direct resource management and stakeholders communication and reporting
P.2.5.1	Assign responsibilities for resource management
P.2.5.2	Require competent and motivated business and IT personnel
P.2.5.3	Develop escalation guidelines
P.2.5.4	Promote a positive ISS culture
P.2.5.5	Develop reporting and communication principles and guidelines
P.2.5.6	Develop principles for safeguarding resources
P.3	Monitor/Control
P.3.1	Assess the effectiveness of ISS management activities
P.3.1.1	Provide feedback on ISS performance results and their impacts on the organization
P.3.2	Check the compliance with legislation, regulations, contractual obligations and statutory requirements
P.3.2.1	Report to stakeholders the organization's practices for ISS are aligned with the nature of its business
P.3.3	Consider the changing business, legal and regulatory environment and their potential of information risk
P.3.4	Select the metrics for the ISS performance from a business perspective
P.3.5	Provide feedback and transparency over ISS costs, benefits and risks
P.3.6	Commission audits to verify compliance with the level of accountability desired (agreed/ determined) for ISS
AR	Artifacts
AR.1	Information Systems Security strategy
AR.1.1	Decision making model
AR.2	Information Systems Security program
AR.2.1	Investment distribution
AR.2.2	Resource allocation
AR.2.3	Responsibility assignment
AR.3	Information Systems Security policy and guidelines

CT number	CT definition
AR.3.1	Authority levels
AR.3.2	Escalation guidelines
AR.3.3	Reporting and communicating structure
AR.4	Information Systems Security performance program
AR.4.1	Reporting and communicating actions
AR.4.1.1	Stakeholder’s feedback
AR.4.2	Recommended actions to address resource management deviations
AR.4.3	Audit Reports
AR.5	Risk Management program
AR.5.1	Risk assessment
AR.5.2	Risk management policies
AR.5.2.1	Risk tolerance level
AR.5.3	Risk appetite
AR.5.4	Risk mitigation

5 Artifact Outputs

This chapter complements Chapter 4, as it continues to describe the creation process of the artifacts. Therefore, it continues to follow the broken down DSR steps and guidelines presented in the previous chapter. In the first subsection, the primary artifact (which is the instrument) is described, along with all its versions. The second subsection describes the secondary artifact, which is the methodological guide, created to help implement such instrument. While, the third subsection presents the evaluation of the instrument. The chapter finishes with the last step from the DSR methodology, which is Conclusion, where the communication of the research is presented.

5.1 Questionnaire Construction

Once the Literature was extensively explored, it was time to build the first version of the instrument. This version took what was displayed in the concept tree and literature and translated it into questions.

The type of instrument, in this case a questionnaire, remained the same through all version (displayed in Appendix J – Artifact Construction: Instrument), though a significant difference in the document structure (see Table 59 also in Appendix J – Artifact Construction: Instrument) can be observed from version 0 to version 1, while other minor adjustments can be perceived in later versions. The first version of the instrument (V0) starts out with a facesheet, then transitions into the questions concerning ISSG in Public Administration, divided into two blocks, contrasting with the last version (V5), which also presents a facesheet, with a glossary and references, then the questions about ISSG in Public Administration, which are divided by four dimensions.

The use of a questionnaire as the main element of this study was due to its better fit within the context of the study. Fink [2003] describes it as a method of survey instrument which is "a system for collecting information from people, its questions can be arranged into mailed or self-administered questionnaires, or into telephone interviews. In a self-administered questionnaire, the questions can be found on paper or on a computer on-line (via Internet) or off-line."

Therefore, the questionnaire to be acceptable, needs to have specific objectives, a sound research, a sound choice of population, a reliable and valid instrument, appropriate management and analysis, and should also emphasize on asking straightforward questions [Fink 2003].

Also, the questionnaire consists first of a facesheet, which is the first thing the respondent should see and where the structure of the document is presented. Usually this first part is described in the first page of the questionnaire and gives general information about the study, such as the universe in which the study is going to be conducted and its purpose [Kerlinger 1986]. The facesheet also has questions to identify the City Hall and the participant. These questions are intended not only to know the participant but also to be used as a reliabily assessment [Kerlinger 1986].

After the facesheet comes the questions about the subject of the study. The type of questions used in this instrument are closed questions; because of their advantages in large studies, with answers more reliable and consistent over time; plus in the end, they are easier to interpret and to perform a statistical analysis [Fink 2003].

Since this is a closed questions questionnaire, the possible answers are already in place. Therefore, the types of responses present in this questionnaire are called nominal or categorical for the most part, including the yes or no answers; and ordinal for questions where the respondent is provided a rate [Fink 2003].

- **Questionnaire Version 0**

On the first version of the questionnaire, denominated Version 0 (V0), aside from the facesheet, which offers insights about the study, the questionnaire and also elucidates information surrounding the city hall and the respondent; uses questions surrounding the context of ISSG in Public Administration, translated from the concepts that were displayed in the first concept tree and in literature. These questions are grouped into two blocks. The first block represents general questions, focuses on the ISSG knowledge and perception from the City Hall respondent.

The second block is divided into five groups, derived from the ISG components set out in NIST SP 800-100 [Bowen et al. 2006]; while the questions, which were used as examples for planning an ISG audit in GTAG® 15 [Love et al. 2010] which also had some concepts found in the first version of the concept tree, were arranged in accordingly within these categories. A correlation between the instrument questions and the GTAG questions (Table 60); also a correlation of the instrument and the concepts of the concept tree (Table 61), can be found in Appendix J – Artifact Construction: Instrument.

The initial part, which consisted of the general questions, was divided into three questions as presented in Table 18. The first two questions focus on ISSG and the third question talks about COBIT® 5 Process Capability Model. The answers from questions 1 to 3 possessed a straightforward answer type, both questions 1 and 3 are a simple yes or no question, while question 2 uses a scale from 1 to 5. However, the answer for sub-question 3.1, presents a complex nature, because it involves the knowledge of the inquiree surrounding the five EDM processes of COBIT® 5 and the COBIT® 5 Process Capability Model.

Table 18 – Instrument V0 – General Questions

1	Have you heard about Information Systems Security Governance (ISSG) before today?
2	Did the introductory definition of ISSG helped you understand the subject or meets your prior knowledge of the subject?
3	Are you aware of COBIT 5 Process Capability Model (Process Capability Attribute and Process Assessment Model)?
3.1	How would you rate, the organization's EDM processes according to COBIT 5 Process Capability Model?
a)	EDM01 – Ensure Governance Framework setting and Maintenance
b)	EDM02 – Ensure Benefits Delivery
c)	EDM03 – Ensure Risk Optimisation
d)	EDM04 – Ensure Resource Optimisation
e)	EDM05 – Ensure Stakeholder Transparency

The second block starts by grouping the questions encompassing the ISG component of Strategic Planning. Concepts such as roles and responsibilities, objectives, strategic alignment, cost-effectiveness, support, compliance, policies and effective ISG can be found within this group of questions. Also, the structure of this group, which is composed of seven questions (displayed in Table 19), has answers based on a simple yes and no answer.

Table 19 – Instrument V0 – Strategic Planning Group

4	Are roles and responsibilities for the Information Systems (IS) activity formally defined?
5	Are the objectives and strategies of ISG well described and defined?
6	How are business unit and/or individual performance objectives tied to IS objectives? Do they support the IS activity?
7	Does each component of the ISG structure have sufficient capital and operating expense budgets to support IS efforts?
8	Are procedures in place to oversee IS incidents including public and investor relations and coordination with law enforcement?
9	Are IS policies supported by written standards? Are the standards supported by written procedures?
10	Does your organization have a ISS program? And Is it in effect/implemented?

The next group of questions, Table 20, is comprised of the Organizational Structure component of ISG, with seven questions and concepts encompassing roles, responsibilities, accountability and organizational structure (from which concepts of reporting lines and document communication).

Table 20 – Instrument V0 – Organizational Structure Group

11	Who is formally responsible for IS?
12	Who is accountable for the ISS program in the organization?
13	To whom does this person formally report?
14	Are there any committee functions, boards or other groups that IS staff regularly reports to either on an informal basis or a more formal steering function?
15	What is the career level of the person in charge of IS? Is this an officer-level position or a managerial position? Does this individual have other roles?
16	Are roles and responsibilities, accountability, and performance for all IS responsibilities formally defined?
a)	Is the CISO driving the IS activity or mostly reporting compliance?

After the organizational structure component, comes the Roles and Responsibilities component, displayed in Table 21. This group regards concepts such as responsibilities, reporting lines, document communication, policies, risk management, and compliance. These concepts can be found within the three questions, that comprise this group.

Table 21 – Instrument V0 – Roles and Responsibilities Group

17	Under what circumstances does the board need to be engaged?
18	What are the IS risks that the board would deem unacceptable?
19	How often is this criteria reviewed?

The fourth ISG component to be used as a group divider is Enterprise Architecture. In this group eight questions are displayed (Table 22), with components from both the procedural and technical component of concept tree version 1. Concepts such as value delivery, reporting lines, ISG integration with the organization, risk management and effective ISG from the first component can be found within these questions. The same applies for the concepts such as policies, support, documentation and its refinement reviews, from the second component.

Table 22 – Instrument V0 – Enterprise Architecture Group

20	What information exchanges are formally defined?
a)	Are they sufficient?
21	Is IS a consideration in the organization's IT strategy?
a)	Is IS a consideration in other business units strategy, processes, and procedures? Has the IS activity added value?
22	Does the IS activity get effective/meaningful feedback from the groups it works with?
23	What is the escalation path that IS news/alerts must follow?
a)	Is there a formal meeting schedule?
24	Does the organization has a risk management plan, process, procedure, policy?

The last ISG component to group the instrument questions is Policies and Guidance. This group presents fifthteen question, though it is also divided in three, as seen on Table 23. The first division uses the questions from GTAG® 15, while the second division pertains to the City Hall, and the last division is focused on the ISS policy. The first division uses concepts of responsibilities, compliance and reviews. The second division asks about a key role in ISSG, compliance and the regulations applicable within the study context.

Table 23 – Instrument V0 – Policies and Guidance Group

25	What regulations, laws, and contractual requirements apply to the organization?
26	How often, and when, were regulations last reviewed to understand IS requirements? Is the legal department involved in the review, or is interpretation left to non-legal staff?
a)	Does legal counsel consult with the IS activity to assess requirements during the contract process?
27	Is there an internal or external regulatory compliance group, and when did the IS activity last meet with them?
a)	What legal environment issues affect ISG and why?
28	What contracts have IS components?
29	When did the IS activity last review contractual requirements with legal counsel?
30	Does de City Hall has a designated data protection officer?
31	To what extent is the City Hall IS compliant with legislations, regulations, security policies and rules? (1 – non-compliant and 5 – completely compliant)
a)	Is the City Hall aware of the GDPR?
b)	Was the City Hall aware of the PGETIC?
c)	Is the City Hall aware of the Estratégia 2020?
32	Does your organization has a ISS policy?
a)	How would you evaluate the coverage (clarity, subject, policies, reporting lines, responsibilities) of the ISS program?
b)	Is the ISS policy available and to whom?

- **Questionnaire Version 1**

The subsequent version of the instrument, version 1 (V1), is similar in structure to the prior version. Both versions possess a facesheet, are divided into two blocks and have an overall of 32 questions. In this version the facesheet is displayed in a separate page and has brief description of the study and a definition of ISSG; and also have instructions on how to fill the questionnaire and explains the security of the study.

Another difference from the prior version of the instrument is the focuses of the blocks and the concept tree version and elements used to group the questions, in this case concept tree number four.[32] This version starts out by focusing on the block that has the ISSG general questions, while the block that focuses on the ISSG questions specific to the public administration comes in second.

Also, within the first block, questions were grouped by concepts found within the main goals of concept tree 4, which are in order: strategic alignment, value delivery, accountability and compliance. This separation can be observed in Table 24. Additionally, a large majority of the questions are of simple answers (yes and no type), twenty-four out of thirty-four; the additional eleven questions range from: five answers where the respondent has to choose a time period, two answers to where the respondent has to choose from one of the roles (Governing body, Executive manager, CISO, DPO, In-line manager or None

[32] The use of concept tree version 4 in this version of the instrument pertains to the halt of the instrument creation after version 0. Once, after the creation of the instrument version 0 and the concept tree version 4 simultaneously, it was perceived a better approach to first focus on the refinement of the concept tree before continue to create new versions of the instrument.

of the above), and other three questions related to the person in charge of the ISS (such as career level, position, and function). Another mention are the minor grammar corrections and question separation, present in this version of the instrument.

In order to clarify the changes from version 0 to version 1, two matrixes were created and they are displayed within Appendix J – Artifact Construction: Instrument. The first one Table 64 represents the changes in the structure of the instrument, question numbers in version 0 and their respective numbers in version 1. The second matrix, Table 62 and Table 63, correlates the question numbers of version 1 with the concepts of the concept tree version 4, and the link to the concept, in this case D (for direct) and i (for indirect).

Table 24 – Instrument V1 – ISSG General Questions

1	Does the organization have an ISS program, and is it in effect/implemented?
2	Are the objectives and strategies for ISSG clearly described and defined?
3	Are the ISS objectives tied to the performance objectives of individuals or other business units?
a)	Does these objectives support the ISS activity?
4	Is ISS a consideration in other parts of the organization (aka strategy, processes and procedures)?
a)	Does the IT strategy consider ISS?
5	Does each component of the ISSG structure have sufficient capital and operating expense budget to support the ISS effort?
6	Has the ISS activity added value to other business units?
7	Does the ISS activity receive effective/meaningful feedback from the groups(units) it works with?
8	Are the ISS performance metrics tied to the organization's perspective?
9	How often is the effectiveness of the ISS activity assessed?
10	Are procedures in place to oversee ISS incidents, including public and investor relations, and is there any coordination with law enforcement?
11	Are the roles and responsibilities for the ISS activity formally defined?
12	Are the roles and responsibilities, the accountability, and the performance for all ISS responsibilities formally defined?
13	Who is formally accountable and responsible for the ISS program in the organization?
a)	To whom does this person formally report?
14	Are there any other functions, boards or groups that the ISS staff has to report regularly; either on an informal basis or in a more formal steering function?
15	What is the career level of the person in charge of the ISS?
a)	Is this an officer-level position or a managerial position?
b)	Does this person have other roles?
16	Is the CISO driving the ISS activity or mostly reporting compliance?
17	Is there an escalation path that the ISS news/alerts must follow?
18	Are ISS policies supported by written standards? Are those standards supported by written procedures?
19	Is there an information exchange formally defined?
a)	Is the definition for the information exchange sufficient?
20	Is ISS compliance with contractual requirements, laws and regulations enforced in the organization?
21	How often are regulations reviewed to understand the ISS requirements?
a)	Is the legal department involved in the review process?
22	When did the ISS activity last review a contractual requirement with the legal counsel?
a)	Does the legal counsel consult with the ISS activity to assess the requirements during a contract process?
23	Is there a specific circumstance in which the board needs to be engaged?
a)	Are there any risks that the board would deem unacceptable?
b)	How often are those risks reviewed?
24	Is there an internal or external regulatory compliance group (auditors), and when did the ISS activity last met with them?

As it was previously mentioned, the focus of this block (Table 25) is specific to ISSG in Public Administration, primarily the City Hall. Furthermore, this group is divided into two segments, the first focuses on City Hall itself, regarding ISS policy and compliance with laws and regulations; while the second focuses on the respondent perception.

Table 25 – ISSG Specific Questions for Public Administration

25	Does your organization have a ISS program?
a)	How would you evaluate the coverage (clarity, subject, policies, reporting lines, responsibilities) of the ISS program?
26	Does your organization have a ISS policy?
a)	Is the ISS policy available and to whom?
27	To what extent is the City Hall IS compliant with legislations, regulations, security policies and rules?
28	Is the City Hall aware of the GDPR?
a)	Does de City Hall have a designated data protection officer?
29	Was the City Hall aware of the *PGETIC*?
a)	Is the City Hall aware of the *Estratégia 2020*?
30	Have you heard about Information Systems Security Governance (ISSG) before today?
31	Did the introductory definition of ISSG helped you understand the subject or meets your prior knowledge of the subject?
32	Are you aware of COBIT 5 Process Capability Model (Process Capability Attribute and Process Assessment Model)?
a)	How would you rate, the organization's EDM processes according to COBIT 5 Process Capability Model? (check a box for the Process Capability and PAM for each process name)
	EDM01 – Ensure Governance Framework setting and Maintenance
	EDM02 – Ensure Benefits Delivery
	EDM03 – Ensure Risk Optimisation
	EDM04 – Ensure Resource Optimisation
	EDM05 – Ensure Stakeholder Transparency

- **Questionnaire Version 2**

Within this version of the questionnaire, version 2 (V2), aside from the facesheet, which was equal from the previous version, the remaining structure suffered alterations. In this version of the questionnaire, the sixty-one questions were separated between the generic dimensions (artifacts, processes, goals and agents), found during the document comparison 4.1.3.1; and another division named others, present at the time of its conception to hold questions that had not yet been placed in one of the prior dimensions. The reason behind this change was so that the instrument could better characterize each dimension, and later help in the process of evaluation and improvement of the ISSG.

Version 2 starts out in the Artifacts part, with fourteen questions, from which nine have simple yes or no answers. For the remaining five questions (2a, 2b, 3b, 4a and 5a), the respondent can choose from three answer options that would best describe his/her point of view of the subject, varying from a low, neutral or high agreement. The emphasis of the questions from this part is to evaluate the concepts, innate from the division with the same name of concept tree version 4, such as: ISS strategy, ISS program, ISS policy and guidelines, ISS performance program and Risk management program.

The second part, called Processes, is also used to evaluate the concepts from the process dimension of version 4 of the concept tree. In the concept tree, the concepts of this dimension are also grouped under the EDM processes; however, in the instrument, this part doesn't maintain this division, though the concepts are usually evaluated following the order found in Table 55 of Appendix I – Artifact Construction: Concept Tree versions. This part also has the largest number of questions of the document, a total of twenty-six questions; of which eleven are of yes or no answer, another fourteen have a scale from 1 to 5, with a value distributed by a percentage interval of 20% (hence number 1 is from 0 to 20%, number 2 is 21 to 40%, number 3 is 41 to 60%, number 4 is 61 to 80% and number 5 is 81 to 100%). At the time, question 9b didn't have any answers to be chosen from.

The next part, Goals, is composed of seven questions. The questions range from 2 questions of yes or no kind of answer, and 5 questions that used the same scale displayed within the process part of the instrument. These questions are designed to evaluate the goals concept represented in the concept tree version 4, for the goals dimension. Amongst those concepts are the concepts of strategic alignment, value delivery, accountability and compliance; respectively viewed in questions 20 and 21, 22 a through c, 23, and 24.

The Goals part was then followed by the Agents part and consists of questions meant to evaluate the responsibilities some ISSG roles, found within concept tree version 4. Therefore, this part was comprised of nine questions. In the initial three questions, the respondent had to choose from four artifacts (ISS strategy, ISS program, ISS policies and guidelines, ISS performance program, Risk management program) which of those artifacts was the responsibility of the role in question. Note that this was the only part of the instrument where the respondent could choose more than one option; since, in literature, some roles were responsible for more than one artifact. The remaining six questions also had four answers to choose from (Governing body, Executive management, In-line management, or Stakeholders), these options represent the roles in which, each of the main role in question had to report to.

The last part, from question 27 until the end, represents the division called Others, present at the time of the conception of this version, which was already explained at the beginning of this section. Table 26 displays the questions and their order, present in this version of the questionnaire, along with their dimension separation.

Table 26 – Instrument V2 Questions

1	Does the organization has an ISS strategy?
a)	Is a decision making model present?
2	Does an ISS program exists in the organization?
a)	How would the effectiveness of this ISS program be qualified?
b)	Are investment distribution, resource allocation and responsibility assignment contemplated to which extent in the ISS program?
3	Has an ISS policy and guidelines been created in the organization?
a)	Are the ISS policy and guidelines implemented in the organization?
b)	In regards of the authority levels, the escalation guidelines and the reporting and communicating structure; how would you evaluate their definition, description and clarity?
4	Is there a program in place to assess the ISS performance?
a)	Does the ISS performance program contemplate actions for communicating and reporting events, actions to address resource management deviations and audit reports? To which extent?
b)	In the reporting and communication's actions, is stakeholder's feedback discussed?
c)	Is there any information gathered from the ISS performance program? If so, is this information, used to select the metrics in accordance with the business perspective?
5	Is a risk management program present at the organization?
a)	How well is the risk subject (such as risk assessment, risk policies, risk tolerance level, risk appetite and risk mitigation) discussed in the program?
6	How would you evaluate the alignment of the ISS with the business strategy
a)	Does the business initiatives considers the ISS issues
b)	Are the business objective supported by the ISS
c)	How does the organization handle the results from the ISS performance? Does the organization prioritizes and initiate the required actions?
7	Are benefits (such as: good results, profits or advantages) perceived from the investments in ISS?
8	How would you describe the commitment of the executive management in
a)	Protecting the information assets
b)	Making ISS related decisions
c)	Developing and approving the ISS strategy and policy
d)	Allocating investments and resources
9	Does the organization follows a risk management policy to manage the risks encountered?
a)	Is the risk appetite described in the policy?
b)	How is the risk appetite determined?
10	Does the organization has a guideline/plan to follow to determine the risk appetite for new risks?
11	How much is covered in the resource management of the ISS program?
a)	Assignment of responsibilities
b)	Have competent and motivated personnel
c)	Promotion of a positive information security culture
12	How much is covered of the stakeholders communication and reporting in the ISS program?
a)	Reporting and communication principles and guidelines
b)	Principles for safeguarding the resources
c)	Escalation guidelines
13	How would you quantify the effectiveness (accomplishment/completion of what was set out) of the management of the information security activities?
14	Does the selected information security performance metrics ponder the business perspective?
15	Are the results of the information security performance used in providing feedback and demonstrating their impacts on the organization?
16	Is the ISS program reviewed to verify their compliance with legislation, regulations, contractual obligations and statutory requirements?
a)	Is the compliance with the organizations information security practices and its alignment to nature of the organizations business, reported to the stakeholders?
17	Are independent audits commissioned to verify the information security level determined in the organization?
18	Does the ISS strategy considers the changes in different types of environment (business, legal and regulatory) and their potential information risk?
19	Is there a feedback provided by the organization, that regards the transparency of IT costs, benefits and risks?
20	To which stand are the needs of the stakeholders balanced in the process of creating an ISSG strategy?
21	Are the ISSG fundaments integrated within all levels of the organization?

22	To which percentage is the value for the governance of the ISS perceived by the organization?
a)	The cost-effectiveness (accomplish what was set out, considering the cost)
b)	The efficiency (degree of achieving the desired result with little waste)
c)	The optimization of resources, assets and capabilities
23	Has the ISSG set out rules that makes people/roles accountable for their actions/responsibilities?
24	How much is compliance (the conformity to fulfill official requirements) a part of the ISSG in the organization?
25	Mark the correspondent artifact, that each role is responsible for developing.
a)	Governing body
b)	Executive management
c)	Chief Information Security Officer (CISO)
26	Mark the correspondent reporting role, that each main role is responsible for reporting to.
a)	Governing body
b)	Executive management
c)	Auditors
d)	Data Protection Officer (DPO)
e)	Chief Information Security Officer (CISO)
f)	Employees
27	Does the ISS strategy considers and balances the stakeholders needs?
28	Has the ISS strategy changed in order to prioritize some aspects approved by the ISS performance results?
29	Have the investments on ISS being evaluated, to very their value?
30	How committed is the executive management in protecting the information assets?
31	Does the executive management make decisions based on ISS?
32	Which role is responsible for developing and approving the ISS strategy and policies in the organization?
33	Are investments and resources allocated in order to secure support for the ISS activity?
34	Does the organization carries out a risk management program?
35	Are the ISS performance metrics developed to accommodate the business perspective?
36	Are authority levels, escalation guidelines, and reporting and communicating structure covered under the ISS policy or guidelines?
37	How would you evaluate the accomplishment of the ISSG goals for
a)	Strategic alignment
b)	Value delivery
c)	Accountability (accept responsibility for the ISSG actions in the organization)
d)	Compliance (fulfill requirements in accordance with some specified standard)

From these last fourteen questions, which pertains to the others part, only question 37 was incorporated in the next version of the questionnaire, as it can be seen in Table 73 of Appendix J – Artifact Construction: Instrument, where it shows the evolution of the subsequent versions. The other questions were incorporated under questions from the previous parts, which were similar in their objectives.

- **Questionnaire Version 3**

From version 2 to this next version of the instrument, version 3 (V3), some changes were made to the composition of the facesheet, as well as to the document structure and a redesign of some answers. For instance, within the facesheet, the ideas behind the first paragraph were shortened, for a simpler understanding of the study objective. Also, the removal of the table, which contained the study universe and other questions, that was deemed unnecessary for the respondent's point of view. Additionally, the facesheet incorporated (after the respondent characterization table) a terminology definitions table, which presented the definitions found in literature for key concepts used largely across the instrument.

Another change that happened from v2 to v3 was the removal of the others part; the questions contained therein have been incorporated elsewhere in the instrument. Lastly, the changes to the format of some answers, which comes in the form of a Likert scale.[33] This scale was used to standardize the answers that already used the respondent's agreement point of view and on those answers that had already used a rudimental percentage scale.

These new changes could be perceived throughout the instrument. The Likert scale was incorporated in the first dimension of the instrument (shown in Table 27), which deals with the Artifacts of ISSG; in questions 2a, 2b, 3c, 4a and 5a. These questions are associated with the concepts of effectiveness, communicating and reporting, and risks. Also, within this version, question 3b was introduced; which inquires about the availability of the ISS policy, found within GTAG® 15.

Table 27 – Instrument V3 – Artifacts Questions

1	Does the organization has an ISS strategy?
a)	Is a decision making model present?
2	Does an ISS program exists in the organization?
a)	How would the effectiveness (accomplishment/completion of planned activities) of the ISS program be qualified? (**Scale measures**: 1 – not effective [between 0 and 20% accomplished]; 3 – somewhat effective [between 41 and 60% accomplished]; 5 – very effective [between 81 and 100% accomplished])
b)	Is investment distribution, resource allocation and responsibility assignment contemplated to which extent in the ISS program? (**Scale measures**: 1 – not contemplated; 3 – sufficiently contemplated; 5 – fully contemplated)
3	Has an ISS policy and guidelines been created in the organization?
a)	Are the ISS policy and guidelines implemented in the organization?
b)	To whom is the ISS policy available?
c)	In regards of the authority levels, the escalation guidelines and the reporting and communicating structure; how would you evaluate their definition, description and clarity? (**Scale measures**: 1 – poorly covered; 3 – sufficiently covered; 5 – very well covered)
4	Is there a program in place to assess the ISS performance (the use measures to determine to which stand the organization's ISS needs were met)?
a)	Does the ISS performance program contemplate, to which extent, the actions for communicating and reporting events, actions to address resource management deviations and audit reports? (**Scale measures**: 1 – poorly contemplated; 3 – sufficiently contemplated; 5 – very well contemplated)
b)	In the reporting and communication's actions, is stakeholder's feedback discussed?
c)	Is there any information gathered from the ISS performance program? If so, is this information, used to select the metrics in accordance with the business perspective?
5	Is a risk management program present at the organization?
a)	How well is the risk subject (such as risk assessment, risk policies, risk tolerance level, risk appetite and risk mitigation) discussed in the program? (**Scale measures**: 1 – poorly discussed; 3 – sufficiently discussed; 5 – very well discussed)

[33] Likert scale is one of the most fundamental and frequently used psychometric tools; designed to measure 'attitude' in a scientifically accepted and validated manner, since 1932 [Joshi et al. 2015].

The next division to suffer adjustments, was the Process dimension; the questions for this dimension are displayed in Table 28. This version of the instrument introduced new questions (9a, 9c, 11, 13, 13a, 13b, 15a, 17, 19b, 22, 22a and 22b) to this dimension, that relates to the concepts of risk management policy, ISS incidents, the person in charge of the ISS, the ISS activity (comprise of activities such as risk appetite, information security strategy and policy, and information security culture) and compliance. A total of nineteen questions, from the process dimension, used Likert scale as a form of answer; most of them used a range of 1 to 5, while five of them (9c, 15a, 19b, 22 and 22b) used a range of 1 thru 3.

Table 28 – Instrument V3 – Process Questions

6	How would you evaluate the alignment of the ISS with the business strategy ... (**Scale measures**: 1 – poorly aligned; 3 – sufficiently aligned; 5 – completely aligned)
a)	when considering the ISS issues in the business initiatives?
b)	to support the business objectives?
c)	in handling the results from the ISS performance; and when prioritizing and/or initiating the required actions derived from the results of the ISS performance?
7	Are benefits (such as: good results, profits or advantages) perceived from the investments in ISS?
8	How would you describe the commitment of the executive management in ... (**Scale measures**: 1 – not committed; 3 – sufficiently committed; 5 – fully committed)
a)	protecting the information assets?
b)	making ISS related decisions?
c)	developing and approving the ISS strategy and policy?
d)	allocating investments and resources?
9	Does the organization follow a risk management policy to manage the risks encountered?
a)	Are ISS policies supported by written standards; and are those standards supported by written procedures?
b)	Is the risk appetite described in the policy?
c)	How often are the risks reviewed? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)
10	Does the organization has a guideline/plan to follow to determine the risk appetite for new risks?
11	Are procedures in place to oversee ISS incidents, including public and investor relations, and is there any coordination with law enforcement?
12	How much is covered in the resource management of the ISS program for ... (**Scale measures**: 1 – not covered; 3 – sufficiently covered; 5 – fully covered)
a)	assignment of responsibilities?
b)	having competent and motivated personnel?
c)	promoting a positive information security culture?
13	What is the career level of the person in charge of the ISS?
a)	Is this an officer-level position or a managerial position?
b)	Does this person has other roles?
14	How much is covered of the stakeholders communication and reporting in the ISS program for ... (**Scale measures**: 1 – poorly covered; 3 – sufficiently covered; 5 – very well covered)
a)	reporting and communication of principles and guidelines?
b)	principles for safeguarding the resources?
c)	escalation guidelines?
15	How would you quantify the effectiveness (accomplishment/completion of what was set out) of the management of the information security activities? (**Scale measures**: 1 – not effective [between 0 and 20% accomplished]; 2 – between 21 and 40% accomplished; 3 – somewhat effective [between 41 and 60% accomplished]; 4 – between 61 and 80% accomplished; 5 – very effective [between 81 and 100% accomplished])
a)	How often is the effectiveness of the ISS activity assessed? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)
16	Does the selected information security performance metrics ponder the business perspective?
17	Does the ISS activity receive effective/meaningful feedback from the groups(units) it works with?

18	Are the results of the information security performance used in providing feedback and demonstrating their impacts on the organization?
19	Is the ISS program reviewed to verify their compliance with legislation, regulations, contractual obligations and statutory requirements?
a)	Is the compliance with the organizations information security practices and its alignment to nature of the organizations business, reported to the stakeholders?
b)	Is there an internal or external regulatory compliance group (auditors), and when did the ISS activity last met with them? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)
20	Are independent audits commissioned to verify the information security level determined in the organization?
21	Does the ISS strategy considers the changes in different types of environment (business, legal and regulatory) and their potential information risk?
22	How often are regulations reviewed to understand the ISS requirements? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)
a)	Is the legal department involved in the review process?
b)	When did the ISS activity last review a contractual requirement with the legal counsel? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)
23	Is there a feedback provided by the organization, that regards the transparency of IT costs, benefits and risks?

These changes also appear in the goals division (Table 29); with the introduction of questions 24, 24a, 24b, 24c and 25. These new questions, along with questions 27a, 27b, 27c and 29, use the Likert scale to measure the concepts associated with the ISSG goals, found in concept tree v4. The range of scale varies from 1 to 5, for the questions within this dimension.

Table 29 – Instrument V3 – Goals Questions

24	How would you evaluate the accomplishment of the ISSG goals for … (**Scale measures**: 1 – not accomplished; 3 – sufficiently accomplished; 5 – fully accomplished)
a)	strategic alignment ?
b)	value delivery ?
c)	accountability (accept responsibility for the ISSG actions in the organization)?
d)	compliance (fulfill requirements in accordance with some specified standard)?
25	To which extent are the needs of the stakeholders balanced in the process of creating an ISSG strategy? (**Scale measures**: 1 – not balanced; 3 – sufficiently balanced; 5 – fully balanced)
26	Are the ISSG fundaments integrated within all levels of the organization?
27	To which degree is the value for the governance of the ISS perceived by the organization … (**Scale measures**: 1 – no value added [between 0 and 20%]; 2 – between 21 and 40%; 3 – fair amount of value added [between 41 and 60%]; 4 – between 61 and 80%; 5 – a lot of value added [between 81 and 100%])
a)	the cost-effectiveness (accomplish what was set out, considering the cost)?
b)	the efficiency (degree of achieving the desired result with little waste)?
c)	the optimization of resources, assets and capabilities?
28	Has the ISSG set out rules that makes people/roles accountable for their actions/responsibilities?
29	How much is compliance (the conformity to fulfill official requirements) a part of the ISSG in the organization? (**Scale measures**: 1 – not important [between 0 and 20% of compliance]; 3 – somewhat important [between 41 and 60% of compliance]; 5 – very important [between 81 and 100% of compliance])

In the last part of this survey (Table 30), the Agents dimension, the initial change occurred in question 30b, where once the role described by the generic role of Executive Management, found in literature; was replaced to be in accordance with the study environment. Therefore, the role of Executive Management came to be described as City Hall Executive; which describes a group usually formed by the city hall mayor and members of the city council. Because of the changes to this role, adjustments had to be made to question 31, where once the question presented executive management as a main role, became two distinct roles (Mayor and City Councilor); also, a question for the role CIO was added. Finally, question 32 was introduced in this version of the instrument.

Table 30 – Instrument V3 – Agents Questions

30	Mark the correspondent artifact, that each role is responsible for developing. (Multiple choices accepted)
a)	Governing body
b)	City Hall executive (group usually formed by the city hall mayor and members of the city council)
c)	Chief Information Security Officer (CISO)
31	Mark the correspondent reporting role, that each main role is responsible for reporting to?
a)	Governing body
b)	Mayor
c)	City Councilor
d)	Chief Information Officer (CIO)
e)	Auditors
f)	Data Protection Officer (DPO)
g)	Chief Information Security Officer (CISO)
h)	Employees
32	Is the CISO driving the ISS activity or mostly reporting compliance?

- **Questionnaire Version 4**

Very few changes were made from version 3 to this version of the instrument, version 4 (V4). Both versions use concept tree v4, the instrument structure (such as the dimension divisions) and the elements of the facesheet remains the same.

The differences in the first division, Artifacts, are mostly changes to the question composition, although the idea behind the questions remain the same. The questions that underwent modifications from one version to another were: 3b, 4c and 5a.

Next division to undergo modifications was the Process division. Changes were made to the composition of questions 6c, 10, 15, 16, 18, 19a, 20 and 22a. Also, question 9a (from V3) was removed; and question 9c (also from V3) took its place in this version. Question 9a (V3) dealt with the compliance of ISS policies, and this concept was already being evaluated under question 24d (V4) from the next division, Goals.

In the Goals division, few changes were made, they were mostly additions to the existing questions. For instance, in question 24a and 24b, descriptions for their concepts were added; and in question 26, the examples of ISSG fundamentals were added.

Lastly, the modifications adopted in the Agents dimension are similar to those in the Goals division. The descriptions for the roles were added to questions: 30a, 30c, 31b, 31c, 31d, 31e, 31f and 31h. These modifications, and the modifications made in previous dimensions, of this version of instrument, can be observed in Table 31.

Table 31 – Instrument V4 Questions

1	Does the organization has an ISS strategy?
a)	Is a decision making model present?
2	Does an ISS program exists in the organization?
a)	How would the effectiveness (accomplishment/completion of planned activities) of the ISS program be qualified? (**Scale measures**: 1 – not effective [between 0 and 20% accomplished]; 3 – somewhat effective [between 41 and 60% accomplished]; 5 – very effective [between 81 and 100% accomplished])
b)	Is investment distribution, resource allocation and responsibility assignment contemplated to which extent in the ISS program? (**Scale measures**: 1 – not contemplated; 3 – sufficiently contemplated; 5 – fully contemplated)
3	Has an ISS policy and guidelines been created in the organization?
a)	Are the ISS policy and guidelines implemented in the organization?
b)	To whom are the ISS policy and guidelines available?
c)	In regards of the authority levels, the escalation guidelines and the reporting and communicating structure; how would you evaluate their definition, description and clarity? (**Scale measures**: 1 – poorly covered; 3 – sufficiently covered; 5 – very well covered)
d)	Is the ISS policy supported by written standards; and are those standards supported by written procedures?
4	Is there a program in place to assess the ISS performance (the use measures to determine to which stand the organization's ISS needs were met)?
a)	Does the ISS performance program contemplate, to which extent, the actions for communicating and reporting events, actions to address resource management deviations and audit reports? (**Scale measures**: 1 – poorly contemplated; 3 – sufficiently contemplated; 5 – very well contemplated)
b)	In the reporting and communication's action, is stakeholder's feedback discussed?
c)	Is the information gathered from the ISS performance considered when selecting new metrics, that are in accordance with the business objectives?
5	Is a risk management program present at the organization?
a)	How well the risk subject (such as risk assessment, risk policies, risk tolerance level, risk appetite and risk mitigation) is discussed in the program? (**Scale measures**: 1 – poorly discussed; 3 – sufficiently discussed; 5 – very well discussed)
6	How would you evaluate the alignment of the ISS with the business strategy ... (**Scale measures**: 1 – poorly aligned; 3 – sufficiently aligned; 5 – completely aligned)
a)	when considering the ISS issues in the business initiatives?
b)	to support the business objectives?
c)	in handling the results from the ISS performance, like prioritizing and/or initiating the required actions derived from those results?
7	Are benefits (such as: good results, profits or advantages) perceived from the investments in ISS?
8	How would you describe the commitment of the executive management in ... (**Scale measures**: 1 – not committed; 3 – sufficiently committed; 5 – fully committed)
a)	protecting the information assets?
b)	making ISS related decisions?
c)	developing and approving the ISS strategy and policy?
d)	allocating investments and resources?
9	Does the organization follow a risk management policy to manage the risks encountered?
a)	How often are the risks reviewed? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)
b)	Is the risk appetite described in the policy?
10	Is there a guideline/plan to be followed to determine the risk appetite for new risks?
11	Are procedures in place to oversee ISS incidents, including public and investor relations, and is there any coordination with law enforcement?
12	How much is covered in the resource management of the ISS program for ... (**Scale measures**: 1 – not covered; 3 – sufficiently covered; 5 – fully covered)
a)	assignment of responsibilities?
b)	having competent and motivated personnel?
c)	promoting a positive information security culture?
13	What is the career level of the person in charge of the ISS?
a)	Is this an officer-level position or a managerial position?
b)	Does this person has other roles?
14	How much is covered of the stakeholders communication and reporting in the ISS program for ... (**Scale measures**: 1 – poorly covered; 3 – sufficiently covered; 5 – very well covered)
a)	reporting and communication of principles and guidelines?

b)	principles for safeguarding the resources?
c)	escalation guidelines?
15	How would you quantify the effectiveness of the ISS activities? (**Scale measures**: 1 – not effective [between 0 and 20% accomplished]; 2 – between 21 and 40% accomplished; 3 – somewhat effective [between 41 and 60% accomplished]; 4 – between 61 and 80% accomplished; 5 – very effective [between 81 and 100% accomplished])
a)	How often is the effectiveness of the ISS activity assessed? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)
16	Does the selected ISS performance metrics ponder the business perspective?
17	Does the ISS activity receive effective/meaningful feedback from the groups(units) it works with?
18	Are the results of the ISS performance used in providing feedback and demonstrating their impacts on the organization?
19	Is the ISS program reviewed to verify their compliance with legislation, regulations, contractual obligations and statutory requirements?
a)	Is the compliance of the information security practices and their alignment to the organization's business nature, reported to the stakeholders?
b)	Is there an internal or external regulatory compliance group (auditors), and when did the ISS activity last met with them? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)
20	Are independent audits commissioned to verify the determined level for the information security?
21	Does the ISS strategy considers the changes in different types of environment (business, legal and regulatory) and their potential information risk?
22	How often are regulations reviewed to understand the ISS requirements? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)
a)	Is the legal department involved in the review process of the ISS activity?
b)	When did the ISS activity last review a contractual requirement with the legal counsel? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)
23	Is there a feedback provided by the organization, that regards the transparency of IT costs, benefits and risks?
24	How would you evaluate the accomplishment of the ISSG goals for ... (**Scale measures**: 1 – not accomplished; 3 – sufficiently accomplished; 5 – fully accomplished)
a)	strategic alignment (the link between the ISS strategy and the organization's business)?
b)	value delivery (the delivery of promised benefits while optimizing costs)?
c)	accountability (accept responsibility for the ISSG actions in the organization)?
d)	compliance (fulfill requirements in accordance with some specified standard)?
25	To which extent are the needs of the stakeholders balanced in the process of creating an ISSG strategy? (**Scale measures**: 1 – not balanced; 3 – sufficiently balanced; 5 – fully balanced)
26	Are the ISSG fundaments (such as goals and objectives) integrated within all levels of the organization?
27	To which degree is the value for the governance of the ISS perceived by the organization ... (**Scale measures**: 1 – no value added [between 0 and 20%]; 2 – between 21 and 40%; 3 – fair amount of value added [between 41 and 60%]; 4 – between 61 and 80%; 5 – a lot of value added [between 81 and 100%])
a)	the cost-effectiveness (accomplish what was set out, considering the cost)?
b)	the efficiency (degree of achieving the desired result with little waste)?
c)	the optimization of resources, assets and capabilities?
28	Has the ISSG set out rules that makes people/roles accountable for their actions/responsibilities?
29	How much is compliance (the conformity to fulfill official requirements) a part of the ISSG in the organization? (**Scale measures**: 1 – not important [between 0 and 20% of compliance]; 3 – somewhat important [between 41 and 60% of compliance]; 5 – very important [between 81 and 100% of compliance])
30	Mark the correspondent artifact, that each role is responsible for developing. (Multiple choices accepted)
a)	Governing body (person or group accountable for the organization's performance and conformity)
b)	City Hall executive (group usually formed by the city hall mayor and members of the city council)
c)	Chief Information Security Officer (CISO) (responsible for all the ISS activities)
31	Mark the correspondent reporting role, that each main role is responsible for reporting to?
a)	Governing body
b)	Mayor (person elected to act as head of a city)
c)	City Councilor (member of the legislative body that governs the city)
d)	Chief Information Officer (CIO) (responsible for the ISS program, policy; and its compliance)
e)	Auditors (responsible for assessing the governance activities compliance with the standards)
f)	Data Protection Officer (DPO) (responsible for overseeing the data protection strategy, implementation and compliance with the GDPR)
g)	Chief Information Security Officer (CISO)
h)	Employees (individual who is payed to work)
32	Is the CISO driving the ISS activity or mostly reporting compliance?

- **Questionnaire Version 5**

The fifth and final version of the instrument was produced. This version (V5, which can be found within Figure 28 of Appendix J – Artifact Construction: Instrument) uses the concept tree v5, which was produced using the COBIT® 5 version; and later reviewed to be compatible with COBIT® 2019 version. Equally, the instrument was designed with COBIT® 5 as a base and later revised to fit the COBIT® 2019 version. In both instances, no necessary changes were perceived needed.

The structure of the instrument didn't change much from the previous version (V4). Within the facesheet, modifications are present in the first paragraph, and with the removal of the confidentiality paragraph. This first part is also accompanied by a instruction on how to fill out the questionnaire. Either by following the flux presented inside a parenthesis, at the end of either the question itself or within their answer.

Also, another adjustment to the facesheet is present in the terminologies definitions. These definitions were modified to portrait what was seen in literature. Therefore, citations were added to the definitions along with a list of references.

After the facesheet, comes the dimensions part; which starts out from the artifacts dimension. Similar to version 4, this part only suffers a couple of grammatical changes in questions 1a, 2b, 3, 4c and 5a. The next dimension to present alterations is the Process dimension. In this version, this dimension continues to have the largest amount of question; which also experienced the most alterations. Nevertheless, the alterations already mentioned in the artifacts dimension, along with those on the next dimensions, are visible in Table 32.

The alterations found inside the Process dimensions not only pertain to grammatical changes, which happened in questions 6a, 6b, 6c, 7, 10, 16, 20a, 20c, 21, 22 and 24. Some of these changes happened in order to a better fit to the study's context, while others (e.g. questions 6c, 10, 20a, 21 and 24) pertained to the breakdown of questions from V4 into two separate questions on V5. This last alteration is evident in questions 11, 17 and 19b of version 4; that became, in order, questions 11 and 12, 17 and 18, 20b and 20c in version 5. Apart from those changes, questions 13 and 13b (from version 4) were transferred to the agents dimension in version 5, which will be later discussed; and question 13a (also from version 4) was removed from this version, since the level was already innate to the roles in question. The last adjustment, in this block, happened to the scale measurement of question 15, which became more compact.

The following dimension to be altered was the Goals dimension, which, apart from question 26, all other questions in this block suffered some degree of change. In question 25a, organization's business was changed to organization's activity, in order to better fit the study's context. Question 27, where once was ISSG fundamentals, changed the focus to view only ISSG goals and objectives. While question 28 the modification came in the form of a summary of the scale measurements. Also, within question 28 the changes were, specifically in questions 28a and 28b, in the concept for the first one, and in the description of the concept on the second. A difference between V4 to V5 is that the question 27c (V4) was incorporated under de concept of question 28b of version 5. Questions 29 and 30 also suffered some alterations, the first focused the accountability of people and their actions. While in the second, a description of compliance was added.

Within the last dimension, the Agent's part of the questionnaire, another change was yet again observed in this version, to fit the study's context. Question 31 was added to characterize the role responsible for the ISS inside the organization, with options from generic roles found in literature (like CIO and CISO), or specific roles from the City Hall context such as Mayor, City Councilor or other City Hall employee. This also had some ramifications in questions 32 and 33, where this characterization was used instead of the specific role. Also, the other questions that compose question 31, were dislodged from version 4 to version 5. Regarding question 31a, it was first a separate question (32) within version 4 of the instrument, and also referred to the role of CISO. Other changes can be perceive in the other questions nested within question 31.

Questions 31b and 31c, respectively questions 13 and 13b from version 4, both focus on the role of the person in charge of the organization, the first focuses on their career level, and the second focuses if this role performs another role within the organization. The first question, 31b, adds another row of answer (e.g. Others). While in question 31c, a small grammar change was made. Another significant change was observed within the answer columns of question 32; that for all the questions nested under it, another column with the answer "Not Assigned" was added.

Table 32 – Instrument V5 Questions

1	Does the organization has an ISS strategy?
a)	In the ISS strategy is a decision making model present?
2	Does an ISS program exists in the organization?
a)	How would the effectiveness (accomplishment/completion of planned activities) of the ISS program be qualified? (**Scale measures**: **1** – not effective [between 0 and 20% accomplished]; **3** – somewhat effective [between 41 and 60% accomplished]; **5** – very effective [between 81 and 100% accomplished])
b)	The investment distribution, resource allocation and responsibility assignment contemplated to which extent in the ISS program? (**Scale measures**: **1** – not contemplated; **3** – sufficiently contemplated; **5** – fully contemplated)
3	Have an ISS policy and guidelines been created in the organization?

a)	Are the ISS policy and guidelines implemented in the organization?
b)	To whom are the ISS policy and guidelines available?
c)	In regards of the authority levels, the escalation guidelines and the reporting and communicating structure; how would you evaluate their definition, description and clarity? (**Scale measures**: **1** – poorly covered; **3** – sufficiently covered; **5** – very well covered)
d)	Is the ISS policy supported by written standards; and are those standards supported by written procedures?
4	Is there a program in place to assess the ISS performance (the use measures to determine to which stand the organization's ISS needs were met)?
a)	Does the ISS performance program contemplate, to which extent, the actions for communicating and reporting events, actions to address resource management deviations and audit reports? (**Scale measures**: **1** – poorly contemplated; **3** – sufficiently contemplated; **5** – very well contemplated)
b)	In the reporting and communication's action, is stakeholder's feedback discussed?
c)	Is the information gathered from the ISS performance considered when selecting new metrics, that are in accordance with the organization's objectives?
5	Is a risk management program present at the organization?
a)	How well the risk subject (such as risk assessment, risk management policies, risk tolerance level, risk appetite and risk mitigation) is discussed in the program? (**Scale measures**: **1** – poorly discussed; **3** – sufficiently discussed; **5** – very well discussed)
6	How would you evaluate the alignment of the ISS with the business strategy ... (**Scale measures**: **1** – poorly aligned; **3** – sufficiently aligned; **5** – completely aligned)
a)	when considering the ISS issues in the organization initiatives?
b)	to support the organization objectives?
c)	in handling the results from the ISS performance, like prioritizing or initiating the required actions derived from those results?
7	Are benefits (such as: good results or advantages) perceived from the investments in ISS?
8	How would you describe the commitment of the executive management in ... (**Scale measures**: **1** – not committed; **3** – sufficiently committed; **5** – fully committed)
a)	protecting the information assets?
b)	making ISS related decisions?
c)	developing and approving the ISS strategy and policy?
d)	allocating investments and resources?
9	Does the organization follow a risk management policy to manage the risks encountered?
a)	How often are the risks reviewed? (**Scale measures**: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)
b)	Is the risk appetite described in the policy?
10	Is there a guideline or plan to be followed to determine the risk appetite for new risks?
11	Are procedures in place to oversee ISS incidents, including public and investor relations?
12	Are there procedures in place, that coordinate with law enforcement, to oversee ISS incidents?
13	How much is covered in the resource management of the ISS program for ... (**Scale measures**: **1** – not covered; **3** – sufficiently covered; **5** – fully covered)
a)	assignment of responsibilities?
b)	having competent and motivated personnel?
c)	promoting a positive information security culture?
14	How much is covered of the stakeholders communication and reporting in the ISS program for ... (**Scale measures**: **1** – poorly covered; **3** – sufficiently covered; **5** – very well covered)
a)	reporting and communication of principles and guidelines?
b)	principles for safeguarding the resources?
c)	escalation guidelines?
15	How would you quantify the effectiveness of the ISS activities? (**Scale measures**: **1** – not effective [between 0 and 20% accomplished]; **3** – somewhat effective [between 41 and 60% accomplished]; **5** – very effective [between 81 and 100% accomplished])
a)	How often is the effectiveness of the ISS activity assessed? (**Scale measures**: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)
16	Does the selected ISS performance metrics ponder the organization's perspective?
17	Does the ISS activity receive effective and meaningful feedback from the groups(units) it works with?
18	Does the ISS activity provide effective and meaningful feedback to the groups(units) it works with?
19	Are the results of the ISS performance used in providing feedback and demonstrating their impacts on the organization?
20	Is the ISS program reviewed to verify its compliance with legislation, regulations, contractual obligations and statutory requirements?
a)	Is the compliance of the ISS practices and their alignment to the nature of the organization's purpose, reported to the stakeholders?
b)	Is there an internal or external regulatory compliance group (auditors)?
c)	When did the ISS activity last meet with the auditors?

	(**Scale measures**: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)
21	Are independent audits commissioned to verify the determined level for the organization's ISS?
22	Does the ISS strategy considers the changes in different types of environment (organizational, legal and regulatory) and their potential information risk?
23	How often are regulations reviewed to understand the ISS requirements? (**Scale measures**: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)
a)	Is the legal department involved in the review process of the ISS activity?
b)	When did the ISS activity last review a contractual requirement with the legal counsel? (**Scale measures**: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)
24	Is there a feedback provided by the organization, that regards the transparency over ISS costs, benefits and risks?
25	How would you evaluate the accomplishment of the ISSG goals for ... (**Scale measures**: **1** – not accomplished; **3** – sufficiently accomplished; **5** – fully accomplished)
a)	strategic alignment (the link between the ISS strategy and the organization's activity)?
b)	value delivery (the delivery of promised benefits while optimizing costs)?
c)	accountability (accept responsibility for the ISSG actions in the organization)?
d)	compliance (fulfill requirements in accordance with regulations, laws and contractual obligations)?
26	To which extent are the needs of stakeholders balanced in the process of creating an ISS strategy? (**Scale measures**: **1** – not balanced; **3** – sufficiently balanced; **5** – fully balanced)
27	Are the ISSG goals and objectives integrated within all levels of the organization?
28	To which degree is the value for the governance of the ISS perceived by the organization in relation to ... (**Scale measures**: **1** – no value added [between 0 and 20%]; **3** – fair amount of value added [between 41 and 60%]; **5** – a lot of value added [between 81 and 100%])
a)	effectiveness (accomplishment of what was set out to be done)?
b)	efficiency (achieve the desired result with little waste)?
29	Has the ISSG set out rules that makes people accountable for their actions?
30	How much is compliance a part of the ISSG in the organization? (**Scale measures**: **1** – not important [between 0 and 20% of compliance]; **3** – somewhat important [between 41 and 60% of compliance]; **5** – very important [between 81 and 100% of compliance])
31	Who is the **person in charge of the organization's ISS**?
a)	Is the person in charge driving the ISS activity or mostly reporting compliance?
b)	What is the career level of the person in charge of the ISS?
c)	Does the person in charge of the ISS have other roles in the organization?
32	Mark the correspondent artifact, that each role is responsible for developing. (Multiple choices accepted)
a)	Governing body (person or group accountable for the organization's performance and conformity)
b)	City Hall executive (group usually formed by the City Hall Mayor and members of the City Council)
c)	Person in charge of the organization's ISS
33	Mark the correspondent reporting role, that each main role is responsible for reporting to?
a)	Governing body
b)	Mayor (person elected to act as head of a city)
c)	City Councilor (member of the legislative body that governs the city)
d)	Person in charge of the organization's ISS
e)	Auditors (person responsible for assessing the governance activities compliance with the standards)
f)	Data Protection Officer (DPO) (person responsible for overseeing the data protection strategy, implementation and compliance with the GDPR)
g)	Employees (individual who is payed to work)

Along with the final version, an accessory was created, which was the translated version of the instrument. This development took into consideration the native language of the environment (Portuguese), which the instrument was to be implemented. This translated version can be found within Figure 29 of Appendix K – Instrument Accessory – Translated Version

5.2 Methodological Guide

Besides the instrument, which was the initial artifact, another artifact was created for this study. This secondary artifact was the methodological guide, which is displayed within Appendix L – Artifact Construction: Methodological Guide, its intent was to help with the evaluation of the instrument. For that matter, the guide was composed after the completion of instrument.

This secondary document is divided into six parts. Aside from the first and last part, respectively the introduction and conclusion, which represents the introduction of the subject, the study and their objectives; and the conclusions observed throughout the document construction, the remaining four parts of the guide are as follows: evolution of the evaluation method, evaluation principles, evaluation process, and evaluation measures.

The second part of the document (evolution of the evaluation method), is dedicated to future interactions of the instrument and consequently the changes made to subsequent versions of the guide. Next, the evaluation principles part, were based on the principles present in the methodological guide of the study for the Portuguese City Halls Internet Presence (part 3.1.2.1). Which defines seven principles, used by the guide: current evaluation measures, interactive development of the evaluation method, independence/impartiality of the evaluation method, evaluation and transparency, consistency of observations/evaluations between studies, and results relevance.

The fourth part, evaluation process, describes the process to evaluate the ISSG in the Portuguese Local Public Administration in five phases (data collection, data validation, data treatment, data analysis and improvements). The final part, evaluation measures, is divided additionally into three parts; where the criteria, indicators and the global indicator (also known as ISSG index) are displayed. The criteria are split into four, same as encountered within the instrument, and the objectives of the indicators for each criterion is explained. Then the seventy-six indicators are detailed, along with their indicator type, indicator value and indicator weight; some indicators may present sub indicators and sub indicators value.

Finally, the global indicator (e.g. ISSG index) is explained. It was designed to quantify the amount of ISSG a City Hall possesses. There are two paths to calculate the ISSG index, and they are referenced as global or as scenarios (a more in-depth description is given shortly). In the case of the scenarios path, there are also two scenarios to choose from, scenario 1 (Sc1) and scenario 2 (Sc2).

Also in the ISSG index calculation, weights are assigned to each Criteria and Indicator. The criteria weights differ in value, depending on the path used. If the path used is the global path or the scenario 1 of the scenario, their criteria weights are the same, while if scenario 2 is used the criteria weights are different.

In order to help with the calculation of the global indicator, Table 33 was created. In it, all the criteria (Artifacts (AR), Processes (P), Goals (G), and Agents (Ag)) and indicators are displayed in a compact form, alongside their pondered weights

Table 33 – Criteria and Indicators Weights

Criteria	Criteria weight		Indicator		Indicator weight
	Sc1	Sc2			
Ar	25%	20%	Ar.i1	ISS strategy presence	7%
			Ar.i1a	Decision making model presence	5%
			Ar.i2	ISS program presence	7%
			Ar.i2a	ISS program effectiveness	7%
			Ar.i2b	ISS program properties	5%
			Ar.i3	ISS policy and guidelines presence	7%
			Ar.i3a	ISS policy and guidelines implementation	7%
			Ar.i3b	ISS policy and guidelines availability	7%
Artifacts			Ar.i3c	ISS policy and guidelines properties	5%
			Ar.i3d	ISS policy and guidelines basis	7%
			Ar.i4	ISS performance program presence	7%
			Ar.i4a	ISS performance program properties	5%
			Ar.i4b	Stakeholder's feedback	5%
			Ar.i4c	Metrics selection	7%
			Ar.i5	Risk management program presence	7%
			Ar.i5a	Risk management program properties	5%
				Total weight for Ar indicators	100%
P	25%	20%	P.i6	Alignment of ISS and Business strategy	
			P.i6a	ISS issues alignment	3%
			P.i6b	Organization's objectives support	3%
			P.i6c	Response to ISS performance results	3%
			P.i7	Benefits perception	3%
			P.i8	Executive management commitment	
			P.i8a	Information assets protection	3%
			P.i8b	ISS related decisions	3%
			P.i8c	ISS strategy and policy development and approval	3%
			P.i8d	Allocation of investments and resources	3%
			P.i9	Risk management policy	3%
			P.i9a	Risk review timeline	3%
			P.i9b	Risk appetite presence	2.2%
			P.i10	Risk appetite for new risks	3%
			P.i11	ISS incident supervision	2.2%
			P.i12	ISS incident coordination	2.2%
Processes			P.i13	Resource management	
			P.i13a	Responsibility assignment	3%
			P.i13b	Adequate personnel	2.2%
			P.i13c	Security culture	3%
			P.i14	Stakeholders communication and reporting	
			P.i14a	Principles and guidelines for communicating and reporting	3%
			P.i14b	Principles to safeguard resources	2.2%
			P.i14c	Escalation guidelines	3%
			P.i15	ISS activity effectiveness	3%
			P.i15a	ISS activity effectiveness assessment timeline	3%
			P.i16	ISS performance metrics alignment	3%
			P.i17	ISS activity feedback return	2.2%
			P.i18	Delivery of ISS activity feedback	2.2%
			P.i19	ISS performance results feedback	2.2%
			P.i20	ISS program compliance	3%
			P.i20a	Compliance alignment report	2.2%
			P.i20b	Presence of Auditors	3%

			P.i20c	Auditors meetings timeline	3%
			P.i21	ISS level	3%
			P.i22	Environment changes and risks	3%
			P.i23	Revision of regulations timeline	3%
			P.i23a	Reviewing process	2.2%
			P.i23b	Reviewing process timeline	3%
			P.i24	ISS feedback transparency	3%
				Total weight for P indicators	100%
G	25%	20%	G.i25	ISSG goals	
			G.i25a	Strategic alignment	11%
			G.i25b	Value delivery	11%
			G.i25c	Accountability	11%
			G.i25d	Compliance	11%
			G.i26	Balance stakeholders needs	11%
Goals			G.i27	ISSG goals and objectives integration	8%
			G.i28	ISSG value perception	
			G.i28a	ISSG effectiveness	11%
			G.i28b	ISSG efficiency	11%
			G.i29	ISSG accountability	7%
			G.i30	ISSG compliance	8%
				Total weight for G indicators	100%
Ag	25%	40%	Ag.i31	Person in charge of the organization's ISS	8%
			Ag.i31a	Role responsibility	6%
			Ag.i31b	Role career level	6%
			Ag.i31c	Role distribution	6%
			Ag.i32	Artifact creation	
			Ag.i32a	Governing body's artifacts	8%
			Ag.i32b	City Hall executive artifacts	8%
			Ag.i32c	Person in charge of the organization's ISS artifacts	8%
Agents			Ag.i33	Reporting structure	
			Ag.i33a	Governing body	8%
			Ag.i33b	Mayor	6%
			Ag.i33c	City Councilor	6%
			Ag.i33d	Person in charge of the organization's ISS reporting	8%
			Ag.i33e	Auditors	8%
			Ag.i33f	Data Protection Officer	8%
			Ag.i33g	Employees	6%
				Total weight for Ag indicators	100%
Total	100%				

Also, within the global indicator part, is a description on how to calculate the index. The initial part of the index calculation can be performed following the steps indicated within part 5.3 of the guide (inside Appendix L – Artifact Construction: Methodological Guide); or using the generic formulas developed to summarize the process, displayed bellow.

$$IV = AV_n \times QW_n$$

$$CV_D = \sum_{n=1}^{TQ} [IV]$$

Or

$$CV_D = \sum_{n=1}^{TQ} [AV_n \times QW_n]$$

These summarized generic formulas, shows two ways to calculate the indicator value (IV) and the criteria value (CV). Also, within the formulas, the other elements (in order of appearance) represented are: the answer value[34] (AV) given to each question of the instrument, the respective indicator weight (QW), n represents the question number, D represents the criteria (which can be AR, P, G or Ag), and TQ represents the total of question of said criteria.

Once the initial portion of the index is calculated and the criteria value is achieved, then starts the second portion, which uses the criteria value (of each of the criteria) and their weights to evaluate the ISSG index. The criteria weights were assigned in accordance with the method used.

The ISSG index uses one of two methods to evaluate the amount of ISSG a City Hall possesses, and they are: global or by scenario. In the first method (global – a.k.a. EISSGLPAG), the City Hall is evaluated as a whole, with no distinction if it already possesses an ISSG in place or not. Therefore, the criteria weights remain the same 25% for each of the criteria. At the end of this part, Table 34, displays the formulas with the weights of the criteria for each method.

While for the calculation of the second method, by scenarios, the City Halls are evaluated according to the presence of an ISSG. Hence, two different paths can be calculated under the scenario's method. The path is decided by the answer given to the first question of the instrument, and each path (scenario1 or scenario 2) presents different weights to their criteria.

The first scenario (Sc1 – a.k.a EISSGLPA1) represents a City Hall with an ISSG already in place. Therefore, each criterion is evaluated equally (with the same 25% criterion weight, similar to the weights of the global method), in order to evaluate which aspect needs to be improved. While the second scenario (Sc2 – a.k.a. EISSGLPA2), the City Hall doesn't possess a formal ISSG in place, consequently the instrument will help with the implementation by demonstrating the aspects that needs to be worked on. The weights are different from the previous two, as it can be observed in Table 34, with the highest weight being Agents(Ag) with 40%.

Table 34 – ISSG index formulas

Method	Formula
Global	$i(EISSGLPAG) = 25\%\ x\ Ar + 25\%\ x\ P + 25\%\ x\ G + 25\%\ x\ Ag$
Scenario 1	$i(EISSGLPA1) = 25\%\ x\ Ar + 25\%\ x\ P + 25\%\ x\ G + 25\%\ x\ Ag$
Scenario 2	$i(EISSGLPA2) = 20\%\ x\ Ar + 20\%\ x\ P + 20\%\ x\ G + 40\%\ x\ Ag$

[34] The values for each indicator is found in part 5.3 of the methodological guide; or in the accessory created to help with this process displayed in Appendix M – Methodological Guide Accessory – Instrument V5 Cheat Sheet. This accessory is to be used by the aplicator and possesses the instrument answers accompanied by their value.

5.3 Evaluation and Performance Measures

Guideline 3 (Design Evaluation)

The next step of the DSR methodology is evaluation; which evaluates the intrument's objectives either from a literature review, or from the use of experts. The second can be performed either by a focus group or a consensus panel [Litwin 2003]. They will help in define and clarify objectives, to better fit the questionnaire's context of ISSG in Portuguese Local Public Administration. However due to the constrict of time, this part wasn't able to be fully performed.

Concurrent to what was mentioned in the previous paragraph, psychometrics was used to evaluate the instrument itself. These metrics provide the researchers a way to quantify with precision the measurements of qualitative concepts [Litwin 2003]. Since it is difficult to assess the quality of data collected; it was used a form, which assesses the accuracy of the collected data from the instrument [Litwin 2003].

One method, to assess the data from the questionnaire, is by attesting their reliability[35], in which, to minimize error (from random or measurement kind), and make sure the accurate reflection of data is provided [Litwin 2003]. The first workaround is the selection of a large representative sample (in order to minimize random error); which, in this case, is being met by the evaluation of the 308 City Halls that compose the Portuguese Local Public Administration. The other workaround are the precise answers of the instrument, which minimizes the measurement error.

