Mapping and Integration of Enterprise Governance of IT Practices

Renato Filipe Jacob Esteves Lourinho
Instituto Superior Técnico
Universidade de Lisboa, Portugal
renato.lourinho@tecnico.ulisboa.pt

Abstract*— Appropriate governance of information technology (IT) is critical to fully harness the benefits of IT investments in organizations. Enterprise Governance of IT (EGIT) can be deployed using a mixture of various structures, processes and relational mechanisms. Examples of process mechanisms are frameworks and ISO standards, such as COIBT 5 and ISO 27001. Yet, despite the availability of well-defined standards and frameworks as effective EGIT practices, organizations face a great deal of challenges when adopting these best-practices for process improvement, even more so when using multiple practices simultaneously. In order to reduce the perceived complexity of these practices and their complementary use, an Enterprise Architecture (EA) metamodel representation of ISO 27001 and its mapping with COBIT 5 was proposed using ArchiMate, an EA modeling language. To enable the completeness of the metamodel, ISO 27001 is extended with the ISO Technical Specification 33052 and 33072 which propose a Process Reference Model and a Process Assessment Model respectively. Afterwards, the research proposal was demonstrated by applying the ISO 27001 and COBIT 5 mapping metamodel to a COBIT 5 process. To demonstrate how this research helps reduce the perceived complexity of simultaneous assessments, a field study was conducted in a real organization for a specific COBIT 5 process. Finally, through peer-reviewed communication of early iterations of the proposal and interviews with field experts, the research proposal was evaluated based on generic evaluation criteria according to Design Science Research Methodology (DSRM).

Keywords*— ArchiMate, COBIT 5, Enterprise Architecture, Enterprise Governance of Information Technology, ISO 27001, ISO TS 33072.

I. Introduction

IT has the potential to support both existing and new business strategies, and as such it has moved from being a commodity service to be a strategic asset within today's digital enterprises [1]. Given this relatively new-found importance of IT, Enterprise Governance of IT (EGIT) has also gained new focus [1].

EGIT can be defined as "an integral part of corporate governance and addresses the definition and implementation of processes, structures and relational mechanisms in the organization that enable both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from IT-enabled business investments" [1].

Examples of process mechanisms are EGIT frameworks, Best Practices and ISO standards. The term EGIT Practices is used throughout this paper to refer to all standards and frameworks described.

While there is no single, complete, off-the-shelf EGIT Practice, there are several EGIT Practices available that can serve as useful starting points for developing a governance model [2]. Researchers agree that COBIT, ITIL, and ISO 27000 family are the most valuable and popular practices currently being adopted [3-5].

However, a recent study highlighted the fact that, despite acknowledging the importance of adopting EGIT Practices, many organizations have not adopted them [6]. Also, Winniford points out that less than half of the US companies surveyed had implemented any type of IT service management practice [7].

Thus, the main goal of this research is to reduce the complexity of COBIT 5 and ISO 27001 by designing visual models of these EGIT Practices, facilitating in this way their understanding. Therefore, we propose to use ArchiMate, as the Enterprise Architecture (EA) language, to model COBIT 5 and ISO 27001 metamodels, enabling in this way the integration of these EGIT Practices.

To enable this integration, we also present a modeled extension of ISO 27001 with the recent ISO Technical Specification (TS) 33052 – Process Reference Model (PRM) and ISO TS 33072 – Process Assessment Model (PAM) as these documents define relevant concepts that may be matched to COBIT concepts.

This paper is structured as follows: Section II presents a more detailed description of the research methodology; Section III states the problem in-depth; Section IV presents the related literature which describe the mechanisms and other approaches that inspired this research; Section V presents the proposal; Section VI presents an example demonstration of our mapping and integration; Section VII presents the theoretical evaluation for our models; Finally, Section VIII contains final conclusions, limitations and discussion of future work related to the topic.

II. Research Methodology

Our research follows the Design Science Research Methodology (DSRM). It involves a rigorous process to design artifacts to solve observed problems, to make research contributions, to evaluate the designs, and to communicate the results to appropriate audiences [8].

As per [9], this research methodology is applied according to the two processes of DSR in Information Systems: Build and Evaluate. Building is the process of constructing an artifact for a specific purpose; evaluation is the process of determining how well the artifact performs [9]. The Build process is in this research composed by two stages (Constructs Definitions and Model Construction) whereas the Evaluate process is comprised by only one (Evaluation) (Table I).

TABLE I. DESIGN SCIENCE RESEARCH METHODOLOGY

Build		**Evaluate**
Constructs Definitions	**Model Construction**	**Evaluation**
- Domain Definition - ISO 27001 and ISO TS 33052/33072 to ArchiMate Ontological Mapping	- ISO 27001 and ISO TS 33072 Metamodel - Integration of COBIT 5 and ISO 27001 Metamodels	- Prat's Criteria Hierarchy - Field study and interviews

III. Problem

Despite the growing importance of EGIT in organizations, several problems regarding EGIT Practices remain. IT organizations are facing the challenging, but necessary, transition to manage IT based on business priorities. They are looking for EGIT mechanisms, such as ISO 27001 and COBIT 5, to help them meet the challenge [10]. In fact, their adoption and practice is argued to be the most effective approach and guidance for organizations first considering proper implementation of EGIT [11].

The implementation of EGIT Practices should be consistent with the enterprise's risk management and control framework, appropriate for the enterprise, and integrated with other methods and practices that are being used [12]. Therefore, management and staff must understand what to do, how to do it and why it is important to do it [12]. However, there seems to be some confusion regarding EGIT Practices and how best to use them [10].

For example, there is no fully complete EGIT Practice to be used as a comprehensive off-the-shelf solution to ensure the alignment between service management and the organization's concepts and artifacts [13]. In fact, different EGIT Practices are often used as complementary and, most of the times, simultaneously too. Parallel projects imply a duplication of investments and costs, and even with shared infrastructures we cannot avoid a duplication of data repositories, procedures and human resources, being hard to define a way for teams not to compete or maintain different efforts aligned [13].

Since all these EGIT Practices overlap, using them independently prevents organizations from asserting full IT management and governance because each practice has limitations in its application to the management of specific IT areas [14].

Individually, it has been stated that COBIT cannot work alone as it is not very detailed, and shows what to do but not how to do [15]. Moreover, its implementation was found to be difficult as it is too generic, and thus requires expert knowledge [16].

