SEMANTIC MANAGEMENT OF ENTERPRISE INFORMATION SYSTEMS THROUGH ONTOLOGIES

Valentina Casola and Rosario Catelli

Department of Electrical Engineering and Information Technologies (DIETI),
University of Naples Federico II, Naples, Italy

ABSTRACT

This article introduces a model for cloud-aware enterprise governance with a focus on its semantic aspects. It considers the need for Business-IT/OT and Governance-Security alignments. The proposed model suggests the usage of ontologies as specific tools to address the governance of each IT/OT environment in a holistic way. The concrete utilization of ISO and NIST standards allows to correctly structure the ontological model: in fact, by using these well-known international standards it is possible to significantly reduce terminological and conceptual inconsistencies already in the design phase of the ontology. This also brings a considerable advantage in the operational management phase of the company certifications, congruently aligned with the knowledge structured in this manner. The semantic support within the model suggests further possible applications in different departments of the company, with the aim of evaluating and managing projects in an optimal way, integrating different but important points of view of stakeholders.

KEYWORDS

Cloud, Enterprise, Governance, Information management, Ontology, Semantic systems

1. INTRODUCTION

For most organisations, data and the technology that supports this data represent their most precious assets but also most underestimated. Information Technology (IT) is on the whole considered as an utility of a corporation [5] and its inherent intricacy requests the introduction of assorted assessment, management, and governance models and therefore led to the explosive growth of the discipline of information systems (IS) research throughout the last thirty years [28]. Such models aim to be each typically applicable and capable to handle specific corporate issues, e.g., cloud manufacturing-based product life cycle management [27]. The requirement for assurance regarding the worth of IT, the management of IT-related risks and augmented needs for management over data are currently considered strategic and creation of value possible through their alignment [32]. Value, risk and management are at the heart of IT governance, whose responsibility lies with both management and the board of directors, and consists of leadership, organisational structures and processes that ensure that the company’s IT supports and extends the organisation’s strategies and objectives .

The increasing complexity of IT is linked to a twofold aspect: on the one hand, IT becomes increasingly pervasive within companies, embracing both their core business and staff services, and on the other hand, the way in which IT services are delivered becomes increasingly intricate and difficult to manage (just think of the gradual transition from on-premise software to that

David C. Wyld et al. (Eds): NLP, JSE, MLTEC, DMS, NeTIOT, ITCS, SIP, CST, ARIA - 2020
pp. 25-40, 2020. CS & IT - CSCP 2020 DOI: 10.5121/csit.2020.101403

provided in the cloud, which in turn can be IaaS, PaaS, Saas and so on). Therefore, meeting the increasingly restrictive demands coming from the various business areas is challenging and will affect the time needed to deliver the services (for example, to verify the security according to corporate policies) and the costs related to them (the assessment of which becomes increasingly difficult).

For instance, to address queries associated with price and scaling capability, several organisations are considering driving their IT from resource-based approach to service-based approach, with the flexibility to scale the IT capability up and down as requested, that is a cloud based computing approach. Starting with the concept of economies of scale, the sharing of converging resources and infrastructures is at the heart of the concept of cloud computing. In order to obtain a shared but secure environment it is necessary to apply a correct governance strategy based on a model capable of taking into account the increasingly numerous forms through which cloud services are provided, in full respect of the needs of stakeholders, customer contracts and regulatory, legal and privacy aspects, perhaps unifying IT management and governance models [3].

This poses specific challenges on enterprise information systems. To enhance interoperability among all enterprise stakeholder and in order to avoid any misunderstanding, it is needed to be very careful at the semantic level to get clear red from company level right down to technical level and to provide clear objectives. For these reasons, our work explores the possibilities related to the creation and improvement of a domain ontology building methodology whose aim is to bright words and terminologies used among enterprises employees and information systems.

The remainder of the work is structured as follows: we summarise background and state of the art in Section 2 and Section 3 respectively, than we illustrate our methodology, an use case and some considerations in Section 4, finally we outline conclusion and future work in Section 5.

2. BACKGROUND

The cloud paradigm is progressively transforming into a mainstream paradigm and is considered as a serious subject of analysis in computer science. As a result, “cloud computing” is becoming a watchword within the company. The recognition of digital devices therefore the current use of the web translates into an ever-increasing demand for cloud computing. Cloud computing allows huge economies of scale in IT service delivery, but together it faces a variety of challenges. Benefits that are primarily related to it include rapid deployment, pay-per-use, lower prices, scalability, rapid provisioning, fast elasticity, ubiquitous network access, increased resiliency, protection against network attacks, low-cost disaster recovery and data storage solutions, on-demand security checks, real-time detection of system intrusions and rapid restart of services. Therefore, the move to cloud services makes users more efficient, facilitates collaboration with their colleagues, and provides continuous access to alternative digital services [19]. However, cloud applications, like all alternative technologies, face several sensitive issues related to the risks they introduce into the business [36].

For example, moving information to the cloud while offering great convenience for users because they do not have to worry about the complexity of direct management of storage infrastructure hardware [33], the Data Storage as a Service (DSaaS) introduces many challenges to information security (e.g. CIA) that should be addressed, and historically, information security issues are the domain of IT governance.

Although cloud services share infrastructures to produce compliant and guaranteed IT services, IT governance is required to ensure:

- governance framework setting and maintenance;
- benefits delivery;
- risk optimisation; – resource optimisation; – stakeholder engagement.

In order to meet these IT governance requirements in a cloud-based environment, it is always necessary to provide a complete asset inventory of all objects from completely different business departments, and related to your technology (servers, software, switches, etc..), your infrastructure (rooms, buildings, racks, air conditioning systems, power supply units, etc..), and your organisation (service level agreements, contracts, data, suppliers, people, roles and responsibilities, organisational units, etc..), and their relationships and inter dependencies.