Aside from its reliability, the instrument should also be attested for its validity. This means that the instrument should also be assessed on how well the instrument measures what is intended to measure [Litwin 2003].

As an initial step to assess the validity of the instrument, two pretests were generated. The first would emulate the answers of a City Hall that already had an ISSG present (Scenario 1) would give, while the second would emulate the answers of a City Hall that does not have an ISSG present (Scenario 2). These two sets of answers, were each placed on a table, created in order to display the answers for each scenario and their respective points. Table 74 and Table 77, represent respectively Scenario 1 and Scenario 2, and can be found in Appendix N – Instrument Evaluation: Pretest.

Also, within the same Appendix, two radar charts are displayed. They were created, one for each scenario. Where Figure 32 represent Scenario 1 and Figure 33 represents Scenario 2. Comparing

[35] "a statistical measure of the reproducibility or stability of data gathered by the survey instrument" [Litwin 2003]

the charts between both scenarios, the area for the first scenario is bigger than the area of the second scenario. This is expected, since the first scenario reflects a City Hall with ISSG implemented, therefore with more elements of the criterias implemented.

Additionally, right after the radar chart, is a table that represents the criterion value for each criterion of the respective scenario. The creation of Table 75 and Table 78 helps to assess the discrepancy found against each criteria. Those findings are explained within the subsequent paragraphs.

A greater discrepancy, in numbers, visible between scenarios is for the artifacts and processes criteria, showed in the chart, with one of the scenarios having the top right side of the chart bigger and closer to the edge (where the values were closer to 1). This discrepancy appears in scenario 1 which represents a City Hall that has ISSG implemented, thus having more elements of the criteria implemented, resulting in higher values for the artifacts and processes criterias (in order values of 0,77 and 0,72). These previous values are greater than what it is seen in the same criteria for scenario 2, which are 0,50 and 0,38 values for artifacts and processes criterias.

As for the other two remaining criteria, Goals and Agents, the values diverge slightly for Goals, with a difference of only 0,08 between the scenarios, where scenario 1 value is 0,54 and the value for scenario 2 is 0,46. There is a similar difference for the Agents criterion, though the values difference is double than in Goals, with a total of 0,16. Also in this criterion, the scenario 1 value is higher than in scenario 2, the first has a value of 0,62 while the value for the second is 0,46.

Within the criteria on both scenarios, the highest value encountered was for the Artifacts criteria, in scenario 1, with a total value of 0,77, while the lower value was found in scenario 2, for the Process criteria, with a value of 0,38. The criteria which had the biggest discrepancy was the Process criteria, with a difference in value of 0.34. Also, the criterion with the shortest amount of discrepancy in values was the Goals criterion, with a 0.08 value difference.

The final aspect of the scenarios evaluated was the global indicator (a.k.a ISSG index). Their results would be evaluated against a five-point scale, displayed in Table 35. The scale classes vary from poorly implemented to successfully implemented, and help determine the achievement of ISSG within the City Hall. Furthermore, this range could help sorting City Halls by the value achieved.

Table 35 – ISSG Index Scale

Value	Implementation
0 to 25%	Poorly implemented
26 to 50%	Slightly Implemented
51 to 75%	Reasonably implemented
76 to 90%	Well Implemented
91 to 100%	Successfully Implemented

The tables containing the formulas used to evaluate the ISSG index and the respective value for each scenario can be found in Table 76 for scenario 1 and in Table 79 for scenario 2, both within Appendix N – Instrument Evaluation: Pretest. Each table evaluates the ISSG index for the global method and the respective scenario method. Scenario 1 presented the same value of 0,66, for both the global evaluation and the scenario 1 evaluation, since both of these methods have the same criteria weights.

While scenario 2, which in this case, had the same value for both evaluations (global and scenario 2) of 0,45; even though there is a difference between the criteria weights for scenario 2, a balance was perceived.

It is worth mention that the scenarios are placed at different levels within the index scale. Where scenario 1 appears at a higher level than scenario 2, respectively placed as reasonably implemented and the other as slightly implemented. Therefore the City Hall's ISSG in scenario 1 is better implemented than in scenario 2, which is in line with the instrument's expectations.

5.4 Conclusion

Guideline 7 (Communication of Research)

Finally, the last step in the DSR methodology is the communication of the results. These results are the creation of this document (thesis), where the instrument created and its contents are explained; which will be later presented to a board (in the form of a thesis defence). It should be noted that the objectives set out in the first Chapter: the creation of an artifact/instrument to evaluate the ISSG in local public administration have been accomplished, as well as the creation of a secondary artifact, the methodological guide, to help surveyors on how to perform the evaluation of the instrument created.

6 Conclusions

This document was designed with the intent of outlining the phases that constitute this research work. Within the next four sections, a summarized discussion of the efforts made in order to produce this document will be displayed, while considering the previously stipulated objectives found in part 1.2 of Chapter 1.

Within the next sections of this chapter, the subsequent topics will be discussed: contributions, limitations, future works, and the final considerations. As the name suggests, the first division will convey the contributions that have been added due to the development of this study. The second division will present the limitations of the developed work; whereas the third division, presents the ideas for future works, based in this study, that were also envisioned while developing the study. Finally, the last part, will present the final considerations of the work.

6.1 Contributions

In regards of the contributions of this work, one should start by analyzing what was proposed and set on the first chapter of this document. The three main objectives set out were: Characterize the ISSG activity; Create an ISSG assessment tool for the Local Public Administration context; and Create a Methodological Guide for the application of the assessment tool for the ISSG in the Local Public Administration context.

The first objective was carried out by an extensive literature review, located in Chapter 2. Within the literature review, five documents, that best represented the subject, were analyzed in depth. From this analysis, it was possible to find the key elements in order to characterize the ISSG activity. Thus, not only fulfilling the objective, but contributing to clarify the subject of the study.

To fulfill the second objective, an evaluation instrument, in a form of a questionnaire, was created. The instrument used, as a base for its creation, the knowledge gather from the literature review of the ISSG subject (Chapter 2) and the literature review of Chapter 3 (which focused on ISSG within the context of the Portuguese Local Public Administration, and the DSR methodology used in this study). The steps used to develop the instrument are found across Chapter 4 (Artifact Creation Process) and Chapter 5 (Artifact Outputs).

Also, within the same chapter (Artifact Outputs) is the description of the methodological guide, which was created to assist in the instrument application. Consequently, representing the fulfillment of the final objective.

These three objectives were formulated in order to elucidate the research question posed by this study. The question “How to evaluate the ISSG in Local Public Administration bodies?” derived from a gap observed in previous studies that showed a slow adoption of ISS policies by Portuguese City Halls. Therefore, with the creation of the study’s instrument, the goal was to be able to evaluate the ISSG in the Portuguese Local Public Administration. Thus, attempting to answer the proposed question, and also bridge the gap found within the context of the Portuguese City Halls.

6.2 Limitations

The major limitation of this study is the non-validation of the instrument. Time restrictions interfered in the performance of the evaluation step of DSR, with the instrument and methodological guide not being able to be reviewed by either a focus group or a consensus panel. This was partially overcome by the extensive literature review process, used in the development of the instrument; complemented by the performance of two pretests.

6.3 Future Work

Throughout the development of this study, several other paths could have been followed. Those paths represent opportunities that have been left unexplored. Therefore, these opportunities should be considered in a future work.

As a first suggestion, would be the review of the instrument by a focus group or an consensus panel. This review would allow the validation of the instrument and methodological guide for a better fine tune of the questionnaire within the context of its application, either in the Portuguese territory or some other country.

In addition to this suggestion, another could be made that the criteria weights should also be reviewed to incorporate and reflect changes of the different environments (such as legal, organizational, technological and political). This would lead to a better characterization of the study’s context, either within the Portuguese territory or other country.

Another suggestion would be the implementation of the study's instrument in the Portuguese territory. In order to evaluate the current state of the Portuguese City Halls, as well as to analyze the City Halls by scenarios.

Among these analyzes, a ranking regarding the City Halls could be produced; that would display the highest and lower amongst them. This rank could check the discrepancy between the City Halls, either by region or by district, and check positive actions that could be carried out in other locations.

6.4 Final Considerations

Lately, the intensity and impact an organization (in this case the Portuguese City Halls) may suffer, once a failure occurs in their Information Systems, has increased exponentially, due to an increase in daily use of information and the dependency on Information Systems by the City Halls. Therefore, the concerns about this type of risk have become key issues in organizations.

Those risks prompted the Portuguese Government to improve the performance of this sector through governance, as it can be observed in *Estratégia TIC 2020* (part 3.1.3.2). Though, as revealed in this study, by analyzing recent studies in this area, the actions taken by the government, indicated a lack of adoption by the City Halls.

This problem, exemplified by the lower adoption of ISS policies in City Halls, inspired the development of this study that focuses on the ISSG in the Local Public Administration, as to why those ISS policies adoptions were low. In order to better investigate this perspective, a stipulated set of objectives was produced, that once completed would produce a characterization of the ISSG activity, and an instrument that would allow for the evaluation of the ISSG in the Portuguese Local Public Administration (e.g. City Halls).

The instrument was set to evaluate different aspects of ISSG, and was created using the most relevant literature in the area. While its initial focus was to be applied in the Portuguese context; the instrument could also be used in other countries, though a review would be advised to better fit into that particular context.

As final considerations, one could highlight the contributions to the area created by the unique point of view presented in this work; which focuses on the Evaluation of the Information Systems Security Governance of the Portuguese Local Public Administration, mainly their City Halls, which have not been explored so far, as it was demonstrated by the literature research within this document. In addition, it is expected that with the creation of the study's main artifacts (the evaluation instrument for ISSG in the

Portuguese City Halls and the accompanied methodological guide), they will help to enrich the knowledge within the area of Information Systems, especially with regard to Information Systems Security Governance.

Appendices

Appendix A – Literature and Concept Matrices

This appendix is comprised of four matrices, that were used in Chaper 2 - Literature Review. The first table, Table 36, presents the documents used to create this study and the place where each of them was gathered. The table also shows their number of citations. Also the documents are ordered from newest to oldest, and their ordering number is correlated for the number of the articles presented in the following concept tables.

The next table, Table 37, is the concept matrix for govenance, where the IT related articles are crossed with concepts related to information systems security governance. Than the connection is created by using the page number in article in which the concept appears, is mentioned or reffered.

The concept matrix for public administration, Table 38, presents the connection between the articles, and the concepts related to the portuguese local public administration. Their connection is also created with the number from the page in the article, which the concept appears, is mentioned or reffered.

The last concept matrix, Table 39, presents the connection between the articles, and the concepts of the methodology. The connection is created again, with the number from the page in the article where the concept appears, is mentioned or reffered.

Table 36 – Literature Matrix

Order	Document			Research						Citations
	Title	Author	Year	RepositoriUM	B-on	Google Scholar	Scopus	Web of Knowledge	Others	
1	*Caracterização Infraestrutural , Aplicacional e Funcional das Tecnologias e Sistemas de Informação nas Câmaras Municipais Portuguesas.*	Almeida, I. A.	2017						x	
2	*Lista de Municípios.*	Associação Nacional Municípios Portugueses	2017						x	
3	*European Commission, Eurostat, NUTS - Nomenclature of territorial units for statistics, NUTS Maps.*	Eurostat	2017						x	
4	*Proposed Framework for Information Systems Security for e-Governance in Developing Nations.*	Gupta, R., Muttoo, S. K., and Pal, S. K.	2017							
5	*Strengthening digital society against cyber shocks: Key findings from the Global State of Information Security Survey 2018, 20.*	PricewaterhouseCoopers	2017						x	
6	*Candidatos à Presidência da Câmara.*	Secretaria Geral Ministério da Administração Interna	2017						x	
7	*Eleições Autárquicas 2017, 1 outubro, Resultados, Portugal Continente e Regiões Autónomas, Território Nacional, Câmara Municipal.*	Secretaria Geral Ministério da Administração Interna	2017						x	
8	*Presença na Internet das Câmaras Municipais Portuguesas em 2016 : Estudo sobre Local e-Government em Portugal.*	Soares, D., Amaral, L., and Ferreira, L.	2017						x	
9	*2017 Data Breach Investigations Report.*	Verizon	2017						x	
10	*Regulation 2016/679 of the European parliament and the Council of the European Union.*	European Union	2016						x	
11	*População média anual residente (N.º) por Local de residência (Distrito/ Região), Sexo e Grupo etário (Por ciclos de vida); Anual.*	INE	2016						x	
12	*Evolução da Institucionalização de Políticas de Segurança de Sistemas de Informação na Administração Pública Portuguesa.*	Lopes, I. M., and Oliveira, P.	2016						x	
13	*Information system security governance: Technology Intelligence perspective.*	Zaydi, M., and Nasserddine, B.	2016				x			
14	*O que é o PGETIC?*	Agência para Modernização Administrativa	2015						x	
15	*IT Security Governance in E-banking.*	Tsiakis, T., Kargidis, T., and Chatzipoulidis, A.	2015				x			
16	*IT Governance in Public Administrations.*	Querido, D.	2014						x	
17	*ISO/IEC 27014:2013 - Information technology - security techniques - Governance of information security.*	ISO/IEC	2013						x	
18	*The Applicability of ISO /IEC 27014 : 2013 For Use Within General Medical Practice.*	Mahncke, R. J.	2013			x				
19	*Sintomatologia do Desalinhamento e Desajustamento de Sistemas de informação*	Fidalgo, P.	2013	x						

Order	Document			Research						Citations
	Title	Author	Year	RepositoriUM	B-on	Google Scholar	Scopus	Web of Knowledge	Others	
20	*COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT.*	ISACA	2012						x	61
21	*COBIT 5: Enabling Processes.*	ISACA	2012						x	
22	*Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal.*	Lopes, I. M.	2012	x						
23	*Information security governance in Saudi organizations: an empirical study.*	Abu-Musa, A.	2010				x			18
24	*A Design Research Approach to Developing User Innovation Workshops in Second Life.*	Helms, R., Giovacchini, E., Teigland, R., and Kohler, T.	2010			x				11
25	*Information Systems Security Policies : A Survey in Portuguese Public Administration.*	Lopes, I. M., and de Sá-Soares, F.	2010	x						
26	*Global Technology Audit Guide (GTAG®) 15 Information Security Governance.*	Love, P., Reinhard, J., Schwab, A. J., and Spafford, G.	2010						x	
27	*Corporate Governance.*	Reinert, K. A., Rajan, R. S., Glass, A. J., and Davis, L. S.	2010						x	
28	*Information security governance.*	von Solms, S. H., and von Solms, R.	2009						x	
29	*Identifying Governance Dimensions to Evaluate Information Systems Security in Organizations.*	Dhillon, G., Tejay, G., and Weiyin, H.	2007				x			10
30	*A Three Cycle View of Design Science Research.*	Hevner, A. R.	2007			x				983
31	*A Paradigmatic Analysis of Information Systems as a Design Science.*	Iivari, J.	2007			x				454
32	*An Information Security Governance Framework.*	Veiga, A. Da, and Eloff, J. H. P.	2007				x			97
33	*Information Security Handbook : A Guide for Managers.*	Bowen, P., Hash, J., and Wilson, M.	2006						x	
34	*Interpretação da Segurança de Sistemas de Informação Segundo a Teoria da Acção.*	de Sá-Soares, F.	2005	x						
35	*Design Science in Information Systems Research.*	Hevner, A. R., March, S. T., Park, J., and Ram, S.	2004		x					
36	*Direito Administrativo Geral - Tomo I - Introdução e princípios fundamentais (1a Edição).*	Sousa, M. R. de, and Matos, A. S. de.	2004						x	
37	*Design Science Research in Information Systems.*	Vaishnavi, V., and Kuechler, B.	2004						x	
38	*Applying information security governance.*	Moulton, R., and Coles, R. S.	2003					x		
39	*Strategic Planning for Information Systems (3rd ed.).*	Ward, J., and Peppard, J. O. E.	2002						x	
40	*Resolução do Conselho de Ministros n.º 22/2001.*	Presidência do Conselho de Ministros	2001						x	
41	*Managing Information System Security.*	Dhillon, G.	1997						x	
42	*Design and natural science research on information technology.*	March, S. T., and Smith, G. F.	1995				x			1527
43	*Modeling Design Processes.*	Takeda, H., Veerkamp, P., Tomiyama, T., and Yoshikawa, H.	1990				x			233
44	*Foundations of Behavioral Research (3rd Edition).*	Kerlinger, F. N.	1986						x	
45	*Constituição da República Portuguesa.*	Assembleia da República Portuguesa	1976						x	

Table 37 – Governance Concept Matrix

Concept/Article		32	38	20	27	29	28	23	33	13	17	15	18
Governance	Definition		580;	13; 31;	227;								
	Models					6-7;				2;	2; 3; 5;	253;	35;
Corporate governance	Definition		580;				1-2;						
	Structure						2-4; 6; 18-19; 26-27;						
	Responsibilities					6;	2-4;						
IT Governance	Definition						9-11;	228;			2-3;		
	Importance			13;			10-11;			1;			
ISG	Definition		581;	31;			24-25;	228;	2;	3;	1-2;		30;
	Purpose	369;	584;	24;			24-25;		2;	3;			
	Importance	361-362; 369-370;	581;	13;			25;	229-230;	2;	2; 6;	iv;		29-30;
	Objectives		582;	13;					2;		2;	253;	
	Roles	368;	583;	24;					8-12;		iv; 1-2;		35-37;
	Responsibilities	363; 367-369;	581; 583-584;	24; 27-29;		2;			9-12;	3;			
	COBIT						11-14; 20; 26; 41-43; 48-49;	244;		3-4;		255;	
	ISO	364; 369-370;					20; 43-58;	242;		3-4;		255;	
	Other frameworks	363-368; 370;	584;			2-6;	4-6;	232-237;	12-14;	3; 5;		253; 256;	
ISSG	Definition					1; 7;							

Table 38 – Public Administration Concept Matrix

Concept/ Article			25	22	12	8	1	15
Public Administration	Definition	Importance	61;	2-4; 45-46;	240;	1;	1;	3-5;
	Responsibilities		61;		240;		3;	
	Dimension	Population	62; 65;		241-242;	61-66;		
		City Council Electoral Dimension	66;	48;	243;			
	Information System Security	Use	62;	71-76;	242;			
		Policies	64;	13-42;	242; 245;			
		Future Work	68;		245;			
	Survey	Reason			240-241;	52;		
		Description	65;	77-78;	241;		43-62;	28-36;
		Structure	65-66;	78-80;	242;	6-15;	63-69;	37-41;
		Results	66-68;	81-96;	242-244;	16-51;	69-104;	42-50;
		Limitations		80-81;	244;	56;	106;	53;
	IT Governance	Definition					28-29;	10-11;
		Frameworks					29-34;	12-15;
	PGETIC							15-19; 23-25;
	Research Method	Description				2; 5-6;	8-12;	7-8; 25-27;
		Results				3;		

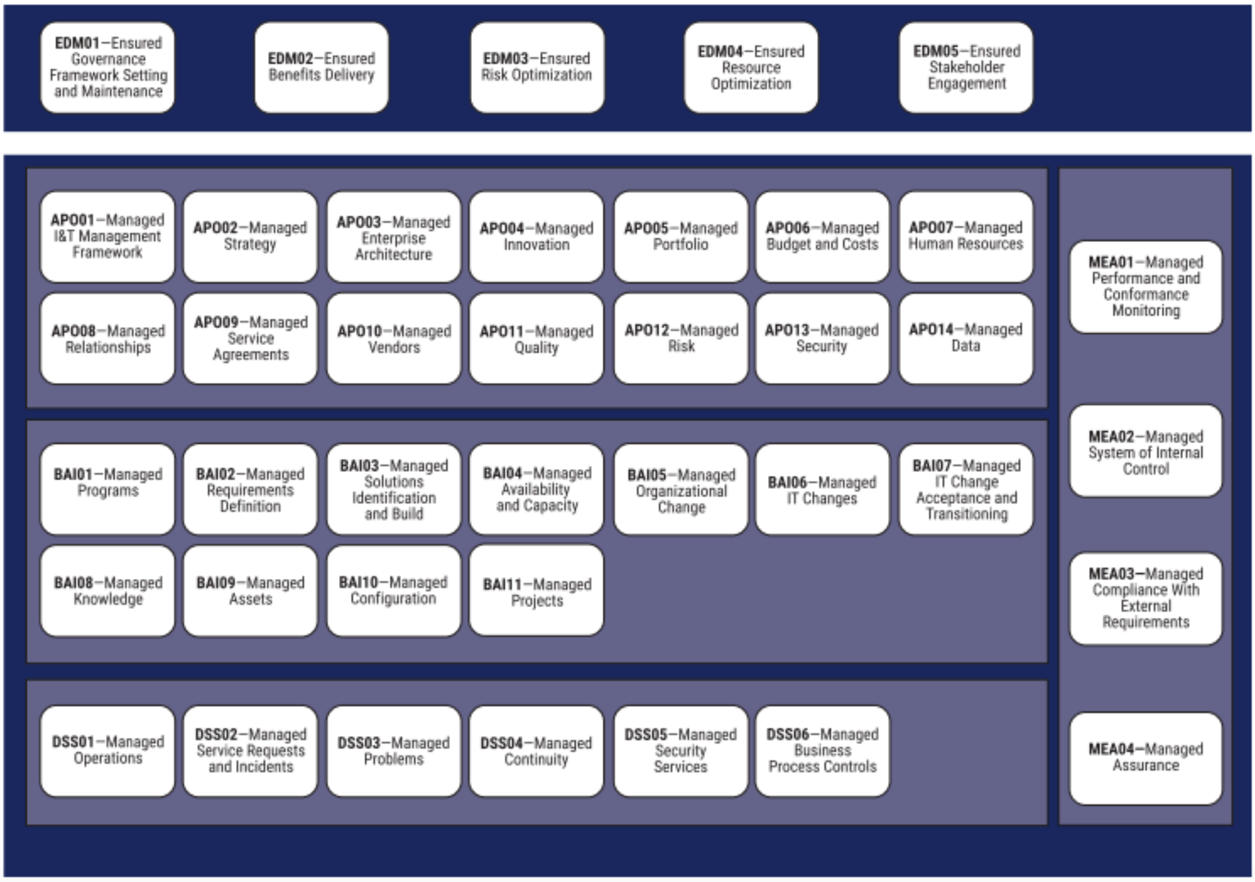
Table 39 – DSR Concept Matrix

<table>
<tr><th colspan="4">Concept / Article</th><th colspan="2">30</th><th colspan="2">35</th><th colspan="2">24</th><th>31</th><th colspan="2">42</th><th colspan="2">43</th><th colspan="2">37</th><th colspan="2">19</th></tr>
<tr><td colspan="4">Definition</td><td colspan="2"></td><td colspan="2"></td><td colspan="2">8;</td><td></td><td colspan="2"></td><td colspan="2"></td><td colspan="2">1; 9;</td><td colspan="2"></td></tr>
<tr><td colspan="4">Description</td><td colspan="2"></td><td colspan="2"></td><td colspan="2">4; 27;</td><td></td><td colspan="2"></td><td colspan="2"></td><td colspan="2">1;</td><td colspan="2"></td></tr>
<tr><td colspan="4">History</td><td colspan="2"></td><td colspan="2"></td><td colspan="2">8;</td><td>39;</td><td colspan="2"></td><td colspan="2"></td><td colspan="2">2;</td><td colspan="2"></td></tr>
<tr><td colspan="4">Reasons</td><td colspan="2"></td><td colspan="2"></td><td colspan="2">10;</td><td></td><td colspan="2"></td><td colspan="2">37;</td><td colspan="2">3;</td><td colspan="2">80;</td></tr>
<tr><td rowspan="23">Methodology</td><td rowspan="6">Research</td><td rowspan="4">Approach</td><td>Knowledge</td><td colspan="2">89-90;</td><td colspan="2">76; 80; 99;</td><td rowspan="4">4; 27;</td><td>6; 8-9;</td><td>45; 47; 49; 53;</td><td colspan="2">251-254; 257;</td><td colspan="2">38-39; 44;</td><td colspan="2">2; 4-5; 9; 15;</td><td colspan="2">88; 92;</td></tr>
<tr><td>Principles</td><td colspan="2"></td><td colspan="2"></td><td>9;</td><td></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>Procedures</td><td colspan="2"></td><td colspan="2"></td><td>9-10;</td><td></td><td colspan="2"></td><td colspan="2"></td><td colspan="2">8;</td><td colspan="2"></td></tr>
<tr><td>Analysis</td><td colspan="2"></td><td colspan="2"></td><td>8;</td><td></td><td colspan="2"></td><td colspan="2">38;</td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2">IS context</td><td colspan="2">87-88; 92;</td><td colspan="2">75-79; 81; 88-89; 98-99;</td><td colspan="2"></td><td>39; 41;43; 45; 48-49; 54-55;</td><td colspan="2"></td><td colspan="2"></td><td colspan="2">1-3; 8-9;</td><td colspan="2">81; 85; 89;</td></tr>
<tr><td colspan="2">Limitations</td><td colspan="2"></td><td colspan="2">81; 98-99;</td><td colspan="2">27;</td><td></td><td colspan="2">254;</td><td colspan="2">43;</td><td colspan="2">6;</td><td colspan="2"></td></tr>
<tr><td colspan="2" rowspan="3">Paradigmas</td><td>Behaviour Science</td><td rowspan="3">88;</td><td></td><td rowspan="3">76;</td><td>75-77; 79-80; 84-85; 88; 98;</td><td colspan="2"></td><td></td><td colspan="2"></td><td colspan="2">37;</td><td colspan="2"></td><td colspan="2">81;</td></tr>
<tr><td>Natural Science Research</td><td>87;</td><td>76; 98;</td><td colspan="2"></td><td></td><td colspan="2">252-262;</td><td colspan="2"></td><td colspan="2">2;</td><td colspan="2">81-82; 85;</td></tr>
<tr><td>Design Science</td><td>91;</td><td>75-80; 84; 88; 98-99;</td><td colspan="2"></td><td>41; 43; 47-49; 52-55;</td><td colspan="2">252-258;</td><td colspan="2">37;</td><td colspan="2">2; 15;</td><td colspan="2">81-82; 85;</td></tr>
<tr><td colspan="2" rowspan="3">Philosophy</td><td>Ontology</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td>41-45; 53-54;</td><td colspan="2"></td><td colspan="2"></td><td colspan="2">9-10;</td><td colspan="2">84; 87;</td></tr>
<tr><td>Epistemology</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td>45-49; 53-54;</td><td colspan="2"></td><td colspan="2"></td><td colspan="2">9-10;</td><td colspan="2">84-87;</td></tr>
<tr><td>Axiology</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td></td><td colspan="2"></td><td colspan="2"></td><td colspan="2">9-10;</td><td colspan="2">85-87;</td></tr>
<tr><td colspan="2" rowspan="2">Perspectives</td><td>Positivist</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td></td><td colspan="2"></td><td colspan="2"></td><td colspan="2">9; 12;</td><td colspan="2"></td></tr>
<tr><td>Interpretative</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td></td><td colspan="2"></td><td colspan="2"></td><td colspan="2">9;</td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td>Design</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td></td><td colspan="2"></td><td colspan="2"></td><td colspan="2">2-4;</td><td colspan="2"></td></tr>
<tr><td colspan="2" rowspan="3">Cycles</td><td>Design</td><td rowspan="3">88;</td><td>88; 90-91;</td><td colspan="2">88;</td><td colspan="2">27;</td><td></td><td colspan="2"></td><td colspan="2">38-39; 41-43; 46;</td><td colspan="2">10;</td><td colspan="2">86-87; 89; 93-94;</td></tr>
<tr><td>Rigor</td><td>88-90;</td><td colspan="2">80; 87-88; 99;</td><td colspan="2">8; 27;</td><td>50-52; 55;</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2">88; 91-92;</td></tr>
<tr><td>Relevance</td><td>88-89;</td><td colspan="2">85;</td><td colspan="2"></td><td></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2">86-88; 91;</td></tr>
<tr><td rowspan="5">Design Process</td><td rowspan="5">Steps</td><td>Problem Awareness</td><td colspan="2">89;</td><td rowspan="5">78; 81;</td><td>79; 85;</td><td rowspan="5">7-10;</td><td>10-11;</td><td></td><td rowspan="5">252;</td><td></td><td rowspan="5">37-38; 40-41;</td><td>43;</td><td rowspan="5">5;</td><td>5; 8; 11;</td><td rowspan="5">90;</td><td>80; 91-92;</td></tr>
<tr><td>Suggestion</td><td colspan="2"></td><td></td><td>10-11;</td><td></td><td></td><td>43;</td><td>5; 11;</td><td>92;</td></tr>
<tr><td>Development</td><td colspan="2">90;</td><td>85;</td><td>8-10;</td><td>51;</td><td>252; 254; 258; 261;</td><td>38-39; 42-43; 45;</td><td>5; 11-12;</td><td>89; 93;</td></tr>
<tr><td>Evaluation</td><td colspan="2">89-90;</td><td>79; 85-87; 99;</td><td>7; 9;</td><td>50; 54-55;</td><td>254; 258; 261; 263;</td><td>42-43;</td><td>5; 12;</td><td>94;</td></tr>
<tr><td>Conclusion</td><td colspan="2"></td><td></td><td></td><td></td><td></td><td>43; 46;</td><td>5; 12;</td><td>94;</td></tr>
</table>

Concept / Article			30	35		24		31		42		43		37		19	
		Interactivity	89-90;		85; 88;		27;	52;					38-42; 44;		5; 9;		89;
Artifact	Outputs	Constructs		75; 78; 84; 88; 98;	77-78; 83;	8-10;		41-42; 44; 46; 54;	43;	251-254; 256; 260; 262; 263;	253; 256; 261;	38;		1; 5-6; 8; 15;	6;	82; 84; 93-94;	82;
		Model			77-78; 83; 87;				43-44; 47;		253; 256-257; 260-261; 263;	37; 47;			6;		82-83;
		Methods			77; 79; 84; 86-87;				43; 46; 50;		253; 257; 261-263;				6; 11;		83;
		Intantiations			77; 79; 84; 87;				43;		258; 260-262;				6;		83;
		Better Theories			99;				45; 49; 52-53;		254; 259; 262-263;	37; 38;			6; 7;		83-84;
	Guidelines	Design Artifact			82-84; 87;				50-51;			47;					88-89; 91-94;
		Problem Relevance			84-85;				52;								
		Design Evaluation			85;				52;			41-42;					
		Contributions			81; 87;		9;										
		Research Rigor			87; 88;				50-51;			41; 44;					
		Search Process			88;				51;			44;					
		Communication			90;		9; 27;										
	Paper Example			77; 85-87; 89; 90-97		4-8; 11-28;		45;		262-263;		43; 46;		12-14;		92-95;	

Appendix B – COBIT® 2019 COBIT Core Model

COBIT® 2019 presents 40 processes for the enterprise I&T. These processes are separated between Govenance and Management objectives. Figure 17 presents these processes structured in accordance with these separation, dark blue for Governance objectives and Light blue for Management objectives.



EDM01–Ensured Governance Framework Setting and Maintenance
EDM02–Ensured Benefits Delivery
EDM03–Ensured Risk Optimization
EDM04–Ensured Resource Optimization
EDM05–Ensured Stakeholder Engagement

APO01–Managed I&T Management Framework
APO02–Managed Strategy
APO03–Managed Enterprise Architecture
APO04–Managed Innovation
APO05–Managed Portfolio
APO06–Managed Budget and Costs
APO07–Managed Human Resources
APO08–Managed Relationships
APO09–Managed Service Agreements
APO10–Managed Vendors
APO11–Managed Quality
APO12–Managed Risk
APO13–Managed Security
APO14–Managed Data

BAI01–Managed Programs
BAI02–Managed Requirements Definition
BAI03–Managed Solutions Identification and Build
BAI04–Managed Availability and Capacity
BAI05–Managed Organizational Change
BAI06–Managed IT Changes
BAI07–Managed IT Change Acceptance and Transitioning
BAI08–Managed Knowledge
BAI09–Managed Assets
BAI10–Managed Configuration
BAI11–Managed Projects

DSS01–Managed Operations
DSS02–Managed Service Requests and Incidents
DSS03–Managed Problems
DSS04–Managed Continuity
DSS05–Managed Security Services
DSS06–Managed Business Process Controls

MEA01–Managed Performance and Conformance Monitoring
MEA02–Managed System of Internal Control
MEA03–Managed Compliance With External Requirements
MEA04–Managed Assurance

Figure 17 – COBIT® 2019 Process Reference Model

Source: ISACA [2018b]

Appendix C – Portuguese Population by City Hall

In Table 40 the 308 city halls are grouped by NUTS designation and code, and their caracteristics. These caracteristics include which district the city halls belong to, which zone is located in, the size dimension, and the resident population.

Table 40 – Portuguese Population by City Hall

Adapted from: Eurostat [2017], INE [2016] and Soares et al.[2017]

NUTS	Code	Name	District	ICI Zone	Dimension	Population (2016)
NUTS I	1	Continente				9809414
NUTS II	11	Norte				3584575
NUTS III	111	Alto Minho				233813
City Hall	1111601	Arcos de Valdevez	Viana do Castelo	Coastal	Medium	21324
City Hall	1111602	Caminha	Viana do Castelo	Coastal	Small	15971
City Hall	1111603	Melgaço	Viana do Castelo	Coastal	Small	8400
City Hall	1111604	Monção	Viana do Castelo	Coastal	Small	18192
City Hall	1111605	Paredes de Coura	Viana do Castelo	Coastal	Small	8712
City Hall	1111606	Ponte da Barca	Viana do Castelo	Coastal	Small	11392
City Hall	1111607	Ponte de Lima	Viana do Castelo	Coastal	Medium	42060
City Hall	1111608	Valença	Viana do Castelo	Coastal	Small	13437
City Hall	1111609	Viana do Castelo	Viana do Castelo	Coastal	Medium	85445
City Hall	1111610	Vila Nova de Cerveira	Viana do Castelo	Coastal	Small	8880
NUTS III	112	Cávado				404664
City Hall	1120301	Amares	Braga	Coastal	Small	18182
City Hall	1120302	Barcelos	Braga	Coastal	Large	117683
City Hall	1120303	Braga	Braga	Coastal	Large	181182
City Hall	1120306	Esposende	Braga	Coastal	Medium	33947
City Hall	1120310	Terras de Bouro	Braga	Coastal	Small	6560
City Hall	1120313	Vila Verde	Braga	Coastal	Medium	47110
NUTS III	119	Ave				415671
City Hall	1190304	Cabeceiras de Basto	Braga	Coastal	Small	15959
City Hall	1190307	Fafe	Braga	Coastal	Medium	48906
City Hall	1190308	Guimarães	Braga	Coastal	Large	153995
City Hall	1191705	Mondim de Basto	Vila Real	Interior	Small	7079
City Hall	1190309	Póvoa de Lanhoso	Braga	Coastal	Medium	21521
City Hall	1190311	Vieira do Minho	Braga	Coastal	Small	12134
City Hall	1190312	Vila Nova de Famalicão	Braga	Coastal	Large	132337
City Hall	1190314	Vizela	Braga	Coastal	Medium	23740
NUTS III	11A	Área Metropolitana do Porto				1719021
City Hall	11A0104	Arouca	Aveiro	Coastal	Medium	21211
City Hall	11A0107	Espinho	Aveiro	Coastal	Medium	29560
City Hall	11A1304	Gondomar	Porto	Coastal	Large	165743
City Hall	11A1306	Maia	Porto	Coastal	Large	136011
City Hall	11A1308	Matosinhos	Porto	Coastal	Large	173339
City Hall	11A0113	Oliveira de Azeméis	Aveiro	Coastal	Medium	66496
City Hall	11A1310	Paredes	Porto	Coastal	Medium	86263
City Hall	11A1312	Porto	Porto	Coastal	Large	214119
City Hall	11A1313	Póvoa de Varzim	Porto	Coastal	Medium	62344
City Hall	11A0109	Santa Maria da Feira	Aveiro	Coastal	Large	138867
City Hall	11A1314	Santo Tirso	Porto	Coastal	Medium	68983
City Hall	11A0116	São João da Madeira	Aveiro	Coastal	Medium	21460
City Hall	11A1318	Trofa	Porto	Coastal	Medium	38210
City Hall	11A0119	Vale de Cambra	Aveiro	Coastal	Medium	21676
City Hall	11A1315	Valongo	Porto	Coastal	Medium	95411
City Hall	11A1316	Vila do Conde	Porto	Coastal	Medium	79327
City Hall	11A1317	Vila Nova de Gaia	Porto	Coastal	Large	300001
NUTS III	11B	Alto Tâmega				87941
City Hall	11B1702	Boticas	Vila Real	Interior	Small	5217
City Hall	11B1703	Chaves	Vila Real	Interior	Medium	39682
City Hall	11B1706	Montalegre	Vila Real	Interior	Small	9337

NUTS	Code	Name	District	ICI Zone	Dimension	Population (2016)
City Hall	11B1709	Ribeira de Pena	Vila Real	Interior	Small	6144
City Hall	11B1712	Valpaços	Vila Real	Interior	Small	15336
City Hall	11B1713	Vila Pouca de Aguiar	Vila Real	Interior	Small	12225
NUTS III	11C	Tâmega e Sousa				420854
City Hall	11C1301	Amarante	Porto	Coastal	Medium	53947
City Hall	11C1302	Baião	Porto	Coastal	Small	19255
City Hall	11C0106	Castelo de Paiva	Aveiro	Coastal	Small	15797
City Hall	11C0305	Celorico de Basto	Braga	Coastal	Small	19341
City Hall	11C1804	Cinfães	Viseu	Interior	Small	18897
City Hall	11C1303	Felgueiras	Porto	Coastal	Medium	56950
City Hall	11C1305	Lousada	Porto	Coastal	Medium	46900
City Hall	11C1307	Marco de Canaveses	Porto	Coastal	Medium	52110
City Hall	11C1309	Paços de Ferreira	Porto	Coastal	Medium	56838
City Hall	11C1311	Penafiel	Porto	Coastal	Medium	70333
City Hall	11C1813	Resende	Viseu	Interior	Small	10486
NUTS III	11D	Douro				193202
City Hall	11D1701	Alijó	Vila Real	Interior	Small	10933
City Hall	11D1801	Armamar	Viseu	Interior	Small	5876
City Hall	11D0403	Carrazeda de Ansiães	Bragança	Interior	Small	5795
City Hall	11D0404	Freixo de Espada à Cinta	Bragança	Interior	Small	3409
City Hall	11D1805	Lamego	Viseu	Interior	Medium	25219
City Hall	11D1704	Mesão Frio	Vila Real	Interior	Small	4058
City Hall	11D1807	Moimenta da Beira	Viseu	Interior	Small	9778
City Hall	11D1707	Murça	Vila Real	Interior	Small	5558
City Hall	11D1812	Penedono	Viseu	Interior	Small	2683
City Hall	11D1708	Peso da Régua	Vila Real	Interior	Small	16037
City Hall	11D1710	Sabrosa	Vila Real	Interior	Small	5956
City Hall	11D1711	Santa Marta de Penaguião	Vila Real	Interior	Small	6763
City Hall	11D1815	São João da Pesqueira	Viseu	Interior	Small	7269
City Hall	11D1818	Sernancelhe	Viseu	Interior	Small	5437
City Hall	11D1819	Tabuaço	Viseu	Interior	Small	6081
City Hall	11D1820	Tarouca	Viseu	Interior	Small	7752
City Hall	11D0409	Torre de Moncorvo	Bragança	Interior	Small	7853
City Hall	11D0914	Vila Nova de Foz Côa	Guarda	Interior	Small	6673
City Hall	11D1714	Vila Real	Vila Real	Interior	Medium	50072
NUTS III	11E	Terras de Trás-os-Montes				109409
City Hall	11E0401	Alfândega da Fé	Bragança	Interior	Small	4630
City Hall	11E0402	Bragança	Bragança	Interior	Medium	33766
City Hall	11E0405	Macedo de Cavaleiros	Bragança	Interior	Small	14722
City Hall	11E0406	Miranda do Douro	Bragança	Interior	Small	7029
City Hall	11E0407	Mirandela	Bragança	Interior	Medium	22141
City Hall	11E0408	Mogadouro	Bragança	Interior	Small	8674
City Hall	11E0410	Vila Flor	Bragança	Interior	Small	6170
City Hall	11E0411	Vimioso	Bragança	Interior	Small	4173
City Hall	11E0412	Vinhais	Bragança	Interior	Small	8104
NUTS II	16	Centro				2243934
NUTS III	16B	Oeste				358029
City Hall	16B1001	Alcobaça	Leiria	Coastal	Medium	54628
City Hall	16B1101	Alenquer	Lisboa	Coastal	Medium	43287
City Hall	16B1102	Arruda dos Vinhos	Lisboa	Coastal	Small	14703
City Hall	16B1005	Bombarral	Leiria	Coastal	Small	12603
City Hall	16B1104	Cadaval	Lisboa	Coastal	Small	13783
City Hall	16B1006	Caldas da Rainha	Leiria	Coastal	Medium	51557
City Hall	16B1108	Lourinhã	Lisboa	Coastal	Medium	25619
City Hall	16B1011	Nazaré	Leiria	Coastal	Small	14350
City Hall	16B1012	Óbidos	Leiria	Coastal	Small	11656

NUTS	Code	Name	District	ICI Zone	Dimension	Population (2016)
City Hall	16B1014	Peniche	Leiria	Coastal	Medium	26848
City Hall	16B1112	Sobral de Monte Agraço	Lisboa	Coastal	Small	10295
City Hall	16B1113	Torres Vedras	Lisboa	Coastal	Medium	78700
NUTS III	16D	Região de Aveiro				363752
City Hall	16D0101	Águeda	Aveiro	Coastal	Medium	46600
City Hall	16D0102	Albergaria-a-Velha	Aveiro	Coastal	Medium	24348
City Hall	16D0103	Anadia	Aveiro	Coastal	Medium	27805
City Hall	16D0105	Aveiro	Aveiro	Coastal	Medium	77241
City Hall	16D0108	Estarreja	Aveiro	Coastal	Medium	26242
City Hall	16D0110	Ílhavo	Aveiro	Coastal	Medium	38406
City Hall	16D0112	Murtosa	Aveiro	Coastal	Small	10341
City Hall	16D0114	Oliveira do Bairro	Aveiro	Coastal	Medium	23746
City Hall	16D0115	Ovar	Aveiro	Coastal	Medium	54481
City Hall	16D0117	Sever do Vouga	Aveiro	Coastal	Small	11702
City Hall	16D0118	Vagos	Aveiro	Coastal	Medium	22840
NUTS III	16E	Região de Coimbra				439507
City Hall	16E0601	Arganil	Coimbra	Coastal	Small	11317
City Hall	16E0602	Cantanhede	Coimbra	Coastal	Medium	35606
City Hall	16E0603	Coimbra	Coimbra	Coastal	Large	134348
City Hall	16E0604	Condeixa-a-Nova	Coimbra	Coastal	Small	17473
City Hall	16E0605	Figueira da Foz	Coimbra	Coastal	Medium	59956
City Hall	16E0606	Góis	Coimbra	Coastal	Small	3936
City Hall	16E0607	Lousã	Coimbra	Coastal	Small	17201
City Hall	16E0111	Mealhada	Aveiro	Coastal	Medium	20095
City Hall	16E0608	Mira	Coimbra	Coastal	Small	12017
City Hall	16E0609	Miranda do Corvo	Coimbra	Coastal	Small	12845
City Hall	16E0610	Montemor-o-Velho	Coimbra	Coastal	Small	25570
City Hall	16E1808	Mortágua	Viseu	Interior	Small	9075
City Hall	16E0611	Oliveira do Hospital	Coimbra	Coastal	Small	19767
City Hall	16E0612	Pampilhosa da Serra	Coimbra	Coastal	Small	4112
City Hall	16E0613	Penacova	Coimbra	Coastal	Small	14200
City Hall	16E0614	Penela	Coimbra	Coastal	Small	5556
City Hall	16E0615	Soure	Coimbra	Coastal	Small	17799
City Hall	16E0616	Tábua	Coimbra	Coastal	Small	11623
City Hall	16E0617	Vila Nova de Poiares	Coimbra	Coastal	Small	7011
NUTS III	16F	Região de Leiria				287770
City Hall	16F1002	Alvaiázere	Leiria	Coastal	Small	6789
City Hall	16F1003	Ansião	Leiria	Coastal	Small	12449
City Hall	16F1004	Batalha	Leiria	Coastal	Small	15835
City Hall	16F1007	Castanheira de Pêra	Leiria	Coastal	Small	2736
City Hall	16F1008	Figueiró dos Vinhos	Leiria	Coastal	Small	5757
City Hall	16F1009	Leiria	Leiria	Coastal	Large	125523
City Hall	16F1010	Marinha Grande	Leiria	Coastal	Medium	38561
City Hall	16F1013	Pedrógão Grande	Leiria	Coastal	Small	3516
City Hall	16F1015	Pombal	Leiria	Coastal	Medium	52971
City Hall	16F1016	Porto de Mós	Leiria	Coastal	Medium	23633
NUTS III	16G	Viseu Dão Lafões				256928
City Hall	16G0901	Aguiar da Beira	Guarda	Interior	Small	4934
City Hall	16G1802	Carregal do Sal	Viseu	Interior	Small	9472
City Hall	16G1803	Castro Daire	Viseu	Interior	Small	14344
City Hall	16G1806	Mangualde	Viseu	Interior	Small	19048
City Hall	16G1809	Nelas	Viseu	Interior	Small	13354
City Hall	16G1810	Oliveira de Frades	Viseu	Interior	Small	9999
City Hall	16G1811	Penalva do Castelo	Viseu	Interior	Small	7387
City Hall	16G1814	Santa Comba Dão	Viseu	Interior	Small	10756
City Hall	16G1816	São Pedro do Sul	Viseu	Interior	Small	15875

NUTS	Code	Name	District	ICI Zone	Dimension	Population (2016)
City Hall	16G1817	Sátão	Viseu	Interior	Small	11835
City Hall	16G1821	Tondela	Viseu	Interior	Medium	27315
City Hall	16G1822	Vila Nova de Paiva	Viseu	Interior	Small	4833
City Hall	16G1823	Viseu	Viseu	Interior	Medium	97849
City Hall	16G1824	Vouzela	Viseu	Interior	Small	9927
NUTS III	16H	Beira Baixa				82731
City Hall	16H0502	Castelo Branco	Castelo Branco	Interior	Medium	53127
City Hall	16H0505	Idanha-a-Nova	Castelo Branco	Interior	Small	8540
City Hall	16H0506	Oleiros	Castelo Branco	Interior	Small	5197
City Hall	16H0507	Penamacor	Castelo Branco	Interior	Small	5005
City Hall	16H0508	Proença-a-Nova	Castelo Branco	Interior	Small	7623
City Hall	16H0511	Vila Velha de Ródão	Castelo Branco	Interior	Small	3239
NUTS III	16I	Médio Tejo				236256
City Hall	16I1401	Abrantes	Santarém	Interior	Medium	36284
City Hall	16I1402	Alcanena	Santarém	Interior	Small	13063
City Hall	16I1408	Constância	Santarém	Interior	Small	3990
City Hall	16I1410	Entroncamento	Santarém	Interior	Medium	20797
City Hall	16I1411	Ferreira do Zêzere	Santarém	Interior	Small	8126
City Hall	16I1413	Mação	Santarém	Interior	Small	6586
City Hall	16I1421	Ourém	Santarém	Interior	Medium	44751
City Hall	16I1417	Sardoal	Santarém	Interior	Small	3792
City Hall	16I0509	Sertã	Castelo Branco	Interior	Small	14983
City Hall	16I1418	Tomar	Santarém	Interior	Medium	37795
City Hall	16I1419	Torres Novas	Santarém	Interior	Medium	35420
City Hall	16I0510	Vila de Rei	Castelo Branco	Interior	Small	3355
City Hall	16I1420	Vila Nova da Barquinha	Santarém	Interior	Small	7314
NUTS III	16J	Beiras e Serra da Estrela				218961
City Hall	16J0902	Almeida	Guarda	Interior	Small	6203
City Hall	16J0501	Belmonte	Castelo Branco	Interior	Small	6506
City Hall	16J0903	Celorico da Beira	Guarda	Interior	Small	7167
City Hall	16J0503	Covilhã	Castelo Branco	Interior	Medium	48184
City Hall	16J0904	Figueira de Castelo Rodrigo	Guarda	Interior	Small	5845
City Hall	16J0905	Fornos de Algodres	Guarda	Interior	Small	4720
City Hall	16J0504	Fundão	Castelo Branco	Interior	Medium	27355
City Hall	16J0906	Gouveia	Guarda	Interior	Small	12923
City Hall	16J0907	Guarda	Guarda	Interior	Medium	39858
City Hall	16J0908	Manteigas	Guarda	Interior	Small	3139
City Hall	16J0909	Mêda	Guarda	Interior	Small	4740
City Hall	16J0910	Pinhel	Guarda	Interior	Small	8843
City Hall	16J0911	Sabugal	Guarda	Interior	Small	11242
City Hall	16J0912	Seia	Guarda	Interior	Medium	23027
City Hall	16J0913	Trancoso	Guarda	Interior	Small	9209
NUTS II	17	Área Metropolitana de Lisboa				2821349
NUTS III	170	Área Metropolitana de Lisboa				2821349
City Hall	1701502	Alcochete	Setúbal	Coastal	Small	19020
City Hall	1701503	Almada	Setúbal	Coastal	Large	169330
City Hall	1701115	Amadora	Lisboa	Coastal	Large	178169
City Hall	1701504	Barreiro	Setúbal	Coastal	Medium	75978
City Hall	1701105	Cascais	Lisboa	Coastal	Large	210889
City Hall	1701106	Lisboa	Lisboa	Coastal	Large	504964
City Hall	1701107	Loures	Lisboa	Coastal	Large	207567
City Hall	1701109	Mafra	Lisboa	Coastal	Medium	82581
City Hall	1701506	Moita	Setúbal	Coastal	Medium	64767
City Hall	1701507	Montijo	Setúbal	Coastal	Medium	55742
City Hall	1701116	Odivelas	Lisboa	Coastal	Large	156083
City Hall	1701110	Oeiras	Lisboa	Coastal	Large	174249

NUTS	Code	Name	District	ICI Zone	Dimension	Population (2016)
City Hall	1701508	Palmela	Setúbal	Coastal	Medium	64146
City Hall	1701510	Seixal	Setúbal	Coastal	Large	165123
City Hall	1701511	Sesimbra	Setúbal	Coastal	Medium	50972
City Hall	1701512	Setúbal	Setúbal	Coastal	Large	116979
City Hall	1701111	Sintra	Lisboa	Coastal	Large	383946
City Hall	1701114	Vila Franca de Xira	Lisboa	Coastal	Large	140844
NUTS II	18	Alentejo				718087
NUTS III	181	Alentejo Litoral				94291
City Hall	1811501	Alcácer do Sal	Setúbal	Coastal	Small	12000
City Hall	1811505	Grândola	Setúbal	Coastal	Small	14662
City Hall	1810211	Odemira	Beja	Coastal	Medium	24917
City Hall	1811509	Santiago do Cacém	Setúbal	Coastal	Medium	29047
City Hall	1811513	Sines	Setúbal	Coastal	Small	13665
NUTS III	184	Baixo Alentejo				119024
City Hall	1840201	Aljustrel	Beja	Interior	Small	8493
City Hall	1840202	Almodôvar	Beja	Interior	Small	6888
City Hall	1840203	Alvito	Beja	Interior	Small	2469
City Hall	1840204	Barrancos	Beja	Interior	Small	1687
City Hall	1840205	Beja	Beja	Interior	Medium	34021
City Hall	1840206	Castro Verde	Beja	Interior	Small	7082
City Hall	1840207	Cuba	Beja	Interior	Small	4698
City Hall	1840208	Ferreira do Alentejo	Beja	Interior	Small	7941
City Hall	1840209	Mértola	Beja	Interior	Small	6424
City Hall	1840210	Moura	Beja	Interior	Small	14080
City Hall	1840212	Ourique	Beja	Interior	Small	4825
City Hall	1840213	Serpa	Beja	Interior	Small	14809
City Hall	1840214	Vidigueira	Beja	Interior	Small	5607
NUTS III	185	Lezíria do Tejo				239977
City Hall	1851403	Almeirim	Santarém	Interior	Medium	22912
City Hall	1851404	Alpiarça	Santarém	Interior	Small	7209
City Hall	1851103	Azambuja	Lisboa	Coastal	Medium	22258
City Hall	1851405	Benavente	Santarém	Interior	Medium	29965
City Hall	1851406	Cartaxo	Santarém	Interior	Medium	23939
City Hall	1851407	Chamusca	Santarém	Interior	Small	9510
City Hall	1851409	Coruche	Santarém	Interior	Small	18272
City Hall	1851412	Golegã	Santarém	Interior	Small	5508
City Hall	1851414	Rio Maior	Santarém	Interior	Medium	20582
City Hall	1851415	Salvaterra de Magos	Santarém	Interior	Medium	21567
City Hall	1851416	Santarém	Santarém	Interior	Medium	58255
NUTS III	186	Alto Alentejo				108588
City Hall	1861201	Alter do Chão	Portalegre	Interior	Small	3263
City Hall	1861202	Arronches	Portalegre	Interior	Small	2952
City Hall	1861203	Avis	Portalegre	Interior	Small	4338
City Hall	1861204	Campo Maior	Portalegre	Interior	Small	8115
City Hall	1861205	Castelo de Vide	Portalegre	Interior	Small	3058
City Hall	1861206	Crato	Portalegre	Interior	Small	3300
City Hall	1861207	Elvas	Portalegre	Interior	Medium	21270
City Hall	1861208	Fronteira	Portalegre	Interior	Small	3059
City Hall	1861209	Gavião	Portalegre	Interior	Small	3533
City Hall	1861210	Marvão	Portalegre	Interior	Small	3173
City Hall	1861211	Monforte	Portalegre	Interior	Small	3064
City Hall	1861212	Nisa	Portalegre	Interior	Small	6446
City Hall	1861213	Ponte de Sor	Portalegre	Interior	Small	15489
City Hall	1861214	Portalegre	Portalegre	Interior	Medium	22922
City Hall	1861215	Sousel	Portalegre	Interior	Small	4606
NUTS III	187	Alentejo Central				156207

NUTS	Code	Name	District	ICI Zone	Dimension	Population (2016)
City Hall	1870701	Alandroal	Évora	Interior	Small	5271
City Hall	1870702	Arraiolos	Évora	Interior	Small	7057
City Hall	1870703	Borba	Évora	Interior	Small	6950
City Hall	1870704	Estremoz	Évora	Interior	Small	13156
City Hall	1870705	Évora	Évora	Interior	Medium	53294
City Hall	1870706	Montemor-o-Novo	Évora	Interior	Small	16129
City Hall	1870707	Mora	Évora	Interior	Small	4382
City Hall	1870708	Mourão	Évora	Interior	Small	2511
City Hall	1870709	Portel	Évora	Interior	Small	6016
City Hall	1870710	Redondo	Évora	Interior	Small	6567
City Hall	1870711	Reguengos de Monsaraz	Évora	Interior	Small	10254
City Hall	1870712	Vendas Novas	Évora	Interior	Small	11463
City Hall	1870713	Viana do Alentejo	Évora	Interior	Small	5263
City Hall	1870714	Vila Viçosa	Évora	Interior	Small	7894
NUTS II	15	Algarve				441469
NUTS III	150	Algarve				441469
City Hall	1500801	Albufeira	Faro	Coastal	Medium	40633
City Hall	1500802	Alcoutim	Faro	Coastal	Small	2403
City Hall	1500803	Aljezur	Faro	Coastal	Small	5609
City Hall	1500804	Castro Marim	Faro	Coastal	Small	6402
City Hall	1500805	Faro	Faro	Coastal	Medium	61073
City Hall	1500806	Lagoa	Faro	Coastal	Medium	22799
City Hall	1500807	Lagos	Faro	Coastal	Medium	30714
City Hall	1500808	Loulé	Faro	Coastal	Medium	69344
City Hall	1500809	Monchique	Faro	Coastal	Small	5386
City Hall	1500810	Olhão	Faro	Coastal	Medium	45143
City Hall	1500811	Portimão	Faro	Coastal	Medium	55453
City Hall	1500812	São Brás de Alportel	Faro	Coastal	Small	10536
City Hall	1500813	Silves	Faro	Coastal	Medium	36476
City Hall	1500814	Tavira	Faro	Coastal	Medium	25263
City Hall	1500815	Vila do Bispo	Faro	Coastal	Small	5192
City Hall	1500816	Vila Real de Santo António	Faro	Coastal	Small	19043
NUTS I	2	Região Autónoma dos Açores				245283
NUTS II	20	Região Autónoma dos Açores				245283
NUTS III	200	Região Autónoma dos Açores				245283
City Hall	2004301	Angra do Heroísmo	Açores	Islands	Medium	34423
City Hall	2004501	Calheta	Açores	Islands	Small	3278
City Hall	2004901	Corvo	Açores	Islands	Small	460
City Hall	2004701	Horta	Açores	Islands	Small	14759
City Hall	2004201	Lagoa	Açores	Islands	Small	14728
City Hall	2004801	Lajes das Flores	Açores	Islands	Small	1494
City Hall	2004601	Lajes do Pico	Açores	Islands	Small	4591
City Hall	2004602	Madalena	Açores	Islands	Small	5948
City Hall	2004202	Nordeste	Açores	Islands	Small	4952
City Hall	2004203	Ponta Delgada	Açores	Islands	Medium	68352
City Hall	2004204	Povoação	Açores	Islands	Small	6080
City Hall	2004205	Ribeira Grande	Açores	Islands	Medium	32770
City Hall	2004401	Santa Cruz da Graciosa	Açores	Islands	Small	4301
City Hall	2004802	Santa Cruz das Flores	Açores	Islands	Small	2198
City Hall	2004603	São Roque do Pico	Açores	Islands	Small	3295
City Hall	2004502	Velas	Açores	Islands	Small	5213
City Hall	2004302	Vila da Praia da Vitória	Açores	Islands	Medium	21532
City Hall	2004101	Vila do Porto	Açores	Islands	Small	5653
City Hall	2004206	Vila Franca do Campo	Açores	Islands	Small	11256
NUTS I	3	Região Autónoma da Madeira				254876
NUTS II	30	Região Autónoma da Madeira				254876

NUTS	Code	Name	District	ICI Zone	Dimension	Population (2016)
NUTS III	300	Região Autónoma da Madeira				254876
City Hall	3003101	Calheta	Madeira	Islands	Small	10946
City Hall	3003102	Câmara de Lobos	Madeira	Islands	Medium	34047
City Hall	3003103	Funchal	Madeira	Islands	Large	104813
City Hall	3003104	Machico	Madeira	Islands	Medium	20453
City Hall	3003105	Ponta do Sol	Madeira	Islands	Small	8557
City Hall	3003106	Porto Moniz	Madeira	Islands	Small	2390
City Hall	3003201	Porto Santo	Madeira	Islands	Small	5162
City Hall	3003107	Ribeira Brava	Madeira	Islands	Small	12446
City Hall	3003108	Santa Cruz	Madeira	Islands	Medium	44026
City Hall	3003109	Santana	Madeira	Islands	Small	6876
City Hall	3003110	São Vicente	Madeira	Islands	Small	5160

Appendix D – Portuguese City Hall Election, Political Parties Results

Table 41 shows the percentage each Political party received according to the number of city halls they won in the 2017 election. The total number of voter for each party is also accounted for.

Table 41 – Portuguese City Hall Election, Political Parties Result

Adapted from: Secretaria Geral Ministério da Administração Interna [2017]

Parties	%	Votes	City Hall Presidents
PS	**37,82**	1.956.618	159
PPD/PSD	**16,07**	831.536	79
PCP-PEV	**9,45**	489.089	24
PPD/PSD.CDS-PP	**8,79**	454.521	16
GRUPO CIDADÃOS	**6,79**	351.352	17
CDS-PP	**2,59**	134.099	6
PPD/PSD.CDS-PP.MPT.PPM	**1,71**	88.541	1
PPD/PSD.CDS-PP.PPM	**1,45**	75.171	2
PS-BE-JPP-PDR-NC	**0,46**	23.577	1
L-PS	**0,32**	16.409	1
JPP	**0,29**	14.818	1
NC	**0,24**	12.499	1

Appendix E – Evolution of e-Governance Initiatives in Portugal

The table presented in this Appendix, Table 42, depicts the evolution of e-governance initiatives in Portugal over the years. As it was previously mentioned in 3.1.1, the term initially used was electronic government. The table displays the creation of agencies, plans and programs; also, the adoption of strategies, the launch of initiatives, and the priorities for that moment in time.

Table 42 – Evolution of e-Governance Initiatives in Portugal

Adapted from: Soares [2009] and Agência para a Modernização Administrativa [2014, 2017].

Year	Initiative
1996	Launch of the **national initiative for Information Society** Creation of the **mission for Information Society**
1997	Publication of the **Green Book for Information Society**
2000	Portugal assumes the presidency of the EU Council ("Innovation" and "Information Society" are defined as a priority) EU adoption of the **Lisbon Strategy** EU adoption of the **eEurope Action Plan** Creation of the Interministerial Commission for Information Society (**CISI**) Adoption of the Operational Program for Information Society (**POSI**)
2002	Creation of the Innovation and Knowledge Mission Unit (**UMIC**)
2003	Publication and approval of the **Plan of Action for Information Society** Publication and approval of the **Plan of Action for Electronic Government** Approval of the **strategic lines for a large-scale reform of the Public Administration**
2004	Presented the initiative "**Futuro 2010 - Programa Operacional para a Sociedade do Conhecimento**" Launch of the "**Portal do Cidadão**" (Citizen's Portal) Presented the government's strategy for the development of information and knowledge "Sociedade da Informação e do Conhecimento 2005-2006"
2005	Establishment of the Agency for Knowledge Society I.P. (**UMIC – IP**), succeeding the previous Innovation and Knowledge Mission Unit (UMIC) Presented the Operational Program for Public Administration 2004-2006 (**POAP**) Introduced the Operational Program for Knowledge Society (**POS_C**) Creation of the Administrative Modernization Coordination Unit (**UCMA**) Launch of the Action Program for Information and Knowledge Society "**LigarPortugal**" Launch of the Restructuring Program for the Central State Administration (**PRACE**) Presented the **Technological Plan**
2006	Launch of the **SIMPLEX** Program
2007	Creation of **AMA** - "Agência para a Modernização Administrativa" (Agency for Administrative Modernization), I.P. **State Secretariat for Administrative Modernization** (**GSEMA**) assumes the responsibility previously held by UCMA Portugal assumes the Presidency of the EU Council ("digital inclusion" is defined as a priority)
2008	Launch of the City Hall SIMPLEX (**SIMPLEX Autárquico**)
2011	Creation of the **State Secretariat for Local Administration and Administrative Reform** Creation of the Plan for the Reduction and Improvement of the Central State Administration (**PREMAC**) Creation of the Project Group for Information and Communication Technologies (**GPTIC**)
2012	Creation of the Strategic Plan for the Rationalization and Reduction of ICT Costs in Public Administration (**PGETIC**)
2014	Launch of the *"**Programa Aproximar**"* Strategy
2016	Launch of **SIMPLEX+ 2016** Constitution of the Council for Information and Communication Technologies in Public Administration (**CTIC**)
2017	Launch of the ICT 2020 Strategy (**Estratégia TIC 2020**)

Appendix F – *Estratégia TIC 2020*

Within this appendix, tables containing the summary of the strategy will be presented. Table 43 presents the three main axels, their twelve measures and their 37 actions. Table 44 presents the governmental areas and its strategic projects. Table 45 shows the sectorial plan for the governmental areas, the general activities for each of the governance actions from measure 01 of the first axel. Worth mentioning that the second and third tables, are written in Portuguese, because an official translated version could not be found.

