

Accountability for Information Security Roles and Responsibilities, Part 1

Using COBIT 5 for Information Security in ArchiMate

In recent years, information security has evolved from its traditional orientation, focused mainly on technology, to become part of the organization's strategic alignment, enhancing the need for an aligned business/information security policy.^{1,2} Information security is an important part of organizations since there is a great deal of information to protect, and it becomes important for the long-term competitiveness and survival of organizations. Thus, the information security roles are defined by the security they provide to the organizations and must be able to understand the value proposition of security initiatives, which leads to better operational responses regarding security threats.³

Organizations and their information storage infrastructures are vulnerable to cyberattacks and other threats.⁴ Many of these attacks are highly sophisticated and designed to steal confidential information. Therefore, enterprises that deal with a lot of sensitive information should be prepared for these threats because information is one of an organization's most valuable assets, and having the right information at the right time can lead to greater profitability.⁵ Enterprises are increasingly

recognizing information and related technologies as critical business assets that need to be governed and managed in effective ways.⁶

Information security is a business enabler that is directly connected to stakeholder trust, either by addressing business risk or by creating value for enterprises, such as a competitive advantage.⁷ Moreover, information security plays a key role in an organization's daily operations because the integrity and confidentiality of its information must be ensured and available to those who need it.⁸



Tiago Catarino

Is currently working in the Portfolio and Investment Department at INCM (Portuguese Mint and Official Printing Office). In the scope of his professional activity, he develops specialized activities in the field of information systems architectures in several transversal projects to the organization. His main academic interests are in the areas of enterprise architecture, enterprise engineering, requirements engineering and enterprise governance, with emphasis on IS architecture and business process engineering.

André Vasconcelos, Ph.D.

Is an assistant professor in the Computer Science and Engineering department at Instituto Superior Técnico, University of Lisbon (Portugal) and a researcher at Instituto de Engenharia de Sistemas e Computadores-Investigação e Desenvolvimento (INESC-ID) (Lisbon, Portugal). He has developed strategic advice in the area of information systems and business in several organizations. In the scope of his professional activity, he develops specialized advisory activities in the field of enterprise architecture for several digital transformation projects. He has written more than 80 publications, and he has been involved in several international and national research projects related to enterprise architecture, information systems evaluation and e-government, including several European projects.

These enterprises, in particular enterprises with no external compliance requirements, will often use a general operational or financial team to house the main information security blueprint, which can cover technical, physical and personnel-related security and works quite successfully in many ways.⁹

Nonetheless, organizations should have a single person (or team) responsible for information security—depending on the organization's maturity level—taking control of information security policies and management.¹⁰ This leads chief information security officers (CISOs) to take a central role in organizations, since not having someone in the organization who is accountable for information security increases the chances of a major security incident.¹¹

Some industries place greater emphasis on the CISO's role than others, but once an organization gets to a certain size, the requirement for a dedicated information security officer becomes too critical to avoid, and not having one can result in a higher risk of data loss, external attacks and inefficient response plans. Moreover, an organization's risk is not proportional to its size, so small enterprises may not have the same global footprint as large organizations; however, small and mid-sized organizations face nearly the same risk.¹²

COBIT® 5 for Information Security is a professional guide that helps enterprises implement information security functions. It can be instrumental in providing more detailed and more practical guidance for information security professionals, including the CISO role.^{13, 14}

The Problem

COBIT 5 for Information Security helps security and IT professionals understand, use, implement and direct important information security activities. With this guidance, security and IT professionals can make more informed decisions, which can lead to more value creation for enterprises.¹⁵

In particular, *COBIT 5 for Information Security* recommends a set of processes that are instrumental in guiding the CISO's role and provides 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.

However, *COBIT 5 for Information Security* does not provide a specific approach to define the CISO's role. Such an approach would help to bridge the gap between the desired performance of CISOs and their current roles, increasing their effectiveness and completeness, which, in turn, would improve the maturity of information security in the organization.

Moreover, this framework does not provide insight on implementing the role of the CISO in organizations, such as what the CISO must do based on COBIT® processes. It provides a "thinking approach and structure," so users must think critically when using it to ensure the best use of COBIT.

“THE CISO'S ROLE IS STILL VERY ORGANIZATION-SPECIFIC, SO IT CAN BE DIFFICULT TO APPLY ONE FRAMEWORK TO VARIOUS ENTERPRISES.”