Within the space of analysis of data systems and also in management science it is a typical approach to try to identify a model that correctly represents a specific problem and then use the model in order to produce relevant recommendations. A model that aspires to capture the complexity of contemporary computing and data management should apply a holistic view and at the same time build on existing best practices within specific areas (e.g., economic, legal, political and technological), and should therefore address these aspects:

- a medium-sized organisation generally has thousands of technical and infrastructural objects to inventory;
- the model should be able to offer data regarding the possession of objects, also considering possible interrelationships (e.g. the information element X is a component of document Y which is maintained by department Z);
- the model should jointly offer information regarding regulatory compliance and therefore think of a multifaceted reading (for example, regulatory needs could rely on the legal entity of the service provider and/or the location of a specific infrastructure element, the characteristics and/or possession of the information element).

3. State of the Art

This section presents the required definitions and concepts in the areas of cloud governance and enterprise architecture management.

3.1. Cloud Governance

Cloud governance is a natural extension of IT governance [25], but to date there are mainly two approaches used by the industry to manage cloud services. The first considers cloud providers as common service providers aiming to manage them with typical approaches adopted for non-cloud service providers. This approach involves that part of the industry expects these cloud providers to acquire the role of globally reliable mediators for the type of service provided, as ascertained by [21]. This implies an increasing demand for specific certifications (e.g. ISO 9001, ISO 27001) as a guarantee of quality and security for the services offered. The second approach instead, more pointed towards internal management, aims to enhance IT governance by making it ”cloud-aware”, shifting the focus towards the adoption of IT governance frameworks, such as ITIL and COBIT, that are sufficiently updated to keep taking into account the disruption of the cloud world and that can act as a gateway to its better integration within the corporate world.

3.2. Enterprise Architecture Management

Enterprise Architecture Management (or EAM) is a “management practice that establishes, maintains and uses a coherent set of guidelines, architecture principles and governance regimes that provide direction and practical help in the design and development of an enterprise’s architecture to achieve its vision and strategy” [1] so it aims to model all relevant components of a corporation and their relationships with many objectives.

The use of a holistic model that includes IT governance and cloud aware EAM methods leads to some advantages:

- organisations can have compelled to maintain a distinctive inventory and a rule set to confirm compliance with several normative and standard requirements;
- it is a viable and simple way to establish strong and resilient cloud governance;
- greater focus on corporate goal that reduces the conflict among heterogeneous stakeholder teams because the right formalisation guarantees traceable and repeatable results, facilitating the division of labour among the stakeholder teams [13] [14].

On the other hand, a “model” approach also has disadvantages:

- it depicts the enterprise architecture as a snapshot in time, not offering reiterative process support for future architecture solutions and tests against different scenarios;
- it is prohibitively time-intensive to keep updated and leaves too much room for error as changes to the architecture occur unchecked and isolated in the heads of small groups of architecture specialists.

To bring the highly distributed knowledge of the contributing stakeholders should be a main objective of EAM. For this reason, successful enterprise architecture programs are approached from a management perspective as opposed to a modelling perspective, and planning tools should support not only the modelling of architecture, but also the creation of roll-out and implementation plans for continuous improvement over time. In this way is possible the support of collaboration in a wide group of stakeholders from both business and IT (C-level, IT strategists, planning teams, technology implementer and business analysts) who contribute to the EA management and planning process. In this way EAM will support sustainable business strategy realisation.

4. A NOVEL DOMAIN ONTOLOGY BUILDING METHODOLOGY

Our methodology tries to sketch the optimal way to ensure the best possible solution to domain ontology building problem. Despite several methods are improving their capabilities to find and describe with enough generality high level domain concepts, building the so-called upper ontologies (e.g. SUMO, BFO, CCO and so on), there is a void we need to fill in to overcome limitations left behind (or below from the point of view of an ontologist). The main reason is that the ontology building problem, whatever you say, is a domain and specific problem that arise from the bottom, from the need to give an answer to a question in your specific research field and, in that moment, it shows itself like an instrument. An ontology is firstly useful when it is able to clearly define a common vocabulary for researcher who need to share information in a specific domain. Secondly, it includes machine-interpretable definitions of basic concepts in the domain and relations among them [18]. Nonetheless, there are always several viable alternatives to model a domain, but the specific implemented method is too often left apart and only the final ontology is shown. The development of an ontology can be divided in 7 steps [18]:

1. determine the domain and scope of the ontology;
2. consider reusing existing ontologies;
3. enumerate important terms in the ontology;
4. define the classes and the class hierarchy;
5. define the properties of classes - slots;
6. define the facets of the slots;
7. create instances.

Our methodology suggests some practical hints about these steps. First and foremost, the brainstorming activity around the first step is not trivial. Great importance should be done to the definition of the limits of you work to avoid any bias towards sub fields of your domain which are not the focus you had in mind at the beginning. The same approach should be applied looking into existing ontologies: the reuse can be more useful if you are able to extract concepts and terms from .owl files and understand if a smarter way to use them is possible. A chance not considered until now and proposed by us consists in leveraging something existing to enumerate important terms in the ontology: ISO always defines terms and definitions vocabularies across its operating domains, although as we will see, some incongruities must be fix. ISO vocabularies give us an important advantage through the path of the ontology development: they avoid to us to forget the overview out of our domain (so we will be ready to create links and bridges to the external domains) and strengthen the initial audit activity needed to enumerate terms. Left apart step 7, that is mostly practical, step 4 to 6 are really intertwined. In out method we suggest a multi-dictionary approach to get out of them: that we name "Ontological Research" consists in a research activity through ISO, NIST and Cambridge Dictionary. On the one hand, it is possible to extract a technical meaning from standards and understand where and why they want to go, but it is on your own to refine their meanings and put them in the correct way. The main problem using only technical standards is due to their circular definition: they usually define something referring themselves to something else and so on, until you are at the beginning again. On the other hand, it is possible to extract a semantic meaning from Cambridge Dictionary to mix and match what standards say, trying to solve their circularity. To build a working ontology, the knowledge engineer must understand where is needed to stop circularity and find the best elementary definition: it is true that this could be extremely subjective, however standards and vocabularies can lead you and help you through the path. It follows an illustrative figure of our methodology in Figure 1.