Table 43 – Estratégia TIC 2020 Axels, Measures and Actions

Source: Agência para a Modernização Administrativa [2018a]

Axel	Measure	Action
Integration and Interoperability	M01 - Governance	Define and implement a cross-sectional governance model for the ICT
		Consolidate the ICT governance model for each governmental area
	M02 – Sectorial Action Plans	Approve and publish ICT sectorial plans per governmental area, aligned with strategy, allocations and sectorial competences
		Elaborate annual project and ICT investment plans
	M03 – Interoperability	Provide an electronic service catalogue
		Extend interoperability to document management solutions
		Mass use the interoperability platform (iAP) for administrative simplification and modernization initiatives
	M04 – Common ICT architectures	Define and implement common ICT architectures
		Optimize ICT investments
		Define and implement a national information security strategy
Innovation and Competitiveness	M05 – Electronic ID	Develop and provide a Citizen Card with new features
		Allow a single authentication of citizens in Public Administration (PA) sites and systems
		Provide the SCAP - *Sistema de Certificação de Atributos Profissionais* (Professional Competences Certification System) for signing and authentication
	M06 – Transparency and participation	Extend the open data disclosure and use via dados.gov.pt
		Disclose execution indicators and benefits accomplished by executing PA policies, initiatives and projects
		Provide instruments that facilitate the participation of citizen in public decision processes
	M07 – Electronic services	Integrate user experience in service processes
		Define common standards and models for the uniformization of the graphics and usability of electronic services
		Consolidate electronic services in *Portal do Cidadão*
		Provide information in the *Portal do Cidadão*, depending on citizen location
		Provide citizen document exchange
		Automate PA service provision and response to life events
		Adopt virtual workstations, by incorporating the Bring Your Own Device (BYOD) concept
		Drive the adoption of mobile ways of work and work from home in the PA
		Implement Wi-Fi roaming in the PA – GOVroam
		Scan the PA's physical archive
	M08 – Sectorial innovation	Develop sectorial actions to improve provided service quality and/or PA internal effectiveness by using the ICT
Resource Sharing	M09 – ICT centre of competence	Define the operation model and drive the development of an ICT centre of competences
		Promote the development of Digital Competences
	M10 – Datacenter & cloud	Capitalize and concentrate computation capacity in data processing centres
		Create an interoperable cloud
	M11 – Communications	Rationalize voice and data communications
		Implement a common multi-service communications network
		Define and implement unified communication strategies
	M12 – Common and open source APPs	Globally manage State software cross-sectional licensing needs (including creation, reuse and negotiation)
		Promote and disseminate open source software (OSS)
		Create and promote the PA software catalogue

Table 44 – Governamental Areas and their Strategic Projects

Source: Agência para a Modernização Administrativa [2017]

Governmental Area	Strategic Projects
Negócios Estrangeiros	Camões + Serviços no mundo
	Gestor documental e plano de classificação documental do MNE
	Apoio ao investidor
	Plataforma de Interoperabilidade e Comunicações do MNE
Presidência e modernização administrativa	Serviço de notificações eletrónicas
	Bolsa de documentos
	Pontos únicos de contacto (Portal do Cidadão e Plataformas de Licenciamento)
	Sistema interoperável de gestão documental
	Livro amarelo eletrónico
Finanças	IRS automático
	PAEP – Desenvolvimento e implementação da Plataforma da Administração e do Emprego Público
	PLAFIO – Planeamento financeiro e orçamentação e ECE- Entidade Contabilística Estado responsabilidade da UNILEO
	Centralização da rede de comunicações do MF (Voz e Dados)
	Cloud AP - Piloto da nuvem interoperável da AP
Defesa Nacional	Federação de service desk das entidades da defesa
	Federação de identidades
	Apoio à tomada de decisão
	Portal das instituições da memória da defesa nacional
	Capitania online
Administração interna	GeoMAI
	Georreferenciação de meios MAI
	Segurança informática da Rede Nacional de Segurança Interna (RNSI)
	Gestão do atendimento ao cidadão na PSP e GNR
	Atualização do Sistema Integrado de Informações Operacionais de Polícia (SIIOP) da GNR.
Justiça	Tribunal+
	BUPi, balcão único do prédio
	Transcrição automática
	Plataforma de Transparência da Justiça
	Serviços Comuns do Ministério da Justiça
Autarquias locais, igualdade e imigração	SIIAL - Sistema Integrado de Informação das Autarquias Locais
	App Apoio contra a violência doméstica
	My CNAI - Centros Nacionais de Apoio ao Imigrante
	App immigrant welcome
	Portugal Concilia
Cultura	Portal da cultura
	Portuguese news hub
Ciência, tecnologia e Ensino superior	Mais ciência menos burocracia
	Responsabilidade cultural e patrimonial
	Plataforma de gestão de concursos da Fundação para a Ciência e Tecnologia (AGIL)
	Plataforma de suporte à gestão, produção e acesso a informação sobre a atividade científica nacional (PTCRIS)
Educação	Escola 360
	Plataforma digital da educação
	Sistema integrado de gestão do recrutamento do pessoal docente e não docente
	Big data para gestão financeira
	Portal e passaporte qualifica
Trabalho, solidariedade e segurança social	Plataforma da segurança social;
	Plataforma de serviços base
	Solução de relacionamento
	Big data e combate à fraude
	Plataforma de gestão documental do MTSSS

Saúde	Catálogo de serviços TIC
	Portefólio e orçamento TIC
	Interoperabilidade na saúde
	Competências TIC saúde
	Racionalização dos centros de dados
Planeamento e infraestruturas	Sistema de Informação Portugal 2020
	Evolução da Plataforma de Gestão Integrada das Infraestruturas de Portugal (PGI)
	Ferramenta de gestão documental
	Sistema integrado de gestão de condutores, veículos e transportes (SIGCTV)
	Portal base
Economia	Livro de reclamações online
	Portal do turismo +
	Gestão dos sistemas de incentivos
	Balcão do empreendedor +
	Geoportal2020
Ambiente	Título único ambiental (TUA)
	Planeamento territorial online + REN digital
	iFAMA, Plataforma única de inspeção e fiscalização da agricultura, mar e ambiente
	Plataforma da renda apoiada
	Sistemas de gestão documental
Agricultura, florestas e Desenvolvimento rural	Cloud Agricultura, Florestas e Desenvolvimento Rural e Mar
	Desktop as a Service - DaaS
	Rede única de comunicações fixas MAFDR
	Sistema para gestão documental e tramitação processual da Agricultura, Florestas e Desenvolvimento Rural e Mar (SGDPi)
	Interoperabilidade Agricultura, Florestas e Desenvolvimento Rural e Mar
Mar	JUL – Janela Única Logística
	VTS+ Sistema de Controlo de Tráfego Marítimo modernizado
	Balcão Único da Administração Marítima, Pescas e Ordenamento
	PSOEM – Plano de Situação do Ordenamento do Espaço Marítimo Nacional
	Licenças, Títulos e Certificados eletrónicos para as atividades marítimas

Table 45 – Activities for Measure 01 for each Governmental Area

Source: Agência para a Modernização Administrativa [2017]

Governmental Area	**Axel - Integration and Interoperability** **Measure - M01 - Governance** **Action:**	
	Define and implement a cross-sectional governance model for the ICT	**Consolidate the ICT governance model for each governmental area**
Negócios Estrangeiros	–	Propor e implementar Modelo para a Racionalização da Função TIC na AP Central
Presidência e modernização administrativa	Definição e Implementação de Governação transversal das TIC na AP	Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP) Propor e implementar Modelo para a Racionalização da Função TIC na AP Central Publicar catálogos de serviços, pricing e níveis de serviço das áreas governamentais
Finanças	–	Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP) Propor e implementar Modelo para a Racionalização da Função TIC na AP Central Publicar catálogos de serviços, pricing e níveis de serviço das áreas governamentais
Defesa Nacional	–	Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP) Propor e implementar Modelo para a Racionalização da Função TIC na AP Central
Administração interna	Definição e Implementação de Governação transversal das TIC na AP	Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP)
Justiça	Definição e Implementação de Governação transversal das TIC na AP	Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP) Propor e implementar Modelo para a Racionalização da Função TIC na AP Central Publicar catálogos de serviços, pricing e níveis de serviço das áreas governamentais
Autarquias locais, igualdade e imigração	Definição e Implementação de Governação transversal das TIC na AP Constituir o Grupo de Projeto para as TIC na AP Local e elaborar o Plano Estratégico para as TIC na AP Local	Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP) Propor e implementar Modelo para a Racionalização da Função TIC na AP Central Publicar catálogos de serviços, pricing e níveis de serviço das áreas governamentais
Cultura	–	–
Ciência, tecnologia e Ensino superior	–	Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP) Propor e implementar Modelo para a Racionalização da Função TIC na AP Central Publicar catálogos de serviços, pricing e níveis de serviço das áreas governamentais
Educação	–	Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP) Propor e implementar Modelo para a Racionalização da Função TIC na AP Central Publicar catálogos de serviços, pricing e níveis de serviço das áreas governamentais

Governmental Area	Axel - Integration and Interoperability Measure - M01 - Governance Action:	
	Define and implement a cross-sectional governance model for the ICT	Consolidate the ICT governance model for each governmental area
Trabalho, solidariedade e segurança social	–	Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP) Publicar catálogos de serviços, pricing e níveis de serviço das áreas governamentais
Saúde	Definição e Implementação de Governação transversal das TIC na AP	Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP) Propor e implementar Modelo para a Racionalização da Função TIC na AP Central Publicar catálogos de serviços, pricing e níveis de serviço das áreas governamentais
Planeamento e infraestruturas	–	Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP)
Economia	–	Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP) Propor e implementar Modelo para a Racionalização da Função TIC na AP Central Publicar catálogos de serviços, pricing e níveis de serviço das áreas governamentais
Ambiente	–	–
Agricultura, florestas e Desenvolvimento rural	–	Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP) Propor e implementar Modelo para a Racionalização da Função TIC na AP Central
Mar	–	Governação das TIC ao nível ministerial e intraministerial (identificação dos CIO da AP) Propor e implementar Modelo para a Racionalização da Função TIC na AP Central

Appendix G – Artifact Construction: Instantiations of Relevant ISSG Documents

This Appendix contains the summary tables for the relevant documents (COBIT® 2019, NIST SP 800-100, ISO/IEC 27014, GTAG® 15 and Veiga & Eloff ISG framework) ISSG that were discussed in 2.2.3.2 and is divided by categories. These summary tables (Table 46, Table 47, Table 48, Table 49 and Table 50) are distributed as Document overview; Governance definition; Objectives; Dimensions; Attributes; Metrics and Analysis.

Table 46 – COBIT® 2019 Summary Table

Document:	COBIT® 2019
Document Overview	COBIT is described as "a framework for the governance and management of enterprise information and technology, aimed at the whole enterprise"[ISACA 2018c, p. 13]. Comprised of four publications (Introduction and Methodology; Governance and Management Objectives; Designing an Information and Technology Governance Solution; and Implementing and Optimizing an Information Technology Governance Solution) that provides a foundation to create a customized governance program for Information and Technology (I&T), that is the right-size for the needs of the enterprise.
Governance Definition	The document describes the governance discipline as: "ensures that the stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives" [ISACA 2018d, p. 15].
Objectives	To make a clear distinction between governance and management Types of activities Organizational structure Purpose
Dimensions	1. COBIT Principles 2. Governance System and Components 3. Governance and Management Objectives 4. Performance Management 5. Design and Tailored Governance System 6. Implement Enterprise Governance of I&T
Attributes	1.1 Governance System Principles Provide Stakeholder value Holistic Approach Dynamic Governance System Governance Distinct from Management Tailored to Enterprise Needs End to End Governance System 1.2 Governance Framework Principles Based on a Conceptual Model Open and Flexible Aligned to Major Standards 2.1 Governance and Management Objectives (EDM Processes) 2.2 Components of a Governance System Processes Organizational Structure Principles, Policies and Frameworks Information Culture, Ethics and Behavior People, Skills and Competences Services, Infrastructure application 2.3 Focus Areas 2.4 Design Factors Enterprise Strategy Enterprise Goals Risk Profile I&T-Related Issues Threat Landscape Compliance Requirements Role of IT Sourcing Model of IT IT Implementation Methods Technology Adoption Strategy Enterprise Size Future Factors 2.5 Goals Cascade 3.1 EDM01 – Ensure governance framework setting and maintenance 3.2 EDM02 – Ensure benefits delivery 3.3 EDM03 – Ensure risk optimization 3.4 EDM04 – Ensure resource optimization 3.5 EDM05 – Ensure stakeholder engagement 4.1 Principles Simple to understand and to use Consistent and support the COBIT Conceptual Model Provide reliable, repeatable and relevant results

	Flexible Support different types of assessment 4.2 Process Capability Levels Rating Process Activities 4.3 Focus Area Maturity Level 4.4 Manage Performance of Other Governance System Components Organizational structures Information Items Culture and Behavior 5.1 Impact of Design Factors Management objectives priority/selection Component variation Need for specific focus area 5.2 Stages and Steps in the Design Process Understand the enterprise context and strategy Determine the initial scope of governance system Refine the scope of governance system Conclude the governance system design 6.1 COBIT Implementation Guide Purpose 6.2 COBIT Implementation Approach What are the drivers Where are we now Where do we want to be What needs to be done How do we get there Did we get there How do we keep the momentum going
Metrics	COBIT Performance Management (CPM) model Principles Simple to understand and to use Consistent and support the COBIT Conceptual Model Provide reliable, repeatable and relevant results Flexible Support different types of assessment Manage Performance of Processes Process Capability Levels Rating Process Activities Focus Area Maturity Level Manage Performance of Other Governance System Components Organizational structures Information Items Culture and Behavior
Analysis	CPM used to: analyze how they can improve achieve the required level for processes and other components COBIT Implementation Approach (continual improvement) phases: What are the drivers Where are we now Where do we want to be What needs to be done How do we get there Did we get there How do we keep the momentum going

Table 47 – NIST SP 800-100 Summary Table

Document:	**NIST Special Publication 800-100 – Information Security Governance**
Document Overview	The document was created by the American Federal Government to manage and govern the Information Security. Designed to direct managers so they can establish and implement ISG in their organizations.
Governance Definition	ISG is defined in this document as: “the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk” [Bowen et al. 2006, p. 2].
Objectives	Ensure agencies are proactively implementing appropriate information security controls to support their mission at a cost-effective manner, while managing evolving risks. Ensure appropriate level of support of agency’s mission. Properly implement current and future information security requirements. Establish in each agency a formal ISG structure.
Dimensions	1. Requirements 2. Components 3. Challenges and Keys to Success.
Attributes	1.1 U.S. Congress 1.2 Office of Management and Budget (OMB) 1.3 Government Accountability Office (GAO) 1.4 Agencies 1.5 Key Legislative Acts and Documents 2.1 Strategic Planning 2.2 Organizational Structure 2.3 Roles and Responsibilities 2.4 Enterprise Architecture 2.5 Policies and Guidance 2.6 Ongoing Monitoring 3.1 Balancing requirements 3.2 Balancing laws and regulations 3.3 Maintaining currency 3.4 Prioritize funding
Metrics	Performance Reference Model (PRM) Plans of Actions and Milestones (POAM) Performance measurements and metrics Incident statistics
Analysis	Periodic assessments and reports Annual report on the effectiveness of agency’s information security program Refreshed strategic plan every three years Information security performance measures reported to FISMA (quarterly and annually) Incident and events statistics Network Monitoring Continuous assessment Configuration management and control

Table 48 – ISO/IEC 27014 Summary Table

Document:	**ISO/IEC 27014:2013 - Information Technology – Security techniques – Governance of Information Security**
Document Overview	This document is an International Standard that provides guidance on Information Security Governance; and is applicable to all types and sizes of organizations. This version of the document was created in 2013 by a joint technical comitee of ISO and IEC participants, that meets every 4 years.
Governance Definition	The document describes ISG as "system by which an organisation's information security activities are directed and controlled" [ISO/IEC 2013, p. 1].
Objectives	Strategic aligment Align the information security objectives and strategy with business objectives and strategy Value delivery Deliver value to the governing body and to stakeholders Accountability Ensure that information risk is being adequately addressed
Dimensions	1. Roles and Responsibilities (Definition) 2. Principles 3. Processes
Attributes	1.1 Governing body 1.2 Executive management 1.3 Stakeholders 2.1 Organization-wide information security 2.2 Risk-based approach 2.3 Direction of investiment decisions 2.4 Conformance of internal and external requirements 2.5 Security-positive environment 2.6 Review performance of business outcomes 3.1 Evaluate 3.2 Direct 3.3 Monitor 3.4 Communicate 3.5 Assure
Metrics	The executive manager selects the appropriate (from a business perspective) performance metrics in the Monitor process
Analysis	The governing body performs mandated reviews of a performance measurement program. Also, in the Assure process, the governing body also commissions independent and objective security audits

Table 49 – GTAG 15 Summary Table

Document:	GTAG 15 – Auditing Information Security Governance
Document Overview	The document consists of a practice guide which provides detailed guidance for conducting internal audit activities. A thought process to determine what matters to the organization and to assist the Chief Audit Executive(CAE) incorporate into the audit plan an audit of ISG, are some of the document's approaches. The audit plan will focus on the organization's ISG activities and if those activities delivers correct behaviors, practices and IS execution.
Governance Definition	The document doesn't define ISG, since it states that multiple definitions can be found across organization and standard setting bodies [Love et al. 2010, p. 1]. Although it presents three common themes: Promote good IS practices with clear direction and understanding at all levels. Controlling IS risks associated with business. Create overall IS activity that reflects organization's needs and risk appetite levels.
Objectives	Define ISG. Help internal auditors understand the right questions to ask and know what documentation is required. Describe the IAA's role in ISG.
Dimensions	1. Information Security Governance 2. Effective Information Security Governance 3. Efficient Information Security Governance 4. Chief Audit Executive (CAE) concerns about ISG 5. Internal Audit Activity (IAA) role in ISG 6. Auditing ISG 7. Samples (questions/topics)
Attributes	1.1 Information Security Roles and Responsibilities Board of Directors Executive Management Staff and Line-of-Business Managers Internal Auditors 2.1 Needs to involve appropriate organizational personnel 2.2 Defines an appropriate framework or methodology to guide its activities 2.3 Uniform IS risk evaluations 2.4 Yield quantifiable and measurable deliverables 2.5 Adapt its priorities based on legal, regulatory, and business changes 2.6 Deploy policies and standards that reflect the organization's risk appetite and are practical, reasonable, and enforceable 3.1 Encorages proportional control 3.2 Observe proportional control in the design of reporting 3.3 Adaptable enough to handle systems that cannot cost-effectively or technically conform to policies and standards 4.1 Regulatory actions 4.2 Reputational damage 4.3 Competitive advantage 4.4 Contractual noncompliance 4.5 Inaccurate or incomplete data 4.6 Fraud 5.1 IAA's responsibilities related to ISG 5.2 Auditor background and experience level 5.3 Audits of ISG Benchmark the ISG activity against independent standards 6.1 Planning Organizational structure Purpose/objectives of each component of the environment Documented communication that occurs among reporting lines Risk appetite Integration of ISG within the organization External influences that could affect ISG structure 6.2 Testing Stakeholder Concerns Reporting and Communication lines Key Performance Indicators (KPI) and their use Alignment of supporting documentation with governance structure Alignment with risk appetite 6.3 Analyzing Accountability Design Effectiveness Information Security Program Effectiveness

	Efficiency Resource Levels Value added Continuous Improvement 7.1 Is the organization's risk appetite well defined and understood? 7.2 Is there a defined, effective information security process? 7.3 Is there effective organizational support for the information security governance activity? 7.4 Does the organization monitor the ongoing health of the information security governance activity? 7.5 Has the organization taken steps to improve its governance over time?
Metrics	Key Performance Indicators (KPIs)
Analysis	Benchmark the ISG activity against independent standards Periodic reviews Multiyear audit plan Reviews of management reporting, approval and documentation of exceptions, consistency of risk assessments, effective use of metrics

Table 50 – Veiga & Eloff Summary Table

Document:	Veiga & Eloff ISG Framework
Document Overview	Created with the intention to serve as a starting point for ISG. Derived from an analysis of four existing ISG approaches, to create a new more comprehensive ISG framework.
Governance Definition	The document describes ISG as: "the overall manner in which information security is deployed to mitigate risks" [Veiga and Eloff 2007, p. 362].
Objectives	Evaluate the four current approaches of ISG frameworks to construct a new comprehensive ISG framework, that considers the technical, procedural and behavioral components To provide an all-encompassing (single point of reference) for ISG.
Dimensions	1. Information Security Phases 2. ISG framework – existing approaches 3. New approach to ISG framework Technical components Procedural components Human Behavioral components
Attributes	1.1 Information Security phase I Securing IT environment 1.2 Information Security phase II Information security incorporated to organizational structure 1.3 Information Security phase III Information security incorporated to everyday practices performed by employees (information security culture) 1.4 Information Security phase IV Development and role of ISG (risk prevention was a key driver) 2.1 ISO 177995 & 27001 2.2 PROTECT 2.3 Capability Maturity Model 2.4 Information Security Architecture (ISA) 3.1 Leadership and governance 3.2 Security Management and Organization 3.3 Security Policies 3.4 Security Program Management 3.5 User Security Management 3.6 Technology Protection and Operations
Metrics	Number of security incidents Empirical results of awareness surveys
Analysis	Risk assessments

Appendix H – COBIT 5 Summary

In Table 51, a summary of the outdated version of COBIT, version 5, is presented. This table was used in the creation of the concept tree versions 1 to 5.

Table 51 – COBIT 5 Summary Table

Document:	COBIT 5
Document Overview	The document is a part of a large product family and consists of a framework designed for governing and managing the enterprise IT. The framework is built upon five principles, with an extensive guidance on the enablers for governance and management of enterprise IT.
Governance Definition	The document describes the governance discipline as: "ensures that the stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives" [ISACA 2012b, p. 14].
Objectives	To make a clear distinction between governance and management Types of activities Organizational structure Purpose
Dimensions	1. Governance and Management 2. Interactions between governance and management Enabler structure 3. COBIT 5 Process Reference Model
Attributes	1.1 Governance role definition and responsibility Evaluate Direct Monitor Board of directors 1.2 Management definition and responsibility 2.1 Processes 2.2 Information 2.3 Organisational structures 2.4 Principles, policies and frameworks 2.5 Culture, ethics and behaviour 2.6 People, skills and competencies 2.7 Services, infrastructure and applications 3.1 EDM01 – Ensure governance framework setting and maintenance 3.2 EDM02 – Ensure benefits delivery 3.3 EDM03 – Ensure risk optimisation 3.4 EDM04 – Ensure resource optimisation 3.5 EDM05 – Ensure stakeholder transparency
Metrics	COBIT 5 Process Capability Model (a mean to measure the performance of any of the governance processes)
Analysis	COBIT 5 Process Capability Model (will allow areas for improvement to be identified)

Appendix I – Artifact Construction: Concept Tree versions

In this Appendix, the evolution and refinement of the concept tree are exposed. Five versions of the concept tree were created (cf. Figure 18, Figure 19, Figure 20, Figure 21, and Figure 22). The first version, more rudimental, underwent alterations until the lastest version, which is more refined, was reached. The interations demonstrate changes in the structure of the concept tree and the fine-tuning of the contents.

Following each concept tree, Table 52, Table 53, Table 54, Table 55, Table 17 demonstrate their numbered concepts, used in the comparison matrices. The first matrix created, split into Table 56 and Table 57, uses an "x" to cross reference the location of the concepts from Concept tree version 1 to their counterparts in the version 2. Also, within version 2, concept Resource optimization (G.2.3) is highlighted by an orange background; this emphasis represents a concept that was added, therefore it does not possess an equivalent concept in version 1.

Then Table 58 compares versions 2 thru 5, by using their numbered concepts, it also emphasizes the differences between versions with the use of a blue background to represent the concepts that changed location in the following version, the use of an orange background to represent concepts that were removed from the following version, and the use of red lettering to highlight the words or parts of the question that were modified. Similar highlights are displayed in the instrument matrix version (Appendix J – Artifact Construction: Instrument).

Concept Tree Version 1

- 1- Human behavioral component
  - a. Roles
    - i. Governing body
    - ii. Stakeholders
    - iii. Executive management
    - iv. Auditors
    - v. DPO (GDPR)
  - b. Responsibilities
- 2- Procedural component
  - a. Processes (EDM)
    - i. Evaluate
    - ii. Direct
    - iii. Monitor/Control
  - b. Objectives/purpose
    - i. Strategic alignment
    - ii. Value delivery
    - iii. Accountability
  - c. Needs (balanced)
  - d. Organizational structure
    - i. Reporting lines
    - ii. Document communication
    - iii. ISG integration within the organization
  - e. Security culture
    - i. Trust
    - ii. Privacy
  - f. Risk program
    - i. Risk management
    - ii. Risk appetite
    - iii. Risk mitigation
  - g. Cost-effective
  - h. Effective ISG
  - i. Efficient ISG
- 3- Technical component
  - a. Controls
    - i. KPI's
  - b. Policies
  - c. Performance
  - d. Support
  - e. Compliance
  - f. Documentation
    - i. Reports
    - ii. Assessments
    - iii. Reviews
  - g. Audits

Figure 18 – Concept Tree Version 1

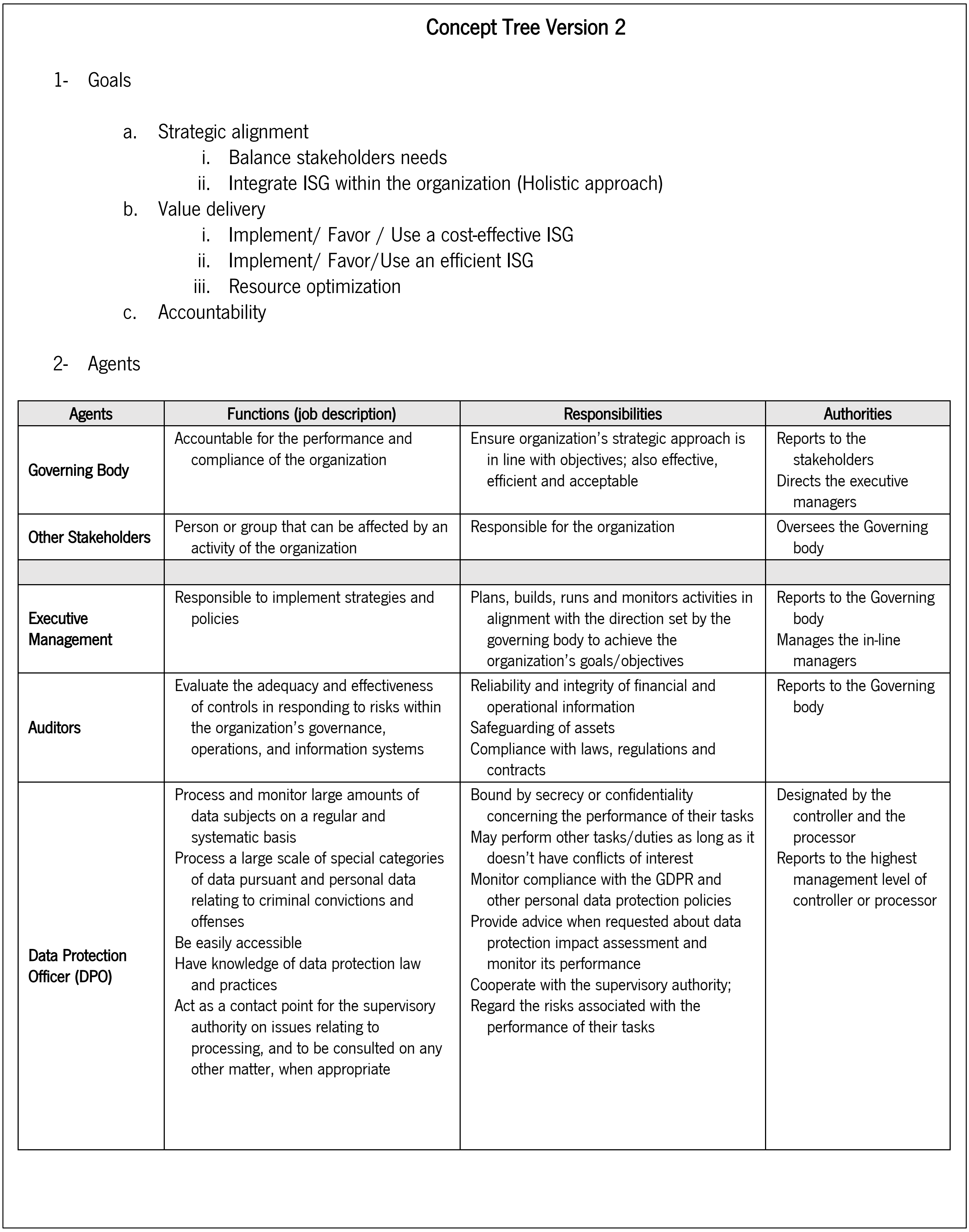
        h. Physical Document
            i. Document type/purpose
            ii. Targeted audience
            iii. Review period

4- Change management

    a. Business continuity plan
    b. Capability Maturity Model

Table 52 – Concept Tree Version 1 Numbered Concepts

CT number	**CT definition**
H	Human behavioral component
H.1	Roles
H.1.1	Governing body
H.1.2	Stakeholders
H.1.3	Executive management
H.1.4	Auditors
H.1.5	DPO (GDPR)
H.2	Responsibilities
P	Procedural component
P.1	Processes (EDM)
P.1.1	Evaluate
P.1.2	Direct
P.1.3	Monitor/Control
P.2	Objectives/purpose
P.2.1	Strategic alignment
P.2.2	Value delivery
P.2.3	Accountability
P.3	Needs (balanced)
P.4	Organizational structure
P.4.1	Reporting lines
P.4.2	Document communication
P.4.3	ISG integration within the organization
P.5	Security culture
P.5.1	Trust
P.5.2	Privacy
P.6	Risk program
P.6.1	Risk management
P.6.2	Risk appetite
P.6.3	Risk mitigation
P.7	Cost-effective
P.8	Effective ISG
P.9	Efficient ISG
T	Technical component
T.1	Controls
T.1.1	KPI's
T.2	Policies
T.3	Performance
T.4	Support
T.5	Compliance
T.6	Documentation
T.6.1	Reports
T.6.2	Assessments
T.6.3	Reviews
T.7	Audits
T.8	Physical Document
T.8.1	Document type/purpose
T.8.2	Targeted audience
T.8.3	Review period
C	Change management
C.1	Business continuity plan
C.2	Capability Maturity Model



Concept Tree Version 2

1- Goals

   a. Strategic alignment
      i. Balance stakeholders needs
      ii. Integrate ISG within the organization (Holistic approach)
   b. Value delivery
      i. Implement/ Favor / Use a cost-effective ISG
      ii. Implement/ Favor/Use an efficient ISG
      iii. Resource optimization
   c. Accountability

2- Agents

Agents	Functions (job description)	Responsibilities	Authorities
Governing Body	Accountable for the performance and compliance of the organization	Ensure organization's strategic approach is in line with objectives; also effective, efficient and acceptable	Reports to the stakeholders Directs the executive managers
Other Stakeholders	Person or group that can be affected by an activity of the organization	Responsible for the organization	Oversees the Governing body
Executive Management	Responsible to implement strategies and policies	Plans, builds, runs and monitors activities in alignment with the direction set by the governing body to achieve the organization's goals/objectives	Reports to the Governing body Manages the in-line managers
Auditors	Evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems	Reliability and integrity of financial and operational information Safeguarding of assets Compliance with laws, regulations and contracts	Reports to the Governing body
Data Protection Officer (DPO)	Process and monitor large amounts of data subjects on a regular and systematic basis Process a large scale of special categories of data pursuant and personal data relating to criminal convictions and offenses Be easily accessible Have knowledge of data protection law and practices Act as a contact point for the supervisory authority on issues relating to processing, and to be consulted on any other matter, when appropriate	Bound by secrecy or confidentiality concerning the performance of their tasks May perform other tasks/duties as long as it doesn't have conflicts of interest Monitor compliance with the GDPR and other personal data protection policies Provide advice when requested about data protection impact assessment and monitor its performance Cooperate with the supervisory authority; Regard the risks associated with the performance of their tasks	Designated by the controller and the processor Reports to the highest management level of controller or processor

Figure 19 – Concept Tree Version 2

Concept Tree Version 2

3- Processes

- Evaluate
  - Assess the support of business objectives
  - Assesses the Change management
    - Estimates the Capability Maturity Model
- Direct
  - Supervise the Risk Management plan
    - Risk appetite
    - Risk mitigation
  - Oversee the Security Culture
    - Information security Policies
    - Trust concerns
    - Privacy concerns
  - Supervise the Business Continuity plan
- Monitor/Control
  - Compliance with internal and external requirements
  - Apply Performance metrics (KPI's)
    - Reports
    - Assessments
    - Reviews
  - Revise the Physical Document
    - Purpose
    - Intended audience
    - Review period

4- Controls

- Audits (independent + objective)

Table 53 – Concept Tree Version 2 Numbered Concepts

CT number	**CT definition**
G	Goals
G.1	Strategic alignment
G.1.1	Balance stakeholders needs
G.1.2	Integrate ISG within the organization (Holistic approach)
G.2	Value delivery
G.2.1	Implement/ Favor / Use a cost-effective ISG
G.2.2	Implement/ Favor/Use an efficient ISG
G.2.3	Resource optimization
G.3	Accountability
Ag	Agents
Ag.1	Governing Body
Ag.2	Other Stakeholders
Ag.3	Executive Management
Ag.4	Auditors
Ag.5	Data Protection Officer (DPO)
P	Processes
P.1	Evaluate
P.1.1	Assess the support of business objectives
P.1.2	Assesses the Change management
P.1.2.1	Estimates the Capability Maturity Model
P.2	Direct
P.2.1	Supervise the Risk Management plan
P.2.1.1	Risk appetite
P.2.1.2	Risk mitigation
P.2.2	Oversee the Security Culture
P.2.2.1	Information security Policies
P.2.2.2	Trust concerns
P.2.2.3	Privacy concerns
P.2.3	Supervise the Business Continuity plan
P.3	Monitor/Control
P.3.1	Compliance with internal and external requirements
P.3.2	Apply Performance metrics (KPI's)
P.3.2.1	Reports
P.3.2.2	Assessments
P.3.2.3	Reviews
P.3.3	Revise the Physical Document
P.3.3.1	Purpose
P.3.3.2	Intended audience
P.3.3.3	Review period
C	Controls
C.1	Audits (independent + objective)

Concept Tree Version 3

1- Goals

   a. Strategic alignment
      i. Balance stakeholders needs
      ii. ISG integration within the organization (Holistic approach)
   b. Value delivery
      i. ISG cost-effectiveness
      ii. ISG efficiency
      iii. Resource optimization
   c. Accountability
   d. Compliance

2- Agents

Agents	Functions (job description)	Responsibilities	Authorities
Governing Body	Accountable for the performance and compliance of the organization Responsible for ensuring the information security policies, procedures and practices are adequate Provide information security protections, and that they are commensurate with the risk and magnitude of harm of the information and information systems Ensure the information security program provides security to all systems that support the organization's operation Ensure the information security processes are integrated with the organizations strategic and operational mission Ensure organization has trained personnel to support compliance with information security policies, processes, standards and guidelines Ensures that all information security policies are sufficiently coordinated to ensure effective implementation of cross-cutting/convergent security objectives	Ensure organization's strategic approach is in line with objectives; also effective, efficient and acceptable Integrate information security to strategic planning process by establishing and documenting information security strategies that support the agency's strategic and performance planning activities; and revise them whenever occurs a major change in the information security environment Ultimately responsible for the information security Responsible for the line-item control over all information security activities. Receive report from all information security practitioners Responsible for the policy development, the oversight of responsibilities and budget responsibilities over department information security program Designate the executive management and delegate authority, ensuring compliance with applicable information security requirements Monitor the status of their programs to ensure the information security activities are providing appropriate support for the mission; policies and procedures are current and aligned with evolving technologies; and controls are accomplishing their purpose	Reports to the stakeholders Directs the executive managers

Figure 20 – Concept Tree Version 3

Concept Tree Version 3

Agents	Functions (job description)	Responsibilities	Authorities
Executive Management	Responsible to implement strategies and policies Develop and maintain organization-wide information security program Develop and maintain information policies, procedures, control techniques to address applicable requirements	Plans, builds, runs and monitors activities in alignment with the direction set by the governing body to achieve the organization's ISG goals/objectives Responsible for implementing and monitoring information security practices and controls within their respective units Designates the SAISO Ensure compliance with information security requirements Reports to the governing body about the effectiveness of the information security program and the progress of remedial actions Implement security enhancement tools Address security breaches and disruptions Address privacy issues	Reports to the Governing body Manages the in-line managers
Auditors	Evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems	Reliability and integrity of financial and operational information Safeguarding of assets Compliance with laws, regulations and contracts	Reports to the Governing body
Data Protection Officer (DPO)	Process and monitor large amounts of data subjects on a regular and systematic basis Process a large scale of special categories of data pursuant and personal data relating to criminal convictions and offenses Be easily accessible Have knowledge of data protection law and practices Act as a contact point for the supervisory authority on issues relating to processing, and to be consulted on any other matter, when appropriate	Bound by secrecy or confidentiality concerning the performance of their tasks May perform other tasks/duties as long as it doesn't have conflicts of interest Monitor compliance with the GDPR and other personal data protection policies Provide advice when requested about data protection impact assessment and monitor its performance Cooperate with the supervisory authority; Regard the risks associated with the performance of their tasks	Designated by the executive management Reports to the governing body
Employees			

Concept Tree Version 3

Agents	Functions (job description)	Responsibilities	Authorities
Senior Agency Information Security Officer (SAISO)	Perform Information security duties (primary duty) Support the CIO in the annual reporting Head an office with mission and resources to assist in the compliance of information security resources Facilitate the development of subordinate plans to provide adequate information security for networks, facilities, systems or groups of information systems Ensure agency personnel and contractors receive appropriate information security awareness training Ensure preparation and maintenance of plans and procedures to provide continuous operations for information systems that support the agency's operations and assets Compare and correlate a variety of real-time and statistic information from a number of ongoing activities	Periodically assess the risks and the magnitude of harm of information and information systems that support the operations and assets Develop and maintain a risk-based and cost-effective information security policies, procedures and control techniques to address requirements throughout each agency lifecycle of information system Train and oversee personnel with significant responsibilities for information security Periodically test and evaluate the effectiveness of information security policies, procedures and practices Establish and maintain a process for planning, implementing, evaluating and documenting remedial actions to address any deficiencies in information security policies, procedures and practices Develop and implement procedures for detecting, reporting and responding to security incidents	Designated by the CIO Responsibilities assigned by FISMA
Other Stakeholders (Customers, user, suppliers, partners)	Person or group has an interest in an ISS activity, project or service of an organization	Responsible for the organization	Oversees the Governing body

3- Processes

- Evaluate
  - Assess the alignment of ISS to business strategy
    - Ensure business initiatives takes into account information security issues
    - Ensure that information security adequately supports and sustains the business objectives
    - Respond to information security performance results, prioritize and initiate required actions
  - Realize benefits/value from information security investments
- Direct
  - Ensure the commitment of executive management to protect information assets and make information security related decisions
  - Develop and approve the information security strategy and policy

Concept Tree Version 3

    - Allocate adequate investments and resources
        - Ensure it-agility
        - Ensure optimization of IT assets, resources and capabilities
    - Direct organization’s risk management
        - Determine organization’s risk appetite
        - Develop risk management policies
    - Direct resource management and stakeholders communication and reporting
        - Assign responsibilities for resource management
        - Ensure competent and motivated business and IT personnel
        - Develop escalation guidelines
        - Promote a positive information security culture
        - Develop reporting and communication principles and guidelines
        - Develop principles for safeguarding resources
- Monitor/Control
    - Assess the effectiveness of information security management activities
        - Provide feedback on information security performance results and their impacts on the organization
    - Check the compliance with legislation, regulations, contractual obligations and statutory requirements.
        - Report to external stakeholders that the organization practices a level of information security commensurate with the nature of its business.
    - Consider the changing business, legal and regulatory environment and their potential of information risk
    - Select appropriate information security performance metrics from business perspective
    - Feedback on transparency of IT costs, benefits and risks
    - Commission independent and objective opinion (audits) of how it is complying with its accountability for the desired level of information security.

4. Artifacts

- Produce the Information Systems Security strategy
    - Decision making model
- Create an Information Systems Security program
    - Investment distribution
    - Resource allocation
    - Responsibility assignment
- Develop an Information Systems Security policy and guidelines
    - Authority levels
    - Escalation guidelines
    - Reporting and communicating structure
- Create an Information Systems Security performance program
    - Reporting and communicating
        - Stakeholder’s feedback
            - Governance effectiveness
            - Risk Management issues
    - Recommended actions to address resource management deviations
    - Audit Reports

Concept Tree Version 3

- Create a Risk Management program
    - Risk assessment
    - Risk policies
        - Risk tolerance level
    - Risk appetite
    - Risk mitigation

Table 54 – Concept Tree Version 3 Numbered Concepts

CT number	CT definition
G	Goals
G.1	Strategic alignment
G.1.1	Balance stakeholders needs
G.1.2	Integrate ISG within the organization (Holistic approach)
G.2	Value delivery
G.2.1	ISG cost-effectiveness
G.2.2	ISG efficiency
G.2.3	Resource optimization
G.3	Accountability
G.4	Compliance
Ag	Agents
Ag.1	Governing Body
Ag.2	Executive Management
Ag.3	Auditors
Ag.4	Data Protection Officer (DPO)
Ag.5	Employees
Ag.6	Senior Agency Information Security Officer (SAISO)
Ag.7	Other Stakeholders (Customers, user, suppliers, partners)
P	Processes
P.1	Evaluate
P.1.1	Assess the alignment of ISS to business strategy
P.1.1.1	Ensure business initiatives takes into account information security issues
P.1.1.2	Ensure that information security adequately supports and sustains the business objectives
P.1.1.3	Respond to information security performance results, prioritize and initiate required actions
P.1.2	Realize benefits/value from information security investments
P.2	Direct
P.2.1	Ensure the commitment of executive management to protect information assets and make information security related decisions
P.2.2	Develop and approve the information security strategy and policy
P.2.3	Allocate adequate investments and resources
P.2.3.1	Ensure it-agility
P.2.3.2	Ensure optimization of IT assets, resources and capabilities
P.2.4	Direct organization's risk management
P.2.4.1	Determine organization's risk appetite
P.2.4.2	Develop risk management policies
P.2.5	Direct resource management and stakeholders communication and reporting
P.2.5.1	Assign responsibilities for resource management
P.2.5.2	Ensure competent and motivated business and IT personnel
P.2.5.3	Develop escalation guidelines
P.2.5.4	Promote a positive information security culture
P.2.5.5	Develop reporting and communication principles and guidelines
P.2.5.6	Develop principles for safeguarding resources
P.3	Monitor/Control
P.3.1	Assess the effectiveness of information security management activities
P.3.1.1	Provide feedback on information security performance results and their impacts on the organization
P.3.2	Check the compliance with legislation, regulations, contractual obligations and statutory requirements
P.3.2.1	Report to external stakeholders that the organization practices a level of information security commensurate with the nature of its business.
P.3.3	Consider the changing business, legal and regulatory environment and their potential of information risk
P.3.4	Select appropriate information security performance metrics from business perspective
P.3.5	Feedback on transparency of IT costs, benefits and risks
P.3.6	Commission independent and objective opinion (audits) of how it is complying with its accountability for the desired level of information security.
AR	Artifacts
AR.1	Produce the Information Systems Security strategy

CT number	CT definition
AR.1.1	Decision making model
AR.2	Create an Information Systems Security program
AR.2.1	Investment distribution
AR.2.2	Resource allocation
AR.2.3	Responsibility assignment
AR.3	Develop an Information Systems Security policy and guidelines
AR.3.1	Authority levels
AR.3.2	Escalation guidelines
AR.3.3	Reporting and communicating structure
AR.4	Create an Information Systems Security performance program
AR.4.1	Reporting and communicating
AR.4.1.1	Stakeholder's feedback
AR.4.1.1.1	Governance effectiveness
AR.4.1.1.2	Risk Management issues
AR.4.2	Recommended actions to address resource management deviations
AR.4.3	Audit Reports
AR.5	Create a Risk Management program
AR.5.1	Risk assessment
AR.5.2	Risk policies
AR.5.2.1	Risk tolerance level
AR.5.3	Risk appetite
AR.5.4	Risk mitigation

Concept Tree Version 4

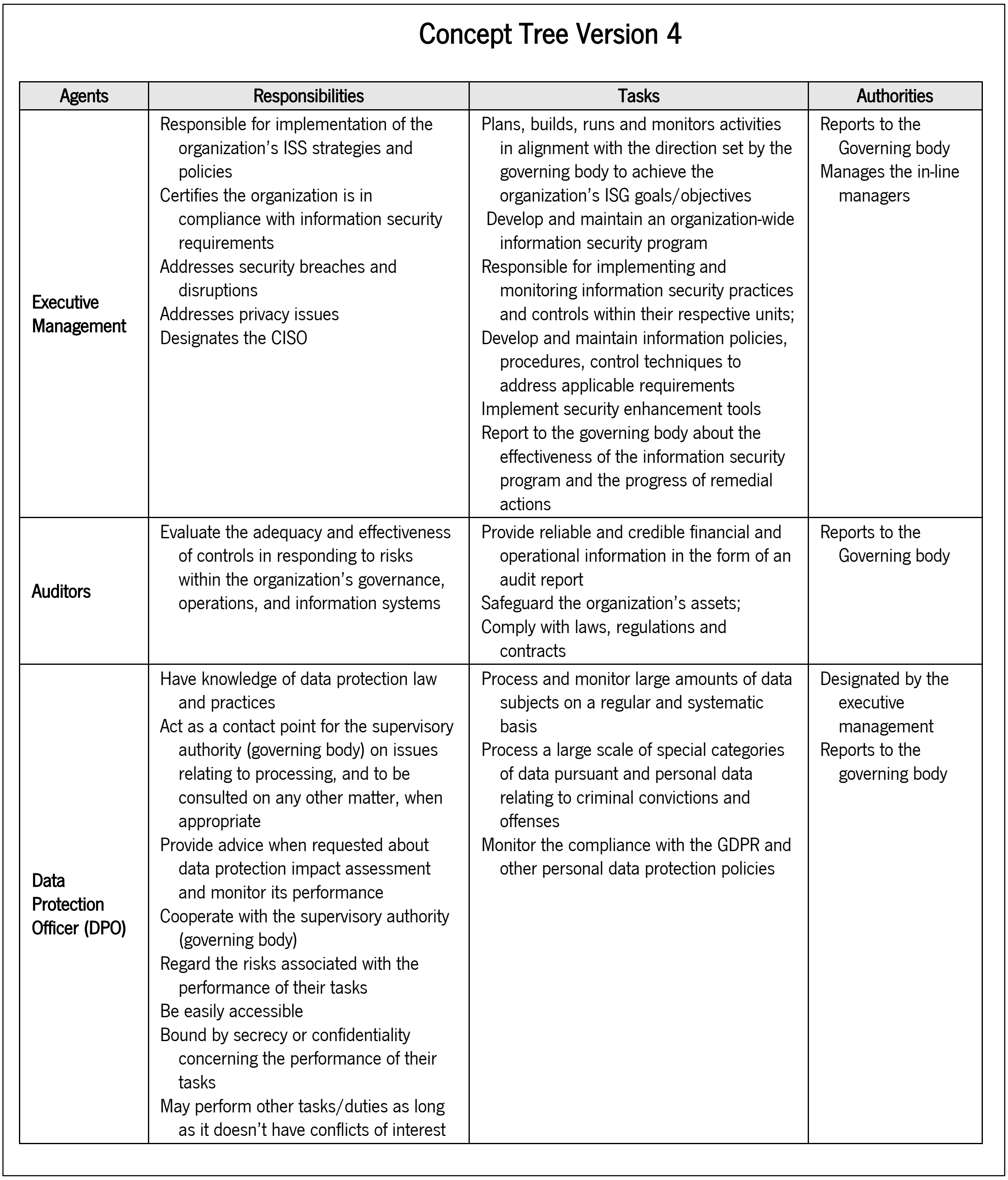
1- Goals

a. Strategic alignment
    i. Balancing stakeholders needs
    ii. ISG integration within the organization (Holistic approach)
b. Value delivery
    i. ISG cost-effectiveness
    ii. ISG efficiency
        1. IT-agility
    iii. Resource, assets and capabilities optimization
c. Accountability
d. Compliance

2- Agents

Agents	Responsibilities	Tasks	Authorities
Governing Body	Certify that the organization's strategic approach is in line with objectives; and is also effective, efficient and acceptable Ensure the information security processes are integrated with the organization's strategic and operational mission Ultimately responsible for the information security Accountable for the performance and compliance of the organization's ISS Responsible for the line-item control over all information security activities. Receive report from all information security practitioners Responsible for the policy development, the oversight of responsibilities and budget responsibilities over department information security program Responsible for adequacy of the information security policies, procedures and practices Ensures that all information security policies are sufficiently coordinated to ensure effective implementation of cross-cutting/convergent security objectives Designate the executive management and delegate authority, ensuring compliance with applicable information security requirements Confirm that the organization has trained personnel to support compliance with information security policies, processes, standards and guidelines Ensure the information security program provides security to all systems that support the organization's operation	Integrate information security to strategic planning process by establishing and documenting information security strategies that support the agency's strategic and performance planning activities; and revise them whenever occurs a major change in the information security environment Monitor the status of the organization's programs to ensure the information security activities are providing appropriate support for the mission; policies and procedures are current and aligned with evolving technologies; and controls are accomplishing their purpose Provide information security protections, and that they are commensurate with the risk and magnitude of harm of the information and information systems	Reports to the stakeholders Directs the executive management

Figure 21 – Concept Tree Version 4



Concept Tree Version 4

Agents	Responsibilities	Tasks	Authorities
Executive Management	Responsible for implementation of the organization’s ISS strategies and policies Certifies the organization is in compliance with information security requirements Addresses security breaches and disruptions Addresses privacy issues Designates the CISO	Plans, builds, runs and monitors activities in alignment with the direction set by the governing body to achieve the organization’s ISG goals/objectives Develop and maintain an organization-wide information security program Responsible for implementing and monitoring information security practices and controls within their respective units; Develop and maintain information policies, procedures, control techniques to address applicable requirements Implement security enhancement tools Report to the governing body about the effectiveness of the information security program and the progress of remedial actions	Reports to the Governing body Manages the in-line managers
Auditors	Evaluate the adequacy and effectiveness of controls in responding to risks within the organization’s governance, operations, and information systems	Provide reliable and credible financial and operational information in the form of an audit report Safeguard the organization’s assets; Comply with laws, regulations and contracts	Reports to the Governing body
Data Protection Officer (DPO)	Have knowledge of data protection law and practices Act as a contact point for the supervisory authority (governing body) on issues relating to processing, and to be consulted on any other matter, when appropriate Provide advice when requested about data protection impact assessment and monitor its performance Cooperate with the supervisory authority (governing body) Regard the risks associated with the performance of their tasks Be easily accessible Bound by secrecy or confidentiality concerning the performance of their tasks May perform other tasks/duties as long as it doesn’t have conflicts of interest	Process and monitor large amounts of data subjects on a regular and systematic basis Process a large scale of special categories of data pursuant and personal data relating to criminal convictions and offenses Monitor the compliance with the GDPR and other personal data protection policies	Designated by the executive management Reports to the governing body

Concept Tree Version 4

Agents	Responsibilities	Tasks	Authorities
Chief Information Security Officer (CISO)	Perform Information security duties (primary duty) Head an office with mission and resources to assist in the compliance of information security resources Ensure the preparation and maintenance of plans and procedures to provide continuous operations for information systems that support the agency's operations and assets Facilitate the development of subordinate plans to provide adequate information security for networks, facilities, systems or groups of information systems Support the CIO/Executive management in the annual reporting Certify that agency personnel and contractors receive appropriate information security awareness training	Develop and maintain a risk-based and cost-effective information security policies, procedures and control techniques to address requirements throughout the lifecycle of information system Establish and maintain a process for planning, implementing, evaluating and documenting remedial actions to address any deficiencies in information security policies, procedures and practices Develop and implement procedures for detecting, reporting and responding to security incidents Compare and correlate a variety of real-time and statistic information from a number of ongoing activities Train and oversee personnel with significant responsibilities for information security Periodically test and evaluate the effectiveness of information security policies, procedures and practices Periodically assess the risks and the magnitude of harm of information and information systems that support the operations and assets	Designated by the CIO/Executive management Responds to the Executive Management Responsible for in-line management
Employees	Comply with organization's policies and guidelines Comply with ISS laws and regulations	Perform activities according to/following the organization's policies and guidelines	Reports to in-line manager
Other Stakeholders (Customers, user, suppliers, partners)	Person or group has an interest in an ISS activity, project or service of an organization	Abide by the ISS policies set out by the organization	Oversees the organization ISS activity, project or service Hold organization accountable for their ISS

3- Processes

- Evaluate
  - Assess the alignment of ISS to business strategy
    - Verify that business initiatives takes into account information security issues
    - Verify that information security supports and sustains the business objectives
    - Respond to information security performance results, prioritize and initiate required actions
  - Assess benefits/value from information security investments
- Direct
  - Oversee the commitment of executive management to protect information assets and make information security related decisions
  - Develop and approve the information security strategy and policy
  - Allocate investments and resources

Concept Tree Version 4

  - Direct organization’s risk management
    - Determine organization’s risk appetite
    - Develop risk management policies
  - Direct resource management and stakeholders communication and reporting
    - Assign responsibilities for resource management
    - Require competent and motivated business and IT personnel
    - Develop escalation guidelines
    - Promote a positive information security culture
    - Develop reporting and communication principles and guidelines
    - Develop principles for safeguarding resources
- Monitor/Control
  - Assess the effectiveness of information security management activities
    - Provide feedback on information security performance results and their impacts on the organization
  - Check the compliance with legislation, regulations, contractual obligations and statutory requirements.
    - Report to stakeholders the organization’s practices for information security are aligned with the nature of its business.
  - Consider the changing business, legal and regulatory environment and their potential of information risk
  - Select the metrics for the information security performance from a business perspective
  - Provide feedback on transparency of IT costs, benefits and risks
  - Commission audits to verify compliance with the level of accountability desired (agreed/ determined) for information security.

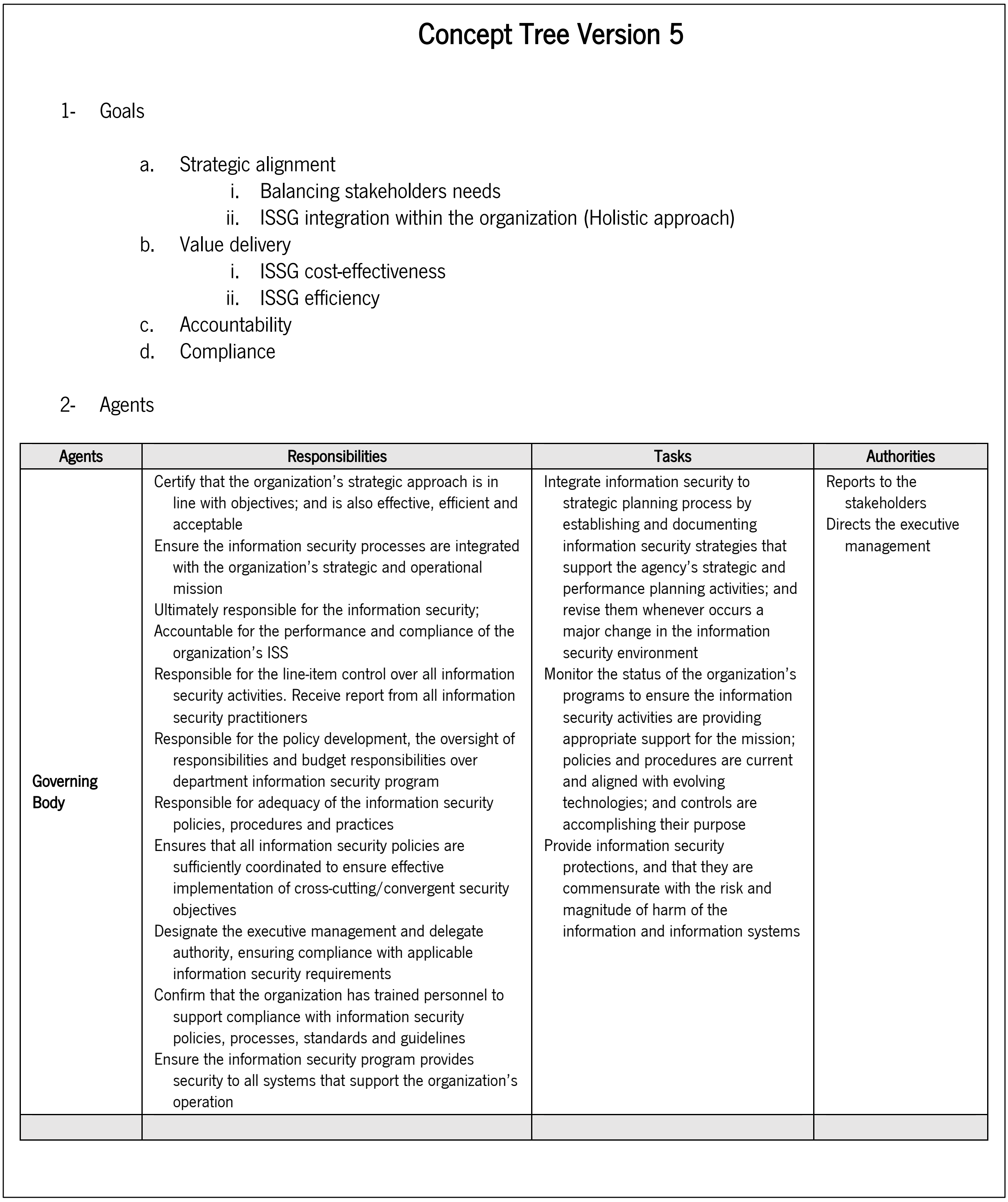
4- Artifacts

- Produce the Information Systems Security strategy
  - Elaborate a Decision making model
- Create an Information Systems Security program
  - Contemplate the Investment distribution
  - Contemplate the Resource allocation
  - Contemplate the Responsibility assignment
- Develop an Information Systems Security policy and guidelines
  - Covering Authority levels
  - Covering Escalation guidelines
  - Covering the Reporting and communicating structure
- Create an Information Systems Security performance program
  - Contemplate the Reporting and communicating actions
    - Stakeholder’s feedback
  - Recommended actions to address resource management deviations
  - Contemplate Audit Reports
- Create a Risk Management program
  - Regarding Risk assessment
  - Regarding Risk policies
    - Risk tolerance level
  - Regarding Risk appetite
  - Regarding Risk mitigation

Table 55 – Concept Tree Version 4 Numbered Concepts

CT number	CT definition
G	Goals
G.1	Strategic alignment
G.1.1	Balancing stakeholders needs
G.1.2	ISG integration within the organization (Holistic approach)
G.2	Value delivery
G.2.1	ISG cost-effectiveness
G.2.2	ISG efficiency
G.2.2.1	IT-agility
G.2.3	Resource, assets and capabilities optimization
G.3	Accountability
G.4	Compliance
Ag	Agents
Ag.1	Governing Body
Ag.2	Executive Management
Ag.3	Auditors
Ag.4	Data Protection Officer (DPO)
Ag.5	Chief Information Security Officer (CISO)
Ag.6	Employees
Ag.7	Other Stakeholders (Customers, user, suppliers, partners)
P	Processes
P.1	Evaluate
P.1.1	Assess the alignment of ISS to business strategy
P.1.1.1	Verify that business initiatives takes into account information security issues
P.1.1.2	Verify that information security supports and sustains the business objectives
P.1.1.3	Respond to information security performance results, prioritize and initiate required actions
P.1.2	Assess benefits/value from information security investments
P.2	Direct
P.2.1	Oversee the commitment of executive management to protect information assets and make information security related decisions
P.2.2	Develop and approve the information security strategy and policy
P.2.3	Allocate investments and resources
P.2.4	Direct organization’s risk management
P.2.4.1	Determine organization’s risk appetite
P.2.4.2	Develop risk management policies
P.2.5	Direct resource management and stakeholders communication and reporting
P.2.5.1	Assign responsibilities for resource management
P.2.5.2	Require competent and motivated business and IT personnel
P.2.5.3	Develop escalation guidelines
P.2.5.4	Promote a positive information security culture
P.2.5.5	Develop reporting and communication principles and guidelines
P.2.5.6	Develop principles for safeguarding resources
P.3	Monitor/Control
P.3.1	Assess the effectiveness of information security management activities
P.3.1.1	Provide feedback on information security performance results and their impacts on the organization
P.3.2	Check the compliance with legislation, regulations, contractual obligations and statutory requirements
P.3.2.1	Report to stakeholders the organization’s practices for information security are aligned with the nature of its business.
P.3.3	Consider the changing business, legal and regulatory environment and their potential of information risk
P.3.4	Select the metrics for the information security performance from a business perspective
P.3.5	Provide feedback on transparency of IT costs, benefits and risks
P.3.6	Commission audits to verify compliance with the level of accountability desired (agreed/ determined) for information security
AR	Artifacts
AR.1	Produce the Information Systems Security strategy
AR.1.1	Elaborate a Decision making model
AR.2	Create an Information Systems Security program

CT number	CT definition
AR.2.1	Contemplate the Investment distribution
AR.2.2	Contemplate the Resource allocation
AR.2.3	Contemplate the Responsibility assignment
AR.3	Develop an Information Systems Security policy and guidelines
AR.3.1	Covering Authority levels
AR.3.2	Covering Escalation guidelines
AR.3.3	Covering the Reporting and communicating structure
AR.4	Create an Information Systems Security performance program
AR.4.1	Contemplate the Reporting and communicating actions
AR.4.1.1	Stakeholder’s feedback
AR.4.2	Recommended actions to address resource management deviations
AR.4.3	Contemplate Audit Reports
AR.5	Create a Risk Management program
AR.5.1	Regarding Risk assessment
AR.5.2	Regarding Risk policies
AR.5.2.1	Risk tolerance level
AR.5.3	Regarding Risk appetite
AR.5.4	Regarding Risk mitigation



Concept Tree Version 5

1- Goals

  a. Strategic alignment
    i. Balancing stakeholders needs
    ii. ISSG integration within the organization (Holistic approach)
  b. Value delivery
    i. ISSG cost-effectiveness
    ii. ISSG efficiency
  c. Accountability
  d. Compliance

2- Agents

Agents	Responsibilities	Tasks	Authorities
Governing Body	Certify that the organization's strategic approach is in line with objectives; and is also effective, efficient and acceptable Ensure the information security processes are integrated with the organization's strategic and operational mission Ultimately responsible for the information security; Accountable for the performance and compliance of the organization's ISS Responsible for the line-item control over all information security activities. Receive report from all information security practitioners Responsible for the policy development, the oversight of responsibilities and budget responsibilities over department information security program Responsible for adequacy of the information security policies, procedures and practices Ensures that all information security policies are sufficiently coordinated to ensure effective implementation of cross-cutting/convergent security objectives Designate the executive management and delegate authority, ensuring compliance with applicable information security requirements Confirm that the organization has trained personnel to support compliance with information security policies, processes, standards and guidelines Ensure the information security program provides security to all systems that support the organization's operation	Integrate information security to strategic planning process by establishing and documenting information security strategies that support the agency's strategic and performance planning activities; and revise them whenever occurs a major change in the information security environment Monitor the status of the organization's programs to ensure the information security activities are providing appropriate support for the mission; policies and procedures are current and aligned with evolving technologies; and controls are accomplishing their purpose Provide information security protections, and that they are commensurate with the risk and magnitude of harm of the information and information systems	Reports to the stakeholders Directs the executive management

Figure 22 – Concept Tree Version 5

Agents	Responsibilities	Tasks	Authorities
Executive Management	Responsible for implementation of the organization's ISS strategies and policies Certifies the organization is in compliance with information security requirements Addresses security breaches and disruptions; Addresses privacy issues; Designates the CISO	Plans, builds, runs and monitors activities in alignment with the direction set by the governing body to achieve the organization's ISSG goals/objectives Develop and maintain an organization-wide information security program Responsible for implementing and monitoring information security practices and controls within their respective units Develop and maintain information policies, procedures, control techniques to address applicable requirements Implement security enhancement tools Report to the governing body about the effectiveness of the information security program and the progress of remedial actions	Reports to the Governing body Manages the in-line managers
Auditors	Evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems	Provide reliable and credible financial and operational information in the form of an audit report Safeguard the organization's assets Comply with laws, regulations and contracts	Reports to the Governing body
Data Protection Officer (DPO)	Have knowledge of data protection law and practices Act as a contact point for the supervisory authority (governing body) on issues relating to processing, and to be consulted on any other matter, when appropriate Provide advice when requested about data protection impact assessment and monitor its performance Cooperate with the supervisory authority (governing body) Regard the risks associated with the performance of their tasks Be easily accessible Bound by secrecy or confidentiality concerning the performance of their tasks May perform other tasks/duties as long as it doesn't have conflicts of interest	Process and monitor large amounts of data subjects on a regular and systematic basis Process a large scale of special categories of data pursuant and personal data relating to criminal convictions and offenses Monitor the compliance with the GDPR and other personal data protection policies	Designated by the executive management Reports to the governing body

Agents	Responsibilities	Tasks	Authorities
Chief Information Security Officer (CISO)	Perform Information security duties (primary duty) Head an office with mission and resources to assist in the compliance of information security resources Ensure the preparation and maintenance of plans and procedures to provide continuous operations for information systems that support the agency's operations and assets Facilitate the development of subordinate plans to provide adequate information security for networks, facilities, systems or groups of information systems Support the CIO/Executive management in the annual reporting Certify that agency personnel and contractors receive appropriate information security awareness training	Develop and maintain a risk-based and cost-effective information security policies, procedures and control techniques to address requirements throughout the lifecycle of information system Establish and maintain a process for planning, implementing, evaluating and documenting remedial actions to address any deficiencies in information security policies, procedures and practices Develop and implement procedures for detecting, reporting and responding to security incidents Compare and correlate a variety of real-time and statistic information from a number of ongoing activities Train and oversee personnel with significant responsibilities for information security Periodically test and evaluate the effectiveness of information security policies, procedures and practices Periodically assess the risks and the magnitude of harm of information and information systems that support the operations and assets	Designated by the CIO/Executive management Responds to the Executive Management Responsible for in-line management
Employees	Comply with organization's policies and guidelines Comply with ISS laws and regulations	Perform activities according to/following the organization's policies and guidelines	Reports to in-line manager
Other Stakeholders (Customers, user, suppliers, partners)	Person or group has an interest in an ISS activity, project or service of an organization	Abide by the ISS policies set out by the organization	Oversees the organization ISS activity, project or service Hold organization accountable for their ISS

