The Role of the Chief Information Security Officer

Tiago Martins Catarino

Thesis to obtain the Master of Science Degree in

Information Systems and Computer Engineering

Supervisors: Prof. André Ferreira Ferrão Couto e Vasconcelos

Prof. Miguel Leitão Bignolas Mira da Silva

Examination Committee

Chairperson: Prof. Paolo Romano

Supervisor: Prof. André Ferreira Ferrão Couto e Vasconcelos

Member of the Committee: Prof. José Manuel Nunes Salvador Tribolet

May 2016

Acknowledgments

First and foremost, I would like to express my gratitude to my supervisor, Prof. André Vasconcelos, for all his valuable guidance and advice. He helped me greatly with all his support, dedication, wisdom and useful critiques.

Secondly, I wish to express my sincere appreciation to my co-supervisor, Prof. Miguel Mira da Silva, for his steadfast guidance and valuable advice.

Likewise, a special word of gratitude to all my family and close friends that supported me. Despite seeming irrelevant in the context of this work, this indirect help was a major contribution to this thesis.

A sincere thanks is due to Bruno Fragoso, Rodrigo Monteiro and Tiago Sampaio, who offered their time and advice in order to help enrich this work, thus making its path an easier and more interesting endeavor. This also extends to all my colleagues and friends at the INOV Digital Services Innovation research group, who were always helpful, available and open for any kind of discussion or advice.

Next, I would like to express my gratitude to all professionals of the government owned company, named DemoCorp in this work, which promptly hosted the demonstration. Their contributions remain anonymous in this dissertation, for confidentiality purposes.

Finally, I must express my very profound gratitude to my parents, Ana and Mário, and to my girlfriend, Inês, for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Resumo

O *COBIT 5 for Information Security*, que é baseado na framework COBIT 5, fornece uma orientação para os profissionais de segurança da informação, adicionando conteúdos específicos de segurança da informação, que inclui o *Chief Information Security Officer* (CISO). Além disso, eleva a Arquitetura Empresarial (AE) como área processual relevante, com o intuito de criar e manter os facilitadores de governação e gestão dos Sistemas de Informação.

A informação é um dos ativos mais importantes organizações, por isso a necessidade de protegê-la tem vindo a aumentar. Na verdade, a segurança da informação tem ganho cada vez mais importância nas organizações, o que eleva a importância do papel do CISO. Este papel é responsável pela segurança da informação das empresas em todas as suas formas. A eficácia e eficiência da segurança de informação poderão ser afetadas negativamente por uma implementação deficiente do CISO.

Para facilitar a implementação adequada do papel do CISO, propomos um método para implementar este papel nas organizações, utilizando o *COBIT 5 for Information Security* em *ArchiMate*. Tal método integra o *COBIT 5 for Information Security* com os princípios, métodos e modelos da AE, utilizando a notação *ArchiMate* para descrever a AE. O método é composto por 7 passos, que incluem a modelação do CISO (baseado no *COBIT 5 for Information Security*) e o desenho do *AS-IS* da organização em análise. Além disso, os passos incluem o mapeamento entre as funções de negócio, tipos de informação, outputs de processos e práticas-chave entre a organização e o *COBIT 5*, tendo em conta a implementação do CISO. O último passo do método tem como objetivo o desenho do *TO-BE* do papel do CISO, tendo em conta as decisões estratégicas tomadas pela organização.

Ao seguir o método, as empresas podem definir e implementar adequadamente o papel do CISO e otimizar o valor entregue pela segurança de informação. Este método permite às organizações, com base no *COBIT 5 for Information Security*, alinhar a migração para o *TO-BE* do papel do CISO, considerando as suas próprias especificidades e orientações estratégicas de nível maturidade a atingir.

Durante a investigação, nomeadamente na implementação da solução, foi possível identificar um conjunto de inconsistências entre as responsabilidades do CISO, tendo em conta a análise das matrizes de responsabilidades do *COBIT 5 Enabling Processes* e as responsabilidades listadas no *COBIT 5 for Information Security*. Estas inconsistências podem conduzir a uma incorreta implementação do papel do CISO nas organizações que desejam seguir a framework *COBIT 5*, levando a uma inefetiva governação dos Sistemas de Informação.

A solução proposta foi demonstrada numa empresa pública. Em relação à avaliação, a tese foi avaliada através de um caso real, a fim de aplicar o método proposto na prática.

Palavras-Chave: CISO, COBIT 5, information security, IT Governance, Enterprise Architecture, ArchiMate, design science research methodology.

Abstract

The COBIT 5 for Information Security, based on the COBIT 5 framework, provides guidance to information security professionals by adding information security-specific's contents, which includes the Chief Information Security Officer (CISO). Furthermore, raises the Enterprise Architecture (EA) as relevant procedural area, in order to create and maintain governance and management's enablers.

Information is one of the most important assets in organizations, so the need to protect it is increasing. Indeed, information security has gained more importance in the organizations, which leads to the CISO's role. Such role is responsible for the security of enterprise information in all its forms. Gaps in the implementation of the CISO's role may hinder the effectiveness and efficiency of information security.

To facilitate the achievement of an adequate implementation of CISO's role, we propose a method to implement this role in the organizations, using COBIT 5 for Information Security in ArchiMate. Such method integrates the COBIT 5 for Information Security with EA principles, methods and models, using the ArchiMate notation to describe the EA. The method comprises 7 steps, including the CISO's modeling (based on COBIT 5 for Information Security) and drawing of the organization's AS-IS under consideration. Additionally, the method's steps include the mapping between business functions, types of information, outputs processes and key practices of the organization and COBIT 5, taking into account the implementation of the CISO's role. The last step aims to design the CISO's role TO-BE, taking into account the strategic decisions taken by the organization.

By following the method, enterprises can define and implement properly the CISO's role and may optimize the value delivered by information security. This method allows organizations, based on the COBIT 5 for Information Security, to better cope with the desired CISO's role in the organization, considering their own specificities and strategic guidance maturity level to achieve.

During the investigation, in particularly when implementing the solution, it was possible to identify a particular set of inconsistencies between the roles' assignments, in particular the CISO, which are defined in the assignments matrix charts of COBIT 5 Enabling Processes, and the roles addressed by COBIT 5 for Information Security. These inconsistencies can lead to an incorrect role' implementation of the organizations that want to follow the COBIT 5 framework, leading to an ineffective information technology (IT) governance.

The solution proposal was demonstrated in a government owned company. Regarding the evaluation, the thesis was evaluated through a field study in order to apply the proposed method in practice.

Keywords: CISO, COBIT 5, information security, IT Governance, Enterprise Architecture, ArchiMate, design science research methodology.

Table of Contents

List of Figures

List of Tables

List of Acronyms

Acronym	Term
CISA	Certified Information Systems Auditor
CISO	Chief Information Security Officer
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
COBIT	Control Objectives for Information and related Technology
CSX	Cybersecurity Nexus
DS	Design Science
DSRM	Design Science Research Methodology
EA	Enterprise Architecture
ERM	Enterprise Risk Management
IS	Information System(s)
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISSC	Information Security Steering Committee
IT	Information Technology(ies)
ITIL	IT Infrastructure Library

Glossary

Term	Definition	Source(s)
Architecture	The structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution over time.	[33]
Artifact	Any designed object with an embedded solution to an understood research problem.	[10]
ArchiMate	An open and independent modeling language for enterprise architecture that is support by different tools vendors and consulting firms, providing instruments to enable enterprise architects to describe, analyze and visualize the relationships among business domains in an unambiguous way.	[14]
Chief Information Security Officer	Overall responsibility of the enterprise information security governance.	[6] [11]
COBIT 5	A complete, internationally accepted framework for governing and managing enterprise information and technology (IT) that supports enterprise executives and management in their definition and achievement of business goals and related IT goals.	[11] [21]
Constructs	Constructs provide the vocabulary and symbols used to define problems and solutions.	[10] [12]
Design Science	Creates and evaluates IT artifacts intended to solve identified organizational problems.	[10] [12]
Design Science Research Methodology	A methodological guideline for effective DS research.	[10] [12]

Enterprise	The highest level (typically) of description of an organization and typically covers all missions and functions. An enterprise will often span multiple organizations.	[33]
Enterprise Architecture	Discipline or process area that aims to establish and maintain a common architecture consisting of business process, information, data, application and technology layers for effectively and efficiently realizing enterprise and IT strategies by creating key models and practices that describe the baseline and target architecture.	[27] [28] [29] [33]
Framework	A structure for content or process that can be used as a tool to structure thinking, ensuring consistency and completeness.	[33]
Governance	Ensures that 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.	[11]
Governance of enterprise IT	A governance view that ensures that information and related technology support and enable the enterprise strategy and the achievement of enterprise objectives.	[11]
Information	An asset that, like other important business assets, is essential to an enterprise's business. It can exist in many forms: printed or written on paper, stored electronically, transmitted by post or electronically, shows on films, or spoken in conversation.	[11]
Information Security	Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability).	[6]
Information System	Interrelated components working together in order to collect, process, store and disseminate information to support decision making, coordination, control, analysis and visualization in an organization.	[34]
Information Technology	All the hardware and software technologies a firm needs to achieve its business objectives.	[34]

Management	Plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.	[11]
Methods	A set of steps used to perform a task – how-to knowledge.	[35]
Models	A set of propositions or statements expressing relationships between constructs.	[35]
Risk	The combination of the probability of an event and its consequence.	[11]
Stakeholder	An individual, team, or organization (or classes thereof) with interests in, or concerns relative to, the outcomes of the architecture. Different stakeholders with different roles will have different concerns.	[33]
View	The representation of a related set of concerns. A view is what is seen from a viewpoint. An architecture view may be represented by a model to demonstrate to stakeholders their areas of interest in the architecture.	[33]
Viewpoint	A definition of the perspective from which a view is taken. It is a specification of the conventions for constructing and using a view (often by means of an appropriate schema or template). A view is what you see; a viewpoint is where you are looking from — the vantage point or perspective that determines what you see.	[33]

1. Introduction

In the last years, information security has evolved from its traditional orientation focused mainly in technology to become part of the organization strategy, enhancing the need for an aligned business/information security policy [1] [2]. Information security is an important part of companies, since there is more information to protect which leads to better operational responses regarding security threats [3].

Companies and their information storage are more vulnerable to cyber-attacks and other threats [4]. These attacks are performed by criminals that want to steal vital information (e.g. intellectual property) from companies [4]. Many of these attacks are more sophisticated in order to steal confidential information. Therefore, companies that deal with sensible information should be prepared for these threats, because information is one of the business' most valuable assets and having the right information at the right time can lead to more profitability. Companies are increasingly recognizing information and related technologies as critical business assets, which need to be governed and managed in an effective way [5].

Information and technology have become a key resource for all enterprises [6], being increasingly more significant in every aspect of business and public life. The need to reduce information risk is constantly intensifying. Such mitigation includes the protection of information and IT related assets from threats [6].

Information security has an important role in day-to-day operations in order to protect the information, which is one of organization's most important assets [7]. Information security is a business enabler, which is strictly connected to stakeholder reliability, either by addressing business risk or by creating value for enterprises, being a competitive advantage [6]. Moreover, security plays a key role in a company's daily operations, since the integrity and confidentiality of their information must be ensured and available to those who need it [7].

Nowadays, cybercriminals are becoming more sophisticated and collaborative with every coming year. To combat these threat, information security professionals should understand these five trends [8]:

- The unintended consequences of state intervention;
- Big data will lead to big problems;
- Mobile applications and the Internet of Things (IoT);
- Cybercrime causes the perfect threat storm;
- Skills gap become an abyss for information security.

In order to tackle the threats and solutions becomes essential for the organizations to have well-skilled information security professionals. Many smaller enterprises cannot justify the creation of a single post, or indeed an information security team dedicated to its management. These enterprises, in particular those with no external compliance requirements, will often use a general operational or financial team

to house the main information security blueprint which can cover the technical as well as the physical and the personnel-related security, which works quite successfully in many ways [9].

Nonetheless, companies should have a single person (or team) responsible for information security, depending on its maturity level, during the control of information security policies and management. This leads the Chief Information Security Officer (CISO) to take a central role in the organizations, since not having someone accountable for information security, greater are the chances for a major security incident to may happen. Furthermore, CISO is expected to have a 360-degree view of the enterprise's information security risks and put in place a set of necessary technologies and processes/activities to soften and minimize the risks [9].

Some industries place some greater requirements on this than others, but once a company get to a certain size the requirement for a dedicated information security officer become too considerable to avoid. Indeed, without one can only ever result in a higher risk of data loss, external attacks and inefficient response plans. Moreover, organization's risk is not proportional to its size, so small companies may not have the same global footprint as large organizations. However, small and mid-sized companies are facing nearly the same risks [9].

COBIT 5 for Information Security is a professional guide that helps companies to define information security functions. This guide is part of COBIT 5's framework [11], focusses on information security and can be instrumental in providing guidance for information security professionals, which includes the CISO's role [6]. Furthermore, it explains each component from an information security perspective and contains guidance on drivers and benefits, principles for information security perspective, enablers for support and alignment with standards [6].

Taking that into account, we propose a method based on accepted standards and frameworks to support companies to implement the CISO's role in order to have the right person with proper skills to govern the enterprise information security.

In this thesis, Section 2 presents the research methodology applied across this master thesis, where a research proposal is developed to solve a problem.

Afterwards, in Section 3, we formulate the research problem, where we explain the issues regarding the implementation of the CISO's role defined in COBIT 5 for Information Security.

Section 4 presents the related work that focusses on three main concepts, which are the CISO, COBIT 5 and EA.

The method to implement the CISO's role and the inconsistencies between the RACI (Responsible, Accountable, Consulted and Informed) charts defined in COBIT 5 Enabling Processes and the enablers' content defined in the COBIT 5 for Information Security and, also, the consequences of these inconsistencies for organizations that want to use the COBIT 5 to define the CISO role are described in Section 5.

Section 6 describes the demonstration of the proposed solution in an organization, named DemoCorp.

The evaluation and communication of this master thesis are addressed in Sections 7 and 8.

Finally, in Section 9 we synthesize the conclusions and future work to be developed, in order to address the problems detected in this research.

2. Research Methodology

The research methodology applied across this master thesis is Design Science Research Methodology (DSRM) [10] [12] [13], where a research proposal is developed to solve a problem [12]. This methodology is an iterative process and incorporates principles, practices, procedures and a process model, which are adequate to conduct Design Science (DS) research in information systems research. The process model provides DS research with a complete methodology [10] [13] and includes a process iteration path, which allows for cycling between activities. The goal of this methodology is to overcome research paradigms, such as descriptive and interpretative research, in which the outputs are most explanatory and, one could argue, are often not applicable to the solution of problems encountered in practice [10].

Note that DSRM process model has six activities (see Figure 1): problem identification and motivation, definition of objectives for a solution, design and development, evaluation, and communication.

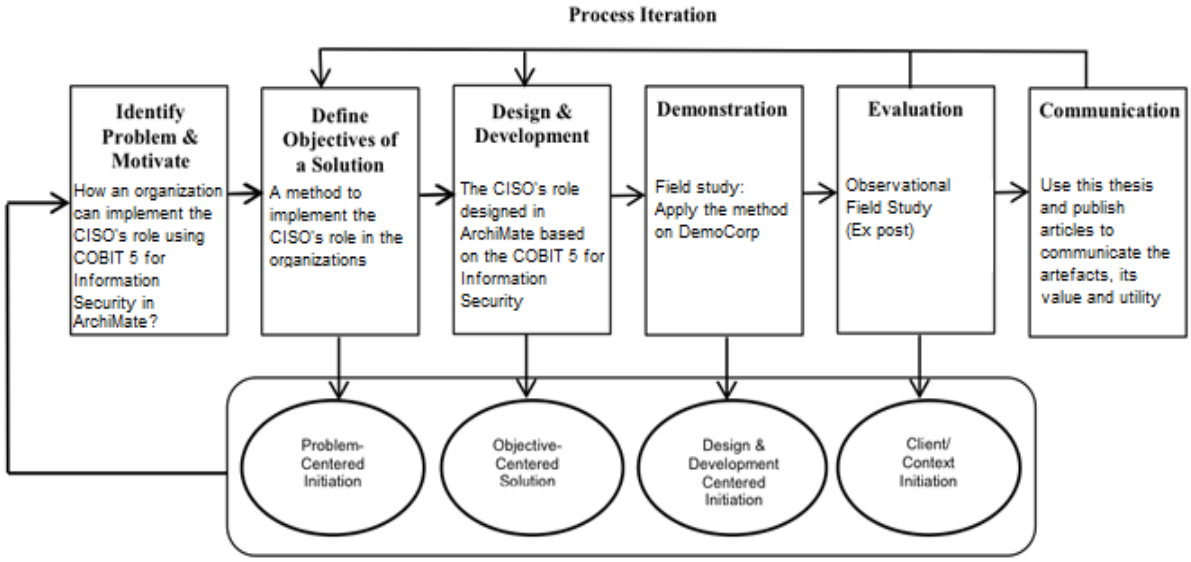


Figure 1 – The DSRM Process Model [1]

Information systems (IS) is an applied research discipline, where researchers frequently apply theory from other disciplines, such as economics, computer science, and the social sciences, among others, in order to solve problems at the intersection of information technology (IT) and organizations [10]. Several researchers have succeeded in the integration of design as a major component of research, in order to solve relevant organization problems [10].

To solve these organizational problems, DSRM proposes the design and development, followed by a demonstration and evaluation of artifacts, which may include models (abstractions and representations), methods (algorithms and practices), constructs (vocabulary and symbols) and instantiations (implemented and prototype systems) [13]. In this thesis, the artefacts will be designed and evaluated by their own intrinsic value, effectiveness in a specific context, in order to achieve the master thesis goal: the creation of a definitive solution to integrate the frameworks for information security and the

organizations, in order to implement the CISO's role using COBIT 5 for Information Security in ArchiMate.

This methodology can prove to be useful throughout this research, because it forces to do research in an iterative way, in order to obtain frequent and valuable feedback for the design process and incremental improvement of it. With this methodology, we hope from this research to achieve more valuable outcomes.

To be coherent with our research work, this dissertation will follow the same structure as DSRM which phases are easily mapped to the structure of this document.

Section 3 (Research Problem) and Section 4 (Related Work) identify the problem and the motivation behind the research work. Section 5 (Proposal) details the objectives of the solution and the proposed solution. The solution is demonstrated in Section 6 (Demonstration) through and evaluated in Section 7 (Evaluation). In Section 8 (Communication) and Section 9 (Conclusion) the research work is concluded with research communication, contributions, limitations and future work.

3. Research Problem

This section describes the “Identify Problem & Motivate” step of the DSRM Process Model and has the objective to describe the research problem and to justify the value of a solution. In addition to that, we will define the specific research problem that will be addressed in the dissertation work.

The information security guide helps security and IT professionals to understand, use, implement and direct important information security activities [6]. With this guidance, security and IT professionals can make more informed decisions, which can lead to create more value to enterprises [6].

In particular, COBIT 5 for Information Security recommends a set of processes that are instrumental in guiding the CISO’s role and examples of information types that are common in an information security governance and management context. Furthermore, it provides a list of desirable characteristics for each information security professional [6].

However, despite COBIT 5 for Information Security [6] seems to tackle most of relevant processes and roles to address the organizational needs, but it does not provide a specific approach. Such approach would help to bridge the gap between the desired performance of the CISO and its current role, increasing its effectiveness and completeness, hence the maturity of information security in the organization.

Moreover, this framework does not provide any viewpoint that helps the enterprises to implement the role of the CISO in their companies, such as what the CISO must do based on COBIT processes. Note that this framework provides a “thinking approach and structure”, so we have to keep critical when using the material to ensure smart use of COBIT.

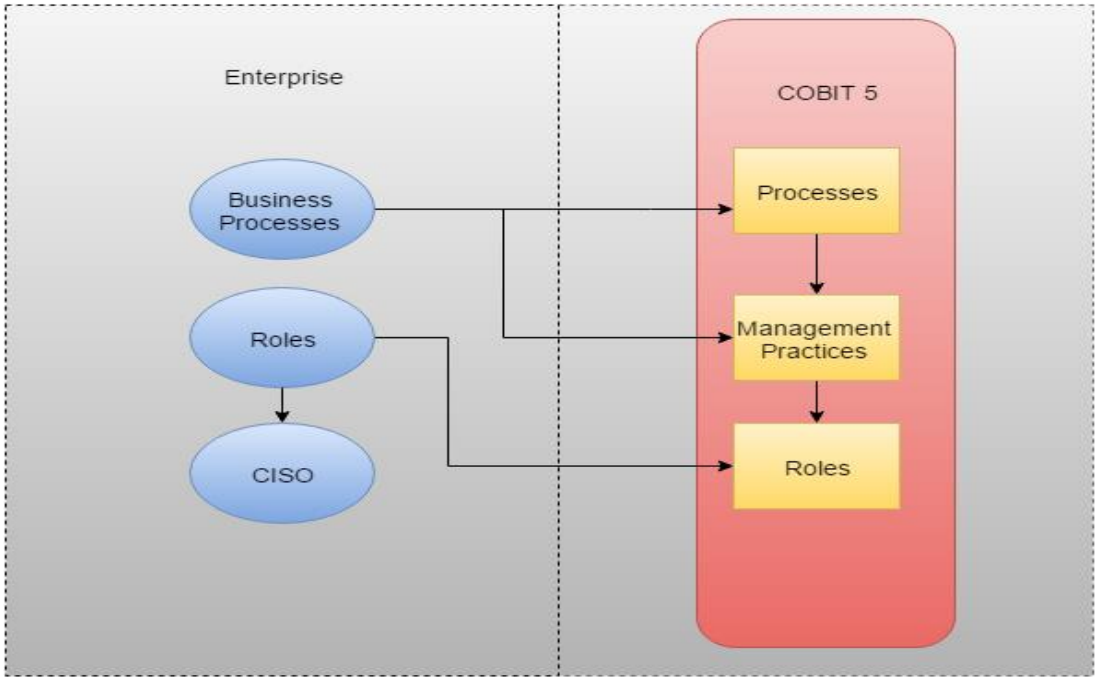


Figure 2 – The non-integration issue of enterprises to COBIT 5

Furthermore, every company has different processes, organization structures or services provided. CISO's role is still too organization-specific, so it can be difficult to apply a framework to one particularly company.

This difficulty happens because it is complicated to align companies' processes, structures, goals or drivers to good practices of the frameworks that are based on processes, organization structures or goals. The mapping of the framework's processes and the organization's business processes is among the many challenges when we try to make an assessment of maturity level on the enterprise processes.

Even COBIT 5 having all the roles well define and a RACI charts for each process, companies have different roles and levels of involvement [6], as we can see in Figure 2, where it is possible to observe the non-integration issue of enterprises' processes and roles to COBIT 5.

ArchiMate is the standard notation for the graphical modeling of EA. Many companies recognize the value of these architectural models in understanding the dependencies between their people, processes, applications, data and hardware. Using ArchiMate allows them to integrate their business and IT strategies.

The challenge to address is how an organization can implement the CISO's role using COBIT 5 for Information Security in ArchiMate. A challenge that, by itself, raises other relevant questions regarding its implementations, such as:

- Can we perform a gap analysis between the organization's AS-IS to what is defined in the COBIT 5 for Information Security, regarding:
    - Processes and base practices;
    - Key practices;
    - Information types;
    - Roles.
- Can the ArchiMate notation model all the concepts defined in the COBIT 5 for Information Security?
- Can we identify inconsistencies between the RACI charts, defined in COBIT 5 Enabling Processes, and the CISO's role addressed by COBIT 5 for Information Security?

Therefore, it is important to make clear for the organization the role and associated processes (and activities), information security's functions, key practices and information's types where the CISO is included/ part of, in order to have the right person with proper skills to govern the enterprise information security. For that, ArchiMate architecture modeling language [14], an Open Group standard, provides support to the description, analysis and visualization of inter-related architectures within and across business domains in order to address stakeholders' needs [5].

4. Related Work

We begin our analysis of related work in a systematic way, by first trying to establish the search space boundaries. This section contains all the concepts related with this master thesis and descriptions of the most important elements, such as CISO, COBIT 5 and EA. These concepts can be visualized in the conceptual map shown below (see Figure 3).

In the beginning, we will present some information about the CISO, COBIT 5 and how this framework can improve the job of information security professionals. Also, will be shown the existing solutions through the approach of the research carried out in recent years about this role.

In the end of this section, we will present some information about EA and the ArchiMate notation.

The information in these sections was extracted from scientific articles, technical books and master thesis published in the previous years. With the use of these contents, it is possible to connect and relate all the subjects that will be handled.

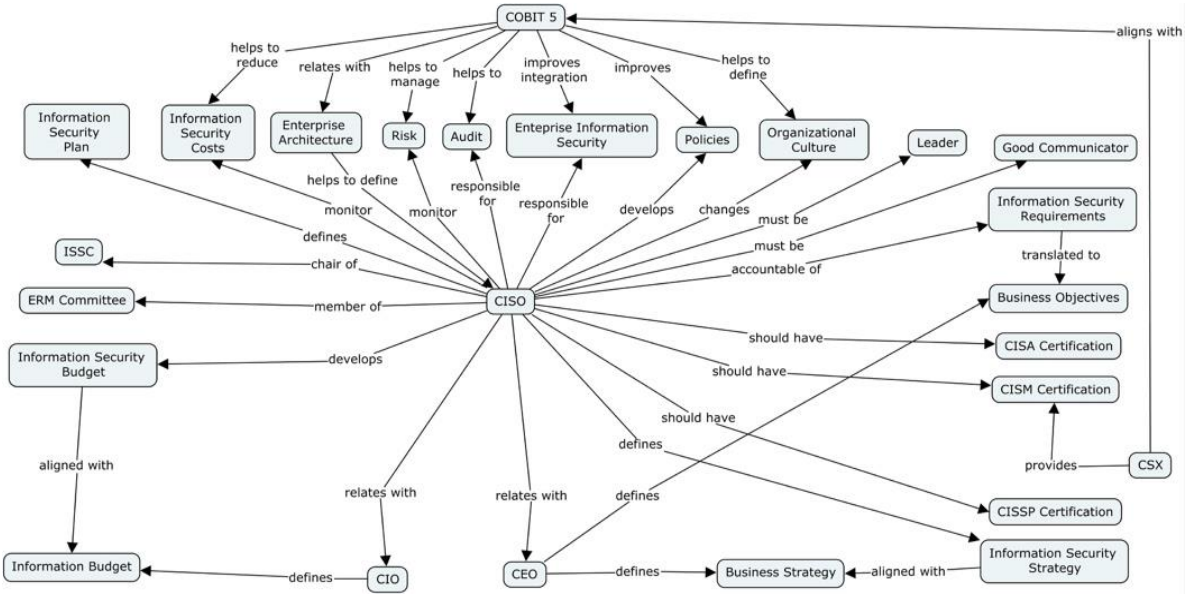


Figure 3 - Conceptual map

4.1. Chief Information Security Officer

The CISO is responsible for risk management, security operations, physical security and balancing business and security objectives [3]. Moreover, he/she is part of Information Security Leadership, which includes [6]:

- Executive management;
- Business management;
- CISO/Information Security Manager (ISM).

The CISO is the senior-level executive within an enterprise and has the responsibility to establish and maintain the enterprise vision, strategy and program in order to ensure that technologies and information assets are protected from unauthorized users [3].

Reducing information and IT risks is one of the role's goals. CISO must direct staff in order to improve the risk management. These staff have the responsibility to identify, develop, implement and maintain all the processes related with information security [3].

The CISO is also part of key information security decision-making entities, which includes [6]:

- CISO;
- Information Security Steering Committee (ISSC);
- ISM;
- Enterprise Risk Management;
- Business owners.

In the past, CISOs' role was only focused on defining technical standards and security policies, validating security controls and assuring the protection of customers' personal data [3].

Nowadays organizations realize that cyber risk is intimately linked to their innovation and growth strategies, so the expectations of CISOs are always changing [3]. The CISO's role includes a new set of skills, such as leadership that involves good communication skills in order to communicate with the management board and managers in all divisions, work with business and up and down the organization. This relationship between CISO and the business is important to enable growth and innovation [15].

The CISO has the primary responsibility of coordinating the confidentiality, integrity and availability of information resources at the enterprise. Another important skill that CISOs must have is translating problems and solutions to a language that business people can understand, which includes Chief Executive Officer (CEO), Chief Information Officer (CIO), business executives and others [15]. This is a key skill, because the CISO must build relationships with all business partners for supporting the mission and vision of the business [15]. In addition, the CISOs must educate their employees in order to implement a new information security culture that is accepted by all [15].

On one hand, the CISOs must include risk as a more central part of their role and understand business priorities in order to take risks to meet business objectives [16].

On the other hand, the CISOs must be aware of the behavior of their employees in order to make sure that information cannot be taken out of the organization [16]. It is also important to make sure that the access to specific information is limited only to those who need it and identify which attackers would be interested in specific organization information's data and what data they are likely to target [7]. Moreover, it is important to know how long it takes to detect a data breach and to stop it, as well as what will be the business impact if a data breach were to occur [15].

The CISOs relates most with CEO and CIO. CISOs must understand what the real risks are and how the business can be affected by them [15]. These relations are very important because business cannot

be separated from security needs, so it is necessary to link business requirements with security requirements, and also business risks with security vulnerabilities and risks [15].

CIOs and CEOs expect that the activities performed by CISOs' departments contribute to the release of new company products, reduce ongoing cost and increase user satisfaction by reducing the waiting time necessary to access the organization's systems [15]. CEOs and CIOs have different interests on the job of the CISO.

CEOs expect that government regulatory compliance requirements are being satisfied and if the audit issues are being reduced every year. Nonetheless, CIOs expect that the security area works side-by-side with the other IT management areas [15].

The CEO is the person that decides how much risk the enterprise will handle, so the CISO should suggest multiple cost and/or risk alternatives. Furthermore, CISO's role is to inform and not to decide, however, they have the possibility to influence a decision when it appears that the organization is taking an excessive risk posture [15].

4.1.1. CISOs challenges

New CISOs may face common challenges, such as [3] [17] [18]:

- Inadequate required skill-set;
- Demonstrate the value of information security and good risk management in financial terms to business;
- Lack of resources and effective team structure;
- Ineffective communications/reporting among stakeholders and throughout the organization;
- Inadequate governance, which includes overall strategy and processes;
- Lack of support or trust from executive management and/or stakeholders;
- Insufficient funding;
- Organizational cultures which act as barriers to the introduction of CISOs.

Additionally, CISOs may face potential security breaches caused by social media. According to a survey commissioned by SunGard Availability Services, IT professionals see security as a serious threat to the organization, due to employee behavior [19]. Leaving the company's laptop in the car, sharing passwords, using weak or lazy passwords and ignoring company security programs, are examples of issues that can lead to the type of data breach that could cost a CISO his or her job [19].

4.1.2. CISOs benefits

Although new CISOs may face challenges in the organizations, they are vital for the success of the companies. Companies that have a CISO derive more value from their information assets, according to the research conducted by IT Policy Compliance Group [20]. So, what are the benefits of having this role implemented?

In the following lines, we list some examples of benefits on having this position implemented [20]:

- Higher customer retention, revenue or profit;
- Reduced financial exposure from data loss;
- Customer data theft or loss lower rates;
- Business productivity related to IT assets with higher levels;
- Lower costs for audits.

4.2. COBIT 5

In this sub-section we will present the COBIT 5 framework [11] and one solution that is adopted by many enterprises that want to implement or maintain the CISO's role. This solution is the COBIT 5 for Information Security and this is a professional guide for information security professionals and other interested parties [6].

4.2.1. COBIT 5 Framework

The COBIT 5 [11] is a framework that includes extensive guidance on enablers for the management and governance of enterprise IT.

This framework is a set of good practices focused on the management and governance of IT [11]. It was released in April 2012 by the Information Systems Audit and Control Association (ISACA) [11]. This framework indicates that governance processes will provide direction to management processes based on business needs and, the governance processes will get feedback from management processes in order to evaluate the directions that are carried out and/or whether adjustments are necessary [21].

COBIT 5 integrates other major frameworks, standards and resources, such as Information Technology Infrastructure Library (ITIL) and related standards from the International Organization for Standardization (ISO) [11].

According to the results from ISACA's 2016 Global COBIT Survey, more than 3 in 4 survey respondents indicate that COBIT 5 helps them address practical business issues beyond governance of enterprise IT. Moreover, was concluded that COBIT 5 leverages proven practices and global thought leadership to enable enterprises of all sizes to enhance stakeholder value [36].

COBIT 5 helps companies of all sizes, whether commercial, not-for-profit or in public sector. Key COBIT 5 users include company executives and consultants in the following domains: Audit and Assurance, Compliance, IT Operations, Governance, Security and Risk Management.

Figure 4 presents the role of COBIT 5 as the umbrella framework that defines the conceptual spectrum of the governance of enterprise IT. For example, ITIL V3 covers just under 30 percent and ISO/IEC 27001 covers just under 15 percent of the governance of enterprise IT [37].

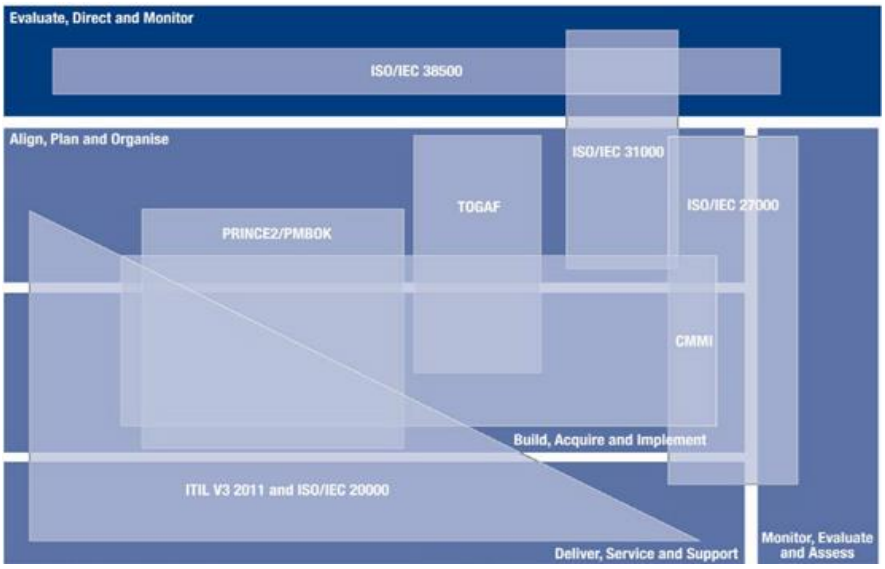


Figure 4 – COBIT 5 Coverage of Other Standards and Frameworks [37]

In this framework, governance and management are separated in different areas. The management processes are categorized by IT life cycle, consisting of four different areas: Align, Plan and Organize (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); and Monitor, Evaluate and Assess (MEA). All these areas contain different processes and some of these areas (APO and MEA) are dedicated to the governance processes that include different IT governance activities [21].