Regarding ISO 27001 many organizations find it difficult and challenging to implement this practice along with other information security management practices [17]. Being employed as a standalone guide and not being integrated into a wider practice for EGIT makes it difficult for organizations that adopt ISO 27000 family standards to implement other EGIT Practices [18].

Therefore, in a time when organizations strive to be efficient and effective, it seems counter-intuitive to be wasting resources by having different organizational departments handling both approaches independently [19]. In that way, organizations are avoiding implementing different EGIT Practices, despite recognizing its importance.

To sum up, the problem that this research intends to help solve is the following one: **Organizations struggle with the complexity and difficulty of understanding different EGIT Practices, and thus adopting these practices simultaneously needs large investments, that sometimes even prevent their adoption.**

The adoption of COBIT 5 in organizations is widely described as challenging due to the high perceived complexity of COBIT 5 [1]. In contrast to objectively measurable complexity, perceived complexity results from the distinctions made by a subjective observer [20].

IV. Related Work

In this section, we describe the main theories and concepts that form the basis of our proposal.

A. *COBIT 5*

COBIT 5 is based on five principles: meeting stakeholder needs; covering the enterprise end-to-end; applying a single, integrated framework; enabling a holistic approach; and separating governance from management [21]. Together these principles enable enterprises to assemble and deploy an effective EGIT and management framework and thus support striking balance between benefits realization, risk management and resources [21].

COBIT 5 evolution unified ISACA's three frameworks: Val IT, a value delivery focused framework; Risk IT, a risk management focused framework and previous COBIT versions. Hence this allowed COBIT 5 to cover the lifecycle of governance and management within the scope of enterprise IT [1] COBIT 5 also introduced a new process-reference model, new processes, updated and expanded goals and metrics, and alignment with the ISO 15504 process-capability-assessment model [21].

B. *ISO 27001 and ISO TS 33052/33072*

The ISO 27000 standard family is known as the "Information Security Management System (ISMS) Family of Standards", providing best practice recommendations on information security management within the context of a broad ISMS [22]. Providing guidelines to follow in implementing and running an ISMS, it enables organizations to assemble a framework for managing the security of information assets. Independent assessment of implemented ISMS is also covered in these standards [22].

ISO 27001 provides requirements for implementing, maintaining, and improving an ISMS [23]. Organizations implement this standard to address security requirements in a consistent, repeatable, and auditable manner [24]. An ISMS provides risk management processes such that it preserves confidentiality, integrity, and availability of information. It is of importance that this risk management process is integrated with the organization's processes and information security is included in a holistic manner within the scope of process design, information systems and controls.

Published in 2016, ISO TS 33072 [25] is an International Standard Technical Specification that proposes a Process Assessment Model (PAM) enabling the assessment of processes based on the ISO 27001 requirements statements. To be able to perform an assessment, ISO TS 33072 presents Base Practices and Information Items/Outcomes which compose the processes defined in ISO TS 33052 [26]. Conceptually, these Base Practices and Information Items are similar to COBIT 5 own Base Practices and Work Products and can be shown to be related as COBIT's holistic nature provides coverage over the domain of information security.

C. *Integrating EGIT Practices*

The basic difference between COBIT and ISO 27001 is that ISO 27001 is only focused on information security, whereas COBIT is focused on more general information technology controls. Thus, COBIT has a broader coverage of general information technology topics, but does not have as many detailed information security requirements as ISO 27001 [27].

Alignment between COBIT and ISO 27001 has been approached by several researches [5, 12, 27, 28] but these researches either map EGIT Practices at a very abstract level, matching process similarity criteria [24, 28], or have mapped previous versions that have been superseded such as COBIT 4.1 and ISO 27001:2005 [5, 12, 27].

Despite these obstacles, such researches provide valuable guidance regarding the alignment of the current versions of COBIT and ISO 27001. One such case is the choice of which process is most adequate for a mapping demonstration. A sought for trait is a high level of similarity between corresponding processes described by the EGIT Practices. For this issue, [28] provide a process level method for analysis between ISO 27001 and COBIT.

D. *ArchiMate*

The objective of the ArchiMate language is to provide well-defined relationships between concepts in different architectures, the detailed modeling of which may be done using other, standard, or proprietary modeling languages. Concepts in the ArchiMate language cover the business, application, and technology layers of an enterprise and provide an extended layer that represents the motivation. Services offered by one layer to another play an important role in relating the layers [29].

ArchiMate provides a uniform representation for diagrams that describe EAs and offers an architectural approach that describes and visualizes the different architecture domains and their underlying relations and dependencies [30].

E. *ArchiMate and EGIT Practices*

As far as the authors are aware, there are few approaches that propose to model and integrate EGIT mechanisms using ArchiMate as the architecture's modeling language, enabling the integration of these EGIT Practices in a standard-based EA representation. We would like to highlight three of them:

Almeida et al. mapped, modeled, and integrated COBIT 5 and COSO in ArchiMate [31].

Another research [32] proposed a model that uses TIPA [33] for the Information Technology Infrastructure Library (ITIL), COBIT PAM and ArchiMate to analyze the impact of ITIL implementation on COBIT processes performance, and vice-versa.

Furthermore, a technical report from the Luxembourg Institute of Science and Technology presents the whole outputs of the conceptual alignment between concepts used to model EA (based on ArchiMate, TOGAF, IAF and DoDAF) and concepts of the Information System Security Risk Management domain model.

These researches were an important contribution to our research. In this research, we decided to use the COBIT 5 metamodel proposed by [32], since the scope of this paper is to map COBIT 5 and ISO 27001.

F. *Modeling Techniques and Principles*

While there are several EGIT Practices well established to support management and Enterprise Governance of IT, there is a lack of theoretical foundation [34], which can contribute to the evolution and adaptation of said EGIT Practices.

To support and enable these evolutions it is common to use models as a form of abstraction from real word scenarios. If the object of research is an abstraction and as such, already a model, then we create models of models, or so-called metamodels as per the defined model stack [35] in Fig. 1.

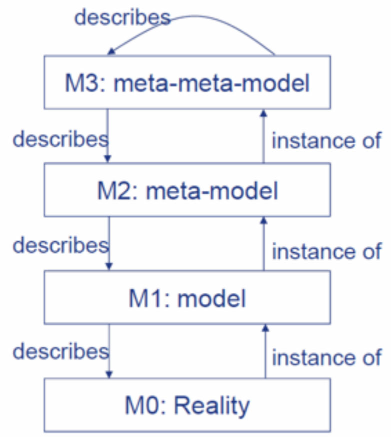


Fig. 1. Model Stack [34]

Metamodels provide concepts, properties, operations and relations needed to design any kind of model [36], enabling the integration of multiple models into a single model by establishing well-defined relationships.

