The Role of the Chief Information Security Officer

Tiago Catarino
Instituto Superior Técnico
tiagomcatarino@tecnico.ulisboa.pt

***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 the CISO's role, we propose a method to implement this role in the organizations, using the COBIT 5 for Information Security in ArchiMate. 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. 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.

1. INTRODUCTION

In the last years, information security has evolved from its traditional orientation focused mainly in technology to become part of the organization strategic alignment, 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]. Many of these attacks are more sophisticated in order to steal confidential information. Therefore, companies that deal with a lot of 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 then loss [4]. Companies are increasingly recognizing information and related technologies as critical business assets, which needs 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 [6].

Information security has an important role in day-to-day operations in order to protect the information [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, such as competitive advantage [6]. Furthermore, information 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].

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 blue print which can cover the technical as well as physical and personnel-related security, which works quite successfully in many ways [8].

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 [8]. This leads the Chief Information Security Officer (CISO) to take a central role in the organizations, since not having someone in the organization that is accountable for information security, greater are the chances for a major security incident to happen [9].

Some industries place 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 and 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. [8]

The COBIT 5 for Information Security is a professional guide that helps companies to implement information security functions. This guide can be instrumental in providing a more detailed and more practical guidance for information security professionals, which includes the CISO's role [6]. This guide is part of COBIT 5's framework, focusses on information security and can be instrumental in providing guidance for information security professionals, which includes the CISO's role [11].

This thesis has the following structure (section): Introduction (1), Research Methodology (2), Research Problem (3), Related Work (4), Proposal (5), Demonstration (6), Evaluation (7), Communication (8), and finally Conclusion (9).

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.

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.

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. Problem

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.

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 problems when we try to make an assessment of maturity level on the enterprise processes.

Even COBIT 5 having all the roles well defined and RACI charts for each process, companies have different roles and levels of involvement [6].

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's 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 outputs 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, 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

This sections contains all the concepts related with this thesis and descriptions of the most important. 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.

4.1. Chief Information Security Officer

The CISO is responsible for risk management, security operations, physical security and balancing business and security objectives [3].

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.

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 [15].

4.2. COBIT 5 Framework

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

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].

The research's focus is information security, so the guide COBIT 5 for Information Security can be followed.

4.3. 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.

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 [24] [25].

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 [26].

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 [27].

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

Other types of information are delivered by this framework but there are some limitations that influence negatively the implementation of the CISO in an organization, such as:

- The framework is extremely focused on information technology industry;
- Does not get into any of the technical details, for example the process "Manage Data" in DSS area, covers everything like backup procedures and mechanisms, capacity management and 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 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.
- Inconsistencies between the RACI charts defined in the COBIT 5 Enabling Processes [16] and the information security-specific roles responsible for producing and/or originating information types, processes' outputs and information's outputs [28].

4.4. 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 [18].

An architecture at the level of an entire organization is called enterprise architecture (EA) [19] [20]. 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 [18].

The EA process creates transparency, delivers information as a basis for control and decision-making, and enables IT governance [18].

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 [18].

Moreover, EA can be related to a number of well-known best practices and standards [18]. As stated in Table I, we present the management areas relevant to EA and the relation between EA and some well-known management practices on each area.

TABLE I. EA MANAGEMENT AREAS VS MANAGEMENT PRACTICES [18]

Strategic Execution	EFQM
Quality Management	ISO 9001
IT Governance	COBIT 5
IT delivery and support	ITI
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.

4.5. ArchiMate

ArchiMate is an open and independent EA modeling language, which is part of the Open Group [14] [21].

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

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 [17].

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 [12].

The Business Layer, which is part of the framework provided by ArchiMate, it is where our problem is address. 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. Furthermore, ArchiMate Motivation and Implementation & Migration extensions are also keys inputs for the solution proposal that will helps to the COBIT 5 for Information Security modeling.

ArchiMate have already shown in academic environment the possibilities it opens in increasing the organizational awareness towards its notations.

5. PROPOSAL

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 [19] [20]. 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 [18].

Although EA and COBIT 5 describe areas of common interest, they do it from different perspectives [18]. 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 [18].

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.