The research's focus is information security, so the guide COBIT 5 for Information Security can be followed. This guide has many enterprise benefits, such as [6]:

1. Reducing complexity and increase cost-effectiveness. This is reached by the improved and easier integration of information security standards along with the following of good practices;
2. Increasing user satisfaction. This is reached by the information security outcomes;
3. Reducing impact by reducing information security incidents;
4. Improving integration in the enterprise information security;
5. Information security function improve management of costs.

Information Security

ISACA defines information security as something that "Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability)" [6].

In other sources, it is described as the practices used to defend information from unauthorized access, use, recording, modification, disclosure, disruption or destruction in order to provide confidentiality, integrity and availability [7].

Information security is an important concept to the research because the CISOs have the overall responsibility of the enterprise information security governance.

Risk Management

Risk management is more than to justify and respond to risk [22]. Risk management enables the identification, assessment, and prioritization of risks (ISO 31000). To minimize, monitor and control the probability of occurring certain events, the use of resources should be coordinated, economical, and convenient applied. Moreover, information risk management ensures that information risk is managed and coordinated to comply with Enterprise Risk Management directives [23] [24].

One of the governance objectives is the risk optimization, so all enterprises should perform an adequate risk management in order to avoid pitfalls and unwanted surprises. If the enterprises adopt risk management, it is possible to achieve their objectives, maintain the cost at a lower level and create value to their stakeholders [23] [24].

This concept is relevant to the research because the CISOs are responsible for risk management and the COBIT 5 framework has processes to manage risk and ensure risk optimization, which the CISO is responsible for.

Organizational Culture

Organizational Culture is one of the COBIT 5's enablers and is very important to the implementation of the CISO role [21].

CISOs have the responsibility to influence and improve the organizational culture in order to support the information security [25].

One of the challenges of this role is to change the behavior of the employees. The employees usually do not accept the information security message, which can lead to the loss of control of information. This problem can be solved if there are key resources that should be available to the CISO, such as expertise, credibility, political access to management board and control sanctions and prizes [25].

The CISO needs to be visible and heard in order to improve the organizational culture [25]. Moreover, it is mandatory to use two-way communication with employees in order to reduce the distance between them and improve effectiveness and engaging them in security initiatives with the aim of improving their behavior [25]. With this behavior change, employees would understand the information security and take actions that could help to protect the organization data.

4.2.2. COBIT 5 for Information Security

COBIT 5 for Information Security is a COBIT 5 Professional Guide for information security professionals and all parties interested of the enterprise.

This framework can lead to the full end-to-end business and IT functional responsibilities of information security. It is based also on five principles [6]:

- Principle 1: Meeting Stakeholder Needs;
- Principle 2: Covering the Enterprise End-to-end;
- Principle 3: Applying a Single, Integrated Framework;
- Principle 4: Enabling a Holistic Approach;
- Principle 5: Separate Governance from Management.

The fourth principle leads to a definition of enablers (see Figure 5) that supports the governance and management system for enterprise IT and information. These set of enablers are key factors to the success and can influence individually, or collectively, the management and governance of information security [6].

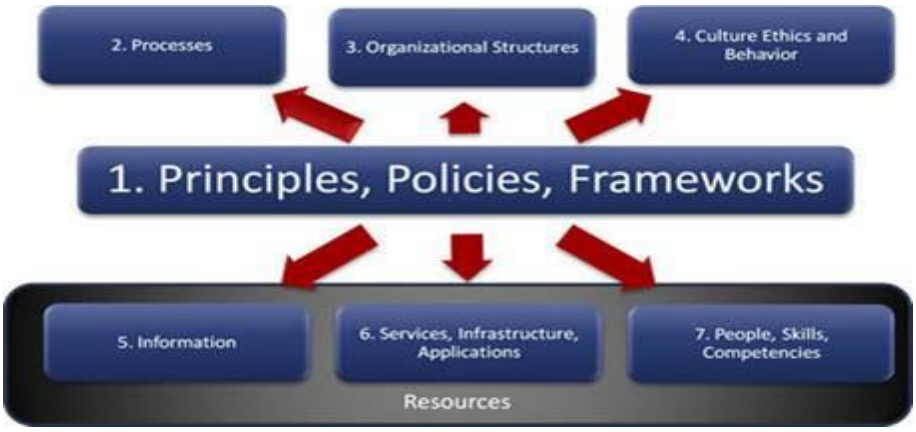


Figure 5 - COBIT 5 for Information Security Enablers [6]

COBIT 5 for Information Security [6], within a typical enterprise defines, the information security roles and structures listed below as:

- Chief Information Security Officer (CISO): overall responsibility of the enterprise information security program;
- Information Security Steering Committee (ISSC): ensuring through monitoring and review that good practices in information security are applied effectively and consistent throughout the organization;
- Information Security Manager (ISM): overall responsibility for the management of information security efforts.

However, when looking to relevant and related literature regarding information security, such definition of information security roles was not so clear.

For instance, ISO/IEC 27001 and ISO/IEC 27002 add information about the organization of information security but do not defines information security roles [38] [39].

On the other hand, the PCI (Payment Card Industry) standard defines the CISO's role as the senior-level executive within an organization responsible for establishing and maintaining programs to ensure information assets are adequately protected. Moreover, defines the Security Manager as the role designated with the overall responsibility for physical security for the card production facility [40].

Moreover, the Governing for Enterprise Security (GES) guide defines the responsibilities of the CISO, although the term Chief Security Officer (CSO) encompasses the CISO, i.e., this guide only lists the responsibilities of the CSO [41].

Therefore, under the scope of this thesis, the roles definition in COBIT 5 will be considered.

Principles, policies and frameworks are a set of communication mechanisms to transmit the instructions and directions of the management and governance bodies [6].

The CISO leads the ISSC, so the policy framework and related policies are attributed to him/her [6]. Policy framework includes information security principles, policy, specific information security policies, information security procedures and information security requirements and documentation [6].

Another important enabler are organizational structures. The CISO is part of the organizational structure and has the overall responsibility of the enterprise information security governance [6].

Yet another key enabler is the Culture, Ethics and Behavior. The behavior of the employees determines the success of the companies, so the CISOs must be aware of the behavior of their teams in order to influence the enterprise culture [6].

Indeed, the organization culture is closely related with members' behavior of the company collectively. The CISO must measure the behavior of the employees over time, so it can be possible to have an adequate view of the information security culture. This measure can be made with the determination of the strength of passwords, swipe card use, and number of laptop locks distributed and used by employees and others.

Furthermore, the CISO is part of the information security management that is at the information security level. One of the jobs that is required for this role is to influence the behavior through communication, rules, norms, incentive or rewards [6].

The information enabler is also very important to the success of the companies. There are a lot of information types that are usual in information security management and governance context.

As stated in Table 1, COBIT 5 for Information Security establishes the relation between the information types and the CISO. The table's goal is to show what the information types are (e.g. information security strategy) that the CISO has to approve, create, be informed of or use.

The caption of the content of next table is:

- A – Approver;
- O – Originator;
- I – Informed of information type;
- U – User of information type.

Table 1 - CISO vs. Information Type [6]

	Information Type									
	Information Security Strategy	Information Security Budget	Information Security Plan	Policies	Information Security Requirements	Awareness Material	Information Security Review Reports	Information Security Service Catalogue	Information Risk Profile	Information Security Dashboard
CISO	O	U	O	O	A	A	A	A	U	U

The People, Skills and Competencies enabler indicates that different information security stakeholders require distinct skill sets [6]. In the case of the CISO, it is very important to have the Certified Information Security Manager (CISM) certification because the CISO is responsible for the information security strategy formulation, which defines and implements the information security goals, vision and mission that should be aligned to the enterprise culture and strategy [6]. Furthermore, CISOs should have other certifications, like Certified Information Systems Auditor (CISA) and CISSP (Certified Information System Security Professional) [6].

The CISO is also the ISSC chair and the connection to Enterprise Risk Management (ERM) committee. ISSC is committee responsible for information security decisions of the whole enterprise [6]. Additionally, the CISO can be a member of the ERM committee in order to provide the committee with advice when the subject is specific information risk [6]. ERM is a committee responsible for all the decision making of the whole enterprise [6]. Such decision-making is relative to assess, control, optimization, finance and monitor risk from all sources in order to increase the value of the enterprise to its stakeholders.

The enablers described before may lead to many challenges when the companies try to implement them. Information security professionals have to define the enterprise information security requirements based on: business plan and strategic intentions, management style, information risk profile and risk appetite[1] [6].

Information Security is important and valuable to an enterprise only when it is sufficiently adapted in order to be aligned with all enterprise operations [6].

The CISO is a key information security decision-making entity. In the following lines, we list the desirable characteristics in a CISO [6]:

[1] Level of risk that an enterprise is prepared to accept, before considering any action necessary to reduce it.

- **Mandate**: has the overall responsibility of the enterprise information security program.
- **Operating principles**: in different kind of situations, the CISO may report to the senior executive management. The connection between executive management and the information security program is made by the CISO. The CISO also needs to communicate and co-ordinate directly with key business stakeholders in order to address needs of information protection. Also, must properly understand the business strategic vision, be a good communicator, build effective relationships with business leaders and be able to translate business objectives to information security requirements.
- **Span of control**: has the responsibility of establishing and maintaining an information security management system (ISMS), defining and maintaining an information security risk treatment plan and also monitoring and reviewing the ISMS.
- **Authority level/decision rights**: responsible for maintaining and implementing the information security strategy. The sign-off of important decisions resides in the function to which the CISO may report that can be a senior executive management team member or the ISSC.
- **Delegation rights**: should delegate tasks to information security managers and business people.
- **Escalation path**: always must escalate key information risk-related issue to the person that is above in the hierarchy (direct supervisor and the ISSC).

CISO is part of an organizational structure, so needs to make informed decisions. It is necessary that an organization structure requires input (such as information) in order to make these decisions (see Table 2).

Table 2 – CISO's Inputs and Outputs [6]

Input	***From***	***Output***	***To***
Risk tolerance	ERM	Information security strategy	ERM committee
Regulatory/compliance mandates	External	Policies, standards, procedures	Enterprise
Business and IT strategy	Organization/IT	Remediation plan to audit recommendations	Audit
Audit reports	Audit	----------	---------

As state in Table 3, we present the high-level RACI chart of the CISO:

Table 3 - High-level RACI Chart of the CISO role [6]

Process Practice	***Level of Involvement (RACI)***
Identify and communicate information security threats, desirable behaviors and changes needed to address these points.	Accountable
Ensure that environmental and facilities management adheres to information security requirements.	Accountable
Protect against malware.	Accountable
Manage network and connectivity security.	Accountable
Manage endpoint security.	Accountable
Manage user identify and logical access.	Accountable
Manage physical access to IT assets.	Accountable
Monitor the infrastructure for security-related events.	Accountable
Provide ways to improve efficiency and effectiveness of the information security functions.	Accountable
Monitor IT risk management.	Responsible
Define and communicate an information security strategy that is in line with the business strategy.	Responsible
Research, define and document information security requirements.	Responsible
Validate information security requirements with stakeholders, business sponsors and technical implementation personnel.	Responsible
Develop information security policies and procedures.	Responsible
Define and implement risk evaluation and response strategies and co-operate with the risk office to manage the information risk.	Responsible
Ensure that potential impact of changes is assessed.	Responsible
Collect and analyze performance and compliance data relating to information security risk management.	Responsible

Limitations of COBIT 5 for Information Security

There are some limitations that influence the implementation of CISO, such as:

- All the framework is extremely focused on IT industry;
- Does not get into any of the technical details, for example the process “Manage Data” in DSS area, which covers everything like backup procedures and mechanisms, capacity management or file system naming. If any enterprise wants to dig into more specific technical details, other tools will be necessary;
- Lack of implementation guidance, because COBIT 5 for Information Security needs to be customized to specific environment, but it does not provide concrete guidelines or methods in order to facilitate the accomplishment of the enterprises;
- Does not provide any diagrams that help to implement in a correct way an information security role (e.g. business process viewpoints);
- Inconsistencies between the RACI charts defined in the COBIT 5 Enabling Processes [21] and the information security-specific roles responsible for producing and/or originating information types, processes’ outputs and information’s outputs [42].

Cybersecurity Nexus

As information security professionals, their skills are evolving, business needs are changing, and standards are rising and with them a new challenge to face: cybersecurity [26].

Cybersecurity Nexus (CSX) is a security knowledge platform and professional program from ISACA, which is focused on cybersecurity. CSX was created for people that manage security of information. This platform shapes the cybersecurity profession, providing new skills for information security professionals [26]. However, what is the relationship between COBIT 5 for Information Security and CSX?

The COBIT 5 for Information Security is a set of good practices that can fit in the knowledge areas/capabilities, which the CISO must have to perform his/her role.

CSX provides training and certifications to professionals, such as CISO. At the end of the CSX roadmap is the professional certification CISM, which is recognition not only of knowledge of the subjects but also, the continuing experience and training [26].

4.3. Enterprise Architecture

An architecture is the fundamental organization of a system embodied in its components, the relationships between them and the environment, as well as the principles guiding its design and evolution [27].

An architecture at the level of an entire organization is called enterprise architecture (EA) [28] [29]. EA is a coherent whole of principles, methods, and models that are used in the design and realization of an enterprise's organization structure, business processes, information systems and infrastructure [27].

The EA process creates transparency, delivers information as a basis for control and decision-making, and enables IT governance [28]. Every organization wants to do the right things at a minimal risk in order to reduce costs and improve benefits. EA supports IT management in order for companies to meet these goals [27].

EA, as we can see, is important to the companies, but what are its goals? The answer is simple: understanding the organization; developing systems, products and services according to business goals; optimizing operations; optimizing organizational resources, including their people and providing alignment between all the layers of the organization: business, data, application and technology [27].

Moreover, EA can be related to a number of well-known best practices and standards [27]. As stated in Table 4, we present the management areas relevant to EA and the relation between EA and some well-known management practices on each area.

Table 4 - EA Management Areas vs Management Practices [27]

Strategic Execution	EFQM
Quality Management	ISO 9001
IT Governance	COBIT 5
IT delivery and support	ITIL
IT implementation	CMM and CMMI

EA assures or creates the necessary tools to promote alignment between the organizational structures involved in the AS-IS process and the TO-BE desired. For that, it is necessary to tailor the existent tools in order to EA can provide a value asset for the organizations.

In this thesis, we will only focus on the ArchiMate with the Business Layer and Motivation, Migration & Implementation extensions that are described in the following sub-section.

4.3.1. ArchiMate

ArchiMate is an open and independent EA modeling language, which is part of the Open Group. This modeling language provides instruments to enable architects to describe, analyze and visualize the relationships among business domains [14] [30].

Further, it provides a graphical language of EA over time (not static), as well as their motivation and rationale. As stated in Figure 6, ArchiMate is divided in 3 layers [14]:

- Business layer: provides services (through products) to customers (external);
- Application layer: provides application services to the business layer;
- Technology layer: provides infrastructure services to the application level.

These three layers share a similar overall structure because the concepts and relationships of each layer are the same but they have different granularity and nature. Every entity in each level is categorized according to three aspects: information, structure and behavior [22].

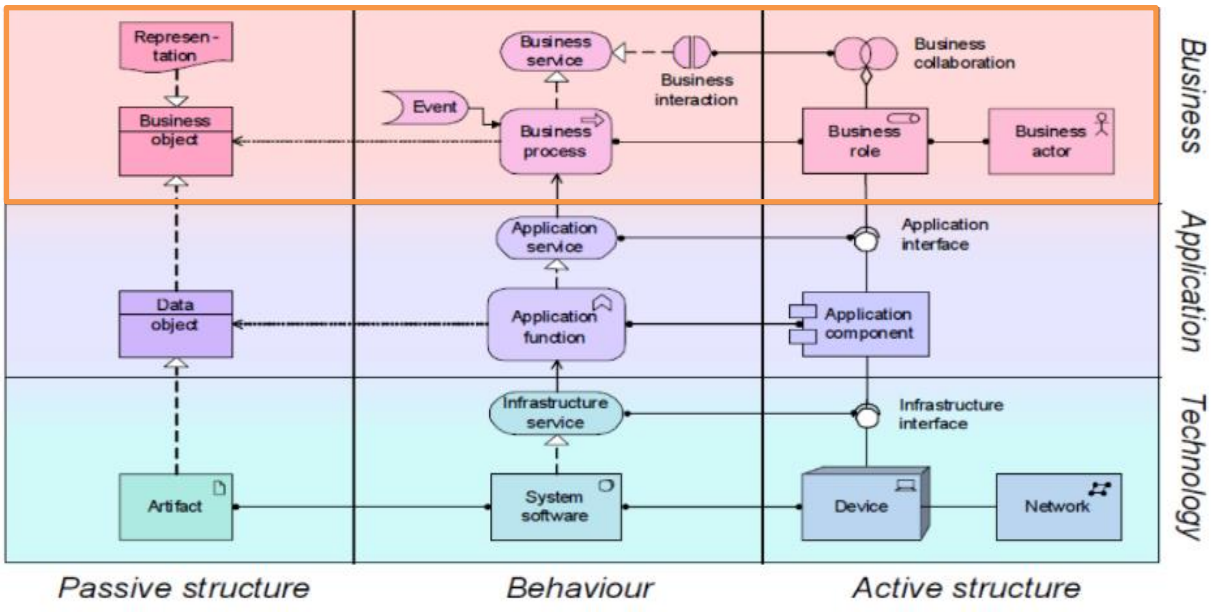


Figure 6 - ArchiMate Layers [14]

ArchiMate is a good alternative compared to the others modeling languages (e.g. UML), because it is more understandable, less complex and does support the integration between Business, Application and Technology layers through various viewpoints [22].

The Business Layer, which is part of the framework provided by ArchiMate, it is where our problem is address, as can be seen in Figure 6. Regarding the problem's formulation in the previous section, the Business Layer Metamodel can be the starting point to provide a first scope of the problem to address. However, only a subset of the Business Layer Metamodel should be optimized (see Figure 7) in order to address the research problem.

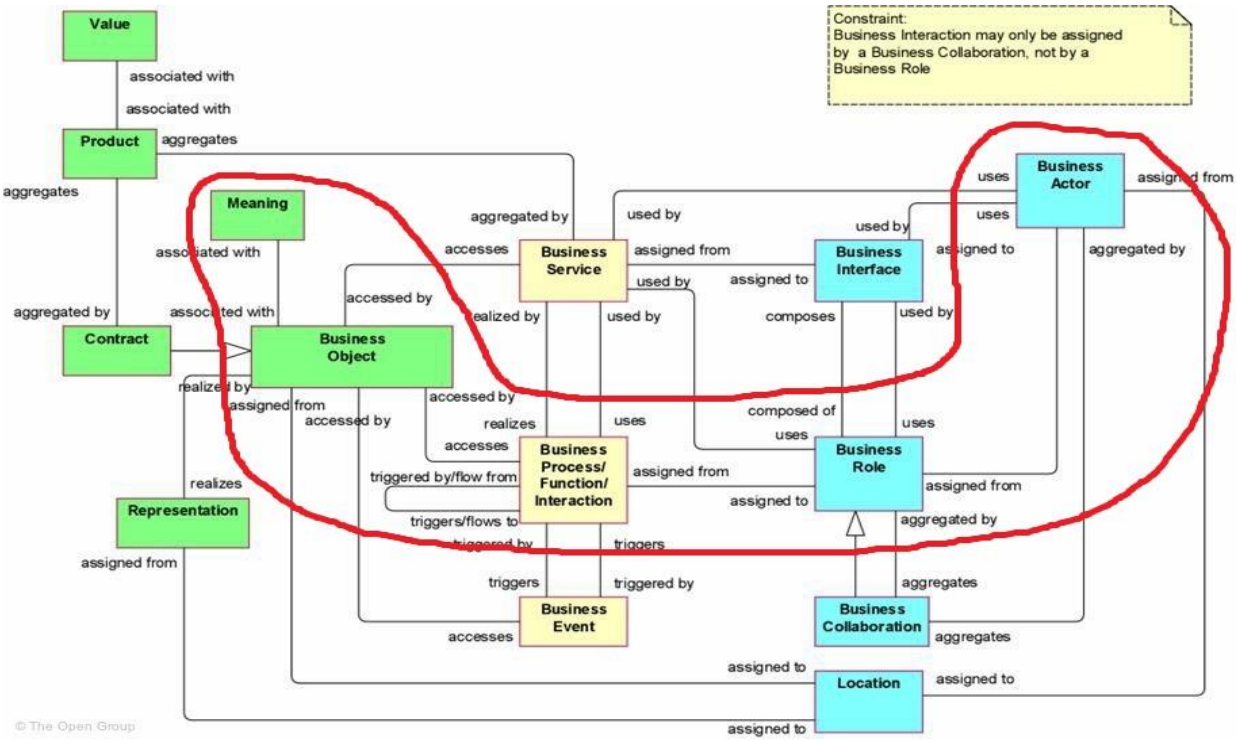


Figure 7 - Business Layer Metamodel [14]

Furthermore, ArchiMate Motivation, Implementation & Migration extension are also keys inputs for the solution proposal that will helps to the COBIT 5 for Information Security modeling. The Figure 8 illustrates that motivation extension walks side by side along the all architectural development.

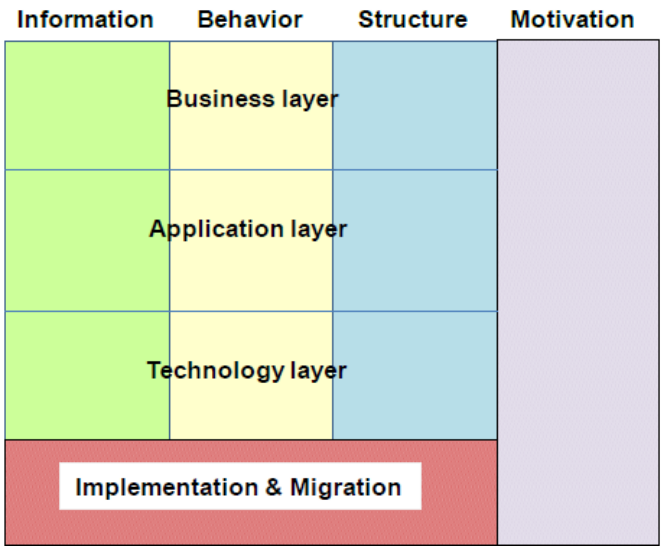


Figure 8 - ArchiMate extensions [14]

ArchiMate have already shown in academic environment the possibilities it opens in increasing the organizational awareness towards its notations, as can be seen in the following sub-section.

4.3.2. Other Researches

Silva [2] proposed an EA representation for the TIPA (Tudor's ITSM Process Assessment) framework by using the EA standard ArchiMate. Moreover, in this research a set of viewpoints that illustrates the process assessment was also defined [2]. This provides TIPA with a standard visual notation (ArchiMate) and a link between process assessment and EA principles [2].

Vicente [1] has proposed a specific EA definition for organizations that need to manage IT services. The research goal was an EA approach to design an architecture with the motivations, principles, concepts and methods of ITL to perform IT service management, using the ArchiMate [1].

Based on the COBIT 5 process *APO03 Manage enterprise architecture*, Cadete [5] has proposed an EA approach, which integrates COBIT and principles, methods and models of EA, using the ArchiMate modeling language to describe the EA. Such approach had the goal to improve the outcomes of COBIT 5 process assessment and process improvement initiatives [5]. Cadete worked on developing a proposal to solve the problem related to the ontological mismatch between the COBIT and EA domains, which implies an enabler performance risk: the threats of missing the expected targets for benefits and costs for the governance of enterprise IT in general; and for governance initiatives in particular [5]. This integration was made by creating viewpoints in order to be able to model the COBIT 5 and EA, using the ArchiMate [5].

Regarding this thesis, we will extend the ontological mapping between COBIT 5 for Information Security and ArchiMate.

5. Proposal

In Section 4, we analyzed related work in order to identify and define some key concepts, which are relevant for the correct definition of the CISO's role.

In addition, we have identified one solution (COBIT 5 for Information Security) that can be followed by the organizations but it does not address all the organization's needs, which the proposed solution should address. Furthermore, we defined the thesis problem that should be solved.

5.1. Thesis Objectives

We aim to propose a method using ArchiMate to integrate COBIT 5 for Information Security with EA principles, methods and models in order to properly implement the CISO's role.

To maximize the effectiveness of the solution, we propose to embed the COBIT 5 for Information Security's processes, information and organization structures enablers' rationale directly in the models of EA. This thesis focuses only in the CISO's responsibilities in an organization, therefore all the modeling is performed according to the level of involvement 'Responsible' (R), defined in COBIT 5 for Information Security's enablers.

This work has ambitious objectives, to create a method that:

1. Figures out what processes and activities, key practices and business functions that the CISO should be held responsible;
2. Identifies information types that the CISO is responsible to originate;
3. Finds what organization's roles are performing the CISO's job;
4. Hopefully improves the information security maturity level of the organization;
5. Identifies inconsistencies between roles' assignments, in particular the CISO's role, which are defined in the assignments matrix charts of COBIT 5 Enabling Processes, and the roles addressed by COBIT 5 for Information Security.

We also propose to demonstrate the solution by applying it to one government owned company (field study), named DemoCorp in this work. This work will be evaluated by the field study demonstration.

5.2. Using COBIT 5 for Information Security with ArchiMate

As we have identified in previous sections, COBIT 5 for Information Security helps to implement the CISO's role, but does not provide an approach in order to facilitate the implementation of this role in organizations.

EA by supporting a holistic organization view, it helps in designing the business, information and technology architecture, as well as designing the IT solutions [27] [28] [29]. Moreover, EA may change

business processes according to the strategy and business requirements [27] [28]. As COBIT is the framework for governance and management of enterprise IT, EA is defined as a framework to use in architecting the operating or business model and systems in order to meet vision, mission, and business goals and to deliver the enterprise strategy [27].

ArchiMate is a modeling language for EA and there are many enterprises that have the business processes modelled in this language [14]. Unfortunately, COBIT 5 does not have any viewpoints of its processes represented in ArchiMate (or other modeling language) in order to facilitate the definition of the CISO's role, and then it is complicated to connect the COBIT 5 and company's processes and activities.

Although EA and COBIT 5 describe areas of common interest, they do it from different perspectives [27]. COBIT 5 focuses on how one enterprise should organize the (secondary) IT function and EA concentrates on the (primary) business and IT structures, processes, information and technology of the enterprise [27].

We can conclude that EA and IT Governance (provided by COBIT 5) go hand in hand, and if we are looking for value creation in the enterprise, we should focus on putting together EA and COBIT 5. Although COBIT 5 does not provide a practical way to implement this role, it can be used with EA [5].

In the figure below, we represent the proposed method's steps for implementing the CISO's role using COBIT 5 for Information Security in ArchiMate.

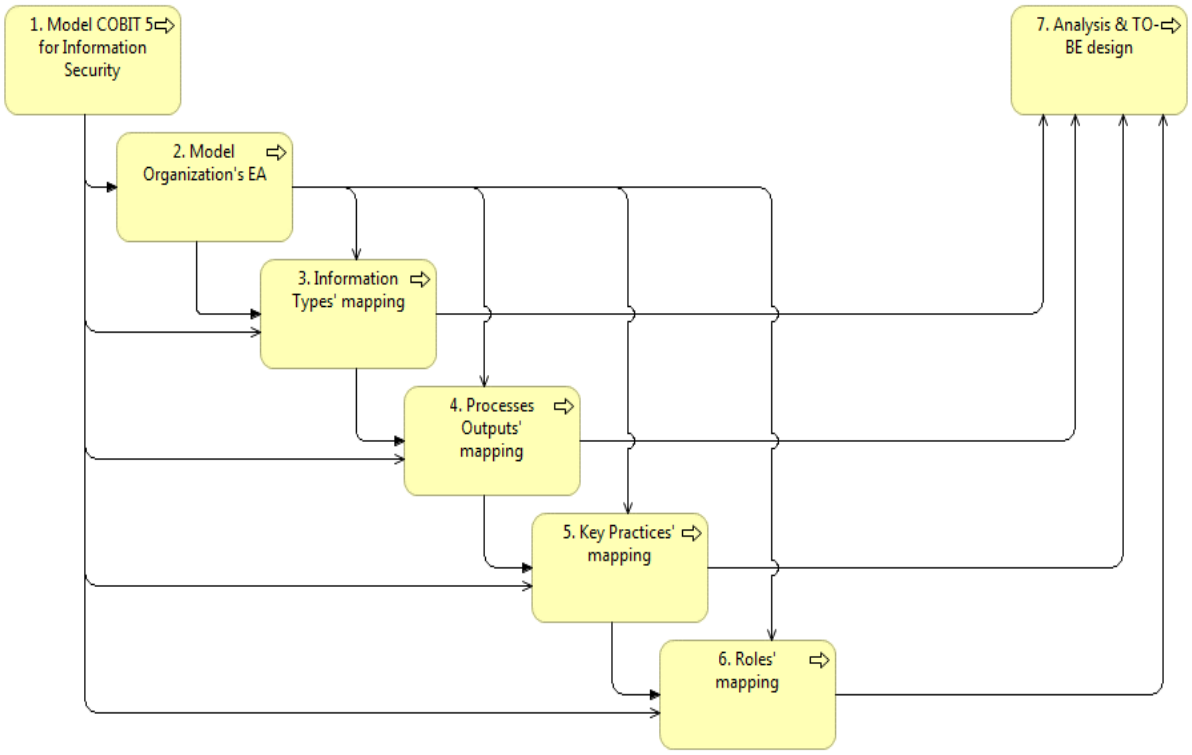


Figure 9 - Solution proposal

This research proposes a business architecture that makes the problem clear for the company, and at the same time potentiates new possible scenarios. However, as seen in previous section, ArchiMate notation provides tools that can help to get the job done, these tools do not provide a clear path to be followed appropriately with the identified need.

The proposed solution needs to have a walkthrough process that can aspirate for a greater efficiency in achieving the expected solution. Furthermore, in Section 3, we formulated the research problem that restricts the spectrum of the architecture views' system of interest, so the Business Layer, Motivation and Migration & Implementation extensions are only part of the research's scope. Such modeling will follow the architecture viewpoints (see Table 5) defined in ArchiMate.

Table 5 - Solution's Step - ArchiMate Viewpoints

Solution's Step	**ArchiMate Architecture Viewpoint**			
	Organization viewpoint	Business Process viewpoint	Motivation viewpoint	Migration Viewpoint
1. Model COBIT 5 for Information Security	X	X	X	
2. Model Organization's EA	X	X		
3. Information types' mapping		X		
4. Processes output's mapping		X		
5. Key practices' mapping		X		
6. Roles' mapping	X			
7. Analysis & TO-BE design				X

Each architecture viewpoint will only represent some concepts that are related with COBIT 5 for Information Security (see Figures 10, 11, 12 and 13).

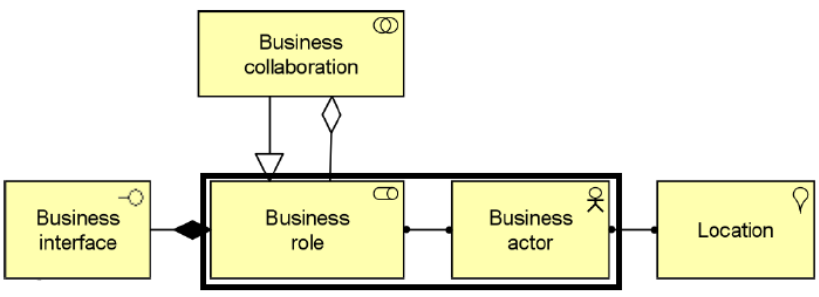


Figure 10 - Organization Viewpoint [14]

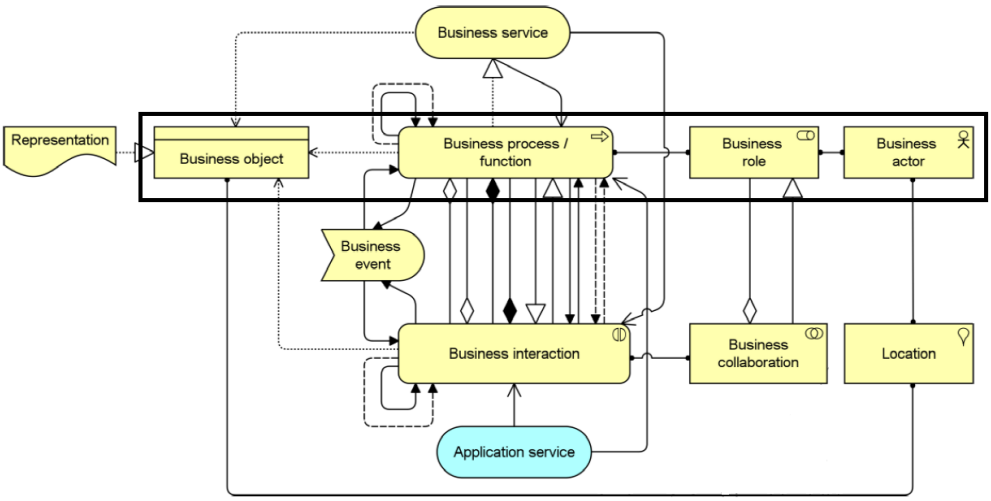


Figure 11 - Business Process Viewpoint [14]

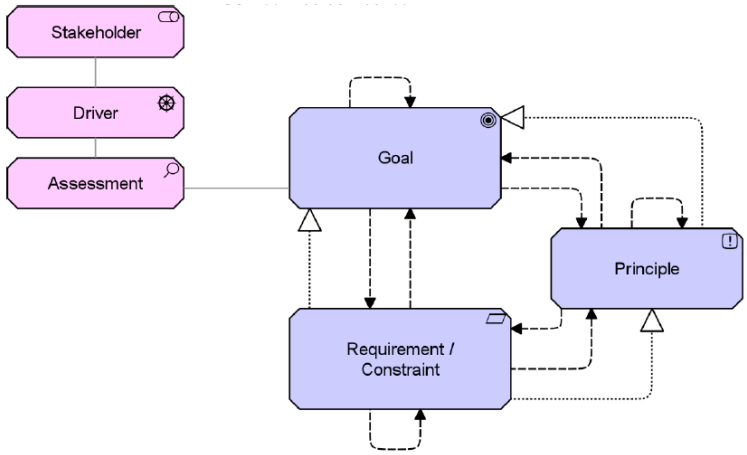


Figure 12 - Motivation Viewpoint [14]

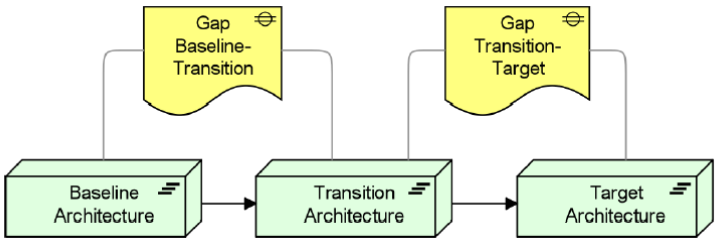


Figure 13 - Migration Viewpoint [14]

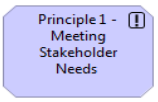
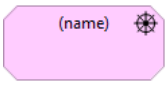
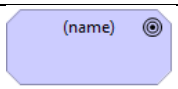
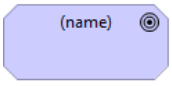
5.2.1. STEP 1 – Model COBIT 5 for Information Security

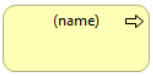
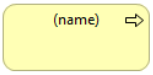
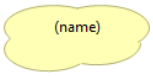
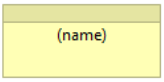
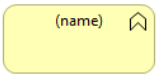
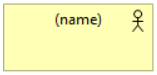
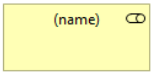
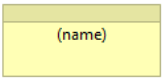
Inputs: COBIT 5 for Information Security Documentation

Outputs: CISO TO-BE Business Functions, Processes' Outputs, Key Practices and Information Types

Firstly, we aim to model the COBIT 5 for Information Security, regarding the scope of the CISO's role, using ArchiMate as the modeling language. In Table 6 is proposed the ontological mapping between COBIT 5 for Information Security and ArchiMate's concepts, regarding the definition of the CISO's role.