3- Processes

- Evaluate
  - Assess the alignment of ISS to business strategy
    - Verify that business initiatives takes into account ISS issues
    - Verify that ISS supports and sustains the business objectives
    - Respond to ISS performance results, prioritize and initiate required actions
  - Assess benefits/value from ISS investments

- Direct
    - Oversee the commitment of executive management to protect information assets and make ISS related decisions
    - Develop and approve the ISS strategy and policy
    - Allocate investments and resources
    - Direct organization's risk management program
        - Determine organization's risk appetite
        - Develop risk management policies
    - Direct resource management and stakeholders communication and reporting
        - Assign responsibilities for resource management
        - Require competent and motivated business and IT personnel
        - Develop escalation guidelines
        - Promote a positive ISS culture
        - Develop reporting and communication principles and guidelines
        - Develop principles for safeguarding resources
- Monitor/Control
    - Assess the effectiveness of ISS management activities
        - Provide feedback on ISS performance results and their impacts on the organization
    - Check the compliance with legislation, regulations, contractual obligations and statutory requirements
        - Report to stakeholders the organization's practices for ISS are aligned with the nature of its business
    - Consider the changing business, legal and regulatory environment and their potential of information risk
    - Select the metrics for the ISS performance from a business perspective
    - Provide feedback and transparency over ISS costs, benefits and risks
    - Commission audits to verify compliance with the level of accountability desired (agreed/ determined) for ISS

4- Artifacts

- Information Systems Security strategy
    - Decision making model
- Information Systems Security program
    - Investment distribution
    - Resource allocation
    - Responsibility assignment
- Information Systems Security policy and guidelines
    - Authority levels
    - Escalation guidelines
    - Reporting and communicating structure
- Information Systems Security performance program
    - Reporting and communicating actions
        - Stakeholder's feedback
    - Recommended actions to address resource management deviations
    - Audit Reports
- Risk Management program
    - Risk assessment
    - Risk management policies
        - Risk tolerance level
    - Risk appetite
    - Risk mitigation

Table 17 – Concept Tree Version 5 Numbered Concepts

CT number	CT definition
G	Goals
G.1	Strategic alignment
G.1.1	Balancing stakeholders needs
G.1.2	ISSG integration within the organization (Holistic approach)
G.2	Value delivery
G.2.1	ISSG cost-effectiveness
G.2.2	ISSG efficiency
G.3	Accountability
G.4	Compliance
Ag	Agents
Ag.1	Governing Body
Ag.2	Executive Management
Ag.3	Auditors
Ag.4	Data Protection Officer (DPO)
Ag.5	Chief Information Security Officer (CISO)
Ag.6	Employees
Ag.7	Other Stakeholders (Customers, user, suppliers, partners)
P	Processes
P.1	Evaluate
P.1.1	Assess the alignment of ISS to business strategy
P.1.1.1	Verify that business initiatives takes into account ISS issues
P.1.1.2	Verify that ISS supports and sustains the business objectives
P.1.1.3	Respond to ISS performance results, prioritize and initiate required actions
P.1.2	Assess benefits/value from ISS investments
P.2	Direct
P.2.1	Oversee the commitment of executive management to protect information assets and make ISS related decisions
P.2.2	Develop and approve the ISS strategy and policy
P.2.3	Allocate investments and resources
P.2.4	Direct organization's risk management program
P.2.4.1	Determine organization's risk appetite
P.2.4.2	Develop risk management policies
P.2.5	Direct resource management and stakeholders communication and reporting
P.2.5.1	Assign responsibilities for resource management
P.2.5.2	Require competent and motivated business and IT personnel
P.2.5.3	Develop escalation guidelines
P.2.5.4	Promote a positive ISS culture
P.2.5.5	Develop reporting and communication principles and guidelines
P.2.5.6	Develop principles for safeguarding resources
P.3	Monitor/Control
P.3.1	Assess the effectiveness of ISS management activities
P.3.1.1	Provide feedback on ISS performance results and their impacts on the organization
P.3.2	Check the compliance with legislation, regulations, contractual obligations and statutory requirements
P.3.2.1	Report to stakeholders the organization's practices for ISS are aligned with the nature of its business
P.3.3	Consider the changing business, legal and regulatory environment and their potential of information risk
P.3.4	Select the metrics for the ISS performance from a business perspective
P.3.5	Provide feedback and transparency over ISS costs, benefits and risks
P.3.6	Commission audits to verify compliance with the level of accountability desired (agreed/ determined) for ISS

CT number	CT definition
AR	Artifacts
AR.1	Information Systems Security strategy
AR.1.1	Decision making model
AR.2	Information Systems Security program
AR.2.1	Investment distribution
AR.2.2	Resource allocation
AR.2.3	Responsibility assignment
AR.3	Information Systems Security policy and guidelines
AR.3.1	Authority levels
AR.3.2	Escalation guidelines
AR.3.3	Reporting and communicating structure
AR.4	Information Systems Security performance program
AR.4.1	Reporting and communicating actions
AR.4.1.1	Stakeholder’s feedback
AR.4.2	Recommended actions to address resource management deviations
AR.4.3	Audit Reports
AR.5	Risk Management program
AR.5.1	Risk assessment
AR.5.2	Risk management policies
AR.5.2.1	Risk tolerance level
AR.5.3	Risk appetite
AR.5.4	Risk mitigation

Concept Tree Version 1 to 2 Matrix

Table 56 – Concept Tree Version 2 against Version 1 (Part 1 – Human Behavioral and Procedural Components)

CT Version 1 CT Version 2		Human behavioral component	Roles	Governing body	Stakeholders	Executive management	Auditors	DPO (GDPR)	Responsibilities	Procedural component	Processes (EDM)	Evaluate	Direct	Monitor/Control	Objectives/purpose	Strategic alignment	Value delivery	Accountability	Needs (balanced)	Organizational structure	Reporting lines	Document communication	ISG integration within the organization	Security culture	Trust	Privacy	Risk program	Risk management	Risk appetite	Risk mitigation	Cost-effective	Effective ISG	Efficient ISG
		H	H.1	H.1.1	H.1.2	H.1.3	H.1.4	H.1.5	H.2	P	P.1	P.1.1	P.1.2	P.1.3	P.2	P.2.1	P.2.2	P.2.3	P.3	P.4	P.4.1	P.4.2	P.4.3	P.5	P.5.1	P.5.2	P.6	P.6.1	P.6.2	P.6.3	P.7	P.8	P.9
G	Goals																																
G.1	Strategic alignment														x	x																	
G.1.1	Balance stakeholders needs																		x														
G.1.2	Integrate ISG within the organization (Holistic approach)																			x			x										
G.2	Value delivery														x		x															x	
G.2.1	Implement/ Favor / Use a cost-effective ISG																														x		
G.2.2	Implement/ Favor/Use an efficient ISG																																x
G.2.3	Resource optimization																																
G.3	Accountability														x			x															
Ag	Agents																																
Ag.1	Governing Body		x	x					x																								
Ag.2	Other Stakeholders		x		x				x																								
Ag.3	Executive Management		x			x			x																								
Ag.4	Auditors		x				x		x																								
Ag.5	Data Protection Officer (DPO)		x					x	x																								

CT Version 1		Human behavioral component	Roles	Governing body	Stakeholders	Executive management	Auditors	DPO (GDPR)	Responsibilities	Procedural component	Processes (EDM)	Evaluate	Direct	Monitor/Control	Objectives/purpose	Strategic alignment	Value delivery	Accountability	Needs (balanced)	Organizational structure	Reporting lines	Document communication	ISG integration within the organization	Security culture	Trust	Privacy	Risk program	Risk management	Risk appetite	Risk mitigation	Cost-effective	Effective ISG	Efficient ISG
CT Version 2		H	H.1	H.1.1	H.1.2	H.1.3	H.1.4	H.1.5	H.2	P	P.1	P.1.1	P.1.2	P.1.3	P.2	P.2.1	P.2.2	P.2.3	P.3	P.4	P.4.1	P.4.2	P.4.3	P.5	P.5.1	P.5.2	P.6	P.6.1	P.6.2	P.6.3	P.7	P.8	P.9
P	Processes																																
P.1	Evaluate										x	x																					
P.1.1	Assess the support of business objectives																																
P.1.2	Assesses the Change management																																
P.1.2.1	Estimates the Capability Maturity Model																																
P.2	Direct										x		x								x	x											
P.2.1	Supervise the Risk Management plan																										x	x					
P.2.1.1	Risk appetite																												x				
P.2.1.2	Risk mitigation																													x			
P.2.2	Oversee the Security Culture																							x									
P.2.2.1	Information security Policies																																
P.2.2.2	Trust concerns																								x								
P.2.2.3	Privacy concerns																									x							
P.2.3	Supervise the Business Continuity plan																																
P.3	Monitor/Control										x			x																			
P.3.1	Compliance with internal and external requirements																																
P.3.2	Apply Performance metrics (KPI's)																																
P.3.2.1	Reports																																
P.3.2.2	Assessments																																
P.3.2.3	Reviews																																
P.3.3	Revise the Physical Document																																

CT Version 1 CT Version 2		Human behavioral component	Roles	Governing body	Stakeholders	Executive management	Auditors	DPO (GDPR)	Responsibilities	Procedural component	Processes (EDM)	Evaluate	Direct	Monitor/Control	Objectives/purpose	Strategic alignment	Value delivery	Accountability	Needs (balanced)	Organizational structure	Reporting lines	Document communication	ISG integration within the organization	Security culture	Trust	Privacy	Risk program	Risk management	Risk appetite	Risk mitigation	Cost-effective	Effective ISG	Efficient ISG
		H	H.1	H.1.1	H.1.2	H.1.3	H.1.4	H.1.5	H.2	P	P.1	P.1.1	P.1.2	P.1.3	P.2	P.2.1	P.2.2	P.2.3	P.3	P.4	P.4.1	P.4.2	P.4.3	P.5	P.5.1	P.5.2	P.6	P.6.1	P.6.2	P.6.3	P.7	P.8	P.9
P.3.3.1	Purpose																																
P.3.3.2	Intended audience																																
P.3.3.3	Review period																																
C	Controls																																
C.1	Audits (independent + objective)																																

Table 57 – Concept Tree Version 2 against Version 1 (Part 2 – Technical and Change Management Components)

CT Version 2	CT Version 1	Technical component	Controls	KPI’ s	Policies	Performance	Support	Compliance	Documentation	Reports	Assessments	Reviews	Audits	Physical Document	Document type/purpose	Targeted audience	Review period	Change management	Business continuity plan	Capability Maturity Model
		T	T.1	T.1.1	T.2	T.3	T.4	T.5	T.6	T.6.1	T.6.2	T.6.3	T.7	T.8	T.8.1	T.8.2	T.8.3	C	C.1	C.2
G	Goals																			
G.1	Strategic alignment																			
G.1.1	Balance stakeholders needs																			
G.1.2	Integrate ISG within the organization (Holistic approach)																			
G.2	Value delivery																			
G.2.1	Implement/ Favor / Use a cost-effective ISG																			
G.2.2	Implement/ Favor/Use an efficient ISG																			
G.2.3	Resource optimization																			
G.3	Accountability																			
Ag	Agents																			
Ag.1	Governing Body																			
Ag.2	Other Stakeholders																			
Ag.3	Executive Management																			
Ag.4	Auditors																			
Ag.5	Data Protection Officer (DPO)																			
P	Processes																			
P.1	Evaluate																			
P.1.1	Assess the support of business objectives						x													
P.1.2	Assesses the Change management																	x		
P.1.2.1	Estimates the Capability Maturity Model																			x
P.2	Direct																			
P.2.1	Supervise the Risk Management plan																			

CT Version 2	CT Version 1	Technical component	Controls	KPI’ s	Policies	Performance	Support	Compliance	Documentation	Reports	Assessments	Reviews	Audits	Physical Document	Document type/purpose	Targeted audience	Review period	Change management	Business continuity plan	Capability Maturity Model
		T	T.1	T.1.1	T.2	T.3	T.4	T.5	T.6	T.6.1	T.6.2	T.6.3	T.7	T.8	T.8.1	T.8.2	T.8.3	C	C.1	C.2
P.2.1.1	Risk appetite																			
P.2.1.2	Risk mitigation																			
P.2.2	Oversee the Security Culture																			
P.2.2.1	Information security Policies				x															
P.2.2.2	Trust concerns																			
P.2.2.3	Privacy concerns																			
P.2.3	Supervise the Business Continuity plan																		x	
P.3	Monitor/Control		x			x														
P.3.1	Compliance with internal and external requirements							x												
P.3.2	Apply Performance metrics (KPI’s)			x																
P.3.2.1	Reports								x	x										
P.3.2.2	Assessments								x		x									
P.3.2.3	Reviews								x			x								
P.3.3	Revise the Physical Document													x						
P.3.3.1	Purpose														x					
P.3.3.2	Intended audience															x				
P.3.3.3	Review period																x			
C	Controls																			
C.1	Audits (independent + objective)												x							

Concept Tree Version 2 to 5 Comparison

Table 58 – Concept Tree Versions 2 to 5 Comparison

V2		V3		V4		V5	
G	Goals	G	Goals	G	Goals	G	Goals
G.1	Strategic alignment	G.1	Strategic alignment	G.1	Strategic alignment	G.1	Strategic alignment
G.1.1	Balance stakeholders needs	G.1.1	Balance stakeholders needs	G.1.1	Balancing stakeholders needs	G.1.1	Balancing stakeholders needs
G.1.2	Integrate ISG within the organization (Holistic approach)	G.1.2	Integrate ISG within the organization (Holistic approach)	G.1.2	ISG integration within the organization (Holistic approach)	G.1.2	ISSG integration within the organization (Holistic approach)
G.2	Value delivery	G.2	Value delivery	G.2	Value delivery	G.2	Value delivery
G.2.1	Implement/ Favor / Use a cost-effective ISG	G.2.1	ISG cost-effectiveness	G.2.1	ISG cost-effectiveness	G.2.1	ISSG cost-effectiveness
G.2.2	Implement/ Favor/Use an efficient ISG	G.2.2	ISG efficiency	G.2.2	ISG efficiency	G.2.2	ISSG efficiency
				G.2.2.1	IT-agility		
G.2.3	Resource optimization	G.2.3	Resource optimization	G.2.3	Resource, assets and capabilities optimization		
G.3	Accountability	G.3	Accountability	G.3	Accountability	G.3	Accountability
		G.4	Compliance	G.4	Compliance	G.4	Compliance
Ag	Agents	Ag	Agents	Ag	Agents	Ag	Agents
Ag.1	Governing Body	Ag.1	Governing Body	Ag.1	Governing Body	Ag.1	Governing Body
Ag.2	Other Stakeholders	Ag.2	Executive Management	Ag.2	Executive Management	Ag.2	Executive Management
Ag.3	Executive Management	Ag.3	Auditors	Ag.3	Auditors	Ag.3	Auditors
Ag.4	Auditors	Ag.4	Data Protection Officer (DPO)	Ag.4	Data Protection Officer (DPO)	Ag.4	Data Protection Officer (DPO)
Ag.5	Data Protection Officer (DPO)	Ag.5	Employees	Ag.5	Chief Information Security Officer (CISO)	Ag.5	Chief Information Security Officer (CISO)
		Ag.6	Senior Agency Information Security Officer (SAISO)	Ag.6	Employees	Ag.6	Employees
		Ag.7	Other Stakeholders (Customers, user, suppliers, partners)	Ag.7	Other Stakeholders (Customers, user, suppliers, partners)	Ag.7	Other Stakeholders (Customers, user, suppliers, partners)
P	Processes	P	Processes	P	Processes	P	Processes
P.1	Evaluate	P.1	Evaluate	P.1	Evaluate	P.1	Evaluate
		P.1.1	Assess the alignment of ISS to business strategy	P.1.1	Assess the alignment of ISS to business strategy	P.1.1	Assess the alignment of ISS to business strategy

V2		V3		V4		V5	
		P.1.1.1	Ensure business initiatives takes into account information security issues	P.1.1.1	Verify that business initiatives takes into account information security issues	P.1.1.1	Verify that business initiatives takes into account ISS issues
P.1.1	Assess the support of business objectives	P.1.1.2	Ensure that information security adequately supports and sustains the business objectives	P.1.1.2	Verify that information security supports and sustains the business objectives	P.1.1.2	Verify that ISS supports and sustains the business objectives
P.1.2	Assesses the Change management	P.1.1.3	Respond to information security performance results, prioritize and initiate required actions	P.1.1.3	Respond to information security performance results, prioritize and initiate required actions	P.1.1.3	Respond to ISS performance results, prioritize and initiate required actions
P.1.2.1	Estimates the Capability Maturity Model	P.1.2	Realize benefits/value from information security investments	P.1.2	Assess benefits/value from information security investments	P.1.2	Assess benefits/value from ISS investments
P.2	Direct	P.2	Direct	P.2	Direct	P.2	Direct
		P.2.1	Ensure the commitment of executive management to protect information assets and make information security related decisions	P.2.1	Oversee the commitment of executive management to protect information assets and make information security related decisions	P.2.1	Oversee the commitment of executive management to protect information assets and make ISS related decisions
		P.2.2	Develop and approve the information security strategy and policy	P.2.2	Develop and approve the information security strategy and policy	P.2.2	Develop and approve the ISS strategy and policy
		P.2.3	Allocate adequate investments and resources	P.2.3	Allocate investments and resources	P.2.3	Allocate investments and resources
		P.2.3.1	Ensure it-agility				
		P.2.3.2	Ensure optimization of IT assets, resources and capabilities				
P.2.1	Supervise the Risk Management plan	P.2.4	Direct organization’s risk management	P.2.4	Direct organization’s risk management	P.2.4	Direct organization’s risk management program
P.2.1.1	Risk appetite	P.2.4.1	Determine organization’s risk appetite	P.2.4.1	Determine organization’s risk appetite	P.2.4.1	Determine organization’s risk appetite
P.2.1.2	Risk mitigation	P.2.4.2	Develop risk management policies	P.2.4.2	Develop risk management policies	P.2.4.2	Develop risk management policies
		P.2.5	Direct resource management and stakeholders communication and reporting	P.2.5	Direct resource management and stakeholders communication and reporting	P.2.5	Direct resource management and stakeholders communication and reporting
		P.2.5.1	Assign responsibilities for resource management	P.2.5.1	Assign responsibilities for resource management	P.2.5.1	Assign responsibilities for resource management
		P.2.5.2	Ensure competent and motivated business and IT personnel	P.2.5.2	Require competent and motivated business and IT personnel	P.2.5.2	Require competent and motivated business and IT personnel
		P.2.5.3	Develop escalation guidelines	P.2.5.3	Develop escalation guidelines	P.2.5.3	Develop escalation guidelines
P.2.2	Oversee the Security Culture	P.2.5.4	Promote a positive information security culture	P.2.5.4	Promote a positive information security culture	P.2.5.4	Promote a positive ISS culture
P.2.2.1	Information security Policies	P.2.5.5	Develop reporting and communication principles and guidelines	P.2.5.5	Develop reporting and communication principles and guidelines	P.2.5.5	Develop reporting and communication principles and guidelines

V2		V3		V4		V5	
P.2.2.2	Trust concerns	P.2.5.6	Develop principles for safeguarding resources	P.2.5.6	Develop principles for safeguarding resources	P.2.5.6	Develop principles for safeguarding resources
P.2.2.3	Privacy concerns						
P.2.3	Supervise the Business Continuity plan						
P.3	Monitor/Control	P.3	Monitor/Control	P.3	Monitor/Control	P.3	Monitor/Control
		P.3.1	Assess the effectiveness of information security management activities	P.3.1	Assess the effectiveness of information security management activities	P.3.1	Assess the effectiveness of ISS management activities
		P.3.1.1	Provide feedback on information security performance results and their impacts on the organization	P.3.1.1	Provide feedback on information security performance results and their impacts on the organization	P.3.1.1	Provide feedback on ISS performance results and their impacts on the organization
P.3.1	Compliance with internal and external requirements	P.3.2	Check the compliance with legislation, regulations, contractual obligations and statutory requirements	P.3.2	Check the compliance with legislation, regulations, contractual obligations and statutory requirements	P.3.2	Check the compliance with legislation, regulations, contractual obligations and statutory requirements
		P.3.2.1	Report to external stakeholders that the organization practices a level of information security commensurate with the nature of its business	P.3.2.1	Report to stakeholders the organization's practices for information security are aligned with the nature of its business	P.3.2.1	Report to stakeholders the organization's practices for ISS are aligned with the nature of its business
		P.3.3	Consider the changing business, legal and regulatory environment and their potential of information risk	P.3.3	Consider the changing business, legal and regulatory environment and their potential of information risk	P.3.3	Consider the changing business, legal and regulatory environment and their potential of information risk
P.3.2	Apply Performance metrics (KPI's)	P.3.4	Select appropriate information security performance metrics from business perspective	P.3.4	Select the metrics for the information security performance from a business perspective	P.3.4	Select the metrics for the ISS performance from a business perspective
P.3.2.1	Reports	P.3.5	Feedback on transparency of IT costs, benefits and risks	P.3.5	Provide feedback on transparency of IT costs, benefits and risks	P.3.5	Provide feedback and transparency over ISS costs, benefits and risks
P.3.2.2	Assessments	P.3.6	Commission independent and objective opinion (audits) of how it is complying with its accountability for the desired level of information security	P.3.6	Commission audits to verify compliance with the level of accountability desired (agreed/ determined) for information security	P.3.6	Commission audits to verify compliance with the level of accountability desired (agreed/ determined) for ISS
P.3.2.3	Reviews						
P.3.3	Revise the Physical Document						
P.3.3.1	Purpose						
P.3.3.2	Intended audience						
P.3.3.3	Review period						
C	Controls	AR	Artifacts	AR	Artifacts	AR	Artifacts
		AR.1	Produce the Information Systems Security strategy	AR.1	Produce the Information Systems Security strategy	AR.1	Information Systems Security strategy
		AR.1.1	Decision making model	AR.1.1	Elaborate a Decision making model	AR.1.1	Decision making model
		AR.2	Create an Information Systems Security program	AR.2	Create an Information Systems Security program	AR.2	Information Systems Security program

V2		V3		V4		V5	
		AR.2.1	Investment distribution	AR.2.1	Contemplate the Investment distribution	AR.2.1	Investment distribution
		AR.2.2	Resource allocation	AR.2.2	Contemplate the Resource allocation	AR.2.2	Resource allocation
		AR.2.3	Responsibility assignment	AR.2.3	Contemplate the Responsibility assignment	AR.2.3	Responsibility assignment
		AR.3	Develop an Information Systems Security policy and guidelines	AR.3	Develop an Information Systems Security policy and guidelines	AR.3	Information Systems Security policy and guidelines
		AR.3.1	Authority levels	AR.3.1	Covering Authority levels	AR.3.1	Authority levels
		AR.3.2	Escalation guidelines	AR.3.2	Covering Escalation guidelines	AR.3.2	Escalation guidelines
		AR.3.3	Reporting and communicating structure	AR.3.3	Covering the Reporting and communicating structure	AR.3.3	Reporting and communicating structure
		AR.4	Create an Information Systems Security performance program	AR.4	Create an Information Systems Security performance program	AR.4	Information Systems Security performance program
		AR.4.1	Reporting and communicating	AR.4.1	Contemplate the Reporting and communicating actions	AR.4.1	Reporting and communicating actions
		AR.4.1.1	Stakeholder's feedback	AR.4.1.1	Stakeholder's feedback	AR.4.1.1	Stakeholder's feedback
		AR.4.1.1.1	Governance effectiveness				
		AR.4.1.1.2	Risk Management issues				
		AR.4.2	Recommended actions to address resource management deviations	AR.4.2	Recommended actions to address resource management deviations	AR.4.2	Recommended actions to address resource management deviations
C.1	Audits (independent + objective)	AR.4.3	Audit Reports	AR.4.3	Contemplate Audit Reports	AR.4.3	Audit Reports
		AR.5	Create a Risk Management program	AR.5	Create a Risk Management program	AR.5	Risk Management program
		AR.5.1	Risk assessment	AR.5.1	Regarding Risk assessment	AR.5.1	Risk assessment
		AR.5.2	Risk policies	AR.5.2	Regarding Risk policies	AR.5.2	Risk management policies
		AR.5.2.1	Risk tolerance level	AR.5.2.1	Risk tolerance level	AR.5.2.1	Risk tolerance level
		AR.5.3	Risk appetite	AR.5.3	Regarding Risk appetite	AR.5.3	Risk appetite
		AR.5.4	Risk mitigation	AR.5.4	Regarding Risk mitigation	AR.5.4	Risk mitigation

Appendix J – Artifact Construction: Instrument

Within this appendix, one will discover the matrixes for the respective version of the concept tree with the respective questions from their counterpart instrument version, followed by the version of the Instrument in question.

The appendix starts out with Table 59 that presents the differences, in the document structure, between instrument versions. Followed by two matrices, for the V0 of the instrument. The first one links the V0 to the GTAG questions (which is used as a base). While the second matrix, links the V0 with the concepts of concept tree v1. Subsequently, the instrument V0 is displayed.

Then the appendix progresses to elucidate the creation of the V1 of the instrument, which is composed by another two matrices; the initial matrix (split into Table 62 and Table 63) links V1 with the concept tree v4 (exposing the connection strength between questions and concepts, displayed with a red D for direct or an blue i for indirect); and another that links the questions of V1 to their counterparts in V0. Only after these matrices are presented is the V1 of the instrument displayed.

For the next versions of the instrument, V2 to V4, the manner in which their elements are displayed possesses the same structure. This structure is comprised by a matrix, that links the version of the instrument in question (either V2, V3 or V4) to the v4 of the concept tree. Followed by the instrument version (which could also be either V2, V3 or V4) that was created.

Finally, the last version of the instrument, V5, also presents a matrix; which, in this case, links the instrument V5 questions to the concept tree V5. Then, a table displaying the evolution of the instrument questions is presented. Lastly, the fifth and final version of the instrument is displayed.

As mentioned above, Table 73, compares the questions from versions 2 thru 5 of the instrument. The changes observed are highlighted in different colors: in a blue background, for questions that suffered modifications (such as grammar or context) in the following version; in a yellow background, for questions that switched location in the following version; and in an orange background, for questions that were removed from the following version.

Also, within the Table, there were another two types of highlight. The first was words or parts of the question, using a red lettering; those represented the parts that were modified in the question. The second was a green background, on the right side of the question, which represented the new questions numbers (for the questions that were split) in the following version.

Table 59 – Instrument Versions Document Structure

Instrument		Concept Tree Version	Relevant Documents	Table
Version	Total of questions			
V0	46	CT1	GTAG® 15	59 & 60
V0 x V1	-	-	-	63
V1	47	CT4	COBIT® 5	61 & 62
V2	78			64 &65
V3	83			66 & 67
V4	83			68 & 69
V5	84	CT5	COBIT® 2019	70 & 71

- Matrix for Instrument V0 and GTAG® 15 Questions

Table 60 – Instrument V0 and GTAG® 15 Questions Matrix

SQ0 GTAG	1	2	3	3.1	4	5	6	7	8	9	10	11	12	13	14	15	16	a)	17	18	19	20	a)	21	a)	22	23	a)	24	25	26	a)	27	a)	28	29	30	31	a)	b)	c)	32	a)	b)
4.1.1.																																												
1												x																																
2																																												
3																																												
4																																												
5															x																													
6																x																												
7																	x																											
8																																												
9																		x																										
10																																												
4.1.2.																																												
1					x																																							
2							x																																					
3								x																																				
4									x																																			
5										x																																		
4.1.3.																																												
1																						x																						
2																							x																					
3																																												
4																									x																			
5																											x																	
4.1.4.																																												
1																			x																									

SQO GTAG	1	2	3	3.1	4	5	6	7	8	9	10	11	12	13	14	15	16	a)	17	18	19	20	a)	21	a)	22	23	a)	24	25	26	a)	27	a)	28	29	30	31	a)	b)	c)	32	a)	b)
2																																												
3																				x																								
4																					x																							
4.1.5 .																																												
1																								x																				
2																										x																		
3																												x																
4																																												
4.1.6 .																																												
1																														x														
2																															x													
3																																	x											
4																																												
5																																			x									
6																																				x								
7																																x												
8																																												
9																																												
10																																		x										
11																																												
12																																												

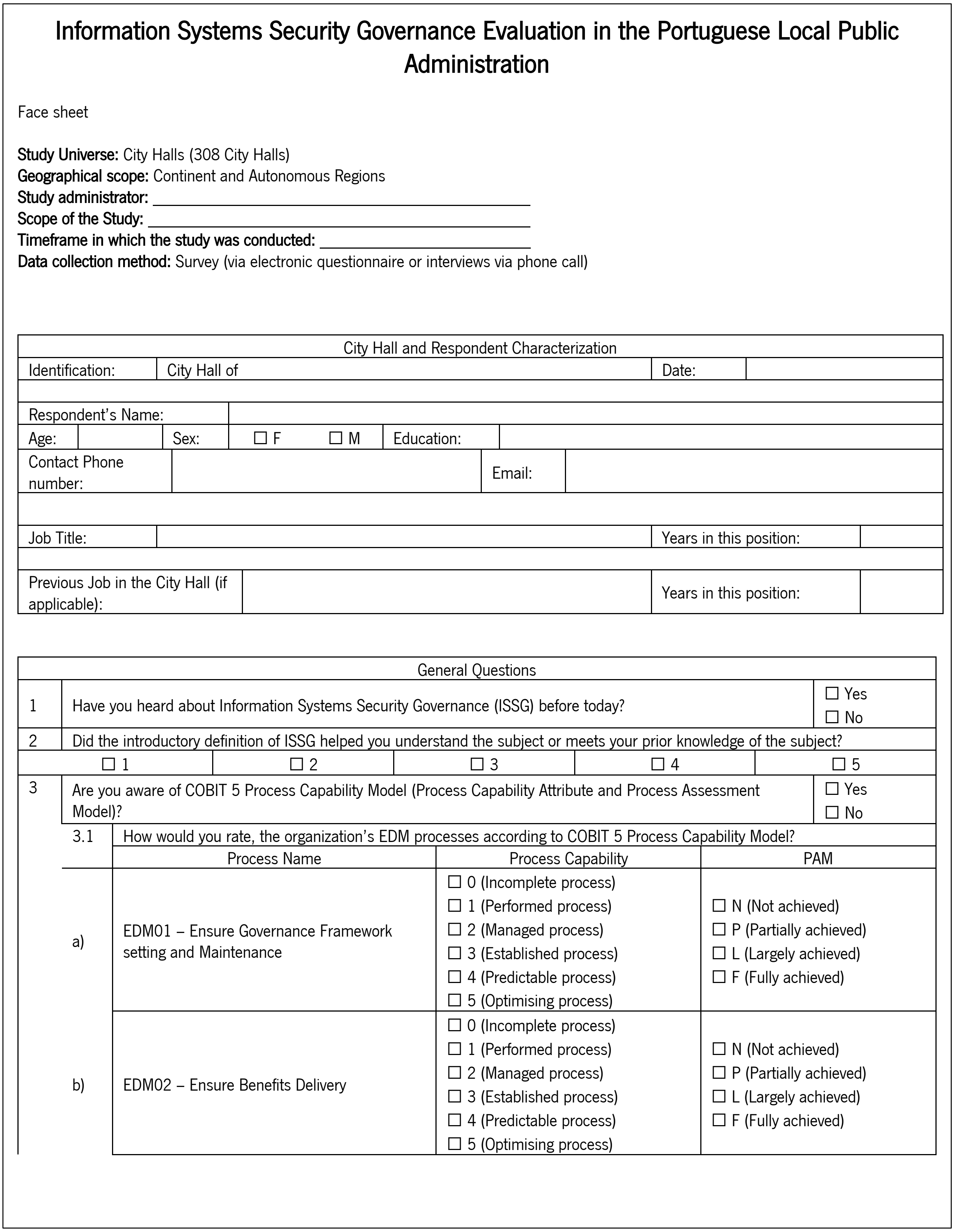
- Matrix for Instrument v0 and Concept Tree Version 1

Table 61 – Instrument V0 and Concept Tree V1 Matrix

SQ0 CT1	1	2	3	3.1	a)	b)	c)	d)	e)	4	5	6	7	8	9	10	11	12	13	14	15	16	a)	17	18	19	20	a)	21	a)	22	23	a)	24	25	26	a)	27	a)	28	29	30	31	a)	b)	c)	32	a)	b)
H																																																	
H.1										x							x				x	x	x															x				x							x
H.1.1																																																	
H.1.2																																																	
H.1.3																																																	
H.1.4																																																	
H.1.5																																																	
H.2	x	x								x							x					x		x													x												
P																																																	
P.1				x	x	x	x	x	x																																								
P.1.1				x	x	x	x	x	x																																								
P.1.2				x	x	x	x	x	x																																								
P.1.3				x	x	x	x	x	x																																								
P.2											x	x																																					
P.2.1											x	x																																					
P.2.2																													x																				
P.2.3																		x				x																											
P.3																																																	
P.4																			x	x	x			x																									
P.4.1																			x	x				x								x																	
P.4.2																						x		x																									x
P.4.3																													x		x						x	x	x				x					x	
P.5	x	x																																															
P.5.1																																																	
P.5.2																																																	
P.6																																																	
P.6.1																									x									x					x										
P.6.2																																																	
P.6.3																																																	

SQ0 CT1	1	2	3	3.1	a)	b)	c)	d)	e)	4	5	6	7	8	9	10	11	12	13	14	15	16	a)	17	18	19	20	a)	21	a)	22	23	a)	24	25	26	a)	27	a)	28	29	30	31	a)	b)	c)	32	a)	b)
P.7													x																																				
P.8																x														x																			
P.9																																																	
T																																																	
T.1																																																	
T.1.1																																																	
T.2														x	x									x										x	x												x	x	x
T.3																																																	
T.4													x															x																				x	
T.5	x													x	x											x									x	x		x	x	x	x	x	x	x	x	x		x	
T.6																											x																						
T.6.1																																																	
T.6.2																																																	
T.6.3																																	x			x					x								
T.7																																																	
T.8																																																	
T.8.1																																																	
T.8.2																																																	
T.8.3																																																	
C																																																	
C.1																																																	
C.2			x	x	x	x	x	x	x																																								

- Instrument v0



Information Systems Security Governance Evaluation in the Portuguese Local Public Administration

Face sheet

Study Universe: City Halls (308 City Halls)
Geographical scope: Continent and Autonomous Regions
Study administrator: ____
Scope of the Study: ____
Timeframe in which the study was conducted: ____________________
Data collection method: Survey (via electronic questionnaire or interviews via phone call)

City Hall and Respondent Characterization						
Identification:	City Hall of				Date:	
Respondent's Name:						
Age:		Sex:	□ F □ M	Education:		
Contact Phone number:				Email:		
Job Title:					Years in this position:	
Previous Job in the City Hall (if applicable):					Years in this position:	

General Questions					
1	Have you heard about Information Systems Security Governance (ISSG) before today?				□ Yes □ No
2	Did the introductory definition of ISSG helped you understand the subject or meets your prior knowledge of the subject?				
□ 1	□ 2	□ 3	□ 4	□ 5	
3	Are you aware of COBIT 5 Process Capability Model (Process Capability Attribute and Process Assessment Model)?				□ Yes □ No
	3.1	How would you rate, the organization's EDM processes according to COBIT 5 Process Capability Model?			
		Process Name	Process Capability	PAM	
	a)	EDM01 – Ensure Governance Framework setting and Maintenance	□ 0 (Incomplete process) □ 1 (Performed process) □ 2 (Managed process) □ 3 (Established process) □ 4 (Predictable process) □ 5 (Optimising process)	□ N (Not achieved) □ P (Partially achieved) □ L (Largely achieved) □ F (Fully achieved)	
	b)	EDM02 – Ensure Benefits Delivery	□ 0 (Incomplete process) □ 1 (Performed process) □ 2 (Managed process) □ 3 (Established process) □ 4 (Predictable process) □ 5 (Optimising process)	□ N (Not achieved) □ P (Partially achieved) □ L (Largely achieved) □ F (Fully achieved)	

Figure 23 – Instrument Version 0

c)	EDM03 – Ensure Risk Optimisation	☐ 0 (Incomplete process) ☐ 1 (Performed process) ☐ 2 (Managed process) ☐ 3 (Established process) ☐ 4 (Predictable process) ☐ 5 (Optimising process)	☐ N (Not achieved) ☐ P (Partially achieved) ☐ L (Largely achieved) ☐ F (Fully achieved)
d)	EDM04 – Ensure Resource Optimisation	☐ 0 (Incomplete process) ☐ 1 (Performed process) ☐ 2 (Managed process) ☐ 3 (Established process) ☐ 4 (Predictable process) ☐ 5 (Optimising process)	☐ N (Not achieved) ☐ P (Partially achieved) ☐ L (Largely achieved) ☐ F (Fully achieved)
e)	EDM05 – Ensure Stakeholder Transparency	☐ 0 (Incomplete process) ☐ 1 (Performed process) ☐ 2 (Managed process) ☐ 3 (Established process) ☐ 4 (Predictable process) ☐ 5 (Optimising process)	☐ N (Not achieved) ☐ P (Partially achieved) ☐ L (Largely achieved) ☐ F (Fully achieved)

Strategic Planning (Purpose and Objective)		
4	Are roles and responsibilities for the Information System (IS) activity formally defined?	☐ Yes ☐ No
5	Are the objectives and strategies of ISG well described and defined?	☐ Yes ☐ No
6	How are business unit and/or individual performance objectives tied to IS objectives? Do they support the IS activity?	☐ Yes ☐ No
7	Does each component of the ISG structure have sufficient capital and operating expense budgets to support IS efforts?	☐ Yes ☐ No
8	Are procedures in place to oversee IS incidents including public and investor relations and coordination with law enforcement?	☐ Yes ☐ No
9	Are IS policies supported by written standards? Are the standards supported by written procedures?	☐ Yes ☐ No
10	Does your organization have a ISS program? And Is it in effect/implemented?	☐ Yes ☐ No

Organizational Structure		
11	Who is formally responsible for IS?	☐ Governing body ☐ Executive management ☐ Data Protection Officer ☐ In-line Manager ☐ None of the above
12	Who is accountable for the ISS program in the organization?	☐ Governing body ☐ Executive management ☐ Data Protection Officer ☐ In-line Manager ☐ None of the above
13	To whom does this person formally report?	☐ Stakeholders ☐ Governing body ☐ Executive management ☐ Data Protection Officer ☐ In-line Manager ☐ None of the above

14		Are there any committee functions, boards or other groups that IS staff regularly reports to either on an informal basis or a more formal steering function?	☐ Yes ☐ No	
15		What is the career level of the person in charge of IS? Is this an officer-level position or a managerial position? Does this individual have other roles?	☐ Officer ☐ Managerial	☐ Yes ☐ No
16		Are roles and responsibilities, accountability, and performance for all IS responsibilities formally defined?	☐ Yes ☐ No	
	a)	Is the CISO driving the IS activity or mostly reporting compliance?	☐ Driving ☐ Compliance	

Roles and Responsibilities (Risk appetite)		
17	Under what circumstances does the board need to be engaged?	
18	What are the IS risks that the board would deem unacceptable?	
19	How often is this criteria reviewed?	☐ less than 1 year ☐ between 1 and 2 years ☐ more than 2 years

Enterprise Architecture (Document communication – reporting lines)/ (ISG integration)			
20		What information exchanges are formally defined?	
	a)	Are they sufficient?	☐ Yes ☐ No
21		Is IS a consideration in the organization's IT strategy?	☐ Yes ☐ No
	a)	Is IS a consideration in other business units strategy, processes, and procedures? Has the IS activity added value?	☐ Yes ☐ No
22		Does the IS activity get effective/meaningful feedback from the groups it works with?	☐ Yes ☐ No
23		What is the escalation path that IS news/alerts must follow?	
	a)	Is there a formal meeting schedule?	☐ Yes ☐ No
24		Does the organization has a risk management plan, process, procedure, policy?	☐ Yes ☐ No

Policies and Guidance (external influences)				
25		What regulations, laws, and contractual requirements apply to the organization?		
26		How often, and when, were regulations last reviewed to understand IS requirements? Is the legal department involved in the review, or is interpretation left to non-legal staff?	☐ less than 1 year ☐ between 1 and 2 years ☐ more than 2 years	☐ Yes ☐ No
	a)	Does legal counsel consult with the IS activity to assess requirements during the contract process?	☐ Yes ☐ No	
27		Is there an internal or external regulatory compliance group, and when did the IS activity last meet with them?	☐ Yes ☐ No	☐ less than 1 year ☐ between 1 and 2 years ☐ more than 2 years
	a)	What legal environment issues affect ISG and why?		
28		What contracts have IS components?		
29		When did the IS activity last review contractual requirements with legal counsel?	☐ less than 1 year ☐ between 1 and 2 years ☐ more than 2 years	

30	Does de City Hall has a designated data protection officer?			☐ Yes ☐ No
31	To what extent is the City Hall IS compliant with legislations, regulations, security policies and rules? (1 – non-compliant and 5 – completely compliant)			
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
	a)	Is the City Hall aware of the GDPR?		☐ Yes ☐ No
	b)	Was the City Hall aware of the *PGETIC*?		☐ Yes ☐ No
	c)	Is the City Hall aware of the *Estratégia 2020*?		☐ Yes ☐ No
32	Does your organization has a ISS policy?			☐ Yes ☐ No
	a)	How would you evaluate the coverage (clarity, subject, policies, reporting lines, responsibilities) of the ISS program?		☐ Poorly covered ☐ Sufficiently covered ☐ Very well covered
	b)	Is the ISS policy available and to whom?	☐ Only to organization's employees ☐ To organization's employees and contractors ☐ Is available to everyone with clearance ☐ Is available to everyone	

- Matrix for Instrument v1 and Concept Tree v4

Table 62 – Matrix Instrument v1 and Concept Tree 4 (Part 1)

CT4 SQ1	G	G.1	G.1.1	G.1.2	G.2	G.2.1	G.2.2	G.2.2.1	G.2.3	G.3	G.4	Ag	Ag.1	Ag.2	Ag.3	Ag.4	Ag.5	Ag.6	Ag.7	P	P.1	P.1.1	P.1.1.1	P.1.1.2	P.1.1.3	P.1.2	P.2	P.2.1	P.2.2	P.2.3	P.2.4	P.2.4.1	P.2.4.2
1				i																		i											
2		D			i																		i	i									
3				D		D																		i									
3a		i																						D									
4				i			i	i															D										
4a				D			D	D															D	i						i			
5							i		i															D		i				D			
6					D																					D							
7																																	
8				D			i		i															D	i	i							
9					i	i																		i	i	D		i			i		
10					i					i	i																	D			i		
11										D		i																					
12				i	i					D		i																					
13												D																i					
13a												D																D					
14																																	
15												D																i					
15a									i	i		D																i					
15b									D	i		i																		D			
16									D	i							D											D					
17											D	i																					
18				i			i				D																		i				
19											i																						
19a				i			i																					i					
20											D												i										
21											i												D										
21a										D		D											i	i					i				
22										i	D	i											i						i				

CT4 SQ1	G	G.1	G.1.1	G.1.2	G.2	G.2.1	G.2.2	G.2.2.1	G.2.3	G.3	G.4	Ag	Ag.1	Ag.2	Ag.3	Ag.4	Ag.5	Ag.6	Ag.7	P	P.1	P.1.1	P.1.1.1	P.1.1.2	P.1.1.3	P.1.2	P.2	P.2.1	P.2.2	P.2.3	P.2.4	P.2.4.1	P.2.4.2
22a				i			i			D	D	i												D					i				
23										i	D	i													i			i					
23a			i	i			i				D	i																					
23b							i				D																						
24							i		i	D	D	i			D								i	i				i					
25				D		i																	i					i					
25a				i						i	i													i								i	
26				D							i												D										
26a										i	i	D																					
27										i	D	i																					
28				i			i				D												i	i									
28a				i	i					D	D	i				D							i	i									
29				i						i	D												i	i									
29a				i	i					i	D												i	i									
30							i			D	D	D																i					
31											i	D											i	i		i							
32		i			i					i	D	D																D					
32a				i	i					D	D	i											D	D									

Table 63 – Matrix Instrument v1 and Concept Tree 4 (Part 2)

CT4 SQ1	P.2.5	P.2.5.1	P.2.5.2	P.2.5.3	P.2.5.4	P.2.5.5	P.2.5.6	P.3	P.3.1	P.3.1.1	P.3.2	P.3.2.1	P.3.3	P.3.4	P.3.5	P.3.6	AR	AR.1	AR.1.1	AR.2	AR.2.1	AR.2.2	AR.2.3	AR.3	AR.3.1	AR.3.2	AR.3.3	AR.4	AR.4.1	AR.4.1.1	AR.4.2	AR.4.3	AR.5	AR.5.1	AR.5.2	AR.5.2.1	AR.5.3	AR.5.4
1																				D																		
2																		D	i																			
3										i				i														i										
3a									i				i							i																		
4											i	i	i																									
4a			i		i								D		i						i	i							i									
5															i						D	D									i							
6									i																													
7									D	D					i				i										D	i	i	i						
8									i	i				D	i																							
9	i								D	i																												
10									D		i	i										i	i	D					D	D		i	i					
11	i	D																					D	i					i	i			i					
12		i		i		i	i																D	D					i	i								
13	D																			D				i				i					i					
13a																							i	i						i								
14						i																					D		i	i								
15			D																			i	i		i													
15a			D																			i	i		i													
15b																						D																
16																i													i	i								
17				i		i				i																D	D		i	i	i							
18											D	i	i											D	i	i	i				i		i					
19										i														D	i	i	D											
19a						i																		D	i	i	i											
20											D	i	i			i								i								i						
21											i	i	D																									
21a											D	i	i			i																						
22											i	i	i						i				i															
22a													i		i				i																			
23											D	D			i	i			i							D	D		D	D								
23a																																	D					
23b									D	D	D	i																										

CT4 SQ1	P.2.5	P.2.5.1	P.2.5.2	P.2.5.3	P.2.5.4	P.2.5.5	P.2.5.6	P.3	P.3.1	P.3.1.1	P.3.2	P.3.2.1	P.3.3	P.3.4	P.3.5	P.3.6	AR	AR.1	AR.1.1	AR.2	AR.2.1	AR.2.2	AR.2.3	AR.3	AR.3.1	AR.3.2	AR.3.3	AR.4	AR.4.1	AR.4.1.1	AR.4.2	AR.4.3	AR.5	AR.5.1	AR.5.2	AR.5.2.1	AR.5.3	AR.5.4
24											i	i				i														i	i	i						
25																				D	i	i	i															
25a		i			i										i					i				i				i					i					
26																								D	i	i	i											
26a																								D	i	i	i											
27											D	i	i			i																						
28											D	i	i																									
28a											D	i	i																									
29											D	i	i							i																		
29a											D	i	i							i																		
30											D	i	i					D	i	D				D				D					D					
31											D	i																										
32											D	i			i			i	i												i							
32a									D	i	D	i			i			i													i							

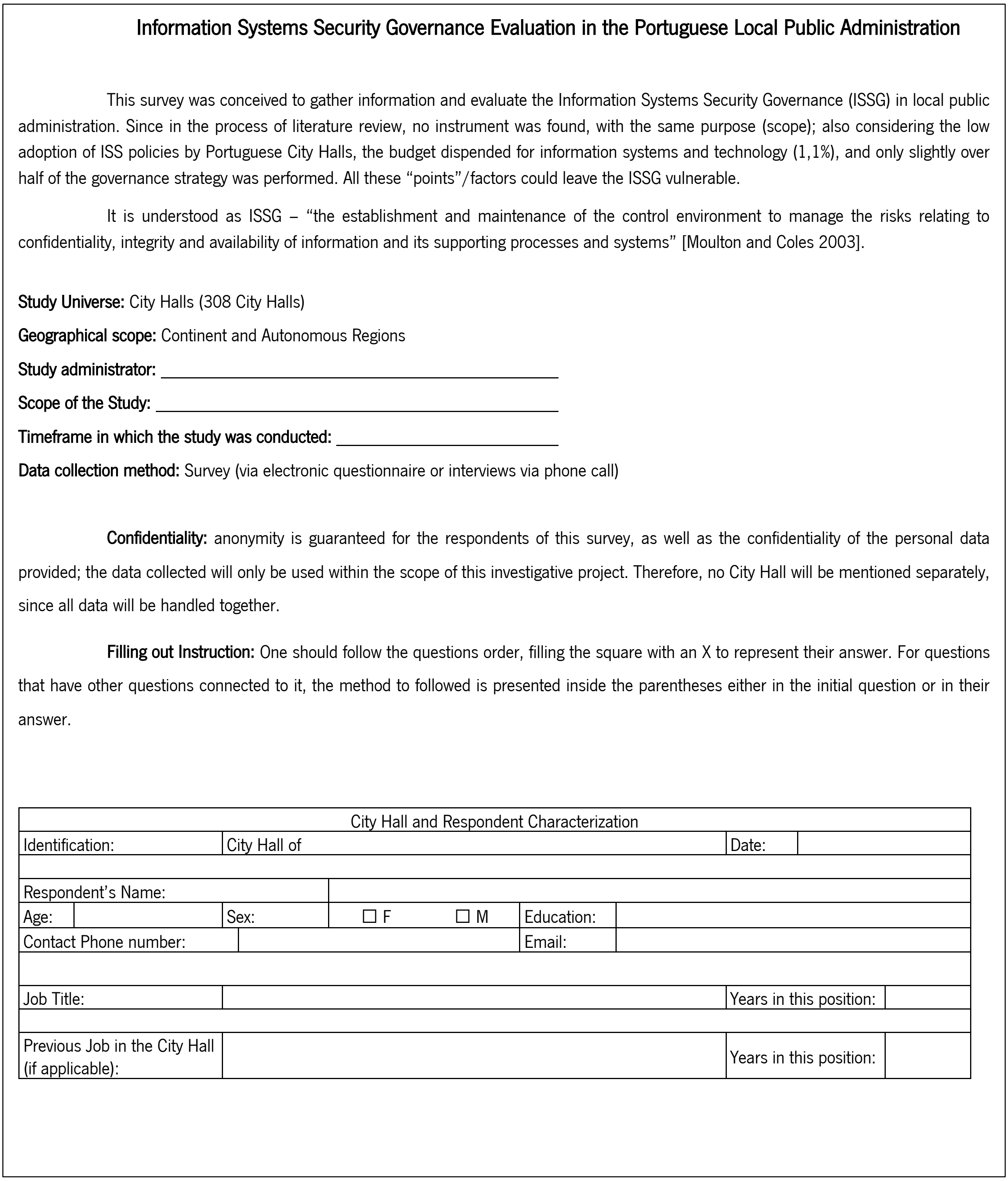
- Matrix for Instrument v1 Questions and Instrument v0 Questions

Table 64 – Instrument v1 and Instrument v0 Questions Matrix

V1/V0	1	2	3	a)	4	a)	5	6	7	8	9	10	11	12	13	a)	14	15	a)	b)	16	17	18	19	a)	20	21	a)	22	a)	23	a)	b)	24	25	a)	26	a)	27	28	a)	29	a)	30	31	32	a)
1																																												x			
2																																													x		
3																																														x	
3.1																																															x
a)																																															x
b)																																															x
c)																																															x
d)																																															x
e)																																															x
4													x																																		
5		x																																													
6			x	x																																											
7							x																																								
8												x																																			
9																							x																								
10	x																																														
11															x																																
12															x																																
13																x																															
14																	x																														
15																		x	x	x																											
16														x																																	
a)																					x																										
17																															x																
18																																x															
19																																	x														
20																								x																							
a)																									x																						
21						x																																									

V1 / V0	1	2	3	a)	4	a)	5	6	7	8	9	10	11	12	13	a)	14	15	a)	b)	16	17	18	19	a)	20	21	a)	22	a)	23	a)	b)	24	25	a)	26	a)	27	28	a)	29	a)	30	31	32	a)
a)					x			x																																							
22									x																																						
23																						x																									
a)																																															
24																																															
25																										x																					
26																											x	x																			
a)																														x																	
27																																		x													
a)																																															
28																																															
29																													x																		
30																																									x						
31																																							x								
a)																																								x							
b)																																										x					
c)																																											x				
32																																					x										
a)																																				x											
b)																																						x									

- Instrument v1



Information Systems Security Governance Evaluation in the Portuguese Local Public Administration

This survey was conceived to gather information and evaluate the Information Systems Security Governance (ISSG) in local public administration. Since in the process of literature review, no instrument was found, with the same purpose (scope); also considering the low adoption of ISS policies by Portuguese City Halls, the budget dispended for information systems and technology (1,1%), and only slightly over half of the governance strategy was performed. All these "points"/factors could leave the ISSG vulnerable.

It is understood as ISSG – "the establishment and maintenance of the control environment to manage the risks relating to confidentiality, integrity and availability of information and its supporting processes and systems" [Moulton and Coles 2003].

Study Universe: City Halls (308 City Halls)

Geographical scope: Continent and Autonomous Regions

Study administrator: ____

Scope of the Study: ____

Timeframe in which the study was conducted: ______________________

Data collection method: Survey (via electronic questionnaire or interviews via phone call)

Confidentiality: anonymity is guaranteed for the respondents of this survey, as well as the confidentiality of the personal data provided; the data collected will only be used within the scope of this investigative project. Therefore, no City Hall will be mentioned separately, since all data will be handled together.

Filling out Instruction: One should follow the questions order, filling the square with an X to represent their answer. For questions that have other questions connected to it, the method to followed is presented inside the parentheses either in the initial question or in their answer.

City Hall and Respondent Characterization					
Identification:	City Hall of			Date:	
Respondent's Name:					
Age:		Sex:	☐ F ☐ M	Education:	
Contact Phone number:				Email:	
Job Title:				Years in this position:	
Previous Job in the City Hall (if applicable):				Years in this position:	

Figure 24 – Instrument Version 1

ISSG General Questions

Strategic Alignment			
1	Does the organization have an ISS program, and is it in effect/implemented?		□ Yes □ No
2	Are the objectives and strategies for ISSG clearly described and defined?		□ Yes □ No
3	Are the ISS objectives tied to the performance objectives of individuals or other business units?		□ Yes (proceed to 3a) □ No (proceed to 4)
	a)	Does these objectives support the ISS activity?	□ Yes □ No
4	Is ISS a consideration in other parts of the organization (aka strategy, processes and procedures)?		□ Yes (proceed to 4a) □ No (proceed to 5)
	a)	Does the IT strategy consider ISS?	□ Yes □ No
5	Does each component of the ISSG structure have sufficient capital and operating expense budget to support the ISS effort?		□ Yes □ No
Value Delivery			
6	Has the ISS activity added value to other business units?		□ Yes □ No
7	Does the ISS activity receive effective/meaningful feedback from the groups(units) it works with?		□ Yes □ No
8	Are the ISS performance metrics tied to the organization's perspective?		□ Yes □ No
9	How often is the effectiveness of the ISS activity assessed?		□ less than 1 year □ between 1 and 2 years □ more than 2 years
10	Are procedures in place to oversee ISS incidents, including public and investor relations, and is there any coordination with law enforcement?		□ Yes □ No
Accountability			
11	Are the roles and responsibilities for the ISS activity formally defined?		□ Yes □ No
12	Are the roles and responsibilities, the accountability, and the performance for all ISS responsibilities formally defined?		□ Yes □ No
13	Who is formally accountable and responsible for the ISS program in the organization? (proceed to 13a)		□ Governing body □ Executive management □ CISO □ Data Protection Officer □ In-line Manager □ None of the above
	a)	To whom does this person formally report?	□ Governing body □ Executive management □ CISO □ Data Protection Officer □ In-line Manager □ None of the above
14	Are there any other functions, boards or groups that the ISS staff has to report regularly; either on an informal basis or in a more formal steering function?		□ Yes □ No
15	What is the career level of the person in charge of the ISS? (proceed to 15a)		□ University degree □ Technical degree □ High School degree

	a)	Is this an officer-level position or a managerial position? (proceed to 15b)	☐ managerial ☐ officer-level
	b)	Does this person have other roles?	☐ Yes ☐ No
16		Is the CISO driving the ISS activity or mostly reporting compliance?	☐ directing the ISS activity ☐ reporting compliance on the ISS activity
17		Is there an escalation path that the ISS news/alerts must follow?	☐ Yes ☐ No
		Compliance	
18		Are ISS policies supported by written standards? Are those standards supported by written procedures?	☐ Yes ☐ No
19		Is there an information exchange formally defined?	☐ Yes (proceed to 19a) ☐ No
	a)	Is the definition for the information exchange sufficient?	☐ Yes ☐ No
20		Is ISS compliance with contractual requirements, laws and regulations enforced in the organization?	☐ Yes ☐ No
21		How often are regulations reviewed to understand the ISS requirements? (proceed to 21a)	☐ less than 1 year ☐ between 1 and 2 years ☐ more than 2 years
	a)	Is the legal department involved in the review process?	☐ Yes ☐ No
22		When did the ISS activity last review a contractual requirement with the legal counsel? (proceed to 22a)	☐ less than 1 year ☐ between 1 and 2 years ☐ more than 2 years
	a)	Does the legal counsel consult with the ISS activity to assess the requirements during a contract process?	☐ Yes ☐ No
23		Is there a specific circumstance in which the board needs to be engaged?	☐ Yes (proceed to 23a) ☐ No
	a)	Are there any risks that the board would deem unacceptable? (proceed to 23b)	☐ Yes ☐ No
	b)	How often are those risks reviewed?	☐ less than 1 year ☐ between 1 and 2 years ☐ more than 2 years
24		Is there an internal or external regulatory compliance group (auditors), and when did the ISS activity last met with them?	☐ less than 1 year ☐ between 1 and 2 years ☐ more than 2 years

ISSG Specific questions for the Public Administration

25		Does your organization have a ISS program?	☐ Yes (proceed to 25a) ☐ No
	a)	How would you evaluate the coverage (clarity, subject, policies, reporting lines, responsibilities) of the ISS program?	☐ Poorly covered ☐ Sufficiently covered ☐ Very well covered
26		Does your organization have a ISS policy?	☐ Yes (proceed to 26a) ☐ No
	a)	Is the ISS policy available and to whom?	☐ Only to organization’s employees ☐ To organization’s employees and contractors ☐ Is available to everyone with clearance ☐ Is available to everyone

27	To what extent is the City Hall IS compliant with legislations, regulations, security policies and rules? (1 – non-compliant and 5 – completely compliant)			
□ 1	□ 2	□ 3	□ 4	□ 5
28		Is the City Hall aware of the GDPR?		□ Yes □ No
	a)	Does de City Hall have a designated data protection officer?		□ Yes □ No
29		Was the City Hall aware of the *PGETIC*?		□ Yes □ No
	a)	Is the City Hall aware of the *Estratégia 2020*?		□ Yes □ No

General Questions				
30	Have you heard about Information Systems Security Governance (ISSG) before today?			□ Yes □ No
31	Did the introductory definition of ISSG helped you understand the subject or meets your prior knowledge of the subject? (1 –didn't help and 5 – completely helped)			
□ 1	□ 2	□ 3	□ 4	□ 5
32	Are you aware of COBIT 5 Process Capability Model (Process Capability Attribute and Process Assessment Model)?			□ Yes (proceed to 35a) □ No
	a)	How would you rate, the organization's EDM processes according to COBIT 5 Process Capability Model? (check a box for the Process Capability and PAM for each process name)		
		Process Name	Process Capability	PAM
		EDM01 – Ensure Governance Framework setting and Maintenance	□ 0 (Incomplete process) □ 1 (Performed process) □ 2 (Managed process) □ 3 (Established process) □ 4 (Predictable process) □ 5 (Optimising process)	□ N (Not achieved) □ P (Partially achieved) □ L (Largely achieved) □ F (Fully achieved)
		EDM02 – Ensure Benefits Delivery	□ 0 (Incomplete process) □ 1 (Performed process) □ 2 (Managed process) □ 3 (Established process) □ 4 (Predictable process) □ 5 (Optimising process)	□ N (Not achieved) □ P (Partially achieved) □ L (Largely achieved) □ F (Fully achieved)
		EDM03 – Ensure Risk Optimisation	□ 0 (Incomplete process) □ 1 (Performed process) □ 2 (Managed process) □ 3 (Established process) □ 4 (Predictable process) □ 5 (Optimising process)	□ N (Not achieved) □ P (Partially achieved) □ L (Largely achieved) □ F (Fully achieved)
		EDM04 – Ensure Resource Optimisation	□ 0 (Incomplete process) □ 1 (Performed process) □ 2 (Managed process) □ 3 (Established process) □ 4 (Predictable process) □ 5 (Optimising process)	□ N (Not achieved) □ P (Partially achieved) □ L (Largely achieved) □ F (Fully achieved)
		EDM05 – Ensure Stakeholder Transparency	□ 0 (Incomplete process) □ 1 (Performed process) □ 2 (Managed process) □ 3 (Established process) □ 4 (Predictable process) □ 5 (Optimising process)	□ N (Not achieved) □ P (Partially achieved) □ L (Largely achieved) □ F (Fully achieved)

- Matrix for Instrument v2 and Concept Tree v4

Table 65 – Matrix Instrument v2 and Concept Tree 4 (Part 1)

CT4 / SQ2	G	G.1	G.1.1	G.1.2	G.2	G.2.1	G.2.2	G.2.2.1	G.2.3	G.3	G.4	Ag	Ag.1	Ag.2	Ag.3	Ag.4	Ag.5	Ag.6	Ag.7	P	P.1	P.1.1	P.1.1.1	P.1.1.2	P.1.1.3	P.1.2	P.2	P.2.1	P.2.2	P.2.3	P.2.4	P.2.4.1	P.2.4.2	P.2.5
1																																		
a)																																		
2																																		
a)																																		
b)																																		
3																																		
a)				x																														
b)																																		
4																																		
a)																																		
b)																																		
c)																																		
5																																		
a)																																		
6																						x												
a)																							x											
b)																								x										
c)																									x									
7																										x								
8																												x						
a)																												x						
b)																												x						
c)																													x					
d)																														x				
9																															x		x	
a)																																x		
b)																																		
10																																x		
11																																		x

CT4 SQ2	G	G.1	G.1.1	G.1.2	G.2	G.2.1	G.2.2	G.2.2.1	G.2.3	G.3	G.4	Ag	Ag.1	Ag.2	Ag.3	Ag.4	Ag.5	Ag.6	Ag.7	P	P.1	P.1.1	P.1.1.1	P.1.1.2	P.1.1.3	P.1.2	P.2	P.2.1	P.2.2	P.2.3	P.2.4	P.2.4.1	P.2.4.2	P.2.5
a)																																		
b)																																		
c)																																		
12																																		x
a)																																		
b)																																		
c)																																		
13																																		
14																																		
15																																		
16																																		
a)																																		
17																																		
18																																		
19																																		
20			x																															
21				x																														
22					x																													
a)						x																												
b)							x																											
c)									x																									
23										x																								
24											x																							
25												x																	x					
a)													x																					
b)														x																				
c)																	x																	
26												x																						
a)													x																					
b)														x																				
c)															x																			
d)																x																		
e)																	x																	
f)																		x																
27			x																															
28																									x									
29																										x								

CT4 SQ2	G	G.1	G.1.1	G.1.2	G.2	G.2.1	G.2.2	G.2.2.1	G.2.3	G.3	G.4	Ag	Ag.1	Ag.2	Ag.3	Ag.4	Ag.5	Ag.6	Ag.7	P	P.1	P.1.1	P.1.1.1	P.1.1.2	P.1.1.3	P.1.2	P.2	P.2.1	P.2.2	P.2.3	P.2.4	P.2.4.1	P.2.4.2	P.2.5
30																												x						
31																												x						
32												x																	x					
33																														x				
34																															x			
35																																		
36																																		
37	x																																	
a)		x																																
b)					x																													
c)										x																								
d)											x																							

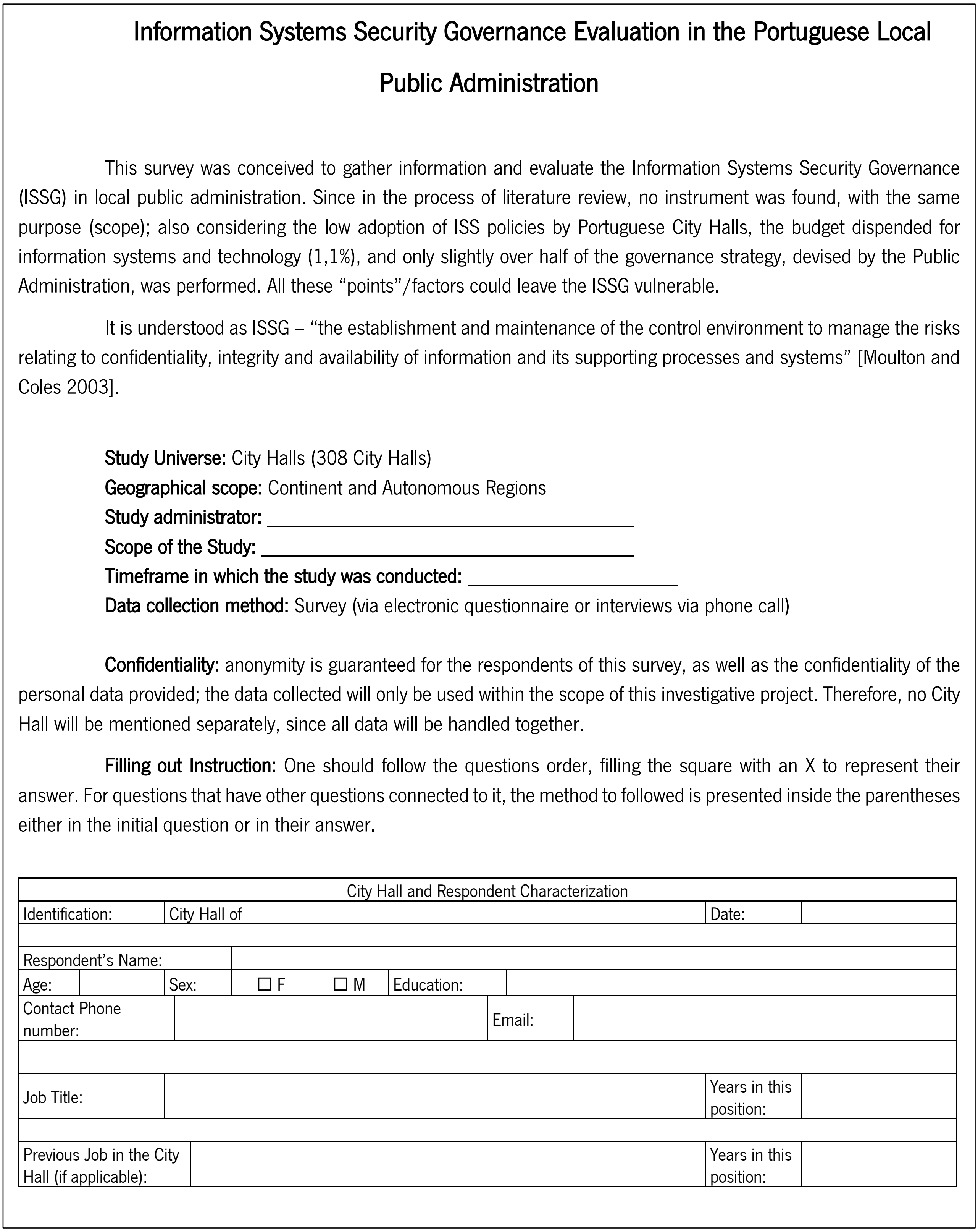
Table 66 – Matrix Instrument v2 and Concept Tree 4 (Part 2)

CT4 SQ2	P.2.5.1	P.2.5.2	P.2.5.3	P.2.5.4	P.2.5.5	P.2.5.6	P.3	P.3.1	P.3.1.1	P.3.2	P.3.2.1	P.3.3	P.3.4	P.3.5	P.3.6	AR	AR.1	AR.1.1	AR.2	AR.2.1	AR.2.2	AR.2.3	AR.3	AR.3.1	AR.3.2	AR.3.3	AR.4	AR.4.1	AR.4.1.1	AR.4.2	AR.4.3	AR.5	AR.5.1	AR.5.2	AR.5.2.1	AR.5.3	AR.5.4
1																	x																				
a)																		x																			
2																			x																		
a)								x																													
b)																				x	x	x															
3																							x														
a)																																					
b)																								x	x	x											
4																											x										
a)																												x		x	x						
b)																													x								
c)													x																								
5																																x					
a)																																	x	x	x	x	x
6																																					
a)																																					
b)																																					
c)																																					
7																																					
8																																					
a)																																					
b)																																					
c)																																					
d)																																					
9																																					
a)																																					
b)																																				x	
10																																					
11																																					
a)	x																																				
b)		x																																			
c)				x																																	

CT4 SQ2	P.2.5.1	P.2.5.2	P.2.5.3	P.2.5.4	P.2.5.5	P.2.5.6	P.3	P.3.1	P.3.1.1	P.3.2	P.3.2.1	P.3.3	P.3.4	P.3.5	P.3.6	AR	AR.1	AR.1.1	AR.2	AR.2.1	AR.2.2	AR.2.3	AR.3	AR.3.1	AR.3.2	AR.3.3	AR.4	AR.4.1	AR.4.1.1	AR.4.2	AR.4.3	AR.5	AR.5.1	AR.5.2	AR.5.2.1	AR.5.3	AR.5.4
12																																					
a)					x																																
b)						x																															
c)			x																																		
13								x																													
14													x																								
15									x																												
16										x																											
a)											x																										
17															x																						
18												x																									
19														x																							
20																																					
21																																					
22																																					
a)																																					
b)																																					
c)																																					
23																																					
24																																					
25																x	x		x				x				x					x					
a)																																					
b)																																					
c)																																					
26									x		x			x																							
a)																																					
b)																																					
c)																																					
d)																																					
e)																																					
f)																																					
27																	x																				
28																																					
29																																					
30																																					
31																																					

CT4 / SQ2	P.2.5.1	P.2.5.2	P.2.5.3	P.2.5.4	P.2.5.5	P.2.5.6	P.3	P.3.1	P.3.1.1	P.3.2	P.3.2.1	P.3.3	P.3.4	P.3.5	P.3.6	AR	AR.1	AR.1.1	AR.2	AR.2.1	AR.2.2	AR.2.3	AR.3	AR.3.1	AR.3.2	AR.3.3	AR.4	AR.4.1	AR.4.1.1	AR.4.2	AR.4.3	AR.5	AR.5.1	AR.5.2	AR.5.2.1	AR.5.3	AR.5.4
32																																					
33																																					
34																																					
35													x																								
36																							x	x	x	x											
37																																					
a)																																					
b)																																					
c)																																					
d)																																					

- Instrument v2



Information Systems Security Governance Evaluation in the Portuguese Local Public Administration

This survey was conceived to gather information and evaluate the Information Systems Security Governance (ISSG) in local public administration. Since in the process of literature review, no instrument was found, with the same purpose (scope); also considering the low adoption of ISS policies by Portuguese City Halls, the budget dispended for information systems and technology (1,1%), and only slightly over half of the governance strategy, devised by the Public Administration, was performed. All these "points"/factors could leave the ISSG vulnerable.