In order to develop high quality models, [37] proposed the so-called *guidelines of modeling*, which propose six principles to raise the quality of information modeling. Since our metamodels are models of models, these principles are applicable and are as follows:

1. *Principle of construction adequacy* states that the quality of a model depends on the representation of reality, the designer viewpoint and context of modeling;
2. *Principle of language adequacy* is related to the adequacy of the chosen modeling language. In our case, ArchiMate is adequate to model and integrate the structural components of COBIT 5 and ISO 27001;
3. *Principle of economic efficiency* suggests restriction on economic factors, meaning that the organization should consider the cost-benefit of modeling;
4. *(5.) Principles of clarity and systematic design* are in regard of the comprehensibility of the model. Systematic design requires consistency and comprehensiveness of the models. These are important for metamodel integration as they directly contribute to the goal of this research of reducing perceived complexity;
6. *Principle of comparability* is also of importance in the metamodel level as metamodels are often used to compare different instances at an abstraction level.

Reference [34] propose that these principles must be extended with three other guidelines to be applicable to metamodeling. The **first guideline** is *"A metamodel has to reveal its principle of metaization"* meaning that there must be an ontological metamodel which forms the base of the developed metamodels – this is covered by the ontological mapping in the proposal.

The **second guideline** states that the metamodeling should be clear in *"mapping between a concept and its meaning in the scope of the metamodel"*. This translates to minimizing or removing linguistic defects such as synonyms or homonyms, where components in different EGIT Practices might have the same name with different semantic meanings. For this research, the ArchiMate metamodel bridges the gaps between concepts.

The **third guideline** proposed is the *"use of semantically rich connections"*. This is since EGIT Practices relationships such as '*is created by*' or '*contains*' are not elementary and/or ambiguous. Thus, a language with semantically rich connections, such as ArchiMate, should be able to provide the designers with the necessary tools to express such relationships.

V. Proposal

One of the most important sections of IT within COBIT, is information security management that covers confidentiality, integrity and availability of resources. Since the issue raised is the area covered by the standard ISO 27001, the best option to meet information security management in COBIT infrastructure is mapping the ISO 27001 standard [27]. The purpose of the mapping is to provide an integrated way for complementary use of COBIT and ISO 27001 for information security management.

Mainly, there are two reasons to start with the conceptual metamodeling of these practices [34]. COBIT 5 is well structured in domains, processes and other components and, therefore, closed and self-contained. Also, COBIT is holistic and represents (nearly) all tasks and processes an IT organization should carry out. ISO 27001 was chosen because it is a security standard for Information Security Management System (ISMS) that is a highly dynamic and complex task due to constant change in the information technology domain [38].

To achieve this mapping, for each COBIT 5 process we looked for every related ISO 27001 control category. Upon assessing the applicability of each mapping, we mapped each individual ISO 27001 control to all COBIT 5 processes. We found that every control in each category was related to the process, meaning that once we found matching process and control categories, none of its controls were irrelevant. To enable a consistent and comprehensive integration, all related concepts must be mapped, including COBIT 5 Base Practices and Work Products. Although the ISO 27001 does not describe equivalent concepts, the recent ISO TS 33052 and ISO TS 33072 do describe similar concepts.

Reference [28] provides empirical evidence to support a certain process choice for demonstration. In this paper, we decided to use the COBIT 5 process "Manage Service Requests and Incidents" for our demonstration which equates to the process "Incident and service request management" in [28], which presents a strong relation between the COBIT 5 process and the ISO 27001 controls.

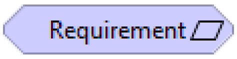
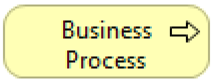
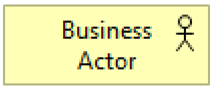
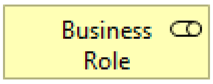
As stated, there are in the literature some mappings regarding these EGIT Practices [27, 28]. However, as the authors are aware, none of the researches use the latest version of both COBIT 5 and ISO 27001 (this means that they map older versions of these mechanisms). Moreover, they do not use an EA representation.

Therefore, we propose to use ArchiMate, as the EA language, to model COBIT 5 and ISO 27001 metamodels, enabling in this way the integration of these EGIT Practices.

A. ISO 27001 Metamodel

To develop a metamodel for ISO 27001 using ArchiMate, we first mapped the main ISO 27001 and ArchiMate concepts, as shown in Table II.

TABLE II. ISO 27001 AND ARCHIMATE ONTOLOGICAL MAPPING

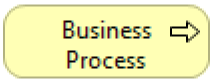
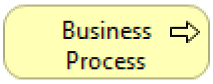
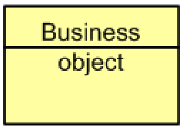
ISO 27001 Concept	ISO 27001 Concept Description [22]	ArchiMate Notation	ArchiMate Concept Description [30]	ArchiMate Representation
Requirement	Need that is stated, generally implied or obligatory.	**Requirement**	A statement of need that must be realized by a system.	
Control Objective	Statement describing what is to be achieved as a result of implementing controls.	**Goal**	An end state that a stakeholder intends to achieve.	
Control	Measure that is modifying risk.	**Business Process**	A behavior element that groups behavior based on an ordering of activities. It is intended to produce a defined set of products of business services.	
Organization	Person or group of people that has its own functions with responsibilities to achieve its objectives.	**Business Actor**	An entity that performs behavior in an organization such as business processes or functions.	
Top Management	Person or group of people who directs and controls an organization at the highest level.	**Stakeholder**	The role of an individual, team, or that represents their interests in, or concerns relative to, the outcome of the architecture.	Stakeholder
Risk Owner	Person or entity with the accountability and authority to manage a risk.	**Business Role**	A named specific behavior of a business actor participating in a given context.	
Information Security Needs	**Policy -** intentions and direction of an organization. **Information need -** insight necessary to manage objectives, goals, risks and problems. **External context -** external environment including key drivers and trends.	**Driver**	A driver is defined as something that creates, motivates, and fuels the change in an organization.	

As this research extends the ISO 27001 metamodel with ISO TS 33052 and 33072 concepts, these are also ontologically mapped to ArchiMate in Table III.

Based on these ontological mappings, we propose the metamodel as shown in Fig. 2.