Table 6 - COBIT 5 for Information Security to ArchiMate ontological mapping

COBIT 5 for Information Security concept	COBIT 5 for Information Security concept description [11] [21] [31]	ArchiMate concept description [14]	ArchiMate notation [30]
Principle 1: Meeting Stakeholder Needs	The COBIT 5 framework is built on five basic principles. Principle 1: Meeting Stakeholder Needs—Enterprises exist to create value for their stakeholders – including stakeholders for information security - by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Since every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT-related goals and mapping these to specific enablers, such as processes and activities.	A principle is defined as a normative property of all systems in a given context, or the way in which they are realized.	
Stakeholder driver	Stakeholder needs are influenced by a number of drivers, e.g., strategy changes, a changing business and regulatory environment, and new technologies.	A driver is defined as something that creates, motivates, and fuels the change in an organization.	
Stakeholder needs	Value creation: The main governance objective of an enterprise, achieved when the three underlying objectives (benefits realization, risk optimization and resource optimization) are all balanced. Stakeholder needs drive the governance objective of value creation: • Benefits realization; • Risk optimization; • Resource optimization.	A goal is defined as an end state that a stakeholder intends to achieve.	
Enterprise Goals	The translation of the enterprise's mission from a statement of intention into performance targets and results.	A goal is defined as an end state that a stakeholder intends to achieve.	
IT-related Goals	A statement describing a desired outcome of enterprise IT in support of enterprise goals. An outcome can be an artefact, a significant change of a state or a significant capability improvement.	A goal is defined as an end state that a stakeholder intends to achieve.	
Enabler Goals	Enablers include processes, organizational structures and information, and for each enabler a set of specific relevant goals can be defined in support of the IT-related goals.	A goal is defined as an end state that a stakeholder intends to achieve.	
Process Goals	A statement describing the desired outcome of a process. An outcome can be an artefact, a significant change of a state or a significant capability improvement of other processes.	A goal is defined as an end state that a stakeholder intends to achieve.	
Information Security-specific Goal	A statement describing the desired outcome of a process, regarding information security. An outcome can be an artefact, a significant change of a state or a significant capability improvement of other processes.	A goal is defined as an end state that a stakeholder intends to achieve.	
Process	Generally, a collection of practices influenced by the enterprise's policies and	A business process is defined as a behavior	

	procedures that takes inputs from a number of sources (including other processes), manipulates the inputs and produces outputs (e.g., products, services).	element that groups behavior based on an ordering of activities. It is intended to produce a defined set of products or business services.	
Base Practices	An activity that, when consistently performed, contributes to achieving a specific process purpose. Base practices are the activities or tasks required to achieve the required outcome for the process. They are specified in the COBIT 5 PAM at a high level without specifying how they are carried out.	A business process is defined as a behavior element that groups behavior based on an ordering of activities. It is intended to produce a defined set of products or business services.	
Process Description	An overview of what the process does and a high-level overview of how the process accomplishes its purpose.	It is a description that expresses the intent of a representation; i.e., how it informs the external user. Meaning is defined as the knowledge or expertise present in a business object or its representation, given a particular context.	
Process Purpose	A description of the overall purpose of the process. The high-level measurable objectives of performing the process and the likely outcomes of effective implementation of the process.	A goal is defined as an end state that a stakeholder intends to achieve.	
Information Types	Identifying the stakeholder of information is essential to optimize the development and distribution of information throughout the enterprise. Example of information types: • Information security strategy; • Information security review reports.	A business object is defined as a passive element that has relevance from a business perspective.	
Business Function	Identifying the stakeholder of information is essential to optimize the development and distribution of information throughout the enterprise.	A business function is defined as a behavior element that groups behavior based on a chosen set of criteria (typically required business resources and/or competences).	
Stakeholder	Anyone who has a responsibility for, an expectation from or some other interest in the enterprise — e.g., shareholders, users, government, suppliers, customers and the public.	A business actor is defined as an organizational entity that is capable of performing behavior.	
Role	Prescribed or expected behavior associated with a particular position or status in a group or organization. A job or a position that has specific set of expectations attached to it.	A business role is defined as the responsibility for performing specific behavior, to which an actor can be assigned.	
Inputs and Outputs	The process work products/artefacts considered necessary to support process's operation.	A business object is defined as a passive element that has relevance from a business perspective.	

The column "COBIT 5 for Information Security concept description" contains definitions and explanations retrieved from COBIT 5 publications [6] [11] [21] [31]. The column "ArchiMate concept description" contains definitions and explanations retrieved from the ArchiMate specification [14]. Furthermore, the semantic matching between the definitions and explanations of these columns contributes for the proposed COBIT 5 for Information Security to ArchiMate ontological mapping.

The proposed ontological mapping enables the design of the COBIT 5 for Information Security Metamodel, as can be seen in the figure below. Note that it is only represented the COBIT 5's concepts that enables the definition of the CISO's role.

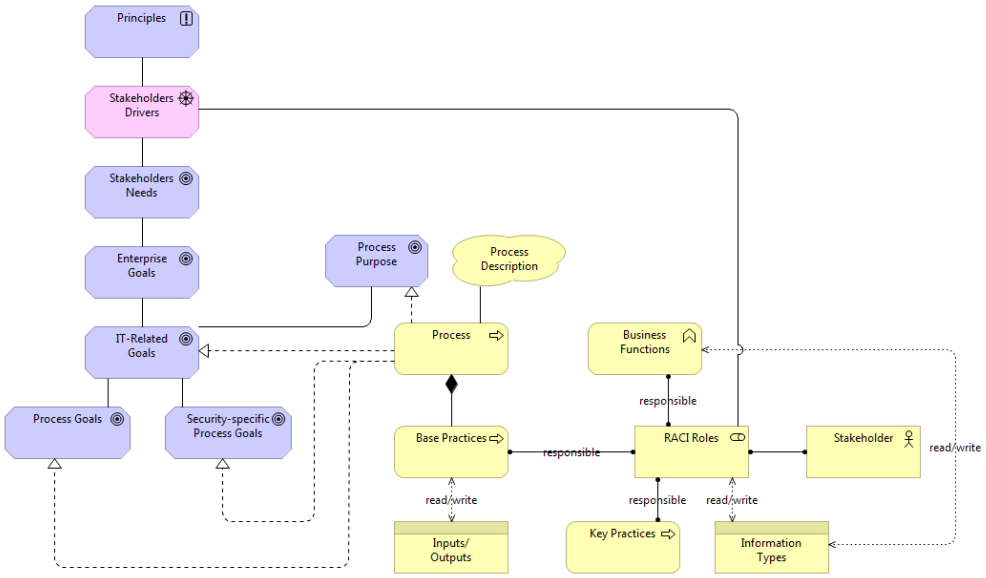


Figure 14 - COBIT 5 for Information Security Metamodel

Based on the metamodel presented in the figure above, we can model the responsibilities of the CISO's role defined in COBIT 5 for Information Security.

Firstly, regarding the definition of the CISO's role, we will model the CISO's business functions and the information types that he/she is responsible to originate, defined in this professional guide, using the ArchiMate notation. In Figure 15 we present the Generic Business Functions and Information Types template that will be used for modeling the CISO's business functions and information types, which are defined in COBIT 5 for Information Security. Such modeling is based on Principles, Policies and Frameworks, Information and Organizational Structures enablers of COBIT 5 for Information Security.

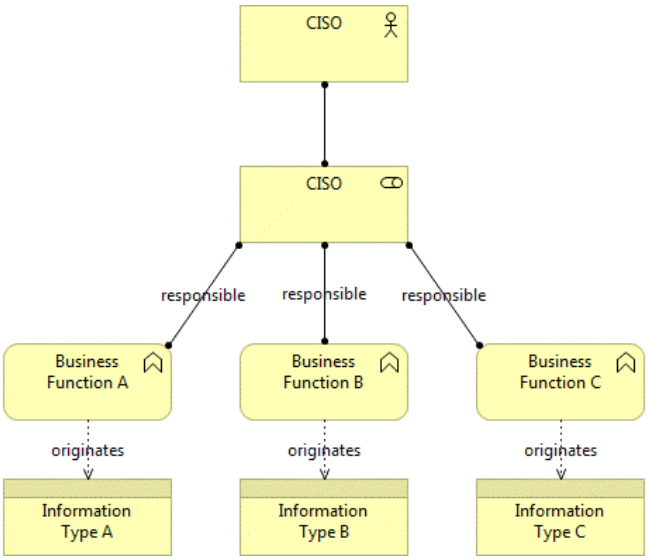


Figure 15 - Generic Business Functions and Information Types template, for viewpoints used in CISO's definition

As we can note, COBIT 5 for Information Security defines information types that are originated by a specific business function. These business functions are assigned to the CISO's role.

Secondly, we will model the COBIT 5 for Information Security's processes and processes' practices in which CISO is responsible for, as can be seen in the table below.

Table 7 - COBIT 5 Processes' Practices in which CISO is Responsible

Chief Information Security Officer (CISO)	**RACI**
EDM03 Ensure Risk Optimization	
EDM03.03 Monitor risk management	**Responsible**
APO01 Manage the IT Management Framework	
APO01.04 Communicate management objectives and direction	**Responsible**
APO12 Manage Risk	
APO12.01 Collect data	**Responsible**
APO12.06 Respond to risk	**Responsible**

Regarding these processes' practices and the assigned CISO's responsibilities, we present the Generic Processes template (see Figure 16) that will be used for CISO processes practices' modeling. Such modeling is based on the Processes enabler of COBIT 5 for Information Security.

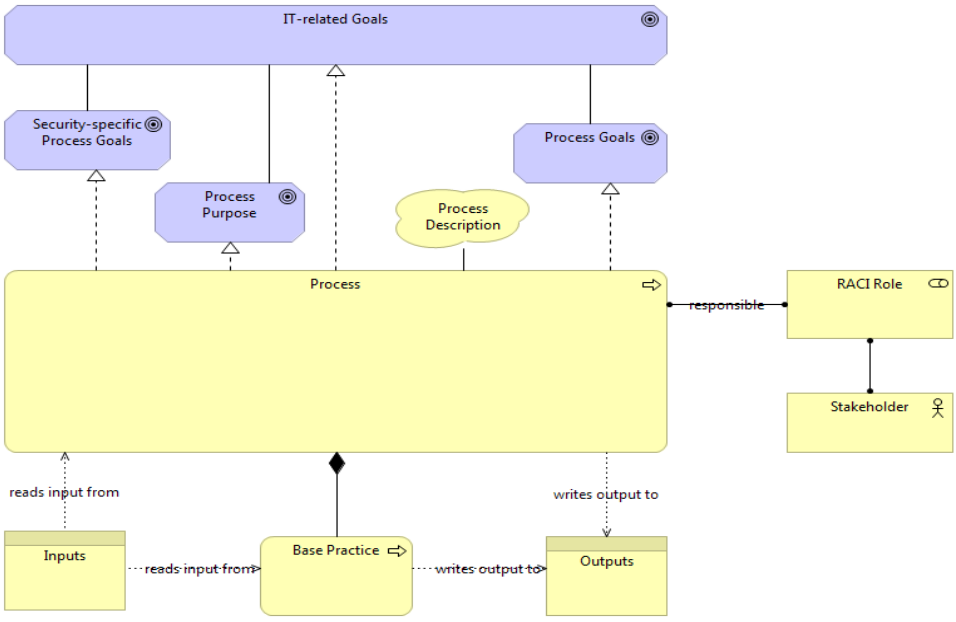


Figure 16 - Generic Processes template, for viewpoints used in CISO's definition

Finally, we will model the key practices that he/she should be held responsible. Regarding these key practices and the assigned CISO's level of involvement, we present the Generic Key Practices template (see Figure 17) that will be used for CISO key practices' modeling. Such modeling is based on the Organizational Structures enabler of COBIT 5 for Information Security.

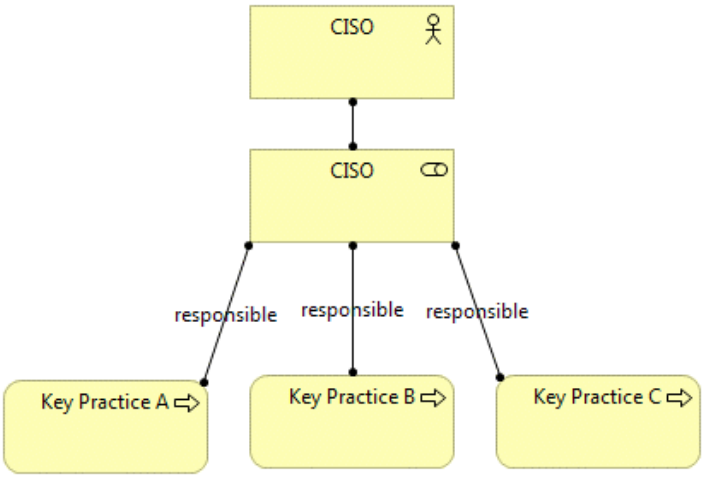


Figure 17 - Generic Key Practices template, for viewpoints used in CISO's definition

As output of this Step, viewpoints' contents will be the input for the detection of such organization's contents, in order to implement the CISO's role.

5.2.2. STEP 2 – Model Organization's EA

Inputs: CISO TO-BE Business Functions, Processes' Outputs, Key Practices and Information Types, Documentation, Informal Meetings

Outputs: Organization AS-IS Business Functions, Processes' Outputs, Key Practices and Information Types

In this step is essential to represent the organizations' EA, regarding the definition of the CISO's role. Such modeling aims to identify organization AS-IS and is based on the preceded figures of STEP 1, i.e., all viewpoints represented will have the same structure.

This step aims to represent all the information related to the definition of the CISO's role in COBIT 5 for Information Security, in order to figure out what processes' outputs, business functions, information types and key practices exists in the organization.

Firstly, we will model the organization's business functions and types of information originated by them, which are related to the business functions and information types of COBIT 5 for Information Security in which the CISO is responsible for, using the ArchiMate notation. In Figure 18 we present the Generic Organization's Business Functions and Information Types template that will be used for organization business functions and information types' representation. This template presents the information types originated, business functions and assigned roles responsibilities.

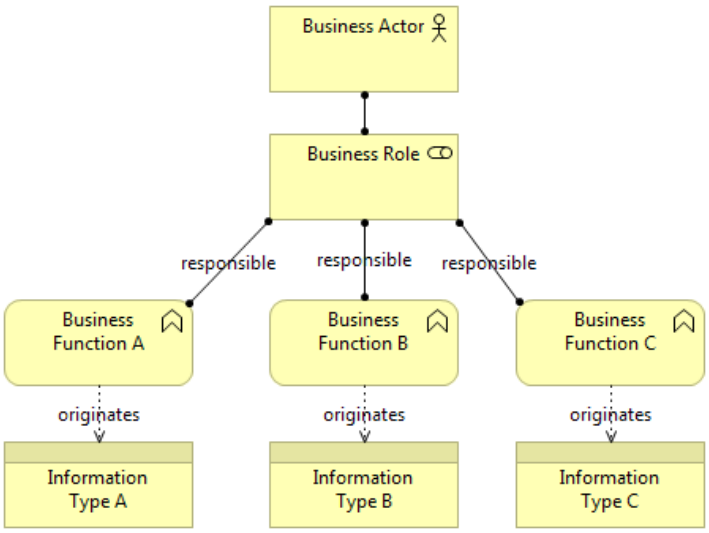


Figure 18 - Generic Organization's Business Functions and Information Types template

Secondly, we will model the organization's processes and processes' practices, which are related to the processes of COBIT 5 for Information Security in which the CISO is responsible for. Regarding these processes and the assigned roles responsibilities, we present the Generic Organization's Processes template (see Figure 19) that will be used for organization processes' modeling.

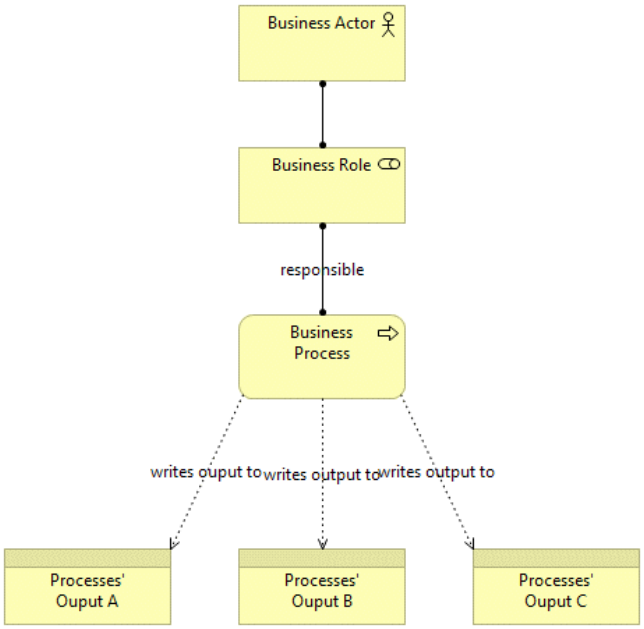


Figure 19 - Generic Organization's Processes template

Finally, will be represented the existent organization's practices, which are related to the key practices of COBIT 5 for Information Security in which the CISO is responsible for. Regarding these key practices and the assigned roles level of involvement, we present the Generic Organization's Key Practices template (see Figure 20) that will be used for organization key practices' representation.

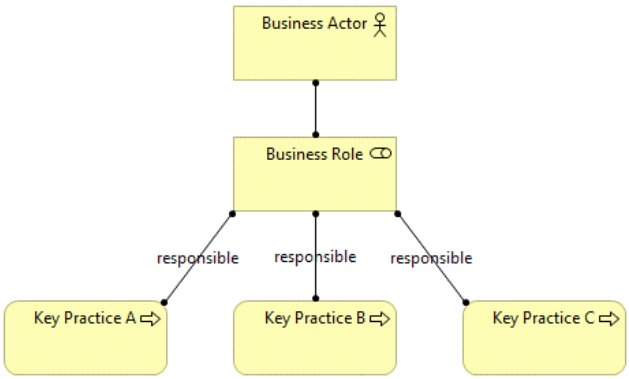


Figure 20 - Generic Organization's Key Practices template

Step 1 and Step 2 provide information about the organization's AS-IS and desired TO-BE, regarding the CISO's role. Moreover, these two steps will be used as inputs of the remaining steps (STEP 3 to 6).

5.2.3. STEP 3 – Information types' mapping

Inputs: Information types, business functions and roles involved – AS-IS (STEP 2) | TO-BE (STEP 1)

Outputs: GAP analysis of information types

In the third step, our goal is to map the organization's information types to the information that CISO should originate, which are defined in COBIT 5 for Information Security. For that, we present the Information Types' mapping template (see Figure 21) in which we map the organization's information types to information types that the CISO should be responsible for originate, defined in COBIT 5 for Information Security. With this, will be possible to identify which information types are missing and who is responsible for them.

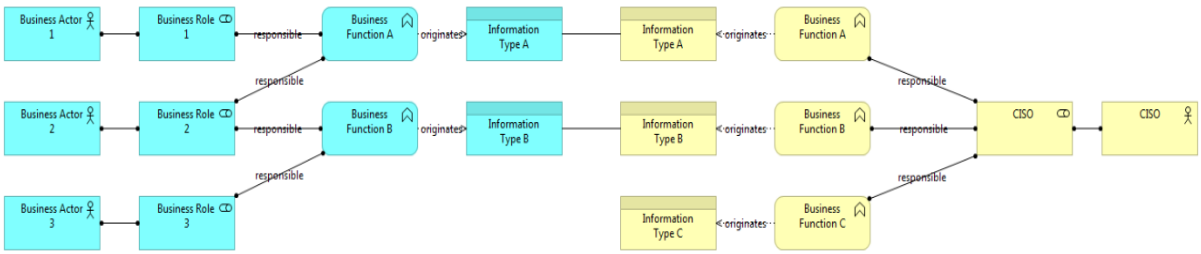


Figure 21 - Generic Information Types' mapping template

If there is not a connection between the organization's information types (represented by the blue color on the left side) and the information types in which the CISO is responsible for originate, defined in COBIT 5 for Information Security (represented by the yellow color on the right side), we can conclude that was detected an information types' gap.

5.2.4. STEP 4 – Processes Outputs' mapping

Inputs: Processes' outputs and roles involved – AS-IS (STEP 2) | TO-BE (STEP 1)

Outputs: GAP analysis of processes' outputs

The fourth step's goal is to map the processes' outputs of the organization to the COBIT 5 for Information Security's processes that the CISO is responsible for. We present the Processes' Outputs' mapping template (see Figure 22) in which we map the processes' outputs of the organization to the desired processes' outputs that the CISO is responsible to produce, defined in COBIT 5 for Information Security. With this, will be possible to identify which process' outputs are missing and who is delivering them.

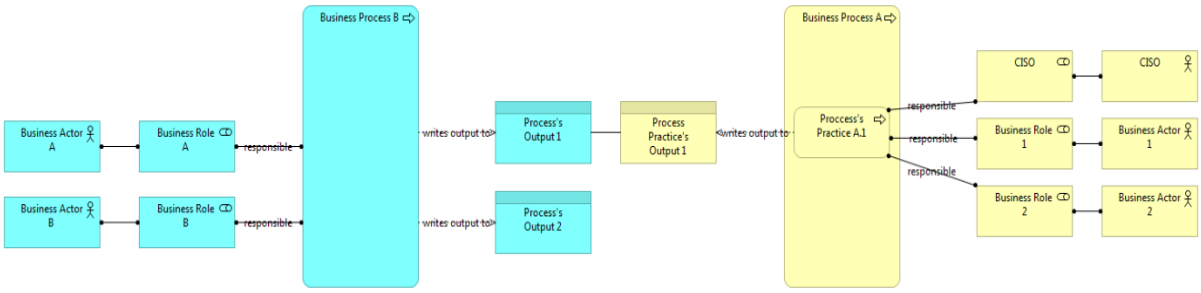


Figure 22 - Generic Processes Outputs' mapping template

If there is not a connection between the process's outputs of the organization (represented by the blue color on the left side) and the processes' outputs in which the CISO is responsible for produce and/or deliver, defined in COBIT 5 for Information Security (represented by the yellow color on the right side), we can conclude that was detected a processes' output gap.

5.2.5. STEP 5 – Key Practices' mapping

Inputs: Key practices and roles involved – AS-IS (STEP 2) | TO-BE (STEP 1)

Outputs: GAP analysis of key practices

In the fifth step, we intend to map the organizations' practices to key practices defined in COBIT 5 for Information Security, which the CISO should be responsible for. For that, we present the Key Practices' mapping template (see Figure 23) in which we map the organization's practices to key practices that the CISO should be responsible for, defined in COBIT 5 for Information Security. With this, will be possible to identify which key practices are missing and who is responsible for them in the organization.

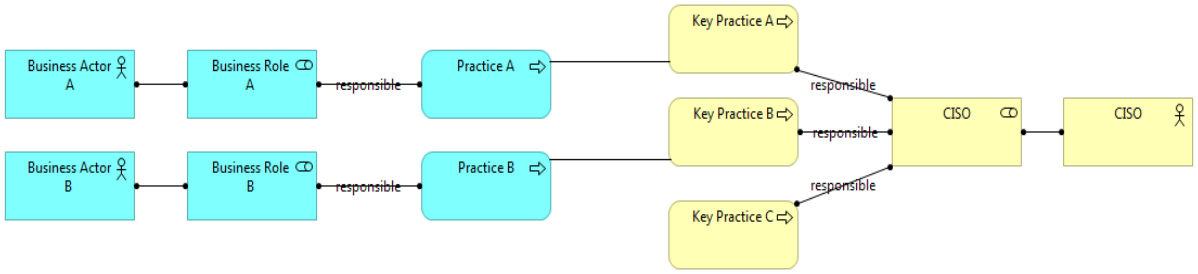


Figure 23 - Generic Key Practices' mapping template

If there is not a connection between the organization's practices (represented by the blue color on the left side) and the key practices in which the CISO is responsible for, defined in COBIT 5 for Information Security (represented by the yellow color on the right side), we can conclude that was detected a key practice's gap.

5.2.6. STEP 6 – Roles' mapping

Inputs: Roles – AS-IS (STEP 2) | TO-BE (STEP 1)

Outputs: Roles which are doing the CISO's job

In this step, we will map the organization's roles to the CISO's role defined in COBIT 5 for Information Security, in order to identify who is performing the CISO's job. For that, we present the Roles' mapping template (see Figure 24) in which we associate the organization's roles that do the CISO's job, defined in COBIT 5 for Information Security. This mapping allows to identify which roles of the organization are performing the job of the CISO.

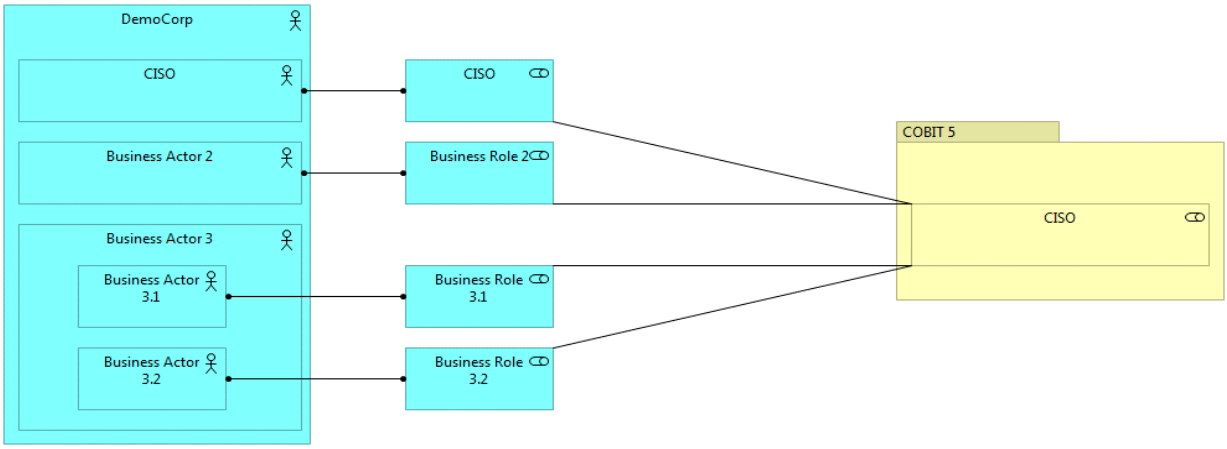


Figure 24 - Generic Roles' mapping template

5.2.7. STEP 7 – Analysis & TO-BE Design

Inputs: Approach to AS-IS (STEP 3 to 6)

Outputs: Solution

In Step 1 is intended to design the responsibilities of the CISO's role, regarding to what is defined in COBIT 5 for Information Security (possible TO-BE).

As stated in Step 2, the organization's EA should be designed based on what was designed in Step 1, in order to perform the mapping in the following steps.

Steps 3, 4, 5 and 6 present the mapping of responsibilities between the CISO (defined in COBIT 5 for Information Security) and existing roles in the organization that are performing the CISO's job.

This step aims to analyze the AS-IS of the organization's EA and design the desired TO-BE, regarding the CISO's role. This step requires:

- Identify organization's information security gaps;
- Discuss with the organization's responsible structures and roles in order to determine whether the responsibilities identified, which should be the CISO (defined in COBIT 5 for Information Security), still belong to these structures or should be assigned to the CISO's role.

For that, as can be seen in the figure below, we present the Migration viewpoint template in which we specify the transition from an existing architecture to a desired architecture, regarding the definition of the CISO's role.

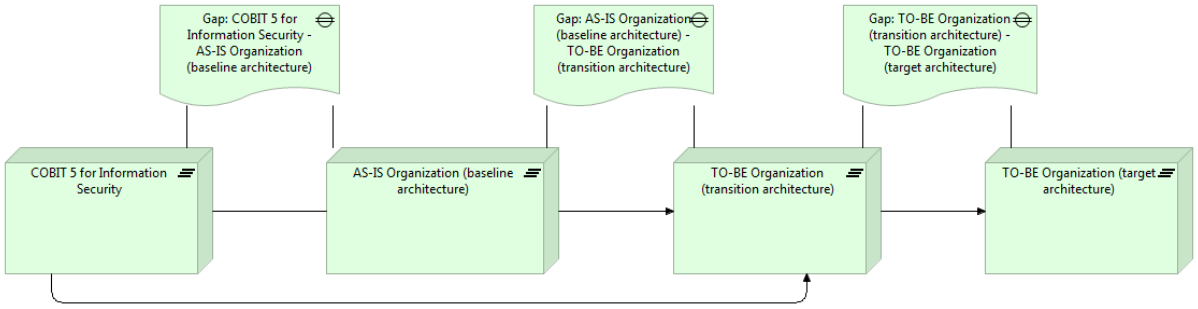


Figure 25 - Generic Migration viewpoint template

The purpose of this step is to design the AS-IS of the organization, identify the gaps between the existent architecture and the responsibilities of the CISO's role, defined in COBIT 5 for Information Security. In addition, this viewpoint allows the organization to discuss the information security gaps detected, so they can implement the role of CISO. For that, it is necessary to make a strategic decision, which may be different from each organization, in order to fix the information security gaps identified.

All information security gaps identified during the mappings between the organization and the CISO's role defined in COBIT 5 for Information Security may not be fixed, as the organization could decide that only some of the detected gaps should be treated. As a result of this decision, some gaps may remain between the organization's TO-BE (target architecture) and what is defined in COBIT 5 for Information Security that should be the responsibilities of the CISO in an organization.

5.3. Roles Inconsistencies

COBIT 5 Enabling Processes proposes an assignment of roles' responsibilities for each management and governance process [21]. In addition, COBIT 5 for Information Security is based on the COBIT 5's processes defined in the enabler guide, but it provides information security-specific contents [6].

A list of characteristics and responsibilities for each information security's roles are presented in the information and organizational structures enablers of COBIT 5 for Information Security [21]. For example, this list includes information types originated by each role (information enabler) and a high-level RACI chart that links processes' activities to organizational structures and/or individual roles in the enterprise [6]. They describe the level of involvement of each role for each process practice: accountable, responsible, consulted or informed (organizational structures enabler) [21].

On the other hand, the RACI charts attached at each processes' practices in COBIT 5 Enabling Processes, highlight the roles that are responsible to perform a specific action for those practices [21].

Moreover, all the specific-security management practices' outputs can be observed in COBIT 5 for Information Security [6]. Making the connection to what is defined in the COBIT 5 Enabling Processes,

we can conclude that the roles responsible to deliver these outputs are different from the roles that originate this kind of information. Note that, in some instances, the organizational structures' outputs and information types originated by information security roles are information delivered by a process, in which case they are process outputs [6].

To illustrate these roles' inconsistency of the COBIT 5 RACI charts, we present in Table 8 the connection between the enablers described before, regarding one information security-specific role - CISO.

Table 8 reveals the relation between the processes' practices of COBIT 5 Enabling Processes and enablers relevant of COBIT 5 for Information to the definition of CISO's role in an organization.

COBIT 5 Enabling Processes describes the roles' responsibility levels, goals, activities, metrics, practices and inputs/outputs of each process, which are related in the COBIT 5's Process Reference Model. For each processes' practice, are presented a set of inputs that influence outputs' production [21].

COBIT 5 for Information Security, for each enabler, adds relevant information security's content [6]. Regarding the definition of the CISO's role, the processes, information and organizational structures enablers can be used for. In the processes enabler, and taking into account the 37 processes described in COBIT 5 Enabling Processes, are attached information security's content, i.e., information security-specific goals, metrics, activities and inputs/outputs [6].

Considering that COBIT 5 is a reference and should be adapted for each organization for a particular context does not imply that these enabler guide and professional guide are misaligned, since, for example, to implement the CISO's role is relevant to know which the processes are in which he/she is responsible for. Such information is only available in the RACI charts of COBIT 5 Enabling Processes [21].

Knowing that the CISO is responsible for certain processes, we can look at COBIT 5 for Information Security and analyze where the CISO is responsible for the processes and other information security-specific's content. Furthermore, in this professional guide, for example, the information enabler enumerates a set of information types that the CISO should originate. These information types are information security-specific's inputs/outputs of the processes' practices [6].

After determining what the processes are in which these information types are outputs, it can be observed that these processes' outputs (specified in COBIT 5 for Information Security) are not part of the CISO's roles, taking into account the processes' RACI charts described in guide COBIT 5: Enabling Processes. This inconsistency also occurs in organizational structures enabler, as it can be seen in Table 8, and leads to various issues associated with IT governance, since it may lead to questions about what the processes and practices that the CISO is responsible for and which are the outputs to be produced and/or delivered in these processes' practices [42].