It is understood as ISSG – "the establishment and maintenance of the control environment to manage the risks relating to confidentiality, integrity and availability of information and its supporting processes and systems" [Moulton and Coles 2003].

Study Universe: City Halls (308 City Halls)
Geographical scope: Continent and Autonomous Regions
Study administrator: ___________________________________
Scope of the Study: ___________________________________
Timeframe in which the study was conducted: ____________________
Data collection method: Survey (via electronic questionnaire or interviews via phone call)

Confidentiality: anonymity is guaranteed for the respondents of this survey, as well as the confidentiality of the personal data provided; the data collected will only be used within the scope of this investigative project. Therefore, no City Hall will be mentioned separately, since all data will be handled together.

Filling out Instruction: One should follow the questions order, filling the square with an X to represent their answer. For questions that have other questions connected to it, the method to followed is presented inside the parentheses either in the initial question or in their answer.

City Hall and Respondent Characterization					
Identification:	City Hall of			Date:	
Respondent's Name:					
Age:		Sex:	□ F □ M	Education:	
Contact Phone number:			Email:		
Job Title:				Years in this position:	
Previous Job in the City Hall (if applicable):				Years in this position:	

Figure 25 – Instrument Version 2

Artifacts

1	Does the organization has an ISS strategy?		□ Yes □ No
	a)	Is a decision making model present?	□ Yes □ No
2	Does an ISS program exists in the organization?		□ Yes □ No
	a)	How would the effectiveness of this ISS program be qualified?	□ Ineffective □ P (Partially achieved) □ Very effective
	b)	Are investment distribution, resource allocation and responsibility assignment contemplated to which extent in the ISS program?	□ Not mentioned □ P (Partially achieved) □ Profusely discussed
3	Has an ISS policy and guidelines been created in the organization?		□ Yes □ No
	a)	Are the ISS policy and guidelines implemented in the organization?	□ Yes □ No
	b)	In regards of the authority levels, the escalation guidelines and the reporting and communicating structure; how would you evaluate their definition, description and clarity?	□ Little to non-existent □ P (Partially achieved) □ Extremely detailed
4	Is there a program in place to assess the ISS performance?		□ Yes □ No
	a)	Does the ISS performance program contemplate actions for communicating and reporting events, actions to address resource management deviations and audit reports? To which extent?	□ Few mentions □ P (Partially achieved) □ Completely covered
	b)	In the reporting and communication's actions, is stakeholder's feedback discussed?	□ Yes □ No
	c)	Is there any information gathered from the ISS performance program? If so, is this information, used to select the metrics in accordance with the business perspective?	□ Yes □ No
5	Is a risk management program present at the organization?		□ Yes □ No
	a)	How well is the risk subject (such as risk assessment, risk policies, risk tolerance level, risk appetite and risk mitigation) discussed in the program?	□ Not well enough □ A regular amount □ Very well

Processes

6	How would you evaluate the alignment of the ISS with the business strategy						
	a)	Does the business initiatives considers the ISS issues	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
	b)	Are the business objective supported by the ISS	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
	c)	How does the organization handle the results from the ISS performance? Does the organization prioritizes and initiate the required actions?	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
7	Are benefits (such as: good results, profits or advantages) perceived from the investments in ISS?			□ Yes □ No			

8	How would you describe the commitment of the executive management in						
	a)	Protecting the information assets	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
	b)	Making ISS related decisions	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
	c)	Developing and approving the ISS strategy and policy	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
	d)	Allocating investments and resources	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
9	Does the organization follows a risk management policy to manage the risks encountered?		□ Yes □ No				
	a)	Is the risk appetite described in the policy?	□ Yes □ No				
	b)	How is the risk appetite determined?					
10	Does the organization has a guideline/plan to follow to determine the risk appetite for new risks?		□ Yes □ No				
11	How much is covered in the resource management of the ISS program?						
	a)	Assignment of responsibilities	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
	b)	Have competent and motivated personnel	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
	c)	Promotion of a positive information security culture	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
12	How much is covered of the stakeholders communication and reporting in the ISS program?						
	a)	Reporting and communication principles and guidelines	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
	b)	Principles for safeguarding the resources	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
	c)	Escalation guidelines	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
13	How would you quantify the effectiveness (accomplishment/completion of what was set out) of the management of the information security activities?		□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
14	Does the selected information security performance metrics ponder the business perspective?		□ Yes □ No				
15	Are the results of the information security performance used in providing feedback and demonstrating their impacts on the organization?		□ Yes □ No				
16	Is the ISS program reviewed to verify their compliance with legislation, regulations, contractual obligations and statutory requirements?		□ Yes □ No				
	a)	Is the compliance with the organizations information security practices and its alignment to nature of the organizations business, reported to the stakeholders?	□ Yes □ No				
17	Are independent audits commissioned to verify the information security level determined in the organization?		□ Yes □ No				
18	Does the ISS strategy considers the changes in different types of environment (business, legal and regulatory) and their potential information risk?		□ Yes □ No				
19	Is there a feedback provided by the organization, that regards the transparency of IT costs, benefits and risks?		□ Yes □ No				

Goals

20	To which stand are the needs of the stakeholders balanced in the process of creating an ISSG strategy?		□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
21	Are the ISSG fundaments integrated within all levels of the organization?				□ Yes □ No		
22	To which percentage is the value for the governance of the ISS perceived by the organization?						
	a)	The cost-effectiveness (accomplish what was set out, considering the cost)	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
	b)	The efficiency (degree of achieving the desired result with little waste)	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
	c)	The optimization of resources, assets and capabilities	□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)
23	Has the ISSG set out rules that makes people/roles accountable for their actions/responsibilities?				□ Yes □ No		
24	How much is compliance (the conformity to fulfill official requirements) a part of the ISSG in the organization?		□ 1 (0 a 20%)	□ 2 (21 – 40%)	□ 3 (41 – 60%)	□ 4 (61 – 80%)	□ 5 (81 – 100%)

Agents

25	Mark the correspondent artifact, that each role is responsible for developing. (Multiple choices accepted)						
		Role	Artifacts				
	a)	Governing body	□ ISS strategy	□ ISS program	□ ISS policies and guidelines	□ ISS performance program	□ Risk management program
	b)	Executive management	□ ISS strategy	□ ISS program	□ ISS policies and guidelines	□ ISS performance program	□ Risk management program
	c)	Chief Information Security Officer (CISO)	□ ISS strategy	□ ISS program	□ ISS policies and guidelines	□ ISS performance program	□ Risk management program

26	Mark the correspondent reporting role, that each main role is responsible for reporting to.					
		Main Role	Reports to			
	a)	Governing body	□ Governing body	□ Executive Management	□ In-Line Management	□ Stakeholders
	b)	Executive management	□ Governing body	□ Executive Management	□ In-Line Management	□ Stakeholders
	c)	Auditors	□ Governing body	□ Executive Management	□ In-Line Management	□ Stakeholders
	d)	Data Protection Officer (DPO)	□ Governing body	□ Executive Management	□ In-Line Management	□ Stakeholders
	e)	Chief Information Security Officer (CISO)	□ Governing body	□ Executive Management	□ In-Line Management	□ Stakeholders
	f)	Employees	□ Governing body	□ Executive Management	□ In-Line Management	□ Stakeholders

Others

27	Does the ISS strategy considers and balances the stakeholders needs?	☐ Yes ☐ No
28	Has the ISS strategy changed in order to prioritize some aspects approved by the ISS performance results?	☐ Yes ☐ No
29	Have the investments on ISS being evaluated, to very their value?	☐ Yes ☐ No
30	How committed is the executive management in protecting the information assets?	☐ 1 (0 a 20%) ☐ 2 (21 – 40%) ☐ 3 (41 – 60%) ☐ 4 (61 – 80%) ☐ 5 (81 – 100%)
31	Does the executive management make decisions based on ISS?	☐ Yes ☐ No
32	Which role is responsible for developing and approving the ISS strategy and policies in the organization?	☐ Governing body ☐ Executive management ☐ CISO ☐ Data Protection Officer ☐ In-line Manager ☐ None of the above
33	Are investments and resources allocated in order to secure support for the ISS activity?	☐ Yes ☐ No
34	Does the organization carries out a risk management program?	☐ Yes ☐ No
35	Are the ISS performance metrics developed to accommodate the business perspective?	☐ Yes ☐ No
36	Are authority levels, escalation guidelines, and reporting and communicating structure covered under the ISS policy or guidelines?	☐ Yes ☐ No

37	How would you evaluate the accomplishment of the ISSG goals for						
	a)	Strategic alignment ()	☐ 1 (0 a 20%)	☐ 2 (21 – 40%)	☐ 3 (41 – 60%)	☐ 4 (61 – 80%)	☐ 5 (81 – 100%)
	b)	Value delivery ()	☐ 1 (0 a 20%)	☐ 2 (21 – 40%)	☐ 3 (41 – 60%)	☐ 4 (61 – 80%)	☐ 5 (81 – 100%)
	c)	Accountability (accept responsibility for the ISSG actions in the organization)	☐ 1 (0 a 20%)	☐ 2 (21 – 40%)	☐ 3 (41 – 60%)	☐ 4 (61 – 80%)	☐ 5 (81 – 100%)
	d)	Compliance (fulfill requirements in accordance with some specified standard)	☐ 1 (0 a 20%)	☐ 2 (21 – 40%)	☐ 3 (41 – 60%)	☐ 4 (61 – 80%)	☐ 5 (81 – 100%)

- Matrix for Instrument v3 and Concept Tree v4

Table 67 – Matrix Instrument v3 and Concept Tree 4 (Part 1)

CT4 SQ3	G	G.1	G.1.1	G.1.2	G.2	G.2.1	G.2.2	G.2.2.1	G.2.3	G.3	G.4	Ag	Ag.1	Ag.2	Ag.3	Ag.4	Ag.5	Ag.6	Ag.7	P	P.1	P.1.1	P.1.1.1	P.1.1.2	P.1.1.3	P.1.2	P.2	P.2.1	P.2.2	P.2.3	P.2.4	P.2.4.1	P.2.4.2
1																																	
1a																																	
2																																	
2a																																	
2b																																	
3																																	
3a				x																													
3b																																	
3c																																	
4								x																									
4a																																	
4b																																	
4c																																	
5																																	
5a																																	
6																						x											
6a																							x										
6b																								x									
6c																									x								
7																										x							
8																												x					
8a																												x					
8b																												x					
8c																													x				
8d																														x			
9																															x		x
9a																																	
9b																																x	
9c																																	

CT4 SQ3	G	G.1	G.1.1	G.1.2	G.2	G.2.1	G.2.2	G.2.2.1	G.2.3	G.3	G.4	Ag	Ag.1	Ag.2	Ag.3	Ag.4	Ag.5	Ag.6	Ag.7	P	P.1	P.1.1	P.1.1.1	P.1.1.2	P.1.1.3	P.1.2	P.2	P.2.1	P.2.2	P.2.3	P.2.4	P.2.4.1	P.2.4.2
10																																x	
11																																	x
12																																	
12a																																	
12b																																	
12c																																	
13												x																					
13a												x																					
13b												x																					
14																																	
14a																																	
14b																																	
14c																																	
15								x																									
15a																																	
16																																	
17																																	
18																																	
19																																	
19a																																	
19b																																	
20																																	
21																																	
22																																	
22a				x																													
22b																																	
23																																	
24	x																																
24a		x																															
24b					x																												
24c										x																							
24d											x																						
25			x																														
26				x																													
27					x																												
27a						x																											
27b							x																										

CT4 SQ3	G	G.1	G.1.1	G.1.2	G.2	G.2.1	G.2.2	G.2.2.1	G.2.3	G.3	G.4	Ag	Ag.1	Ag.2	Ag.3	Ag.4	Ag.5	Ag.6	Ag.7	P	P.1	P.1.1	P.1.1.1	P.1.1.2	P.1.1.3	P.1.2	P.2	P.2.1	P.2.2	P.2.3	P.2.4	P.2.4.1	P.2.4.2
27c									x																								
28										x																							
29											x																						
30												x																	x				
30a													x																				
30b														x																			
30c																	x																
31												x																					
31a													x																				
31b														x																			
31c														x																			
31d														x																			
31e															x																		
31f																x																	
31g																	x																
31h																		x															
32																	x																

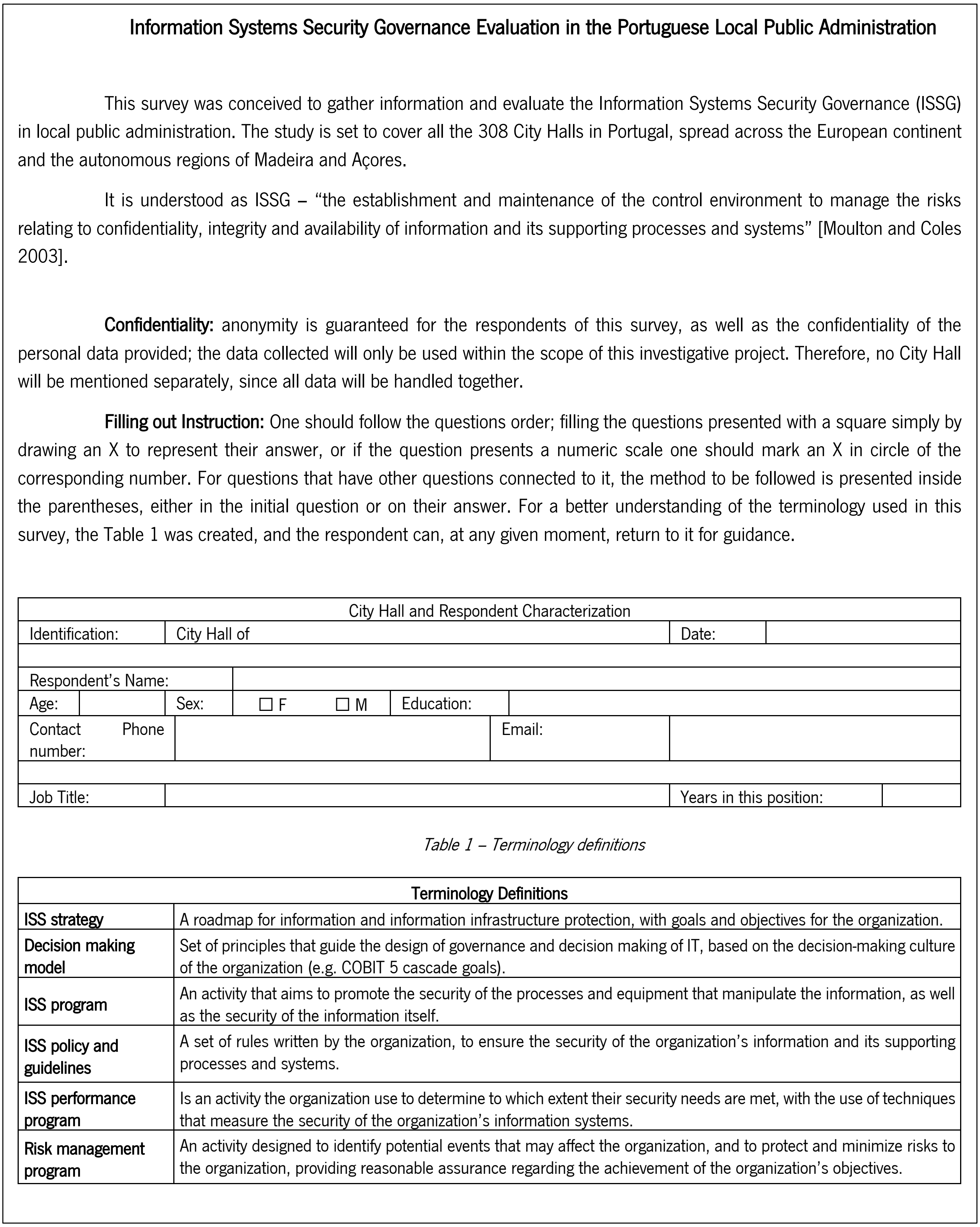
Table 68 – Matrix Instrument v3 and Concept Tree 4 (Part 2)

CT4 / SQ3	P.2.5	P.2.5.1	P.2.5.2	P.2.5.3	P.2.5.4	P.2.5.5	P.2.5.6	P.3	P.3.1	P.3.1.1	P.3.2	P.3.2.1	P.3.3	P.3.4	P.3.5	P.3.6	AR	AR.1	AR.1.1	AR.2	AR.2.1	AR.2.2	AR.2.3	AR.3	AR.3.1	AR.3.2	AR.3.3	AR.4	AR.4.1	AR.4.1.1	AR.4.2	AR.4.3	AR.5	AR.5.1	AR.5.2	AR.5.2.1	AR.5.3	AR.5.4
1																		x																				
1a																			x																			
2																				x																		
2a									x																													
2b																					x	x	x															
3																								x														
3a																																						
3b						x																		x			x											
3c																									x	x	x											
4																												x										
4a																													x		x	x						
4b																														x								
4c														x																								
5																																	x					
5a																																		x	x	x	x	x
6																																						
6a																																						
6b																																						
6c																																						
7																																						
8																																						
8a																																						
8b																																						
8c																																						
8d																																						
9																																						
9a											x		x																									
9b																																						
9c											x		x																									
10																																						
11																																						
12	x																																					

CT4 / SQ3	P.2.5	P.2.5.1	P.2.5.2	P.2.5.3	P.2.5.4	P.2.5.5	P.2.5.6	P.3	P.3.1	P.3.1.1	P.3.2	P.3.2.1	P.3.3	P.3.4	P.3.5	P.3.6	AR	AR.1	AR.1.1	AR.2	AR.2.1	AR.2.2	AR.2.3	AR.3	AR.3.1	AR.3.2	AR.3.3	AR.4	AR.4.1	AR.4.1.1	AR.4.2	AR.4.3	AR.5	AR.5.1	AR.5.2	AR.5.2.1	AR.5.3	AR.5.4
12a		x																																				
12b			x																																			
12c					x																																	
13			x																																			
13a			x																																			
13b			x																																			
14	x																																					
14a						x																																
14b							x																															
14c				x																																		
15									x																													
15a									x	x			x																									
16														x																								
17									x						x																							
18										x																												
19											x																											
19a												x																										
19b											x					x																						
20																x																						
21													x																									
22											x		x																									
22a																																						
22b											x																											
23															x																							
24																																						
24a																																						
24b																																						
24c																																						
24d																																						
25																																						
26																																						
27																																						
27a																																						
27b																																						
27c																																						
28																																						
29																																						

CT4 SQ3	P.2.5	P.2.5.1	P.2.5.2	P.2.5.3	P.2.5.4	P.2.5.5	P.2.5.6	P.3	P.3.1	P.3.1.1	P.3.2	P.3.2.1	P.3.3	P.3.4	P.3.5	P.3.6	AR	AR.1	AR.1.1	AR.2	AR.2.1	AR.2.2	AR.2.3	AR.3	AR.3.1	AR.3.2	AR.3.3	AR.4	AR.4.1	AR.4.1.1	AR.4.2	AR.4.3	AR.5	AR.5.1	AR.5.2	AR.5.2.1	AR.5.3	AR.5.4
30																	x	x		x				x				x					x					
30a																																						
30b																																						
30c																																						
31										x		x			x																							
31a																																						
31b																																						
31c																																						
31d																																						
31e																																						
31f																																						
31g																																						
31h																																						
32																																						

- Instrument v3



Information Systems Security Governance Evaluation in the Portuguese Local Public Administration

This survey was conceived to gather information and evaluate the Information Systems Security Governance (ISSG) in local public administration. The study is set to cover all the 308 City Halls in Portugal, spread across the European continent and the autonomous regions of Madeira and Açores.

It is understood as ISSG – "the establishment and maintenance of the control environment to manage the risks relating to confidentiality, integrity and availability of information and its supporting processes and systems" [Moulton and Coles 2003].

Confidentiality: anonymity is guaranteed for the respondents of this survey, as well as the confidentiality of the personal data provided; the data collected will only be used within the scope of this investigative project. Therefore, no City Hall will be mentioned separately, since all data will be handled together.

Filling out Instruction: One should follow the questions order; filling the questions presented with a square simply by drawing an X to represent their answer, or if the question presents a numeric scale one should mark an X in circle of the corresponding number. For questions that have other questions connected to it, the method to be followed is presented inside the parentheses, either in the initial question or on their answer. For a better understanding of the terminology used in this survey, the Table 1 was created, and the respondent can, at any given moment, return to it for guidance.

City Hall and Respondent Characterization					
Identification:	City Hall of			Date:	
Respondent's Name:					
Age:		Sex:	□ F □ M	Education:	
Contact Phone number:			Email:		
Job Title:				Years in this position:	

Table 1 – Terminology definitions

Terminology Definitions	
ISS strategy	A roadmap for information and information infrastructure protection, with goals and objectives for the organization.
Decision making model	Set of principles that guide the design of governance and decision making of IT, based on the decision-making culture of the organization (e.g. COBIT 5 cascade goals).
ISS program	An activity that aims to promote the security of the processes and equipment that manipulate the information, as well as the security of the information itself.
ISS policy and guidelines	A set of rules written by the organization, to ensure the security of the organization's information and its supporting processes and systems.
ISS performance program	Is an activity the organization use to determine to which extent their security needs are met, with the use of techniques that measure the security of the organization's information systems.
Risk management program	An activity designed to identify potential events that may affect the organization, and to protect and minimize risks to the organization, providing reasonable assurance regarding the achievement of the organization's objectives.

Figure 26 – Instrument Version 3

Artifacts

1	Does the organization has an ISS strategy?		☐ Yes (proceed to 1a) ☐ No (proceed to 2)
	a)	Is a decision making model present? (proceed to 2)	☐ Yes ☐ No
2	Does an ISS program exists in the organization?		☐ Yes (proceed to 2a) ☐ No (proceed to 3)
	a)	How would the effectiveness (accomplishment/completion of planned activities) of the ISS program be qualified? (proceed to 2b) (**Scale measures**: 1 – not effective [between 0 and 20% accomplished]; 3 – somewhat effective [between 41 and 60% accomplished]; 5 – very effective [between 81 and 100% accomplished])	○—○—○—○—○ 1 2 3 4 5
	b)	Is investment distribution, resource allocation and responsibility assignment contemplated to which extent in the ISS program? (**Scale measures**: 1 – not contemplated; 3 – sufficiently contemplated; 5 – fully contemplated)	○—○—○—○—○ 1 2 3 4 5
3	Has an ISS policy and guidelines been created in the organization?		☐ Yes (proceed to 3a) ☐ No (proceed to 4)
	a)	Are the ISS policy and guidelines implemented in the organization?	☐ Yes (proceed to 3b) ☐ No (proceed to 4)
	b)	To whom is the ISS policy available? (proceed to 3c)	☐ Organization's employees ☐ Organization's employees and contractors ☐ Everyone with clearance ☐ Everyone
	c)	In regards of the authority levels, the escalation guidelines and the reporting and communicating structure; how would you evaluate their definition, description and clarity? (**Scale measures**: 1 – poorly covered; 3 – sufficiently covered; 5 – very well covered)	○—○—○—○—○ 1 2 3 4 5
4	Is there a program in place to assess the ISS performance (the use measures to determine to which stand the organization's ISS needs were met)?		☐ Yes (proceed to 4a) ☐ No (proceed to 5)
	a)	Does the ISS performance program contemplate, to which extent, the actions for communicating and reporting events, actions to address resource management deviations and audit reports? (proceed to 4b) (**Scale measures**: 1 – poorly contemplated; 3 – sufficiently contemplated; 5 – very well contemplated)	○—○—○—○—○ 1 2 3 4 5
	b)	In the reporting and communication's actions, is stakeholder's feedback discussed? (proceed to 4c)	☐ Yes ☐ No
	c)	Is there any information gathered from the ISS performance program? If so, is this information, used to select the metrics in accordance with the business perspective?	☐ Yes ☐ No
5	Is a risk management program present at the organization?		☐ Yes (proceed to 5a) ☐ No (proceed to 6)
	a)	How well is the risk subject (such as risk assessment, risk policies, risk tolerance level, risk appetite and risk mitigation) discussed in the program? (**Scale measures**: 1 – poorly discussed; 3 – sufficiently discussed; 5 – very well discussed)	○—○—○—○—○ 1 2 3 4 5

Processes

6		How would you evaluate the alignment of the ISS with the business strategy … (proceed to 6a) (Scale measures: 1 – poorly aligned; 3 – sufficiently aligned; 5 – completely aligned)	
	a)	when considering the ISS issues in the business initiatives? (proceed to 6b)	○—○—○—○—○ 1 2 3 4 5
	b)	to support the business objectives? (proceed to 6c)	○—○—○—○—○ 1 2 3 4 5
	c)	in handling the results from the ISS performance; and when prioritizing and/or initiating the required actions derived from the results of the ISS performance?	○—○—○—○—○ 1 2 3 4 5
7		Are benefits (such as: good results, profits or advantages) perceived from the investments in ISS?	☐ Yes ☐ No
8		How would you describe the commitment of the executive management in … (proceed to 8a) (Scale measures: 1 – not committed; 3 – sufficiently committed; 5 – fully committed)	
	a)	protecting the information assets? (proceed to 8b)	○—○—○—○—○ 1 2 3 4 5
	b)	making ISS related decisions? (proceed to 8c)	○—○—○—○—○ 1 2 3 4 5
	c)	developing and approving the ISS strategy and policy? (proceed to 8d)	○—○—○—○—○ 1 2 3 4 5
	d)	allocating investments and resources?	○—○—○—○—○ 1 2 3 4 5
9		Does the organization follow a risk management policy to manage the risks encountered?	☐ Yes (proceed to 9a) ☐ No (proceed to 10)
	a)	Are ISS policies supported by written standards; and are those standards supported by written procedures? (proceed to 9b)	☐ Yes ☐ No
	b)	Is the risk appetite described in the policy? (proceed to 9c)	☐ Yes ☐ No
	c)	How often are the risks reviewed? (Scale measures: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	○——○——○ 1 2 3
10		Does the organization has a guideline/plan to follow to determine the risk appetite for new risks?	☐ Yes ☐ No
11		Are procedures in place to oversee ISS incidents, including public and investor relations, and is there any coordination with law enforcement?	☐ Yes ☐ No
12		How much is covered in the resource management of the ISS program for … (proceed to 12a) (Scale measures: 1 – not covered; 3 – sufficiently covered; 5 – fully covered)	
	a)	assignment of responsibilities? (proceed to 12b)	○—○—○—○—○ 1 2 3 4 5
	b)	having competent and motivated personnel? (proceed to 12c)	○—○—○—○—○ 1 2 3 4 5
	c)	promoting a positive information security culture?	○—○—○—○—○ 1 2 3 4 5

13	What is the career level of the person in charge of the ISS? (proceed to 13a)		□ University degree □ Technical degree □ High School degree
	a)	Is this an officer-level position or a managerial position? (proceed to 13b)	□ managerial □ officer-level
	b)	Does this person has other roles?	□ Yes □ No
14	How much is covered of the stakeholders communication and reporting in the ISS program for ... (proceed to 14a) (**Scale measures**: 1 – poorly covered; 3 – sufficiently covered; 5 – very well covered)		
	a)	reporting and communication of principles and guidelines? (proceed to 14b)	○—○—○—○—○ 1 2 3 4 5
	b)	principles for safeguarding the resources? (proceed to 14c)	○—○—○—○—○ 1 2 3 4 5
	c)	escalation guidelines?	○—○—○—○—○ 1 2 3 4 5
15	How would you quantify the effectiveness (accomplishment/completion of what was set out) of the management of the information security activities? (proceed to 15a) (**Scale measures**: 1 – not effective [between 0 and 20% accomplished]; 2 – between 21 and 40% accomplished; 3 – somewhat effective [between 41 and 60% accomplished]; 4 – between 61 and 80% accomplished; 5 – very effective [between 81 and 100% accomplished])		○—○—○—○—○ 1 2 3 4 5
	a)	How often is the effectiveness of the ISS activity assessed? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	○—○—○ 1 2 3
16	Does the selected information security performance metrics ponder the business perspective?		□ Yes □ No
17	Does the ISS activity receive effective/meaningful feedback from the groups(units) it works with?		□ Yes □ No
18	Are the results of the information security performance used in providing feedback and demonstrating their impacts on the organization?		□ Yes □ No
19	Is the ISS program reviewed to verify their compliance with legislation, regulations, contractual obligations and statutory requirements?		□ Yes (proceed to 19a) □ No (proceed to 20)
	a)	Is the compliance with the organizations information security practices and its alignment to nature of the organizations business, reported to the stakeholders? (proceed to 19b)	□ Yes □ No
	b)	Is there an internal or external regulatory compliance group (auditors), and when did the ISS activity last met with them? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	○—○—○ 1 2 3
20	Are independent audits commissioned to verify the information security level determined in the organization?		□ Yes □ No
21	Does the ISS strategy considers the changes in different types of environment (business, legal and regulatory) and their potential information risk?		□ Yes □ No
22	How often are regulations reviewed to understand the ISS requirements? (proceed to 22a) (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)		○—○—○ 1 2 3
	a)	Is the legal department involved in the review process?	□ Yes (proceed to 22b) □ No (proceed to 23)
	b)	When did the ISS activity last review a contractual requirement with the legal counsel? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	○—○—○ 1 2 3
23	Is there a feedback provided by the organization, that regards the transparency of IT costs, benefits and risks?		□ Yes □ No

Goals

24	How would you evaluate the accomplishment of the ISSG goals for ... (proceed to 24a) (**Scale measures**: 1 – not accomplished; 3 – sufficiently accomplished; 5 – fully accomplished)		
	a)	strategic alignment ? (proceed to 24b)	○—○—○—○—○ 1 2 3 4 5
	b)	value delivery ? (proceed to 24c)	○—○—○—○—○ 1 2 3 4 5
	c)	accountability (accept responsibility for the ISSG actions in the organization)? (proceed to 24d)	○—○—○—○—○ 1 2 3 4 5
	d)	compliance (fulfill requirements in accordance with some specified standard)?	○—○—○—○—○ 1 2 3 4 5
25	To which extent are the needs of the stakeholders balanced in the process of creating an ISSG strategy? (**Scale measures**: 1 – not balanced; 3 – sufficiently balanced; 5 – fully balanced)		○—○—○—○—○ 1 2 3 4 5
26	Are the ISSG fundaments integrated within all levels of the organization?		☐ Yes ☐ No
27	To which degree is the value for the governance of the ISS perceived by the organization ... (proceed to 27a) (**Scale measures**: 1 – no value added [between 0 and 20%]; 2 – between 21 and 40%; 3 – fair amount of value added [between 41 and 60%]; 4 – between 61 and 80%; 5 – a lot of value added [between 81 and 100%])		
	a)	the cost-effectiveness (accomplish what was set out, considering the cost)? (proceed to 27b)	○—○—○—○—○ 1 2 3 4 5
	b)	the efficiency (degree of achieving the desired result with little waste)? (proceed to 27c)	○—○—○—○—○ 1 2 3 4 5
	c)	the optimization of resources, assets and capabilities?	○—○—○—○—○ 1 2 3 4 5
28	Has the ISSG set out rules that makes people/roles accountable for their actions/responsibilities?		☐ Yes ☐ No
29	How much is compliance (the conformity to fulfill official requirements) a part of the ISSG in the organization? (**Scale measures**: 1 – not important [between 0 and 20% of compliance]; 3 – somewhat important [between 41 and 60% of compliance]; 5 – very important [between 81 and 100% of compliance])		○—○—○—○—○ 1 2 3 4 5

Agents

30	Mark the correspondent artifact, that each role is responsible for developing. (Multiple choices accepted) (proceed to 30 a through c)						
		Role	Artifacts				
	a)	Governing body	□ ISS strategy	□ ISS program	□ ISS policies and guidelines	□ ISS performance program	□ Risk management program
	b)	City Hall executive (group usually formed by the city hall mayor and members of the city council)	□ ISS strategy	□ ISS program	□ ISS policies and guidelines	□ ISS performance program	□ Risk management program
	c)	Chief Information Security Officer (CISO)	□ ISS strategy	□ ISS program	□ ISS policies and guidelines	□ ISS performance program	□ Risk management program

31	Mark the correspondent reporting role, that each main role is responsible for reporting to? (proceed to 31 a through h)					
		Main Role	Reports to			
	a)	Governing body	□ Governing body	□ City Hall Executive	□ In-Line Management	□ Stakeholders
	b)	Mayor	□ Governing body	□ City Hall Executive	□ In-Line Management	□ Stakeholders
	c)	City Councilor	□ Governing body	□ City Hall Executive	□ In-Line Management	□ Stakeholders
	d)	Chief Information Officer (CIO)	□ Governing body	□ City Hall Executive	□ In-Line Management	□ Stakeholders
	e)	Auditors	□ Governing body	□ City Hall Executive	□ In-Line Management	□ Stakeholders
	f)	Data Protection Officer (DPO)	□ Governing body	□ City Hall Executive	□ In-Line Management	□ Stakeholders
	g)	Chief Information Security Officer (CISO)	□ Governing body	□ City Hall Executive	□ In-Line Management	□ Stakeholders
	h)	Employees	□ Governing body	□ City Hall Executive	□ In-Line Management	□ Stakeholders

32	Is the CISO driving the ISS activity or mostly reporting compliance?	□ directing the ISS activity □ reporting compliance on the ISS activity

- Matrix for Instrument v4 and Concept Tree v4

Table 69 – Matrix Instrument v4 and Concept Tree 4 (Part 1)

CT4 / SQ4	G	G.1	G.1.1	G.1.2	G.2	G.2.1	G.2.2	G.2.2.1	G.2.3	G.3	G.4	Ag	Ag.1	Ag.2	Ag.3	Ag.4	Ag.5	Ag.6	Ag.7	P	P.1	P.1.1	P.1.1.1	P.1.1.2	P.1.1.3	P.1.2	P.2	P.2.1	P.2.2	P.2.3	P.2.4	P.2.4.1	P.2.4.2
1																																	
1a																																	
2																																	
2a																																	
2b																																	
3																																	
3a				x																													
3b																																	
3c																																	
3d																																	
4								x																									
4a																																	
4b																																	
4c																																	
5																																	
5a																																	
6																						x											
6a																							x										
6b																								x									
6c																									x								
7																										x							
8																												x					
8a																												x					
8b																												x					
8c																													x				
8d																														x			
9																															x		x
9a																																	
9b																																x	

CT4 SQ4	G	G.1	G.1.1	G.1.2	G.2	G.2.1	G.2.2	G.2.2.1	G.2.3	G.3	G.4	Ag	Ag.1	Ag.2	Ag.3	Ag.4	Ag.5	Ag.6	Ag.7	P	P.1	P.1.1	P.1.1.1	P.1.1.2	P.1.1.3	P.1.2	P.2	P.2.1	P.2.2	P.2.3	P.2.4	P.2.4.1	P.2.4.2
10																															x	
11																																x
12																																
12a																																
12b																																
12c																																
13												x																				
13a												x																				
13b												x																				
14																																
14a																																
14b																																
14c																																
15								x																								
15a																																
16																																
17																																
18																																
19																																
19a																																
19b																																
20																																
21																																
22																																
22a																																
22b																																
23																																
24	x																															
24a		x																														
24b					x																											
24c										x																						
24d											x																					
25			x																													
26				x																												
27					x																											
27a						x																										
27b							x																									

CT4 SQ4	G	G.1	G.1.1	G.1.2	G.2	G.2.1	G.2.2	G.2.2.1	G.2.3	G.3	G.4	Ag	Ag.1	Ag.2	Ag.3	Ag.4	Ag.5	Ag.6	Ag.7	P	P.1	P.1.1	P.1.1.1	P.1.1.2	P.1.1.3	P.1.2	P.2	P.2.1	P.2.2	P.2.3	P.2.4	P.2.4.1	P.2.4.2
27c									x																								
28										x																							
29											x																						
30												x																	x				
30a													x																				
30b														x																			
30c												x																					
31												x																					
31a													x																				
31b														x																			
31c														x																			
31d												x																					
31e															x																		
31f																x																	
31g												x																					
31h																		x															
32																	x																

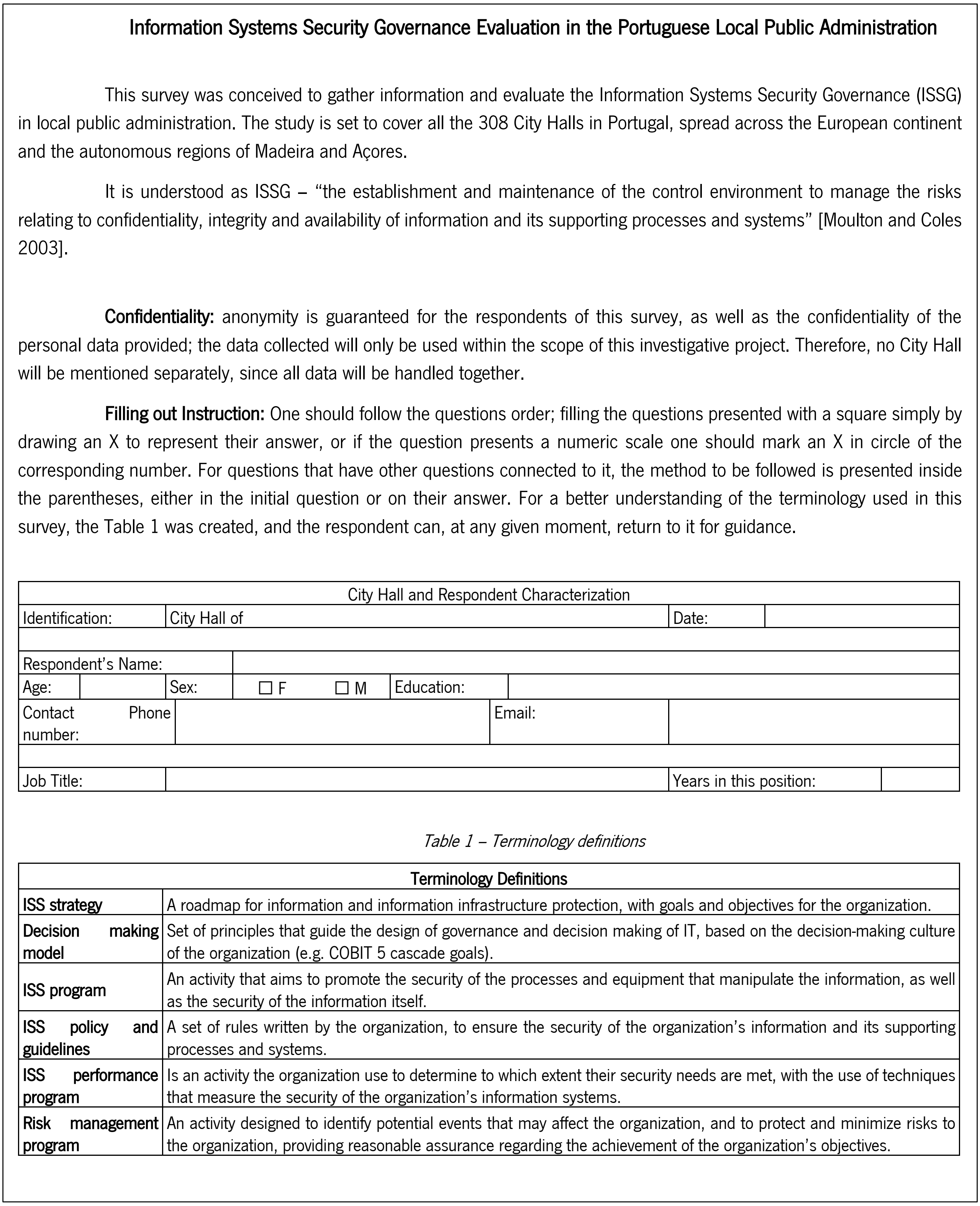
Table 70 – Matrix Instrument v4 and Concept Tree 4 (Part 2)

CT4 / SQ4	P.2.5	P.2.5.1	P.2.5.2	P.2.5.3	P.2.5.4	P.2.5.5	P.2.5.6	P.3	P.3.1	P.3.1.1	P.3.2	P.3.2.1	P.3.3	P.3.4	P.3.5	P.3.6	AR	AR.1	AR.1.1	AR.2	AR.2.1	AR.2.2	AR.2.3	AR.3	AR.3.1	AR.3.2	AR.3.3	AR.4	AR.4.1	AR.4.1.1	AR.4.2	AR.4.3	AR.5	AR.5.1	AR.5.2	AR.5.2.1	AR.5.3	AR.5.4
1																		x																				
1a																			x																			
2																				x																		
2a									x																													
2b																					x	x	x															
3																								x														
3a																																						
3b						x																																
3c														x											x	x	x											
3d											x																											
4																												x										
4a																													x		x	x						
4b																														x								
4c														x																								
5																																	x					
5a																																		x	x	x	x	x
6																																						
6a																																						
6b																																						
6c																																						
7																																						
8																																						
8a																																						
8b																																						
8c																																						
8d																																						
9																																						
9a											x		x																									
9b																																						
10																																						
11																																						
12	x																																					
12a		x																																				

CT4 SQ4	P.2.5	P.2.5.1	P.2.5.2	P.2.5.3	P.2.5.4	P.2.5.5	P.2.5.6	P.3	P.3.1	P.3.1.1	P.3.2	P.3.2.1	P.3.3	P.3.4	P.3.5	P.3.6	AR	AR.1	AR.1.1	AR.2	AR.2.1	AR.2.2	AR.2.3	AR.3	AR.3.1	AR.3.2	AR.3.3	AR.4	AR.4.1	AR.4.1.1	AR.4.2	AR.4.3	AR.5	AR.5.1	AR.5.2	AR.5.2.1	AR.5.3	AR.5.4
12b			x																																			
12c					x																																	
13			x																																			
13a																																						
13b			x																																			
14	x																																					
14a						x																																
14b							x																															
14c				x																																		
15									x																													
15a									x				x																									
16														x																								
17									x																													
18										x																												
19											x																											
19a												x																										
19b											x		x			x																						
20																x																						
21													x																									
22											x		x																									
22a					x						x																											
22b											x																											
23															x																							
24																																						
24a																																						
24b																																						
24c																																						
24d																																						
25																																						
26																																						
27																																						
27a																																						
27b																																						
27c																																						
28																																						
29																																						

CT4 / SQ4	P.2.5	P.2.5.1	P.2.5.2	P.2.5.3	P.2.5.4	P.2.5.5	P.2.5.6	P.3	P.3.1	P.3.1.1	P.3.2	P.3.2.1	P.3.3	P.3.4	P.3.5	P.3.6	AR	AR.1	AR.1.1	AR.2	AR.2.1	AR.2.2	AR.2.3	AR.3	AR.3.1	AR.3.2	AR.3.3	AR.4	AR.4.1	AR.4.1.1	AR.4.2	AR.4.3	AR.5	AR.5.1	AR.5.2	AR.5.2.1	AR.5.3	AR.5.4
30																	x	x		x				x				x					x					
30a																																						
30b																																						
30c																																						
31										x		x			x																							
31a																																						
31b																																						
31c																																						
31d																																						
31e																																						
31f																																						
31g																																						
31h																																						
32																																						

- Instrument v4



Information Systems Security Governance Evaluation in the Portuguese Local Public Administration

This survey was conceived to gather information and evaluate the Information Systems Security Governance (ISSG) in local public administration. The study is set to cover all the 308 City Halls in Portugal, spread across the European continent and the autonomous regions of Madeira and Açores.

It is understood as ISSG – "the establishment and maintenance of the control environment to manage the risks relating to confidentiality, integrity and availability of information and its supporting processes and systems" [Moulton and Coles 2003].

Confidentiality: anonymity is guaranteed for the respondents of this survey, as well as the confidentiality of the personal data provided; the data collected will only be used within the scope of this investigative project. Therefore, no City Hall will be mentioned separately, since all data will be handled together.

Filling out Instruction: One should follow the questions order; filling the questions presented with a square simply by drawing an X to represent their answer, or if the question presents a numeric scale one should mark an X in circle of the corresponding number. For questions that have other questions connected to it, the method to be followed is presented inside the parentheses, either in the initial question or on their answer. For a better understanding of the terminology used in this survey, the Table 1 was created, and the respondent can, at any given moment, return to it for guidance.

City Hall and Respondent Characterization					
Identification:	City Hall of			Date:	
Respondent's Name:					
Age:		Sex:	□ F □ M	Education:	
Contact Phone number:				Email:	
Job Title:				Years in this position:	

Table 1 – Terminology definitions

Terminology Definitions	
ISS strategy	A roadmap for information and information infrastructure protection, with goals and objectives for the organization.
Decision making model	Set of principles that guide the design of governance and decision making of IT, based on the decision-making culture of the organization (e.g. COBIT 5 cascade goals).
ISS program	An activity that aims to promote the security of the processes and equipment that manipulate the information, as well as the security of the information itself.
ISS policy and guidelines	A set of rules written by the organization, to ensure the security of the organization's information and its supporting processes and systems.
ISS performance program	Is an activity the organization use to determine to which extent their security needs are met, with the use of techniques that measure the security of the organization's information systems.
Risk management program	An activity designed to identify potential events that may affect the organization, and to protect and minimize risks to the organization, providing reasonable assurance regarding the achievement of the organization's objectives.

Figure 27 – Instrument Version 4

Artifacts

1		Does the organization has an ISS strategy?	☐ Yes (proceed to 1a) ☐ No (proceed to 2)
	a)	Is a decision making model present? (proceed to 2)	☐ Yes ☐ No
2		Does an ISS program exists in the organization?	☐ Yes (proceed to 2a) ☐ No (proceed to 3)
	a)	How would the effectiveness (accomplishment/completion of planned activities) of the ISS program be qualified? (proceed to 2b) (**<u>Scale measures</u>**: 1 – not effective [between 0 and 20% accomplished]; 3 – somewhat effective [between 41 and 60% accomplished]; 5 – very effective [between 81 and 100% accomplished])	○—○—○—○—○ **1 2 3 4 5**
	b)	Is investment distribution, resource allocation and responsibility assignment contemplated to which extent in the ISS program? (**<u>Scale measures</u>**: 1 – not contemplated; 3 – sufficiently contemplated; 5 – fully contemplated)	○—○—○—○—○ **1 2 3 4 5**
3		Has an ISS policy and guidelines been created in the organization?	☐ Yes (proceed to 3a) ☐ No (proceed to 4)
	a)	Are the ISS policy and guidelines implemented in the organization?	☐ Yes (proceed to 3b) ☐ No (proceed to 4)
	b)	To whom are the ISS policy and guidelines available? (proceed to 3c)	☐ Organization's employees ☐ Organization's employees and contractors ☐ Everyone with clearance ☐ Everyone
	c)	In regards of the authority levels, the escalation guidelines and the reporting and communicating structure; how would you evaluate their definition, description and clarity? (proceed to 3d) (**<u>Scale measures</u>**: 1 – poorly covered; 3 – sufficiently covered; 5 – very well covered)	○—○—○—○—○ **1 2 3 4 5**
	d)	Is the ISS policy supported by written standards; and are those standards supported by written procedures?	☐ Yes ☐ No
4		Is there a program in place to assess the ISS performance (the use measures to determine to which stand the organization's ISS needs were met)?	☐ Yes (proceed to 4a) ☐ No (proceed to 5)
	a)	Does the ISS performance program contemplate, to which extent, the actions for communicating and reporting events, actions to address resource management deviations and audit reports? (proceed to 4b) (**<u>Scale measures</u>**: 1 – poorly contemplated; 3 – sufficiently contemplated; 5 – very well contemplated)	○—○—○—○—○ **1 2 3 4 5**
	b)	In the reporting and communication's action, is stakeholder's feedback discussed? (proceed to 4c)	☐ Yes ☐ No
	c)	Is the information gathered from the ISS performance considered when selecting new metrics, that are in accordance with the business objectives?	☐ Yes ☐ No
5		Is a risk management program present at the organization?	☐ Yes (proceed to 5a) ☐ No (proceed to 6)
	a)	How well the risk subject (such as risk assessment, risk policies, risk tolerance level, risk appetite and risk mitigation) is discussed in the program? (**<u>Scale measures</u>**: 1 – poorly discussed; 3 – sufficiently discussed; 5 – very well discussed)	○—○—○—○—○ **1 2 3 4 5**

Processes

6	How would you evaluate the alignment of the ISS with the business strategy ... (proceed to 6a) (**Scale measures**: 1 – poorly aligned; 3 – sufficiently aligned; 5 – completely aligned)		
	a)	when considering the ISS issues in the business initiatives? (proceed to 6b)	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
	b)	to support the business objectives? (proceed to 6c)	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
	c)	in handling the results from the ISS performance, like prioritizing and/or initiating the required actions derived from those results?	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
7	Are benefits (such as: good results, profits or advantages) perceived from the investments in ISS?		☐ Yes ☐ No
8	How would you describe the commitment of the executive management in ... (proceed to 8a) (**Scale measures**: 1 – not committed; 3 – sufficiently committed; 5 – fully committed)		
	a)	protecting the information assets? (proceed to 8b)	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
	b)	making ISS related decisions? (proceed to 8c)	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
	c)	developing and approving the ISS strategy and policy? (proceed to 8d)	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
	d)	allocating investments and resources?	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
9	Does the organization follow a risk management policy to manage the risks encountered?		☐ Yes (proceed to 9a) ☐ No (proceed to 10)
	a)	How often are the risks reviewed? (proceed to 9b) (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	○ 1 ○ 2 ○ 3
	b)	Is the risk appetite described in the policy?	☐ Yes ☐ No
10	Is there a guideline/plan to be followed to determine the risk appetite for new risks?		☐ Yes ☐ No
11	Are procedures in place to oversee ISS incidents, including public and investor relations, and is there any coordination with law enforcement?		☐ Yes ☐ No
12	How much is covered in the resource management of the ISS program for ... (proceed to 12a) (**Scale measures**: 1 – not covered; 3 – sufficiently covered; 5 – fully covered)		
	a)	assignment of responsibilities? (proceed to 12b)	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
	b)	having competent and motivated personnel? (proceed to 12c)	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
	c)	promoting a positive information security culture?	○ 1 ○ 2 ○ 3 ○ 4 ○ 5

13		What is the career level of the person in charge of the ISS? (proceed to 13a)	☐ University degree ☐ Technical degree ☐ High School degree
	a)	Is this an officer-level position or a managerial position? (proceed to 13b)	☐ managerial ☐ officer-level
	b)	Does this person has other roles?	☐ Yes ☐ No
14		How much is covered of the stakeholders communication and reporting in the ISS program for … (proceed to 14a) (**Scale measures**: 1 – poorly covered; 3 – sufficiently covered; 5 – very well covered)	
	a)	reporting and communication of principles and guidelines? (proceed to 14b)	○—○—○—○—○ 1 2 3 4 5
	b)	principles for safeguarding the resources? (proceed to 14c)	○—○—○—○—○ 1 2 3 4 5
	c)	escalation guidelines?	○—○—○—○—○ 1 2 3 4 5
15		How would you quantify the effectiveness of the ISS activities? (proceed to 15a) (**Scale measures**: 1 – not effective [between 0 and 20% accomplished]; 2 – between 21 and 40% accomplished; 3 – somewhat effective [between 41 and 60% accomplished]; 4 – between 61 and 80% accomplished; 5 – very effective [between 81 and 100% accomplished])	○—○—○—○—○ 1 2 3 4 5
	a)	How often is the effectiveness of the ISS activity assessed? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	○—○—○ 1 2 3
16		Does the selected ISS performance metrics ponder the business perspective?	☐ Yes ☐ No
17		Does the ISS activity receive effective/meaningful feedback from the groups(units) it works with?	☐ Yes ☐ No
18		Are the results of the ISS performance used in providing feedback and demonstrating their impacts on the organization?	☐ Yes ☐ No
19		Is the ISS program reviewed to verify their compliance with legislation, regulations, contractual obligations and statutory requirements?	☐ Yes (proceed to 19a) ☐ No (proceed to 20)
	a)	Is the compliance of the information security practices and their alignment to the organization's business nature, reported to the stakeholders? (proceed to 19b)	☐ Yes ☐ No
	b)	Is there an internal or external regulatory compliance group (auditors), and when did the ISS activity last met with them? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	○—○—○ 1 2 3
20		Are independent audits commissioned to verify the determined level for the information security?	☐ Yes ☐ No
21		Does the ISS strategy considers the changes in different types of environment (business, legal and regulatory) and their potential information risk?	☐ Yes ☐ No
22		How often are regulations reviewed to understand the ISS requirements? (proceed to 22a) (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	○—○—○ 1 2 3
	a)	Is the legal department involved in the review process of the ISS activity?	☐ Yes (proceed to 22b) ☐ No (proceed to 23)
	b)	When did the ISS activity last review a contractual requirement with the legal counsel? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	○—○—○ 1 2 3
23		Is there a feedback provided by the organization, that regards the transparency of IT costs, benefits and risks?	☐ Yes ☐ No

Goals

24	How would you evaluate the accomplishment of the ISSG goals for … (proceed to 24a) (**Scale measures**: 1 – not accomplished; 3 – sufficiently accomplished; 5 – fully accomplished)		
	a)	strategic alignment (the link between the ISS strategy and the organization's business)? (proceed to 24b)	○—○—○—○—○ 1 2 3 4 5
	b)	value delivery (the delivery of promised benefits while optimizing costs)? (proceed to 24c)	○—○—○—○—○ 1 2 3 4 5
	c)	accountability (accept responsibility for the ISSG actions in the organization)? (proceed to 24d)	○—○—○—○—○ 1 2 3 4 5
	d)	compliance (fulfill requirements in accordance with some specified standard)?	○—○—○—○—○ 1 2 3 4 5
25	To which extent are the needs of the stakeholders balanced in the process of creating an ISSG strategy? (**Scale measures**: 1 – not balanced; 3 – sufficiently balanced; 5 – fully balanced)		○—○—○—○—○ 1 2 3 4 5
26	Are the ISSG fundaments (such as goals and objectives) integrated within all levels of the organization?		☐ Yes ☐ No
27	To which degree is the value for the governance of the ISS perceived by the organization … (proceed to 27a) (**Scale measures**: 1 – no value added [between 0 and 20%]; 2 – between 21 and 40%; 3 – fair amount of value added [between 41 and 60%]; 4 – between 61 and 80%; 5 – a lot of value added [between 81 and 100%])		
	a)	the cost-effectiveness (accomplish what was set out, considering the cost)? (proceed to 27b)	○—○—○—○—○ 1 2 3 4 5
	b)	the efficiency (degree of achieving the desired result with little waste)? (proceed to 27c)	○—○—○—○—○ 1 2 3 4 5
	c)	the optimization of resources, assets and capabilities?	○—○—○—○—○ 1 2 3 4 5
28	Has the ISSG set out rules that makes people/roles accountable for their actions/responsibilities?		☐ Yes ☐ No
29	How much is compliance (the conformity to fulfill official requirements) a part of the ISSG in the organization? (**Scale measures**: 1 – not important [between 0 and 20% of compliance]; 3 – somewhat important [between 41 and 60% of compliance]; 5 – very important [between 81 and 100% of compliance])		○—○—○—○—○ 1 2 3 4 5

Agents

30	Mark the correspondent artifact, that each role is responsible for developing. (Multiple choices accepted) (proceed to 30 a through c)						
		Role	Artifacts				
	a)	Governing body (person or group accountable for the organization's performance and conformity)	☐ ISS strategy	☐ ISS program	☐ ISS policies and guidelines	☐ ISS performance program	☐ Risk management program
	b)	City Hall executive (group usually formed by the city hall mayor and members of the city council)	☐ ISS strategy	☐ ISS program	☐ ISS policies and guidelines	☐ ISS performance program	☐ Risk management program
	c)	Chief Information Security Officer (CISO) (responsible for all the ISS activities)	☐ ISS strategy	☐ ISS program	☐ ISS policies and guidelines	☐ ISS performance program	☐ Risk management program

31	Mark the correspondent reporting role, that each main role is responsible for reporting to? (proceed to 31 a through h)					
		Main Role	Reports to			
	a)	Governing body	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders
	b)	Mayor (person elected to act as head of a city)	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders
	c)	City Councilor (member of the legislative body that governs the city)	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders
	d)	Chief Information Officer (CIO) (responsible for the ISS program, policy; and its compliance)	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders
	e)	Auditors (responsible for assessing the governance activities compliance with the standards)	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders
	f)	Data Protection Officer (DPO) (responsible for overseeing the data protection strategy, implementation and compliance with the GDPR)	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders
	g)	Chief Information Security Officer (CISO)	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders
	h)	Employees (individual who is payed to work)	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders

32	Is the CISO driving the ISS activity or mostly reporting compliance?	☐ directing the ISS activity ☐ reporting compliance on the ISS activity

- Matrix for Instrument v5 and Concept Tree v5

Table 71 – Matrix Instrument v5 and Concept Tree 5 (Part 1)

CT5 SQ5	G	G.1	G.1.1	G.1.2	G.2	G.2.1	G.2.2	G.3	G.4	Ag	Ag.1	Ag.2	Ag.3	Ag.4	Ag.5	Ag.6	Ag.7	P	P.1	P.1.1	P.1.1.1	P.1.1.2	P.1.1.3	P.1.2	P.2	P.2.1	P.2.2	P.2.3	P.2.4	P.2.4.1	P.2.4.2
1																															
1a																															
2																															
2a																															
2b																															
3																															
3a				x																											
3b																															
3c																															
3d																															
4																															
4a																															
4b																															
4c																															
5																															
5a																															
6																				x											
6a																					x										
6b																						x									
6c																							x								
7																								x							
8																										x					
8a																										x					
8b																										x					
8c																											x				
8d																												x			
9																													x		x
9a																															
9b																														x	

CT5 SQ5	G	G.1	G.1.1	G.1.2	G.2	G.2.1	G.2.2	G.3	G.4	Ag	Ag.1	Ag.2	Ag.3	Ag.4	Ag.5	Ag.6	Ag.7	P	P.1	P.1.1	P.1.1.1	P.1.1.2	P.1.1.3	P.1.2	P.2	P.2.1	P.2.2	P.2.3	P.2.4	P.2.4.1	P.2.4.2
10																														x	
11																															x
12																															x
13																															
13a																															
13b																															
13c																															
14																															
14a																															
14b																															
14c																															
15																															
15a																															
16																															
17																															
18																															
19																															
20																															
20a																															
20b																															
20c																															
21																															
22																															
23																															
23a																															
23b																															
24																															
25	x																														
25a		x																													
25b					x																										
25c								x																							
25d									x																						
26			x																												
27				x																											
28					x																										
28a						x																									
28b							x																								