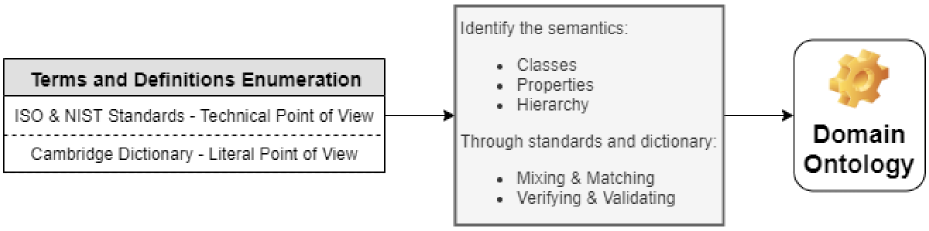

Terms and Definitions Enumeration
ISO & NIST Standards - Technical Point of View
Cambridge Dictionary - Literal Point of View
Identify the semantics:
Classes
Properties
Hierarchy
Through standards and dictionary:
Mixing & Matching
Verifying & Validating
Domain Ontology

Figure 1. Overview of our methodology

4.1. Use Case: Information Security Domain ontology

We decided to focus our work on the Information Security domain, leveraging the terms and definition from ISO/IEC 27000:2018. Because of the novelty of the method, we decided to avoid the reuse of any existing ontology to test thoroughly the possibilities of our method. We have identified "Process" as high-level concept and decided to build a class around it. ISO/IEC 27000:2018 (and also NISTIR 8053) defines a process as a "set of interrelated or interacting activities which transforms inputs into outputs": for this reason we decided to include two related operations, receivesInput() and providesOutput() functions. After that, we have move on the "Activity" concept: ISO/IEC/IEEE 15288:2015 defines an activity as a "set of cohesive tasks of a process" so we were addressed to find out the meaning of the "Task" concept. Here several drawbacks arose because there are at least three conflicting definitions as follows:

- ISO/IEC/IEEE 15288:2015 states that a task is "required, recommended, or permissible action, intended to contribute to the achievement of one or more outcomes of a process";
- ISO 9241-11:2018 states that a task is "set of activities undertaken in order to achieve a specific goal";
- NIST SP 800-181 states that "a task is a specific piece of work that, combined with other identified tasks, composes the work in a specific specialty area or work role".

Which ones could be acceptable? Why? As highlighted in Figure 2 there were several problems to solve, so we started analysing "Task" definitions one by one:

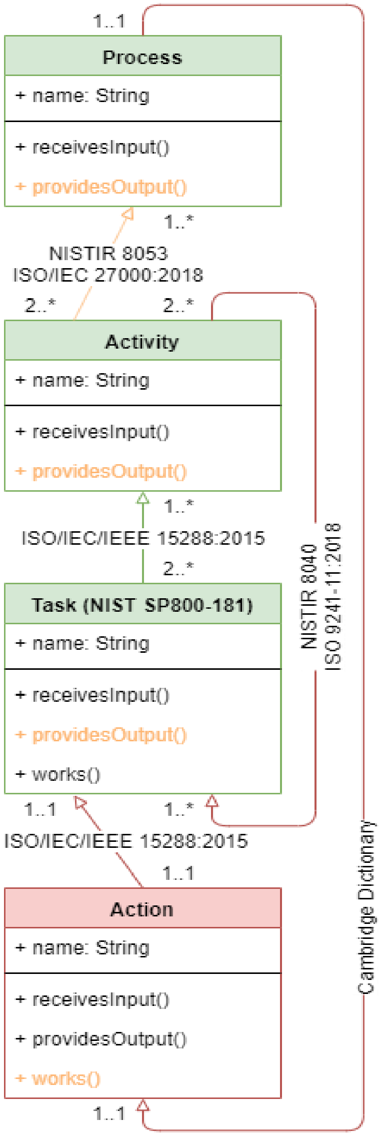


Figure 2. UML-based representation of "Process" class creation

- ISO/IEC/IEEE 15288:2015 leverages the concept of “Action” and speaks about the “Outcome” of a process (is it the same of “output” indicated by ISO/IEC 27000:2018?). Unfortunately, we did not find any standards that define the concept of “Action”. But Cambridge Dictionary does: it defines the concept of “Action” as “the process of doing something, especially when dealing with a problem or difficulty”. This suggested us to overcome this standard definition of “Task” in order to avoid circularity;
- ISO 9241-11:2018 creates circularity, using the already defined “Activity” concept, so we decide to overcome this definition also (but what is a “goal”?);
- NIST SP 800-181 gives us an enough atomic definition of the concept of “Task”, identifying it as “a specific piece of work”. Here, the boundaries of our ontology impose us not to go deeper to avoid any lack of focus on the main topic that is “Information Security”.