Table 8 - COBIT 5 Enabling Processes vs COBIT 5 for Information Security

COBIT 5 Enabling Processes	COBIT 5 for Information Security		
Process Enabler (Base Practice)	**Process Enabler (Output)**	**Information Enabler**	**Organizational Structures Enabler**
APO01.03 - Maintain the enablers of the management system.	Information security and related policies.	CISO is the originator of Information Security Policies.	CISO is responsible for the development information security policies and procedures.
APO02.02 – Assess the current environment, capabilities and performance.	Information security capabilities.	CISO is the originator of the Information Security Plan.	n/d
APO02.05 - Define the strategic plan and road map.	Information security strategy.	CISO is the originator of the Information Security Strategy.	CISO is responsible for the definition and communication of an information security strategy that is in line with the business strategy.
			CISO is responsible for research, definition and documentation of information security requirements.
			CISO is responsible for the validation of information security requirements with stakeholders, business sponsors and technical implementation personnel.
			CISO is responsible for monitoring IT risk management.
APO02.06 - Communicate the IT strategy and direction.	Information security plan.	CISO is the originator of the Information Security Plan.	CISO is responsible for the definition and implementation of risk evaluation and response strategies and co-operate with the risk office to manage the information risk.
			CISO is responsible for ensuring that potential impact of changes is assessed.
			CISO is responsible for collecting and analyzing performance and compliance data relating to information security and information risk management.
APO05.03 - Evaluate and select programs to fund.	Information security program.	n/d	CISO has the overall responsibility of the enterprise's information security program.
APO11.01 - Establish a quality management system (QMS).	Relevant information security good practices and standards.	CISO is the originator of the Information Security Plan.	CISO is responsible for the production of policies, standards and procedures.
APO11.02 - Define and manage quality standards, practices and procedures.	Information security quality standards.	CISO is the originator of the Information Security Plan.	CISO is responsible for the production of policies, standards and procedures.
APO12.04 – Articulate risk.	Information security risk response strategies.	CISO is the originator of the Information Security Plan.	CISO is responsible for the definition and implementation of risk evaluation and response strategies and co-operate with the risk office to manage the information risk.

Furthermore, in Appendix D, we present the RACI charts of each processes' practices presented in the previous table (see Figures 73, 74, 75, 76 and 77). For each figure, we can observe that the CISO is not responsible for the processes' practices that have the information security-specific's outputs [21].

After the analysis of the previous table and figures, we present the Table 9 that illustrates the conceptual inconsistencies between the COBIT 5 Enabling Processes and COBIT 5 for Information Security, regarding the assignment of CISO's roles [42].

Table 9 - CISO's roles inconsistencies between COBIT 5 Enabling Processes and COBIT 5 for Information Security

		COBIT 5 Enabling Processes	**COBIT 5 for Information Security**
		Output's Responsible	**Enabler's Responsible**
#	**Base Practice**		
1	APO01.03 – Maintain the enablers of the management system.	Chief Operating Officer, Chief Information Officer and Head IT Administration.	Chief Information Security Officer.
2	APO02.02 – Assess the current environment, capabilities and performance.	Business Executives, Head Architect, Head Development and Head IT Operations.	Chief Information Security Officer.
3	APO02.05 - Define the strategic plan and road map.	Project Management Office.	Chief Information Security Officer.
4	APO02.06 - Communicate the IT strategy and direction.	Chief Executive Officer, Business Executives and Chief Information Officer.	Chief Information Security Officer.
5	APO05.03 - Evaluate and select programs to fund.	Chief Financial Officer, Business Executives, Strategy Executive Committee, Value Management Office and Chief Information Officer.	Chief Information Security Officer.
6	APO11.01 – Establish a quality management system (QMS).	Chief Information Officer, Head IT Administration and Service Manager.	Chief Information Security Officer.
7	APO11.02 – Define and manage quality standards, practices and procedures.	Business Process Owners, Project Management Office, Head Architect, Head Development, Head IT Operations, Head IT Administration, Service Manager, Information Security Manager, Business Continuity Manager and Privacy Officer.	Chief Information Security Officer.
8	APO12.04 – Articulate risk.	Business Process Owners and Chief Risk Officer.	Chief Information Security Officer.

This table is formulated based on the practices' RACI charts of COBIT 5 Enabling Processes and CISO's roles described in each of the enablers set above. For example, in the first row of the table, the practice "APO01.03 - Maintain the enablers of the management system" has the following roles has responsible [21]:

- Chief Operating Officer;
- Chief Information Officer;
- Head IT Administration.

Analyzing COBIT 5 for Information Security and what was listed in Table 8, is possible to observe that the CISO is responsible for originating the information security's information type "Information Security Policies" (information enabler) and he/she is responsible for the development of information security policies and procedures (key practice of organizational structures enabler). Moreover, regarding these information type and key practice, was observed that practice APO01.03 produces the following information security-specific's output - "Information security policies and related" (process enabler). It would be expected that the CISO was responsible for the process's practice, described in COBIT 5: Enabling Processes. This assignment is not associated with CISO's roles, originating an inconsistency between the COBIT 5 for Information Security and COBIT 5: Enabling Processes [42].

The remaining table's rows are based on the same analysis's principle (contents of Table 8 and Figures 73, 74, 75, 76 and 77).

6. Demonstration

This section corresponds to the demonstration activity of DSRM process model [10].

The demonstration activities aim to demonstrate the use of artifacts to solve the one or more instances of the research problem [10].

One of the resources required for the demonstration is the effective knowledge of how to use the artifacts to solve the research problem and this will be supplied by the proposed method.

We used one midsized government owned company for the demonstration. Such company has a low level of maturity in information security, then centralizing the proposed method to the problem regarding which data is dealt regarding the research problem. Moreover, the ArchiMate notation was used to demonstrate the using of EA to implement the CISO's role.

In order to better address the identified problem, it is important to focus the AS-IS analysis on responsibilities of the organizations' roles and their respective business functions, information types, processes' outputs and key practices. This assessment on the existent Business Functions, Objects, Processes, Roles and Actors involved will allow a better understanding on the existent organization's gaps, which will optimally allow an approach to the solution.

6.1. STEP 1 - Model COBIT 5 for Information Security

The problem to address has a clear main role that is the CISO, which has the responsibility of the enterprise information security program.

In order to tackle this problem, we represented the COBIT 5 for Information Security's enablers, integrating COBIT and principles, methods and models of EA. Such modeling provides a way to map one organization's EA to the CISO's role defined in COBIT 5 for Information Security in order to reach our main goal, which is the implementation of the CISO's role in the organizations. This mapping was done based on the Processes, Principles, Policies and Frameworks, Information and Organizational Structures enablers.

As stated in Section 4, such contents can be identical, because all of the enablers are related.

As a first step of the method, it is required to model the types of information that the CISO is responsible for originating. Figure 26, based on what is defined in COBIT 5 for Information Security, represents the artifact, named CISO's Business Functions and Information Types viewpoint, which illustrates the business functions and associated information types that the CISO should originate.

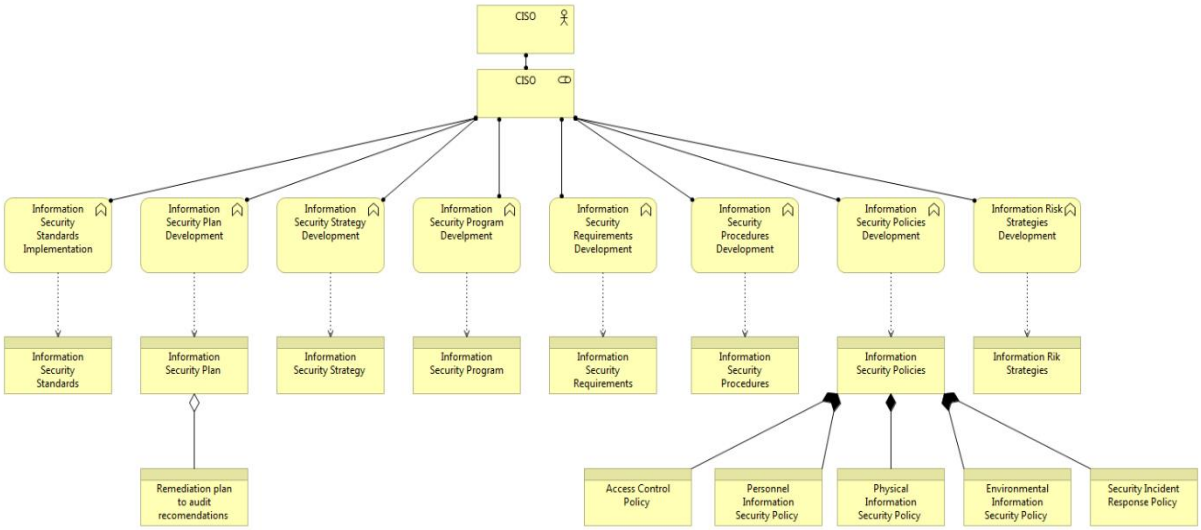


Figure 26 - CISO's Business Functions and Information Types viewpoint

Then, following the method, Figures 27, 28 and 29 present the artifacts, which shows the inputs, outputs and roles responsible of the COBIT 5's processes for which the CISO is responsible.

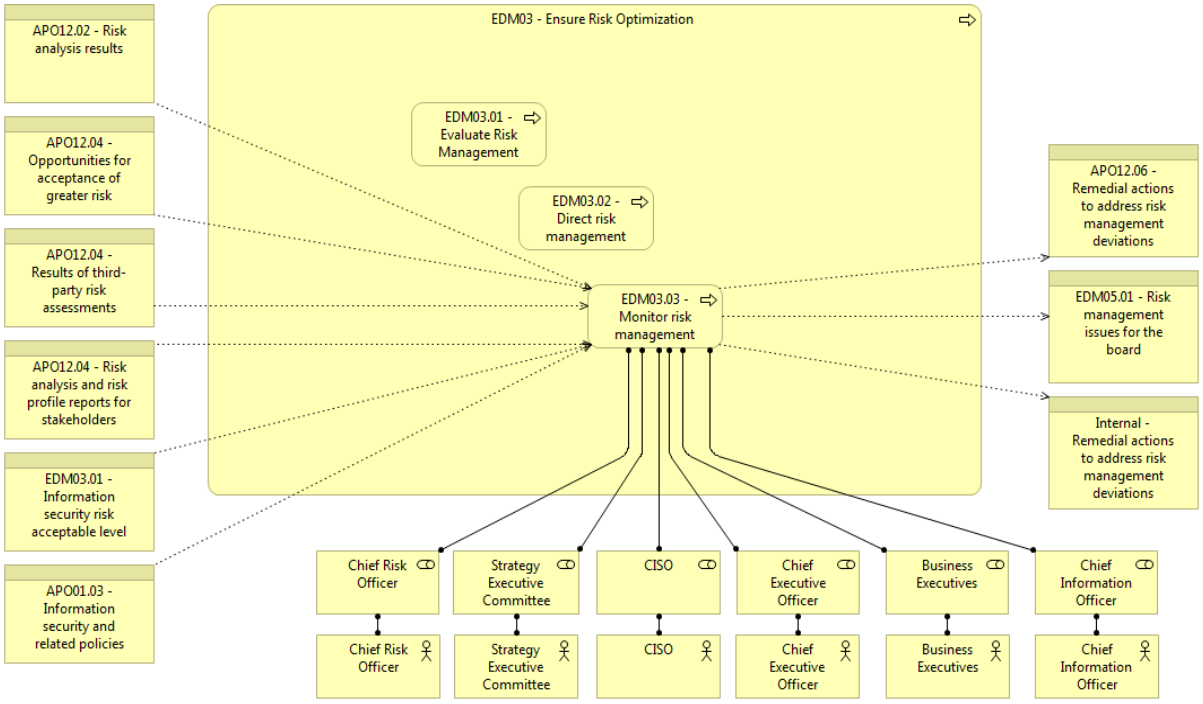


Figure 27 - EDM03 Ensure Risk Optimization Process viewpoint

In Appendix A, the architectural artifacts show the processes *EDM03 Ensure Risk Optimization, APO01 Manage the IT Management Framework* and *APO12 Manage Risk*, and the corresponding IT-related, Process and Security-specific Process Goals (see EDM03 Ensure Risk Optimization/ APO01 Manage the IT Management Framework/ APO12 Manage Risk Process and Goals viewpoint). These viewpoints show the connection between motivation and business process viewpoints.

Moreover, in Appendix A, we present the COBIT 5 Organization Structure viewpoint where the stakeholders and assigned roles defined in COBIT 5 are represented.

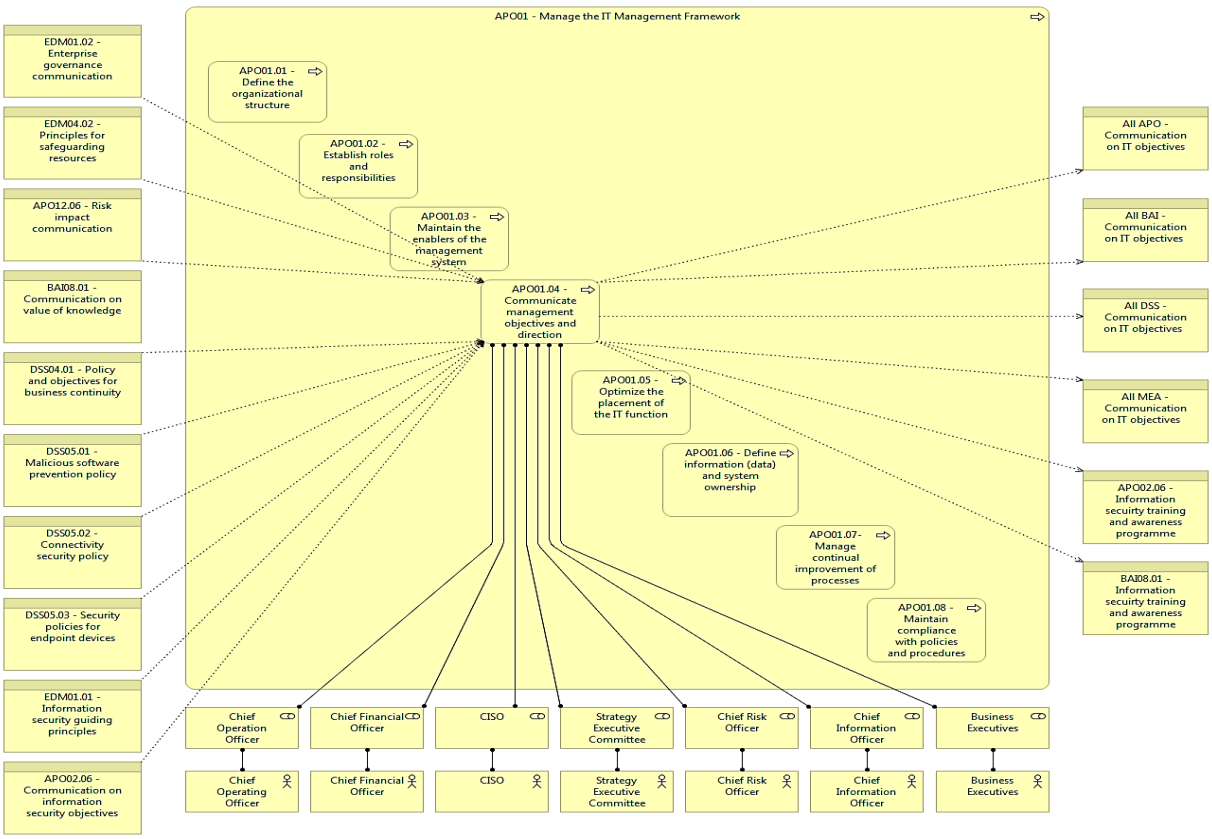


Figure 28 - APO01 Manage the IT Management Framework Process viewpoint

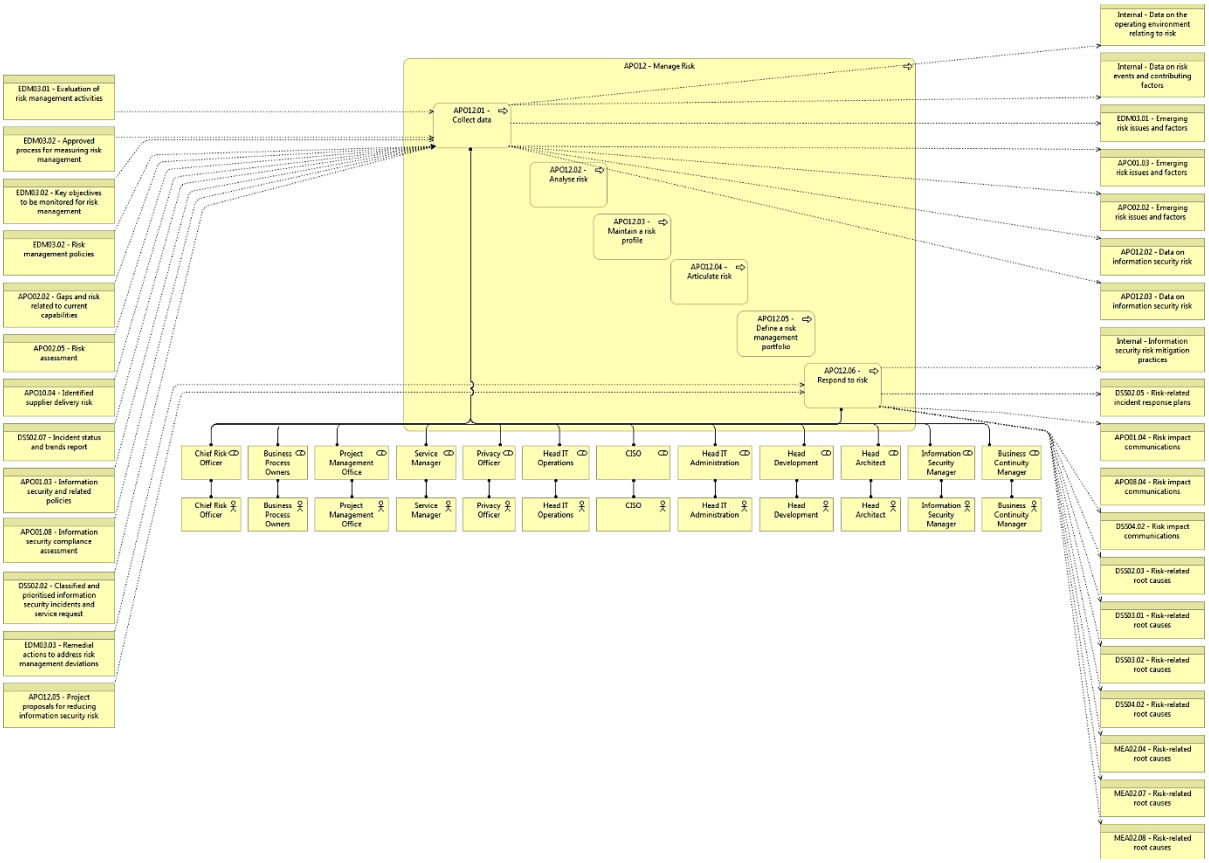


Figure 29 - APO12 Manage Risk Process viewpoint

Following the first step stated in the solution proposal, the following figure presents the key practices for which the CISO could be held responsible.

Figure 30 - CISO's Key Practices viewpoint

We now have the definition of the CISO's role, based on the COBIT 5 for Information Security, to which will be the input for the next steps of the proposed method.

6.2. STEP 2 - Model Organization's EA

In the second step, we model the AS-IS of the organization's EA. In Appendix B we present the interview guide that was used to identify the AS-IS of the DemoCorp.

Following the steps of the proposed method, it is necessary to represent the DemoCorp's business functions and information types, which are related to the CISO's role defined in Step 1 (see Figure 31).

When looking at the organizational and information types originated by each one of the business functions individually, it is possible to observe that the CISO is responsible for the development of information security requirements, policies and procedures. Moreover, this role is responsible for the implementation of information security standards.

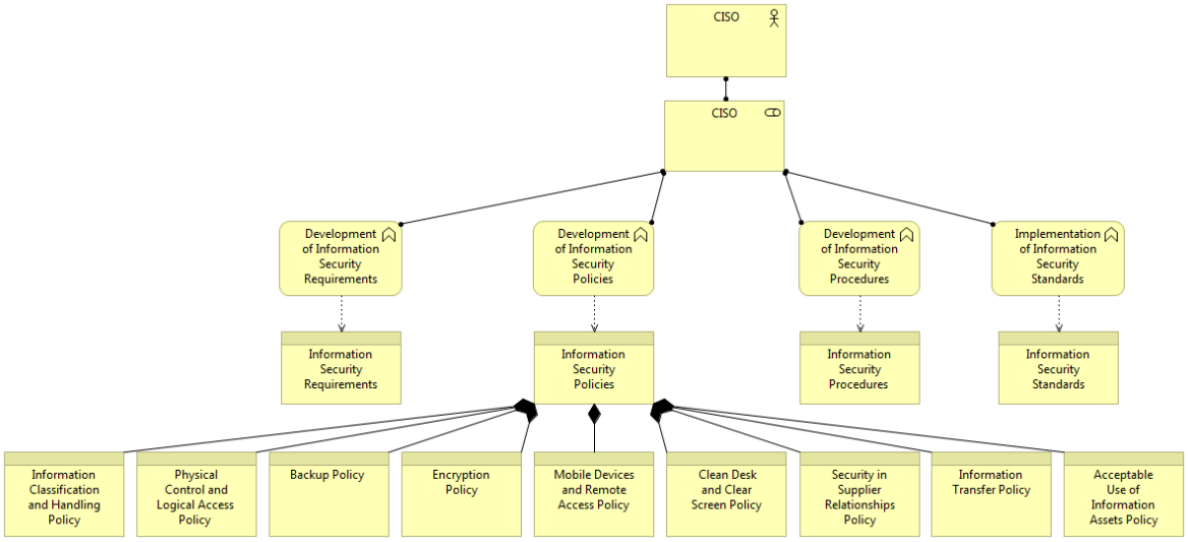


Figure 31 - DemoCorp's Business Functions and Information Types viewpoint

Then, following the proposed method, we model the process that is related to the processes represented in the previous section, for which the CISO is responsible. Figure 32 presents the artifact that shows the inputs, outputs, and roles responsible of the DemoCorp's Information Risk Management process in which the CISO is responsible for.

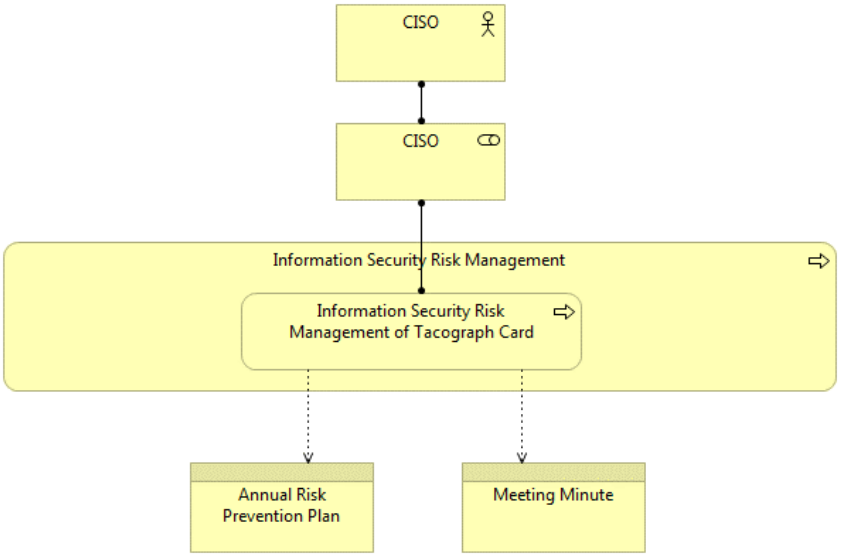


Figure 32 - DemoCorp's Information Security Risk Management Process viewpoint

Finally, we represented the existent organization's key practices, which are related to the key practices of COBIT 5 for Information Security for which the CISO is responsible (see Figure 33). When looking at the roles and practices assigned, it is possible to observe that the CISO is responsible for the development of information security requirements, policies and procedures. Moreover, we can observe that this role is responsible for some practices but is not the only role responsible for those practices.

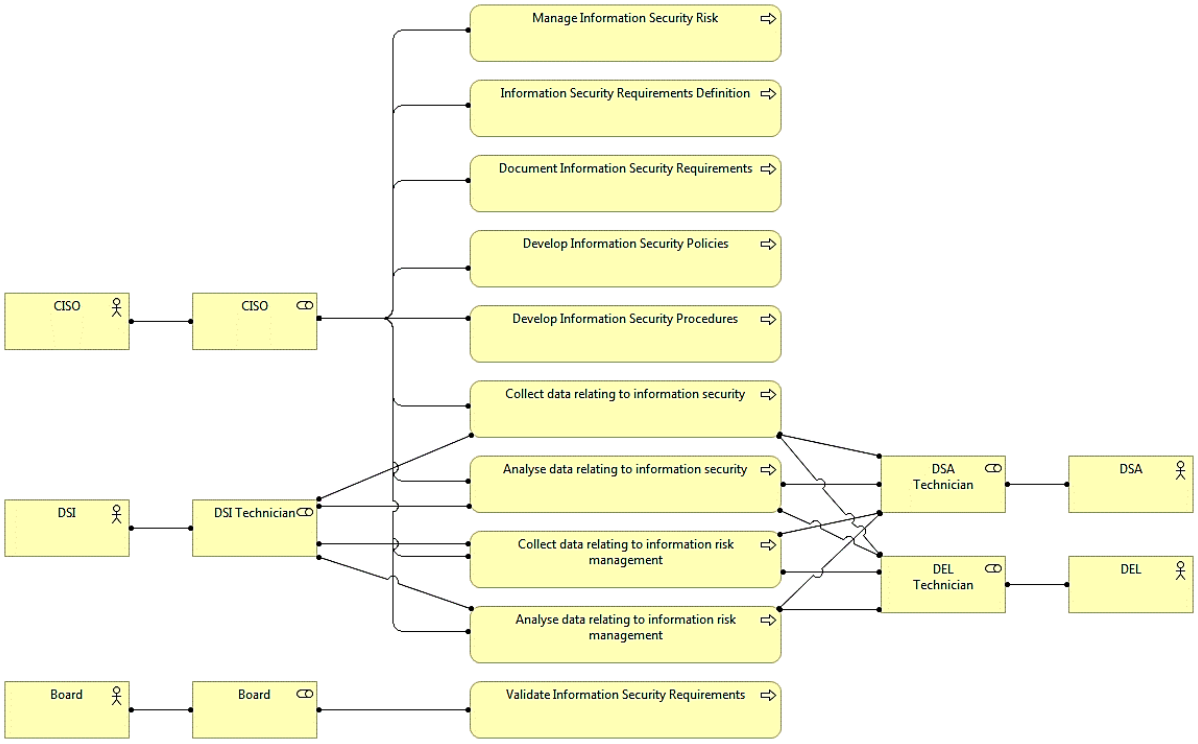


Figure 33 - DemoCorp's Key Practices viewpoint

In Appendix B, we present the DemoCorp Organizational Structure viewpoint that was designed based on the organization viewpoint.

As result of this step, the AS-IS of the organization's EA is modeled, taking into account the definition of CISO's role. Such representation will be the input to the next steps of the proposed method.

6.3. STEP 3 – Information Types' mapping

Regarding the solution proposal's third step, we map the existing DemoCorp to the desired COBIT 5 for Information Security's information types that should be originated by the CISO's role.

In order to have a better understanding of the information types that are being originated or are missing in the DemoCorp, we present two viewpoints. The first viewpoint (see Figure 34) shows the information types of COBIT 5 for Information Security which are originated in the organization, regarding the CISO's role. The second viewpoint (see Figure 35) shows the information types of COBIT 5 for Information Security which are not being originated in the organization.

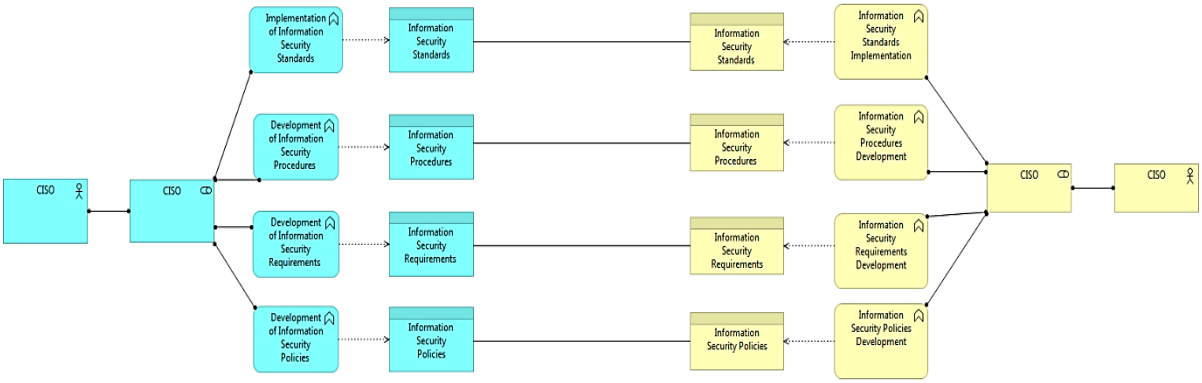


Figure 34 - DemoCorp to COBIT 5 for Information Security's Information Types viewpoint

When looking at this viewpoint, it is possible to identify which types of information are being originated and who is responsible for them in the organization. We can observe that the organization's information types, which are associated with those defined in COBIT 5 for Information Security, are part of the CISO's responsibility, so no one in the organization is performing the CISO's job.

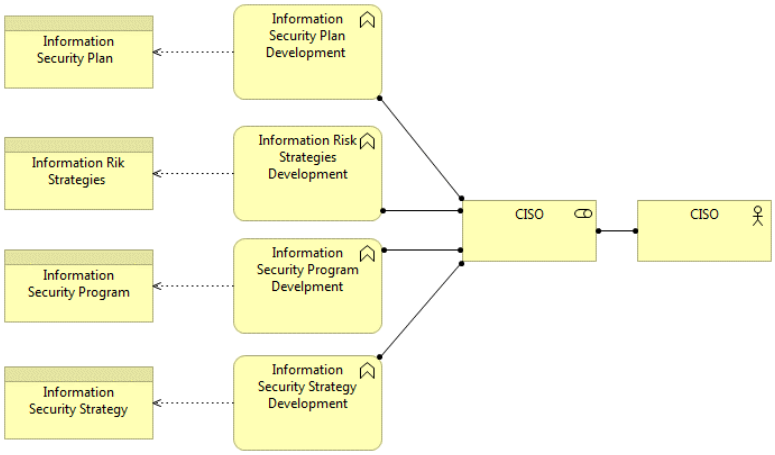


Figure 35 - DemoCorp to COBIT 5 for Information Security's Information Types Missing viewpoint

Figure 35 allows us to detect 4 information security gaps, since the information security plan, information risk strategies, information security program and information security strategy are not defined in the DemoCorp.

6.4. STEP 4 - Processes Outputs' mapping

As stated in Section 5, the fourth step's goal is to map the processes' outputs of the DemoCorp to the COBIT 5 for Information Security's processes that the CISO is responsible for.

Then, we present Figures 36, 37 and 38 in which we map the processes' outputs of the DemoCorp to the desired processes' outputs which the CISO is responsible to produce and/or deliver, defined in COBIT 5 for Information Security. With this, it is possible to identify which process' outputs are missing and who is delivering them, in order to know which role is performing the CISO's job.

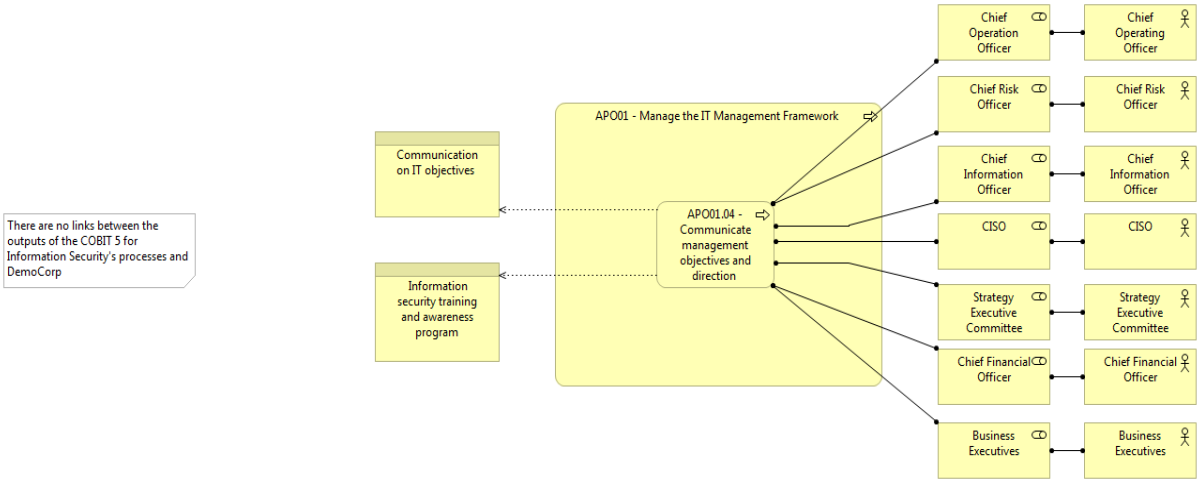


Figure 36 - DemoCorp to APO01 Manage the IT Management Framework Process viewpoint

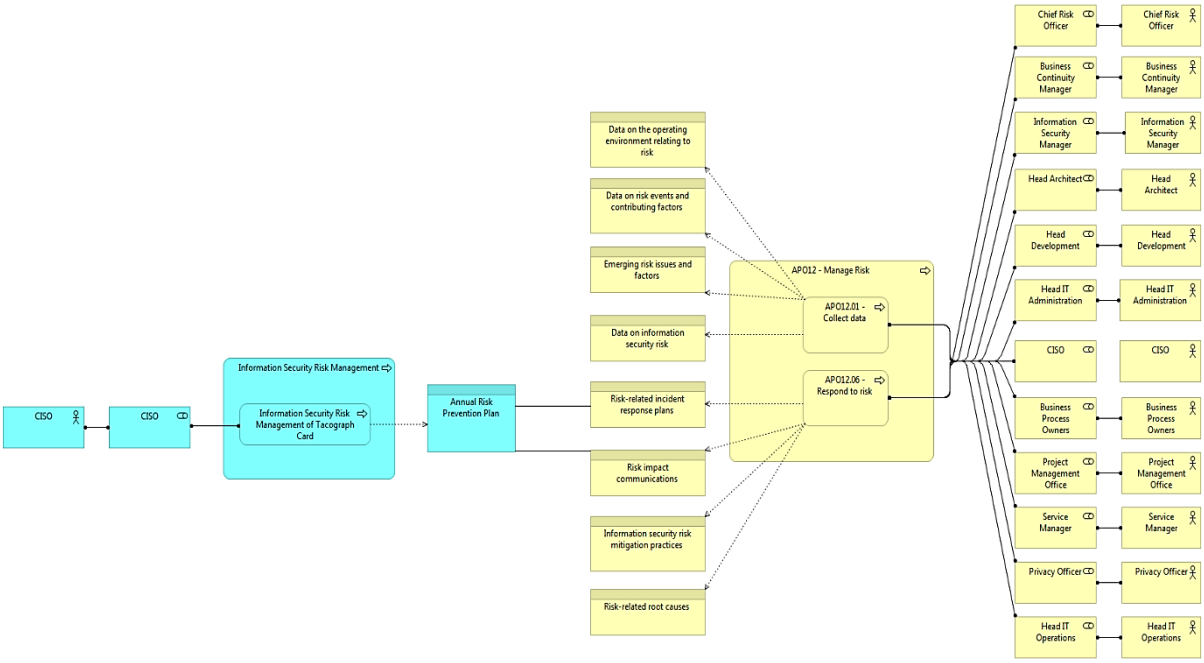


Figure 37 - DemoCorp to APO12 Manage Risk viewpoint

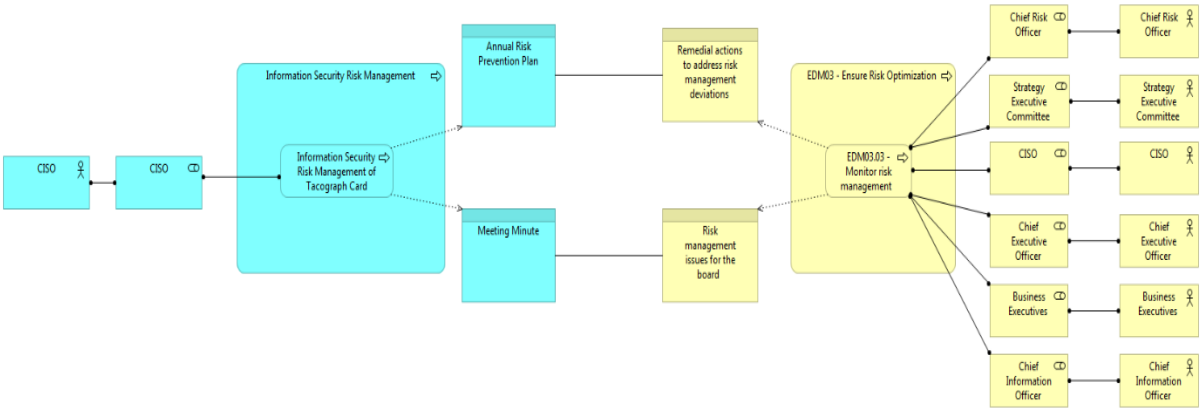


Figure 38 - DemoCorp to EDM03 Ensure Risk Optimization viewpoint

The viewpoints presented above allow us to detect 4 information security gaps, regarding the processes' outputs, which are:

- 2 information security gaps in Figure 36;
- 6 information security gaps in Figure 37;
- 0 information security gaps in Figure 38.