CT5 / SQ5	G	G.1	G.1.1	G.1.2	G.2	G.2.1	G.2.2	G.3	G.4	Ag	Ag.1	Ag.2	Ag.3	Ag.4	Ag.5	Ag.6	Ag.7	P	P.1	P.1.1	P.1.1.1	P.1.1.2	P.1.1.3	P.1.2	P.2	P.2.1	P.2.2	P.2.3	P.2.4	P.2.4.1	P.2.4.2
29								x																							
30									x																						
31										x																					
31a															x																
31b										x																					
31c										x																					
32										x																	x				
32a											x																				
32b												x																			
32c										x																					
33										x																					
33a											x																				
33b												x																			
33c												x																			
33d										x																					
33e													x																		
33f														x																	
33g																x															

Table 72 – Matrix Instrument v5 and Concept Tree 5 (Part 2)

CT5 / SQ5	P.2.5	P.2.5.1	P.2.5.2	P.2.5.3	P.2.5.4	P.2.5.5	P.2.5.6	P.3	P.3.1	P.3.1.1	P.3.2	P.3.2.1	P.3.3	P.3.4	P.3.5	P.3.6	AR	AR.1	AR.1.1	AR.2	AR.2.1	AR.2.2	AR.2.3	AR.3	AR.3.1	AR.3.2	AR.3.3	AR.4	AR.4.1	AR.4.1.1	AR.4.2	AR.4.3	AR.5	AR.5.1	AR.5.2	AR.5.2.1	AR.5.3	AR.5.4
1																		x																				
1a																			x																			
2																				x																		
2a									x																													
2b																					x	x	x															
3																								x														
3a																																						
3b						x																																
3c														x											x	x	x											
3d											x																											
4																												x										
4a																													x		x	x						
4b																														x								
4c														x																								
5																																	x					
5a																																		x	x	x	x	x
6																																						
6a																																						
6b																																						
6c																																						
7																																						
8																																						
8a																																						
8b																																						
8c																																						
8d																																						
9																																						
9a											x		x																									
9b																																						
10																																						
11																																						
12																																						
13	x																																					

CT5 SQ5	P.2.5	P.2.5.1	P.2.5.2	P.2.5.3	P.2.5.4	P.2.5.5	P.2.5.6	P.3	P.3.1	P.3.1.1	P.3.2	P.3.2.1	P.3.3	P.3.4	P.3.5	P.3.6	AR	AR.1	AR.1.1	AR.2	AR.2.1	AR.2.2	AR.2.3	AR.3	AR.3.1	AR.3.2	AR.3.3	AR.4	AR.4.1	AR.4.1.1	AR.4.2	AR.4.3	AR.5	AR.5.1	AR.5.2	AR.5.2.1	AR.5.3	AR.5.4
13a		x																																				
13b			x																																			
13c					x																																	
14	x																																					
14a						x																																
14b							x																															
14c				x																																		
15									x																													
15a									x				x																									
16														x																								
17									x																													
18										x																												
19										x																												
20											x																											
20a												x																										
20b																x																						
20c											x		x																									
21																x																						
22													x																									
23											x		x																									
23a					x						x																											
23b											x																											
24															x																							
25																																						
25a																																						
25b																																						
25c																																						
25d																																						
26																																						
27																																						
28																																						
28a																																						
28b																																						
29																																						
30																																						
31																																						
31a																																						

CT5 / SQ5	P.2.5	P.2.5.1	P.2.5.2	P.2.5.3	P.2.5.4	P.2.5.5	P.2.5.6	P.3	P.3.1	P.3.1.1	P.3.2	P.3.2.1	P.3.3	P.3.4	P.3.5	P.3.6	AR	AR.1	AR.1.1	AR.2	AR.2.1	AR.2.2	AR.2.3	AR.3	AR.3.1	AR.3.2	AR.3.3	AR.4	AR.4.1	AR.4.1.1	AR.4.2	AR.4.3	AR.5	AR.5.1	AR.5.2	AR.5.2.1	AR.5.3	AR.5.4
31b			x																																			
31c			x																																			
32																	x	x		x				x				x					x					
32a																																						
32b																																						
32c																																						
33										x		x			x																							
33a																																						
33b																																						
33c																																						
33d																																						
33e																																						
33f																																						
33g																																						

- Instrument Questions v2 to v5

Table 73 – Instrument Questions v2 to v5

	v2
1	Does the organization has an ISS strategy?
a)	Is a decision making model present?
2	Does an ISS program exists in the organization?
a)	How would the effectiveness of this ISS program be qualified?
b)	Are investment distribution, resource allocation and responsibility assignment contemplated to which extent in the ISS program?
3	Has an ISS policy and guidelines been created in the organization?
a)	Are the ISS policy and guidelines implemented in the organization?

	v3
1	Does the organization has an ISS strategy?
a)	Is a decision making model present?
2	Does an ISS program exists in the organization?
a)	How would the effectiveness (accomplishment/completion of planned activities) of the ISS program be qualified? (Scale measures: 1 – not effective [between 0 and 20% accomplished]; 3 – somewhat effective [between 41 and 60% accomplished]; 5 – very effective [between 81 and 100% accomplished])
b)	Is investment distribution, resource allocation and responsibility assignment contemplated to which extent in the ISS program? (Scale measures: 1 – not contemplated; 3 – sufficiently contemplated; 5 – fully contemplated)
3	Has an ISS policy and guidelines been created in the organization?
a)	Are the ISS policy and guidelines implemented in the organization?
b)	To whom is the ISS policy available?

	v4
1	Does the organization has an ISS strategy?
a)	Is a decision making model present?
2	Does an ISS program exists in the organization?
a)	How would the effectiveness (accomplishment/completion of planned activities) of the ISS program be qualified? (Scale measures: 1 – not effective [between 0 and 20% accomplished]; 3 – somewhat effective [between 41 and 60% accomplished]; 5 – very effective [between 81 and 100% accomplished])
b)	Is investment distribution, resource allocation and responsibility assignment contemplated to which extent in the ISS program? (Scale measures: 1 – not contemplated; 3 – sufficiently contemplated; 5 – fully contemplated)
3	Has an ISS policy and guidelines been created in the organization?
a)	Are the ISS policy and guidelines implemented in the organization?
b)	To whom are the ISS policy and guidelines available?

	v5
1	Does the organization has an ISS strategy?
a)	In the ISS strategy is a decision making model present?
2	Does an ISS program exists in the organization?
a)	How would the effectiveness (accomplishment/completion of planned activities) of the ISS program be qualified? (Scale measures: **1** – not effective [between 0 and 20% accomplished]; **3** – somewhat effective [between 41 and 60% accomplished]; **5** – very effective [between 81 and 100% accomplished])
b)	The investment distribution, resource allocation and responsibility assignment contemplated to which extent in the ISS program? (Scale measures: **1** – not contemplated; **3** – sufficiently contemplated; **5** – fully contemplated)
3	Have an ISS policy and guidelines been created in the organization?
a)	Are the ISS policy and guidelines implemented in the organization?
b)	To whom are the ISS policy and guidelines available?

	v2		v3		v4		v5
b)	In regards of the authority levels, the escalation guidelines and the reporting and communicating structure; how would you evaluate their definition, description and clarity?	c)	In regards of the authority levels, the escalation guidelines and the reporting and communicating structure; how would you evaluate their definition, description and clarity? (**Scale measures**: 1 – poorly covered; 3 – sufficiently covered; 5 – very well covered)	c)	In regards of the authority levels, the escalation guidelines and the reporting and communicating structure; how would you evaluate their definition, description and clarity? (**Scale measures**: 1 – poorly covered; 3 – sufficiently covered; 5 – very well covered)	c)	In regards of the authority levels, the escalation guidelines and the reporting and communicating structure; how would you evaluate their definition, description and clarity? (**Scale measures**: **1** – poorly covered; **3** – sufficiently covered; **5** – very well covered)
				d)	Is the ISS policy supported by written standards; and are those standards supported by written procedures?	d)	Is the ISS policy supported by written standards; and are those standards supported by written procedures?
4	Is there a program in place to assess the ISS performance?	4	Is there a program in place to assess the ISS performance (the use measures to determine to which stand the organization's ISS needs were met)?	4	Is there a program in place to assess the ISS performance (the use measures to determine to which stand the organization's ISS needs were met)?	4	Is there a program in place to assess the ISS performance (the use measures to determine to which stand the organization's ISS needs were met)?
a)	Does the ISS performance program contemplate actions for communicating and reporting events, actions to address resource management deviations and audit reports? To which extent?	a)	Does the ISS performance program contemplate, to which extent, the actions for communicating and reporting events, actions to address resource management deviations and audit reports? (**Scale measures**: 1 – poorly contemplated; 3 – sufficiently contemplated; 5 – very well contemplated)	a)	Does the ISS performance program contemplate, to which extent, the actions for communicating and reporting events, actions to address resource management deviations and audit reports? (**Scale measures**: 1 – poorly contemplated; 3 – sufficiently contemplated; 5 – very well contemplated)	a)	Does the ISS performance program contemplate, to which extent, the actions for communicating and reporting events, actions to address resource management deviations and audit reports? (**Scale measures**: **1** – poorly contemplated; **3** – sufficiently contemplated; **5** – very well contemplated)
b)	In the reporting and communication's actions, is stakeholder's feedback discussed?	b)	In the reporting and communication's actions, is stakeholder's feedback discussed?	b)	In the reporting and communication's action, is stakeholder's feedback discussed?	b)	In the reporting and communication's action, is stakeholder's feedback discussed?
c)	Is there any information gathered from the ISS performance program? If so, is this information, used to select the metrics in accordance with the business perspective?	c)	Is there any information gathered from the ISS performance program? If so, is this information, used to select the metrics in accordance with the business perspective?	c)	Is the information gathered from the ISS performance considered when selecting new metrics, that are in accordance with the business objectives?	c)	Is the information gathered from the ISS performance considered when selecting new metrics, that are in accordance with the organization's objectives?
5	Is a risk management program present at the organization?	5	Is a risk management program present at the organization?	5	Is a risk management program present at the organization?	5	Is a risk management program present at the organization?
a)	How well is the risk subject (such as risk assessment, risk policies, risk tolerance level, risk appetite and risk mitigation) discussed in the program?	a)	How well is the risk subject (such as risk assessment, risk policies, risk tolerance level, risk appetite and risk mitigation) discussed in the program? (**Scale measures**: 1 – poorly discussed; 3 – sufficiently discussed; 5 – very well discussed)	a)	How well the risk subject (such as risk assessment, risk policies, risk tolerance level, risk appetite and risk mitigation) is discussed in the program? (**Scale measures**: 1 – poorly discussed; 3 – sufficiently discussed; 5 – very well discussed)	a)	How well the risk subject (such as risk assessment, risk management policies, risk tolerance level, risk appetite and risk mitigation) is discussed in the program? (**Scale measures**: **1** – poorly discussed; **3** – sufficiently discussed; **5** – very well discussed)

	v2		v3		v4		v5
6	How would you evaluate the alignment of the ISS with the business strategy	6	How would you evaluate the alignment of the ISS with the business strategy … (Scale measures: 1 – poorly aligned; 3 – sufficiently aligned; 5 – completely aligned)	6	How would you evaluate the alignment of the ISS with the business strategy … (Scale measures: 1 – poorly aligned; 3 – sufficiently aligned; 5 – completely aligned)	6	How would you evaluate the alignment of the ISS with the business strategy … (Scale measures: **1** – poorly aligned; **3** – sufficiently aligned; **5** – completely aligned)
a)	Does the business initiatives considers the ISS issues	a)	when considering the ISS issues in the business initiatives?	a)	when considering the ISS issues in the business initiatives?	a)	when considering the ISS issues in the organization initiatives?
b)	Are the business objective supported by the ISS	b)	to support the business objectives?	b)	to support the business objectives?	b)	to support the organization objectives?
c)	How does the organization handle the results from the ISS performance? Does the organization prioritizes and initiate the required actions?	c)	in handling the results from the ISS performance; and when prioritizing and/or initiating the required actions derived from the results of the ISS performance?	c)	in handling the results from the ISS performance, like prioritizing and/or initiating the required actions derived from those results?	c)	in handling the results from the ISS performance, like prioritizing or initiating the required actions derived from those results?
7	Are benefits (such as: good results, profits or advantages) perceived from the investments in ISS?	7	Are benefits (such as: good results, profits or advantages) perceived from the investments in ISS?	7	Are benefits (such as: good results, profits or advantages) perceived from the investments in ISS?	7	Are benefits (such as: good results or advantages) perceived from the investments in ISS?
8	How would you describe the commitment of the executive management in	8	How would you describe the commitment of the executive management in … (Scale measures: 1 – not committed; 3 – sufficiently committed; 5 – fully committed)	8	How would you describe the commitment of the executive management in … (Scale measures: 1 – not committed; 3 – sufficiently committed; 5 – fully committed)	8	How would you describe the commitment of the executive management in … (Scale measures: **1** – not committed; **3** – sufficiently committed; **5** – fully committed)
a)	Protecting the information assets	a)	protecting the information assets?	a)	protecting the information assets?	a)	protecting the information assets?
b)	Making ISS related decisions	b)	making ISS related decisions?	b)	making ISS related decisions?	b)	making ISS related decisions?
c)	Developing and approving the ISS strategy and policy	c)	developing and approving the ISS strategy and policy?	c)	developing and approving the ISS strategy and policy?	c)	developing and approving the ISS strategy and policy?
d)	Allocating investments and resources	d)	allocating investments and resources?	d)	allocating investments and resources?	d)	allocating investments and resources?
9	Does the organization follows a risk management policy to manage the risks encountered?	9	Does the organization follow a risk management policy to manage the risks encountered?	9	Does the organization follow a risk management policy to manage the risks encountered?	9	Does the organization follow a risk management policy to manage the risks encountered?
		a)	Are ISS policies supported by written standards; and are those standards supported by written procedures?	a)	How often are the risks reviewed? (Scale measures: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	a)	How often are the risks reviewed? (Scale measures: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)
a)	Is the risk appetite described in the policy?	b)	Is the risk appetite described in the policy?	b)	Is the risk appetite described in the policy?	b)	Is the risk appetite described in the policy?

	v2		v3			v4			v5
b)	How is the risk appetite determined?	c)	How often are the risks reviewed? (**Scale measures**: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	9a)					
10	Does the organization has a guideline/plan to follow to determine the risk appetite for new risks?	10	Does the organization has a guideline/plan to follow to determine the risk appetite for new risks?		10	Is there a guideline/plan to be followed to determine the risk appetite for new risks?		10	Is there a guideline or plan to be followed to determine the risk appetite for new risks?
		11	Are procedures in place to oversee ISS incidents, including public and investor relations, and is there any coordination with law enforcement?		11	Are procedures in place to oversee ISS incidents, including public and investor relations, and is there any coordination with law enforcement?	11 & 12	11	Are procedures in place to oversee ISS incidents, including public and investor relations?
								12	Are there procedures in place, that coordinate with law enforcement, to oversee ISS incidents?
11	How much is covered in the resource management of the ISS program?	12	How much is covered in the resource management of the ISS program for … (**Scale measures**: 1 – not covered; 3 – sufficiently covered; 5 – fully covered)		12	How much is covered in the resource management of the ISS program for … (**Scale measures**: 1 – not covered; 3 – sufficiently covered; 5 – fully covered)		13	How much is covered in the resource management of the ISS program for … (**Scale measures**: **1** – not covered; **3** – sufficiently covered; **5** – fully covered)
a)	Assignment of responsibilities	a)	assignment of responsibilities?		a)	assignment of responsibilities?		a)	assignment of responsibilities?
b)	Have competent and motivated personnel	b)	having competent and motivated personnel?		b)	having competent and motivated personnel?		b)	having competent and motivated personnel?
c)	Promotion of a positive information security culture	c)	promoting a positive information security culture?		c)	promoting a positive information security culture?		c)	promoting a positive information security culture?
		13	What is the career level of the person in charge of the ISS?		13	What is the career level of the person in charge of the ISS?	31b		
		a)	Is this an officer-level position or a managerial position?		a)	Is this an officer-level position or a managerial position?			
		b)	Does this person has other roles?		b)	Does this person has other roles?	31c		
12	How much is covered of the stakeholders communication and reporting in the ISS program?	14	How much is covered of the stakeholders communication and reporting in the ISS program for … (**Scale measures**: 1 – poorly covered; 3 – sufficiently covered; 5 – very well covered)		14	How much is covered of the stakeholders communication and reporting in the ISS program for … (**Scale measures**: 1 – poorly covered; 3 – sufficiently covered; 5 – very well covered)		14	How much is covered of the stakeholders communication and reporting in the ISS program for … (**Scale measures**: **1** – poorly covered; **3** – sufficiently covered; **5** – very well covered)
a)	Reporting and communication principles and guidelines	a)	reporting and communication of principles and guidelines?		a)	reporting and communication of principles and guidelines?		a)	reporting and communication of principles and guidelines?
b)	Principles for safeguarding the resources	b)	principles for safeguarding the resources?		b)	principles for safeguarding the resources?		b)	principles for safeguarding the resources?
c)	Escalation guidelines	c)	escalation guidelines?		c)	escalation guidelines?		c)	escalation guidelines?

	v2		v3		v4			v5
13	How would you quantify the effectiveness (accomplishment/completion of what was set out) of the management of the information security activities?	15	How would you quantify the effectiveness (accomplishment/completion of what was set out) of the management of the information security activities?	15	How would you quantify the effectiveness of the ISS activities?		15	How would you quantify the effectiveness of the ISS activities?
			(Scale measures: 1 – not effective [between 0 and 20% accomplished]; 2 – between 21 and 40% accomplished; 3 – somewhat effective [between 41 and 60% accomplished]; 4 – between 61 and 80% accomplished; 5 – very effective [between 81 and 100% accomplished])		(Scale measures: 1 – not effective [between 0 and 20% accomplished]; 2 – between 21 and 40% accomplished; 3 – somewhat effective [between 41 and 60% accomplished]; 4 – between 61 and 80% accomplished; 5 – very effective [between 81 and 100% accomplished])			(Scale measures: **1** – not effective [between 0 and 20% accomplished]; **3** – somewhat effective [between 41 and 60% accomplished]; **5** – very effective [between 81 and 100% accomplished])
		a)	How often is the effectiveness of the ISS activity assessed?	a)	How often is the effectiveness of the ISS activity assessed?		a)	How often is the effectiveness of the ISS activity assessed?
			(Scale measures: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)		(Scale measures: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)			(Scale measures: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)
14	Does the selected information security performance metrics ponder the business perspective?	16	Does the selected information security performance metrics ponder the business perspective?	16	Does the selected ISS performance metrics ponder the business perspective?		16	Does the selected ISS performance metrics ponder the organization's perspective?
		17	Does the ISS activity receive effective/meaningful feedback from the groups(units) it works with?	17	Does the ISS activity receive effective/meaningful feedback from the groups(units) it works with?		17	Does the ISS activity receive effective and meaningful feedback from the groups(units) it works with?
							18	Does the ISS activity provide effective and meaningful feedback to the groups(units) it works with?
15	Are the results of the information security performance used in providing feedback and demonstrating their impacts on the organization?	18	Are the results of the information security performance used in providing feedback and demonstrating their impacts on the organization?	18	Are the results of the ISS performance used in providing feedback and demonstrating their impacts on the organization?		19	Are the results of the ISS performance used in providing feedback and demonstrating their impacts on the organization?
16	Is the ISS program reviewed to verify their compliance with legislation, regulations, contractual obligations and statutory requirements?	19	Is the ISS program reviewed to verify their compliance with legislation, regulations, contractual obligations and statutory requirements?	19	Is the ISS program reviewed to verify their compliance with legislation, regulations, contractual obligations and statutory requirements?		20	Is the ISS program reviewed to verify its compliance with legislation, regulations, contractual obligations and statutory requirements?
a)	Is the compliance with the organizations information security practices and its alignment to nature of the organizations business, reported to the stakeholders?	a)	Is the compliance with the organizations information security practices and its alignment to nature of the organizations business, reported to the stakeholders?	a)	Is the compliance of the information security practices and their alignment to the organization's business nature, reported to the stakeholders?		a)	Is the compliance of the ISS practices and their alignment to the nature of the organization's purpose, reported to the stakeholders?
		b)	Is there an internal or external regulatory compliance group (auditors), and when did the ISS activity last met with them?	b)	Is there an internal or external regulatory compliance group (auditors), and when did the ISS activity last met with them?	20b & 20c	b)	Is there an internal or external regulatory compliance group (auditors)?

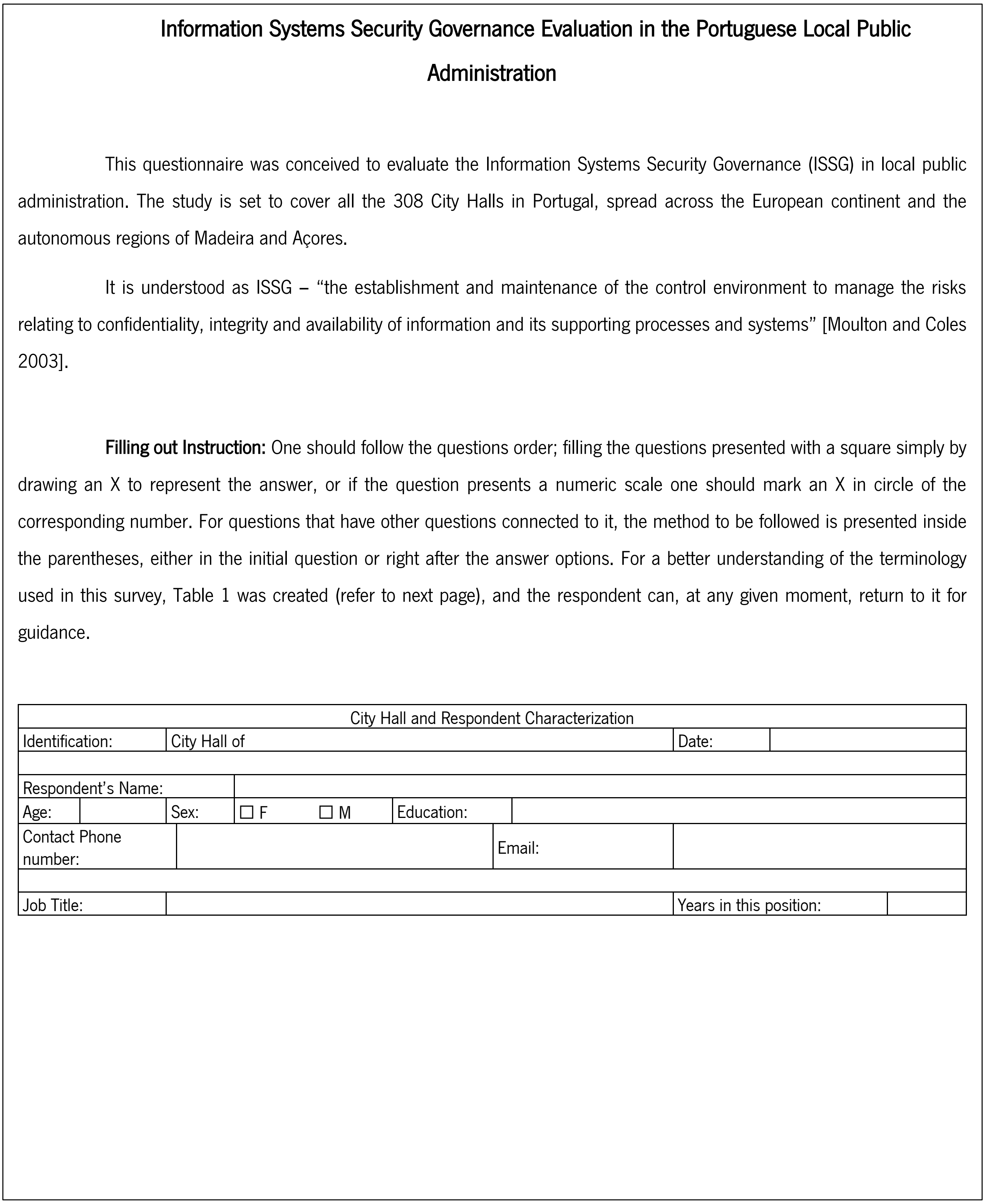
	v2		v3		v4		v5
			(Scale measures: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)		(Scale measures: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	c)	When did the ISS activity last meet with the auditors? (Scale measures: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)
17	Are independent audits commissioned to verify the information security level determined in the organization?	20	Are independent audits commissioned to verify the information security level determined in the organization?	20	Are independent audits commissioned to verify the determined level for the information security?	21	Are independent audits commissioned to verify the determined level for the organization's ISS?
18	Does the ISS strategy considers the changes in different types of environment (business, legal and regulatory) and their potential information risk?	21	Does the ISS strategy considers the changes in different types of environment (business, legal and regulatory) and their potential information risk?	21	Does the ISS strategy considers the changes in different types of environment (business, legal and regulatory) and their potential information risk?	22	Does the ISS strategy considers the changes in different types of environment (organizational, legal and regulatory) and their potential information risk?
		22	How often are regulations reviewed to understand the ISS requirements? (Scale measures: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	22	How often are regulations reviewed to understand the ISS requirements? (Scale measures: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	23	How often are regulations reviewed to understand the ISS requirements? (Scale measures: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)
		a)	Is the legal department involved in the review process?	a)	Is the legal department involved in the review process of the ISS activity?	a)	Is the legal department involved in the review process of the ISS activity?
		b)	When did the ISS activity last review a contractual requirement with the legal counsel? (Scale measures: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	b)	When did the ISS activity last review a contractual requirement with the legal counsel? (Scale measures: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	b)	When did the ISS activity last review a contractual requirement with the legal counsel? (Scale measures: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)
19	Is there a feedback provided by the organization, that regards the transparency of IT costs, benefits and risks?	23	Is there a feedback provided by the organization, that regards the transparency of IT costs, benefits and risks?	23	Is there a feedback provided by the organization, that regards the transparency of IT costs, benefits and risks?	24	Is there a feedback provided by the organization, that regards the transparency over ISS costs, benefits and risks?
		24	How would you evaluate the accomplishment of the ISSG goals for … (Scale measures: 1 – not accomplished; 3 – sufficiently accomplished; 5 – fully accomplished)	24	How would you evaluate the accomplishment of the ISSG goals for … (Scale measures: 1 – not accomplished; 3 – sufficiently accomplished; 5 – fully accomplished)	25	How would you evaluate the accomplishment of the ISSG goals for … (Scale measures: 1 – not accomplished; 3 – sufficiently accomplished; 5 – fully accomplished)
		a)	strategic alignment ?	a)	strategic alignment (the link between the ISS strategy and the organization's business)?	a)	strategic alignment (the link between the ISS strategy and the organization's activity)?
		b)	value delivery ?	b)	value delivery (the delivery of promised benefits while optimizing costs)?	b)	value delivery (the delivery of promised benefits while optimizing costs)?

	v2		v3		v4		v5
		c)	accountability (accept responsibility for the ISSG actions in the organization)?	c)	accountability (accept responsibility for the ISSG actions in the organization)?	c)	accountability (accept responsibility for the ISSG actions in the organization)?
		d)	compliance (fulfill requirements in accordance with some specified standard)?	d)	compliance (fulfill requirements in accordance with some specified standard)?	d)	compliance (fulfill requirements in accordance with regulations, laws and contractual obligations)?
20	To which stand are the needs of the stakeholders balanced in the process of creating an ISSG strategy?	25	To which extent are the needs of the stakeholders balanced in the process of creating an ISSG strategy? (**Scale measures**: 1 – not balanced; 3 – sufficiently balanced; 5 – fully balanced)	25	To which extent are the needs of the stakeholders balanced in the process of creating an ISSG strategy? (**Scale measures**: 1 – not balanced; 3 – sufficiently balanced; 5 – fully balanced)	26	To which extent are the needs of stakeholders balanced in the process of creating an ISS strategy? (**Scale measures**: **1** – not balanced; **3** – sufficiently balanced; **5** – fully balanced)
21	Are the ISSG fundaments integrated within all levels of the organization?	26	Are the ISSG fundaments integrated within all levels of the organization?	26	Are the ISSG fundaments (such as goals and objectives) integrated within all levels of the organization?	27	Are the ISSG goals and objectives integrated within all levels of the organization?
22	To which percentage is the value for the governance of the ISS perceived by the organization?	27	To which degree is the value for the governance of the ISS perceived by the organization ... (**Scale measures**: 1 – no value added [between 0 and 20%]; 2 – between 21 and 40%; 3 – fair amount of value added [between 41 and 60%]; 4 – between 61 and 80%; 5 – a lot of value added [between 81 and 100%])	27	To which degree is the value for the governance of the ISS perceived by the organization ... (**Scale measures**: 1 – no value added [between 0 and 20%]; 2 – between 21 and 40%; 3 – fair amount of value added [between 41 and 60%]; 4 – between 61 and 80%; 5 – a lot of value added [between 81 and 100%])	28	To which degree is the value for the governance of the ISS perceived by the organization in relation to ... (**Scale measures**: **1** – no value added [between 0 and 20%]; **3** – fair amount of value added [between 41 and 60%]; **5** – a lot of value added [between 81 and 100%])
a)	The cost-effectiveness (accomplish what was set out, considering the cost)	a)	the cost-effectiveness (accomplish what was set out, considering the cost)?	a)	the cost-effectiveness (accomplish what was set out, considering the cost)?	a)	effectiveness (accomplishment of what was set out to be done)?
b)	The efficiency (degree of achieving the desired result with little waste)	b)	the efficiency (degree of achieving the desired result with little waste)?	b)	the efficiency (degree of achieving the desired result with little waste)?	b)	efficiency (achieve the desired result with little waste)?
c)	The optimization of resources, assets and capabilities	c)	the optimization of resources, assets and capabilities?	c)	the optimization of resources, assets and capabilities?		
23	Has the ISSG set out rules that makes people/roles accountable for their actions/responsibilities?	28	Has the ISSG set out rules that makes people/roles accountable for their actions/responsibilities?	28	Has the ISSG set out rules that makes people/roles accountable for their actions/responsibilities?	29	Has the ISSG set out rules that makes people accountable for their actions?
24	How much is compliance (the conformity to fulfill official requirements) a part of the ISSG in the organization?	29	How much is compliance (the conformity to fulfill official requirements) a part of the ISSG in the organization? (**Scale measures**: 1 – not important [between 0 and 20% of compliance]; 3 – somewhat important [between 41 and 60% of compliance]; 5 – very important [between 81 and 100% of compliance])	29	How much is compliance (the conformity to fulfill official requirements) a part of the ISSG in the organization? (**Scale measures**: 1 – not important [between 0 and 20% of compliance]; 3 – somewhat important [between 41 and 60% of compliance]; 5 – very important [between 81 and 100% of compliance])	30	How much is compliance a part of the ISSG in the organization? (**Scale measures**: **1** – not important [between 0 and 20% of compliance]; **3** – somewhat important [between 41 and 60% of compliance]; **5** – very important [between 81 and 100% of compliance])
						31	Who is the **person in charge of the organization's ISS**?

	v2			v3		v4			v5
								a)	Is the person in charge driving the ISS activity or mostly reporting compliance?
								b)	What is the career level of the person in charge of the ISS?
								c)	Does the person in charge of the ISS have other roles in the organization?
25	Mark the correspondent artifact, that each role is responsible for developing.		30	Mark the correspondent artifact, that each role is responsible for developing.	30	Mark the correspondent artifact, that each role is responsible for developing.		32	Mark the correspondent artifact, that each role is responsible for developing.
a)	Governing body		a)	Governing body	a)	Governing body (person or group accountable for the organization's performance and conformity)		a)	Governing body (person or group accountable for the organization's performance and conformity)
b)	Executive management	30b	b)	City Hall executive (group usually formed by the city hall mayor and members of the city council)	b)	City Hall executive (group usually formed by the city hall mayor and members of the city council)		b)	City Hall executive (group usually formed by the City Hall Mayor and members of the City Council)
c)	Chief Information Security Officer (CISO)		c)	Chief Information Security Officer (CISO)	c)	Chief Information Security Officer (CISO) (responsible for all the ISS activities)	32c	c)	Person in charge of the organization's ISS
26	Mark the correspondent reporting role, that each main role is responsible for reporting to.		31	Mark the correspondent reporting role, that each main role is responsible for reporting to?	31	Mark the correspondent reporting role, that each main role is responsible for reporting to?		33	Mark the correspondent reporting role, that each main role is responsible for reporting to?
a)	Governing body		a)	Governing body	a)	Governing body		a)	Governing body
b)	Executive management	31b & 31c	b)	Mayor	b)	Mayor (person elected to act as head of a city)		b)	Mayor (person elected to act as head of a city)
			c)	City Councilor	c)	City Councilor (member of the legislative body that governs the city)		c)	City Councilor (member of the legislative body that governs the city)
			d)	Chief Information Officer (CIO)	d)	Chief Information Officer (CIO) (responsible for the ISS program, policy; and its compliance)	33d	d)	Person in charge of the organization's ISS
c)	Auditors		e)	Auditors	e)	Auditors (responsible for assessing the governance activities compliance with the standards)		e)	Auditors (person responsible for assessing the governance activities compliance with the standards)
d)	Data Protection Officer (DPO)		f)	Data Protection Officer (DPO)	f)	Data Protection Officer (DPO) (responsible for overseeing the data protection strategy, implementation and compliance with the GDPR)		f)	Data Protection Officer (DPO) (person responsible for overseeing the data protection strategy, implementation and compliance with the GDPR)
e)	Chief Information Security Officer (CISO)		g)	Chief Information Security Officer (CISO)	g)	Chief Information Security Officer (CISO)	33d	g)	Employees (individual who is payed to work)
f)	Employees		h)	Employees	h)	Employees (individual who is payed to work)			

v2			v3		v4			v5
			32	Is the CISO driving the ISS activity or mostly reporting compliance?	32	Is the CISO driving the ISS activity or mostly reporting compliance?	31a	
27	Does the ISS strategy considers and balances the stakeholders needs?	25 merged						
28	Has the ISS strategy changed in order to prioritize some aspects approved by the ISS performance results?							
29	Have the investments on ISS being evaluated, to very their value?							
30	How committed is the executive management in protecting the information assets?							
31	Does the executive management make decisions based on ISS?							
32	Which role is responsible for developing and approving the ISS strategy and policies in the organization?							
33	Are investments and resources allocated in order to secure support for the ISS activity?							
34	Does the organization carries out a risk management program?							
35	Are the ISS performance metrics developed to accommodate the business perspective?							
36	Are authority levels, escalation guidelines, and reporting and communicating structure covered under the ISS policy or guidelines?							
37	How would you evaluate the accomplishment of the ISSG goals for	24						
a)	Strategic alignment							
b)	Value delivery							
c)	Accountability (accept responsibility for the ISSG actions in the organization)							
d)	Compliance (fulfill requirements in accordance with some specified standard)							

- Instrument v5



Information Systems Security Governance Evaluation in the Portuguese Local Public Administration

This questionnaire was conceived to evaluate the Information Systems Security Governance (ISSG) in local public administration. The study is set to cover all the 308 City Halls in Portugal, spread across the European continent and the autonomous regions of Madeira and Açores.

It is understood as ISSG – "the establishment and maintenance of the control environment to manage the risks relating to confidentiality, integrity and availability of information and its supporting processes and systems" [Moulton and Coles 2003].

Filling out Instruction: One should follow the questions order; filling the questions presented with a square simply by drawing an X to represent the answer, or if the question presents a numeric scale one should mark an X in circle of the corresponding number. For questions that have other questions connected to it, the method to be followed is presented inside the parentheses, either in the initial question or right after the answer options. For a better understanding of the terminology used in this survey, Table 1 was created (refer to next page), and the respondent can, at any given moment, return to it for guidance.

City Hall and Respondent Characterization					
Identification:	City Hall of			Date:	
Respondent's Name:					
Age:		Sex:	☐ F ☐ M	Education:	
Contact Phone number:				Email:	
Job Title:				Years in this position:	

Figure 28 – Instrument Version 5

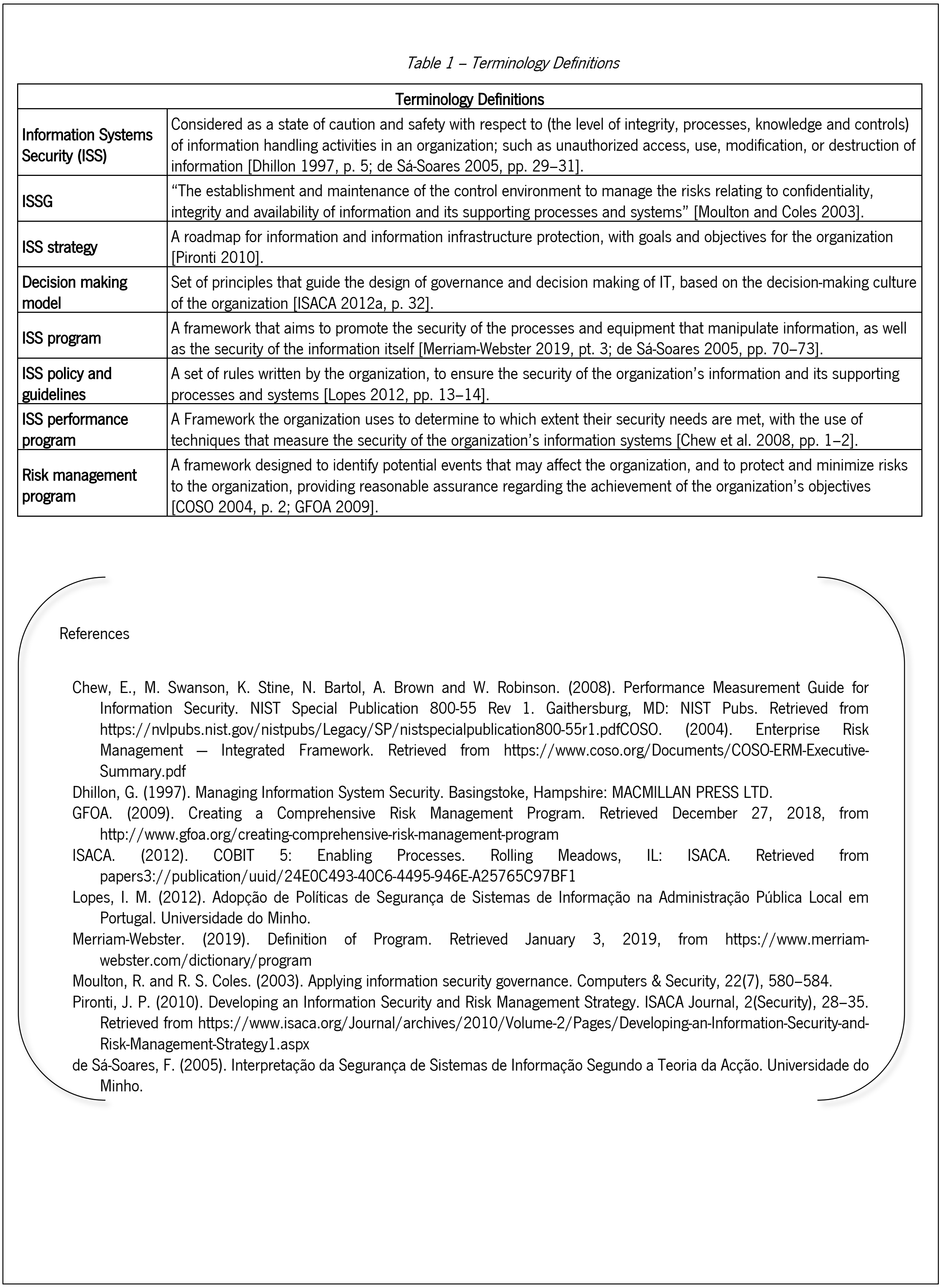


Table 1 – Terminology Definitions

Terminology Definitions	
Information Systems Security (ISS)	Considered as a state of caution and safety with respect to (the level of integrity, processes, knowledge and controls) of information handling activities in an organization; such as unauthorized access, use, modification, or destruction of information [Dhillon 1997, p. 5; de Sá-Soares 2005, pp. 29–31].
ISSG	"The establishment and maintenance of the control environment to manage the risks relating to confidentiality, integrity and availability of information and its supporting processes and systems" [Moulton and Coles 2003].
ISS strategy	A roadmap for information and information infrastructure protection, with goals and objectives for the organization [Pironti 2010].
Decision making model	Set of principles that guide the design of governance and decision making of IT, based on the decision-making culture of the organization [ISACA 2012a, p. 32].
ISS program	A framework that aims to promote the security of the processes and equipment that manipulate information, as well as the security of the information itself [Merriam-Webster 2019, pt. 3; de Sá-Soares 2005, pp. 70–73].
ISS policy and guidelines	A set of rules written by the organization, to ensure the security of the organization's information and its supporting processes and systems [Lopes 2012, pp. 13–14].
ISS performance program	A Framework the organization uses to determine to which extent their security needs are met, with the use of techniques that measure the security of the organization's information systems [Chew et al. 2008, pp. 1–2].
Risk management program	A framework designed to identify potential events that may affect the organization, and to protect and minimize risks to the organization, providing reasonable assurance regarding the achievement of the organization's objectives [COSO 2004, p. 2; GFOA 2009].

References

Chew, E., M. Swanson, K. Stine, N. Bartol, A. Brown and W. Robinson. (2008). Performance Measurement Guide for Information Security. NIST Special Publication 800-55 Rev 1. Gaithersburg, MD: NIST Pubs. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdfCOSO. (2004). Enterprise Risk Management — Integrated Framework. Retrieved from https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

Dhillon, G. (1997). Managing Information System Security. Basingstoke, Hampshire: MACMILLAN PRESS LTD.

GFOA. (2009). Creating a Comprehensive Risk Management Program. Retrieved December 27, 2018, from http://www.gfoa.org/creating-comprehensive-risk-management-program

ISACA. (2012). COBIT 5: Enabling Processes. Rolling Meadows, IL: ISACA. Retrieved from papers3://publication/uuid/24E0C493-40C6-4495-946E-A25765C97BF1

Lopes, I. M. (2012). Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal. Universidade do Minho.

Merriam-Webster. (2019). Definition of Program. Retrieved January 3, 2019, from https://www.merriam-webster.com/dictionary/program

Moulton, R. and R. S. Coles. (2003). Applying information security governance. Computers & Security, 22(7), 580–584.

Pironti, J. P. (2010). Developing an Information Security and Risk Management Strategy. ISACA Journal, 2(Security), 28–35. Retrieved from https://www.isaca.org/Journal/archives/2010/Volume-2/Pages/Developing-an-Information-Security-and-Risk-Management-Strategy1.aspx

de Sá-Soares, F. (2005). Interpretação da Segurança de Sistemas de Informação Segundo a Teoria da Acção. Universidade do Minho.

Artifacts

1	Does the organization has an ISS strategy?		☐ Yes (proceed to 1a) ☐ No (proceed to 2)
	a)	In the ISS strategy is a decision making model present?	☐ Yes ☐ No
2	Does an ISS program exists in the organization?		☐ Yes (proceed to 2a) ☐ No (proceed to 3)
	a)	How would the effectiveness (accomplishment/completion of planned activities) of the ISS program be qualified? (**Scale measures**: **1** – not effective [between 0 and 20% accomplished]; **3** – somewhat effective [between 41 and 60% accomplished]; **5** – very effective [between 81 and 100% accomplished])	○—○—○—○—○ **1 2 3 4 5**
	b)	The investment distribution, resource allocation and responsibility assignment contemplated to which extent in the ISS program? (**Scale measures**: **1** – not contemplated; **3** – sufficiently contemplated; **5** – fully contemplated)	○—○—○—○—○ **1 2 3 4 5**
3	Have an ISS policy and guidelines been created in the organization?		☐ Yes (proceed to 3a) ☐ No (proceed to 4)
	a)	Are the ISS policy and guidelines implemented in the organization?	☐ Yes (proceed to 3b) ☐ No (proceed to 4)
	b)	To whom are the ISS policy and guidelines available?	☐ Organization's employees ☐ Organization's employees and contractors ☐ Everyone with clearance ☐ Everyone
	c)	In regards of the authority levels, the escalation guidelines and the reporting and communicating structure; how would you evaluate their definition, description and clarity? (**Scale measures**: **1** – poorly covered; **3** – sufficiently covered; **5** – very well covered)	○—○—○—○—○ **1 2 3 4 5**
	d)	Is the ISS policy supported by written standards; and are those standards supported by written procedures?	☐ Yes ☐ No
4	Is there a program in place to assess the ISS performance (the use measures to determine to which stand the organization's ISS needs were met)?		☐ Yes (proceed to 4a) ☐ No (proceed to 5)
	a)	Does the ISS performance program contemplate, to which extent, the actions for communicating and reporting events, actions to address resource management deviations and audit reports? (**Scale measures**: **1** – poorly contemplated; **3** – sufficiently contemplated; **5** – very well contemplated)	○—○—○—○—○ **1 2 3 4 5**
	b)	In the reporting and communication's action, is stakeholder's feedback discussed?	☐ Yes ☐ No
	c)	Is the information gathered from the ISS performance considered when selecting new metrics, that are in accordance with the organization's objectives?	☐ Yes ☐ No
5	Is a risk management program present at the organization?		☐ Yes (proceed to 5a) ☐ No (proceed to 6)
	a)	How well the risk subject (such as risk assessment, risk management policies, risk tolerance level, risk appetite and risk mitigation) is discussed in the program? (**Scale measures**: **1** – poorly discussed; **3** – sufficiently discussed; **5** – very well discussed)	○—○—○—○—○ **1 2 3 4 5**

Processes

6	How would you evaluate the alignment of the ISS with the business strategy … (**Scale measures**: **1** – poorly aligned; **3** – sufficiently aligned; **5** – completely aligned)		
	a)	when considering the ISS issues in the organization initiatives?	○—○—○—○—○ 1 2 3 4 5
	b)	to support the organization objectives?	○—○—○—○—○ 1 2 3 4 5
	c)	in handling the results from the ISS performance, like prioritizing or initiating the required actions derived from those results?	○—○—○—○—○ 1 2 3 4 5
7	Are benefits (such as: good results, or advantages) perceived from the investments in ISS?		☐ Yes ☐ No
8	How would you describe the commitment of the executive management in … (**Scale measures**: **1** – not committed; **3** – sufficiently committed; **5** – fully committed)		
	a)	protecting the information assets?	○—○—○—○—○ 1 2 3 4 5
	b)	making ISS related decisions?	○—○—○—○—○ 1 2 3 4 5
	c)	developing and approving the ISS strategy and policy?	○—○—○—○—○ 1 2 3 4 5
	d)	allocating investments and resources?	○—○—○—○—○ 1 2 3 4 5
9	Does the organization follow a risk management policy to manage the risks encountered?		☐ Yes (proceed to 9a) ☐ No (proceed to 10)
	a)	How often are the risks reviewed? (**Scale measures**: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)	○—○—○ 1 2 3
	b)	Is the risk appetite described in the policy?	☐ Yes ☐ No
10	Is there a guideline or plan to be followed to determine the risk appetite for new risks?		☐ Yes ☐ No
11	Are procedures in place to oversee ISS incidents, including public and investor relations?		☐ Yes ☐ No
12	Are there procedures in place, that coordinate with law enforcement, to oversee ISS incidents?		☐ Yes ☐ No
13	How much is covered in the resource management of the ISS program for … (**Scale measures**: **1** – not covered; **3** – sufficiently covered; **5** – fully covered)		
	a)	assignment of responsibilities?	○—○—○—○—○ 1 2 3 4 5
	b)	having competent and motivated personnel?	○—○—○—○—○ 1 2 3 4 5
	c)	promoting a positive information security culture?	○—○—○—○—○ 1 2 3 4 5

14	How much is covered of the stakeholders communication and reporting in the ISS program for … (Scale measures: **1** – poorly covered; **3** – sufficiently covered; **5** – very well covered)		
	a)	reporting and communication of principles and guidelines?	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
	b)	principles for safeguarding the resources?	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
	c)	escalation guidelines?	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
15	How would you quantify the effectiveness of the ISS activities? (Scale measures: **1** – not effective [between 0 and 20% accomplished]; **3** – somewhat effective [between 41 and 60% accomplished]; **5** – very effective [between 81 and 100% accomplished])		○ 1 ○ 2 ○ 3 ○ 4 ○ 5
	a)	How often is the effectiveness of the ISS activity assessed? (Scale measures: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)	○ 1 ○ 2 ○ 3
16	Does the selected ISS performance metrics ponder the organization's perspective?		☐ Yes ☐ No
17	Does the ISS activity receive effective and meaningful feedback from the groups(units) it works with?		☐ Yes ☐ No
18	Does the ISS activity provide effective and meaningful feedback to the groups(units) it works with?		☐ Yes ☐ No
19	Are the results of the ISS performance used in providing feedback and demonstrating their impacts on the organization?		☐ Yes ☐ No
20	Is the ISS program reviewed to verify its compliance with legislation, regulations, contractual obligations and statutory requirements?		☐ Yes (proceed to 19a) ☐ No (proceed to 20)
	a)	Is the compliance of the ISS practices and their alignment to the nature of the organization's purpose, reported to the stakeholders?	☐ Yes ☐ No
	b)	Is there an internal or external regulatory compliance group (auditors)?	☐ Yes ☐ No
	c)	When did the ISS activity last meet with the auditors? (Scale measures: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)	○ 1 ○ 2 ○ 3
21	Are independent audits commissioned to verify the determined level for the organization's ISS?		☐ Yes ☐ No
22	Does the ISS strategy considers the changes in different types of environment (organizational, legal and regulatory) and their potential information risk?		☐ Yes ☐ No
23	How often are regulations reviewed to understand the ISS requirements? (Scale measures: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)		○ 1 ○ 2 ○ 3
	a)	Is the legal department involved in the review process of the ISS activity?	☐ Yes (proceed to 22b) ☐ No (proceed to 23)
	b)	When did the ISS activity last review a contractual requirement with the legal counsel? (Scale measures: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)	○ 1 ○ 2 ○ 3
24	Is there a feedback provided by the organization, that regards the transparency over ISS costs, benefits and risks?		☐ Yes ☐ No

Goals

25		How would you evaluate the accomplishment of the ISSG goals for ... (**Scale measures**: **1** – not accomplished; **3** – sufficiently accomplished; **5** – fully accomplished)	
	a)	strategic alignment (the link between the ISS strategy and the organization's activity)?	○—○—○—○—○ 1 2 3 4 5
	b)	value delivery (the delivery of promised benefits while optimizing costs)?	○—○—○—○—○ 1 2 3 4 5
	c)	accountability (accept responsibility for the ISSG actions in the organization)?	○—○—○—○—○ 1 2 3 4 5
	d)	compliance (fulfill requirements in accordance with regulations, laws and contractual obligations)?	○—○—○—○—○ 1 2 3 4 5
26		To which extent are the needs of stakeholders balanced in the process of creating an ISS strategy? (**Scale measures**: **1** – not balanced; **3** – sufficiently balanced; **5** – fully balanced)	○—○—○—○—○ 1 2 3 4 5
27		Are the ISSG goals and objectives integrated within all levels of the organization?	□ Yes □ No
28		To which degree is the value for the governance of the ISS perceived by the organization in relation to ... (**Scale measures**: **1** – no value added [between 0 and 20%]; **3** – fair amount of value added [between 41 and 60%]; **5** – a lot of value added [between 81 and 100%])	
	a)	effectiveness (accomplishment of what was set out to be done)?	○—○—○—○—○ 1 2 3 4 5
	b)	efficiency (achieve the desired result with little waste)?	○—○—○—○—○ 1 2 3 4 5
29		Has the ISSG set out rules that makes people accountable for their actions?	□ Yes □ No
30		How much is compliance a part of the ISSG in the organization? (**Scale measures**: **1** – not important [between 0 and 20% of compliance]; **3** – somewhat important [between 41 and 60% of compliance]; **5** – very important [between 81 and 100% of compliance])	○—○—○—○—○ 1 2 3 4 5

Agents

31	Who is the **person in charge of the organization’s ISS**?	☐ CIO* ☐ CISO** ☐ Mayor ☐ City Councilor ☐ Other City Hall employee
a)	Is the person in charge driving the ISS activity or mostly reporting compliance?	☐ directing the ISS activity ☐ reporting compliance on the ISS activity
b)	What is the career level of the person in charge of the ISS?	☐ University degree ☐ Technical degree ☐ High School degree ☐ Other
c)	Does the person in charge of the ISS have other roles in the organization?	☐ Yes ☐ No

32	Mark the correspondent artifact, that each role is responsible for developing. (Multiple choices accepted)						
	Role	Artifacts					
a)	Governing body (person or group accountable for the organization’s performance and conformity)	☐ ISS strategy	☐ ISS program	☐ ISS policies and guidelines	☐ ISS performance program	☐ Risk management program	☐ Not assigned
b)	City Hall executive (group usually formed by the City Hall Mayor and members of the City Council)	☐ ISS strategy	☐ ISS program	☐ ISS policies and guidelines	☐ ISS performance program	☐ Risk management program	☐ Not assigned
c)	Person in charge of the organization’s ISS	☐ ISS strategy	☐ ISS program	☐ ISS policies and guidelines	☐ ISS performance program	☐ Risk management program	☐ Not assigned

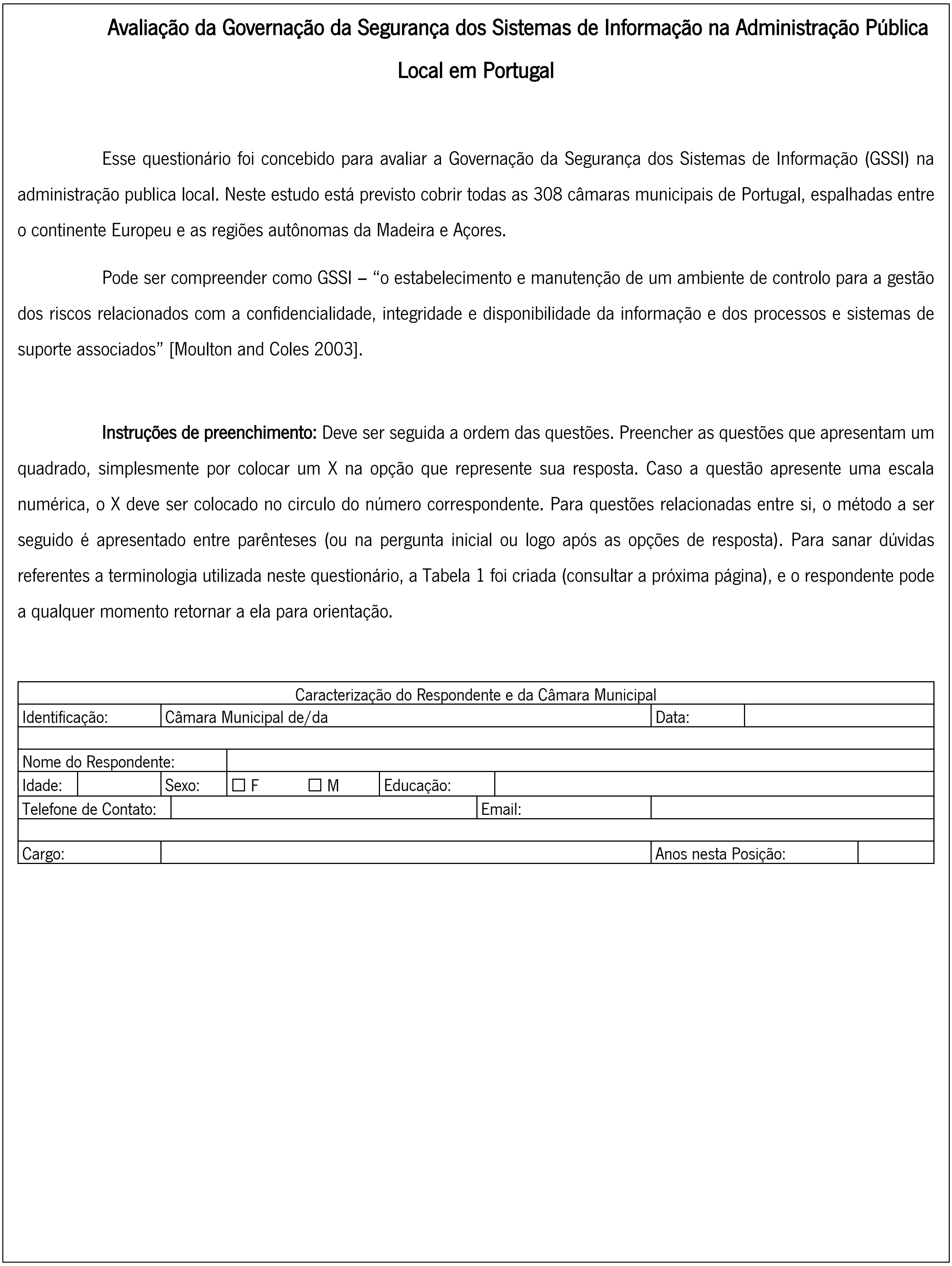
33	Mark the correspondent reporting role, that each main role is responsible for reporting to?				
	Main Role	Reports to			
a)	Governing body	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders
b)	Mayor (person elected to act as head of a city)	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders
c)	City Councilor (member of the legislative body that governs the city)	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders
d)	Person in charge of the organization’s ISS	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders
e)	Auditors (person responsible for assessing the governance activities compliance with the standards)	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders
f)	Data Protection Officer (DPO) (person responsible for overseeing the data protection strategy, implementation and compliance with the GDPR)	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders
g)	Employees (individual who is payed to work)	☐ Governing body	☐ City Hall Executive	☐ In-Line Management	☐ Stakeholders

* Chief Information Officer (CIO) - person responsible for the ISS program, policy; and its compliance.

** Chief Information Security Officer (CISO) - person responsible for all the ISS activities.

Appendix K – Instrument Accessory – Translated Version

The instrument portrayed by Figure 29 of this appendix, is the translated form of the final version of the instrument (V5). Therefore, this version of the instrument was created to better fit the study's context, since the instrument would be applicable to City Halls in the Portuguese territory, and Portuguese is their native language.



Avaliação da Governação da Segurança dos Sistemas de Informação na Administração Pública Local em Portugal

Esse questionário foi concebido para avaliar a Governação da Segurança dos Sistemas de Informação (GSSI) na administração publica local. Neste estudo está previsto cobrir todas as 308 câmaras municipais de Portugal, espalhadas entre o continente Europeu e as regiões autônomas da Madeira e Açores.

Pode ser compreender como GSSI – "o estabelecimento e manutenção de um ambiente de controlo para a gestão dos riscos relacionados com a confidencialidade, integridade e disponibilidade da informação e dos processos e sistemas de suporte associados" [Moulton and Coles 2003].

Instruções de preenchimento: Deve ser seguida a ordem das questões. Preencher as questões que apresentam um quadrado, simplesmente por colocar um X na opção que represente sua resposta. Caso a questão apresente uma escala numérica, o X deve ser colocado no circulo do número correspondente. Para questões relacionadas entre si, o método a ser seguido é apresentado entre parênteses (ou na pergunta inicial ou logo após as opções de resposta). Para sanar dúvidas referentes a terminologia utilizada neste questionário, a Tabela 1 foi criada (consultar a próxima página), e o respondente pode a qualquer momento retornar a ela para orientação.

Caracterização do Respondente e da Câmara Municipal					
Identificação:	Câmara Municipal de/da			Data:	
Nome do Respondente:					
Idade:		Sexo:	☐ F ☐ M	Educação:	
Telefone de Contato:			Email:		
Cargo:				Anos nesta Posição:	

Figure 29 – Instrument V5 – Translated version

Tabela 1 – Definição das Terminologias

Definições das Terminologias	
Segurança dos Sistemas de Informação (SSI)	Considerado como um estado de cautela e segurança em relação (a nível de integridade, processos, conhecimento e controlo) as atividades de manipulação das informações na organização; como o acesso não autorizado, uso, modificação, ou destruição de informações [Dhillon 1997, p. 5; de Sá-Soares 2005, pp. 29–31].
GSSI	"O estabelecimento e manutenção de um ambiente de controlo para o gestão dos riscos relacionados com a confidencialidade, integridade e disponibilidade da informação e dos processos e sistemas de suporte associados" [Moulton and Coles 2003].
Estratégia de SSI	Um guia para informação e para a proteção da infraestrutura da informação, com metas e objetivos para a organização [Pironti 2010].
Modelo de tomada de decisão	Conjunto de princípios que guiam o design da governação e a tomada de decisão da TI, baseado na cultura de tomada de decisões da organização [ISACA 2012ª, p. 32].
Programa de SSI	Uma estrutura que visa promover a segurança dos processos e equipamentos que manipulam a informação, bem como a segurança das próprias informação [Merriam-Webster 2019, pt. 3; de Sá-Soares 2005, pp. 70–73].
Políticas e diretrizes da SSI	Um conjunto de regras escritas pela organização para assegurar a segurança das informações da organização e de seus processos e sistemas de suporte [Lopes 2012, pp. 13–14].
Programa de desempenho da SSI	Uma estrutura usada pela organização para determinar até que ponto suas necessidades de segurança são atendidas, com o uso de técnicas que medem a segurança dos sistemas de informação da organização [Chew et al. 2008, pp. 1–2].
Programa de gestão de riscos	Uma estrutura projetada para identificar potenciais eventos que possam afetar a organização, e para proteger e minimizar os riscos para a organização, fornecendo garantia razoável em relação à realização dos objetivos da organização [COSO 2004, p. 2; GFOA 2009].

Referências

Chew, E., M. Swanson, K. Stine, N. Bartol, A. Brown and W. Robinson. (2008). Performance Measurement Guide for Information Security. NIST Special Publication 800-55 Rev 1. Gaithersburg, MD: NIST Pubs. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdfCOSO. (2004). Enterprise Risk Management — Integrated Framework. Retrieved from https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

Dhillon, G. (1997). Managing Information System Security. Basingstoke, Hampshire: MACMILLAN PRESS LTD.

GFOA. (2009). Creating a Comprehensive Risk Management Program. Retrieved December 27, 2018, from http://www.gfoa.org/creating-comprehensive-risk-management-program

ISACA. (2012). COBIT 5: Enabling Processes. Rolling Meadows, IL: ISACA. Retrieved from papers3://publication/uuid/24E0C493-40C6-4495-946E-A25765C97BF1

Lopes, I. M. (2012). Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal. Universidade do Minho.

Merriam-Webster. (2019). Definition of Program. Retrieved January 3, 2019, from https://www.merriam-webster.com/dictionary/program

Moulton, R. and R. S. Coles. (2003). Applying information security governance. Computers & Security, 22(7), 580–584.

Pironti, J. P. (2010). Developing an Information Security and Risk Management Strategy. ISACA Journal, 2(Security), 28–35. Retrieved from https://www.isaca.org/Journal/archives/2010/Volume-2/Pages/Developing-an-Information-Security-and-Risk-Management-Strategy1.aspx

de Sá-Soares, F. (2005). Interpretação da Segurança de Sistemas de Informação Segundo a Teoria da Acção. Universidade do Minho.