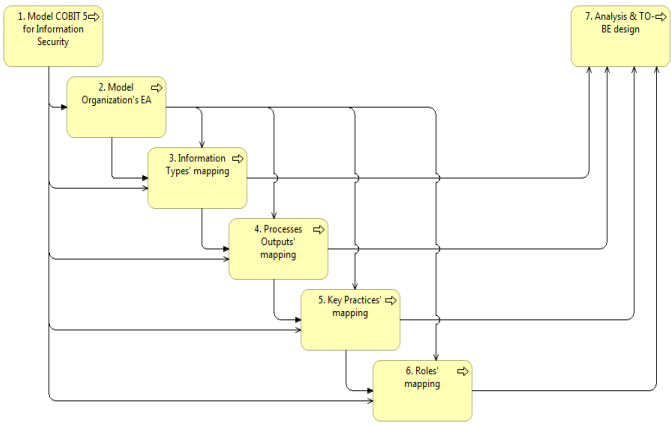


Fig. 1. Proposed Method's Steps

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.

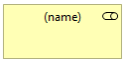
5.1. STEP 1 – Model COBIT 5 for Information Security

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 II is proposed an example of the ontological mapping between COBIT 5 for Information Security and ArchiMate's concepts, regarding the definition of the CISO's role.

TABLE II. COBIT 5 FOR INFORMATION SECURITY TO ARCHIMATE ONTOLOGICAL MAPPING

COBIT 5 for IS concept	COBIT 5 for IS concept description [11] [16] [22]	ArchiMate concept description [14]	ArchiMate notation
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.	
Roles	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.	

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. Such modeling is based on Principles, Policies and Frameworks, Information and Organizational Structures enablers of COBIT 5 for Information Security.

Secondly, we will model the COBIT 5 for Information Security's processes and processes' practices in which CISO is responsible for, which are:

- EDM03.03 Monitor Risk Management;
- APO01.04 Communicate management objectives and direction;
- APO12.01 Collect data;
- APO12.06 Respond to risk.

The modeling of the processes' practices in which the CISO is responsible for is based on the Processes enabler.

Finally, we will model the key practices that he/she should be held responsible. Such modeling is based on the Organizational Structures enabler.

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

5.2. 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.

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.

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.

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

5.3. 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. With this, will be possible to identify which information types are missing and who is responsible for them.

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.

5.4. 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. With this, will be possible to identify which process' outputs are missing and who is delivering them.

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.

5.5. 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. With this, will be possible to identify which key practices are missing and who is responsible for them in the organization.

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.

5.6. 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 role defined in COBIT 5 for Information Security, in order to identify who is performing the CISO's job. This mapping allows to identify which roles of the organization are performing the job of the CISO.

5.7. STEP 7 – Analysis & TO-BE Design

Inputs: Approach to AS-IS

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.

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, described in COBIT 5 for Information Security. Furthermore, this viewpoint allows the organization to discuss the information security gaps detected, so they can properly 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.

In the Section "Demonstration", we will only present the viewpoints corresponding to the information types that the CISO is responsible for originating. Therefore, we will show the viewpoints of Steps 1, 2, 3 and 7, wherein the focus is solely the information types.

6. DEMONSTRATION

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

As a first step of the method, it is required to model the types of information that the CISO is responsible for originating. Figure 2, 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.

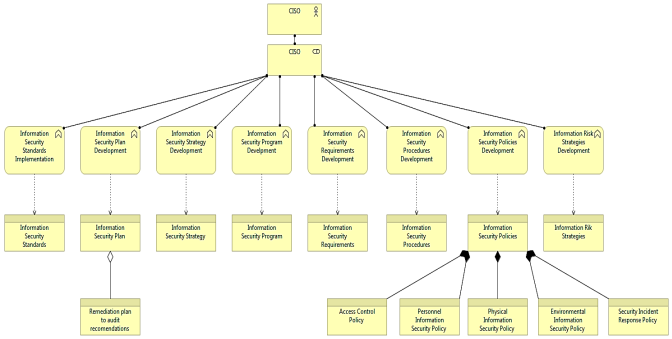


Fig. 2. CISO's Business Functions and Information Types

Then, following the method, it is expected that the processes for which the CISO is responsible for be represented. These viewpoints show the inputs, outputs and roles responsible of the

COBIT 5's process. Moreover, the key practices for which the CISO should be held responsible are required to be represented.

6.2. STEP 2 – Model Organization's EA

In the second step, we model the AS-IS of the organization's EA. Following the 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 3).

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.