Figure 36 allows us to identify 2 information security gaps, since the outputs "Communication on IT objectives" and "Information security training and awareness program" are not delivered in the DemoCorp. Furthermore, Figure 37 presents 6 information security gaps, since the outputs "Data on the operating environment relating to risk", "Data on risk events and contributing factors", "Emerging risk issues and factors", "Data on information security risk", "Information security risk mitigation practices" and "Risk-related root causes" are not produced in the DemoCorp.

Besides that, we can observe that the processes' outputs of the organization, which are associated with those defined in COBIT 5 for Information Security, are part of the CISO's responsibility, so there is not any role that is doing the CISO's job.

6.5. STEP 5 - Key Practices' mapping

In this step, we represent the mapping of the organizations' practices to key practices defined in COBIT 5 for Information Security, which the CISO should be responsible for.

In order to better understand the practices that are being performed or are missing in the DemoCorp, we present two viewpoints. The first viewpoint (Figure 39) shows the key practices of COBIT 5 for Information Security which are defined in the organization. On the other hand, the second viewpoint (Figure 40) shows the key practices of COBIT 5 for Information Security which are not defined in the organization.

For that, we present the Figure 39 in which we map the organization's key practices to key practices that CISO should be held responsible for. To have a better understanding of the assignments between the roles and practices of DemoCorp, see Appendix C in which we present a table that contains the caption of this figure.

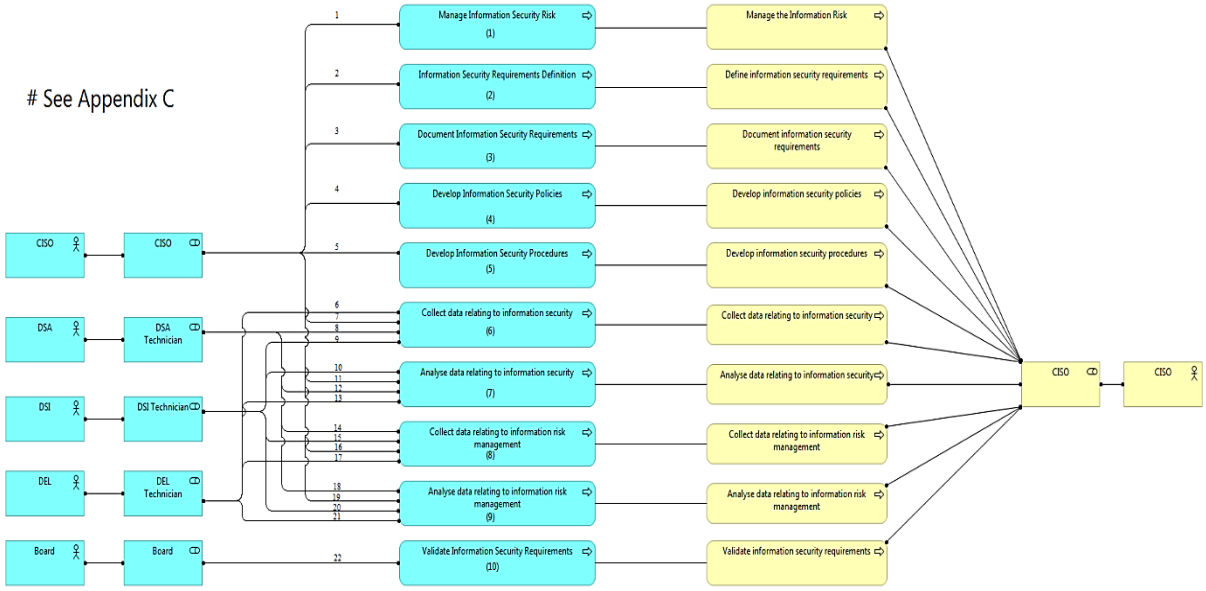


Figure 39 - DemoCorp to COBIT 5 for Information Security's Key Practices viewpoint

When looking at this viewpoint, it is possible to identify which key practices are being performed and who is responsible for them in the organization.

Furthermore, there are 4 DemoCorp's practices in which the CISO is responsible for, although he/she is not the only role that has responsibility for these practices. Moreover, the validation of information security requirements is part of the Board's responsibility, in which the CISO does not have responsibility in this organization's practice.

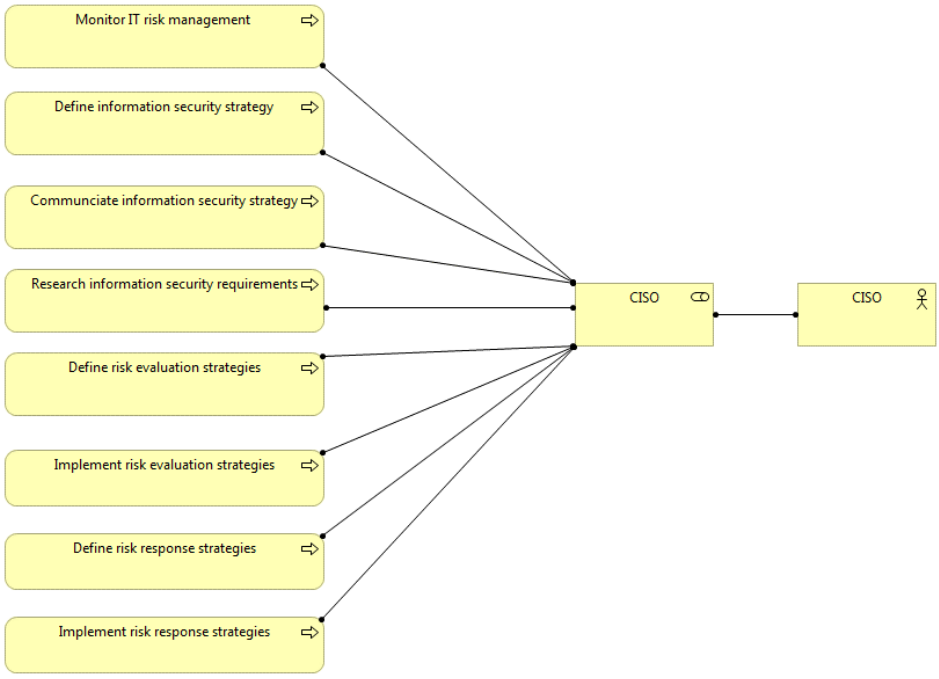


Figure 40 - DemoCorp to COBIT 5 for Information Security's Missing Practices viewpoint

This viewpoint (Figure 40) allows us to detect 8 information security gaps, regarding information security key practices in which the CISO should be held responsible for.

6.6. STEP 6 - Roles' mapping

As stated in Section 5, the sixth step's goal is to map the organization's roles to the CISO role defined in COBIT 5 for Information Security, in order to identify who is performing the CISO's job.

For that, Figure 41 presents the organization's roles which are doing the CISO's job, defined in COBIT 5 for Information Security.

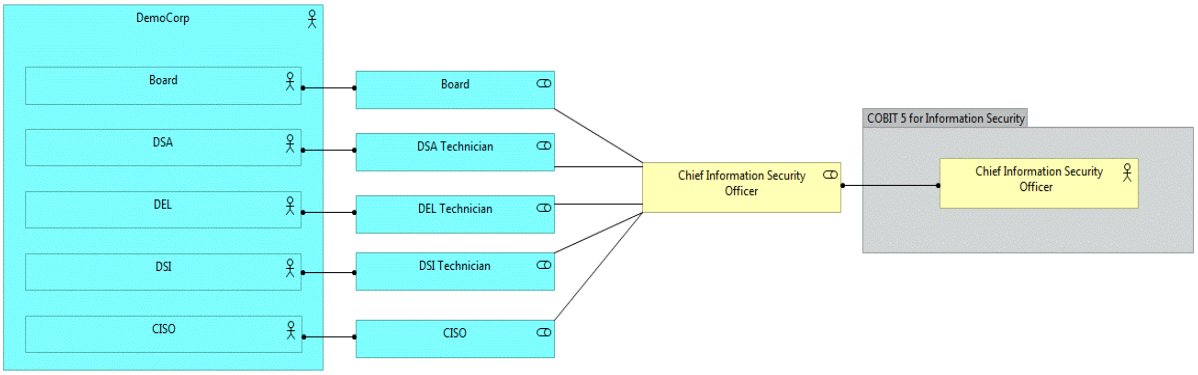


Figure 41 - DemoCorp to COBIT 5 for Information Security's Roles viewpoint

This viewpoint allows us to identify 4 DemoCorp's roles that are performing the CISO's role, which are:

- DSA Technician;
- DEL Technician;
- DSI Technician;
- Board.

All of the mappings presented in Steps 3, 4, 5 and 6 will be the input for the next step of the method.

6.7. STEP 7 - Analysis & TO-BE Design

We identified some information security gaps, such as missing of certain outputs that should have been produced and/or originated by the CISO's role. For example, from COBIT 5 the development of information security strategy does not have any connection to the DemoCorp's information types. These outputs are essential to any enterprise that has security as an essential part of their business. The absence of these concepts can negatively affect the business, i.e., information security does not create value for the organization.

Regarding what was described in Section 5, this step's goal is to design the TO-BE of the organization under review. For that, we present five viewpoints in order to enable a better understanding of what is being represented. These viewpoints focus on:

- Information Types;
- Key Practices.
- Outputs of Process APO01 - Manage the IT Management Framework;
- Outputs of Process APO12 - Manage Risk;
- Outputs of Process EDM03 - Ensure Risk Optimization.

These viewpoints represented follow the template shown in Section 5. In each viewpoint the following 4 plateaus are represented:

- COBIT 5 for Information Security, taking into account the types of information, key practices and processes' outputs of the CISO should be responsible (Step 1).
- AS-IS DemoCorp (baseline architecture), taking into account the types of information, processes' outputs and key practices shown in Step 2.
- TO-BE DemoCorp (transition architecture), which represents the transition architecture of the DemoCorp, with regard to the role of CISO in the organization. This architecture is designed based on the previous two plateaus. In addition, this architecture should be designed based on strategic decision made by DemoCorp that chose to follow the recommended actions for improvement provided in an INFOSEC IT Score, made by a consulting company (see Table 10). Such information security assessment was made in June 2015.
- TO-BE DemoCorp (target architecture), which represent the target of DemoCorp's architecture, based on the COBIT 5 for Information Security.

Furthermore, the 3 following gaps are represented as well:

- Gaps between the plateaus COBIT 5 for Information Security and the AS-IS of DemoCorp (baseline architecture), which identifies what types of information, key practices and processes' outputs that are not defined in the organization and, according to the COBIT 5 for Information Security, are part of the CISO's responsibilities in an organization.
- Gaps between the plateaus AS-IS and TO-BE of the DemoCorp (baseline and transition architecture), which identifies which information types, key practices and processes' outputs that will be part of the DemoCorp's transition architecture. Such selection was made based on the strategic decision of the organization.
- Gaps between the plateaus TO-BE DemoCorp (transition architecture) and TO-BE DemoCorp (target architecture) that identifies which information types, key practices and processes' outputs were not treated in transition architecture due to the strategic decision but will be treated in the DemoCorp's target architecture.

According to the IT Score made by the consulting company, DemoCorp has a lower maturity level than the average government organizations [2.5 vs. 2.8]. Furthermore, DemoCorp business focus suggests a maturity target similar to Financial Services organizations [Level 3].

The EA should be adapted to the organization and not the other way around. As such, the design of the transition architecture must be in accordance with the organization's business needs. As can be seen in the table below, not all the gaps identified are treated in the design of the DemoCorp's transition architecture, since the organization decided that only had to follow the recommendations of the IT Score. These recommendations aim to enable the organization to achieve the Level 3 of Information Security Maturity Level, in order to have a maturity level similar to that of the Financial Services organizations.

Table 10 - Information Security Gaps and Recommended Actions of the IT Score

Method	Information Security Gaps	Is it part of the recommended actions for improvement provided by the consulting company? (Yes/No)
STEP 3	Information Security Plan	**Yes**
	Information Risk Strategies	No
	Information Security Program	**Yes**
	Information Security Strategy	**Yes**
STEP 4	Communication on IT objectives	**Yes**
	Information security training and awareness program	**Yes**
	Data on the operating environment relating to risk	**Yes**
	Data on risk events and contributing factors	**Yes**
	Emerging risk issues and factors	**Yes**
	Data on information security risk	**Yes**
	Information security risk mitigation practices	No
	Risk-related root causes	No
STEP 5	Monitor IT risk management	**Yes**
	Define information security strategy	**Yes**
	Communicate information security strategy	**Yes**
	Research information security requirements	**Yes**
	Define risk evaluation strategies	No
	Implement risk evaluation strategies	No
	Define risk response strategies	No
	Implement risk response strategies	No

As can be seen in the table below, there are 6 recommended actions that DemoCorp should achieve in order to reach the Level 3 of information security maturity level. In order to follow the strategic decision made by the DemoCorp in which the definition of the CISO's role should follow these recommended actions, we mapped them with the information security gaps identified in the Steps 3, 4 and 5.

Table 11 - Mapping of IT Score's Recommended Actions to Information Security Gaps Identified

Recommended actions for improvement	Information Security Gaps	Method's Step (s)
Use published information security frameworks – for example, ISO 27001 and ISO 27002 – to develop a "desired state" vision of the security program, along with associated policies and practices.	Information Security Program	Step 3
	Information Security Strategy	
	Define information security strategy	Step 5
	Communicate information security strategy	
Develop a process catalog detailing security practices.	Monitor IT risk management	Step 5
	Define information security strategy	
	Communicate information security strategy	
	Research information security requirements	
Seek formally approved resources, including budget funds and personnel.	Information Security Plan	Step 3
Begin to formalize processes for cross-organizational communication and collaboration.	Communication on IT objectives	Step 4
	Data on the operating environment relating to risk	
	Data on risk events and contributing factors	
	Emerging risk issues and factors	
	Data on information security risk	
Establish an information security steering committee or working group. This should preferably be a high-level policy approval committee, with membership drawn from line-of-business managers.	None	None
Implement an enterprisewide communications program that focuses on ensuring that employees are aware, willing and able to comply with established security policies.	Information Security Plan	Step 3
	Information security training and awareness program	Step 4

Regarding all the information described above, we present the Figures 42, 43, 44 and 45 that represent the DemoCorp's transition and target architecture, regarding the information types in which the CISO is responsible to originate. Such division of the architecture by 4 viewpoints aims to improve the perception and understanding of the information provided in each of these viewpoints. For a complete view, see the viewpoint named Information Types TO-BE (Complete View), which is in the Appendix C "DemoCorp to COBIT 5 for Information Security Mapping".

Figure 42 represents the AS-IS of DemoCorp, represented by the plateau "AS-IS DemoCorp (baseline architecture)". This viewpoint presents the organization's information types and the types of information that, according to the COBIT 5 for Information Security, the CISO should be responsible for originating, represented in the plateau "COBIT 5 for Information Security". In addition to this mapping between the AS-IS of the organization's architecture and COBIT 5 for Information Security, this viewpoint also represents the information security gaps identified in Section 5, regarding the information types.

Based on what has been described previously (Tables 10 and 11), it was possible to represent the DemoCorp's transition architecture, represented in the plateau "TO-BE DemoCorp (transition architecture)". As can be seen in the "Gap: AS-IS DemoCorp (baseline) - TO-BE DemoCorp (transition)," only the information security gaps "Information Security Plan", "Information Security Program" and "Information Security Strategy" were considered for the transition architecture, according to the strategic decision made by the organization. Finally, the DemoCorp's target architecture will consider the type of information "Information Risk Strategies", which according to the COBIT 5 for Information Security the CISO is responsible to develop.

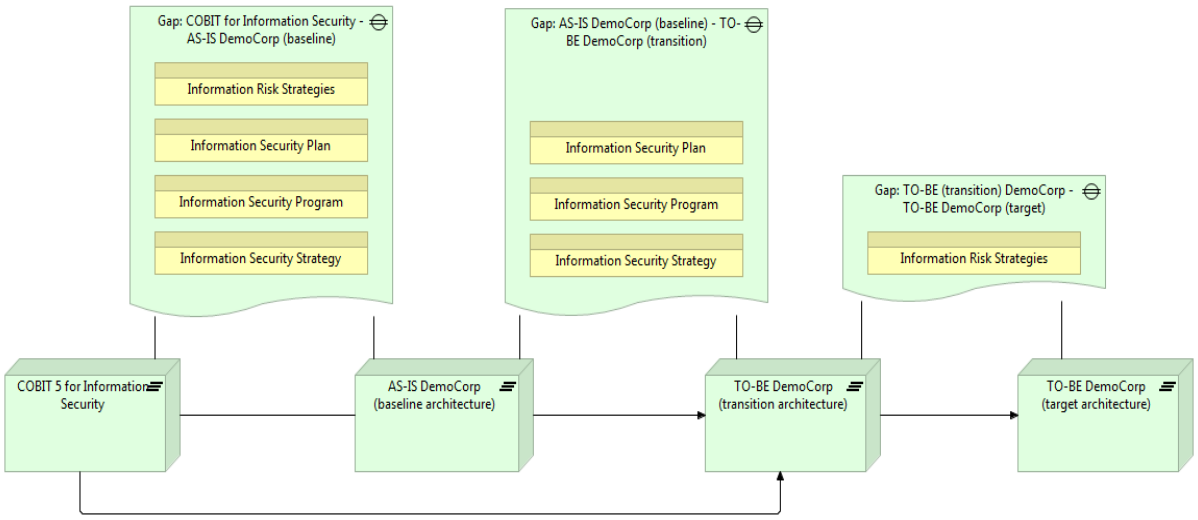


Figure 42 - Migration Viewpoint: Information Types (General)

As can be seen in the figure above, it only presents the gaps between each one of the plateaus. For a better understanding of what is represented in each one of the 4 plateaus, we present Figures 43, 44 and 45 in which the mapping between the DemoCorp's AS-IS and the COBIT 5 for Information Security, regarding the definition of the CISO's role is represented and, also, the design of the DemoCorp's TO-BE (transition and target architecture).

Note that:

- The blue color represents what is defined in DemoCorp;
- The yellow color represents what the COBIT 5 for Information Security defines what should be the responsibilities of the CISO's role;
- The gray color represents what is new, i.e., what will be defined according to the identified gaps.

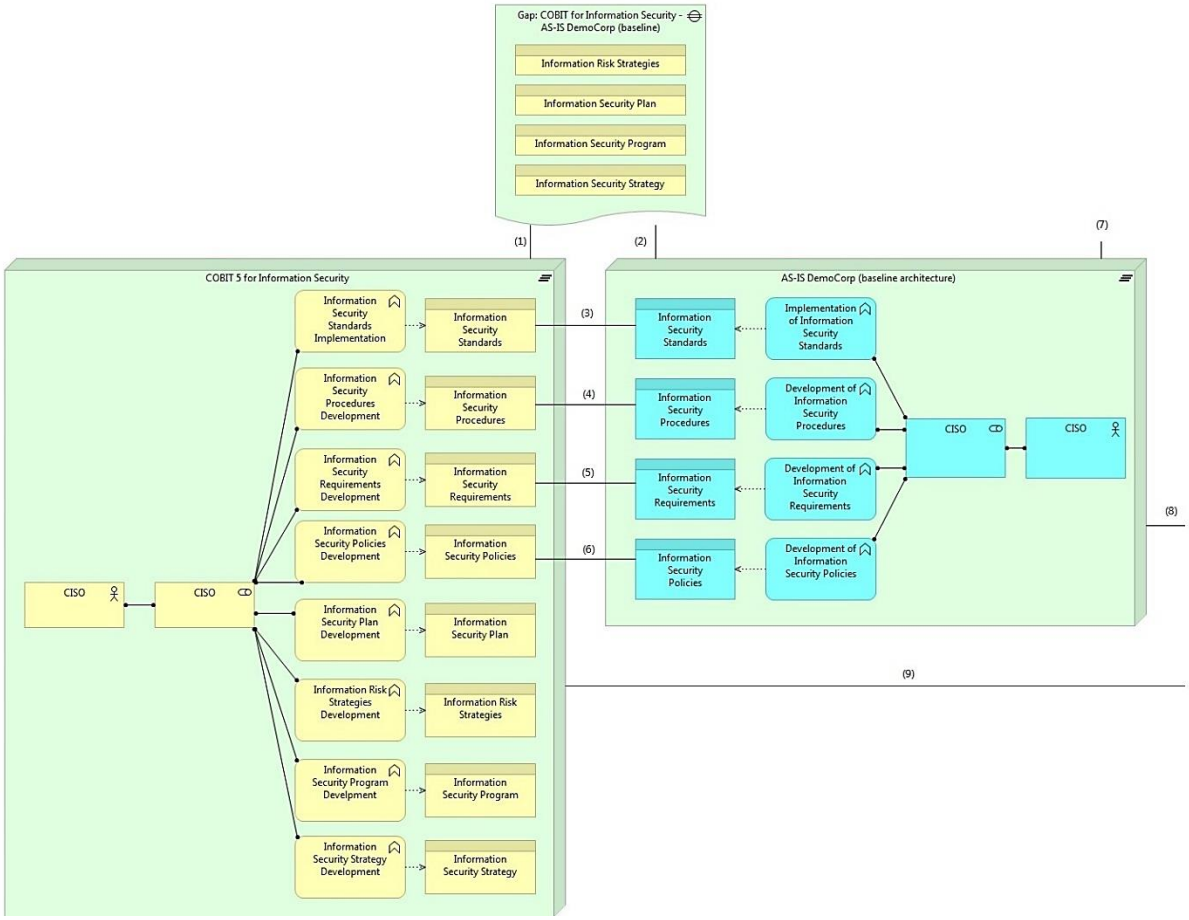


Figure 43 - Migration Viewpoint: Information Types (Part 1)

In the figure shown above, we can see that only the information types "Information Security Standards", "Information Security Procedures", "Information Security Requirements" and "Information Security Policies", presented in the COBIT 5 for Information Security, are defined in DemoCorp, and the CISO is responsible for originating them. The remaining information types are not defined in the organization, as can be seen by the absence of the relation "Association" between the business objects of plateaus "COBIT 5 for Information Security" and "AS-IS DemoCorp (baseline architecture)". Taking that into account the absence of this relation, we identified 4 gaps between the two plateaus previously described ("Information Risk Strategies", "Information Security Plan", "Information Security Program" and "Information Security Strategy").

Figure 44 shows the plateaus "AS-IS DemoCorp (baseline architecture)" and "TO-BE DemoCorp (transition architecture)" and the gaps between them. As can be seen, between the baseline and transition architecture 3 gaps were identified ("Information Security Plan", "Information Security Program" and "Information Security Strategy"). On the plateau of the transition architecture new responsibilities were added to the CISO's role in DemoCorp, i.e., the CISO will be responsible for originating the information types: "Information Security Plan", "Information Security Program" and "Information Security Strategy"; based on the strategic decision stated previously. Note that the design of the plateau "TO-BE DemoCorp (transition architecture)" is based on the analysis of plateaus "COBIT 5 for Information Security "and" AS-IS DemoCorp (baseline architecture)".

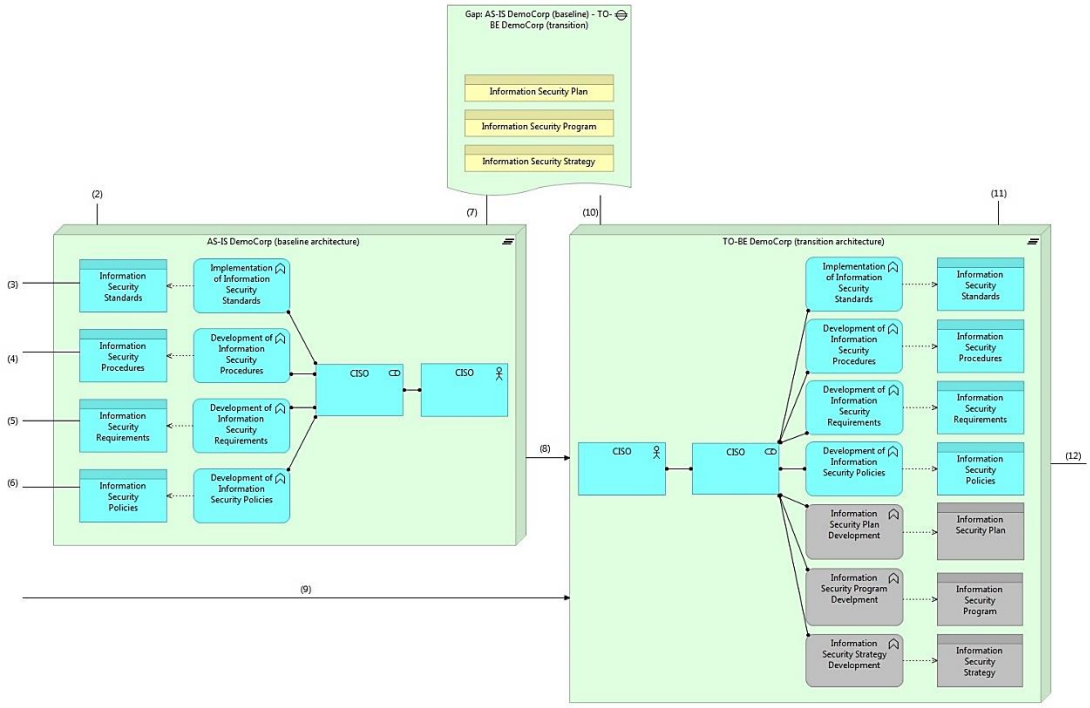


Figure 44 - Migration Viewpoint: Information Types (Part 2)

In the figure shown below are presented the transition and target architectures of the DemoCorp regarding the definition of CISO's role are represented. Between these plateaus one gap was identified, since DemoCorp decided that the CISO should be responsible for originating "Information Risk Strategies", so the responsibilities of the CISO's role of the DemoCorp will be aligned with the responsibilities defined in the COBIT 5 for Information Security.

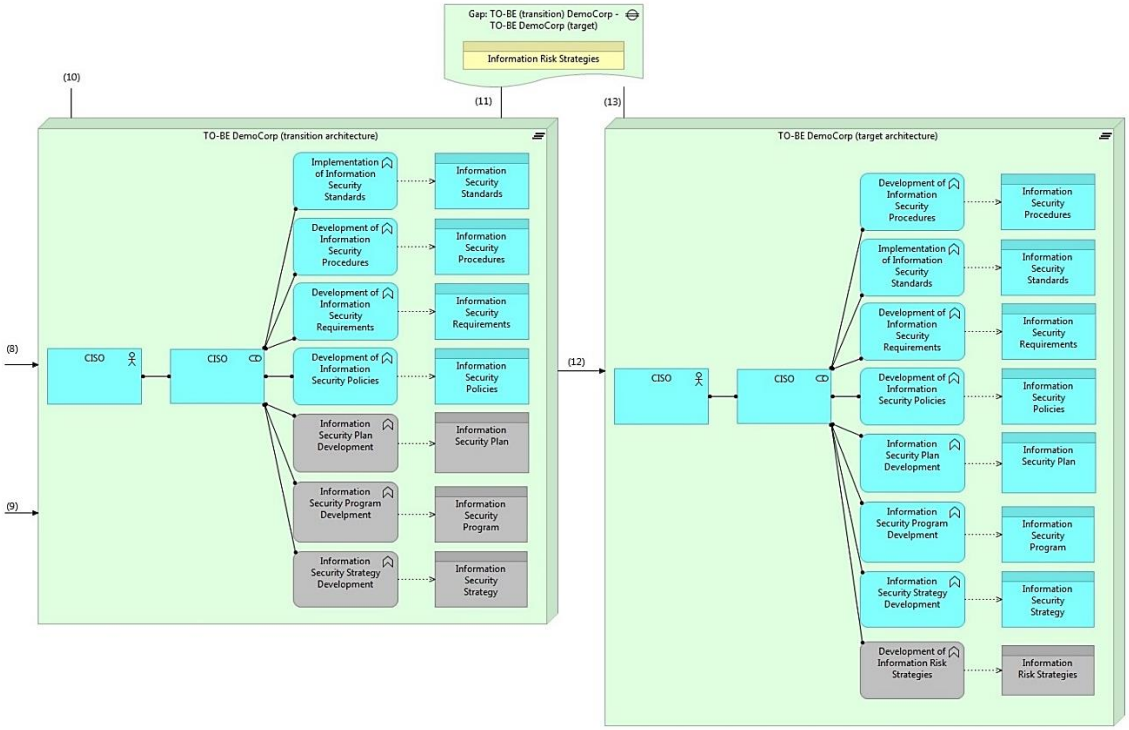


Figure 45 - Migration Viewpoint: Information Types (Part 3)

Regarding the key practices that the CISO should be held responsible for, Figure 46 represents the AS-IS of DemoCorp, represented by the plateau "AS-IS DemoCorp (baseline architecture)", taking that into account the organization's practices and the key practices that, according to the COBIT 5 for Information Security, the CISO should be held responsible for, represented in the plateau "COBIT 5 for Information Security". In addition to this mapping between the AS-IS of the organization's architecture and COBIT 5 for Information Security, this viewpoint also represents the information security gaps identified in Section 5, regarding these key practices.

Based on what has been described in the previous tables (see Tables 10 and 11), it was possible to represent the DemoCorp's transition architecture, represented in the plateau "TO-BE DemoCorp (transition architecture)". As can be seen in the "Gap: AS-IS DemoCorp (baseline) - TO-BE DemoCorp (transition)," only the information security gaps "Monitor IT risk management", "Define information security strategy", "Communicate information security strategy" and "Research information security requirements" were considered for the transition architecture, according to the strategic decision made by the organization. Finally, the DemoCorp's target architecture will consider the key practices "Define risk evaluation strategies", "Implement risk evaluation strategies", "Define risk response strategies" and "Implement risk response strategies", which according to the COBIT 5 for Information Security the CISO is responsible for.

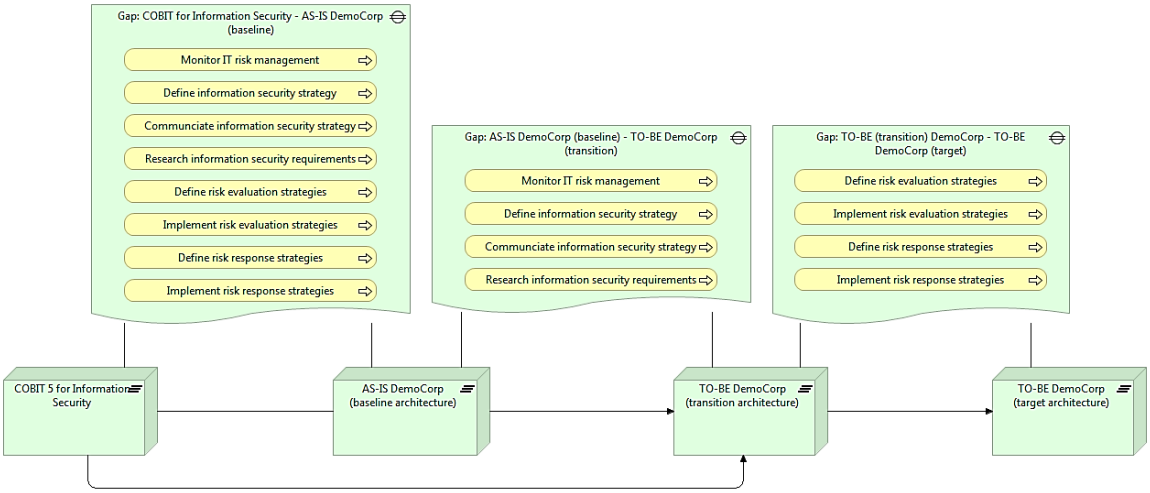


Figure 46 - Migration Viewpoint: Key Practices (General)

As can be seen in the figure above, it only presents the gaps between each one of the plateaus, regarding the key practices. For a better understanding of what is represented in each one of the 4 plateaus, we present Figures 47, 48 and 49 in which there are represented the mapping between the DemoCorp's AS-IS and the COBIT 5 for Information Security and, also, the design of the DemoCorp's TO-BE (transition and target architecture), regarding the key practices in which the CISO should be held responsible for. For a complete view, see the viewpoint named Key Practices (Complete View), which is in the Appendix C "DemoCorp to COBIT 5 for Information Security Mapping".