Artefactos

1		A organização possui uma estratégia de SSI?	□ Sim (prossiga para 1a) □ Não (prossiga para 2)
	a)	Na estratégia de SSI, está presente um modelo de tomada da decisão?	□ Sim □ Não
2		Existe um programa de SSI na organização?	□ Sim (prossiga para 2a) □ Não (prossiga para 3)
	a)	Como seria qualificada a eficácia (realização/conclusão das atividades planejadas) do programa de SSI? (**<u>Medidas da escala:</u> 1** - não eficaz [entre 0 e 20% realizadas]; **3** – pouco eficaz [entre 41 e 60% realizadas]; **5** - muito eficaz [entre 81 e 100% realizadas])	○—○—○—○—○ **1 2 3 4 5**
	b)	A distribuição de investimentos, alocação de recursos e atribuição de responsabilidades são contempladas até que ponto no programa SSI? (**<u>Medidas da escala:</u> 1** - não contemplada; **3** - suficientemente contemplada; **5** - totalmente contemplada)	○—○—○—○—○ **1 2 3 4 5**
3		Foi criada na organização uma política e diretrizes da SSI?	□ Sim (prossiga para 3a) □ Não (prossiga para 4)
	a)	A política e diretrizes da SSI estão implementadas na organização?	□ Sim (prossiga para 3b) □ Não (prossiga para 4)
	b)	Para quem está disponível a política e as diretrizes da SSI?	□ Empregados da organização □ Empregados e contratados da organização □ Todos com autorização □ Todos
	c)	Em relação aos níveis de autoridade, diretrizes hierárquicas e da estrutura de relatórios e comunicação; como avaliaria a definição, descrição e clareza? (**<u>Medidas da escala:</u> 1** - pouco coberto; **3** - suficientemente coberto; **5** - muito bem coberto)	○—○—○—○—○ **1 2 3 4 5**
	d)	A política de SSI é suportada por normas escritas; essas normas são suportadas por procedimentos escritos?	□ Sim □ Não
4		Está estabelecido um programa para avaliar o desempenho da SSI (uso de medidas para determinar em que ponto as necessidades da SSI da organização foram atendidas)?	□ Sim (prossiga para 4a) □ Não (prossiga para 5)
	a)	O programa de desempenho da SSI contempla, em que medida, as ações para comunicar e reportar eventos de forma a solucionar desvios de gestão de recursos e de relatórios de auditoria? (**<u>Medidas da escala</u>: 1** - pouco contemplada; **3** - suficientemente contemplada; **5** - muito bem contemplada)	○—○—○—○—○ **1 2 3 4 5**
	b)	Na ação de reportar e comunicar, o *feedback* das partes interessadas é discutido?	□ Sim □ Não
	c)	As informações recolhidas pelo desempenho da SSI são consideradas na hora de selecionar novas métricas estando de acordo com os objetivos da organização?	□ Sim □ Não
5		Existe um programa de gestão de riscos na organização?	□ Sim (prossiga para 5a) □ Não (prossiga para 6)
	a)	Até que ponto o assunto risco (tal como avaliação de risco, políticas de gestão de risco, nível de tolerância de risco, predisposição ao risco e mitigação de risco) é discutido no programa? (**<u>Medidas da escala:</u> 1** - pouco discutido; **3** - suficientemente discutido; **5** - muito bem discutido)	○—○—○—○—○ **1 2 3 4 5**

Processos

6	Como avaliaria o alinhamento da SSI com a estratégia de negócios... (**Medidas da escala:** **1** - pouco alinhada; **3** - suficientemente alinhada; **5** - completamente alinhada)		
	a)	ao considerar as questões de SSI nas iniciativas da organização?	○—○—○—○—○ **1 2 3 4 5**
	b)	no apoio aos objetivos da organização?	○—○—○—○—○ **1 2 3 4 5**
	c)	para lidar com os resultados do desempenho da SSI, como priorizar ou iniciar as ações necessárias derivadas destes resultados?	○—○—○—○—○ **1 2 3 4 5**
7	São percebidos benefícios (como: bons resultados ou vantagens) através dos investimentos em SSI?		□ Sim □ Não
8	Como descreveria o comprometimento da gestão executiva em... (**Medidas da escala:** **1** - não comprometido; **3** - suficientemente comprometido; **5** - totalmente comprometido)		
	a)	proteger os ativos de informação?	○—○—○—○—○ **1 2 3 4 5**
	b)	tomar decisões relacionadas à SSI?	○—○—○—○—○ **1 2 3 4 5**
	c)	desenvolver e aprovar a estratégia e a política de SSI?	○—○—○—○—○ **1 2 3 4 5**
	d)	alocar investimentos e recursos?	○—○—○—○—○ **1 2 3 4 5**
9	A organização segue uma política de gestão de riscos para gerir os riscos encontrados?		□ Sim (prossiga para 9a) □ Não (prossiga para 10)
	a)	Com que frequência os riscos são revistos? (**Medidas da escala:** **1** = menos de 1 ano; **2** = entre 1 e 2 anos; **3** = mais de 2 anos)	○——○——○ **1 2 3**
	b)	A predisposição ao risco está descrita na política?	□ Sim □ Não
10	Existe uma diretriz ou plano a ser seguido para determinar a predisposição de risco para novos riscos?		□ Sim □ Não
11	Existem procedimentos para supervisionar incidentes de SSI, incluindo nas relações com o público e com investidores?		□ Sim □ Não
12	Existem procedimentos para coordenar com os oficiais jurídicos, para supervisionar os incidentes de SSI?		□ Sim □ Não
13	Quanto está assegurado na gestão de recursos pelo programa SSI para... (**Medidas da escala:** **1** - não assegurado; **3** - suficientemente assegurado; **5** - totalmente assegurado)		
	a)	atribuição de responsabilidades?	○—○—○—○—○ **1 2 3 4 5**
	b)	ter pessoal competente e motivado?	○—○—○—○—○ **1 2 3 4 5**
	c)	promover uma cultura positiva de segurança da informação?	○—○—○—○—○ **1 2 3 4 5**

14		Quanto é assegurado da comunicação e reporte aos *stakeholders* programa SSI para... (**<u>Medidas da escala:</u> 1** - pouco assegurado; **3** - suficientemente assegurado; **5** - muito bem assegurado)	
	a)	reportar e comunicar os princípios e diretrizes?	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
	b)	princípios para salvaguardar os recursos?	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
	c)	diretrizes hierárquicas?	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
15		Como quantificaria a eficácia das atividades de SSI? (**<u>Medidas da escala:</u> 1** - não eficaz [entre 0 e 20% realizadas]; **3** – pouco eficaz [entre 41 e 60% realizadas]; **5** - muito eficaz [entre 81 e 100% realizadas])	○ 1 ○ 2 ○ 3 ○ 4 ○ 5
	a)	Com que frequência é avaliada a eficácia da atividade de SSI? (**<u>Medidas da escala:</u> 1** = menos de 1 ano; **2** = entre 1 e 2 anos; **3** = mais de 2 anos)	○ 1 ○ 2 ○ 3
16		As medidas de desempenho da SSI selecionadas ponderam a perspectiva da organização?	□ Sim □ Não
17		A atividade de SSI recebe um *feedback* eficaz e significativo dos grupos (unidades) com os quais trabalha?	□ Sim □ Não
18		A atividade de SSI reporta um *feedback* eficaz e significativo para os grupos (unidades) com os quais trabalha?	□ Sim □ Não
19		Os resultados do desempenho da SSI são usados para dar *feedback* e demonstrar os impactos na organização?	□ Sim □ Não
20		O programa de SSI é revisto para verificar a conformidade com a legislação, os regulamentos, as obrigações contratuais e os requisitos estatutários?	□ Sim (prossiga para 19a) □ Não (prossiga para 20)
	a)	O cumprimento das práticas de SSI e o alinhamento a natureza do propósito da organização são transmitidos aos *stakeholders*?	□ Sim □ Não
	b)	Existe algum grupo interno ou externo (auditores) de conformidade regulatória?	□ Sim □ Não
	c)	Quando foi a última reunião de SSI com os auditores? (**<u>Medidas da escala:</u> 1** = menos de 1 ano; **2** = entre 1 e 2 anos; **3** = mais de 2 anos)	○ 1 ○ 2 ○ 3
21		São contratadas auditorias independentes para verificar o nível determinado para o SSI da organização?	□ Sim □ Não
22		A estratégia de SSI considera as mudanças nos diferentes tipos de ambiente (organizacional, jurídico e regulatório) e seus potenciais riscos à informação?	□ Sim □ Não
23		Com que frequência os regulamentos são revistos para entender os requisitos de SSI? (**<u>Medidas da escala:</u> 1** = menos de 1 ano; **2** = entre 1 e 2 anos; **3** = mais de 2 anos)	○ 1 ○ 2 ○ 3
	a)	O departamento jurídico está envolvido no processo de revisão da atividade de SSI?	□ Sim (prossiga para 22b) □ Não (prossiga para 23)
	b)	Quando é que aconteceu a ultima revisão dos requisitos contratuais com um assessor jurídico? (**<u>Medidas da escala:</u> 1** = menos de 1 ano; **2** = entre 1 e 2 anos; **3** = mais de 2 anos)	○ 1 ○ 2 ○ 3
24		Existe um *feedback*, fornecido pela organização, no que diz respeito à transparência dos custos, benefícios e riscos da SSI?	□ Sim □ Não

Metas

25	Como avaliaria a realização das metas de GSSI para... (**Medidas da escala:** **1** – não realizado; **3** - suficientemente realizado; **5** - completamente realizado)		
	a)	o alinhamento estratégico (elo entre a estratégia da SSI e a actividade da organização)?	○—○—○—○—○ 1 2 3 4 5
	b)	a entrega de valor (entrega dos benefícios prometidos enquanto otimiza os custos)?	○—○—○—○—○ 1 2 3 4 5
	c)	prestação de contas (aceitação da responsabilidade pelas ações da GSSI na organização)?	○—○—○—○—○ 1 2 3 4 5
	d)	conformidade (cumprir os requisitos de acordo com regulamentos, leis e obrigações contratuais)?	○—○—○—○—○ 1 2 3 4 5
26	Até que ponto as necessidades dos *stakeholders* são balanceadas durante o processo de criação da estratégia de SSI? (**Medidas da escala:** **1** – não balanceada; **3** - suficientemente balanceada; **5** - totalmente balanceada)		○—○—○—○—○ 1 2 3 4 5
27	As metas e os objetivos da GSSI estão integrados em todos os níveis da organização?		□ Sim □ Não
28	Qual é o grau de valor percebido pela organização para a governação de SSI em relação a... (**Medidas da escala:** **1** – nenhum valor adicionado [entre 0 e 20%]; **3** – um certo valor adicionado [entre 41 e 60%]; **5** - bastante valor adicionado [entre 81 e 100%])		
	a)	eficácia (realização do que foi planeado)?	○—○—○—○—○ 1 2 3 4 5
	b)	eficiência (alcançar o resultado desejado com pouco desperdício)?	○—○—○—○—○ 1 2 3 4 5
29	A GSSI estabeleceu regras que tornam as pessoas responsáveis pelas suas ações?		□ Sim □ Não
30	Quanto à conformidade, faz parte da GSSI na organização? (**Medidas da escala:** **1** – não importante [entre 0 e 20% de conformidade]; **3** - um pouco importante [entre 41 e 60% de conformidade]; **5** - muito importante [entre 81 e 100% de conformidade])		○—○—○—○—○ 1 2 3 4 5

Agentes

31		Quem é a **pessoa responsável pela SSI da organização?**	□ CIO* □ CISO** □ Presidente da Câmara □ Vereadores □ Outro funcionário da Câmara Municipal
	a)	A pessoa responsável dirige a atividade de SSI ou simplesmente relata sua conformidade?	□ dirige a atividade de SSI □ informa sobre a conformidade da atividade de SSI
	b)	Qual é o nível de académico da pessoa responsável pela SSI?	□ Ensino Universitário □ Ensino Técnico □ Ensino Secundário □ Outro
	c)	A pessoa responsável pela SSI possui outras funções na organização?	□ Sim □ Não

32	Selecione o artefato correspondente, que cada função é responsável por desenvolver. (Possibilidade de selecionar várias opções)							
		Função	Artefatos					
	a)	*Governing body* (pessoa ou grupo responsável pelo desempenho e conformidade da organização)	□ Estratégia de SSI	□ Programa de SSI	□ Políticas e diretrizes da SSI	□ Programa de desempenho da SSI	□ Programa de gestão de riscos	□ Não Atribuída
	b)	Executivo Camarário (grupo normalmente formado pelo Presidente da Câmara e Vereadores)	□ Estratégia de SSI	□ Programa de SSI	□ Políticas e diretrizes da SSI	□ Programa de desempenho da SSI	□ Programa de gestão de riscos	□ Não Atribuída
	c)	Pessoa responsável pela SSI da organização	□ Estratégia de SSI	□ Programa de SSI	□ Políticas e diretrizes da SSI	□ Programa de desempenho da SSI	□ Programa de gestão de riscos	□ Não Atribuída

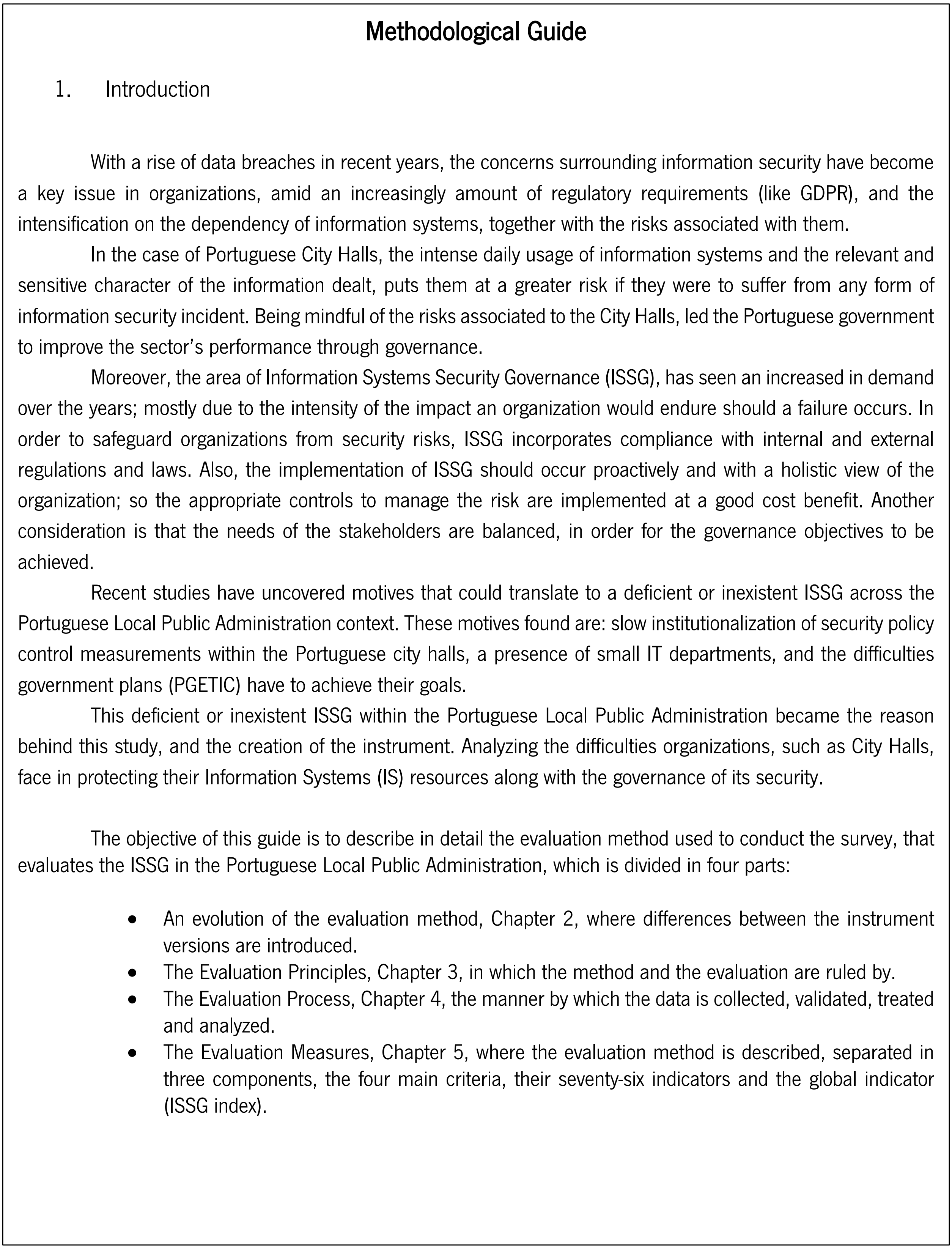
33	Marque para cada função principal, a função correspondente no qual esta deve se reportar?					
		Função principal	Reporta para			
	a)	*Governing body*	□ *Governing body*	□ Executivo Camarário	□ Diretor de departamento municipal	□ Partes Interessadas (*stakeholders*)
	b)	Presidente da Câmara (cidadão eleito para representar um determinado concelho)	□ *Governing body*	□ Executivo Camarário	□ Diretor de departamento municipal	□ Partes Interessadas (*stakeholders*)
	c)	Vereadores (membros do corpo legislativo que governa o concelho)	□ *Governing body*	□ Executivo Camarário	□ Diretor de departamento municipal	□ Partes Interessadas (*stakeholders*)
	d)	Pessoa responsável pela SSI da organização	□ *Governing body*	□ Executivo Camarário	□ Diretor de departamento municipal	□ Partes Interessadas (*stakeholders*)
	e)	Auditores (pessoa responsável por avaliar a conformidade das normas com as atividades de governança)	□ *Governing body*	□ Executivo Camarário	□ Diretor de departamento municipal	□ Partes Interessadas (*stakeholders*)
	f)	Oficial de proteção de dados (DPO) (pessoa responsável pela supervisão da estratégia de proteção de dados, implementação e conformidade com a RGPD)	□ *Governing body*	□ Executivo Camarário	□ Diretor de departamento municipal	□ Partes Interessadas (*stakeholders*)
	g)	Funcionário (indivíduo pago para trabalhar)	□ *Governing body*	□ Executivo Camarário	□ Diretor de departamento municipal	□ Partes Interessadas (*stakeholders*)

* *Chief Information Officer* (CIO) - pessoa responsável pela política e pelo programa de SSI; e sua conformidade.

** *Chief Information Security Officer* (CISO) - responsável por todas as atividades de SSI.

Appendix L – Artifact Construction: Methodological Guide

This appendix displays the secondary artifact created for this study; the methodological guide (cf. Figure 30). This guide is used to help the person, who is administering the instrument, on how to administer and evaluate the instrument. Inside, the process to administer the instrument is detailed, along with the values, wheights and formulas used to evaluate said instrument.



Methodological Guide

1. Introduction

With a rise of data breaches in recent years, the concerns surrounding information security have become a key issue in organizations, amid an increasingly amount of regulatory requirements (like GDPR), and the intensification on the dependency of information systems, together with the risks associated with them.

In the case of Portuguese City Halls, the intense daily usage of information systems and the relevant and sensitive character of the information dealt, puts them at a greater risk if they were to suffer from any form of information security incident. Being mindful of the risks associated to the City Halls, led the Portuguese government to improve the sector's performance through governance.

Moreover, the area of Information Systems Security Governance (ISSG), has seen an increased in demand over the years; mostly due to the intensity of the impact an organization would endure should a failure occurs. In order to safeguard organizations from security risks, ISSG incorporates compliance with internal and external regulations and laws. Also, the implementation of ISSG should occur proactively and with a holistic view of the organization; so the appropriate controls to manage the risk are implemented at a good cost benefit. Another consideration is that the needs of the stakeholders are balanced, in order for the governance objectives to be achieved.

Recent studies have uncovered motives that could translate to a deficient or inexistent ISSG across the Portuguese Local Public Administration context. These motives found are: slow institutionalization of security policy control measurements within the Portuguese city halls, a presence of small IT departments, and the difficulties government plans (PGETIC) have to achieve their goals.

This deficient or inexistent ISSG within the Portuguese Local Public Administration became the reason behind this study, and the creation of the instrument. Analyzing the difficulties organizations, such as City Halls, face in protecting their Information Systems (IS) resources along with the governance of its security.

The objective of this guide is to describe in detail the evaluation method used to conduct the survey, that evaluates the ISSG in the Portuguese Local Public Administration, which is divided in four parts:

- An evolution of the evaluation method, Chapter 2, where differences between the instrument versions are introduced.
- The Evaluation Principles, Chapter 3, in which the method and the evaluation are ruled by.
- The Evaluation Process, Chapter 4, the manner by which the data is collected, validated, treated and analyzed.
- The Evaluation Measures, Chapter 5, where the evaluation method is described, separated in three components, the four main criteria, their seventy-six indicators and the global indicator (ISSG index).

Figure 30 – Artifact – Methodological Guide

2. Evolution of the Evaluation Method

Since this methodological guide pertains to the first available version of the instrument, then it should be used as a basis. However, for further interactions, it is of good measure to review the instrument and analyze it, whether or not changes needs to be implemented. If so, any changes in the instrument and their correspondence in the methodological guide should be written down in this chapter, for documentation and tracking purposes.

3. Evaluation Principles

The evaluation method used in support of the performance for the work that evaluates the ISSG in the Portuguese Local Public Administration, in which this document efforts are to detail, are based in a group of seven principles described as follows:

- Principle 1 – Current evaluation measures

  The evaluation measures shall be subjected to a continuous evaluation process, so that their components (criteria, indicators, sub-indicators), as well as their respective weights, can incorporate and reflect the changes of the different environments (such as technological, organizational, social and political).

- Principle 2 – Interactive development of the evaluation method

  The definition of the evaluation method, especially regarding the evaluation measures, should occur in an interactive and collaborative manner, with the involvement of people from different areas, to promote the method's appropriateness.

- Principle 3 – Independence/Impartiality of the evaluation method

  The definition of the evaluation method, especially regarding the application procedure and the evaluation measures used, must remain independent and free from any other types of influence (such as pressure or interest from other parties), in order to produce a completely unbiased evaluation method.

- Principle 4 – Evaluation method transparency

  The detailed description of the adopted evaluation method, regarding the procedure applied and the evaluation measures used, should be available for public access.

- Principle 5 – Consistency of observations/evaluations performed in a study

  The evaluation method (the applied procedure and the evaluation measures used) chosen (either global or by scenario) should reflect the City Halls study's context, thus obtaining consistent evaluations for the criteria, indicators and sub-indicators, allowing a comparison between the various City Halls to be analyzed.

- Principle 6 – Consistency of observations/evaluations between studies

The evaluation method, adopted in an edition of the study, should be the same or comparable to the method adopted in previous editions of the study, thus allowing for the analysis and evolutionary comparison of the results.

- Principle 7 – Results relevance

The results of applying the evaluation measures, to the entities covered in the studies, should be politically and professionally relevant.

4. Evaluation Process

The process for evaluating the ISSG in the Portuguese Local Public Administration transpires in five phases, as is illustrated in Figure 1.

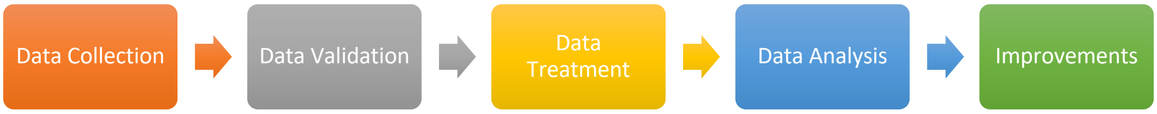


Figure 1 – Evaluation Process

As seen in Figure 1, the first step of the process pertains to data collection, in which is drawn from the answers of the instrument, in this case a questionnaire. Once this process is completed, then comes the steps of data validation and treatment, in order to mold the data so it can be used to compute the index that evaluates the ISSG in Portuguese Local Administration.

The next step is data analysis, where the index is computed for each of the 308 Portuguese City Halls, from this computation a rank can be created as well as other analysis that pertains to the context that is being evaluated. Finally, from those analysis, improvements to the ISSG in Portuguese City Halls may be sought after.

- Data Collection

The process of collecting the data is based on the answers from the instrument that was administered, either via email or interview, to the 308 Portuguese City Halls.

- Data Validation and Treatment

The data gather is then validated and examined for discrepancies (such as no answer or incorrect answer). Afterwards the data is treated, in which the responses are converted into a numerical scoring system, ranging from 0 to 1. The translation rules, for each indicator, is presented in section 5.2, where a detailed description of each indicator is provided.

Subsequently, for each of these values a weight is added; those values are outlined on Table 5, in order to produce the final score of the index, that evaluates the ISSG in the Portuguese Local Public Administration.

- Data Analysis and Improvements

Once the data has been properly treated and calculated, it is then analyzed according to different perspectives. Besides the production and analysis of a global ranking that evaluates the ISSG in the Portuguese City Halls, other analyzes can be carried out. Other kinds of analysis could be an evaluation of the City Hall for each of the four evaluation criteria, or an analysis that is segmented by City Hall size or by region. From those analysis, improvements within the study context can be foreseeing and developed.

5. Evaluation Measures

The instrument is divided into five parts, aside from the first part which represents the face sheet and the terminology definition, the subsequent four parts presents questions surrounding the ISSG in the Portuguese Local Public Administration. These parts are divided in order to represent the four dimensions (Artifacts, Processes, Goals and Agents) found during the document comparison phase of the study. These division is also related in the criteria part of this guide, 5.1.

5.1. Criteria

As mentioned above, the criteria indicators are grouped into four main criteria, and also distinguished by color. The criteria division represent the dimensions of the ISSG, which are Artifacts (Ar), Processes (P), Goals (G) and Agents (Ag). In addition, some criteria are distinguished in gray color, that represents a criteria for an initial question, which does not possess an accompanied answer.

The first criteria (Table 1), Artifacts, has sixteen indicators (Ar.i1 thru Ar.i5a), that encompass information from the tangible ISSG outcomes, such as an ISSG strategy, an ISSG program, policy and guidelines, a performance program and a risk management program.

- Artifacts

Table 1 – Criteria Indicator – Artifacts

Identifier	Label	Description
Ar.i1	ISS strategy presence	Evaluates the existence of an ISS strategy in the organization.
Ar.i1a	Decision making model presence	Evaluates the existence of an decision making model in the ISS strategy of the organization.
Ar.i2	ISS program presence	Evaluates the existence of an ISS program in the organization.
Ar.i2a	ISS program effectiveness	Evaluates the level of effectiveness for the organization's ISS program.
Ar.i2b	ISS program properties	Evaluates to which extent are responsibility assignment, resource allocation and investment distribution contemplated in the organization's ISS program.
Ar.i3	ISS policy and guidelines presence	Evaluates the existence of an ISS policy and guidelines in the organization.
Ar.i3a	ISS policy and guidelines implementation	Evaluates if the ISS policy and guidelines are implemented in the organization.
Ar.i3b	ISS policy and guidelines availability	Evaluates to which group is the ISS policy and guidelines are available in the organization.
Ar.i3c	ISS policy and guidelines properties	Evaluates the amount of coverage for definition, description and clarity used for the authority levels, escalation guidelines, and reporting and communication structure in the organization's ISS policy and guidelines.
Ar.i3d	ISS policy and guidelines basis	Evaluates if the ISS policy and guidelines are supported by written standards and procedures.
Ar.i4	ISS performance program presence	Evaluates the existence of an ISS performance program in the organization.
Ar.i4a	ISS performance program properties	Evaluates the extent in which the actions for communicating and reporting events, addressing resource manage deviations, and audit reports are contemplated in the organization's ISS performance program.
Ar.i4b	Stakeholder's feedback	Evaluates if in the communicating and reporting action, of the organization's ISS performance program, stakeholder's feedback is contemplated.
Ar.i4c	Metrics selection	Evaluates if the results from the ISS performance are considered, and in line with the organization's objectives, when selecting new metrics.
Ar.i5	Risk management program presence	Evaluates the existence of a Risk management program in the organization.
Ar.i5a	Risk management program properties	Evaluates how well are risk assessment, risk management policies, risk tolerance level, risk appetite and risk mitigation are discussed in the Risk management program.

Next, is the Process criteria (Table 2), with a total of thirty six indicators. Within this criterion, the indicators encompass and are divided to represent the EDM processes of ISSG, which are: evaluate, direct and monitor. The indicators used to inform the evaluation process are represented in P.i6 to P.i7; while the indicators used to represent the direct process are from P.i8 to P.i14c; and the monitor process indicators are P.i15 to P.i24.

- Processes

Table 2 – Criteria Indicator – Processes

Identifier	Label	Description
P.i6	Alignment of ISS and Business strategy	Evaluates, in the attached questions, the alignment of ISS to the business strategy subjects such as the alignment of ISS issues, the support of ISS to the business objectives and the response to ISS performance results.
P.i6a	ISS issues alignment	Evaluates how much of the ISS issues are considered when aligned with the organization initiatives.
P.i6b	Organization's objectives support	Evaluates how much ISS support has the organization's objectives.
P.i6c	Response to ISS performance results	Evaluates to which extent the ISS performance results are handled, in order to respond to prioritizing or initiating required actions.
P.i7	Benefits perception	Evaluates if benefits is perceive from the investments in ISS.
P.i8	Executive management commitment	Evaluates, in the attached questions, the executive management commitment to protecting information assets, making ISS related decisions, developing and approving an ISS strategy and policy and allocating investments and resources
P.i8a	Information assets protection	Evaluate how much is the executive management committed in protecting information assets.
P.i8b	ISS related decisions	Evaluate how much is the executive management committed in making ISS related decisions.
P.i8c	ISS strategy and policy development and approval	Evaluate how much is the executive management committed to develop and approve the ISS strategy and policy.
P.i8d	Allocation of investments and resources	Evaluate how much is the executive management committed in allocating investments and resources.
P.i9	Risk management policy	Evaluates if the organization follows a risk management policy when risks are encountered.
P.i9a	Risk review timeline	Evaluates how often are the risks reviewed in the risk management policy.
P.i9b	Risk appetite presence	Evaluates if the risk appetite is described in the risk management policy.
P.i10	Risk appetite for new risks	Evaluates if there is a guide or plan, in the risk appetite, to be followed when new risks are encountered.
P.i11	ISS incident supervision	Evaluate if there are procedures in place to oversee ISS incidents, that may include public and investors relations.
P.i12	ISS incident coordination	Evaluate if there are procedures in place to coordinate the oversight of ISS incidents with law enforcement.
P.i13	Resource management	Evaluates, in the attached questions, the coverage for the assignment of responsibilities, having competent and motivated personnel and the promotion of an information security culture in the resource management activity/component of the ISS program.
P.i13a	Responsibility assignment	Evaluates how much of the responsibility assignment is covered in the resource management activity/component of the ISS program.
P.i13b	Adequate personnel	Evaluates how much is covered regarding the possession of competent and motivated personnel in the resource management activity/component of the ISS program.
P.i13c	Security culture	Evaluates how much is covered regarding the promotion of a positive information security culture in the resource management activity/component of the ISS program.
P.i14	Stakeholders communication and reporting	Evaluates, in the attached questions, the coverage for the principles and guidelines for communicating and reporting, the principles of safeguarding resources and the escalation guidelines in the stakeholders communication and reporting part/component of the ISS program.
P.i14a	Principles and guidelines for communicating and reporting	Evaluates how much of the principles and guidelines for reporting and communicating, is covered in the stakeholders communication and reporting part/component of the ISS program.
P.i14b	Principles to safeguard resources	Evaluates how much is covered regarding the principles for safeguarding the resources, in the stakeholders communication and reporting part/component of the ISS program.
P.i14c	Escalation guidelines	Evaluates how much is covered regarding the escalation guidelines, in the stakeholders communication and reporting part/component of the ISS program.
P.i15	ISS activity effectiveness	Evaluates the perceived amount for the effectiveness of the ISS activity.
P.i15a	ISS activity effectiveness assessment timeline	Evaluates how often is the ISS activity effectiveness assessed.
P.i16	ISS performance metrics alignment	Evaluates if the metrics that are selected for the ISS performance ponder over the organization's perspective.
P.i17	ISS activity feedback return	Evaluates if the ISS activity receives effective or meaningful feedback from other groups or units it works with in the organization.

Identifier	Label	Description
P.i18	Delivery of ISS activity feedback	Evaluates if the ISS activity provides effective or meaningful feedback to other groups or units it works with in the organization.
P.i19	ISS performance results feedback	Evaluates if the results from the ISS performance are used for providing feedback and demonstrating their impacts on the organization.
P.i20	ISS program compliance	Evaluates if the ISS program is reviewed in order to verify their compliance with legislation, regulations, contractual obligations and statutory requirements.
P.i20a	Compliance alignment report	Evaluates if the organization's ISS practices are compliant and aligned with the nature of the organization's purpose, and this is reported to the stakeholders.
P.i20b	Presence of Auditors	Evaluates the existence of an internal or external compliance group (auditors) in the organization.
P.i20c	Auditors meetings timeline	Evaluates how often auditors meet in order to verify the ISS activity.
P.i21	ISS level	Evaluate if independent audits are commissioned to verify if the organization achieved the determined level for the ISS.
P.i22	Environment changes and risks	Evaluates if the ISS strategy considers the changes in the organizational, legal and regulatory environment and their potential risk to the organization.
P.i23	Revision of regulations timeline	Evaluates how often the regulation is review in order to check for changes in the ISS requirements.
P.i23a	Reviewing process	Evaluates if the legal department is involved in the reviewing process of the ISS activity.
P.i23b	Reviewing process timeline	Evaluates how often does the ISS activity reviews contractual requirements with the legal counsel.
P.i24	ISS feedback transparency	Evaluates if the organization provides feedback and transparency of ISS costs, benefits and risks.

The third criteria (Table 3), Goals, encompass topics referred to the main goals of ISSG; such as strategic alignment, value delivery, accountability and compliance. Which is spread across ten indicators (from G.i25 to G.i30).

- Goals

Table 3 – Criteria Indicator – Goals

Identifier	Label	Description
G.i25	ISSG goals	Evaluates, in the attached questions, the accomplishment of ISSG goals, such as strategic alignment, value delivery, accountability and compliance.
G.i25a	Strategic alignment	Evaluates how much of the strategic alignment, of the ISSG goals, has been accomplished.
G.i25b	Value delivery	Evaluates how much of the value delivery, of the ISSG goals, has been accomplished.
G.i25c	Accountability	Evaluates how much of the accountability, of the ISSG goals, has been accomplished.
G.i25d	Compliance	Evaluates how much of the compliance, of the ISSG goals, has been accomplished.
G.i26	Balance stakeholders needs	Evaluates how much of the stakeholders needs are balanced while creating the ISS strategy.
G.i27	ISSG goals and objectives integration	Evaluates if the ISSG goals and objectives are integrated within all levels of the organization.
G.i28	ISSG value perception	Evaluates, in the attached questions, the organization's ISSG perceived value for effectiveness and efficiency.
G.i28a	ISSG effectiveness	Evaluates how much is the value for ISSG effectiveness, perceived by the organization.
G.i28b	ISSG efficiency	Evaluates how much is the value for ISSG efficiency, perceived by the organization.
G.i29	ISSG accountability	Evaluates if there are rules that makes people/roles accountable for their actions/responsibilities.
G.i30	ISSG compliance	Evaluates how much is compliance a part of the organization's ISSG.

The final criterion, Agents (Table 4), encompasses information from the most common roles encountered in ISSG. Their information is also spread across fourteen indicators, which are represented in Ag.i31 thru Ag.i33g.

- Agents

Table 4 – Criteria Indicator – Agents

Identifier	Label	Description
Ag.i31	Person in charge of the organization's ISS	Evaluates who is the person in charge of the organization's ISS.
Ag.i31a	Role responsibility	Evaluates which action is the person in charge of the organization's ISS responsible for.
Ag.i31b	Role career level	Evaluates the career level for the person in charge of the ISS in the organization
Ag.i31c	Role distribution	Evaluate if the person in charge of the organization's ISS have other roles.
Ag.i32	Artifact creation	Evaluates, in the attached questions, which artifacts each of the roles (Governing body, City Hall executive and the Person in charge of the organization's ISS) are responsible for developing.
Ag.i32a	Governing body's artifacts	Evaluates which artifacts each the Governing body is responsible for developing.
Ag.i32b	City Hall executive artifacts	Evaluates which artifacts each the City Hall executive is responsible for developing.
Ag.i32c	Person in charge of the organization's ISS artifacts	Evaluates which artifacts each the Person in charge of the organization's ISS is responsible for developing.
Ag.i33	Reporting structure	Evaluates, in the attached questions, to whom each main role is responsible for reporting.
Ag.i33a	Governing body	Evaluates to whom is the Governing body responsible for reporting.
Ag.i33b	Mayor	Evaluates to whom is the Mayor responsible for reporting.
Ag.i33c	City Councilor	Evaluates to whom is the City Councilor responsible for reporting.
Ag.i33d	Person in charge of the organization's ISS reporting	Evaluates to whom is the Person in charge of the organization's ISS responsible for reporting.
Ag.i33e	Auditors	Evaluates to whom are the Auditors responsible for reporting.
Ag.i33f	Data Protection Officer	Evaluates to whom is the Data Protection Officer responsible for reporting.
Ag.i33g	Employees	Evaluates to whom are the Employees responsible for reporting.

5.2. Indicator

Additionally, a table was created, to present the technical description, for each of the seventy-six indicators. Therefore, each table constitutes an identifier, that is name represents and is formed from the short of the criteria initial (Ar, P, G or Ag), the indicator "i" and a number (which refers to the question number in the questionnaire), followed by the label row, that denotes to the question topic, and the description row (which refers to the goal of the question), that were shown on the criteria tables in 5.1.

Next is the indicator type row, that can be represented either as simple (direct answers) or complex (used in questions with more than one answer). The sub-indicator row represents the indicators possible for the complex indicator type. Next the indicator value, uses a scale from 0 to 1 to qualify the respective response; some responses may require a decision tree. Finally, the indicator weight, which was given in accordance with their relevance within literature and their respective criteria; and is displayed as a percentage.

Identifier	Ar.i1
Label	ISS strategy presence
Description	Evaluates the existence of an ISS strategy in the organization.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	i."Yes" → "1" → if an ISS strategy exists ii."No" → "0" → if an ISS strategy doesn't exist
Indicator weight	7%

Identifier	Ar.i1a
Label	Decision making model presence
Description	Evaluates the existence of an decision making model in the ISS strategy of the organization.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	i."Yes" → "1" → if an decision making model exists ii."No" → "0" → if an decision making model doesn't exist
Indicator weight	5%

Identifier	Ar.i2
Label	ISS program presence
Description	Evaluates the existence of an ISS program in the organization.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if an ISS program exists ii.“No” → “0” → if an ISS program doesn’t exist
Indicator weight	7%

Identifier	Ar.i2a
Label	ISS program effectiveness
Description	Evaluates the level of effectiveness for the organization’s ISS program.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → not effective (between 0 and 20% accomplished) ii.“2” → “0.25” → little effective (between 21 and 40% accomplished) iii.“3” → “0.5” → somewhat effective (between 41 and 60% accomplished) iv.“4” → “0.75” → effective (between 61 and 80% accomplished) v.“5” → “1” → very effective (between 81 and 100% accomplished)
Indicator weight	7%

Identifier	Ar.i2b
Label	ISS program properties
Description	Evaluates to which extent are responsibility assignment, resource allocation and investment distribution contemplated in the organization’s ISS program.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → not contemplated (between 0 and 20% of subject contemplation) ii.“2” → “0.25” → poorly contemplated (between 21 and 40% of subject contemplation) iii.“3” → “0.5” → sufficiently contemplated (between 41 and 60% of subject contemplation) iv.“4” → “0.75” → contemplated (between 61 and 80% of subject contemplation) v.“5” → “1” → fully contemplated (between 81 and 100% of subject contemplation)
Indicator weight	5%

Identifier	Ar.i3
Label	ISS policy and guidelines presence
Description	Evaluates the existence of an ISS policy and guidelines in the organization.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if an ISS policy and guidelines exists ii.“No” → “0” → if an ISS policy and guidelines doesn’t exist
Indicator weight	7%

Identifier	Ar.i3a
Label	ISS policy and guidelines implementation
Description	Evaluates if the ISS policy and guidelines are implemented in the organization.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if the ISS policy and guidelines is implemented ii.“No” → “0” → if the ISS policy and guidelines isn’t implemented
Indicator weight	7%

Identifier	Ar.i3b
Label	ISS policy and guidelines availability
Description	Evaluates to which group is the ISS policy and guidelines are available in the organization.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.Organization’s employees → “0.33” → if the ISS policy is available to the organization’s employees, but isn’t available to others who have clearance for it. ii.Organization’s employees and contractors → “0.67” → if the ISS policy is available to the organization’s employees and contractors, but isn’t available to others who have clearance for it. iii.Everyone with clearance → “1” → if the ISS policy is available to everyone with clearance for it. iv.Everyone → “0” → if the ISS policy is available to everyone, not just to people who have clearance for it.
Indicator weight	7%

Identifier	Ar.i3c
Label	ISS policy and guidelines properties
Description	Evaluates the amount of coverage for definition, description and clarity used for the authority levels, escalation guidelines, and reporting and communication structure in the organization’s ISS policy and guidelines.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → poorly covered (between 0 and 20% of subject covered) ii.“2” → “0.25” → slightly covered (between 21 and 40% of subject covered) iii.“3” → “0.5” → sufficiently covered (between 41 and 60% of subject covered) iv.“4” → “0.75” → well covered (between 61 and 80% of subject covered) v.“5” → “1” → very well covered (between 81 and 100% of subject covered)
Indicator weight	5%

Identifier	Ar.i3d
Label	ISS policy and guidelines basis
Description	Evaluates if the ISS policy and guidelines are supported by written standards and procedures.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if the ISS policy and guidelines is supported ii.“No” → “0” → if the ISS policy and guidelines isn’t supported
Indicator weight	7%

Identifier	Ar.i4
Label	ISS performance program presence
Description	Evaluates the existence of an ISS performance program in the organization.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if an ISS performance program exists ii.“No” → “0” → if an ISS performance program doesn’t exist
Indicator weight	7%

Identifier	Ar.i4a
Label	ISS performance program properties
Description	Evaluates the extent in which the actions for communicating and reporting events, addressing resource manage deviations, and audit reports are contemplated in the organization’s ISS performance program.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → poorly contemplated (between 0 and 20% of subject contemplation) ii.“2” → “0.25” → slightly contemplated (between 21 and 40% of subject contemplation) iii.“3” → “0.5” → sufficiently contemplated (between 41 and 60% of subject contemplation) iv.“4” → “0.75” → well contemplated (between 61 and 80% of subject contemplation) v.“5” → “1” → very well contemplated (between 81 and 100% of subject contemplation)
Indicator weight	5%

Identifier	Ar.i4b
Label	Stakeholder’s feedback
Description	Evaluates if in the communicating and reporting action, of the organization’s ISS performance program, stakeholder’s feedback is contemplated.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if stakeholder’s feedback is contemplated ii.“No” → “0” → if stakeholder’s feedback isn’t contemplated
Indicator weight	5%

Identifier	Ar.i4c
Label	Metrics selection
Description	Evaluates if the results from the ISS performance are considered, and in line with the organization’s objectives, when selecting new metrics.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if the ISS performance results are considered ii.“No” → “0” → if the ISS performance results aren’t considered
Indicator weight	7%

Identifier	Ar.i5
Label	Risk management program presence
Description	Evaluates the existence of a Risk management program in the organization.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if a Risk management program exists ii.“No” → “0” → if a Risk management program doesn’t exist
Indicator weight	7%

Identifier	Ar.i5a
Label	Risk management program properties
Description	Evaluates how well are risk assessment, risk policies, risk tolerance level, risk appetite and risk mitigation are discussed in the Risk management program.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → poorly discussed (between 0 and 20% of subject is discussed) ii.“2” → “0.25” → slightly discussed (between 21 and 40% of subject is discussed) iii.“3” → “0.5” → sufficiently discussed (between 41 and 60% of subject is discussed) iv.“4” → “0.75” → well discussed (between 61 and 80% of subject is discussed) v.“5” → “1” → very well discussed (between 81 and 100% of subject is discussed)
Indicator weight	5%

Identifier	P.i6a
Label	ISS issues alignment
Description	Evaluates how much of the ISS issues are considered when aligned with the business initiatives.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → poorly aligned (between 0 and 20% of subject alignment) ii.“2” → “0.25” → slightly aligned (between 21 and 40% of subject alignment) iii.“3” → “0.5” → sufficiently aligned (between 41 and 60% of subject alignment) iv.“4” → “0.75” → aligned (between 61 and 80% of subject alignment) v.“5” → “1” → completely aligned (between 81 and 100% of subject alignment)
Indicator weight	3%

Identifier	P.i6b
Label	Organization’s objectives support
Description	Evaluates how much ISS support has the organization’s objectives.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → poorly aligned (between 0 and 20% of subject alignment) ii.“2” → “0.25” → slightly aligned (between 21 and 40% of subject alignment) iii.“3” → “0.5” → sufficiently aligned (between 41 and 60% of subject alignment) iv.“4” → “0.75” → aligned (between 61 and 80% of subject alignment) v.“5” → “1” → completely aligned (between 81 and 100% of subject alignment)
Indicator weight	3%

Identifier	P.i6c
Label	Response to ISS performance results
Description	Evaluates to which extent the ISS performance results are handled, in order to respond to prioritizing or initiating required actions.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → poorly aligned (between 0 and 20% of subject alignment) ii.“2” → “0.25” → slightly aligned (between 21 and 40% of subject alignment) iii.“3” → “0.5” → sufficiently aligned (between 41 and 60% of subject alignment) iv.“4” → “0.75” → aligned (between 61 and 80% of subject alignment) v.“5” → “1” → completely aligned (between 81 and 100% of subject alignment)
Indicator weight	3%

Identifier	P.i7
Label	Benefits perception
Description	Evaluates if benefits is perceive from the investments in ISS.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if benefits are perceived ii.“No” → “0” → if benefits aren’t perceived
Indicator weight	3%

Identifier	P.i8a
Label	Information assets protection
Description	Evaluate how much is the executive management committed in protecting information assets.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → not committed (between 0 and 20% of subject commitment) ii.“2” → “0.25” → poorly committed (between 21 and 40% of subject commitment) iii.“3” → “0.5” → sufficiently committed (between 41 and 60% of subject commitment) iv.“4” → “0.75” → committed (between 61 and 80% of subject commitment) v.“5” → “1” → fully committed (between 81 and 100% of subject commitment)
Indicator weight	3%

Identifier	P.i8b
Label	ISS related decisions
Description	Evaluate how much is the executive management committed in making ISS related decisions.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → not committed (between 0 and 20% of subject commitment) ii.“2” → “0.25” → poorly committed (between 21 and 40% of subject commitment) iii.“3” → “0.5” → sufficiently committed (between 41 and 60% of subject commitment) iv.“4” → “0.75” → committed (between 61 and 80% of subject commitment) v.“5” → “1” → fully committed (between 81 and 100% of subject commitment)
Indicator weight	3%

Identifier	P.i8c
Label	ISS strategy and policy development and approval
Description	Evaluate how much is the executive management committed to develop and approve the ISS strategy and policy.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → not committed (between 0 and 20% of subject commitment) ii.“2” → “0.25” → poorly committed (between 21 and 40% of subject commitment) iii.“3” → “0.5” → sufficiently committed (between 41 and 60% of subject commitment) iv.“4” → “0.75” → committed (between 61 and 80% of subject commitment) v.“5” → “1” → fully committed (between 81 and 100% of subject commitment)
Indicator weight	3%

Identifier	P.i8d
Label	Allocation of investments and resources
Description	Evaluate how much is the executive management committed in allocating investments and resources.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → not committed (between 0 and 20% of subject commitment) ii.“2” → “0.25” → poorly committed (between 21 and 40% of subject commitment) iii.“3” → “0.5” → sufficiently committed (between 41 and 60% of subject commitment) iv.“4” → “0.75” → committed (between 61 and 80% of subject commitment) v.“5” → “1” → fully committed (between 81 and 100% of subject commitment)
Indicator weight	3%

Identifier	P.i9
Label	Risk management policy
Description	Evaluates if the organization follows a risk management policy when risks are encountered.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if the risk management policy is followed ii.“No” → “0” → if the risk management policy isn’t followed
Indicator weight	3%

Identifier	P.i9a
Label	Risk review timeline
Description	Evaluates how often are the risks reviewed in the risk management policy.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “1” → if risks are reviewed within a period of less than 1 year ii.“2” → “0.5” → if risks are reviewed within a period between 1 and 2 years iii.“3” → “0” → if risks are reviewed within a period longer than 2 years
Indicator weight	3%

Identifier	P.i9b
Label	Risk appetite presence
Description	Evaluates if the risk appetite is described in the risk management policy.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if risk appetite is described ii.“No” → “0” → if risk appetite isn’t described
Indicator weight	2.2%

Identifier	P.i10
Label	Risk appetite for new risks
Description	Evaluates if there is a guide or plan, in the risk appetite, to be followed when new risks are encountered.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if a guide or plan exists ii.“No” → “0” → if a guide or plan doesn’t exist
Indicator weight	3%

Identifier	P.i11
Label	ISS incident supervision
Description	Evaluate if there are procedures in place to oversee ISS incidents, that may include public and investors relations.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if procedures exists ii.“No” → “0” → if procedures doesn’t exist
Indicator weight	2.2%

Identifier	P.i12
Label	ISS incident coordination
Description	Evaluate if there are procedures in place to coordinate the oversight of ISS incidents with law enforcement.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if procedures exists ii.“No” → “0” → if procedures doesn’t exist
Indicator weight	2.2%

Identifier	P.i13a
Label	Responsibility assignment
Description	Evaluates how much of the responsibility assignment is covered in the resource management activity of the ISS program.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → not covered (between 0 and 20% of subject covered) ii.“2” → “0.25” → poorly covered (between 21 and 40% of subject covered) iii.“3” → “0.5” → sufficiently covered (between 41 and 60% of subject covered) iv.“4” → “0.75” → well covered (between 61 and 80% of subject covered) v.“5” → “1” → fully covered (between 81 and 100% of subject covered)
Indicator weight	3%

Identifier	P.i13b
Label	Adequate personnel
Description	Evaluates how much is covered regarding the possession of competent and motivated personnel in the resource management activity of the ISS program.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → not covered (between 0 and 20% of subject covered) ii.“2” → “0.25” → poorly covered (between 21 and 40% of subject covered) iii.“3” → “0.5” → sufficiently covered (between 41 and 60% of subject covered) iv.“4” → “0.75” → well covered (between 61 and 80% of subject covered) v.“5” → “1” → fully covered (between 81 and 100% of subject covered)
Indicator weight	2.2%

Identifier	P.i13c
Label	Security culture
Description	Evaluates how much is covered regarding the promotion of a positive information security culture in the resource management activity of the ISS program.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → not covered (between 0 and 20% of subject covered) ii.“2” → “0.25” → poorly covered (between 21 and 40% of subject covered) iii.“3” → “0.5” → sufficiently covered (between 41 and 60% of subject covered) iv.“4” → “0.75” → well covered (between 61 and 80% of subject covered) v.“5” → “1” → fully covered (between 81 and 100% of subject covered)
Indicator weight	3%

Identifier	P.i14a
Label	Principles and guidelines for communicating and reporting
Description	Evaluates how much of the principles and guidelines for reporting and communicating, is covered in the stakeholders communication and reporting part of the ISS program.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → poorly covered (between 0 and 20% of subject covered) ii.“2” → “0.25” → slightly covered (between 21 and 40% of subject covered) iii.“3” → “0.5” → sufficiently covered (between 41 and 60% of subject covered) iv.“4” → “0.75” → well covered (between 61 and 80% of subject covered) v.“5” → “1” → very well covered (between 81 and 100% of subject covered)
Indicator weight	3%

Identifier	P.i14b
Label	Principles to safeguard resources
Description	Evaluates how much is covered regarding the principles for safeguarding the resources, in the stakeholders communication and reporting part of the ISS program.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → poorly covered (between 0 and 20% of subject covered) ii.“2” → “0.25” → slightly covered (between 21 and 40% of subject covered) iii.“3” → “0.5” → sufficiently covered (between 41 and 60% of subject covered) iv.“4” → “0.75” → well covered (between 61 and 80% of subject covered) v.“5” → “1” → very well covered (between 81 and 100% of subject covered)
Indicator weight	2.2%

Identifier	P.i14c
Label	Escalation guidelines
Description	Evaluates how much is covered regarding the escalation guidelines, in the stakeholders communication and reporting part of the ISS program.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → poorly covered (between 0 and 20% of subject covered) ii.“2” → “0.25” → slightly covered (between 21 and 40% of subject covered) iii.“3” → “0.5” → sufficiently covered (between 41 and 60% of subject covered) iv.“4” → “0.75” → well covered (between 61 and 80% of subject covered) v.“5” → “1” → very well covered (between 81 and 100% of subject covered)
Indicator weight	3%

Identifier	P.i15
Label	ISS activity effectiveness
Description	Evaluates the perceived amount for the effectiveness of the ISS activity.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → not effective (between 0 and 20% accomplished) ii.“2” → “0.25” → little effective (between 21 and 40% accomplished) iii.“3” → “0.5” → somewhat effective (between 41 and 60% accomplished) iv.“4” → “0.75” → effective (between 61 and 80% accomplished) v.“5” → “1” → very effective (between 81 and 100% accomplished)
Indicator weight	3%

Identifier	P.i15a
Label	ISS activity effectiveness assessment timeline
Description	Evaluates how often is the ISS activity effectiveness assessed.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “1” → if the ISS activity effectiveness is accessed within a period of less than 1 year ii.“2” → “0.5” → if the ISS activity effectiveness is accessed within a period between 1 and 2 years iii.“3” → “0” → if the ISS activity effectiveness is accessed within a period longer than 2 years
Indicator weight	3%

Identifier	P.i16
Label	ISS performance metrics alignment
Description	Evaluates if the metrics that are selected for the ISS performance ponder over the organization’s perspective.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if the metrics are pondered ii.“No” → “0” → if the metrics aren’t pondered
Indicator weight	3%

Identifier	P.i17
Label	ISS activity feedback return
Description	Evaluates if the ISS activity receives effective or meaningful feedback from other groups or units it works with in the organization.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if feedback is received ii.“No” → “0” → if feedback isn’t received
Indicator weight	2.2%

Identifier	P.i18
Label	Delivery of ISS activity feedback
Description	Evaluates if the ISS activity provides effective or meaningful feedback to other groups or units it works with in the organization.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if feedback is provided ii.“No” → “0” → if feedback isn’t provided
Indicator weight	2.2%

Identifier	P.i19
Label	ISS performance results feedback
Description	Evaluates if the results from the ISS performance are used for providing feedback and demonstrating their impacts on the organization.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if ISS performance results are used to provide feedback ii.“No” → “0” → if ISS performance results aren’t used to provide feedback
Indicator weight	2.2%

Identifier	P.i20
Label	ISS program compliance
Description	Evaluates if the ISS program is reviewed in order to verify their compliance with legislation, regulations, contractual obligations and statutory requirements.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if the ISS program is reviewed for compliance ii.“No” → “0” → if the ISS program isn’t reviewed for compliance
Indicator weight	3%

Identifier	P.i20a
Label	Compliance alignment report
Description	Evaluates if the organization’s ISS practices are compliant and aligned with the nature of the organization’s purpose, and this is reported to the stakeholders.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if the ISS practices compliance and alignment are reported to stakeholders ii.“No” → “0” → if the ISS practices compliance and alignment aren’t reported to stakeholders
Indicator weight	2.2%

Identifier	P.i20b
Label	Presence of Auditors
Description	Evaluates the existence of an internal or external compliance group (auditors) in the organization.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if exists ii.“No” → “0” → if it doesn’t exist
Indicator weight	3%

Identifier	P.i20c
Label	Auditors meetings timeline
Description	Evaluates how often auditors meet in order to verify the ISS activity.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “1” → if the ISS activity is verified by auditors within a period of less than 1 year ii.“2” → “0.5” → if the ISS activity is verified by auditors within a period between 1 and 2 years iii.“3” → “0” → if the ISS activity is verified by auditors within a period longer than 2 years
Indicator weight	3%

Identifier	P.i21
Label	ISS level
Description	Evaluate if independent audits are commissioned to verify if the organization achieved the determined level for the ISS.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if independent audits are commissioned ii.“No” → “0” → if independent audits aren’t commissioned
Indicator weight	3%

Identifier	P.i22
Label	Environment changes and risks
Description	Evaluates if the ISS strategy considers the changes in the organizational, legal and regulatory environment and their potential risk to the organization.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if the ISS strategy is considered ii.“No” → “0” → if the ISS strategy isn’t considered
Indicator weight	3%

Identifier	P.i23
Label	Revision of regulations timeline
Description	Evaluates how often the regulation is review in order to check for changes in the ISS requirements.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “1” → if the regulation is reviewed within a period of less than 1 year ii.“2” → “0.5” → if the regulation is reviewed within a period between 1 and 2 years iii.“3” → “0” → if the regulation is reviewed within a period longer than 2 years
Indicator weight	3%

Identifier	P.i23a
Label	Reviewing process
Description	Evaluates if the legal department is involved in the reviewing process of the ISS activity.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if the legal department is involved ii.“No” → “0” → if the legal department isn’t involved
Indicator weight	2.2%

Identifier	P.i23b
Label	Reviewing process timeline
Description	Evaluates how often does the ISS activity reviews contractual requirements with the legal counsel.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “1” → if contractual requirements are reviewed within a period of less than 1 year ii.“2” → “0.5” → if contractual requirements are reviewed within a period between 1 and 2 years iii.“3” → “0” → if contractual requirements are reviewed within a period longer than 2 years
Indicator weight	3%

Identifier	P.i24
Label	ISS feedback transparency
Description	Evaluates if the organization provides feedback and transparency of ISS costs, benefits and risks.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	i."Yes" → "1" → if feedback and transparency is provided for ISS costs, benefits and risks ii."No" → "0" → if feedback and transparency isn't provided for ISS costs, benefits and risks
Indicator weight	3%

Identifier	G.i25a
Label	Strategic alignment
Description	Evaluates how much of the strategic alignment, of the ISSG goals, has been accomplished.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	i."1" → "0" → not accomplished (between 0 and 20% of the strategic alignment accomplished) ii."2" → "0.25" → poorly accomplished (between 21 and 40% of the strategic alignment accomplished) iii."3" → "0.5" → sufficiently accomplished (between 41 and 60% of the strategic alignment accomplished) iv."4" → "0.75" → accomplished (between 61 and 80% of the strategic alignment accomplished) v."5" → "1" → fully accomplished (between 81 and 100% of the strategic alignment accomplished)
Indicator weight	11%

Identifier	G.i25b
Label	Value delivery
Description	Evaluates how much of the value delivery, of the ISSG goals, has been accomplished.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	i."1" → "0" → not accomplished (between 0 and 20% of value delivery accomplished) ii."2" → "0.25" → poorly accomplished (between 21 and 40% of value delivery accomplished) iii."3" → "0.5" → sufficiently accomplished (between 41 and 60% of value delivery accomplished) iv."4" → "0.75" → accomplished (between 61 and 80% of value delivery accomplished) v."5" → "1" → fully accomplished (between 81 and 100% of value delivery accomplished)
Indicator weight	11%

Identifier	G.i25c
Label	Accountability
Description	Evaluates how much of the accountability, of the ISSG goals, has been accomplished.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	i."1" → "0" → not accomplished (between 0 and 20% of accountability accomplished) ii."2" → "0.25" → poorly accomplished (between 21 and 40% of accountability accomplished) iii."3" → "0.5" → sufficiently accomplished (between 41 and 60% of accountability accomplished) iv."4" → "0.75" → accomplished (between 61 and 80% of accountability accomplished) v."5" → "1" → fully accomplished (between 81 and 100% of accountability accomplished)
Indicator weight	11%

Identifier	G.i25d
Label	Compliance
Description	Evaluates how much of the compliance, of the ISSG goals, has been accomplished.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	i."1" → "0" → not accomplished (between 0 and 20% of compliance accomplished) ii."2" → "0.25" → poorly accomplished (between 21 and 40% of compliance accomplished) iii."3" → "0.5" → sufficiently accomplished (between 41 and 60% of compliance accomplished) iv."4" → "0.75" → accomplished (between 61 and 80% of compliance accomplished) v."5" → "1" → fully accomplished (between 81 and 100% of compliance accomplished)
Indicator weight	11%

Identifier	G.i26
Label	Balance stakeholders needs
Description	Evaluates how much of the stakeholders needs are balanced while creating the ISS strategy.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	i."1" → "0" → not balanced (between 0 and 20% of stakeholders needs balanced) ii."2" → "0.25" → poorly balanced (between 21 and 40% of stakeholders needs balanced) iii."3" → "0.5" → sufficiently balanced (between 41 and 60% of stakeholders needs balanced) iv."4" → "0.75" → well balanced (between 61 and 80% of stakeholders needs balanced) v."5" → "1" → fully balanced (between 81 and 100% of stakeholders needs balanced)
Indicator weight	1.82%

Identifier	G.i27
Label	ISSG goals and objectives integration
Description	Evaluates if the ISSG goals and objectives are integrated within all levels of the organization.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if ISSG goals and objectives are integrated ii.“No” → “0” → if ISSG goals and objectives aren’t integrated
Indicator weight	8%

Identifier	G.i28a
Label	ISSG effectiveness
Description	Evaluates how much is the value for ISSG effectiveness, perceived by the organization.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → no value added (between 0 and 20% of perceived ISSG effectiveness) ii.“2” → “0.25” → a small amount of value added (between 21 and 40% of perceived ISSG effectiveness) iii.“3” → “0.5” → a fair amount of value added (between 41 and 60% of perceived ISSG effectiveness) iv.“4” → “0.75” → a large amount of value added (between 61 and 80% of perceived ISSG effectiveness) v.“5” → “1” → a lot of value added (between 81 and 100% of perceived ISSG effectiveness)
Indicator weight	11%

Identifier	G.i28b
Label	ISSG efficiency
Description	Evaluates how much is the value for ISSG efficiency, perceived by the organization.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → no value added (between 0 and 20% of perceived ISSG efficiency) ii.“2” → “0.25” → a small amount of value added (between 21 and 40% of perceived ISSG efficiency) iii.“3” → “0.5” → a fair amount of value added (between 41 and 60% of perceived ISSG efficiency) iv.“4” → “0.75” → a large amount of value added (between 61 and 80% of perceived ISSG efficiency) v.“5” → “1” → a lot of value added (between 81 and 100% of perceived ISSG efficiency)
Indicator weight	11%

Identifier	G.i29
Label	ISSG accountability
Description	Evaluates if there are rules that makes people/roles accountable for their actions/responsibilities.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“Yes” → “1” → if rules for accountability exists ii.“No” → “0” → if rules for accountability doesn’t exist
Indicator weight	7%

Identifier	G.i30
Label	ISSG compliance
Description	Evaluates how much is compliance a part of the organization’s ISSG.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“1” → “0” → not important (between 0 and 20% of compliance) ii.“2” → “0.25” → slightly important (between 21 and 40% of compliance) iii.“3” → “0.5” → somewhat important (between 41 and 60% of compliance) iv.“4” → “0.75” → important (between 61 and 80% of compliance) v.“5” → “1” → very important (between 81 and 100% of compliance)
Indicator weight	8%

Identifier	Ag.i31
Label	Person in charge of the organization’s ISS
Description	Evaluates who is the person in charge of the organization’s ISS.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i.“CIO” → “1” → if is the person in charge of the organization’s ISS (literature point of view) ii.“CISO” → “0.75” → if is the person in charge of the organization’s ISS (literature point of view) iii.“Mayor” → “0.5” → if is the person in charge of the organization’s ISS (study context) iv.“City Councilor” → “0.25” → if is the person in charge of the organization’s ISS (study context) v.“Other City Hall employee” → “0” → if is the person in charge of the organization’s ISS (study context)
Indicator weight	8%

Identifier	Ag.i31a
Label	Role responsibility
Description	Evaluates which action is the person in charge of the organization's ISS responsible for.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i. "Directing the ISS activity" → "1" → if the person in charge is responsible for directing the ISS activity ii. "Reporting compliance on the ISS activity" → "0" → if the person in charge is responsible for only reporting compliance of the ISS activity
Indicator weight	6%

Identifier	Ag.i31b
Label	Role career level
Description	Evaluates the career level for the person in charge of the ISS in the organization
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i. "University degree" → "1" → if the person in charge possess an university degree ii. "Technical degree" → "0,5" → if the person in charge doesn't possess an university degree, but has a high level degree iii. "High School degree" → "0" → if the person in charge only possess a lower level degree iv. "Other" → "0" → if the person in charge possesses another form of degree or doesn't possess any degree
Indicator weight	6%

Identifier	Ag.i31c
Label	Role distribution
Description	Evaluate if the person in charge of the organization's ISS have other roles.
Indicator type	Simple indicator
Sub indicators	––
Indicator value	i. "Yes" → "0" → if the person in charge has other roles within the organization ii. "No" → "1" → if the person in charge doesn't have other roles within the organization
Indicator weight	6%

Identifier	Ag.i32a
Label	Governing body's artifacts
Description	Evaluates which artifacts each the Governing body is responsible for developing.
Indicator type	Complex indicator
Sub indicators	i. "ISS strategy" → A roadmap for information and information infrastructure protection, with goals and objectives for the organization [Pironti 2010] ii. "ISS program" → A framework that aims to promote the security of the processes and equipment that manipulate the information, as well as the security of the information itself [Merriam-Webster 2019, pt. 3; de Sá-Soares 2005, pp. 70–73] iii. "ISS policies and guidelines" → A set of rules written by the organization, to ensure the security of the organization's information and its supporting processes and systems [Lopes 2012, pp. 13–14] iv. "ISS performance program" → Is a framework the organization use to determine to which extent their security needs are met, with the use of techniques that measure the security of the organization's information systems [Chew et al. 2008, pp. 1–2] v. "Risk management program" → A framework designed to identify potential events that may affect the organization, and to protect and minimize risks to the organization, providing reasonable assurance regarding the achievement of the organization's objectives [COSO 2004, p. 2; GFOA 2009] vi. "Not Assigned" → When the role in question does not have any of the artifacts (ISS strategy, ISS program, ISS policies and guidelines, ISS performance program, or Risk management program) assigned to it.
Sub indicator value	i. "0.5" ii. "0" iii. "0.5" iv. "0" v. "0" vi. "0"
Indicator value	• "1" → if the Governing body is responsible for both artifacts (ISS strategy and ISS policies and guidelines) • "0.5" → if the Governing body is responsible for only one artifact (ISS strategy or ISS policies and guidelines) • "0" → if the Governing body isn't responsible for any of the artifacts (ISS strategy and ISS policies and guidelines); or have not been assigned to any of the artifacts
Indicator weight	8%

Identifier	Ag.i32b
Label	City Hall executive artifacts
Description	Evaluates which artifacts each the City hall executive is responsible for developing.
Indicator type	Complex indicator
Sub indicators	i.“ISS strategy” ii.“ISS program” iii.“ISS policies and guidelines” iv.“ISS performance program” v.“Risk management program” vi.“Not Assigned”
Sub indicator value	i.“0” ii.“0.5” iii.“0” iv.“0.5” v.“0” vi.“0”
Indicator value	• “1” → if the City Hall executive is responsible for both artifacts (ISS program and ISS performance program) • “0.5” → if the City Hall executive is responsible for only one artifact (ISS program or ISS performance program) • “0” → if the City Hall executive isn’t responsible for any of the artifacts(ISS program and ISS performance program); or have not been assigned to any of the artifacts
Indicator weight	8%

Identifier	Ag.i32c
Label	Person in charge of the organization’s ISS artifacts
Description	Evaluates which artifacts each the Person in charge of the organization’s ISS is responsible for developing.
Indicator type	Complex indicator
Sub indicators	i.“ISS strategy” ii.“ISS program” iii.“ISS policies and guidelines” iv.“ISS performance program” v.“Risk management program” vi.“Not Assigned”
Sub indicator value	• Question 31 answer – **“CIO”/ “Mayor”/ “City Councilor”** i.“0” ii.“0.5” iii.“0” iv.“0.5” v.“0” vi.“0” • Question 31 answer – **“CISO”** i.“0” ii.“0” iii.“0” iv.“0” v.“1” vi.“0” • Question 31 answer – **“Other City Hall employee”** i.“0” ii.“0” iii.“0” iv.“0” v.“0” vi.“0”
Indicator value	• “1” → if the Person in charge (**“CIO”/ “Mayor”/ “City Councilor”**) is responsible for both artifacts (ISS program and ISS performance program); or if the Person in charge (**“CISO”**) is responsible for the artifact Risk management program • “0.5” → if the Person in charge (**“CIO”/ “Mayor”/ “City Councilor”**) is responsible for only one artifact (ISS program or ISS performance program) • “0” → if the Person in charge (**“CIO”/ “Mayor”/ “City Councilor”**) isn’t responsible for any of the artifacts(ISS program and ISS performance program); or if the Person in charge (**“CISO”**) isn’t responsible for any other artifact; or if the Person in charge (**“Other City Hall employee”**) isn’t responsible for any of the artifacts; or if the Person in charge(**“CIO”/ “CISO” / “Mayor”/ “City Councilor” / “Other City Hall employee”**) have not been assigned to any of the artifacts
Indicator weight	8%

Identifier	Ag.i33a
Label	Governing body
Description	Evaluates to whom is the Governing body responsible for reporting.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	i.“Governing body” → “0” → if the Governing body reports to them ii.“City Hall Executive” → “0” → if the Governing body reports to them iii.“In-Line Management” → “0” → if the Governing body reports to them iv.“Stakeholders” → “1” → if the Governing body reports to them
Indicator weight	8%

Identifier	Ag.i33b
Label	Mayor
Description	Evaluates to whom is the Mayor responsible for reporting.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	i.“Governing body” → “1” → if the Mayor reports to them ii.“City Hall Executive” → “0” → if the Mayor reports to them iii.“In-Line Management” → “0” → if the Mayor reports to them iv.“Stakeholders” → “0” → if the Mayor reports to them
Indicator weight	6%

Identifier	Ag.i33c
Label	City Councilor
Description	Evaluates to whom is the City councilor responsible for reporting.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	i.“Governing body” → “0” → if the City councilor reports to them ii.“City Hall Executive” → “1” → if the City councilor reports to them iii.“In-Line Management” → “0” → if the City councilor reports to them iv.“Stakeholders” → “0” → if the City councilor reports to them
Indicator weight	6%

Identifier	Ag.i33d
Label	Person in charge of the organization’s ISS reporting
Description	Evaluates to whom is the Person in charge of the organization’s ISS responsible for reporting.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	• Question 31 answer – **“CIO”/ “Mayor”** i.“Governing body” → “1” → if the Person in charge of the organization’s ISS reports to them ii.“City Hall Executive” → “0” → if the Person in charge of the organization’s ISS reports to them iii.“In-Line Management” → “0” → if the Person in charge of the organization’s ISS reports to them iv.“Stakeholders” → “0” → if the Person in charge of the organization’s ISS reports to them • Question 31 answer – **“CISO”/ “City Councilor”** i.“Governing body” → “0” → if the Person in charge of the organization’s ISS reports to them ii.“City Hall Executive” → “1” → if the Person in charge of the organization’s ISS reports to them iii.“In-Line Management” → “0” → if the Person in charge of the organization’s ISS reports to them iv.“Stakeholders” → “0” → if the Person in charge of the organization’s ISS reports to them • Question 31 answer – **“Other City Hall employee”** i.“Governing body” → “0” → if the Person in charge of the organization’s ISS reports to them ii.“City Hall Executive” → “0” → if the Person in charge of the organization’s ISS reports to them iii.“In-Line Management” → “1” → if the Person in charge of the organization’s ISS reports to them iv.“Stakeholders” → “0” → if the Person in charge of the organization’s ISS reports to them
Indicator weight	8%

Identifier	Ag.i33e
Label	Auditors
Description	Evaluates to whom are the Auditors responsible for reporting.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	i.“Governing body” → “1” → if the Auditors reports to them ii.“City Hall Executive” → “0” → if the Auditors reports to them iii.“In-Line Management” → “0” → if the Auditors reports to them iv.“Stakeholders” → “0” → if the Auditors reports to them
Indicator weight	8%

Identifier	Ag.i33f
Label	Data Protection Officer
Description	Evaluates to whom is the Data Protection Officer responsible for reporting.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	i.“Governing body” → “1” → if the Data Protection Officer reports to them ii.“City Hall Executive” → “0” → if the Data Protection Officer reports to them iii.“In-Line Management” → “0” → if the Data Protection Officer reports to them iv.“Stakeholders” → “0” → if the Data Protection Officer reports to them
Indicator weight	8%

Identifier	Ag.i33g
Label	Employees
Description	Evaluates to whom are the Employees responsible for reporting.
Indicator type	Simple indicator
Sub indicators	--
Indicator value	i.“Governing body” → “0” → if the Employees reports to them ii.“City Hall Executive” → “0” → if the Employees reports to them iii.“In-Line Management” → “1” → if the Employees reports to them iv.“Stakeholders” → “0” → if the Employees reports to them
Indicator weight	6%

5.3. Global Indicator for ISSG in Portuguese Local Public Administration

Once the criteria and the indicators were presented, begins the calculation of the indicator value, derived from the answers given on the instrument. This step is needed in order to complete the criteria assessment, which will be used to evaluate the ISSG in Portuguese Local Administration.