Nonetheless, the concept of “Action” defined by ISO/IEC/IEEE 15288:2015 inspired us to search for “Outcome” concept. Our first thought was related to the same concept of “Process”: its ISO definition assumes quantitative characteristic, promoting an ungluing from the industrial logic where processes are used to “create value” and not only more objects. Standards don’t define “Output”, “Outcome”, “Result” and “Effect” so we used Cambridge Dictionary:

- output is “an amount of something produced by a person, machine, factory, country, etc...” and this confirmed our first thought was not so wrong;
- outcome is “a result or effect of an action, situation, event, etc...”;
- result is “something that happens or exists because of something else”;
- effect is “the result of a particular influence”.

And then we also searched for “Goal” and surprisingly we found it in NISTIR 8040 – ISO 9241-11:2018 defined as “intended outcome”. Clearly, it was something missing. To promote the “Process” to a qualitative characteristic we decided to significantly change one of its operation: providesOutput() became deliversResults(). The semantic agreement among all the others concept was found also adding these definitions:

- Cambridge Dictionary states the a “situation” is “the set of things that are happening and the conditions that exist at a particular time and place”;
- ISO Guide 73:2009 states that an “event” is an “occurrence or change of a particular set of circumstances”.

Subsequently we decide to treat “Action”, “Situation” and “Event” as object of type “Process”, “Effect” as object of type “Result”. The last problem was about “Outcome”. Analysing one of the notes attached to the definition of “Event” we were directed through a possible solution: it states that “An event without consequences can also be referred to as [...]”. Because of the note we have considered a “consequence” like something with negative connotation although the definition of “Consequence” on ISO/IEC 15026 as “effect (change or non-change), usually associated with an event or condition or with the system and usually allowed, facilitated, cause, prevented, changed, or contributed to by the event, condition, or system” could be considered neutral, while “Outcome” (linked to “Goal” also) like something with positive connotation. Hence, we added two operations to our “Result” class, “hasOutcome” and “hasConsequence”, inherited by that particular “Result-object” that is “Effect”. A sorted “Process” class is represented in Figure 3.

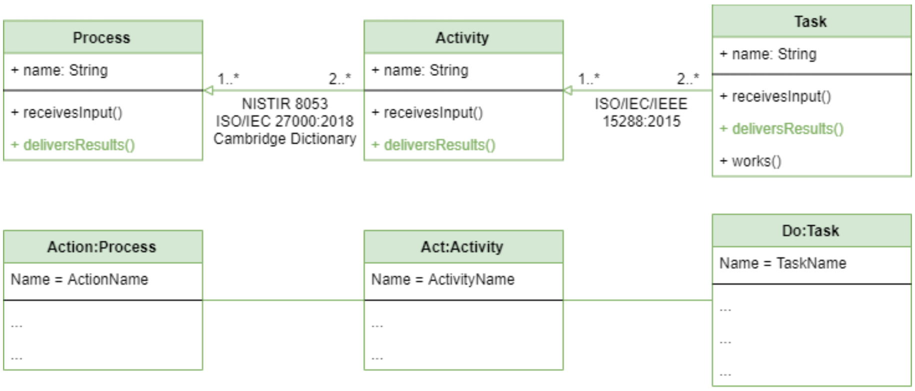


Figure 3. UML-based representation of Process class and related Action-object

4.2. Considerations Over Modern EAM Challenges

In proposing such a model of governance, we have to face several challenges that we could summarise as follows:

1. reduction of the points of view;
2. partiality of the points of view;
3. integration of the EAM within the processes.

The first problem is the identification of points of view that we could consider relevant and that are usually related to stakeholders. But in doing so, we risk excessively narrowing the field of vision: in fact, it is necessary to take into account the points of view of the application situations on which we plan to map the model. This step is fundamental in order to balance the reduced capacity of stakeholders to precisely outline their needs and use cases: this limit is often one of the main reasons behind the failure of a business project. Application situations have a direct impact on the layers needed to build the EAM model, its inter dependencies and the level of granularity of its requirements. For example, if we were to focus on a ”business” perspective, within a model we would certainly find structural objectives, processes and IT elements, but the granularity with which the latter would be defined would certainly be inadequate when we would be from an ”IT” perspective, more focused on the analysis of hardware/software systems and their performance. And even more, this limit would tend to emerge if we put ourselves from an “Information Security” perspective, so that the elements at stake must guarantee certain levels of confidentiality, integrity and confidentiality. Therefore, the identification of relevant points of view and their objectives is a precondition for the correct definition of the desired elements, interrelationships and granularity.

Secondly, care must be taken not to consider only part of the perspectives mentioned above. In fact, what happens in the real world in an ascertained way is due to ”historical” reasons that lead companies to partial problem-solving (think, for example, of the necessary integration of legacy tools within processes that are the subject of the Information Security perspective). In such cases, the challenge for companies is to be able to link these systems together in a coherent way to the perspective considered in order to make them easily manageable.

The third point to consider in order to maintain a consistent EA is to ensure that it is integrated into relevant processes such as change management and the tools needed to manage the data of the same. It may seem trivial, but hold-up or lock-in effects due to the pre-existing (or proprietary) tools perfectly run within the company routines are common and can inhibit the acceptance of new tools and approaches proposed. If the degree of acceptance of what is new is low for this, then the full achievement of the benefits proposed by the new EAM will fail. In particular, the migration of data from legacy tools to new ones often leads to inconsistencies, losses or contradictions, all the greater as the different elements, interrelations and granularity at stake from different perspectives are different. Solving these types of problems requires a very significant effort in terms of human resources. But using semantic tools it is possible, while confining each perspective only to the data relevant to it, to avoid information overflow and to be able to make more informed decisions, also improving access control both for the analysis of the functions and for the editing of the data.