In the figure shown below, it can be seen that not all of the key practices, presented in the COBIT 5 for Information Security, are defined in DemoCorp in which the CISO should be held responsible for. Such

gaps can be seen by the absence of the relation "Association" between the business processes of plateaus "COBIT 5 for Information Security" and "AS-IS DemoCorp (baseline architecture)". This absence of relation between the two plateaus allow us to identify 8 gaps between the two plateaus previously described. To a better understanding of the assignments between the roles and practices of DemoCorp, see Appendix C in which we present Table 12 that contains the caption of this figure.

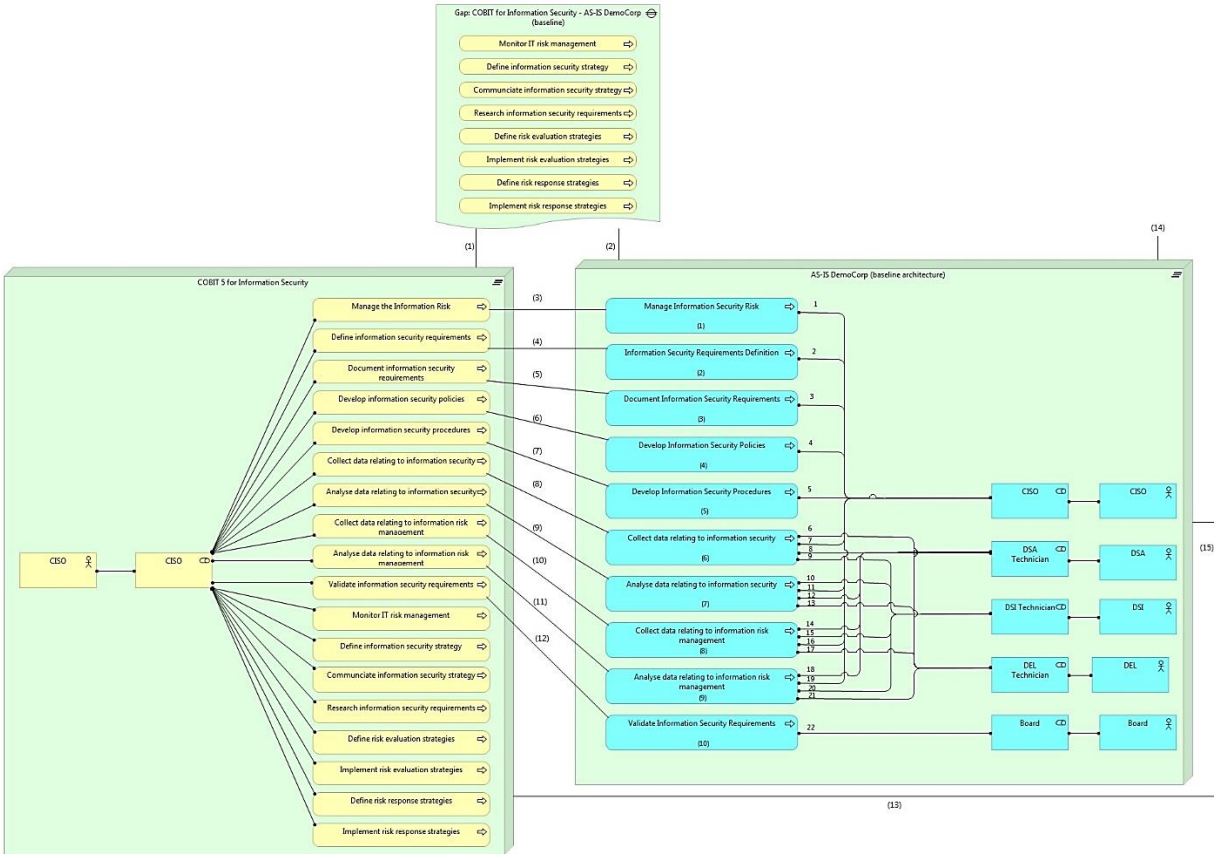


Figure 47 - Migration Viewpoint: Key Practices (Part 1)

Figure 48 shows the plateaus "AS-IS DemoCorp (baseline architecture)" and "TO-BE DemoCorp (transition architecture)" and the gaps between them. As can be seen, between the baseline and transition architecture 4 gaps were identified. On the plateau of the transition architecture new responsibilities were added to the CISO's role in DemoCorp, i.e., the CISO will be responsible for the practices: "Monitor IT risk management", "Define information security strategy", "Communicate information security strategy" and "Research information security requirements"; based on the strategic decision stated previously. Note that the design of the plateau "TO-BE DemoCorp (transition architecture)" is based on the analysis of plateaus "COBIT 5 for Information Security "and" AS-IS DemoCorp (baseline architecture)".

Moreover, Figure 49 presents the transition and target architectures of the DemoCorp, regarding the definition of the CISO's role. Between these plateaus 4 gaps were identified, since DemoCorp decided that the CISO should be held responsible for the practices "Define risk evaluation strategies", "Implement risk evaluation strategies", "Define risk response strategies" and "Implement risk response strategies",

so the responsibilities of the CISO's role of the DemoCorp will be aligned with the responsibilities defined in the COBIT 5 for Information Security.

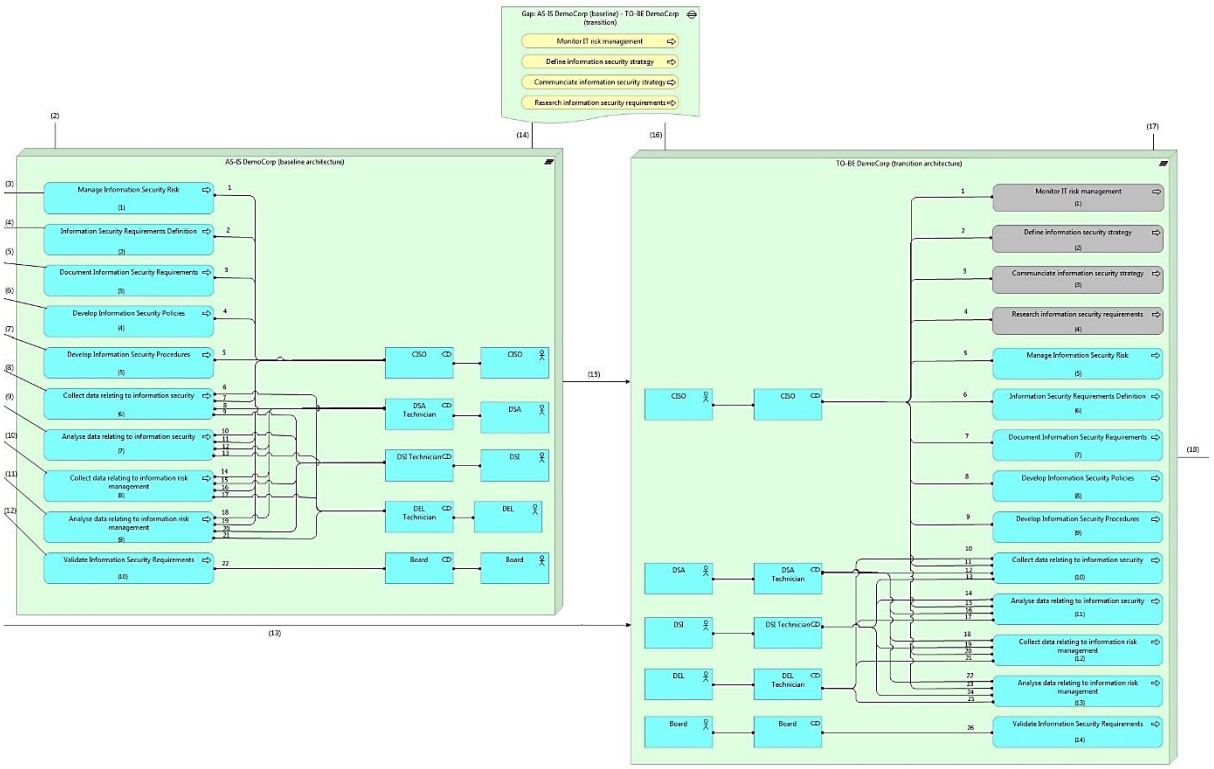


Figure 48 - Migration Viewpoint: Key Practices (Part 2)

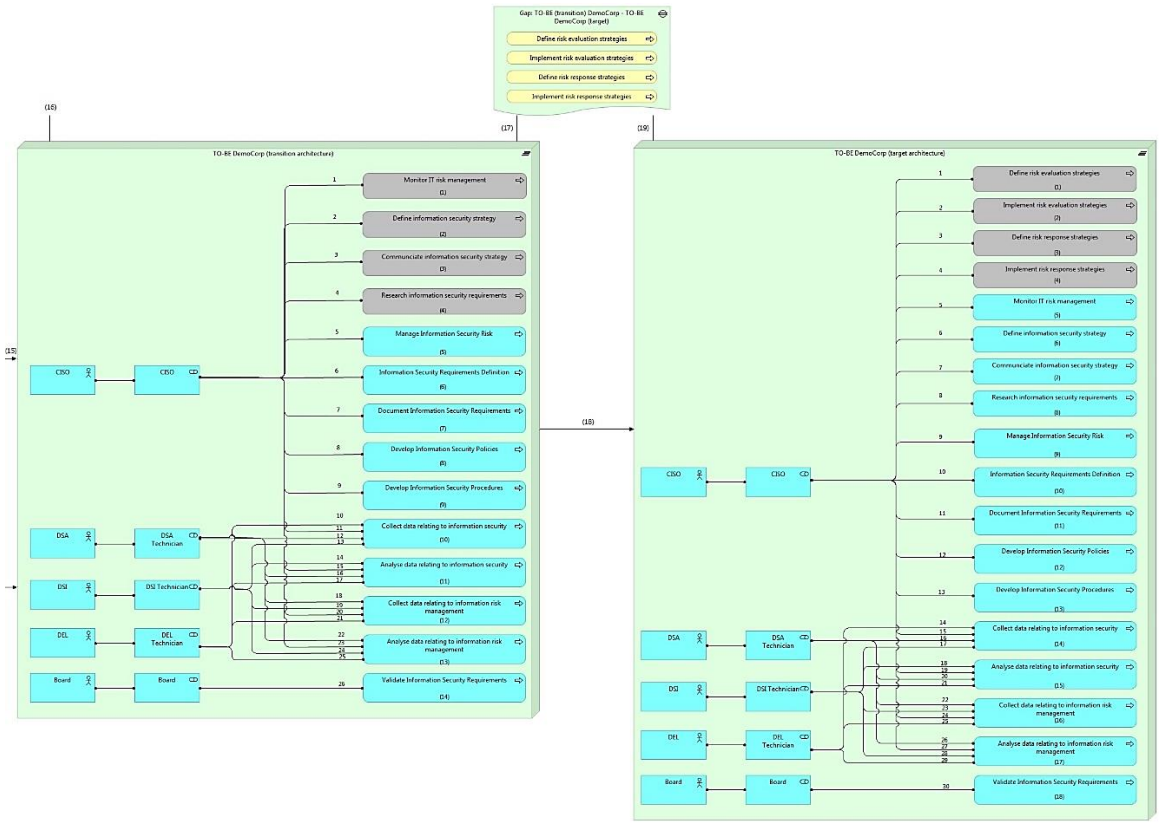


Figure 49 - Migration Viewpoint: Key Practices (Part 3)

In order to better understand the assignments between the roles and practices of DemoCorp, see Appendix C in which we present Tables 12, 13 and 14 that contains the caption of these figures.

Figure 50 represents the AS-IS of DemoCorp, represented by the plateau "AS-IS DemoCorp (baseline architecture)". The processes' outputs of the organization and the outputs of the APO01 Process are designed in this viewpoint in which, according to the COBIT 5 for Information Security, the CISO should be responsible for producing (represented in the plateau "COBIT 5 for Information Security").

Furthermore, this viewpoint represents the information security gaps identified in Section 5, regarding the APO01 process's outputs. Based on what has been described previously, it was possible to represent the DemoCorp's transition architecture, represented in the plateau "TO-BE DemoCorp (transition architecture)". As can be seen in the "Gap: AS-IS DemoCorp (baseline) - TO-BE DemoCorp (transition)," the information security gaps "Communication on IT objectives" and "Information security training and awareness program" were considered for the transition architecture, according to the strategic decision made by the organization.

Since all of the information security gaps were considered for the transition architecture (based on the strategic decision), we can observe that there are no gaps between the plateaus "TO-BE DemoCorp (transition architecture)" and "TO-BE DemoCorp (target architecture)".

For a complete view, see the viewpoint named APO01 Process's Outputs (Complete View), which is in the Appendix C.

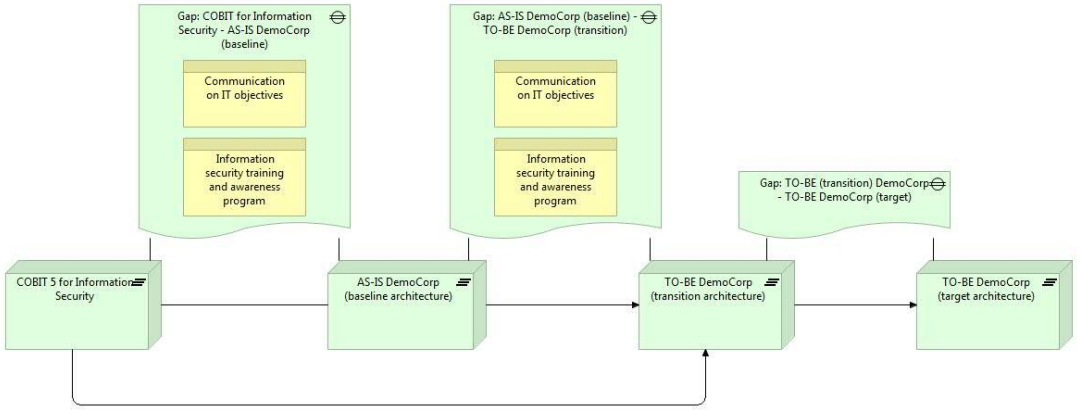


Figure 50 - Migration Viewpoint: APO01 Process's Outputs (General)

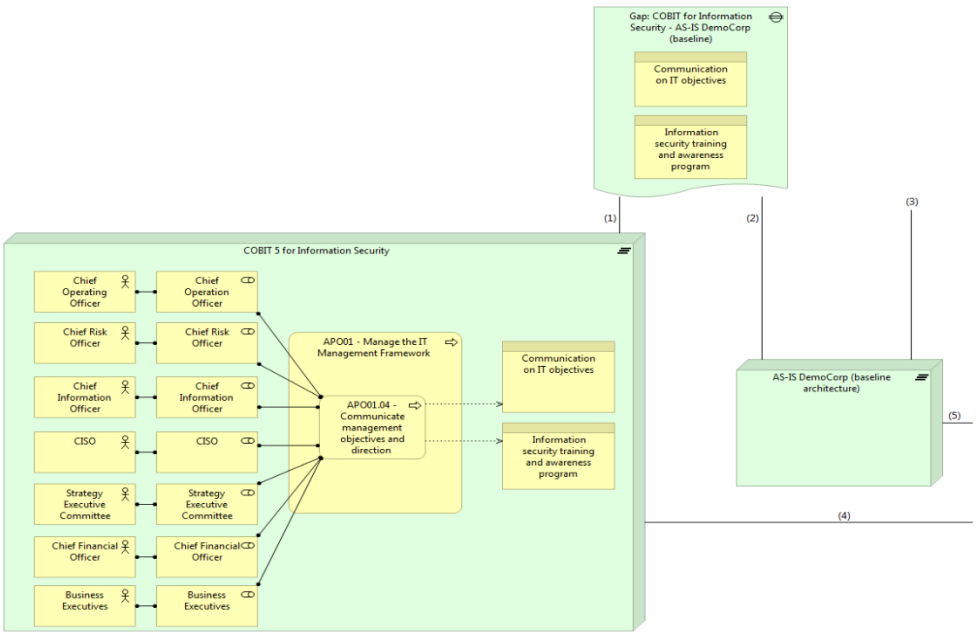


Figure 51 - Migration Viewpoint: APO01 Process's Outputs (Part 1)

In the Figure 51, it can be seen that the outputs "Communication on IT objectives" and "Information security training and awareness program", presented in the COBIT 5 for Information Security, are not defined in DemoCorp, so the CISO is not responsible for producing them, as can be seen by the absence of the relation "Association" between the business objects of plateaus "COBIT 5 for Information Security" and "AS-IS DemoCorp (baseline architecture)". The absence of this relation allows us to identify 2 gaps between the two plateaus previously described ("Communication on IT objectives" and "Information security training and awareness program").

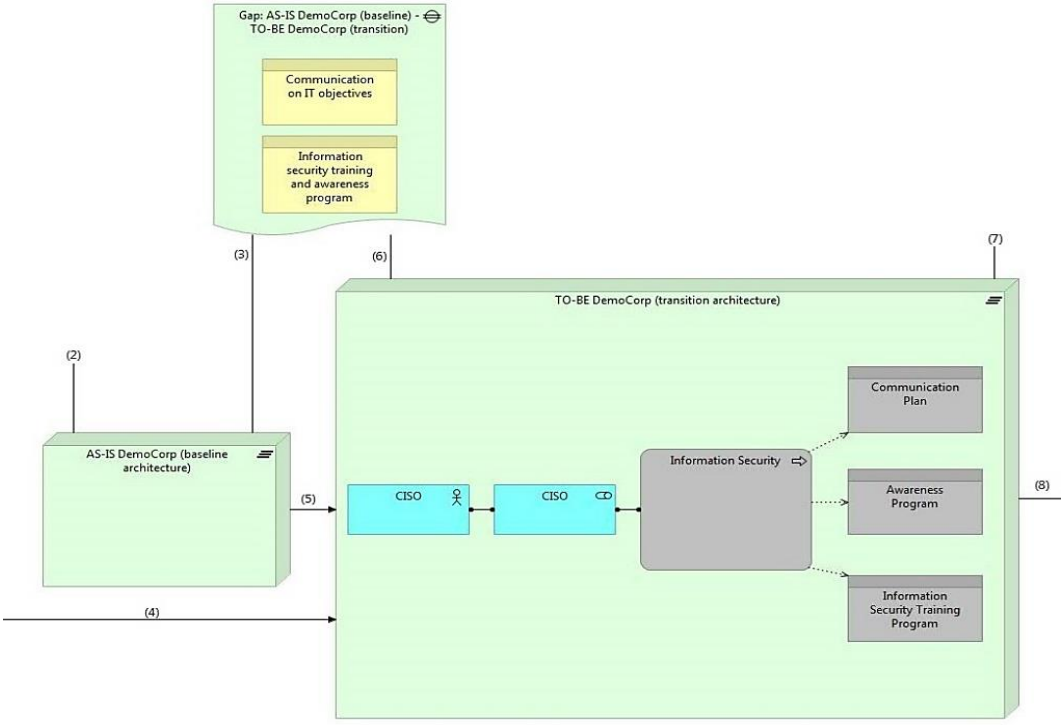


Figure 52 - Migration Viewpoint: APO01 Process's Outputs (Part 2)

Figure 52 shows the plateaus "AS-IS DemoCorp (baseline architecture)" and "TO-BE DemoCorp (transition architecture)" and the gaps between them. As can be seen, between the baseline and transition architecture 2 gaps were identified. On the plateau of the transition architecture new responsibilities were added to the CISO's role in DemoCorp, i.e., the CISO will be responsible for the new Information Security's process in which should produce the outputs "Communication Plan", "Awareness Program" and "Information Security Training Program"; based on the strategic decision described previously. Note that the design of the plateau "TO-BE DemoCorp (transition architecture)" is based on the analysis of plateaus "COBIT 5 for Information Security "and" AS-IS DemoCorp (baseline architecture)".

In the figure shown below we present the transition and target architectures of the DemoCorp, regarding outputs of the process "Information Security" in which the CISO is responsible for. Between these plateaus there are not information security gaps, since the organization decided that the transition architecture should consider all of APO01 process's outputs defined in COBIT 5 for Information Security, in which the CISO is responsible to produce these outputs.

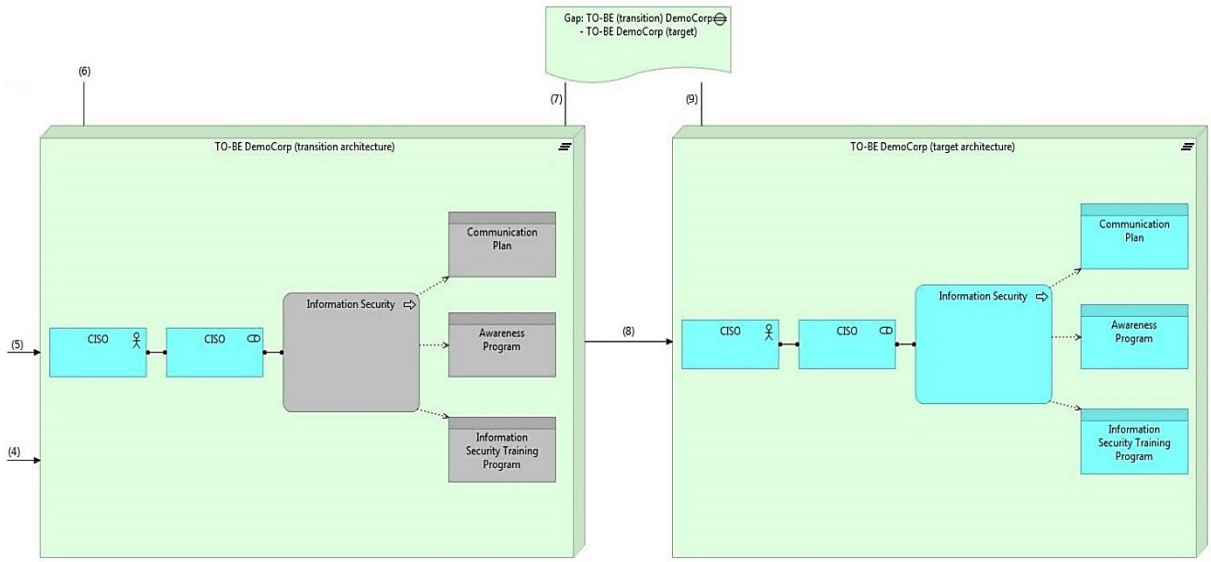


Figure 53 - Migration Viewpoint: APO01 Process's Outputs (Part 3)

Regarding the APO12 process's outputs in which the CISO is responsible for, Figure 54 represents the AS-IS of DemoCorp, represented by the plateau "AS-IS DemoCorp (baseline architecture)", taking that into account the organization's outputs and the APO12 process's outputs that, according to the COBIT 5 for Information Security, the CISO should be held responsible for, represented in the plateau "COBIT 5 for Information Security".

Moreover, this viewpoint represents the information security gaps identified in Section 5, regarding these process's outputs. Based on what has been described in the previous tables (Tables 10 and 11), it was possible to represent the DemoCorp's transition architecture, represented in the plateau "TO-BE DemoCorp (transition architecture)".

As can be seen in the "Gap: AS-IS DemoCorp (baseline) - TO-BE DemoCorp (transition)," only the information security gaps “Data on the operating environment relating to risk”, “Data on risk events and contributing factors”, “Emerging risk issues and factors” and “Data on information security risk” were considered for the transition architecture, according to the strategic decision made by the DemoCorp. The DemoCorp’s target architecture will consider the outputs "Information security risk mitigation practices" and “Risk-related root causes”, which according to the COBIT 5 for Information Security the CISO is responsible for producing.

For a complete view, see the viewpoint named APO12 Process’s Outputs (Complete View), which is in the Appendix C.

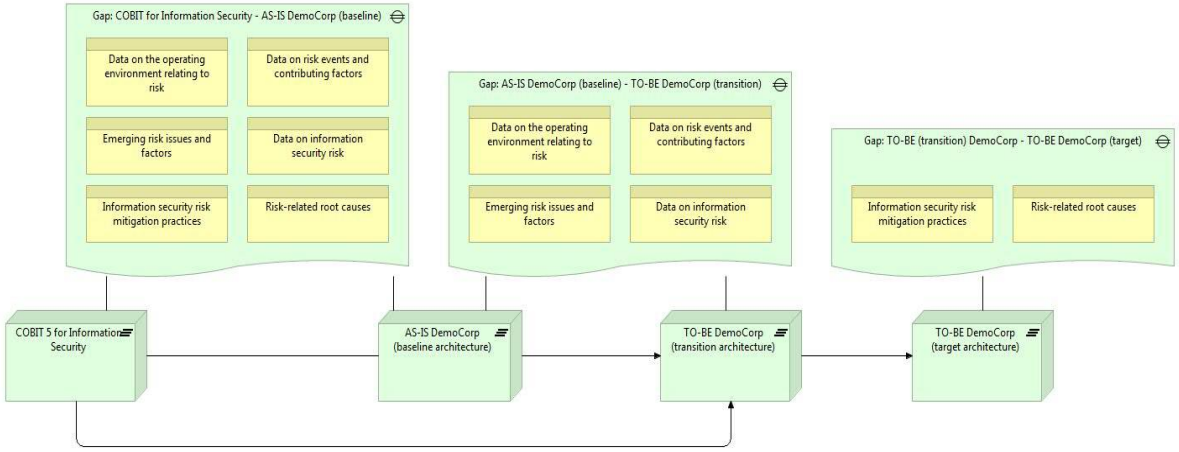


Figure 54 - Migration Viewpoint: APO12 Process’s Outputs (General)

In the Figure 55, we can gauge that 6 outputs, listed in the COBIT 5 for Information Security, are not defined in the organization, so the CISO is not responsible for deliver them, as can be seen by the absence of the relation "Association" between the business objects of plateaus "COBIT 5 for Information Security" and "AS-IS DemoCorp (baseline architecture)”. The absence of this relation allows us to identify 6 information security gaps between the two plateaus previously described (“Data on the operating environment relating to risk”, “Data on risk events and contributing factors”, “Emerging risk issues and factors”, “Data on information security risk”, "Information security risk mitigation practices" and “Risk-related root causes”).

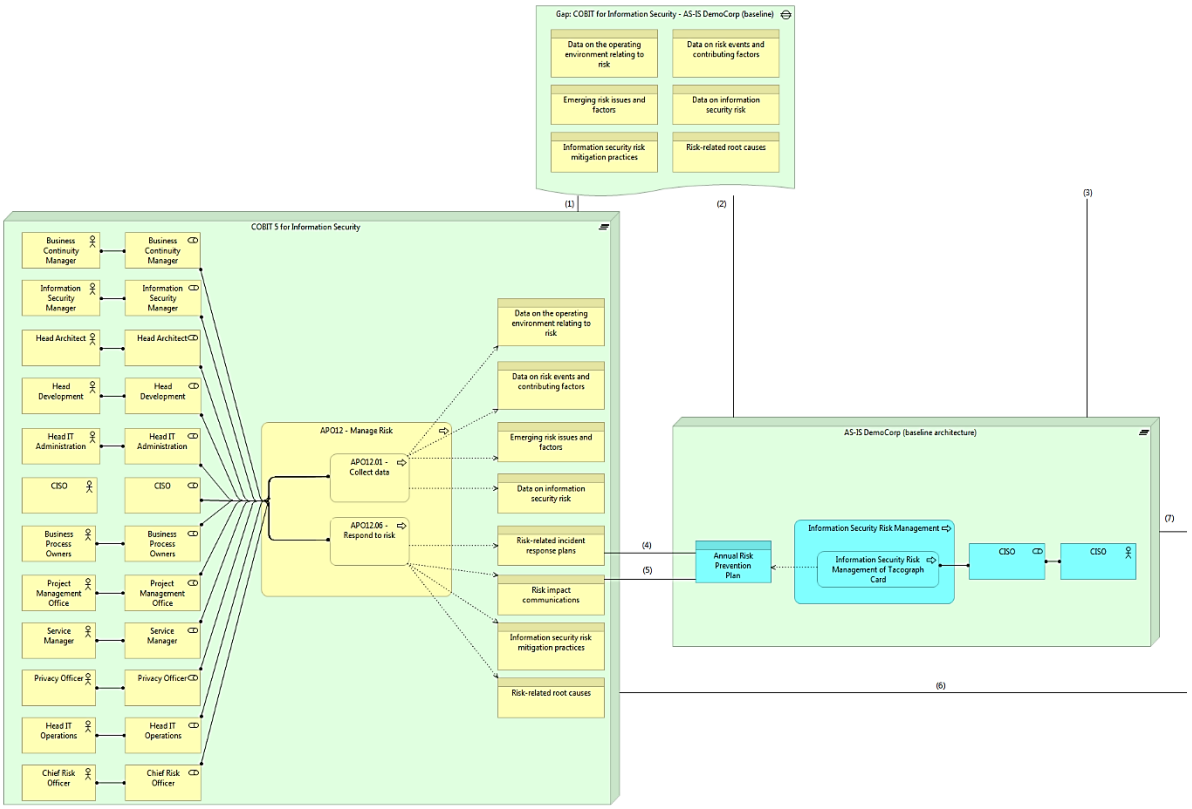


Figure 55 - Migration Viewpoint: APO12 Process's Outputs (Part 1)

Figure 56 shows the plateaus "AS-IS DemoCorp (baseline architecture)" and "TO-BE DemoCorp (transition architecture)" and the gaps between them. As can be seen, between the baseline and transition architecture 4 gaps were identified. On the plateau of the transition architecture new responsibilities were added to the CISO's role in DemoCorp, i.e., the CISO will be responsible for the new Information Security's process in which should produce the outputs "Data on the operating environment relating to risk", Emerging risk issues and factors", "Data on information security risk" and "Data on risk events and contributing factors"; based on the strategic decision described previously. Note that the design of the plateau "TO-BE DemoCorp (transition architecture)" is based on the analysis of plateaus "COBIT 5 for Information Security "and" AS-IS DemoCorp (baseline architecture)".

As can be seen in Figure 57, we present the transition and target architectures of the DemoCorp, regarding the outputs of the processes "Information Security" and "Information Security Risk Management" in which the CISO is responsible for. Between these plateaus there are 2 gaps, since DemoCorp decided that the CISO should be responsible for producing the outputs "Information security risk mitigation practices" and "Risk-related root causes", so the responsibilities of the CISO's role of the organization will be aligned with the responsibilities defined in the COBIT 5 for Information Security.

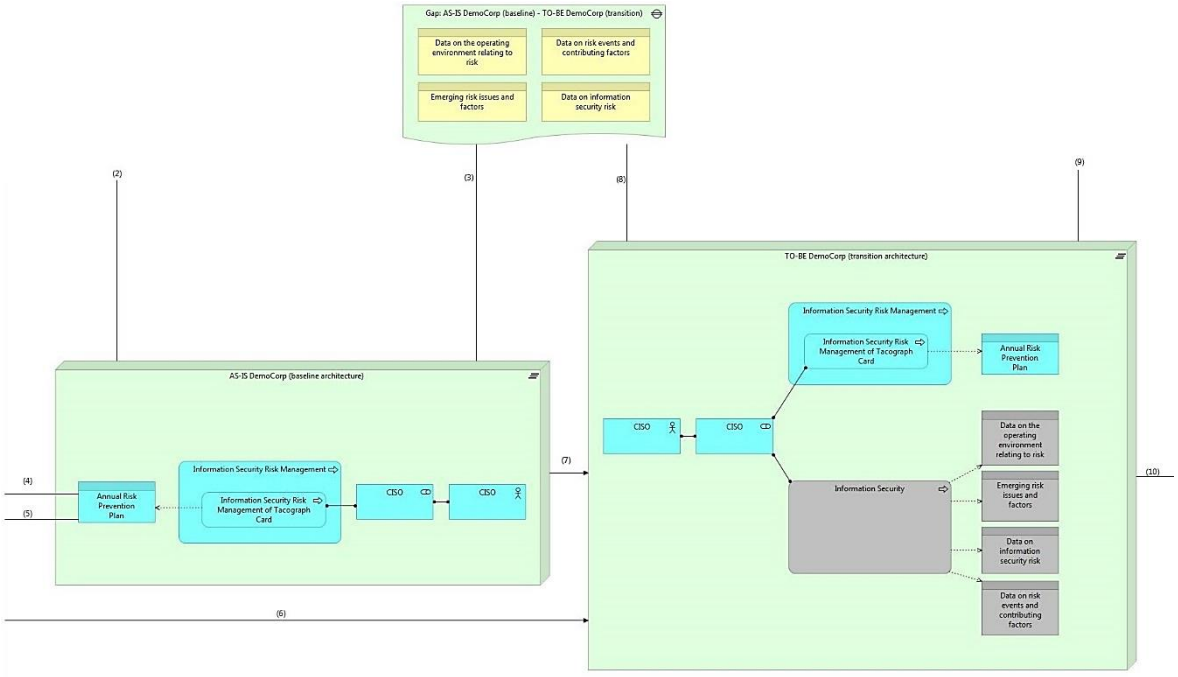


Figure 56 - Migration Viewpoint: APO12 Process's Outputs (Part 2)

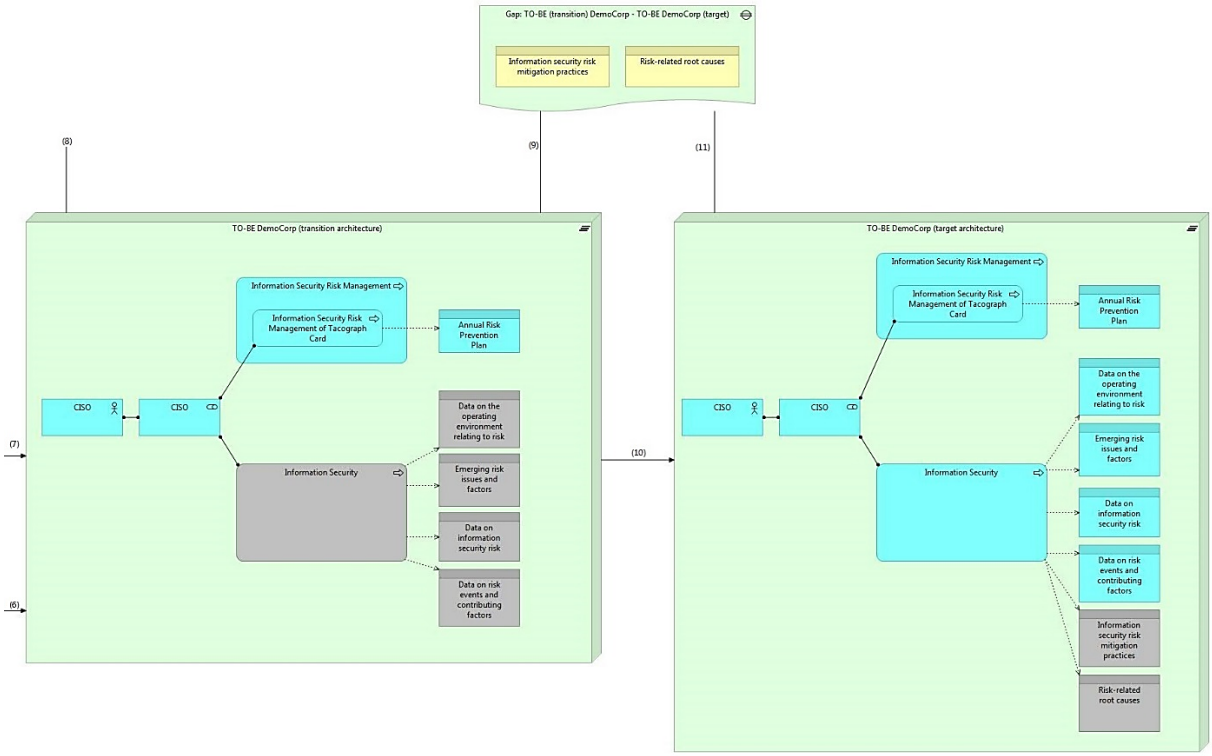


Figure 57 - Migration Viewpoint: APO12 Process's Outputs (Part 3)

Regarding the EDM03 process's outputs in which the CISO is responsible for, Figure 58 represents the AS-IS of DemoCorp, represented by the plateau "AS-IS DemoCorp (baseline architecture)", taking that into account the organization's outputs and the EDM03 process's outputs that, according to the COBIT 5 for Information Security, the CISO should be held responsible for producing, represented in the plateau "COBIT 5 for Information Security".