Some considerations regarding this ISO 27001 metamodel:

Table III. ISO TS 33052/33072 AND ARCHIMATE ONTOLOGICAL MAPPING

ISO TS 33052/33072 Concept	ISO TS 33052/33072 Concept Description [25, 26]	ArchiMate Notation	ArchiMate Concept Description [30]	ArchiMate Representation
Process	Set of interrelated or interacting activities which transforms inputs into outputs.	**Business Process**	As per Table II.	
Base Practice	Activity that, when consistently performed, contributes to achieving a specific process purpose.	**Business Process**	As per Table II.	
Information Item/Outcomes	Observable result of the successful achievement of the process purpose.	**Business Object**	A business object is defined as a passive element that has relevance from a business perspective.	

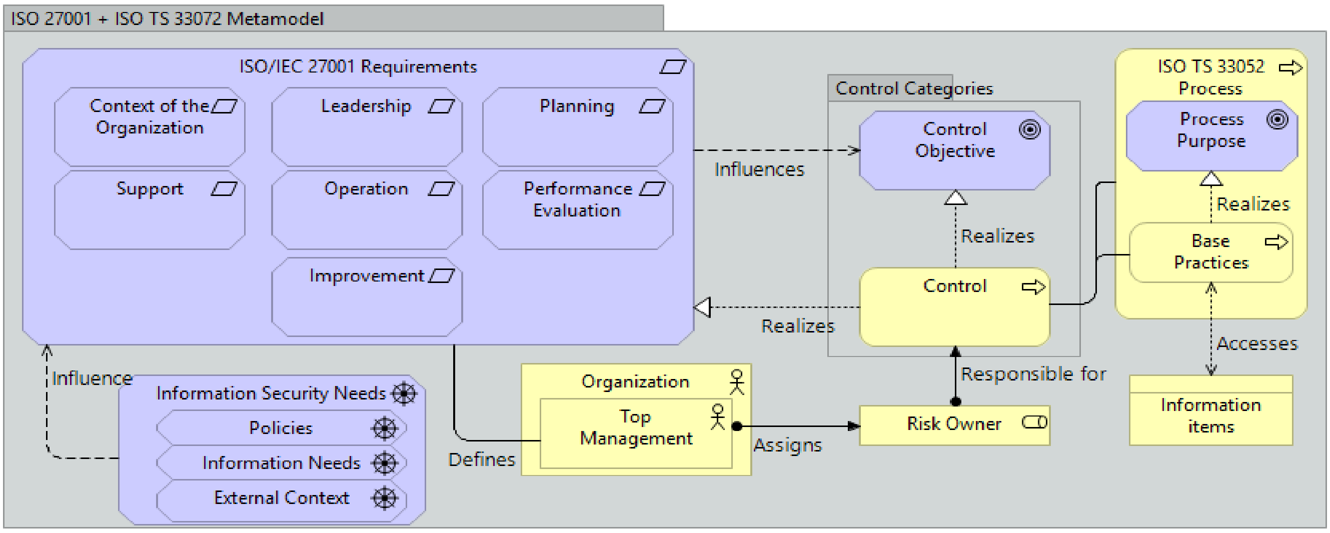


Fig. 2. ISO 27001 and ISO TS 33052/33072 Metamodel

Controls realize requirements by derived relationship through Control Objectives; Requirements influence Control Objectives meaning that implementation of ISO 27001 should fit an organization's risk management and processes already in place. Thus, an organization's needs become a driver which influences requirements, which in turn influence the controls needed to be implemented.

The ISO 27001 presents a set of normative requirements, including a set of controls for management and mitigation of the risks associated with the information assets which the organization seeks to protect. This motivation – Driver in the ArchiMate language – influences which requirements the organization should implement, whether they are security, legal or business requirements.

Thus, as the organizational needs influence the general requirements, so does the choice of those general requirements influence the set of controls (or control categories) and other specific requirements to be implemented.

Also, it is important to note that while ISO TS 33075 Information Items/Outcomes are conceptually equivalent to COBIT's Work Products as they follow the same logic and metamodel defined in the ISO 15504 standard (which is the reference model for maturity models such as the ISO TS 33072), we keep the Information Items terminology throughout this paper to distinguish the COBIT and ISO input/output concepts.

B. *Integration of EGIT Practices Metamodels Using ArchiMate*

In Fig. 3 we propose a metamodel that encompasses COBIT 5, ISO 27001 and ISO TS 33052/33072 using ArchiMate. Some considerations regarding this model: COBIT 5 processes and ISO 27001 controls are related by structural association, meaning they can be mapped from one to another and vice-versa; A COBIT 5 process is composed by one or more ISO 27001 control categories. Each category contains a single control objective and one or more controls.

This integration model is based on the mapping between COBIT 5 processes and ISO 27001 controls performed by the authors. By semantically assessing the descriptions of both processes, control objectives and controls, it was found that when a COBIT 5 process matches one or more ISO 27001 control categories, all the controls pertaining to that set are relevant to the COBIT 5 process. Thus, we consider a direct

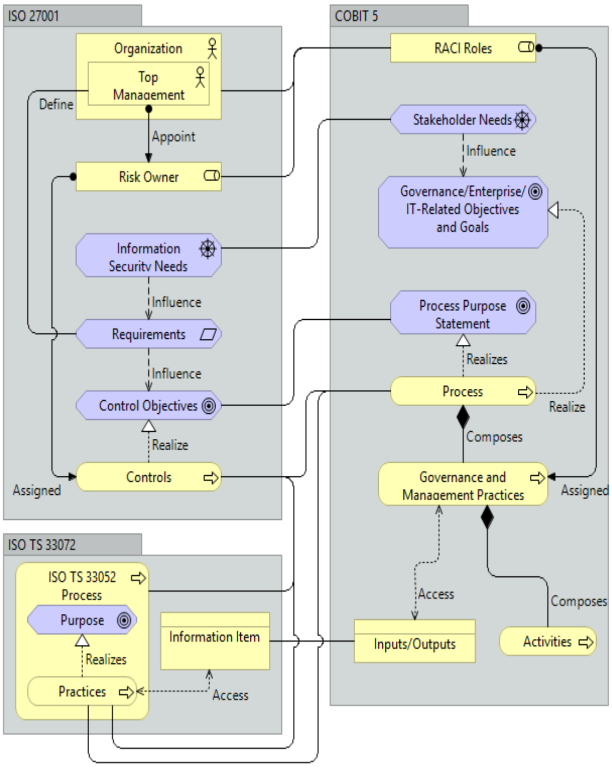


Fig. 3. COBIT 5 – ISO 27001 – ISO TS 33052/33072 Metamodel

structural association between ISO 27001 controls and a COBIT 5 process due to the more generalized scope of COBIT 5 where its processes, in some way or another, relate to an information asset which can be protected.