In the following, a novel way to manage EA models is introduced. It aims to overcome the restrictions mentioned using semantic technologies. The ontologizing of The Enterprise Ontology can help to redefine "the notion of architecting" as stated in [16]:

"In the context of high levels of complexity and uncertainty, the notion of causality often breaks down. Often, one can only assume that everything is in relationship with everything else. Consequently, understanding the ramifications of changes such as disruptive technologies and new architecture models (i.e. cloud computing, outsourcing) is often almost impossible. New resources such as contextual data of customers will have to be used effectively to gain a competitive edge. To face such challenges, the notion of architecting will surely have to be redefined.".

The following conceptual model tries to overcome the above restrictions and is based on a matrix containing six horizontal and three vertical layers (see Figure 4).

The six horizontal layers are:

1. Business Level
2. Integration Level
3. Core Level
4. Staff Level
5. Infrastructure Level
6. IT/OT Level

The three vertical levels are:

1. Information Security
2. Computer and System Security
3. Network and Physical Security

Horizontal layers provide the general paradigm of alignment between company and IT/OT ensuring consistency between business objectives, operations and IT infrastructure. The vertical layers provide the general paradigm of alignment between security, compliance and governance from the point of view of information objects and specific requirements, thus roles and responsibilities. Below is an overview of the main aspects of the model, which will form the basis for the elaboration of the semantic aspects of the model, which will be presented in the next section.

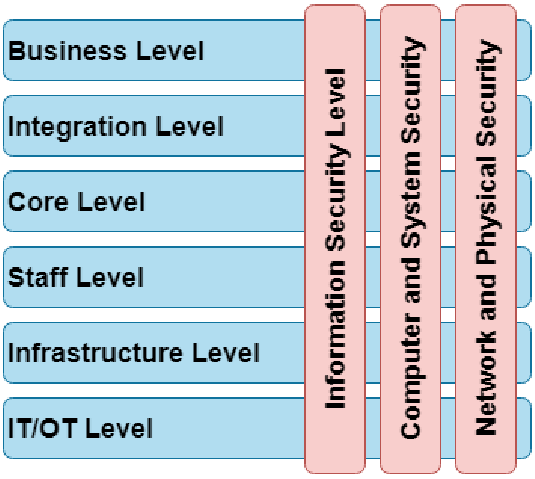

Business Level
Integration Level
Core Level
Staff Level
Infrastructure Level
IT/OT Level
Information Security Level
Computer and System Security
Network and Physical Security

Figure 4. Overview of the EAM model

4.2.1. The Paradigm of Business-IT/OT Alignment

The paradigm of alignment between Business and IT/OT is implemented in six horizontal levels.

1. Business Level.

It defines the company’s global focus, including its mission and strategy, as well as its business model.

2. Integration Level.

It defines the final products to be presented on the market at regional level (EMEA, APAC, etc...), interfacing with the Core Level (of which it defines internal contracts and service levels) and orienting its efforts in order to respond to the needs traced by the Business Level.

3. Core Level.

It deals with the coordination of the Core Departments, which are the organisational units at the heart of the corporate mission and defines the organisational and technical needs.

4. Staff Level.

It provides support to the Core Level, integrating the non-core business functions in a harmonic and ready-to-use way.

5. Infrastructure Level.

It allocates the available resources (software, hardware and network from an IT point of view; but also buildings, local air conditioning, energy and physical access systems) to the staff units as needed (cloud, on premise).

6. IT/OT Level.

It defines the available resources, IT and OT, and manages their organisation (e.g. nodes, type and degree of virtualisation, components, connections and barriers).

4.2.2. The Paradigm Of Governance-Security Alignment

The Governance-Security alignment is embodied within the three vertical levels.

1. Information Security Level.

It establishes roles, responsibilities and accountability with regard to data, information and requirements like relevancy of standards (e.g. ISO 27001), specific governance necessities, yet as business or application-driven necessities (e.g. confidentiality, integrity, availability, reliability, dependability).

2. Computer and System Security Level.

It defines security technical needs (user accesses, disk encryption, etc.) on the basis of internal necessities and external requests as pointed out by Information Security Level. It evaluates and manages cloud computing doable deployment models within the company.

3. Network and Physical Security Level.

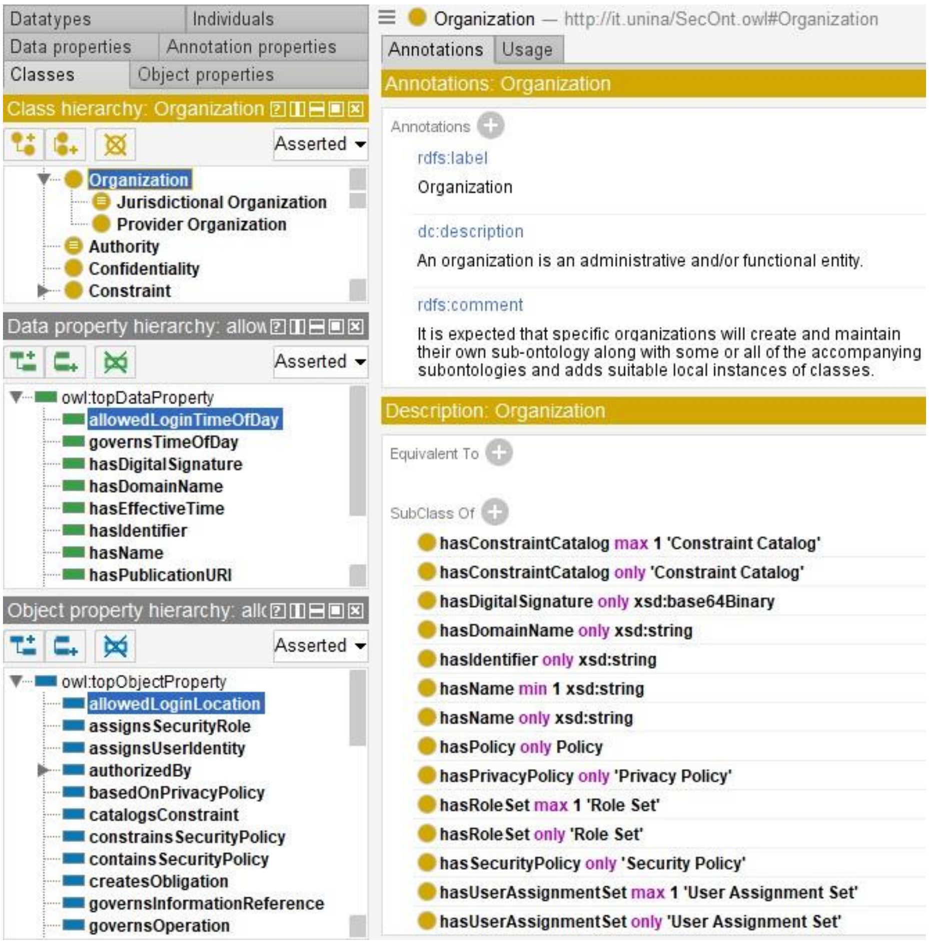
It defines the security of the perimeter within which each asset operates on the basis of internal necessities and external requests as pointed out by Information Security Level, but can act independently if necessary in case of emergency to increase the speed of response.