There are two paths to calculate the global index (a.k.a. ISSG index), and they are referenced as global or as scenarios (a more in-depth description is given shortly). In the case of the scenarios path, there are also two scenarios to choose from, scenario 1 (Sc1) and scenario 2 (Sc2).

Also in the ISSG index calculation, weights are assigned to each Criteria and Indicator. The criteria weights differ in value, depending on the path used. If the path used is the global path or the scenario 1 of the scenario, their criteria weights are the same, while if scenario 2 is used the criteria weights are different.

In order to help with the calculation of the global indicator, Table 5 was created. In it, all the criteria (Artifacts (AR), Processes (P), Goals (G), and Agents (Ag)) and indicators are displayed in a compact form, alongside their pondered weights

Table 5 – Weights for the Criteria and Indicators

Criteria	Criteria weight		Indicator		Indicator weight
	Sc1	Sc2			
Ar	25%	20%	Ar.i1	ISS strategy presence	7%
			Ar.i1a	Decision making model presence	5%
			Ar.i2	ISS program presence	7%
			Ar.i2a	ISS program effectiveness	7%
Artifacts			Ar.i2b	ISS program properties	5%
			Ar.i3	ISS policy and guidelines presence	7%
			Ar.i3a	ISS policy and guidelines implementation	7%
			Ar.i3b	ISS policy and guidelines availability	7%
			Ar.i3c	ISS policy and guidelines properties	5%
			Ar.i3d	ISS policy and guidelines basis	7%
			Ar.i4	ISS performance program presence	7%
			Ar.i4a	ISS performance program properties	5%
			Ar.i4b	Stakeholder’s feedback	5%
			Ar.i4c	Metrics selection	7%
			Ar.i5	Risk management program presence	7%
			Ar.i5a	Risk management program properties	5%
				Total weight for Ar indicators	100%

Criteria	Criteria weight		Indicator		Indicator weight
	Sc1	Sc2			
P	25%	20%	P.i6	Alignment of ISS and Business strategy	
			P.i6a	ISS issues alignment	3%
			P.i6b	Organization’s objectives support	3%
			P.i6c	Response to ISS performance results	3%
Processes			P.i7	Benefits perception	3%
			P.i8	Executive management commitment	
			P.i8a	Information assets protection	3%
			P.i8b	ISS related decisions	3%
			P.i8c	ISS strategy and policy development and approval	3%
			P.i8d	Allocation of investments and resources	3%
			P.i9	Risk management policy	3%
			P.i9a	Risk review timeline	3%
			P.i9b	Risk appetite presence	2.2%
			P.i10	Risk appetite for new risks	3%
			P.i11	ISS incident supervision	2.2%
			P.i12	ISS incident coordination	2.2%
			P.i13	Resource management	
			P.i13a	Responsibility assignment	3%
			P.i13b	Adequate personnel	2.2%
			P.i13c	Security culture	3%
			P.i14	Stakeholders communication and reporting	
			P.i14a	Principles and guidelines for communicating and reporting	3%
			P.i14b	Principles to safeguard resources	2.2%
			P.i14c	Escalation guidelines	3%
			P.i15	ISS activity effectiveness	3%
			P.i15a	ISS activity effectiveness assessment timeline	3%
			P.i16	ISS performance metrics alignment	3%
			P.i17	ISS activity feedback return	2.2%
			P.i18	Delivery of ISS activity feedback	2.2%
			P.i19	ISS performance results feedback	2.2%
Processes			P.i20	ISS program compliance	3%
			P.i20a	Compliance alignment report	2.2%
			P.i20b	Presence of Auditors	3%
			P.i20c	Auditors meetings timeline	3%
			P.i21	ISS level	3%
			P.i22	Environment changes and risks	3%
			P.i23	Revision of regulations timeline	3%
			P.i23a	Reviewing process	2.2%
			P.i23b	Reviewing process timeline	3%
			P.i24	ISS feedback transparency	3%
				Total weight for P indicators	100%
G	25%	20%	G.i25	ISSG goals	
			G.i25a	Strategic alignment	11%
			G.i25b	Value delivery	11%
			G.i25c	Accountability	11%
			G.i25d	Compliance	11%
			G.i26	Balance stakeholders needs	11%
Goals			G.i27	ISSG goals and objectives integration	8%
			G.i28	ISSG value perception	
			G.i28a	ISSG effectiveness	11%
			G.i28b	ISSG efficiency	11%
			G.i29	ISSG accountability	7%
			G.i30	ISSG compliance	8%
				Total weight for G indicators	100%
Ag	25%	40%	Ag.i31	Person in charge of the organization’s ISS	8%
			Ag.i31a	Role responsibility	6%
			Ag.i31b	Role career level	6%
Agents			Ag.i31c	Role distribution	6%
			Ag.i32	Artifact creation	
			Ag.i32a	Governing body’s artifacts	8%

		Ag.i32b	City Hall executive artifacts	8%
		Ag.i32c	Person in charge of the organization’s ISS artifacts	8%
		Ag.i33	Reporting structure	
		Ag.i33a	Governing body	8%
		Ag.i33b	Mayor	6%
		Ag.i33c	City Councilor	6%
		Ag.i33d	Person in charge of the organization’s ISS reporting	8%
		Ag.i33e	Auditors	8%
		Ag.i33f	Data Protection Officer	8%
		Ag.i33g	Employees	6%
			Total weight for Ag indicators	100%
Total	100%			

As previously mentioned, the first step collects the answer given, for each question on the instrument, and allocates their respective value (the answer value will be represented as AV in the generic formula), which is displayed in part 5.2. Then, the indicator value (represented as IV) is calculated using an weighted arithmetic mean, where the answer value (AV) is multiplied by their respective indicator weight (represented as QW), presented in Table 5. The weights displayed in Table 5 were pondered over the importance the question has over the subject, and if the question is fundamental, complementary or repeated (analyses the same concept through a different manner).

After the indicator value (IV) of each question is determined; the sum of all indicator values, of each criteria questions, generates the value for the respective criterion (represented as CV). The detailed structure, with all questions and their weights, for each of the criterion (which are represented by the dimension’s initials), are presented beneath:

Ar = 7% x Ar.i1 + 5% x Ar.i1a + 7% x Ar.i2 +7% x Ar.i2a + 5% x Ar.i2b + 7% x Ar.i3 + 7% x Ar.i3a + 7% x Ar.i3b + 5% x Ar.i3c + 7% x Ar.i3d + 7% x Ar.i4 + 5% x Ar.i4a + 5% x Ar.i4b + 7% x Ar.i4c + 7% x Ar.i5 + 5% x Ar.i5a

P = 3% x P.i6a + 3% x P.i6b + 3% x P.i6c + 3% x P.i7 + 3% x P.i8a + 3% x P.i8b + 3% x P.i8c + 3% x P.i8d + 3% x P.i9 + 3% x P.i9a + 2.2% x P.i9b + 3% x P.i10 + 2.2% x P.i11 + 2.2% x P.i12 + 3% x P.i13a + 2.2% x P.i13b + 3% x P.i13c + 3% x P.i14a + 2.2% x P.i14b + 3% x P.i14c + 3% x P.i15 + 3% x P.i15a + 3% x P.i16 + 2.2% x P.i17 + 2.2% x P.i18 + 2.2% x P.i19 + 3% x P.i20 + 2.2% x P.i20a + 3% x P.i20b + 3% x P.i20c + 3% x P.i21 + 3% x P.i22 + 3% x P.i23 + 2.2% x P.i23a + 3% x P.i23b + 3% x P.i24

G = 11% x G.i25a + 11% x G.i25b + 11% x G.i25c + 11% x G.i25d + 11% x G.i26 + 8% x G.i27 + 11% x G.i28a + 11% x G.i28b + 7% x G.i29 + 8% x G.i30

Ag = 8% x Ag.i31 + 6% x Ag.i31a + 6% x Ag.i31b + 6% x Ag.i31c + 8% x Ag.i32a + 8% x Ag.i32b + 8% x Ag.i32c + 8% x Ag.i33a + 6% x Ag.i33b + 6% x Ag.i33c + 8% x Ag.i33d + 8% x Ag.i33e + 8% x Ag.i33f + 6% x Ag.i33g

Summarized generic formulas, of the steps mentioned prior, are displayed below. The formulas, presented below, shows two ways to calculate the indicator value (IV) and the criteria value (CV). Also, within the formulas, other elements such as: n represents the question number, D represents the criteria (which can be AR, P, G or Ag), and TQ represents the total of question of said criteria. These formulas are:

$$IV = AV_n \times QW_n$$

$$CV_D = \sum_{n=1}^{TQ} [IV]$$

Or

$$CV_D = \sum_{n=1}^{TQ} [AV_n \times QW_n]$$

From this stage, calculations for the global indicator can begin. This global indicator (ISSG index) is calculated by the sum of the criteria values. The criteria weight assigned is in accordance with the method chosen (either general or by scenarios). These methods evaluate the amount of ISSG a City Hall possesses.

In the first method (global – a.k.a. EISSGLPAG), the City Hall is evaluated as a whole, with no distinction if it already possesses an ISSG in place or not. Therefore, the criteria weights remains the same 25% for each of the criteria. The equation used to calculate the weight, for the first method, is displayed below.

$$i(EISSGLPAG) = 25\%\ x\ Ar + 25\%\ x\ P + 25\%\ x\ G + 25\%\ x\ Ag$$

However in the scenario method, the City Halls are evaluated according to the presence of an ISSG. Hence, two different paths (Scenario 1 or Scenario 2), that can be calculated under the scenario's method. The definition of the scenario path comes from the answer given on the indicator Ar.i1; where the respondent answers if the City Hall already has an ISS strategy (which is one of ISSG's outputs) or not. Each scenario has different weights to their criteria.

The first scenario (Sc1 – a.k.a EISSGLPA1) represents a City Hall with an ISSG already in place. Therefore, each criterion is evaluated equally, with the same 25% criteria weight as in the global method. Which in this case, the instrument serves as a continuous improvement tool; assessing which aspect needs to be improved. The equation, to calculate the ISSG evaluation index for the first scenario, is presented below:

$$i(EISSGLPA1) = 25\%\ x\ Ar + 25\%\ x\ P + 25\%\ x\ G + 25\%\ x\ Ag$$

While the calculations for second scenario (Sc2 – a.k.a. EISSGLPA2) differs slightly, since the notion of the City Hall does not possesses a formal ISSG in place. Still, that doesn't mean the City Hall doesn't possess elements from ISSG in place; in this case, the instrument can be used to evaluate the status of those elements. Consequently, the instrument will serve as an ISSG implementation tool, by demonstrating the aspects that needs to be worked on. Therefore the index of this scenario, has different weights to their criteria, to match with the implementation process.

$$i(EISSGLPA2) \ = 20\%\ x\ Ar + 20\%\ x\ P + 20\%\ x\ G + 40\%\ x\ Ag$$

The weights assigned, in this methodological guide, for the instrument are a result from the sensitivity and knowledge accumulated throughout this study. Subjectivity may arise when it comes to this subject, the weights presented here were extensively analyzed from the ISSG literature. Therefore, the values found are judged to be as appropriate as possible for the subject.

6. Conclusion

During the course of this document, a detailed description was made, on how to conduct the evaluation of the Information Systems Security Governance of the Portuguese Local Public Administration, from the instrument created. The document which was divided into evaluation process, principles, measures and the evolution of the method covers all the objectives set out, for this document, in the first Chapter, which would deem it successful.

The method created in this document was based on a literature review, which was applied in a similar context, in which the instrument is inserted. The document in question, assessed the websites of Portuguese City Halls [Soares et al. 2017], in order to evaluate their public services, and the quality of their online public services.

The description given to procedures on how to apply the method or the evaluation measures, were created in the most detailed manner possible, thus fulfilling Principle 4, set on Chapter 3. This action was deemed crucial to provide the largest amount of detail inside this document, in order to allow the reader to successfully be able to implement the ISSG evaluation of the Portuguese Local Public Administration, therefore comprehending and verifying the status of the City Hall in question, which in its core would fulfill Principle 7.

Another aspect deemed primordial are the evaluation measures used (i.e., the criteria, indicators and eventually sub-indicators) which consist of the results from the relevant literature review of the theme and context. Thus fulfilling the first, second and third principle, described on Chapter 3.

Also, the weights attributed to each indicator and criteria, in the previous part were also defined by the knowledge gather from the literature review. This action intends to fulfill Principles 5 and 6, where the consistency of the study, against all of the City Halls and against versions of the study, is evaluated.

The study is aware that the measures aspect may have some subjectivity, although the criteria, indicators, and in particular the weights, were widely analyzed against the literature, in a sense that the empirical values found are considered to be the most adjusted.

References

Chew, E., M. Swanson, K. Stine, N. Bartol, A. Brown and W. Robinson. (2008). Performance Measurement Guide for Information Security. NIST Special Publication 800-55 Rev 1. Gaithersburg, MD: NIST Pubs. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

COSO. (2004). Enterprise Risk Management — Integrated Framework. Retrieved from https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

GFOA. (2009). Creating a Comprehensive Risk Management Program. Retrieved December 27, 2018, from http://www.gfoa.org/creating-comprehensive-risk-management-program

Lopes, I. M. (2012). Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal. Universidade do Minho.

Merriam-Webster. (2019). Definition of Program. Retrieved January 3, 2019, from https://www.merriam-webster.com/dictionary/program

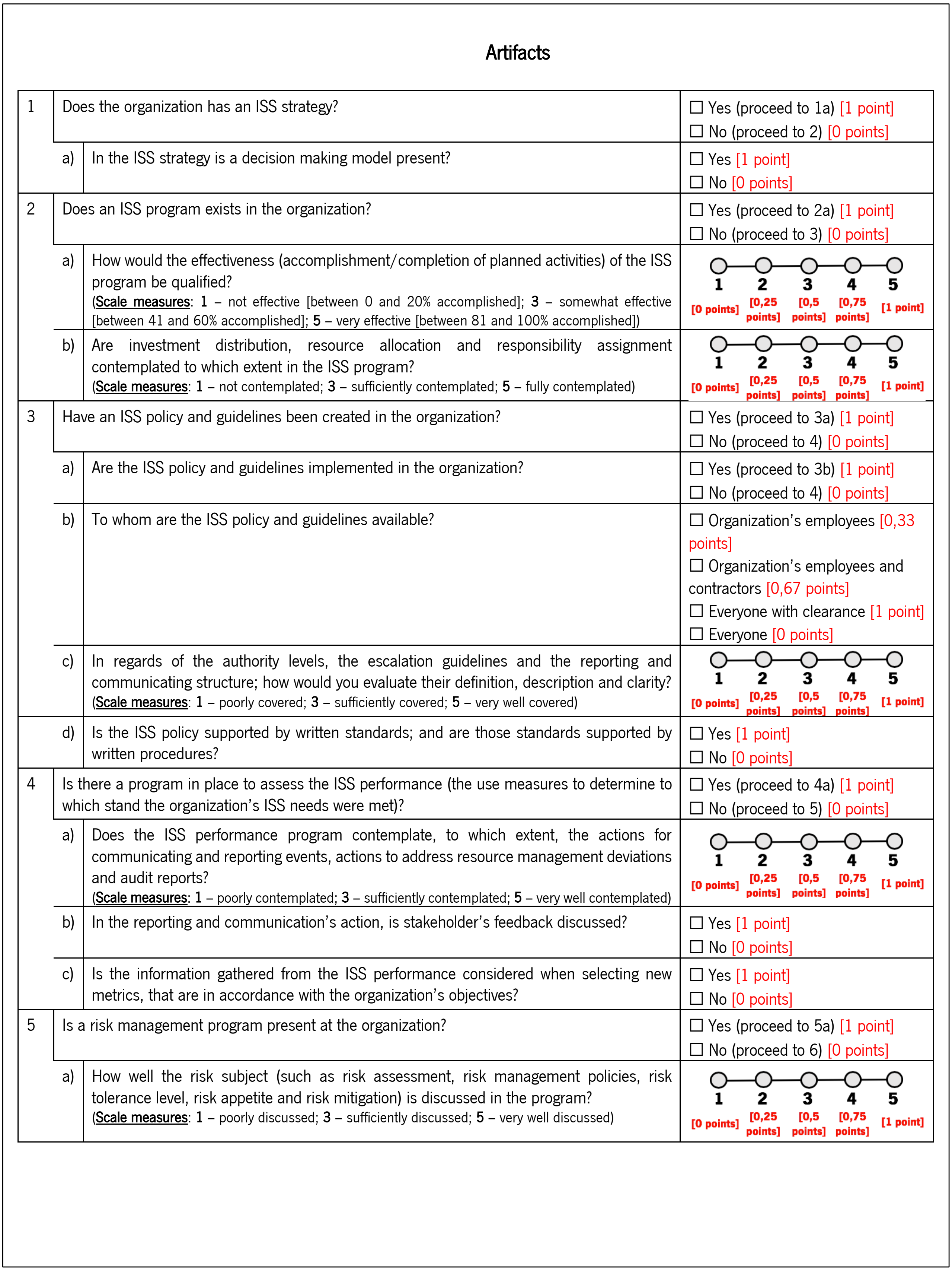
Pironti, J. P. (2010). Developing an Information Security and Risk Management Strategy. ISACA Journal, 2(Security), 28–35. Retrieved from https://www.isaca.org/Journal/archives/2010/Volume-2/Pages/Developing-an-Information-Security-and-Risk-Management-Strategy1.aspx

de Sá-Soares, F. (2005). Interpretação da Segurança de Sistemas de Informação Segundo a Teoria da Acção. Universidade do Minho.

Soares, D., L. Amaral and L. Ferreira. (2017). Presença na Internet das Câmaras Municipais Portuguesas em 2016 : Estudo sobre Local e-Government em Portugal. Guimarães: Gávea – Observatório da Sociedade da Informação.

Appendix M – Methodological Guide Accessory – Instrument V5 Cheat Sheet

A modified version of the Instrument V5, present in this appendix through Figure 31, was created so aplicators could assess the value for the respondent answer in an easier manner, which wouldn’t necessarily need a large amount of effort. In this accessory, the answer values given in the methodological guide is presented right by the answers in the questionnaire.



Artifacts

1	Does the organization has an ISS strategy?		☐ Yes (proceed to 1a) [1 point] ☐ No (proceed to 2) [0 points]
	a)	In the ISS strategy is a decision making model present?	☐ Yes [1 point] ☐ No [0 points]
2	Does an ISS program exists in the organization?		☐ Yes (proceed to 2a) [1 point] ☐ No (proceed to 3) [0 points]
	a)	How would the effectiveness (accomplishment/completion of planned activities) of the ISS program be qualified? (Scale measures: **1** – not effective [between 0 and 20% accomplished]; **3** – somewhat effective [between 41 and 60% accomplished]; **5** – very effective [between 81 and 100% accomplished])	○—○—○—○—○ **1** [0 points] **2** [0,25 points] **3** [0,5 points] **4** [0,75 points] **5** [1 point]
	b)	Are investment distribution, resource allocation and responsibility assignment contemplated to which extent in the ISS program? (Scale measures: **1** – not contemplated; **3** – sufficiently contemplated; **5** – fully contemplated)	○—○—○—○—○ **1** [0 points] **2** [0,25 points] **3** [0,5 points] **4** [0,75 points] **5** [1 point]
3	Have an ISS policy and guidelines been created in the organization?		☐ Yes (proceed to 3a) [1 point] ☐ No (proceed to 4) [0 points]
	a)	Are the ISS policy and guidelines implemented in the organization?	☐ Yes (proceed to 3b) [1 point] ☐ No (proceed to 4) [0 points]
	b)	To whom are the ISS policy and guidelines available?	☐ Organization's employees [0,33 points] ☐ Organization's employees and contractors [0,67 points] ☐ Everyone with clearance [1 point] ☐ Everyone [0 points]
	c)	In regards of the authority levels, the escalation guidelines and the reporting and communicating structure; how would you evaluate their definition, description and clarity? (Scale measures: **1** – poorly covered; **3** – sufficiently covered; **5** – very well covered)	○—○—○—○—○ **1** [0 points] **2** [0,25 points] **3** [0,5 points] **4** [0,75 points] **5** [1 point]
	d)	Is the ISS policy supported by written standards; and are those standards supported by written procedures?	☐ Yes [1 point] ☐ No [0 points]
4	Is there a program in place to assess the ISS performance (the use measures to determine to which stand the organization's ISS needs were met)?		☐ Yes (proceed to 4a) [1 point] ☐ No (proceed to 5) [0 points]
	a)	Does the ISS performance program contemplate, to which extent, the actions for communicating and reporting events, actions to address resource management deviations and audit reports? (Scale measures: **1** – poorly contemplated; **3** – sufficiently contemplated; **5** – very well contemplated)	○—○—○—○—○ **1** [0 points] **2** [0,25 points] **3** [0,5 points] **4** [0,75 points] **5** [1 point]
	b)	In the reporting and communication's action, is stakeholder's feedback discussed?	☐ Yes [1 point] ☐ No [0 points]
	c)	Is the information gathered from the ISS performance considered when selecting new metrics, that are in accordance with the organization's objectives?	☐ Yes [1 point] ☐ No [0 points]
5	Is a risk management program present at the organization?		☐ Yes (proceed to 5a) [1 point] ☐ No (proceed to 6) [0 points]
	a)	How well the risk subject (such as risk assessment, risk management policies, risk tolerance level, risk appetite and risk mitigation) is discussed in the program? (Scale measures: **1** – poorly discussed; **3** – sufficiently discussed; **5** – very well discussed)	○—○—○—○—○ **1** [0 points] **2** [0,25 points] **3** [0,5 points] **4** [0,75 points] **5** [1 point]

Figure 31 – Instrument V5 Answers Values

Processes

6		How would you evaluate the alignment of the ISS with the business strategy ... (Scale measures: 1 – poorly aligned; 3 – sufficiently aligned; 5 – completely aligned)	
	a)	when considering the ISS issues in the organization initiatives?	○ 1 [0 points] ○ 2 [0,25 points] ○ 3 [0,5 points] ○ 4 [0,75 points] ○ 5 [1 point]
	b)	to support the organization objectives?	○ 1 [0 points] ○ 2 [0,25 points] ○ 3 [0,5 points] ○ 4 [0,75 points] ○ 5 [1 point]
	c)	in handling the results from the ISS performance, like prioritizing or initiating the required actions derived from those results?	○ 1 [0 points] ○ 2 [0,25 points] ○ 3 [0,5 points] ○ 4 [0,75 points] ○ 5 [1 point]
7		Are benefits (such as: good results or advantages) perceived from the investments in ISS?	□ Yes [1 point] □ No [0 points]
8		How would you describe the commitment of the executive management in ... (Scale measures: 1 – not committed; 3 – sufficiently committed; 5 – fully committed)	
	a)	protecting the information assets?	○ 1 [0 points] ○ 2 [0,25 points] ○ 3 [0,5 points] ○ 4 [0,75 points] ○ 5 [1 point]
	b)	making ISS related decisions?	○ 1 [0 points] ○ 2 [0,25 points] ○ 3 [0,5 points] ○ 4 [0,75 points] ○ 5 [1 point]
	c)	developing and approving the ISS strategy and policy?	○ 1 [0 points] ○ 2 [0,25 points] ○ 3 [0,5 points] ○ 4 [0,75 points] ○ 5 [1 point]
	d)	allocating investments and resources?	○ 1 [0 points] ○ 2 [0,25 points] ○ 3 [0,5 points] ○ 4 [0,75 points] ○ 5 [1 point]
9		Does the organization follow a risk management policy to manage the risks encountered?	□ Yes (proceed to 9a) [1 point] □ No (proceed to 10) [0 points]
	a)	How often are the risks reviewed? (Scale measures: 1 = less than 1 year; 2 = between 1 and 2 years; 3 = more than 2 years)	○ 1 [1 point] ○ 2 [0,5 points] ○ 3 [0 points]
	b)	Is the risk appetite described in the policy?	□ Yes [1 point] □ No [0 points]
10		Is there a guideline or plan to be followed to determine the risk appetite for new risks?	□ Yes [1 point] □ No [0 points]
11		Are procedures in place to oversee ISS incidents, including public and investor relations?	□ Yes [1 point] □ No [0 points]
12		Are there procedures in place, that coordinate with law enforcement, to oversee ISS incidents?	□ Yes [1 point] □ No [0 points]
13		How much is covered in the resource management of the ISS program for ... (Scale measures: 1 – not covered; 3 – sufficiently covered; 5 – fully covered)	
	a)	assignment of responsibilities?	○ 1 [0 points] ○ 2 [0,25 points] ○ 3 [0,5 points] ○ 4 [0,75 points] ○ 5 [1 point]
	b)	having competent and motivated personnel?	○ 1 [0 points] ○ 2 [0,25 points] ○ 3 [0,5 points] ○ 4 [0,75 points] ○ 5 [1 point]
	c)	promoting a positive information security culture?	○ 1 [0 points] ○ 2 [0,25 points] ○ 3 [0,5 points] ○ 4 [0,75 points] ○ 5 [1 point]

14	How much is covered of the stakeholders communication and reporting in the ISS program for … (**Scale measures**: **1** – poorly covered; **3** – sufficiently covered; **5** – very well covered)		
	a)	reporting and communication of principles and guidelines?	○ **1** [0 points] ○ **2** [0,25 points] ○ **3** [0,5 points] ○ **4** [0,75 points] ○ **5** [1 point]
	b)	principles for safeguarding the resources?	○ **1** [0 points] ○ **2** [0,25 points] ○ **3** [0,5 points] ○ **4** [0,75 points] ○ **5** [1 point]
	c)	escalation guidelines?	○ **1** [0 points] ○ **2** [0,25 points] ○ **3** [0,5 points] ○ **4** [0,75 points] ○ **5** [1 point]
15	How would you quantify the effectiveness of the ISS activities? (**Scale measures**: **1** – not effective [between 0 and 20% accomplished]; **3** – somewhat effective [between 41 and 60% accomplished]; **5** – very effective [between 81 and 100% accomplished])		○ **1** [0 points] ○ **2** [0,25 points] ○ **3** [0,5 points] ○ **4** [0,75 points] ○ **5** [1 point]
	a)	How often is the effectiveness of the ISS activity assessed? (**Scale measures**: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)	○ **1** [1 point] ○ **2** [0,5 points] ○ **3** [0 points]
16	Does the selected ISS performance metrics ponder the organization's perspective?		□ Yes [1 point] □ No [0 points]
17	Does the ISS activity receive effective and meaningful feedback from the groups(units) it works with?		□ Yes [1 point] □ No [0 points]
18	Does the ISS activity provide effective and meaningful feedback to the groups(units) it works with?		□ Yes [1 point] □ No [0 points]
19	Are the results of the ISS performance used in providing feedback and demonstrating their impacts on the organization?		□ Yes [1 point] □ No [0 points]
20	Is the ISS program reviewed to verify its compliance with legislation, regulations, contractual obligations and statutory requirements?		□ Yes (proceed to 19a) [1 point] □ No (proceed to 20) [0 points]
	a)	Is the compliance of the ISS practices and their alignment to the nature of the organization's purpose, reported to the stakeholders?	□ Yes [1 point] □ No [0 points]
	b)	Is there an internal or external regulatory compliance group (auditors)?	□ Yes [1 point] □ No [0 points]
	c)	When did the ISS activity last meet with the auditors? (**Scale measures**: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)	○ **1** [1 point] ○ **2** [0,5 points] ○ **3** [0 points]
21	Are independent audits commissioned to verify the determined level for the organization's ISS?		□ Yes [1 point] □ No [0 points]
22	Does the ISS strategy considers the changes in different types of environment (organizational, legal and regulatory) and their potential information risk?		□ Yes [1 point] □ No [0 points]
23	How often are regulations reviewed to understand the ISS requirements? (**Scale measures**: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)		○ **1** [1 point] ○ **2** [0,5 points] ○ **3** [0 points]
	a)	Is the legal department involved in the review process of the ISS activity?	□ Yes (proceed to 22b) [1 point] □ No (proceed to 23) [0 points]
	b)	When did the ISS activity last review a contractual requirement with the legal counsel? (**Scale measures**: **1** = less than 1 year; **2** = between 1 and 2 years; **3** = more than 2 years)	○ **1** [1 point] ○ **2** [0,5 points] ○ **3** [0 points]
24	Is there a feedback provided by the organization, that regards the transparency over ISS costs, benefits and risks?		□ Yes [1 point] □ No [0 points]

Goals

25	How would you evaluate the accomplishment of the ISSG goals for … (Scale measures: **1** – not accomplished; **3** – sufficiently accomplished; **5** – fully accomplished)		
	a)	strategic alignment (the link between the ISS strategy and the organization's activity)?	○ **1** [0 points] ○ **2** [0,25 points] ○ **3** [0,5 points] ○ **4** [0,75 points] ○ **5** [1 point]
	b)	value delivery (the delivery of promised benefits while optimizing costs)?	○ **1** [0 points] ○ **2** [0,25 points] ○ **3** [0,5 points] ○ **4** [0,75 points] ○ **5** [1 point]
	c)	accountability (accept responsibility for the ISSG actions in the organization)?	○ **1** [0 points] ○ **2** [0,25 points] ○ **3** [0,5 points] ○ **4** [0,75 points] ○ **5** [1 point]
	d)	compliance (fulfill requirements in accordance with regulations, laws and contractual obligations)?	○ **1** [0 points] ○ **2** [0,25 points] ○ **3** [0,5 points] ○ **4** [0,75 points] ○ **5** [1 point]
26	To which extent are the needs of stakeholders balanced in the process of creating an ISS strategy? (Scale measures: **1** – not balanced; **3** – sufficiently balanced; **5** – fully balanced)		○ **1** [0 points] ○ **2** [0,25 points] ○ **3** [0,5 points] ○ **4** [0,75 points] ○ **5** [1 point]
27	Are the ISSG goals and objectives integrated within all levels of the organization?		□ Yes [1 point] □ No [0 points]
28	To which degree is the value for the governance of the ISS perceived by the organization in relation to … (Scale measures: **1** – no value added [between 0 and 20%]; **3** – fair amount of value added [between 41 and 60%]; **5** – a lot of value added [between 81 and 100%])		
	a)	effectiveness (accomplishment of what was set out to be done)?	○ **1** [0 points] ○ **2** [0,25 points] ○ **3** [0,5 points] ○ **4** [0,75 points] ○ **5** [1 point]
	b)	efficiency (achieve the desired result with little waste)?	○ **1** [0 points] ○ **2** [0,25 points] ○ **3** [0,5 points] ○ **4** [0,75 points] ○ **5** [1 point]
29	Has the ISSG set out rules that makes people accountable for their actions?		□ Yes [1 point] □ No [0 points]
30	How much is compliance a part of the ISSG in the organization? (Scale measures: **1** – not important [between 0 and 20% of compliance]; **3** – somewhat important [between 41 and 60% of compliance]; **5** – very important [between 81 and 100% of compliance])		○ **1** [0 points] ○ **2** [0,25 points] ○ **3** [0,5 points] ○ **4** [0,75 points] ○ **5** [1 point]

Agents

31	Who is the **person in charge of the organization's ISS**?		☐ CIO [1 point] ☐ CISO [0,75 points] ☐ Mayor [0,5 points] ☐ City Councilor [0,25 points] ☐ Other City Hall employee [0 points]
	a)	Is the person in charge driving the ISS activity or mostly reporting compliance?	☐ directing the ISS activity [1 point] ☐ reporting compliance on the ISS activity [0 points]
	b)	What is the career level of the person in charge of the ISS?	☐ University degree [1 point] ☐ Technical degree [0,5 points] ☐ High School degree [0 points] ☐ Other [0 points]
	c)	Does the person in charge of the ISS have other roles in the organization?	☐ Yes [0 points] ☐ No [1 point]

32	Mark the correspondent artifact, that each role is responsible for developing. (Multiple choices accepted)							
	Role	Artifacts						
a)	Governing body (person or group accountable for the organization's performance and conformity)	☐ ISS strategy **[0,5 points]**	☐ ISS program [0 points]	☐ ISS policies and guidelines **[0,5 points]**	☐ ISS performance program [0 points]	☐ Risk management program [0 points]	☐ Not Assigned [0 points]	
b)	City Hall executive (group usually formed by the City Hall Mayor and members of the City Council)	☐ ISS strategy [0 points]	☐ ISS program **[0,5 points]**	☐ ISS policies and guidelines [0 points]	☐ ISS performance program **[0,5 points]**	☐ Risk management program [0 points]	☐ Not Assigned [0 points]	
c)	Person in charge of the organization's ISS	☐ ISS strategy CIO/Mayor/Councilor [0 points] CISO [0 points] Other [0 points]	☐ ISS program **CIO/Mayor/Councilor [0,5 points]** CISO [0 points] Other [0 points]	☐ ISS policies and guidelines CIO/Mayor/Councilor [0 points] CISO [0 points] Other [0 points]	☐ ISS performance program **CIO/Mayor/Councilor [0,5 points]** CISO [0 points] Other [0 points]	☐ Risk management program CIO/Mayor/Councilor [0 points] **CISO [1 point]** Other [0 points]	☐ Not Assigned [0 points]	

33	Mark the correspondent reporting role, that each main role is responsible for reporting to?				
	Main Role	Reports to			
a)	Governing body	☐ Governing body [0 points]	☐ City Hall Executive [0 points]	☐ In-Line Management [0 points]	☐ Stakeholders **[1 point]**
b)	Mayor (person elected to act as head of a city)	☐ Governing body **[1 point]**	☐ City Hall Executive [0 points]	☐ In-Line Management [0 points]	☐ Stakeholders [0 points]
c)	City Councilor (member of the legislative body that governs the city)	☐ Governing body [0 points]	☐ City Hall Executive **[1 point]**	☐ In-Line Management [0 points]	☐ Stakeholders [0 points]
d)	Person in charge of the organization's ISS	☐ Governing body **CIO/Mayor [1 point]** CISO/Councilor [0 points] Other [0 points]	☐ City Hall Executive CIO/Mayor [0 points] **CISO/Councilor [1 point]** Other [0 points]	☐ In-Line Management CIO/Mayor [0 points] CISO/Councilor [0 points] **Other [1 point]**	☐ Stakeholders CIO/Mayor [0 points] CISO/Councilor [0 points] Other [0 points]
e)	Auditors (person responsible for assessing the governance activities compliance with the standards)	☐ Governing body **[1 point]**	☐ City Hall Executive [0 points]	☐ In-Line Management [0 points]	☐ Stakeholders [0 points]
f)	Data Protection Officer (DPO) (person responsible for overseeing the data protection strategy, implementation and compliance with the GDPR)	☐ Governing body **[1 point]**	☐ City Hall Executive [0 points]	☐ In-Line Management [0 points]	☐ Stakeholders [0 points]
g)	Employees (individual who is payed to work)	☐ Governing body [0 points]	☐ City Hall Executive [0 points]	☐ In-Line Management **[1 point]**	☐ Stakeholders [0 points]

Chief Information Officer (CIO) - person responsible for the ISS program, policy; and its compliance.
Chief Information Security Officer (CISO) - person responsible for all the ISS activities.

Appendix N – Instrument Evaluation: Pretest

The pretests included within this appendix were used as an initial attempt to verify the validity of the instrument produced. Complementing those tests, a radar chart was created in order to visualize the differences that may appear within the criteria between one scenario to another.

The order of appearance in this appendix is the same for each of the scenarios. First are the answers given on the instrument for each scenario (Table 74 and Table 77) , alongside the answer to each question is their value, which is expressed in 5.2 of the methodological guide. Also representing each scenario a radar chart alongside with two tables are displayed. The first table corresponds to the values for each criterion, while the second represents the global indicator/index calculation. Hence, Figure 32 and Figure 33 represent the radar chart for scenario 1 and scenario 2, while Table 75 and Table 78 represent their criteria values, and Table 76 and Table 79 represent their global indicator/index calculations. The first scenario represents a City Hall with ISSG present, while scenario 2 the City Hall doesn't have an ISSG yet.

Table 74 – Pretest – Scenario 1 – Answer Value

Question	Resspondent answer	Answer value
1	Yes	1
1a	No	0
2	Yes	1
2a	3	0,5
2b	2	0,25
3	Yes	1
3a	Yes	1
3b	Organization's employees	0,33
3c	3	0,5
3d	Yes	1
4	Yes	1
4a	3	0,5
4b	Yes	1
4c	Yes	1
5	Yes	1
5a	4	0,75
6		
6a	2	0,25
6b	3	0,5
6c	3	0,5
7	Yes	1
8		
8a	4	0,75
8b	4	0,75
8c	4	0,75
8d	3	0,5
9	Yes	1
9a	3	0
9b	Yes	1
10	Yes	1
11	Yes	1
12	Yes	1
13		
13a	3	0,5
13b	2	0,25
13c	3	0,5
14		
14a	4	0,75
14b	4	0,75
14c	5	1
15	4	0,75
15a	2	0,5
16	Yes	1
17	Yes	1
18	Yes	1
19	Yes	1
20	Yes	1
20a	Yes	1
20b	Yes	1
20c	2	0,5
21	Yes	1
22	Yes	1
23	3	0
23a	Yes	1
23b	3	0
24	Yes	1

Question	Resspondent answer		Answer value		
25					
25a	2		0,25		
25b	3		0,5		
25c	4		0,75		
25d	5		1		
26	4		0,75		
27	No		0		
28					
28a	2		0,25		
28b	2		0,25		
29	Yes		1		
30	4		0,75		
31	CISO		0,75		
31a	directing the ISS activity		1		
31b	University degree		1		
31c	No		1		
32					
32a	ISS strategy	ISS policies and guidelines	0,5	0,5	1
32b	ISS program		0,5		0,5
32c	ISS program		0		0
33					
33a	Stakeholders		1		
33b	Governing body		1		
33c	City Hall Executive		1		
33d	Governing body		0		
33e	City Hall Executive		0		
33f	City Hall Executive		0		
33g	In-Line Management		1		

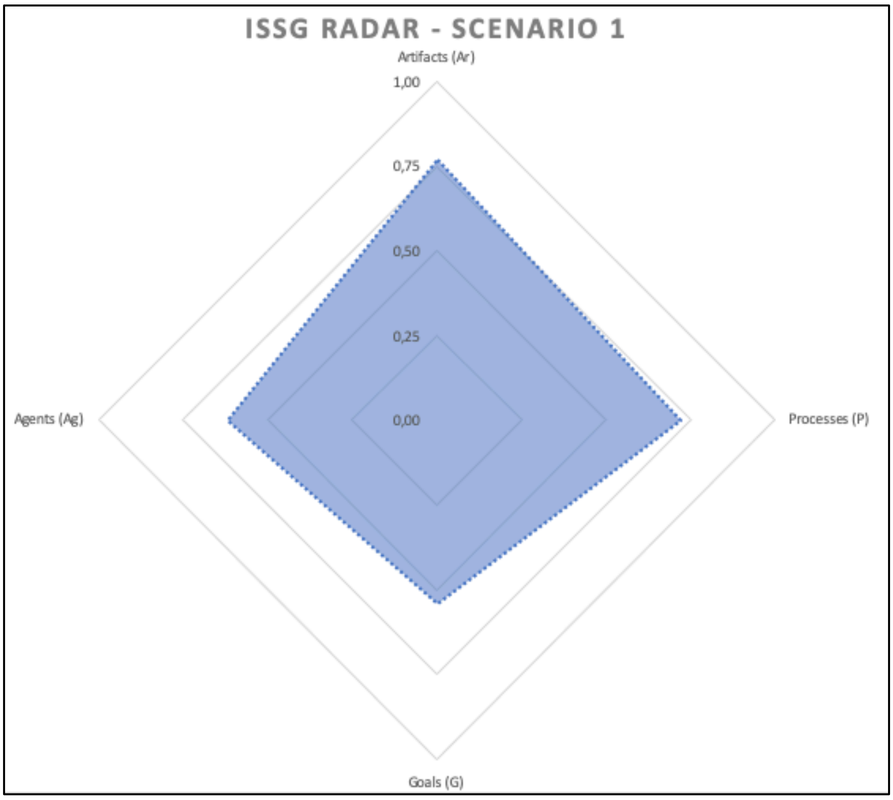


Figure 32 – Scenario 1 – Criteria Radar

Table 75 – ISSG Criteria Radar – Scenario 1

Radar ISSG SC1			
Artifacts (Ar)	**Processes (P)**	**Goals (G)**	**Agents (Ag)**
0,77	0,72	0,54	0,62

Table 76 – Global Indicator Calculus – Scenario 1

Global evaluation formula	$\mathrm{i(EISSGLPAG)} = 25\%\ \mathrm{x\ Ar} + 25\%\ \mathrm{x\ P} + 25\%\ \mathrm{x\ G} + 25\%\ \mathrm{x\ Ag}$
Global evaluation calculus	$\mathrm{i(EISSGLPAG)} = 25\%\ \mathrm{x}\ 0{,}77 + 25\%\ \mathrm{x}\ 0{,}72 + 25\%\ \mathrm{x}\ 0{,}54 + 25\%\ \mathrm{x}\ 0{,}62 = 0{,}66$
Scenario 1 evaluation formula	$\mathrm{i(EISSGLPA1)} = 25\%\ \mathrm{x\ Ar} + 25\%\ \mathrm{x\ P} + 25\%\ \mathrm{x\ G} + 25\%\ \mathrm{x\ Ag}$
Scenario 1 evaluation calculus	$\mathrm{i(EISSGLPA1)} = 25\%\ \mathrm{x}\ 0{,}77 + 25\%\ \mathrm{x}\ 0{,}72 + 25\%\ \mathrm{x}\ 0{,}54 + 25\%\ \mathrm{x}\ 0{,}62 = 0{,}66$

Table 77 – Pretest – Scenario 2 – Answer Value

Question	Resspondent answer	Answer value
1	No	0
1a	No	0
2	Yes	1
2a	2	0,25
2b	2	0,25
3	Yes	1
3a	Yes	1
3b	Organization's employees	0,33
3c	3	0,5
3d	Yes	1
4	No	0
4a	1	0
4b	Yes	1
4c	No	0
5	Yes	1
5a	3	0,5
6		
6a	2	0,25
6b	4	0,75
6c	1	0
7	Yes	1
8		
8a	2	0,25
8b	2	0,25
8c	2	0,25
8d	2	0,25
9	No	0
9a	3	0
9b	No	0
10	No	0
11	Yes	1
12	Yes	1
13		
13a	4	0,75
13b	3	0,5
13c	2	0,25
14		
14a	2	0,25
14b	1	0
14c	4	0,75
15	3	0,5
15a	3	0
16	No	0
17	Yes	1
18	No	0
19	No	0
20	Yes	1
20a	Yes	1
20b	Yes	1
20c	2	0,5
21	No	0
22	No	0
23	2	0,5
23a	No	0
23b	3	0
24	Yes	1

Question	Resspondent answer		Answer value		
25					
25a	2		0,25		
25b	2		0,25		
25c	3		0,5		
25d	4		0,75		
26	2		0,25		
27	No		0		
28					
28a	3		0,5		
28b	3		0,5		
29	Yes		1		
30	4		0,75		
31	City Councilor		0,25		
31a	reporting compliance on the ISS activity		0		
31b	University degree		1		
31c	No		1		
32					
32a	ISS policies and guidelines		0,5		0,5
32b	ISS program	ISS policies and guidelines	0,5	0	0,5
32c	ISS program	Risk management program	0,5	0	0,5
33					
33a	City Hall Executive		0		
33b	Stakeholders		0		
33c	City Hall Executive		1		
33d	City Hall Executive		1		
33e	City Hall Executive		0		
33f	City Hall Executive		0		
33g	In-Line Management		1		

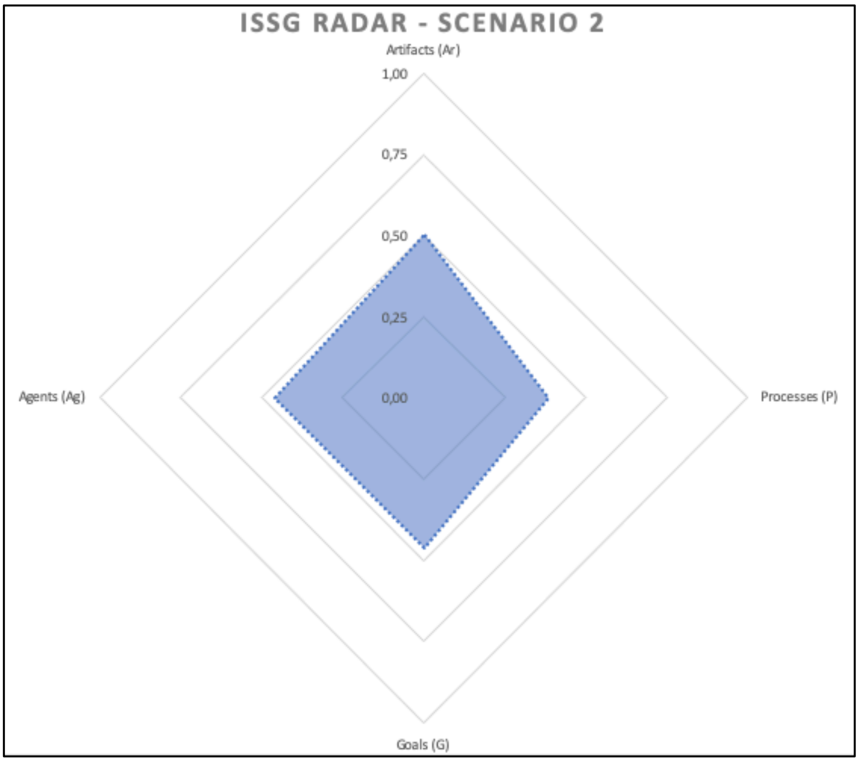


Figure 33 – Scenario 2 – Criteria Radar

Table 78 – ISSG Criteria Radar – Scenario 2

Radar ISSG SC2			
Artifacts (Ar)	**Processes (P)**	**Goals (G)**	**Agents (Ag)**
0,50	0,38	0,46	0,46

Table 79 – Global Indicator Calculus – Scenario 2

Global evaluation formula	$\mathrm{i(EISSGLPAG)} = 25\%\ \mathrm{x}\ \mathrm{Ar} + 25\%\ \mathrm{x}\ \mathrm{P} + 25\%\ \mathrm{x}\ \mathrm{G} + 25\%\ \mathrm{x}\ \mathrm{Ag}$
Global evaluation calculus	$\mathrm{i(EISSGLPAG)} = 25\%\ \mathrm{x}\ 0{,}50 + 25\%\ \mathrm{x}\ 0{,}38 + 25\%\ \mathrm{x}\ 0{,}46 + 25\%\ \mathrm{x}\ 0{,}46 = 0{,}45$
Scenario 2 evaluation formula	$\mathrm{i(EISSGLPA2)} = 20\%\ \mathrm{x}\ \mathrm{Ar} + 20\%\ \mathrm{x}\ \mathrm{P} + 20\%\ \mathrm{x}\ \mathrm{G} + 40\%\ \mathrm{x}\ \mathrm{Ag}$
Scenario 2 evaluation calculus	$\mathrm{i(EISSGLPA2)} = 20\%\ \mathrm{x}\ 0{,}50 + 20\%\ \mathrm{x}\ 0{,}38 + 20\%\ \mathrm{x}\ 0{,}46 + 40\%\ \mathrm{x}\ 0{,}46 = 0{,}45$

References

Abu-Musa, A. (2010). Information security governance in Saudi organizations: an empirical study. *Information Management & Computer Security*, *18*(4), 226–276.

Agência para a Modernização Administrativa. (2014). Programa Aproximar - Estratégia para a Reorganização dos Serviços de Atendimento da Administração Pública. Retrieved October 14, 2018, from https://www.historico.portugal.gov.pt/pt/o-governo/arquivo-historico/governos-constitucionais/gc20/os-temas/20140925-aproximar/aproximar.aspx

Agência para a Modernização Administrativa. (2017). Estratégia TIC 2020. Retrieved April 23, 2018, from https://tic.gov.pt/pt/web/tic/-/estrategia-tic-2020?redirect=%2F

Agência para a Modernização Administrativa. (2018a). ICT STRATEGY 2020. Retrieved from https://tic.gov.pt/documents/37177/109352/CTIC_TIC2020_Estrategia_TIC_EN.pdf/3d260b59-ec1a-072f-e84c-84e6648f3cda

Agência para a Modernização Administrativa. (2018b). Transformação digital - TIC. Retrieved from https://www.ama.gov.pt/web/agencia-para-a-modernizacao-administrativa/pgetic

Agência para Modernização Administrativa. (2015). O que é o PGETIC? — TIC.GOV.PT. Retrieved December 29, 2017, from https://tic.gov.pt/pgetic

Almeida, I. A. (2017). *Caracterização Infraestrutural , Aplicacional e Funcional das Tecnologias e Sistemas de Informação nas Câmaras Municipais Portuguesas*. Universidade do Minho.

Assembleia Constituinte. Constituição da República Portuguesa, Diário da República Eletrónico § (2005). Portugal: Diário da República Eletrónico. Retrieved from https://dre.pt/web/guest/legislacao-consolidada/-/lc/337/202004071757/128226/exportPdf/normal/1/cacheLevelPage?_LegislacaoConsolidada_WAR_drefrontofficeportlet_rp=diploma

Associação Nacional Municípios Portugueses. (2017). Lista de Municípios. Retrieved December 8, 2017, from http://anmp.pt/munp/mun/mun101l1.php?cod=20140110

Bowen, P., J. Hash and M. Wilson. (2006). Information Security Handbook : A Guide for Managers. In *NIST Special Publication 800-100*. Scotts Valley, CA: CreateSpace. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

Chew, E., M. Swanson, K. Stine, N. Bartol, A. Brown and W. Robinson. (2008). *Performance Measurement Guide for Information Security. NIST Special Publication 800-55 Rev 1*. Gaithersburg, MD: NIST Pubs. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

COSO. (2004). Enterprise Risk Management — Integrated Framework. Retrieved from https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

Dhillon, G. (1997). *Managing Information System Security*. Basingstoke, Hampshire: MACMILLAN PRESS LTD.

Dhillon, G. (2007). Corporate Governance for IS Security. In *Principles of Information Systems Security: Text and Cases* pp. 198–218. Hoboken: John Wiley & Sons.

Dhillon, G., G. Tejay and H. Weiyin. (2007). Identifying Governance Dimensions to Evaluate Information Systems Security in Organizations. In *Proceedings of the Annual Hawaii International Conference on System Sciences* pp. 1–9.

European Union. (2016). Regulation 2016/679 of the European parliament and the Council of the European Union. *Official Journal of the European Communities*, 1–88. www.doi.org/http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf

Eurostat. (2017). European Commission, Eurostat, NUTS - Nomenclature of territorial units for statistics, NUTS Maps. Retrieved November 30, 2017, from http://ec.europa.eu/eurostat/web/nuts/nuts-maps-.pdf-

Fink, A. (2003). The Survey Handbook. In *The Survey Kit 2* 2nd Editio, Vol. 1. Thousand Oaks, California: Sage Publications.

GFOA. (2009). Creating a Comprehensive Risk Management Program. Retrieved December 27, 2018, from http://www.gfoa.org/creating-comprehensive-risk-management-program

Gupta, R., S. K. Muttoo and S. K. Pal. (2017). Proposed Framework for Information Systems Security for e-Governance in Developing Nations. In *10th International Conference on Theory and Practice of Electronic Governance - ICEGOV '17* pp. 546–547. New Delhi, India.

Helms, R., E. Giovacchini, R. Teigland and T. Kohler. (2010). A Design Research Approach to Developing User Innovation Workshops in Second Life. *Journal of Virtual Worlds Research*, *3*(1), 3–36.

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*, *19*(2), 87–92.

Hevner, A. R., S. T. March, J. Park and S. Ram. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

Iivari, J. (2007). A Paradigmatic Analysis of Information Systems as a Design Science. *Scandanavian Journal of Information Systems*, *19*(2), 39–64.

INE. (2016). População média anual residente (N.º) por Local de residência (Distrito/ Região), Sexo e Grupo etário (Por ciclos de vida); Anual. *Instituto Nacional de Estatística*. Retrieved from https://www.ine.pt/bddXplorer/htdocs/printable.jsp?id=9Cny-4RTcwiEPr6zqjmCN2a8_29252&lingua_cd=PT

Instituto Nacional de Estatística. (2018). INE - Divisão administrativa. Retrieved August 19, 2018, from https://www.ine.pt/xportal/ine/portal/portlets/html/conteudos/listaContentPage.jsp?BOUI=6251013&xlang=PT

ISACA. (2012a). *COBIT 5: Enabling Processes*. Rolling Meadows, IL: ISACA. Retrieved from papers3://publication/uuid/24E0C493-40C6-4495-946E-A25765C97BF1

ISACA. (2012b). *COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT*. ISACA.

ISACA. (2013). *COBIT 5: Enabling Information*. Rolling Meadows, IL: ISACA.

ISACA. (2018a). *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution*. Schaumburg, IL: ISACA.

ISACA. (2018b). *COBIT® 2019 Framework: Governance and Management Objectives*. Schaumburg, IL: ISACA.

ISACA. (2018c). *COBIT® 2019 Framework: Introduction and Methodology*. Schaumburg, IL: ISACA.

ISACA. (2018d). *COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution*. Schaumburg, IL: ISACA.

ISACA. (2018e). Introducing COBIT 2019 - OVERVIEW November 2018. Retrieved from http://www.isaca.org/COBIT/Documents/COBIT-2019-Toolkit_fmk_eng_1118.zip

ISACA. (2019a). Frequently Asked Questions: COBIT 2019. Retrieved April 6, 2019, from http://www.isaca.org/COBIT/Pages/FAQs-COBIT-2019.aspx

ISACA. (2019b). ISACA - Glossary. Retrieved October 27, 2019, from https://www.isaca.org/Pages/Glossary.aspx?tid=1263&char=C

ISO/IEC. (2013). ISO/IEC 27014:2013 - Information technology - security techniques - Governance of information security. International Organization for Standartization/International Electrotechnical Comission.

ISO/IEC. (2019). ISO/IEC DIS 27014 – Information security, cybersecurity and privacy protection – Governance of information security. Retrieved December 6, 2019, from https://www.iso.org/standard/74046.html

Joshi, A., S. Kale, S. Chandel and D. Pal. (2015). Likert Scale: Explored and Explained. *British Journal of Applied Science & Technology*, *7*(4), 396–403. www.doi.org/10.9734/bjast/2015/14975

Kerlinger, F. N. (1986). *Foundations of Behavioral Research* 3rd Editio. Orlando, Florida: Harcourt Brace Jovanovich College Publishers.

Litwin, M. S. (2003). How to Assess and Interpret Survey Psychometrics. In *The Survey Kit 2* 2nd Editio, Vol. 8. Thousand Oaks, California: Sage Publications.

Lopes, I. M. (2012). *Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal*. Universidade do Minho.

Lopes, I. M. and F. de Sá-Soares. (2010). Information Systems Security Policies : A Survey in Portuguese Public Administration. In *IADIS International Conference Information Systems* pp. 61–69.

Lopes, I. M. and P. Oliveira. (2016). Evolução da Institucionalização de Políticas de Segurança de Sistemas de Informação na Administração Pública Portuguesa. In *11th Iberian Conference on Information Systems and Technologies (CISTI)* pp. 240–245.

Love, P., J. Reinhard, A. J. Schwab and G. Spafford. (2010). *Global Technology Audit Guide (GTAG®) 15 Information Security Governance*. Altamonte Springs, FL: The Institute of Internal Auditors [IIA].

Mahncke, R. J. (2013). The Applicability of ISO/IEC27014 : 2013 For Use Within General Medical Practice. In *2nd Australian eHealth Informatics and Security Conference* pp. 29–38. Perth, Australia.

March, S. T. and G. F. Smith. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266.

Merriam-Webster. (2019). Definition of Program. Retrieved January 3, 2019, from https://www.merriam-webster.com/dictionary/program

Moulton, R. and R. S. Coles. (2003). Applying information security governance. *Computers & Security*, *22*(7), 580–584.

Pironti, J. P. (2010). Developing an Information Security and Risk Management Strategy. *ISACA Journal*, *2*(Security), 28–35. Retrieved from https://www.isaca.org/Journal/archives/2010/Volume-2/Pages/Developing-an-Information-Security-and-Risk-Management-Strategy1.aspx

Presidência do Conselho de Ministros. (2001). Resolução do Conselho de Ministros n.º 22/2001. Retrieved December 26, 2017, from https://www.anacom.pt/render.jsp?contentId=961538

PricewaterhouseCoopers. (2017). Strengthening digital society against cyber shocks: Key findings from the Global State of Information Security Survey 2018, 20. Retrieved from https://www.pwc.com/us/en/cybersecurity/information-security-survey.html

Querido, D. F. C. da S. (2014). *IT Governance in Public Administrations*. Instituto Superior Técnico de Lisboa. Retrieved from https://fenix.tecnico.ulisboa.pt/departamentos/dei/dissertacao/846778572210194

Reinert, K. A., R. S. Rajan, A. J. Glass and L. S. Davis. (2010). Corporate Governance. In *The Princeton encyclopedia of the world economy.* Vol. 1, pp. 227–232. Princeton, New Jersey: Princeton University Press.

de Sá-Soares, F. (2005). *Interpretação da Segurança de Sistemas de Informação Segundo a Teoria da Acção*. Universidade do Minho.

Secretaria Geral Ministério da Administração Interna. (2017). Eleições Autárquicas 2017, 1 outubro, Resultados, Portugal Continente e Regiões Autónomas, Território Nacional, Câmara Municipal. *Secretaria Geral Ministério Da Administração Interna*. Retrieved from https://www.eleicoes.mai.gov.pt/autarquicas2017/

Soares, D. (2009). *Interoperabilidade entre Sistemas de Informaçao na Administraçao Pública*. Universidade do Minho. Retrieved from http://repositorium.sdum.uminho.pt/handle/1822/10539

Soares, D., L. Amaral and L. Ferreira. (2017). Presença na Internet das Câmaras Municipais Portuguesas em 2016 : Estudo sobre Local e-Government em Portugal. Guimarães: Gávea – Observatório da Sociedade da Informação.

Sousa, M. R. de and A. S. de Matos. (2004). *Direito Administrativo Geral - Tomo I - Introdução e princípios fundamentais* 1a Edição. Lisboa: Dom Quixote.

Takeda, H., P. Veerkamp, T. Tomiyama and H. Yoshikawa. (1990). Modeling Design Processes. *AI Magazine*, *11*(4), 37–48.

Vaishnavi, V. and B. Kuechler. (2004). Design Science Research in Information Systems. Retrieved October 3, 2017, from http://www.desrist.org/design-research-in-information-systems/

Veiga, A. Da and J. H. P. Eloff. (2007). An Information Security Governance Framework. *Information Systems Management*, *24*, 361–372.

Verizon. (2017). 2017 Data Breach Investigations Report. *Verizon Business Journal*, (1), 1–48. www.doi.org/10.1017/CBO9781107415324.004

von Solms, S. H. and R. von Solms. (2009). *Information security governance*. NewYork, NY: Springer.

Ward, J. and J. O. E. Peppard. (2002). *Strategic Planning for Information Systems* 3rd ed. Chichester, West Sussex: John Wiley & Sons Ltd.

Zaydi, M. and B. Nasserddine. (2016). Information system security governance: Technology Intelligence perspective. In *Advanced Communication Systems and Information Security (ACOSIS), International Conference* pp. 1–6. IEEE.