Every organization has different processes, organizational structures and services provided. The CISO's role is still very organization-specific, so it can be difficult to apply one framework to various enterprises. This difficulty occurs because it is complicated to align organizations' processes, structures, goals or drivers to good practices of the framework that are based on processes, organizational structures or goals. The mapping of COBIT to the organization's business processes is among the many challenges that arise when assessing an enterprise's process maturity level.

COBIT® 5 has all the roles well defined and responsible, accountable, consulted and informed (RACI) charts can be created for each process, but different organizations have different roles and levels of involvement in information security responsibility.

ArchiMate is the standard notation for the graphical modeling of enterprise architecture (EA). Many

organizations recognize the value of these architectural models in understanding the dependencies between their people, processes, applications, data and hardware. Using ArchiMate helps organizations 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 organizations perform a gap analysis between the organization's as-is status to what is defined in *COBIT 5 for Information Security*, regarding:
 - Processes and base practices?
 - Key practices?
 - Business functions and information types?
 - Roles?
- Can ArchiMate's notation model all the concepts defined in *COBIT 5 for Information Security*?

Therefore, it is important to make it clear to organizations that the role and associated processes (and activities), information security functions, key practices, and information outputs where the CISO is included have the right person with the right skills to govern the enterprise's information security. For that, ArchiMate architecture modeling language, an Open Group standard, provides support for the description, analysis and visualization of interrelated architectures within and across business domains to address stakeholders' needs.¹⁶

EA and ArchiMate

EA is a coherent set of whole of principles, methods and models that are used in the design and realization of an enterprise's organizational structure, business processes, information systems and infrastructure.^{17, 18, 19} The EA process creates

“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 STATE.”

transparency, delivers information as a basis for control and decision-making, and enables IT governance.²⁰

EA is important to organizations, but what are its goals? The answers are simple:

- Understanding the organization
- Developing systems, products and services according to business goals
- Optimizing operations
- Optimizing organizational resources, including people
- Providing alignment between all the layers of the organization, i.e., business, data, application and technology²¹

Moreover, EA can be related to a number of well-known best practices and standards. **Figure 1** shows the management areas relevant to EA and the relation between EA and some well-known management practices of each area.

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 state. To promote alignment, it is necessary to tailor the existing tools so that EA can provide a value asset for organizations.

Figure 1—EA Management Areas vs. Management Practices

Strategic execution	European Foundation for Quality Management (EFQM)
Quality management	International Organization for Standardization (ISO) 9001
IT governance	COBIT 5
IT delivery and support	Information Technology Infrastructure Library (ITIL)
IT implementation	Capability Maturity Model (CMM) and Capability Maturity Model Integration (CMMI)

“ALTHOUGH EA AND COBIT® 5 DESCRIBE AREAS OF COMMON INTEREST, THEY DO IT FROM DIFFERENT PERSPECTIVES.”

The research here focuses on ArchiMate with the business layer and motivation, migration and implementation extensions.

ArchiMate provides a graphical language of EA over time (not static), and motivation and rationale. ArchiMate is divided in three layers: 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.²²

ArchiMate is a good alternative compared to other modeling languages (e.g., Unified Modeling Language [UML]) because it is more understandable, less complex and supports the integration across the business, application and technology layers through various viewpoints.²³

The business layer, which is part of the framework provided by ArchiMate, is where the question of defining the CISO's role is addressed. The business layer metamodel can be the starting point to provide the initial scope of the problem to address. Furthermore, ArchiMate's motivation and implementation and migration extensions are also key inputs for the solution proposal that helps with the *COBIT 5 for Information Security* modeling.

Proposal

EA, by supporting a holistic organization view, helps in designing the business, information and technology architecture, and designing the IT solutions.^{24, 25} COBIT® is a framework for the governance and management of enterprise IT, and EA is defined as a framework to use in architecting the operating or business model and systems to

meet vision, mission and business goals and to deliver the enterprise strategy.²⁶

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

Figure 2 shows the proposed method's steps for implementing the CISO's role using *COBIT 5 for Information Security* in ArchiMate.

This research proposes a business architecture that clearly shows the problem for the organization and, at the same time, reveals new possible scenarios. It also proposes 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. ArchiMate notation provides tools that can help get the job done, but these tools do not provide a clear path to be followed appropriately with the identified need.