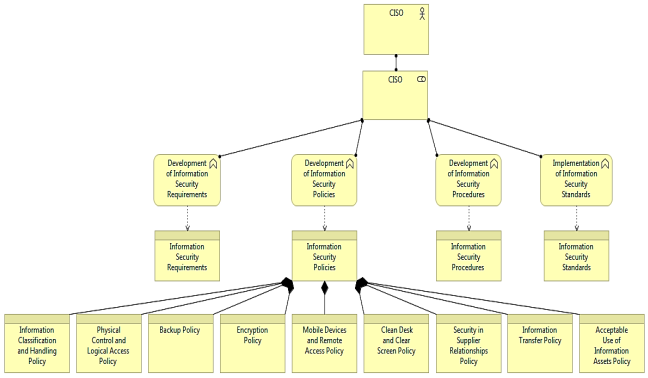


Fig. 3. DemoCorp's Business Functions and Information Types viewpoint

Then, it is required to model the organization's processes that are related to the processes represented in the previous section, for which the CISO is responsible.

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. When looking at roles and practices assigned, it is possible to observe which key practices the CISO is responsible for. Furthermore, some organization's practices cannot be part of the responsibilities of the CISO, i.e., there are other roles in the DemoCorp performing the CISO's job.

6.3. STEP 3 – Information types' mapping

Regarding the solution proposal's third step, in Figure 4 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.

When looking at this mapping, it is possible to identify which types of information are being originated and who is responsible for them in the organization. Moreover, this mapping allows us to detect information security gaps, since some information types are not defined in the DemoCorp, such as the information security plan, information risk strategies, information security program and information security strategy.

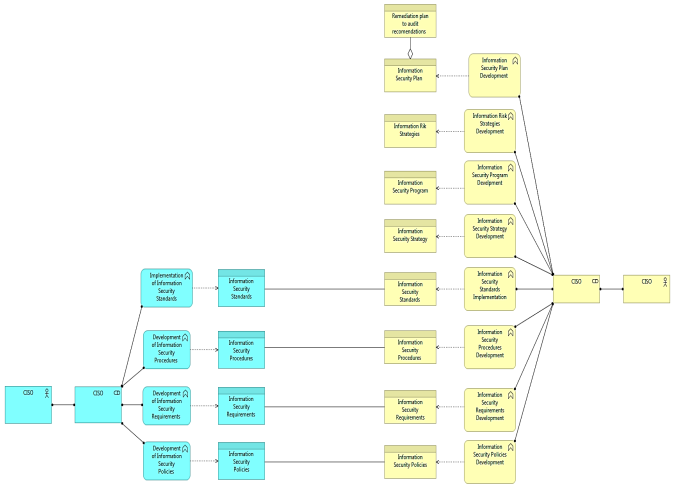


Fig. 4. Information Types' mapping viewpoint

6.4. STEP 4 – Processes output's mapping

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, the mapping of 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, is required for this step (see Figure 4). With this, it is possible to identify which process' outputs are missing and who is delivering them, in order to know which role is doing the CISO's job.

6.5. STEP 5 – Key Practices' mapping

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

This mapping allows us to detect information security gaps, regarding information security practices in which the CISO should be held responsible for.

6.6. STEP 6 – Roles' mapping

As stated in Section 4, 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, it is represented the organization's roles which are doing the CISO's job, defined in COBIT 5 for Information Security.

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

All of the mappings presented in Steps 3, 4, 5 and 6 will be the input for the next step of the proposed 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. 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 4, 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;
- Outputs of Process APO01 - Manage the IT Management Framework;
- Outputs of Process APO12 - Manage Risk;
- Outputs of Process EDM03 - Ensure Risk Optimization;
- Key Practices.

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 kinds of information, and outputs key practices the processes 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 INFOSEC IT Score.
- 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.

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.

Since the organization decided that only had to follow the IT Score's recommendations, not all the gaps identified are treated in the design of the DemoCorp's transition architecture. These recommendations aim to enable the organization to have a maturity level similar to that of the Financial Services organizations.

Figure 5 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 4, regarding the information types. Based on what has been described previously, we model 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.

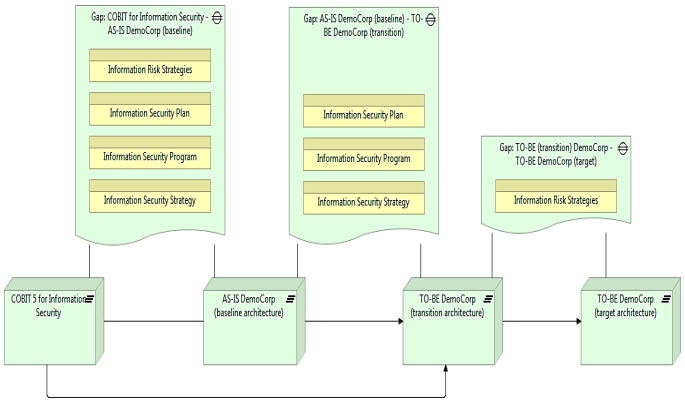


Fig. 5. Migration viewpoint: Information Types (Complete view)