Regarding the relationships between Base Practices, while some ISO 27001 controls map exclusively to some ISO TS 33052 process and vice-versa, and therefore its related Base Practices, this is not always the case and thus we cannot state that all controls map directly to these processes; but all controls map to one or more Base Practices in an *ad-hoc* relation. Consequently, the same reasoning applies to Work Products and Information Items.

C. Modeling Principles Fitness

1) Principle of construction adequacy

This principle judges the adequacy of the model to the reality, the designer's viewpoint, and modeling context. Context wise, the models in this proposal are fundamentally theoretical, and as such they have been developed based on the EGIT Practices' documentation and the related literature. Accordingly, the designer's (the authors') viewpoint is also theoretical and thus the models are focused on abstracting the concepts and establishing the existing relationships between the determined concepts.

As the models strictly follow the architectures described in the EGIT Practices' documentations, we consider the models to fit adequately for the intended purposes.

2) Principle of language adequacy

The ArchiMate core language provides the basic concepts and relationships to fulfil the general EA modeling needs. It offers an architectural approach that describes and visualizes the different architecture domains and their underlying relations and dependencies.

As such, ArchiMate fits the purpose of our metamodels which is to compare, map and integrate different EGIT Practices at a component level. As this principle also includes consistency and completeness, meaning that our models do not include any symbol that is not present in the language metamodel, our ontological mapping between ISO 27001, ISO TS 33052/33072 and COBIT 5 (in the related literature) shows that ArchiMate is adequate as our modeling language.

3) Principle of economic efficiency

As our goal is to develop an integration metamodel from a theoretical perspective, this principle is in a sense, not applicable to the development of our models, although in practice reducing the perceived complexity of integrating COBIT and ISO 27001 promotes economic efficiency within an organization as an outcome of this research.

4) 5) Principle of clarity and systematic design

This principle is assured by the modeling language ArchiMate, as a visual architectural language, and our ontological mapping between its concepts and the EGIT Practices concepts, since we include all relevant concepts for the scope of this research, thus obtaining a comprehensive metamodel which fulfils the systematic design principle.

6) Principle of comparability

As the goal of this research is to compare and integrate the COBIT and ISO 27001 metamodels, this principle is fulfilled by bridging semantical discrepancies through the ArchiMate metamodel. Moreover, as COBIT is a comprehensive EGIT Practice that also provides coverage of the ISM domain, many concepts are semantically compatible and therefore comparable.

VI. Demonstration

This section describes the assessment performed for the COBIT 5 process "DSS02 – Manage Service Requests and Incidents" in a real organization, the Portuguese Navy's IT Oversight division (Superintendência de Tecnologias de Informação – STI), specifically in the Computer Incident Response Capability Core (Núcleo CIRC – NCIRC) responsible for Information Security Management (ISM) and the IT and Communications Administration (Direção de Tecnologias de Informação e Comunicação – DITIC) which houses the service requests and incident Service Desk.

In order to properly assess the process in an unfamiliar organization, it was relevant to first establish the context of the process performed in a top-down perspective, as to enable us to describe holistically the "as-is" state of the process.

In 2015, the Navy's STI compiled an Administrative Directive (Directiva Sectorial da STI, 2015) document describing, within STI's scope, future goals, and lines of action to achieve those goals. From this document we could establish the relevant Strategic Goals (modeled by a Goal concept in ArchiMate), Lines of Action (modeled as the homonym concept in ArchiMate 3.0 Strategic Layer) and from these, establish which STI competencies (modeled as Capability concept in ArchiMate 3.0 Strategic Layer) and actual resources (modeled as Resource concept in ArchiMate 3.0 Strategic Layer) are relevant (DITIC and NCIRC) to drill-down and assess the process in question.

With the relevant resources established, we modeled the contextual organizational viewpoint of the process. Its utility is to understand at a glance which functions, and internal processes are triggered by incident or service request events, what roles and actors are assigned to those functions, and what applications and applicational data are involved in this management process.

To enable the process capability assessment, it was then required to assess the existence of process deliverables as outputs and match them to COBIT 5 "Output" definitions.

To this end, we compiled an interview questionnaire with a set of questions for each "Base Practice".

Once the process was assessed and found to be at Capability Level 1 and thus the "DSS02 – Manage Service Requests and Incidents" "Outputs" are largely defined and produced, we can assert that the process "Outcomes" are realized. We can then map the assessed COBIT 5 process "Outputs" to their ISO TS 33072 counterparts and then trace back to the mapped ISO 27001 controls.

Figure 4 shows the resulting ArchiMate viewpoint of the mapped concepts. The "incident and service request classification schemes and models" output is marked as orange because while it was assessed to be defined and used, it was also assessed to not be properly managed (a requirement for further Process Capability Level achievement). Thus, we cannot assert that the mapped ISO 27001 control is completely executed. As such, it becomes an identified "pain point" of the "as-is" process and a target for process improvement.

The COBIT 5 process outputs "fulfilled service requests" and "approved service requests" are marked blue and show no relation to ISO TS 33072 Information Items (and so they are unable to trace back to ISO 27001 controls) since COBIT 5 framework has a broader coverage of EGIT domains than ISO 27001, so they fall out-of-scope for ISO 27001 controls.

The ISO 27001 controls within the "17.1 – Business Continuity" control group are marked red as they are related to COBIT 5 process inputs and as such, they are to be assessed and mapped from the outputs of COBIT 5 another process.

VII. Evaluation

Existing frameworks for evaluation in DSR characterize evaluation strategies along two dimensions, *naturalistic* versus *artificial*, and *ex-ante* versus *ex-post*. Ex-post evaluates instantiation classed artifacts while ex-ante evaluation assesses an uninstantiated artifact [40]. Naturalistic evaluation explores the performance of a solution technology in its real environment. Artificial evaluation includes laboratory experiments, field experiments, simulations, criteria-based analysis, theoretical arguments and mathematical proofs [41].