4.3. Ontologized Eam Model

Ontologies are a means of formally shaping the structure of a [26]. They provide a shared understanding of certain domains that can be communicated between people and application systems [8]. Ontologies aim to determine “semantic agreements”, reducing language ambiguity and knowledge variations between agents, which can cause errors, misunderstandings and inefficiencies [2]. Given their importance, ontologies are seen as the cornerstone of many promising technologies such as, for example, the semantic web and related data, reporting an abundant implementation in literature like [9],[22]. The scope of IT/OT service management is very far from this trend, although there are several attempts to use ontologies in some areas such as the life cycle of cloud services [15], software system development and IT service management processes [30], quality of service - security metrics [6], facilitation of operational procedures in public administration [24], service management in the Internet of Things [23] or IT service management for business-IT integration [31].

4.3.1. An Ontology-Based Approach

The application of ontologies in the various fields requires careful reflection on the basic mappings between the higher ideas and the application cases. Starting from [31] there is an ontological approach for the establishment of a scientific technique that allows to implement the ontology approach in an extremely easy and well-defined way, thus supporting its use. The reference standard related to the development of ontologies is the web ontology Language (OWL) defined by the World Wide Web Consortium (W3C). The OWL allows the use of various logical formalisms to mechanically process domain information by providing value-added reasoning services to classify individuals, verify the consistency of information bases and deduce new types of information within the taxonomy. The ontologies outlined under the OWL embrace classes as sets of individuals, individuals as examples of classes and properties as binary relationships between individuals. Among the different ontological development environments, the best known is certainly Protege, an open source program that allows both the development of ontologies and their visualisation, although in the case of complex ontologies it is more appropriate to employ specialised tools in visualisation such as OWL-VisMod [10]. The idea of representing a collection of terms as enterprise related ontology has been projected over fifteen years [29] and there are timid attempts to represent corporate governance in semantic ways, particularly in the fields of information security [7] and IT governance [4], hence the application of enterprise design governance in public administration [20]. Of explicit interest is that the pioneering work of [34] in the field of compliance management, which fits well as a starting point for reflection within the modelling of the Information Security Level. The ontology introduced is based on what is available at the state of the art and seeks to improve and combine it into a single coherent and global ontology for the EAM, extending a number of approaches presented in [34] following an approach supported by [31] and drawing on [17]. An extract of the ontology is shown in Figure 5.



Organization — http://it.unina/SecOnt.owl#Organization

Class hierarchy: Organization

- Organization
  - Jurisdictional Organization
  - Provider Organization
- Authority
- Confidentiality
- Constraint

Data property hierarchy: allow

- owl:topDataProperty
  - allowedLoginTimeOfDay
  - governsTimeOfDay
  - hasDigitalSignature
  - hasDomainName
  - hasEffectiveTime
  - hasIdentifier
  - hasName
  - hasPublicationURI

Object property hierarchy: allc

- owl:topObjectProperty
  - allowedLoginLocation
  - assignsSecurityRole
  - assignsUserIdentity
  - authorizedBy
  - basedOnPrivacyPolicy
  - catalogsConstraint
  - constrainsSecurityPolicy
  - containsSecurityPolicy
  - createsObligation
  - governsInformationReference
  - governsOperation

Annotations: Organization

Annotations

rdfs:label
Organization

dc:description
An organization is an administrative and/or functional entity.

rdfs:comment
It is expected that specific organizations will create and maintain their own sub-ontology along with some or all of the accompanying subontologies and adds suitable local instances of classes.