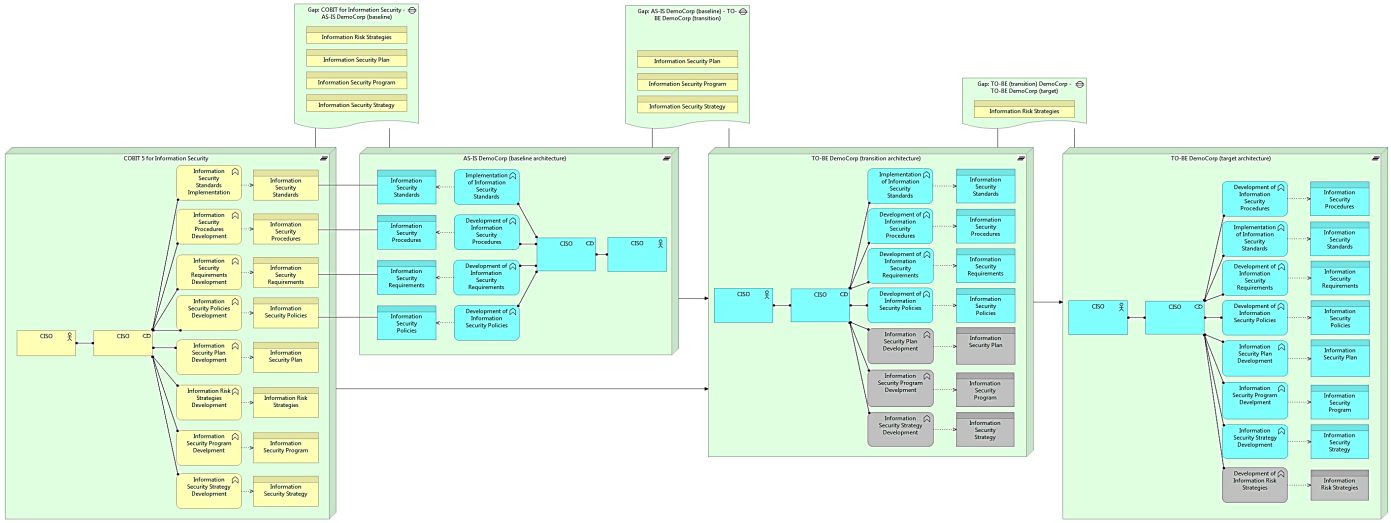


Fig. 6. Migration viewpoint: Information Types (Zoom-In)

As can be seen in the Figure 5, 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 Figure 6 (figure above) 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.

7. Evaluation

The evaluation of this work was accomplished by using the demonstration scenario at one government owned company.

For the evaluation, we compared the impact of the proposed method's implementation with the former approach used to implement the CISO's role in the DemoCorp and identified the relationship between the number of identified gaps and the evolution of DemoCorp's architecture.

7.1. Method Applied

Before applying the proposed method in this thesis, 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 and/or producing. Furthermore, the level of information security maturity remained lower than government organizations average [2.5 vs. 2.8].

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.

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 [23].

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

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

8. Communication

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

- *18th IEEE Conference on Business Informatics (CBI);*
- *13th European Mediterranean & Middle Eastern Conference on Information Systems (EMCIS).*

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 that should be seen as a framework in support of management and governance that provides a "thinking approach and structure" with very useful examples.

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. 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. 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.

We provided an effective solution that address the research problem and enables the information security implementation, particularly the CISO's role. 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. 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.

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?". [Online]. Available: http://www.computerweekly.com/opinion/Security-Zone-Do-You-Need-a-CISO. [Accessed: 24-Nov-2015].

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

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

[18] M. Lankhorst. "Enterprise Architecture at Work". Springer. 2005. ISBN: [978-3-540-24371-7].

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

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

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

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

[23] 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].

[24] ISO/IEC. "ISO/IEC 27001: Information Security Management System". ISO/IEC. Geneva. 2013.

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

[26] PCI Security Standards Council. "Payment Card Industry (PCI) Card Production". PCI Security Standards Council. USA. 2015.

[27] J. Westby and J. Allen. "Governing for Enterprise Security (GES) Implementation Guide". Software Engineering Institute. CMU/SEI-2007-TN-020. 2007.

[28] 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.