With these evaluation strategies in mind, this research was evaluated in a two-fold manner: in earlier iterations the evaluation was on an ex-ante, artificial based evaluation through the theoretical instantiation presented in Chapter 5 as well as criteria-based analysis and peer-reviews. More recent iterations were evaluated on an ex-post and combination of naturalistic and artificial evaluation strategies through an instantiation in a real organization and by interviewing our point-of-contact practitioners in the Portuguese Navy with a criteria-based questionnaire as to assess the applicability of our models.

For this questionnaire we used the evaluation criteria hierarchy recommended by Prat et al. [40] described in Figure 5, which highlights in blue the criteria selected for the earlier – ex-ante, artificial – evaluations and in red the criteria relevant for the later – ex-post, naturalistic – evaluation.

VIII. Conclusion

In this paper, we illustrate the modeling and integration of COBIT 5 and ISO 27001 metamodels using ArchiMate, enabling the integration of these EGIT Practices and their inclusion into the scope of existing EA techniques.

Thus, we believe the visual representation of COBIT 5 and

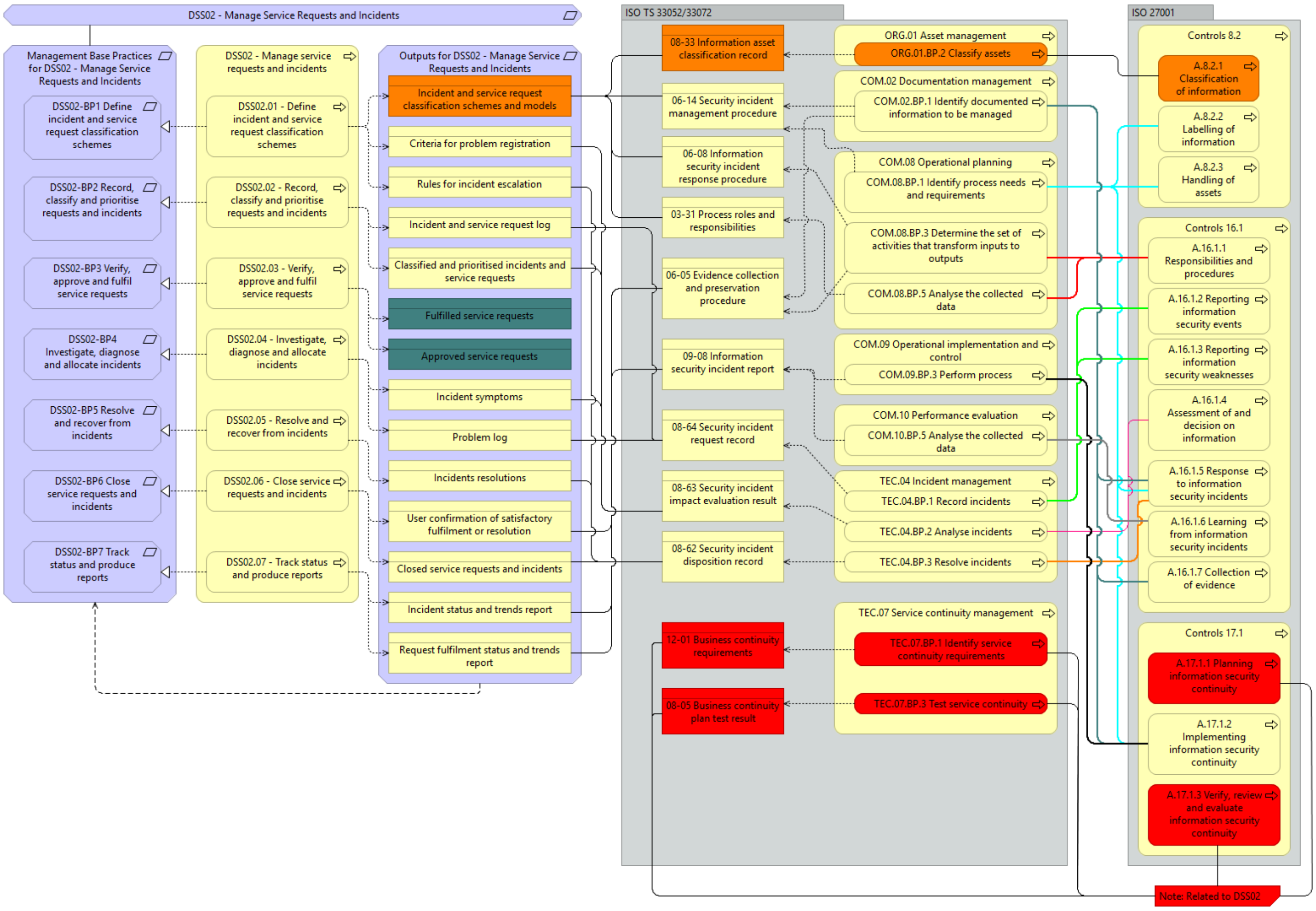

DSS02 - Manage Service Requests and Incidents
Management Base Practices for DSS02 - Manage Service Requests and Incidents
DSS02-BP1 Define incident and service request classification schemes
DSS02-BP2 Record, classify and prioritise requests and incidents
DSS02-BP3 Verify, approve and fulfil service requests
DSS02-BP4 Investigate, diagnose and allocate incidents
DSS02-BP5 Resolve and recover from incidents
DSS02-BP6 Close service requests and incidents
DSS02-BP7 Track status and produce reports
DSS02 - Manage service requests and incidents
DSS02.01 - Define incident and service request classification schemes
DSS02.02 - Record, classify and prioritise requests and incidents
DSS02.03 - Verify, approve and fulfil service requests
DSS02.04 - Investigate, diagnose and allocate incidents
DSS02.05 - Resolve and recover from incidents
DSS02.06 - Close service requests and incidents
DSS02.07 - Track status and produce reports
Outputs for DSS02 - Manage Service Requests and Incidents
Incident and service request classification schemes and models
Criteria for problem registration
Rules for incident escalation
Incident and service request log
Classified and prioritised incidents and service requests
Fulfilled service requests
Approved service requests
Incident symptoms
Problem log
Incidents resolutions
User confirmation of satisfactory fulfilment or resolution
Closed service requests and incidents
Incident status and trends report
Request fulfilment status and trends report
ISO TS 33052/33072
08-33 Information asset classification record
06-14 Security incident management procedure
06-08 Information security incident response procedure
03-31 Process roles and responsibilities
06-05 Evidence collection and preservation procedure
09-08 Information security incident report
08-64 Security incident request record
08-63 Security incident impact evaluation result
08-62 Security incident disposition record
12-01 Business continuity requirements
08-05 Business continuity plan test result
ORG.01 Asset management
ORG.01.BP.2 Classify assets
COM.02 Documentation management
COM.02.BP.1 Identify documented information to be managed
COM.08 Operational planning
COM.08.BP.1 Identify process needs and requirements
COM.08.BP.3 Determine the set of activities that transform inputs to outputs
COM.08.BP.5 Analyse the collected data
COM.09 Operational implementation and control
COM.09.BP.3 Perform process
COM.10 Performance evaluation
COM.10.BP.5 Analyse the collected data
TEC.04 Incident management
TEC.04.BP.1 Record incidents
TEC.04.BP.2 Analyse incidents
TEC.04.BP.3 Resolve incidents
TEC.07 Service continuity management
TEC.07.BP.1 Identify service continuity requirements
TEC.07.BP.3 Test service continuity
ISO 27001
Controls 8.2
A.8.2.1 Classification of information
A.8.2.2 Labelling of information
A.8.2.3 Handling of assets
Controls 16.1
A.16.1.1 Responsibilities and procedures
A.16.1.2 Reporting information security events
A.16.1.3 Reporting information security weaknesses
A.16.1.4 Assessment of and decision on information
A.16.1.5 Response to information security incidents
A.16.1.6 Learning from information security incidents
A.16.1.7 Collection of evidence
Controls 17.1
A.17.1.1 Planning information security continuity
A.17.1.2 Implementing information security continuity
A.17.1.3 Verify, review and evaluate information security continuity
Note: Related to DSS02