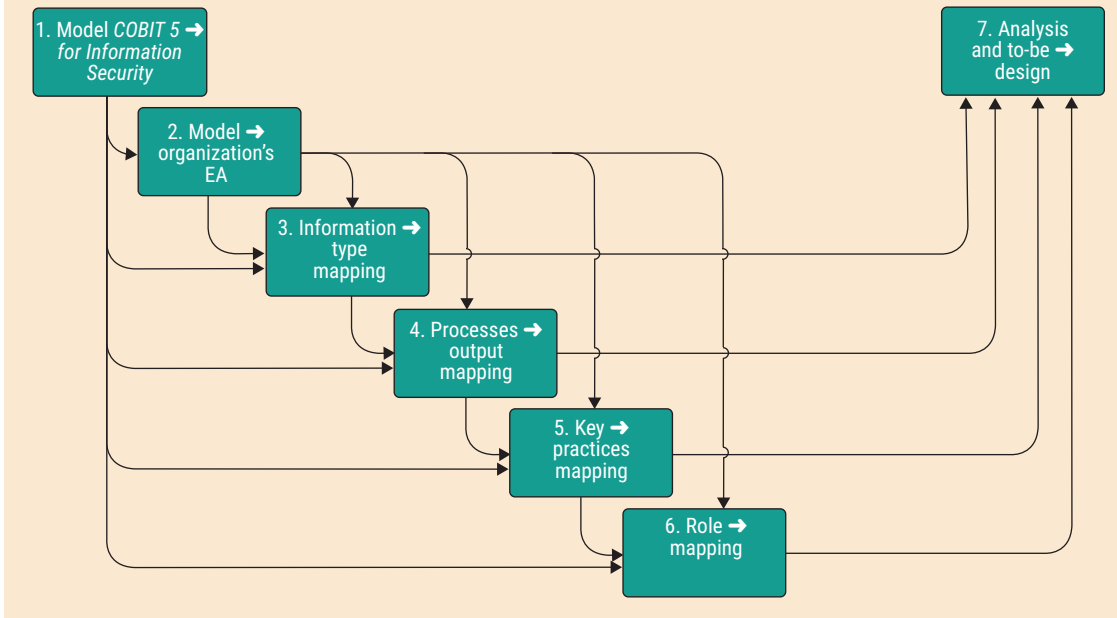
To maximize the effectiveness of the solution, it is recommended to embed the *COBIT 5 for Information Security* processes, information and organization structures enablers' rationale directly in the models of EA. The following focuses only on the CISO's responsibilities in an organization; therefore, all the modeling is performed according to the level of involvement "responsible" (R), as defined in *COBIT 5 for Information Security's* enablers.

The research problem formulated restricts the spectrum of the architecture views' system of interest, so the business layer, motivation, and migration and implementation extensions are the only part of the research's scope. Such modeling follows the ArchiMate's architecture viewpoints, as shown in **figure 3**.

Step 1—Model COBIT 5 for Information Security

In this step, inputting *COBIT 5 for Information Security* results in the outputs of CISO to-be business functions, process outputs, key practices and information types.

Figure 2—Proposed Method's Steps



COBIT 5 for Information Security can be modeled with regard to the scope of the CISO's role, using ArchiMate as the modeling language. **Figure 4** shows an example of the mapping between *COBIT 5 for Information Security* and ArchiMate's concepts regarding the definition of the CISO's role. The semantic matching between the definitions and explanations of these columns contributes to the proposed *COBIT 5 for Information Security* to ArchiMate mapping.

The definition of the CISO's role, the CISO's business functions and the information types that

the CISO is responsible for originating, defined in *COBIT 5 for Information Security*, will first be modeled using the ArchiMate notation. Such modeling is based on the Principles, Policies and Frameworks and the Information and Organizational Structures enablers of *COBIT 5 for Information Security*.

COBIT 5 for Information Security's processes and related practices for which the CISO is responsible will then be modeled. Those processes and practices are:

Figure 3—Solution's Step—ArchiMate Viewpoints

Proposed Method's Step	ArchiMate's Architecture Viewpoint			
	Organization Viewpoint	Business Process Viewpoint	Motivation Viewpoint	Migration Viewpoint
1. Model <i>COBIT 5 for Information Security</i>	X	X	X	
2. Model organization's EA	X	X	X	
3. Business functions mapping			X	
4. Processes output mapping		X		
5. Key practices mapping		X		
6. Role mapping	X			
7. Analysis and to-be design				X

Figure 4—COBIT 5 for Information Security to ArchiMate Ontological Mapping


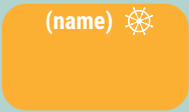
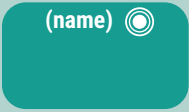
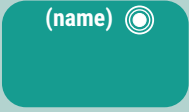
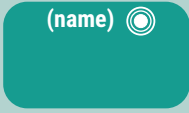
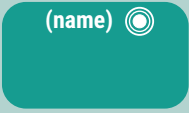