In addition, this viewpoint shows the information security gaps identified in Section 5, regarding these process's outputs. Based on what has been described in the previous tables (Tables 10 and 11), it was possible to represent the DemoCorp's transition architecture, represented in the plateau "TO-BE DemoCorp (transition architecture)".

As can be seen in the "Gap: AS-IS DemoCorp (baseline) - TO-BE DemoCorp (transition)," there are no information security gaps between the plateaus "COBIT 5 for Information Security" and "AS-IS DemoCorp (baseline architecture)", so, according to what is defined in the COBIT 5 for Information Security, the CISO of the DemoCorp is responsible to produce all of the EDM03 process's outputs.

For a better understanding, see the viewpoint named EDM03 Process's Outputs (Complete View), which is in the Appendix C.

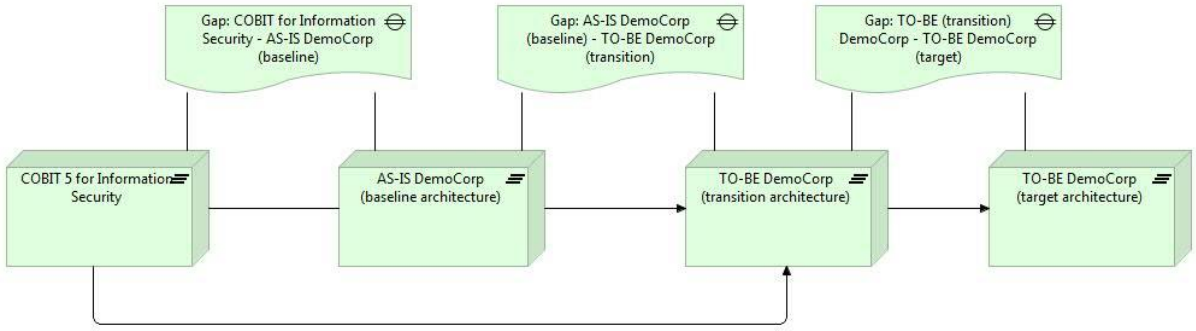


Figure 58 - Migration Viewpoint: EDM03 Process's Outputs (General)

In the Figure 59, it can be seen that the 2 process's outputs, listed in the COBIT 5 for Information Security, are defined in the organization, so the CISO is responsible for producing them, as can be seen by the relation "Association" between the business objects of plateaus "COBIT 5 for Information Security" and "AS-IS DemoCorp (baseline architecture)".

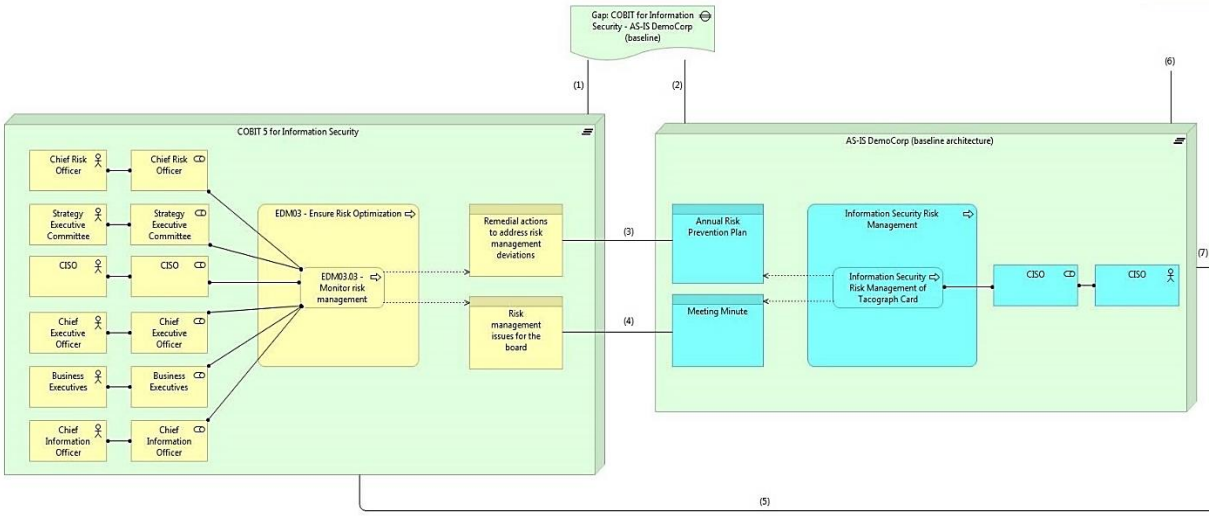


Figure 59 - Migration Viewpoint: EDM03 Process's Outputs (Part 1)

Figure 60 shows the plateaus "AS-IS DemoCorp (baseline architecture)" and "TO-BE DemoCorp (transition architecture)" and the gaps between them. As can be seen, between the baseline and

transition architecture no information security gaps were identified, so the transition architecture is equal to the baseline architecture. Note that the design of the plateau "TO-BE DemoCorp (transition architecture)" is based on the analysis of plateaus “COBIT 5 for Information Security “and” AS-IS DemoCorp (baseline architecture)”.

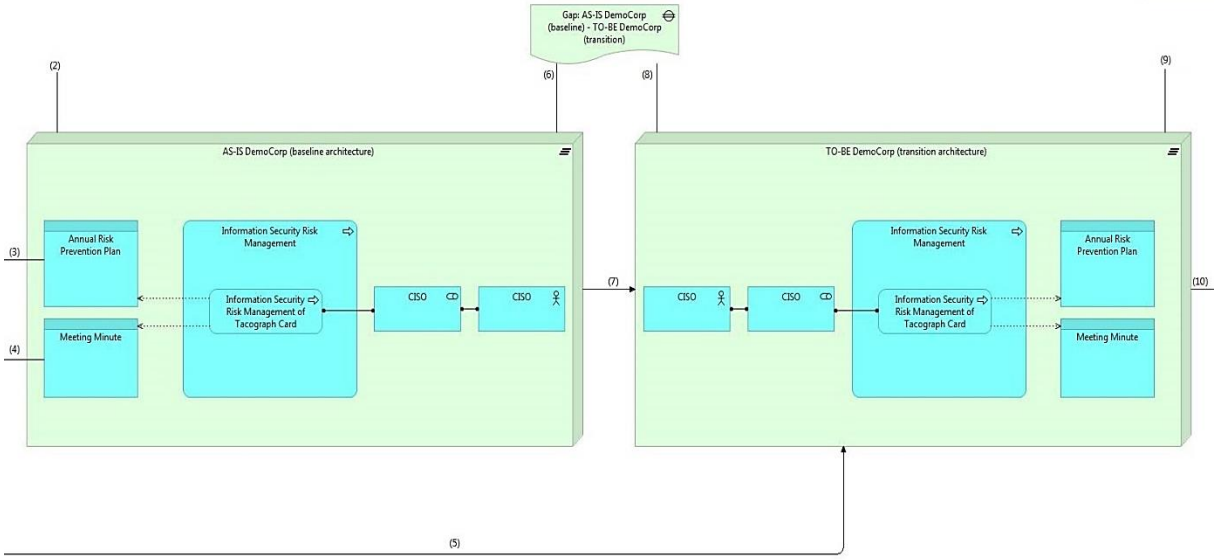


Figure 60 - Migration Viewpoint: EDM03 Process’s Outputs (Part 2)

In the following figure, we present the transition and target architectures of the DemoCorp, regarding the outputs of the process “Information Security Risk Management” in which the CISO is responsible for. Between these plateaus there are no gaps, so the responsibilities of the CISO’s role of the organization are aligned with the responsibilities defined in the COBIT 5 for Information Security.

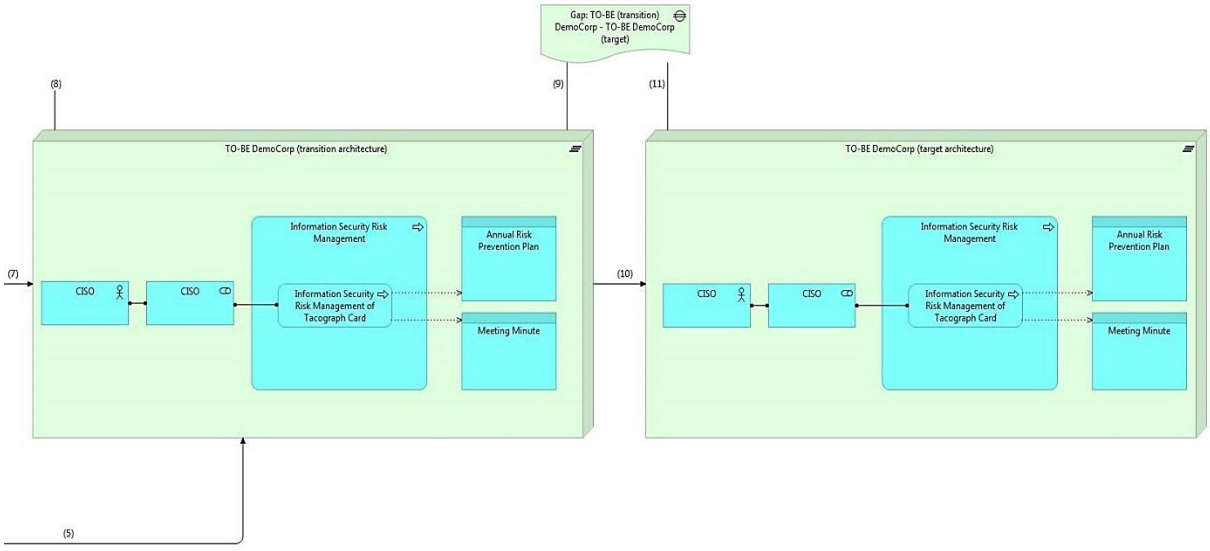


Figure 61 - Migration Viewpoint: EDM03 Process’s Outputs (Part 3)

7. Evaluation

This section corresponds to the evaluation activity of the DSRM process model [10]. The evaluation activities aim to observe and measure how well the artifacts support a solution to the research problem [10]. This activity intends to compare the objectives of a solution to actual observed results from use of the artifacts presented in the Section 6.

The evaluation of this work was accomplished by using the demonstration scenario at one government owned company, named DemoCorp (field study) in this research work.

For the evaluation, we used the following approach:

- Compare the impact of the proposed method's implementation with the former approach used to implement the CISO's role in the DemoCorp;
- Identify the relationship between the number of identified gaps and the evolution of DemoCorp's architecture.

7.1. Method Applied

In 2008, the CISO's role in the DemoCorp was established under the certification project (1st Phase), in compliance with the respective certification process's requirements. At this stage, the person responsible for performing the CISO's role had other responsibilities in the organization beside those of the CISO.

Later, In April 2014 (2nd Phase), the CISO's role became an organic structure, keeping the same person with other responsibilities in the organization besides those of the CISO.

In the recent past (3rd phase), a new person was appointed to the position of CISO.

In August 2015 (4th phase), a new person was appointed to the position of CISO, as the former ceased functions in the organization.

In November of the same year (5th phase), following a contest procedure, a new CISO was appointed by the Board, keeping up to date in office.

Before applying the proposed method in this research work, the CISO's responsibilities were not fully defined, i.e., doubts remained about its scope in the organization, regarding the processes, documentation and practices that should be responsible for managing, producing and/or originating. Furthermore, the level of information security maturity remained lower than government organizations average [2.5 vs. 2.8].

Several organization’s objectives were achieved with the application of this method, such as:

- Choose of one reference framework (COBIT 5 for Information Security) to follow, in order to fulfill the governance model;
- Definition of the CISO’s role, based on the definition described in the framework.

With the implementation of the CISO’s role is expected that the organization can reach the maturity Level [2.8] of information security, which is one of its major goals for 2016. Since the TO-BE design was made according the recommendations provided by the consulting company who conducted the IT Score, it is expected that by the end of the year the role of the CISO will be implemented in accordance with the COBIT 5 for Information Security sets but tailored to the organization's context, since this framework should be seen as a toolkit in support of management, i.e., we need to keep critical when using the material to ensure smart use of COBIT.

Unanimous opinions reside on the problem being very common and on the fact that the proposed method adds value to the field and is a good compilation of the best practices provided in COBIT 5 for Information Security. Not only the method was accepted in the DemoCorp, but in some cases opened business and collaboration opportunities.

7.2. Gap Analysis

A field study is defended by some authors as the most gainful method of evaluation, due to its practical nature bringing higher organizational impact and even quality than other methods [32].

For the gap analysis, the Step 7 of the proposed solution to implement the CISO’s role in the organization was analyzed.

In the Figure 62 are shown the identified gaps between the plateaus of each one of the viewpoints modeled in Step 7 "TO-BE Analysis & Design" of the proposed method.

As can be seen, the number of gaps (in general) among the plateaus decreases between AS-IS (baseline architecture) and TO-BE (transition architecture) and, only the viewpoints "APO01 Process's outputs (Complete view)" and "EDM03 Process's outputs (Complete view)” do not present such gaps’ reduction.

Regarding the “APO01 Process’s outputs (Complete view)” viewpoint, this difference occurs because there are no elements in the AS-IS of DemoCorp that could be mapped to the responsibilities of the CISO’s role, defined in COBIT 5 for Information Security, in regard to the outputs of this process. Consequently, there is the same number of gaps between the AS-IS and TO-BE (transition architecture) of DemoCorp, since in the TO-BE these gaps are addressed and such CISO’s responsibilities that were missing are added to its scope of action, based on the strategic decision of DemoCorp who decided to follow the IT Score recommendations.

On the other hand, we can observe that zero gaps were identified between the outputs of the EDM03 process and the DemoCorp, since the CISO of the organization is responsible for producing similar outputs to those that are listed in the COBIT 5 for Information Security.

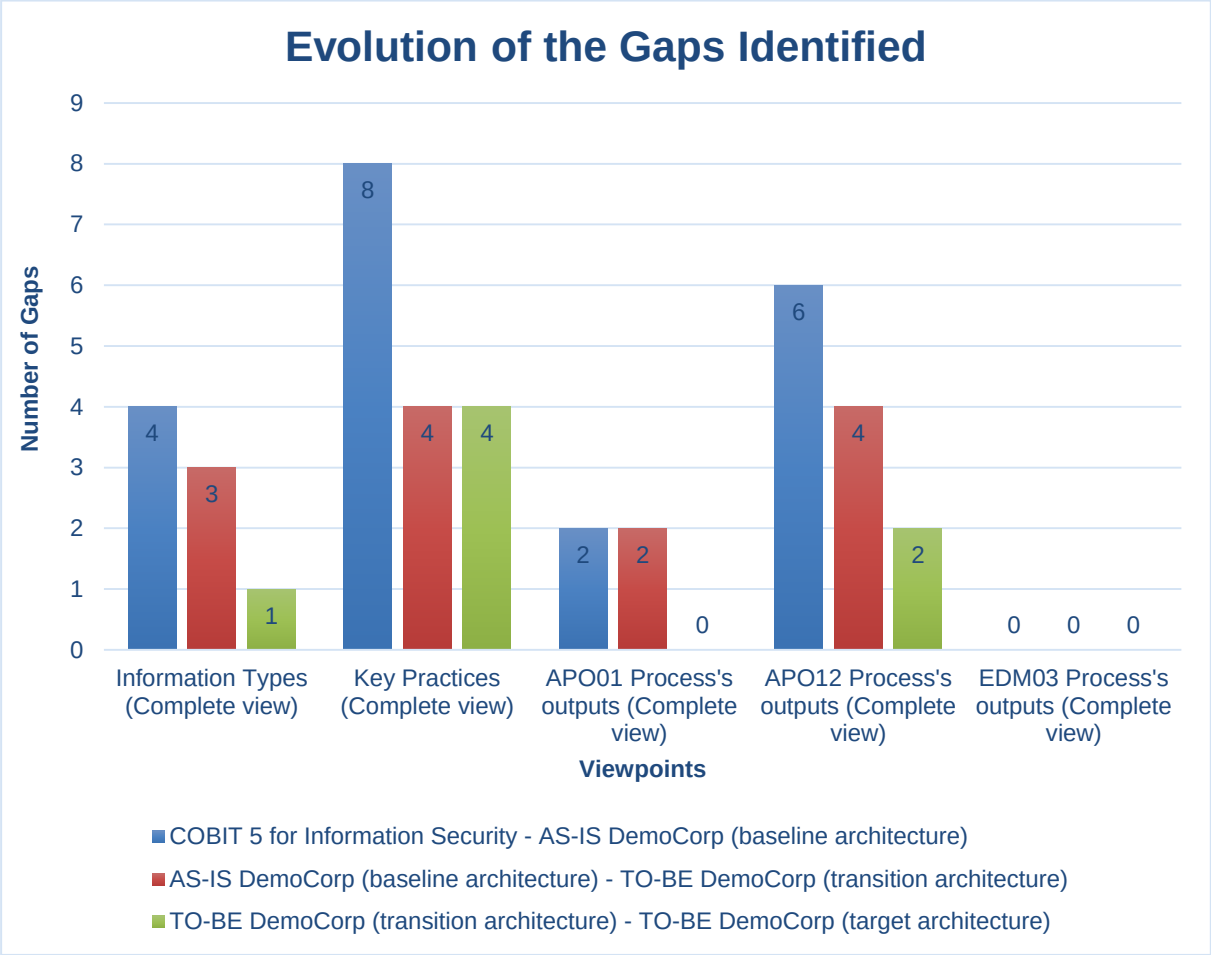


Figure 62 - Evolution of the Gaps Identified

With the decrease of the gaps can be assumed that the proposed method applied in the organization had a positive effect, since it was possible to assign new responsibilities to the CISO's role, according to the organization's context. Furthermore, the method has been properly adapted to the organization and a strategic decision was followed to draw the TO-BE of the CISO's role in the company.

The following objectives of the solution were fully achieved, so the proposed artefact was effective:

- Figures out what processes and activities, key practices and business functions that the CISO should be held responsible;
- Identifies information types that the CISO is responsible to originate;
- Finds what organization's roles are performing the CISO's job;
- Hopefully improves the information security maturity level of the organization.

By following up these recommendations, it will be possible for the organization to achieve the desired information security maturity level [2.8].

8. Communication

The communication section corresponds to the communication activity of the DSRM process model [10].

The communications activity aims to communicate the problem and its importance, the artifact, its utility and novelty, the rigor of its design, and its effectiveness to researchers and other relevant audience [10]. Moreover, the communication activity tests the acceptance of the research work outcomes, which provides information about the problem's importance, the solution objective's viability, the artifacts' utility and the outcomes' value.

This research work was shared with DemoCorp the filed study's company, by having the proposed method applied to its particular case.

To communicate our work, we have submitted two papers to the following conferences:

- ***18th IEEE Conference on Business Informatics (CBI)***. The paper proposes our method to implement the CISO's role in organizations using COBIT 5 for Information Security in ArchiMate;
- ***13th European Mediterranean & Middle Eastern Conference on Information Systems (EMCIS)***. This paper identifies inconsistencies between the RACI charts of COBIT 5 Enabling Processes and the COBIT 5 for Information Security, regarding the definition and implementation of the CISO's role.

The paper submitted in the **EMCIS** conference was accepted as a full paper to be presented in the conference.

9. Conclusion

Companies, which approach information security governance, invest in frameworks to address assignments involved in the action of IT governance. Simultaneously, we observe that roles and assigned responsibilities are defined in the COBIT 5 framework.

COBIT 5 should be seen as a framework in support of management and governance that provides a “thinking approach and structure” with very useful examples. Moreover, it is important to stay critical when using the material to ensure the correct use of the COBIT 5 framework.

Consequently, in the previous sections, we presented architectural artifacts that had the goal to create a method for implementing the CISO’s role in an organization. Such method represents the COBIT 5 for Information Security using ArchiMate and, after, to map the organizations that intend to implement the CISO’s role to the COBIT 5 for Information Security.

The related work provided information about the key concepts, which are relevant to be part of the desired solution. These concepts are related to the following artifacts: modeling the COBIT 5 for Information Security, mapping this professional guide to the ArchiMate, and providing a set of viewpoints that address the problem regarding the implementation of the CISO’s role in an organization.

After the analysis of the related work, we formulated the research problem, as a search for a solution for implementing the CISO’s role in an organization, using the COBIT 5 for Information Security in ArchiMate.

Furthermore, we provided artifacts, regarding the guide COBIT 5 for Information Security and the map in one organization, named DemoCorp. These artifacts have special importance because they provide viability of the research work. With this proposal we have demonstrated that it is possible to identify information security gaps, using COBIT 5 for Information Security.

Moreover, roles’ inconsistencies were presented, taking into account the definition of the CISO’s role. Such inconsistencies influence negatively the IT governance of the organizations that want to use COBIT 5 for Information Security to define the roles of information security professionals. Inconsistencies were found from the analysis of RACI Charts, presented in COBIT 5 Enabling Processes, and Information, Organizational Structures and Processes enablers’ content, described in COBIT 5 for Information Security.

As said in COBIT 5 Enabling Processes, RACI charts are a suggestion of responsibilities’ assignment. Furthermore, COBIT 5 for Information Security guides complements the COBIT 5 Enabling Processes, so it was expected that the roles responsible for originating a specify-security information type were, also, responsible for the process that produces this type of specific-security information.

In Section 6, we designed the framework using the ArchiMate modeling language. After, regarding the

representation of COBIT 5 for Information Security, we also decide to represent the organization using ArchiMate notation in order to be able to map it to the framework.

The COBIT 5 for Information Security guidelines were used for identify, (re)define and manage the objectives of the solution. Furthermore, the COBIT 5 for Information Security was used for the development of the desired method to implement the CISO's role.

We provided an effective solution that address the research problem and enables the information security implementation, particularly the CISO's role. This solution was based on the COBIT 5 for Information Security. The proposed method mapped one organization to responsibilities of the CISO's role (defined in COBIT 5 for Information Security), which goal was to identify the key practices, information types and processes' outputs that are missing. Also, we mapped the roles of the DemoCorp to the COBIT 5's roles in order to know who is performing the CISO's job. All of these maps were made using the ArchiMate notation.

The proposed solution produced was based on globally accepted frameworks (such as COBIT 5) and standards (such as ArchiMate), which can lead to a better value of the solution delivered. These frameworks and standards help the adoption of the desired proposed solution and increasing the level of acceptance in the organizations.

We conclude that the proposed method can help organizations to detect the information security gaps and to implement the CISO's role correctly, increasing the value delivery by information security.

9.1. Contributions

In this sub-section we summarize the dissertation contributions to the practice and to the knowledge base. Therefore, these are the main research contributions of this dissertation:

- A method for implementing the CISO's role using COBIT 5 for Information Security in ArchiMate, which comprises 7 steps with the following features:
    - An ontological mapping between COBIT 5 for Information Security and ArchiMate, placing COBIT 5 concepts on EA domains (Step 1);
    - A set of viewpoints for using in COBIT 5 roles definition and implementation (Step 1);
    - A set of viewpoints to represent the organizations' EA (Step 2);
    - A set of viewpoints to represent the mapping of organizations' EA and the COBIT 5 for Information Security, in order to implement the CISO's role, with the following characteristics (Steps 3 to 7):
        - Their efficacy and utility was validated in one government owned company;
        - Their constructs are based on ArchiMate notation (version 2.1).
- Identification of inconsistencies between roles' assignments, in particular the CISO's role, which are defined in the assignments matrix charts of COBIT 5 Enabling Processes, and the roles addressed by COBIT 5 for Information Security.

In hindsight, we should however emphasize that the main contribution is the proposed method. In fact, besides its value in the CISO's role implementation, the method also adds something that COBIT 5 for Information Security lacked: viewpoints for implementation guidance.

Finally, this thesis also enabled 2 research communication opportunities, as described in Section 8.

9.2. Limitations

Concerning the limitations of this research the following were found:

- It is possible that the proposed method has not the same level of usefulness when the information security professional applying it does not have much experience in the field (ArchiMate and COBIT 5 for Information Security);
- The method is not a stand-alone tool, does not substitute the reading of the familiarity with the methodologies and tools it is founded in;
- This research proposal only identifies inconsistencies regarding the CISO's role definition provided in COBIT 5 Enabling Processes and COBIT 5 for Information Security;
- This proposal only focuses on the Business Layer, Motivation and Migration & Implementation extensions;
- This research proposal does not provide a connection between governance and management of information security.

9.3. Future Work

There is still plenty of research that can be done having this thesis as a basis.

Based on the outcomes of this work, we may point to the following opportunities for related future work:

- Conduct further DSRM work, integrating more aspects of the COBIT 5 for Information Security professional guide;
- Extend the scope and/or depth of the thesis work, e.g. by:
    - Development of a solution's proposal that addresses the inconsistencies detected, allowing to establish a correct connection between the guides COBIT 5 Enabling Processes and COBIT 5 for Information Security, in order to enable IT governance for different companies to deliver more value to the business, should be way to go.
    - Demonstrating and evaluating the method in more government owned companies;
    - Demonstrating and evaluating the method in private sector organizations, eventually comparing the results with those obtained in the public sector domain;
    - Specializing the proposed method by industry/type of organization (e.g. SME and Banking);
    - Extending the research proposal in order to comprise others architectural levels (application and technology layers);

- Extending the proposal in order to connect the governance and management of information security;
- A future research could include a proposed framework to guide researchers to analyze documents and standards of IT governance and specify inconsistencies and, a definition and conceptualization of inconsistencies (e.g. how are they defined and what levels of inconsistencies might exist), could be addressed.

In short, in times where cost and value generation are such important drivers, information security, more than ever, should deliver more value and turn organizations more effective and efficient. EA does not tell us how to design specific organizations that have the CISO's role definition and implementation as a main concern, and COBIT 5 for Information Security does not provide implementation guidance.

Therefore, we hope this research work can help to join the best of both words, one method that integrates the EA and COBIT 5 approaches, complementary on organizations, with distinct organizational structures, that have much more to gain from aligning together instead of waling apart.

References

[1] M. Vicente. "Enterprise Architecture and ITIL (master thesis report)". Instituto Superior Técnico, Portugal, 2013.

[2] N. Silva. "Modeling a Process Assessment Framework in ArchiMate (master thesis report)". Instituto Superior Técnico. Portugal. 2014.

[3] D. Whitten. “The Chief Information Security Officer: An Analysis of the Skills Required for Success”. Texas A&M University. United States of America. 2008. doi: [10.1080/08874417.2008.11646017].

[4] F. Souza. “An information security blueprint, part 1”. [Online]. Available: http://www.csoonline.com/article/2125095/network-security/an-information-security-blueprint--part-1.html. [Accessed: 15-Dec-2015].

[5] G. Cadete. “Using Enterprise Architecture for Implementing Governance with COBIT 5 (master thesis report)”. Instituto Superior Técnico. Portugal. 2015.

[6] ISACA. "COBIT 5 for Information Security". ISACA. USA. 2012. ISBN: [978-1-60420-255-7].

[7] N. Olijnyk. “A quantitive examination of the intellectual profile and evolution of information security from 1965 to 2015”. *Scientometrics*. 105:883-904. 2015. doi: [10.1007/s11192-015-1708-1].

[8] T. Olavsrud. “5 information security trends that will dominate 2016”. [Online]. Available: http://www.cio.com/article/3016791/security/5-information-security-trends-that-will-dominate-2016.html. [Accessed: 12-May-2016].

[9] S. Moffatt. “Security Zone: Do you need a CISO?”. ComputerWeekly. 2012.

[10] K. Peffers, T. Tuunanen, M. A. Rothenberger and S. Chatterjee. "A Design Science Research Methodology for Information Systems Research". *Journal of Management Information Systems.* Vol. 24 No.3. 2007. ISBN: [0742–1222].

[11] ISACA. "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT". ISACA. USA. 2012. ISBN: [978-1-60420-237-3].

[12] A. Hevner, S. March, J. Park and S. Ram. "Design Science in Information Systems Research". *MIS Quarterly.* Vol. 28 No.1. March 2004. doi: [10.2753/MIS0742-1222240302].

[13] A. Hevner and S. Chatterjee. “Design Research in Information Systems”. Springer. 2010.

[14] The Open Group. "ArchiMate 2.1 Specification". Van Haren Publishing. The Netherlands. 2013. ISBN: [1-937218-43-0].

[15] T. Fitzgerald. “Clarifying the Roles of Information Security: 13 Questions the CEO, CIO, and CISO must ask each other”. *Information Systems Security.* 16:257-263. 2007. doi: [10.1080/10658980701746577].

[16] W. Ashford. “CISO role evolves towards balancing business and security objectives”. ComputerWeekly. 2012.

[17] S. Ragan. “The biggest challenges faced by CIOs/CISOs heading into 2015”. [Online]. Available: http://www.csoonline.com/article/2858343/data-protection/the-biggest-challenges-faced-by-cios-cisos-heading-into-2015.html. [Accessed: 15-Sept-2015].

[18] N. Hockin. “Deloitte reveals top challenges facing new chief information security officers”. Available: http://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-reveals-top-challenges-facing-new-cisos.html. [Accessed: 22-Nov-2015].

[19] S. Poremba. “10 Ways Employees Compromise Their Company’s Cyber Security”. Forbes. 2015.

[20] K. Kessinger. “New Report Show Benefits of CISOs”. ISACA. 2010.

[21] ISACA. "COBIT 5: Enabling Processes". ISACA. USA. 2012. ISBN: [978-1-60420-241-0].

[22] M. Silva and P. Vicente. “A Conceptual Model for Integrated Governance, Risk and Compliance”. Instituto Superior Técnico. Portugal. 2011.

[23] N. Mayer, B. Barafort, M. Picard and S. Cortina. “An ISO Compliant and Integrated Model for IT GRC (Governance, Risk Management and Compliance)”. Luxembourg Institute of Science and Technology. Luxembourg. 2015. doi [10.1007/978-3-319-24647-5_8].

[24] N. Mayer, E. Grandry, C. Feltus and E. Goettelmann. “Towards the ENTRI Framework: Security Risk Management enhanced by the use of Enterprise Architectures”. Luxembourg Institute of Science and Technology. Luxembourg. 2015. doi [10.1007/978-3-319-19243-7_42].

[25] D. Ashenden and A. Sasse. “CISOs and organizational culture: Their own worst enemy”. *Computers & Security*. Elsevier Ltd. 2013.

[26] ISACA. “CyberSecurity Nexus”. ISACA.USA. 2015.

[27] M. Lankhorst. “Enterprise Architecture at Work”. Springer. 2005. ISBN: [978-3-540-24371-7].

[28] K. Niemann. “From Enterprise Architecture to IT Governance”. Vieweg. 2006. ISBN: [978-3-8348-0198-2].

[29] V. Grembergen and S. de Haes. “Implementing Information Technology Governance: Models, Practices and Cases”. IGI Publishing. 2007. ISBN: [1599049244].

[30] Archi. "Archi - The Free ArchiMate Modelling Tool". Available: http://www.archimatetool.com/. [Accessed: 10-July-2015].

[31] ISACA. “COBIT Process Assessment Model (PAM): Using COBIT 5”. ISACA. USA. 2013. ISBN: [978-1-60420-264-9].

[32] D. Arnott and G. Pervan. “How relevant is fieldwork to DSS design-science research?”. Frontiers in Artificial Intelligence and Applications. Vol. 212, pp. 108–119. 2010. ISBN: [10.3233/978-1-60750-576-1-108].

[33] The Open Group. “TOGAF Version 9.1”. Van Haren Publishing. The Netherlands. 2013. ISBN: [978-90-8753-679-4].

[34] K. Laudon and J. Laudon. “Management Information Systems”. 12th ed. Pearson. 2012. ISBN: [978-0132142854].

[35] V. Vaishnavi and B. Kuechler. “Design Science Research in Information Systems”. *ISWorld*. 2013.

[36] R. Meadows. “ISACA’s COBIT Framework Turns 20”. Available: http://www.isaca.org/About-ISACA/Press-room/News-Releases/2016/Pages/ISACA-s-COBIT-Framework-Turns-20.aspx. [Accessed: 28-Apr-2016].

[37] J. Barrera. “COBIT Focus”. Available: http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volume-3-July-2013.aspx. Accessed [28-Apr-2016].

[38] ISO/IEC. “ISO/IEC 27001: Information Security Management System”. ISO/IEC. Geneva. 2013.

[39] ISO/IEC. “ISO/IEC 27002: Information technology – Security techniques – Code of practices for information security controls". ISO/IEC. Geneva. 2013.