Fig. 4 Instantiation of a COBIT process with ISO controls, base practices, and information items

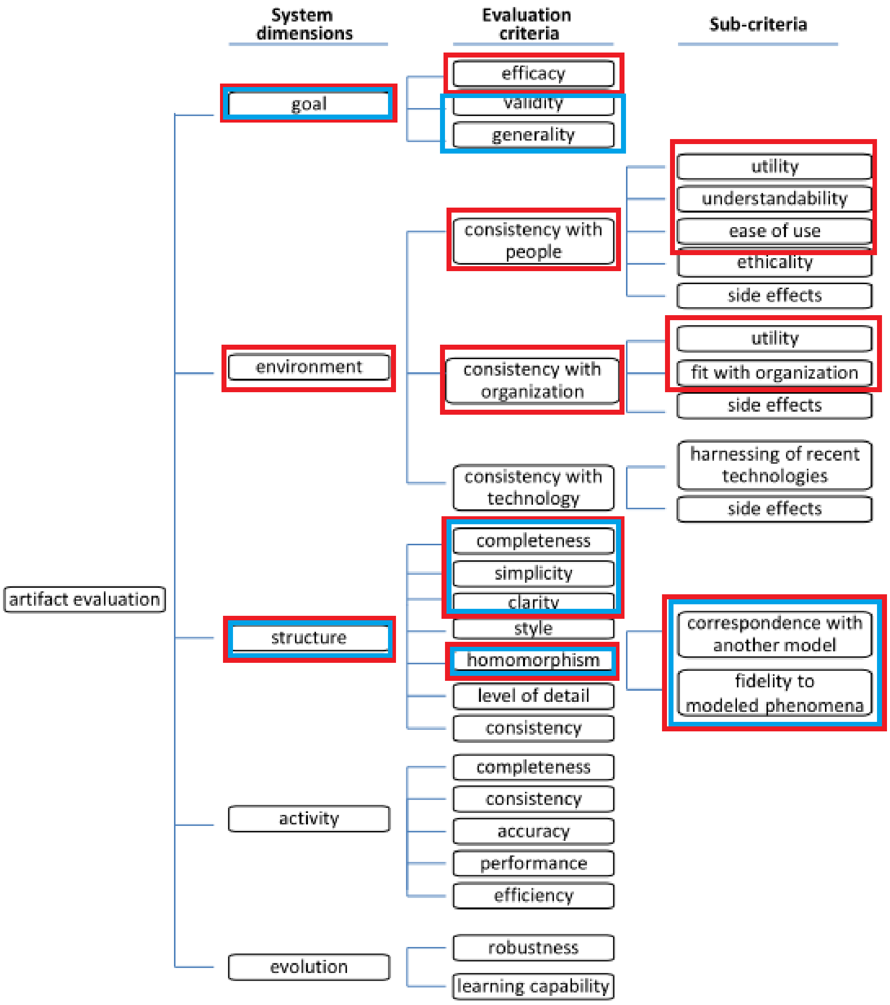


Fig. 5 Evaluation Criteria Hierarchy

ISO 27001 metamodels facilitate knowledge sharing, understanding and communication of these EGIT Practices.

Moreover, we found that COBIT 5 processes match groupings of ISO 27001's control objectives and controls, named control categories and a process can match one or more category. This enables us to say that a large majority of COBIT 5 processes have some relationship with ISO 27001 controls.

Yet, this research also has some limitations. EA models size, level of detail and complexity can make its analysis by human means only a hard task [29]. Moreover, as ArchiMate is a graphical language, it is not prone to automatic analysis. From our evaluation interviews we also noted that ArchiMate models heavily depend on the stakeholder analyzing the architecture. As such, the required knowledge of the ArchiMate core framework and metamodel is also a limitation.

In the future, we plan to implement our EGIT Practices integration models into an EA Management software that will allow us to answer to questions such as: “Attending to the allocated resources, within the different EA layers, what is the cost of maintaining a given COBIT 5 process in my organization?” or “How many resources do we have allocated to comply with a given ISO 27001 control?”

References

[1] S. De Haes and W. Van Grembergen, *Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value, Featuring COBIT 5*, New York, U.S.A: Springer Verlag, 2015.

[2] C. Symons, “IT governance framework: structures, processes and communication,” *IT Governance Series*, Forrester Research, 2005.

[3] T. Coleman and A. Chatfield, “Promises and successful practice in IT governance: a survey of Australian senior IT managers,” *15th Pacific Asia Conference on Information Systems: Quality Research in Pacific, PACIS 2011*, Queensland, pp. 1-15, 2011.

[4] R. S. Debreceny and G. L. Gray, “IT governance and process maturity: a multinational field study,” *Journal of Information Systems*, vol. 27, no. 1, pp. 157-188, 2011.

[5] S. Sahibudin, M. Sharifi, and M. Ayat, “Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations,” *Asia International Conference on Modeling*, 2008.

[6] IT Governance Institute, *Global Status Report on the Governance of Enterprise IT*, ISACA, COBIT 5: Enabling Processes, 2011.