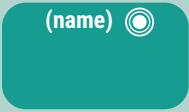
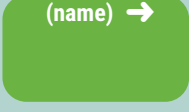
COBIT 5 for Information Security concept	COBIT 5 for Information Security Concept Description	ArchiMate Concept Description	ArchiMate Notation
Principle 1: Meeting Stakeholder Needs	Enterprises exist to create value for their stakeholders—including stakeholders for information security—by maintaining 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 is 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: <ul style="list-style-type: none"> • 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 artifact, 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 artifact, 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 artifact, 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 procedures that takes inputs from a number of sources (including other processes), manipulates the inputs and produces outputs (e.g., products, services).	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.	

Figure 4—COBIT 5 for Information Security to ArchiMate Ontological Mapping (cont.)

COBIT 5 for Information Security concept	COBIT 5 for Information Security Concept Description	ArchiMate Concept Description	ArchiMate Notation
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 Process Assessment Model 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 include: <ul style="list-style-type: none"> 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 competencies).	
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 a specific behavior to which an actor can be assigned.	
Inputs and outputs	The process work products/artifacts considered necessary to support process's operation.	A business object is defined as a passive element that has relevance from a business perspective.	

- Evaluate, Direct and Monitor (EDM) EDM03.03
Monitor risk management
- Align, Plan and Organize (APO) APO01.04
Communicate management objectives and direction
- APO12.01 *Collect data*
- APO12.06 *Respond to risk*

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

Finally, the key practices for which the CISO should be held responsible will be modeled. Such modeling is based on the Organizational Structures enabler. As an output of this step, viewpoints created to

“IF THERE IS NOT A CONNECTION BETWEEN THE ORGANIZATION’S INFORMATION TYPES AND THE INFORMATION TYPES THAT THE CISO IS RESPONSIBLE FOR ORIGINATING, THIS SERVES AS A DETECTION OF AN INFORMATION TYPES GAP.”

model the selected concepts from *COBIT 5 for Information Security* using ArchiMate will be the input for the detection of an organization’s contents to properly implement the CISO’s role.

Step 2—Model Organization’s EA

The inputs for this step are the CISO to-be business functions, processes’ outputs, key practices and information types, documentation, and informal meetings. The outputs are organization as-is business functions, processes’ outputs, key practices and information types.

In this step, it is essential to represent the organization’s EA regarding the definition of the CISO’s role. Such modeling aims to identify the organization’s as-is status 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* to determine what processes’ outputs, business functions, information types and key practices exist in the organization.

This step begins with modeling 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* for which the CISO is responsible) using the ArchiMate notation.

The organization’s processes and practices, which are related to the processes of *COBIT 5 for*

Information Security for which the CISO is responsible, will then be modeled.

Finally, the organization’s current practices, which are related to the key *COBIT 5 for Information Security* practices for which the CISO is responsible, will be represented.

Step 1 and step 2 provide information about the organization’s as-is state and the desired to-be state regarding the CISO’s role. Furthermore, these two steps will be used as inputs of the remaining steps (steps 3 to 6).

Step 3—Information Types Mapping

For this step, the inputs are information types, business functions and roles involved—as-is (step 2) and to-be (step 1). The output is the information types gap analysis.

In the third step, the goal is to map the organization’s information types to the information that the CISO is responsible for producing. With this, it 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 and the information types that the CISO is responsible for originating, this serves as a detection of an information types gap.

Step 4—Processes Outputs Mapping

The inputs are the processes’ outputs and roles involved—as-is (step 2) and to-be (step 1). The output is the 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* processes for which the CISO is responsible. With this, it will be possible to identify which processes’ outputs are missing and who is delivering them.

A missing connection between the processes’ outputs of the organization and the processes’ outputs for which the CISO is responsible to produce and/or deliver indicates a processes’ output gap.

Step 5—Key Practices Mapping

The inputs are key practices and roles involved—as-is (step 2) and to-be (step 1). The output is a gap analysis of key practices.

The fifth step maps the organization's practices to key practices defined in *COBIT 5 for Information Security* for which the CISO should be responsible. With this, it will be possible to identify which key practices are missing and who in the organization is responsible for them.

If there is not a connection between the organization's practices and the key practices for which the CISO is responsible, it indicates a key practice's gap.