Description: Organization

Equivalent To

SubClass Of

- hasConstraintCatalog max 1 'Constraint Catalog'
- hasConstraintCatalog only 'Constraint Catalog'
- hasDigitalSignature only xsd:base64Binary
- hasDomainName only xsd:string
- hasIdentifier only xsd:string
- hasName min 1 xsd:string
- hasName only xsd:string
- hasPolicy only Policy
- hasPrivacyPolicy only 'Privacy Policy'
- hasRoleSet max 1 'Role Set'
- hasRoleSet only 'Role Set'
- hasSecurityPolicy only 'Security Policy'
- hasUserAssignmentSet max 1 'User Assignment Set'
- hasUserAssignmentSet only 'User Assignment Set'

Figure 5. An extract of the proposed ontology

4.3.2. Verification

The verification of a specific ontology requires two phases: the characterisation of the models of ontology up to isomorphism and the indication that these models correspond to the structures supposed for the ontology [11]. These two phases are often conducted using approaches such as the theory of reducibility [12]. But due to the lack of alternative ontologies based on OWL, it is not possible to conduct a test in the sense of phase two at the time of writing. In the first step we must demonstrate that a theorem concerning the connection between the classes of ontology models and thus the class of the supposed structures is often replaced by a theorem concerning the connection between ontology (a theory) and thus theory by axiomizing the supposed structures [11]. This requires that this axiomatization be already identified. Overall, the approach of [12], [11] represents a possible way to formally verify ontology, but the lack of alternative ontologies makes comparison impossible. For this reason, once we have analysed the most common classification approaches within the IT governance domain, we think of the ISO 27001 standard as sufficiently close for a meaningful comparison, since ISO documents specify roles and responsibilities (present in a part of our model) within a certification scheme.

5. Conclusions and Future Works

The presented model integrates approaches from EAM, IT governance and cloud computing so as to produce a holistic governance framework, with a look at the semantic aspects considering information and knowledge objects, roles, as well as necessities. It also attributes exactly the skills for secure management of cloud environments. The Business-IT/OT alignment builds on existing works within the space of EA and extends them by many necessary aspects, detailing more clearly the layers of the model and introducing pregnant semantic relationships between components of the layers. The aspect of the point of view is considered in more details and the integration of the EAM within the processes is deepened, while the governance paradigm follows best practices of literature. The latter extends them applying more recent approaches providing an additional clear view on the relationships between information objects, roles, and specific necessities from the point of view of application domains and client teams. The presented semantic consideration provides a viable framework for the facilitation of state-of-the-art semantic approaches within the additional development of the model. Provided that previous frameworks are modelled using well-known ontologies, this allows authors to formalise the model in a very structured manner and to arrange it for future automatic reasoning and future ontology verification.

The given model with its paradigms may be a viable approach to fill the gap between the standard views of Business – IT/OT alignment and Governance – Security alignment, on the one hand, and integrating the not-postponeable revolution of the cloud, on the other hand. Thus, once completely developed, it will function as a methodological framework for both cloud-aware company and cloud-suppliers, ensuring an improved synergy between requests and offers.

Yet, the work on the model continues to be in its early stages. The queries of precise mappings and reflections between the various levels of the model are still open. Authors expect that a nonstop focus on semantic aspects and also the application of semantic methods can give a possible path to refine the model in this regard. Beside the work on semantic aspects, more work in the context of the model is targeted on 2 main areas. First and foremost, the doable relationships and also the degree of granularity ought to be developed from the point of view of each relevant perspective. Secondly, the compliance issue must be specified a lot of in-depth and to be extended with the potential to produce specific recommendations supported by both Business and IT/OT levels (e.g., an amendment request as a part of the change management): specific extensions of the approach leveraging COBIT and ITIL frameworks could be considered. Finally, the development of a tool based on semantic technologies will follow closely the model growth.

Acknowledgements

This document has been produced thanks to a doctoral grant funded by Hitachi Rail STS S.p.A. (formerly Ansaldo STS S.p.A.), and in particular by the CSAC (Cyber Security and Assurance Control) Department, to which the authors sincerely express their gratitude for the valuable support provided.

REFERENCES

[1] Ahlemann, F., Stettiner, E., Messerschmidt, M., Legner, C.: Strategic enterprise architecture management: challenges, best practices, and future developments. Springer Science & Business Media (2012)

[2] Blanco, C., Lasheras, J., Fernández-Medina, E., Valencia-García, R., Toval, A.: Basis for an integrated security ontology according to a systematic review of existing proposals. Computer Standards & Interfaces 33(4), 372–388 (2011)

[3] Bounagui, Y., Mezrioui, A., Hafiddi, H.: Toward a unified framework for cloud computing governance: An approach for evaluating and integrating it management and governance models. Computer Standards & Interfaces 62, 98–118 (2019)

[4] Brandis, K., Dzombeta, S., Haufe, K.: Towards a framework for governance architecture management in cloud environments: A semantic perspective. Future Generation Computer Systems 32, 274–281 (2014)

[5] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.: Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems 25(6), 599–616 (2009)

[6] Charuenporn, P., Intakosum, S.: Qos-security metrics based on itil and cobit standard for measurement web services. J. UCS 18(6), 775–797 (2012)

[7] Ekelhart, A., Fenz, S., Klemen, M.D., Weippl, E.R.: Security ontology: Simulating threats to corporate assets. In: International Conference on Information Systems Security. pp. 249–259. Springer (2006)

[8] Fensel, D.: Ontologies. In: Ontologies, pp. 11–18. Springer (2001)

[9] Garcia-Crespo, A., Colomo-Palacios, R., Gomez-Berbis, J.M., Ruiz-Mezcua, B.: Semo: a framework for customer social networks analysis based on semantics. Journal of Information Technology 25(2), 178–188 (2010)

[10] García-Peñalvo, F.J., Colomo-Palacios, R., Garcìa, J., Theròn, R.: Towards an ontology modeling tool. a validation in software engineering scenarios. Expert Systems with Applications 39(13), 11468–11478 (2012)

[11] Grüninger, M.: Verification of the owl-time ontology. In: International Semantic Web Conference. pp. 225–240. Springer (2011)

[12] Grüninger, M., Hahmann, T., Hashemi, A., Ong, D.: Ontology verification with repositories. In: FOIS. pp. 317–330. No. 209 (2010)