[7] M. Winniford, S. Conger, and L. Erickson-Harris, “Confusion in the ranks: IT service management practice and terminology,” *Information Systems Management*, vol. 26, no. 2, pp. 98-109, 2009.

[8] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design science in information systems research,” *MIS Quarterly*, vol. 28, no. 1, pp. 75-105, 2004.

[9] S. T. March and G. F. Smith, “Design and natural science research on information technology,” *Decision Support Systems*, vol. 15, no. 4, pp. 251-266, 1995.

[10] P. Hill and K. Turbitt, “Combine ITIL and COBIT to meet business challenges,” BMC Software, 2006.

[11] P. Willson and C. Pollard, “Exploring IT governance in theory and practice in a large multinational organization in Australia,” *Information Systems Management*, vol. 26, no. 2, pp. 98-109, 2009.

[12] P. Nastase, F. Nastase and C. Ionescu, “Challenges generated by the implementation of the IT standards CobiT 4.1, ITIL v3 and ISO/IEC 27002 in enterprises,” *Economic Computation & Economic Cybernetics Studies & Research*, vol. 43, no. 3, pp. 1-16, 2009.

[13] N. Gama, P. Sousa and M. Mira da Silva, “Integrating enterprise architecture and IT service management,” *21st International Conference on Information Systems Development*, Italy, 2012.

[14] M. Gehrmann, “Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations,” *Navus: Revista de Gestão e Tecnologia*, vol. 2, no. 2, pp. 66-77, 2012.

[15] T. Mataracioglu and S. Ozkan, “Governing information security in conjunction with COBIT and ISO 27001,” *arXiv preprint arXiv:1108:2150*, 2011.

[16] R. Pereira and M. Mira da Silva, “Designing a new integrated IT governance and IT management framework based on both scientific and practitioner viewpoint,” *International Journal of Enterprise Information Systems*, vol. 8, no. 4, 2012.

[17] H. Susanto, M. N. Almunawar and Y. C. Tuan, “Information security management system standards: a comparative study of the big five,” *International Journal of Electrical & Computer Sciences*, vol. 11, no. 5, 2011.

[18] B. Von Solms, “Information security governance: COBIT or ISO 17799 or both?” *Computers & Security*, vol. 24, no. 2, pp. 99-104, 2005.

[19] M. Vicente, N. Gama and M. Mira da Silva, “Using ArchiMate to represent ITIL metamodel,” *IEEE International Conference on Business Informatics*, pp. 270-275, 2013.

[20] S. L. Schlindwein and R. Ison, “Human knowing and perceived complexity: implications for systems practice,” *Emergence: Complexity and Organizations*, pp. 27-32, 2004.

[21] ISACA, *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*, 2012.

[22] Information technology – Security techniques – Information security management systems – Overview and vocabulary, ISO Standard 27000, 3rd edition, 2014.

[23] Information technology – Security techniques – Information security management systems – Requirements, ISO Standard 27001, 2nd edition, 2013.

[24] M. Nicho and S. Muamaar, “Towards a taxonomy of challenges in an integrated IT governance framework implementation,” *Journal of International Technology and Information Management*, 2016.

[25] Information Technology – Process Assessment – Process capability assessment model for information security management – ISO Technical Specification 33072, 2016.

[26] Information technology – Process Assessment – Process reference model for information security management, ISO Technical Specification 33052, 2016.

[27] R. Sheikhpour and N. Modiri, “An approach to map COBIT processes to ISO/IEC 27001 information security management controls,” *International Journal of Security and its Applications*, vol. 6, no. 2, pp. 13-28, 2012.

[28] K. Haufe, R. Colomo-Palacios, S. Dzombeta, K. Brandis and V. Stantchev, “Security management standards: a mapping,” *Procedia Computer Science*, vol. 100, pp. 755-761, 2016.

[29] M. Lankhorst, *Enterprise Architecture at Work: Modeling, Communication and Analysis*, 2nd edition, The Enterprise Engineering Series, Springer, 2009.

[30] The Open Group, ArchiMate 2.0 Specification, 2012.

[31] R. Almeida, P. Pinto and M. Mira da Silva, “Using ArchiMate to integrate COBIT 5 and COSO metamodels,” *Europeam, Mediterranean & Middle Eastern Conference on Information Systems*, Krakrow, Poland, 2016A.

[32] R. Almeida, P. Pinto and M. Mira da Silva, “Using ArchiMate to assess COBIT 5 and ITIL implementations,” *25th International Conference on Information Systems Development*, Poland, 2016B.

[33] Luxembourg Institute of Science and Technology, *TIPA for ITIL*. Available: http://www.tipaonline.org [Accessed: 26 Mar. 2017]

[34] M. Goeken and S. Alter, “Towards conceptual metamodeling of IT governance frameworks approach-use-benefits,” *42nd Hawaii International Conference on System Sciences*, IEEE.

[35] K. Hinkelmann, “Meta-Modeling and Modeling Languages,” University of Applied Sciences Northwestern Switzerland FHNW School of Business.

[36] M. Roux-Rouquié and M. Soto, “Virtualizations in systems biology: metamodels and modeling languages for semantic data integration,” *Transactions on Computational Systems Biology I*, vol. 3380, pp. 132, 2005.

[37] R. Schütte and T. Rotthowe, “The guidelines of modeling – an approach to enhance the quality in information models,” *Conceptual Modeling ER 98*, L. Ling, Ram, Ed., Singapore, pp. 240-254, 1998.

[38] D. Milicevic and M. Goeken, “Ontology-based evaluation of ISO 27001,” *Conference on e-Business, e-Services and e-Society*, Berlin Heidelberg, Berlin, pp. 93-102, 2010.

[39] H. Österle, J. Becker, U. Frank, T. Hess, D. Karagiannis, H. Kremar, P. Loos, P. Mertens, A. Oberweis and E. J. Sinz, “Memorandum on design oriented information systems research,” *European Journal on Information Systems*, vol. 20, pp. 7-10, 2011.

[40] N. Prat, L. Comyn-Wattiau and J. Akoka, “Artifact evaluation in information systems design-science research: a holistic view,” *18th Pacific Asia Conference on Information Systems*, Chengdu, China, 2004.

[41] J. Venable, J. Pries-Heje and R. Baskerville, “A comprehensive framework for evaluation in design science research,” *Design Science Research in Information Systems. Advances in Theory and Practice (DESRIST 2012)*. Heidelberg, Berlin. Springer, 2012.