Step 6—Roles Mapping

For this step, the inputs are roles as-is (step 2) and to-be (step 1). The output shows the roles that are doing the CISO's job.

This step maps the organization's roles to the CISO's role defined in *COBIT 5 for Information Security* to identify who is performing the CISO's job.

Step 7—Analysis and To-Be Design

The input is the as-is approach, and the output is the solution.

This step aims to analyze the as-is state of the organization's EA and design the desired to-be state of the CISO's role. This step requires:

- Identifying the organization's information security gaps
- Discussing with the organization's responsible structures and roles to determine whether the responsibilities identified are appropriately assigned

The purpose of this step is to design the as-is state of the organization and identify the gaps between the existent architecture and the responsibilities of the CISO's role as described in *COBIT 5 for Information Security*. Moreover, 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 that may be different for every organization to fix the identified information security gaps.

Conclusion

With the growing emphasis on information security and the reputational—and sometimes monetary—penalties that breaches cause, information security teams are in the spotlight, and they have many responsibilities when it comes to keeping the organization safe. *COBIT 5 for Information Security* effectively details the roles and responsibilities of the CISO and the CISO's team, but knowing what these roles and responsibilities are is only half the battle. Without mapping those responsibilities to the EA, ambiguity around who is responsible for which task may lead to information security gaps, potentially resulting in a breach. Using a tool such as ArchiMate to map roles and responsibilities to the organization's structure can help ensure that someone is responsible for the tasks laid out in *COBIT 5 for Information Security*.

An application of this method can be found in part 2 of this article. It demonstrates the solution by applying it to a government-owned organization (field study).

Endnotes

- 1 Vicente, M.; "Enterprise Architecture and ITIL," Instituto Superior Técnico, Portugal, 2013
- 2 Silva, N.; "Modeling a Process Assessment Framework in ArchiMate," Instituto Superior Técnico, Portugal, 2014
- 3 Whitten, D.; "The Chief Information Security Officer: An Analysis of the Skills Required for Success," *Journal of Computer Information Systems*, vol. 48, iss. 3, March 2008, <https://www.tandfonline.com/doi/abs/10.1080/08874417.2008.11646017>
- 4 De Souza, F.; "An Information Security Blueprint, Part 1," CSO, 3 May 2010, <https://www.csoonline.com/article/2125095/an-information-security-blueprint-part-1.html>
- 5 *Ibid.*

- 6 Cadete, G.; "Using Enterprise Architecture for Implementing Governance With COBIT 5," Instituto Superior Técnico, Portugal, 2015
- 7 ISACA®, *COBIT® 5 for Information Security*, USA, 2012, www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx
- 8 Olijnyk, N.; "A Quantitative Examination of the Intellectual Profile and Evolution of Information Security From 1965 to 2015," *Scientometrics*, vol. 105, iss. 2, p. 883-904
- 9 Olavsrud, T.; "Five Information Security Trends That Will Dominate 2016," *CIO*, 21 December 2015, <https://www.cio.com/article/3016791/5-information-security-trends-that-will-dominate-2016.html>
- 10 *Ibid.*
- 11 Moffatt, S.; "Security Zone: Do You Need a CISO?" *ComputerWeekly*, October 2012, <https://www.computerweekly.com/opinion/Security-Zone-Do-You-Need-a-CISO>
- 12 *Op cit* Olavsrud
- 13 *Op cit* ISACA
- 14 ISACA, *COBIT® 5*, USA, 2012, www.isaca.org/COBIT/Pages/COBIT-5.aspx
- 15 *Op cit* ISACA, *COBIT 5 for Information Security*
- 16 *Op cit* Cadete
- 17 Lankhorst, M.; *Enterprise Architecture at Work*, Springer, The Netherlands, 2005
- 18 Niemann, K. D.; *From Enterprise Architecture to IT Governance*, Springer Vieweg Verlag, Germany, 2006
- 19 Grembergen, W. V.; S. De Haes; *Implementing Information Technology Governance: Models, Practices and Cases*, IGI Publishing, USA, 2007
- 20 *Op cit* Lankhorst
- 21 *Ibid.*
- 22 Vicente, P.; M. M. Da Silva; "A Conceptual Model for Integrated Governance, Risk and Compliance," Instituto Superior Técnico, Portugal, 2011
- 23 The Open Group, "ArchiMate 2.1 Specification," 2013
- 24 *Op cit* Niemann
- 25 *Op cit* Grembergen and De Haes
- 26 *Op cit* Lankhorst
- 27 *Ibid.*