[13] Jonkers, H., Lankhorst, M., Van Buuren, R., Hoppenbrouwers, S., Bonsangue, M.,Van Der Torre, L.: Concepts for modeling enterprise architectures. International Journal of Cooperative Information Systems 13(03), 257–287 (2004)

[14] Jonkers, H., Lankhorst, M.M., ter Doest, H.W., Arbab, F., Bosma, H., Wieringa,R.J.: Enterprise architecture: Management tool and blueprint for the organisation. Information systems frontiers 8(2), 63 (2006)

[15] Joshi, K., Finin, T., Yesha, Y.: Automating cloud services lifecycle through semantic technologies (May 26 2016), uS Patent App. 14/550,264

[16] Lapalme, J., Gerber, A., Van der Merwe, A., Zachman, J., De Vries, M., Hinkelmann, K.: Exploring the future of enterprise architecture: A zachman perspective. Computers in Industry 79, 103–113 (2016)

[17] Mense, A., Blobel, B.: Hl7 standards and components to support implementation of the european general data protection regulation. European Journal for Biomedical Informatics 13(1), 27–33 (2017)

[18] Noy, N.F., McGuinness, D.L., et al.: Ontology development 101: A guide to creating your first ontology (2001)

[19] Park, S.C., Ryoo, S.Y.: An empirical investigation of end-users' switching toward cloud computing: A two factor theory perspective. Computers in Human Behavior 29(1), 160–170 (2013)

[20] Peristeras, V., Mocan, A., Vitvar, T., Nazir, S., Goudos, S.K., Tarabanis, K.: Towards semantic web services for public administration based on the web service modeling ontology (WSMO) and the governance enterprise architecture (GEA). na (2006)

[21] Petruch, K., Stantchev, V., Tamm, G.: A survey on it-governance aspects of cloudcomputing. International Journal of Web and Grid Services 7(3), 268–303 (2011)

[22] Rodríguez-González, A., Colomo-Palacios, R., Guldris-Iglesias, F., Gómez-Berbís, J.M., García-Crespo, A.: Fast: Fundamental analysis support for financial statements. using semantics for trading recommendations. Information Systems Frontiers 14(5), 999–1017 (2012)

[23] Sammarco, C., Iera, A.: Improving service management in the internet of things. Sensors 12(9), 11888–11909 (2012)

[24] Savvas, I., Bassiliades, N.: A process-oriented ontology-based knowledge management system for facilitating operational procedures in public administration. Expert Systems with Applications 36(3), 4467–4478 (2009)

[25] Stantchev, V., Stantcheva, L.: Extending traditional it-governance knowledge towards soa and cloud governance. International Journal of Knowledge Society Research (IJKSR) 3(2), 30–43 (2012)

[26] Sure, Y., Staab, S., Studer, R.: Ontology engineering methodology. In: Handbookon ontologies, pp. 135–152. Springer (2009)

[27] Talhi, A., Fortineau, V., Huet, J.C., Lamouri, S.: Ontology for cloud manufacturing based product lifecycle management. Journal of Intelligent Manufacturing 30(5), 2171–2192 (2019)

[28] Thomas, O.: Understanding the term reference model in information systems research: history, literature analysis and explanation. In: International Conference on Business Process Management. pp. 484–496. Springer (2005)

[29] Uschold, M., King, M., Moralee, S., Zorgios, Y.: The enterprise ontology. The knowledge engineering review 13(1), 31–89 (1998)

[30] Valiente, M.C., García-Barriocanal, E., Sicilia, M.A.: Applying ontology-based´ models for supporting integrated software development and it service management processes. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 42(1), 61–74 (2011)

[31] Valiente, M.C., Garcia-Barriocanal, E., Sicilia, M.A.: Applying an ontology approach to it service management for business-it integration. Knowledge-Based Systems 28, 76–87 (2012)

[32] Van Grembergen, W., De Haes, S.: Enterprise governance of information technology: achieving strategic alignment and value. Springer Publishing Company, Incorporated (2009)

[33] Wang, C., Wang, Q., Ren, K., Cao, N., Lou, W.: Toward secure and dependable storage services in cloud computing. IEEE transactions on Services Computing 5(2), 220–232 (2011)

[34] Yip, F., Wong, A.K.Y., Parameswaran, N., Ray, P.: Rules and ontology in compliance management. In: 11th IEEE International Enterprise Distributed Object Computing Conference (EDOC 2007). pp. 435–435. IEEE (2007)

[35] Zarrabi, F., Pavlidis, M., Mouratidis, H., Islam, S., Preston, D.: A meta-model for legal compliance and trustworthiness of information systems. In: International Conference on Advanced Information Systems Engineering. pp. 46–60. Springer (2012)

[36] Zissis, D., Lekkas, D.: Addressing cloud computing security issues. Future Generation computer systems 28(3), 583–592 (2012)

AUTHORS

Valentina Casola is Associate Professor at the Department of Electrical Engineering and Information Technologies of the University of Naples Federico II. She graduated in Electronic Engineering with honors in 2001 and received her PhD in Electronic Engineering in 2004. Since 2005 she has taught several courses at the Faculty of Engineering, including: "Electronic Computers I", "Programming I" and "Secure System Design". Her research activities are both theoretical and practical and mainly concern safety assessment methodologies and design methodologies for secure distributed systems. These activities are carried out in collaboration with other academic institutions and international companies in numerous projects. Valentina Casola is author of numerous publications in journals and in international conferences and is member of program committees of numerous international conferences.

Rosario Catelli is a PhD student at the Department of Electrical Engineering and Information Technologies of the University of Naples Federico II. He started his PhD in Hitachi Rails STS then moved to the Institute for High Performance Computing and Networking (ICAR), which is part of the National Research Council. He is currently working in the field of natural language processing.