[40] PCI Security Standards Council. “Payment Card Industry (PCI) Card Production”. PCI Security Standards Council. USA. 2015.

[41] J. Westby and J. Allen. “Governing for Enterprise Security (GES) Implementation Guide”. Software Engineering Institute. 2007. doi: [CMU/SEI-2007-TN-020].

[42] T. Catarino, B. Fragoso, A. Vasconcelos and M. Mira da Silva. “Inconsistencies in Information Security Roles”. In *13th European Mediterranean & Middle Eastern Conference on Information Systems (EMCIS),* Krakow, June 23 (accepted), 2016.

Appendixes

Appendix A – COBIT 5 for Information Security

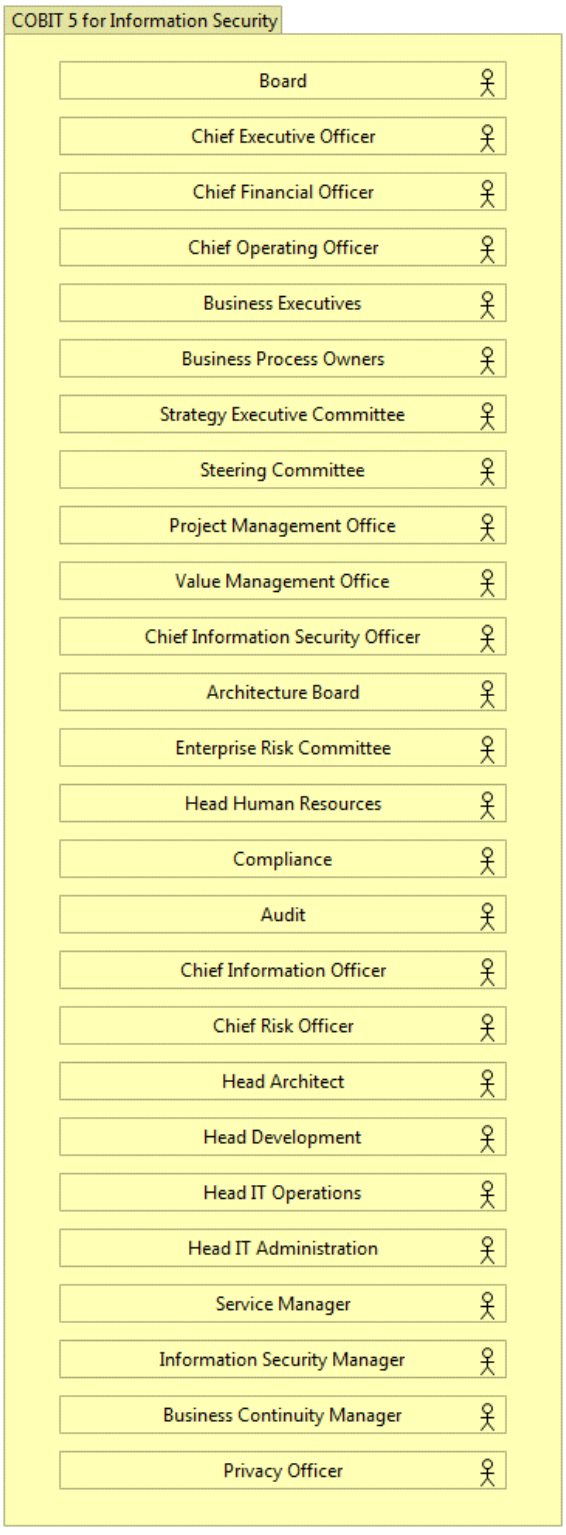


Figure 63 - COBIT 5 Organizational Structure viewpoint

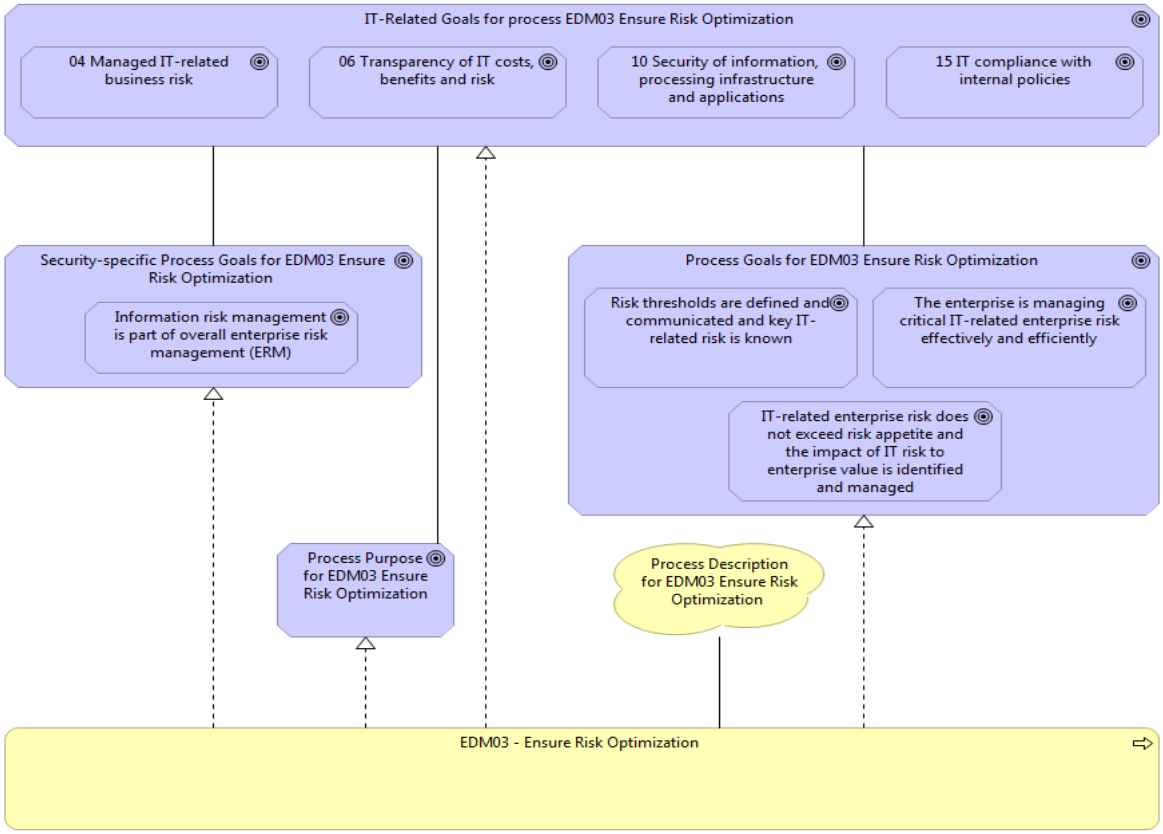


Figure 64 - EDM03 Ensure Risk Optimization Process and Goals viewpoint

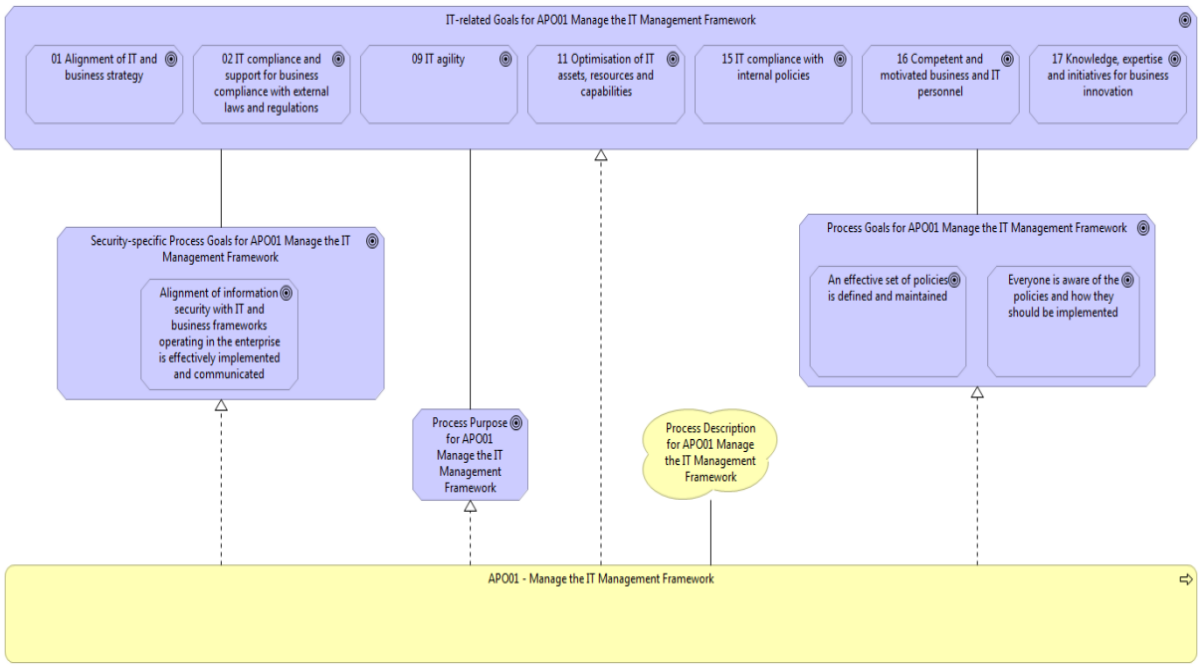


Figure 65 - APO01 Manage the IT Management Framework Process and Goals viewpoint

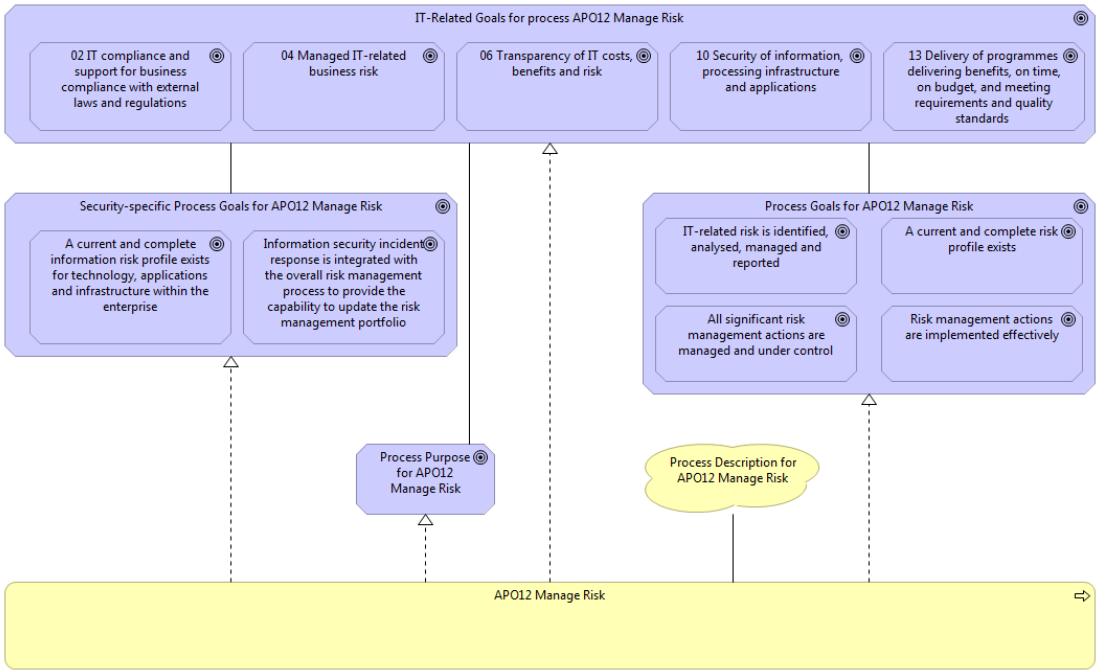


Figure 66 - APO12 Manage Risk Process and Goals viewpoint

Appendix B – DemoCorp

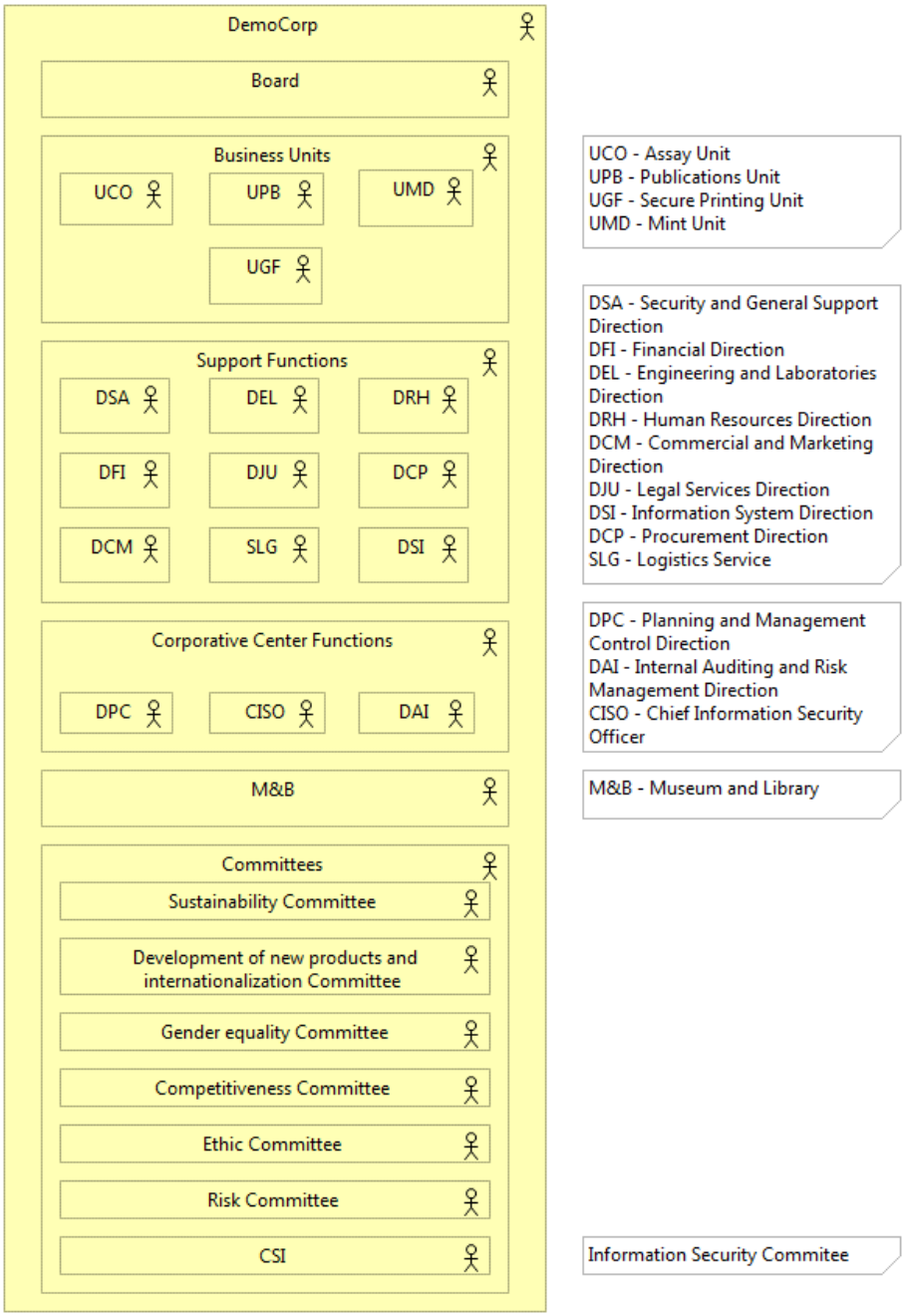


Figure 67 - DemoCorp Organizational Structure viewpoint

Interview guide:

https://docs.google.com/forms/d/1VmptA8lsX1Vg1Ch62Wn2XtiG3KpRGYckBbutZfGVbeA/viewform?usp=send_form

Appendix C – DemoCorp to COBIT 5 for Information Security Mapping

Table 12 - Caption of Figures 39, 47 and 48

Assignment Relation (number)	Source (role)	Target (practice)
1.	CISO	(1)
2.	CISO	(2)
3.	CISO	(3)
4.	CISO	(4)
5.	CISO	(5)
6.	DEL Technician	(6)
7.	CISO	(6)
8.	DSA Technician	(6)
9.	DSI Technician	(6)
10.	DSI Technician	(7)
11.	CISO	(7)
12.	DSA Technician	(7)
13.	DEL Technician	(7)
14.	DSA Technician	(8)
15.	DSI Technician	(8)
16.	CISO	(8)
17.	DEL Technician	(8)
18.	DSA Technician	(9)
19.	CISO	(9)
20.	DSI Technician	(9)
21.	DEL Technician	(9)
22.	Board	(10)

Table 13 - Caption of Figure 48 and 49

Assignment Relation (number)	Source (role)	Target (practice)
1.	CISO	(1)
2.	CISO	(2)
3.	CISO	(3)
4.	CISO	(4)
5.	CISO	(5)
6.	CISO	(6)
7.	CISO	(7)
8.	CISO	(8)
9.	CISO	(9)
10.	DEL Technician	(10)
11.	CISO	(10)
12.	DSA Technician	(10)
13.	DSI Technician	(10)
14.	DSI Technician	(11)
15.	CISO	(11)
16.	DSA Technician	(11)
17.	DEL Technician	(11)
18.	DSA Technician	(12)
19.	DSI Technician	(12)
20.	CISO	(12)
21.	DEL Technician	(12)
22.	DSA Technician	(13)
23.	CISO	(13)
24.	DSI Technician	(13)
25.	DEL Technician	(13)
26.	Board	(14)

Table 14 - Caption of Figure 49

Assignment Relation (number)	Source (role)	Target (practice)
1.	CISO	(1)
2.	CISO	(2)
3.	CISO	(3)
4.	CISO	(4)
5.	CISO	(5)
6.	CISO	(6)
7.	CISO	(7)
8.	CISO	(8)
9.	CISO	(9)
10.	CISO	(10)
11.	CISO	(11)
12.	CISO	(12)
13.	CISO	(13)
14.	DEL Technician	(14)
15.	CISO	(14)
16.	DSA Technician	(14)
17.	DSI Technician	(14)
18.	DSI Technician	(15)
19.	CISO	(15)
20.	DSA Technician	(15)
21.	DEL Technician	(15)
22.	DSA Technician	(16)
23.	DSI Technician	(16)
24.	CISO	(16)
25.	DEL Technician	(16)
26.	DSA Technician	(17)
27.	CISO	(17)
28.	DSI Technician	(17)
29.	DEL Technician	(17)
30.	Board	(18)

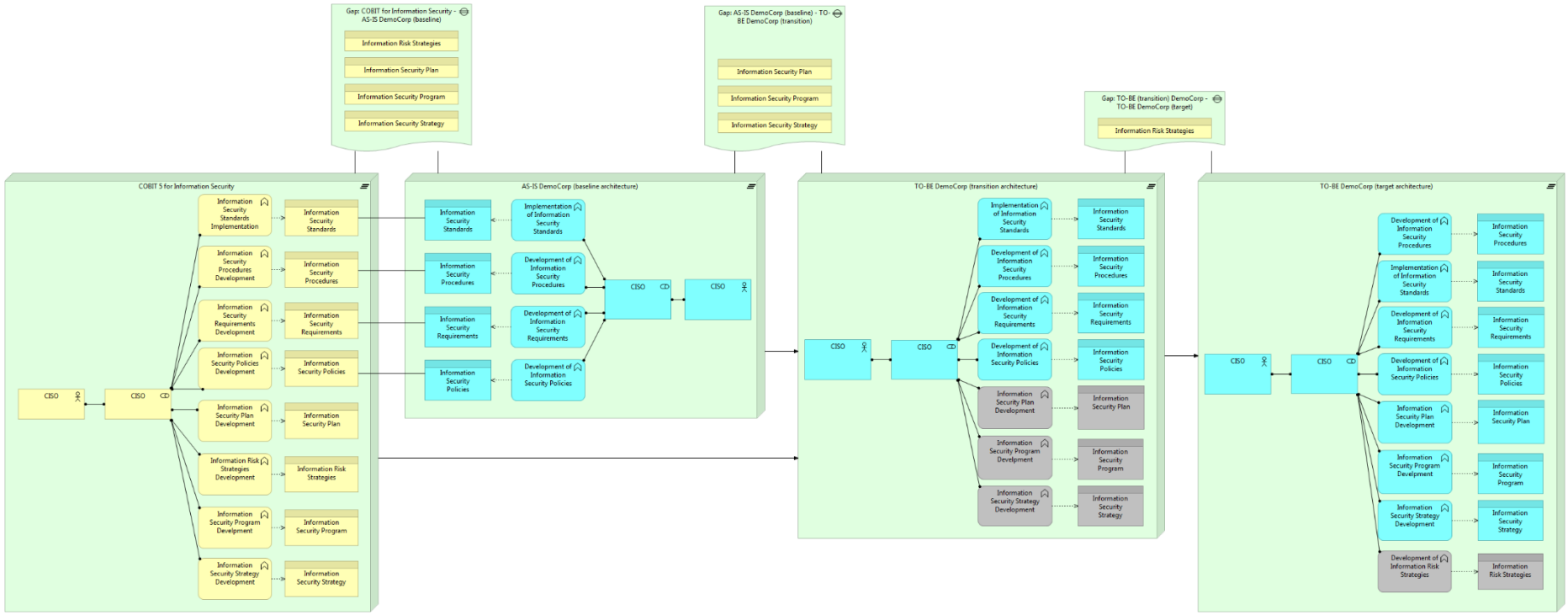


Figure 68 - Information Types (Complete view)

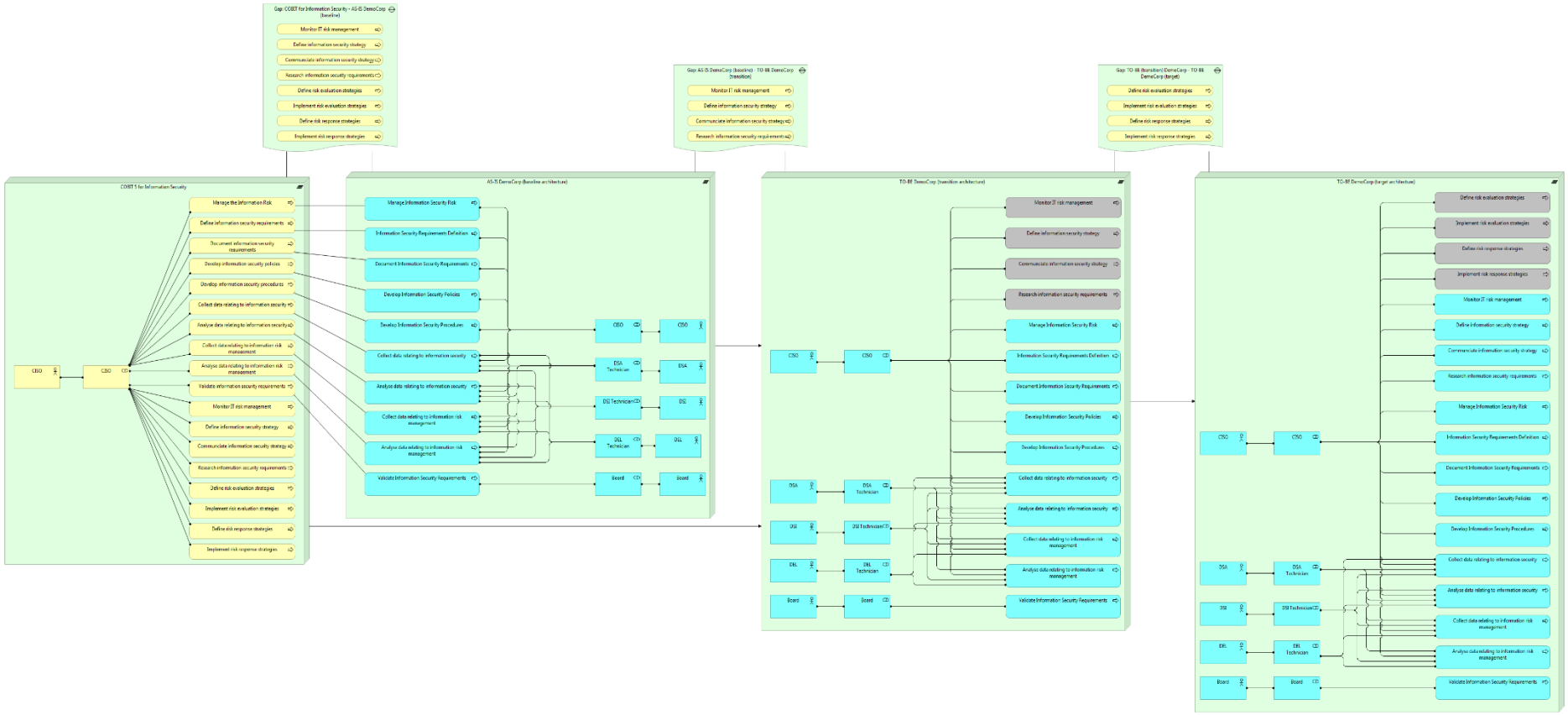


Figure 69 - Key Practices (Complete view)

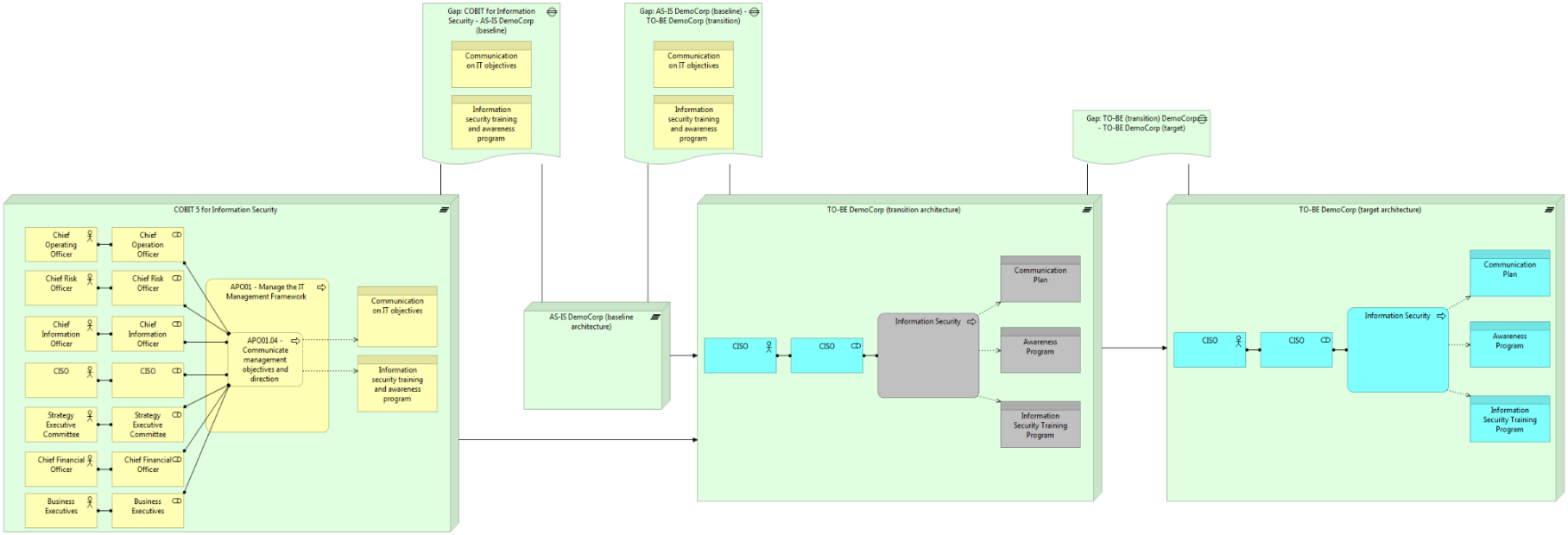


Figure 70 – APO01 Process's Outputs (Complete view)

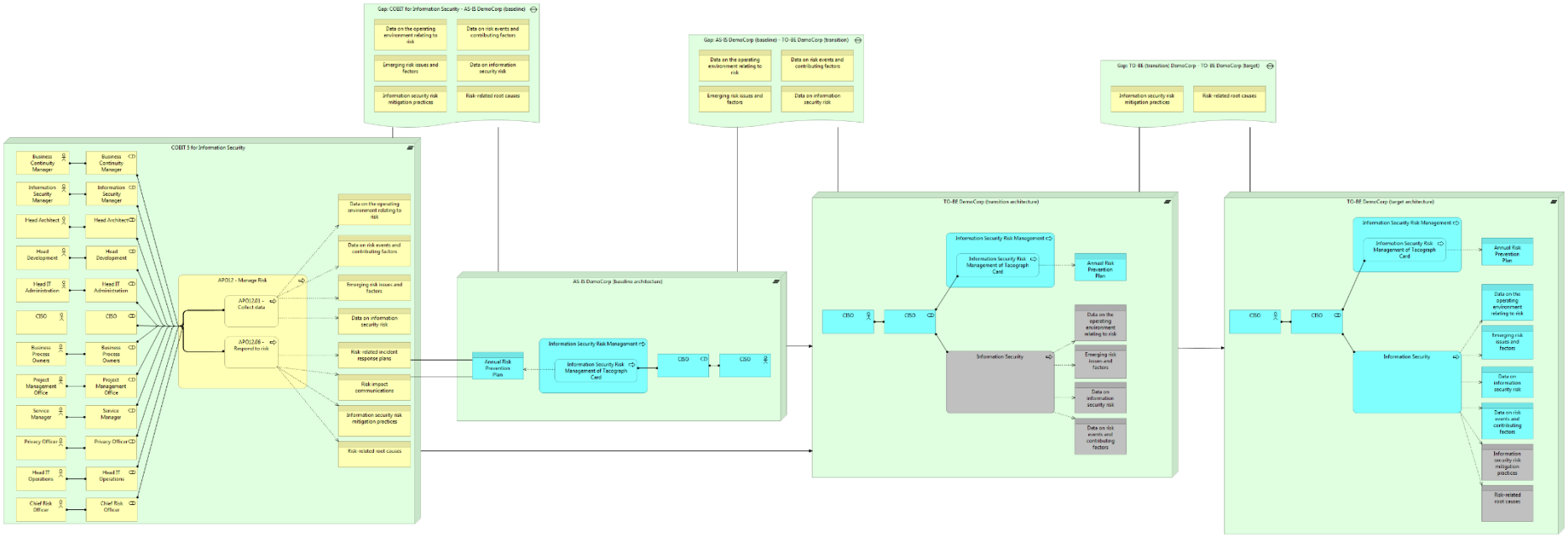


Figure 71 - APO12 Process's Outputs (Complete view)

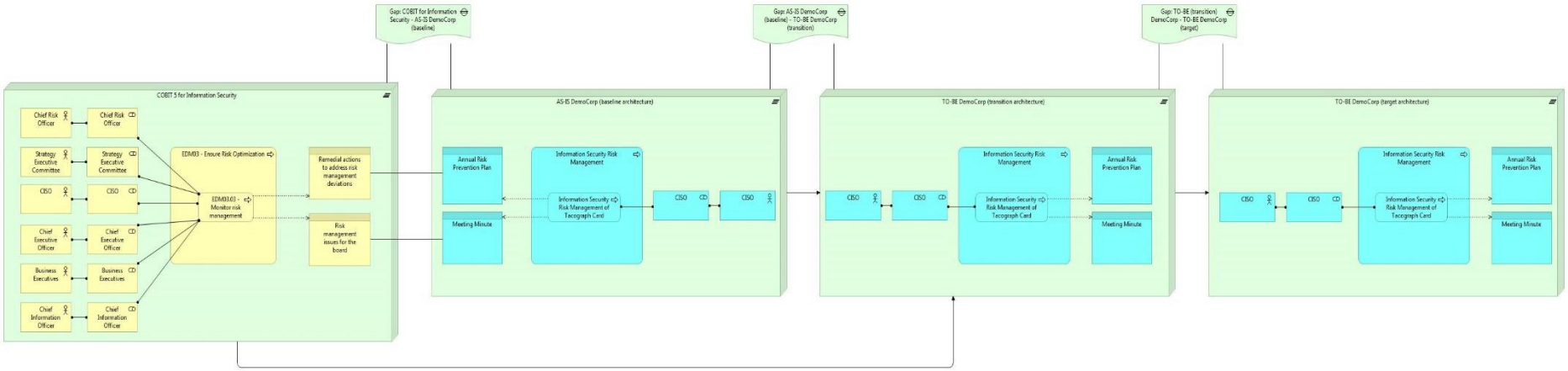


Figure 72 - EDM03 Process's Outputs (Complete view)

Appendix D – COBIT 5 Enabling Processes

AP001 RACI Chart												
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer
AP001.01 Define the organisational structure.		C	C	C	C		I		C			
AP001.02 Establish roles and responsibilities.					I	C			C			
AP001.03 Maintain the enablers of the management system.	C	A	C	R	C	C	I				C	C

Figure 73 - Maintain the enablers of the management system

AP002 RACI Chart												
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer
AP002.01 Understand enterprise direction.		C	C	C	A	C	C				C	C
AP002.02 Assess the current environment, capabilities and performance.		C	C	C	R	C	C				C	
AP002.03 Define the target IT capabilities.		A	C	C	C	I	R		I		C	
AP002.04 Conduct a gap analysis.					R	R	C				C	
AP002.05 Define the strategic plan and road map.		C	I	C	C		C		R		C	C
AP002.06 Communicate the IT strategy and direction.	I	R	I	I	R	I	A	I	I	I	I	I

Figure 74 - APO02.02 – Assess the current environment, capabilities and performance, APO02.05 – Define the strategic plan and road map, APO02.06 – Communicate the IT strategy and direction

APO05 RACI Chart												
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer
APO05.01 Establish the target investment mix.	A	R	R		C					I	C	C
APO05.02 Determine the availability and sources of funds.	C		A		R					C		
APO05.03 Evaluate and select programmes to fund.	C	A	R		R		R			R		

Figure 75 - APO05.03 – Evaluate and select programs to fund

APO11 RACI Chart												
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer
APO11.01 Establish a quality management system (QMS).		C		A	C	I	C	I	I			
APO11.02 Define and manage quality standards, practices and procedures.		C			C	R	C		R			

Figure 76 - APO11.01 – Establish a quality management system (QMS), APO11.02 – Define and manage quality standards, practices and procedures

APO12 RACI Chart												
Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer
APO12.01 Collect data.		I				R			R		R	R
APO12.02 Analyse risk.		I				R			C		R	C
APO12.03 Maintain a risk profile.		I				R			C		A	C
APO12.04 Articulate risk.		I				R			C		R	C

Figure 77 - APO12.04 – Articulate risk