Modelling Access Control Mechanisms in Enterprise Architecture

Extended Abstract

Ricardo Martins, Artur Caetano
Department of Computer Science and Engineering
Instituto Superior Técnico
Lisbon, Portugal
raafm@ist.utl.pt, artur.caetano@ist.utl.pt

Abstract— **In many common enterprise architecture frameworks access control information is not represented in the business and process layer. Access control is composed of three main activities: authentication of users, authorization to perform a certain action and audit of the actions that were performed.**

The main objective of this thesis is to develop a model that is able to aggregate access control information to business process and their related elements. This model will be validated and evaluated in three ways: an informed argument, a set of scenarios and a practical case study to be developed in the Portuguese Department of Investigation and Prosecution.

There is also a brief survey of the related work on the three main areas of interest to this project: Access control mechanisms; Business process modelling languages; and Enterprise architectures frameworks. The access control mechanisms that were analysed are: Mandatory Access Control, Discretionary Access Control, Role Base Access Control (and many derivatives), Task Based Access Control and Attribute Ac-cess Control. Afterwards there is a description of the current support for security in some enterprise architecture frameworks. The business process and workflow modelling languages analysed were: BPMN, ArchiMate. ArchiMate was also analysed from the enterprise architecture framework perspective along with TOGAF ADM and Zachman Framework.

Some future work directions (that were not fully explored in this thesis) include: the full integration of this model in enterprise architecture frameworks and business process modelling languages and the automatic generation of security and audit requirements from business rules.

Keywords-Business process modelling; Access Control Mechanisms; Auditing; Enterprise Architecture; Conceptual modelling

I. Introduction

In this dissertation the work that was done to create and evaluate an access control model for the enterprise architecture business layer is going to be presented. The main objective of this model is to create artefacts to represent previously existing access control rules in the business process layer of enterprise architecture. This thesis will not focus on how to obtain the needed access control rules to apply the proposed model but, some work on this area will be briefly introduced in the related work section (III.B).

Access control enables an authority to control access to resources in a given system and, in the realm of com-puter engineering,. It includes:

- Authentication – Verifies that an entity that is trying to access the system is the one who claims to be.
- Authorization – Checks the permissions required to perform a certain action on a system.
- Audit – Stores some access control events (authentication, actions performed, etc.) to verify that those events are valid.

Access control is a widely studied theme within computer engineering (e.g. RBAC, ACM, ACL) [1, 2]. However, access control (i.e. authentication, authorization and audit) are neither explicitly represented in current standard business process modelling languages nor in the mainstream enterprise architecture frameworks.

In the current enterprise architecture frameworks the access control artefacts are normally represented in the technology layer and this can be a problem because these technologies only exist to support the business, and if the needed access control are not represented in the business process layer artefacts (one of the layers that represents how an enterprise operates) and associated with their instantiation on the technological layer then, there cannot be guarantees that the designed technological access controls truly represent all the needed access controls.

With the access control model created in this thesis it will be possible to represent the access control in the business layer of the enterprise architecture and solve the traceability problem introduced in the previous paragraph. This model is focused on all aspects of access control: access restriction, access granting and access auditability. To restrict access to specific business process elements this model introduces restrictions and related artefacts (to model those restrictions); to grant access this model focus on creating security roles that are associated with specific business roles and permissions connected with them; and to audit the access, this model introduces an artefact that is related to the restrictions that creates access logging on the architectural level.

The evaluation of the artefacts designed in this thesis will follow the guidelines defined in [3]. This evaluation will be made using three methodologies: informed argument, scenarios and a practical case study on the PPOIS-NG.

II. Research Questions

There are four research questions that will be answered by this thesis. These are:

- Q1: Which access control concepts are required in the business process domain?
- Q2: What is the concept structure and what are the relationships between concepts?
- Q3: How to define access control authorization on the business layer of the Enterprise Architecture?
- Q4: How to define access control auditability on the business layer of the Enterprise Architecture?

A. Which access control concepts are required in the business process domain?

The objective of this research question is to reach a set of concepts that allow access control representation in business processes. These concepts must cover all the needed functionality to restrict access to certain elements and allow it in specific conditions or to specific actors.

B. What is the concept structure and what are the relationships between concepts?

In this question the concept structure will be presented along with the relationships between the various concepts introduced in the first question to reach a more dynamic and complete access control system.

C. How to define access control authorization on the business layer of the Enterprise Architecture?

Using the concepts and their relationships introduced in the first and second questions, an access control model for the business layer of the enterprise architecture will be presented. It will also be shown how the concepts will interact with pre-existent elements of the business process domain and how this interaction will create a dynamic access control system.

D. How to define access control auditability on the business layer of the Enterprise Architecture?

All the access control concepts introduced while answering the previous questions will need to be audited, to verify if they are being enforced effectively or according to some predefined rules or laws. To do this, some new concepts will be introduced and their relationship with the rest of the concepts will be presented.

III. Related Work

In this section, some of the related work that was studied while doing this dissertation is going to be introduced. There are three main areas of related work:

- Access Control Methods
- Enterprise architecture
- IT Governance
- Business Process Modelling

The access control methods studied in this thesis are: Mandatory Access Control, Discretionary Access Control, Role based access control, Task based access control and Attribute based access control. In the Enterprise architecture sub-section, some Enterprise architecture frameworks are going to be introduced along with how these frameworks currently support security. After this, IT governance is going to be introduced and how it relates to the problem of this thesis. The Business process modelling section will feature some introduction to this area, and how it can be represented.

A. Access Control Methods

There are several different access control methods, some of these are:

- Mandatory Access Control (MAC) [2]- consists of multiple levels of hierarchical access control that are associated with each user or object. Normally there is a read-down, write-up policy, which means that the user is allowed to read objects with a security label equal or lower than theirs and write objects with a security label equal or higher.
- Discretionary Access Control (DAC) [2] - the user or group privileges are directly associated with specific objects.
- Role based access control (RBAC) [1] - The model has the following core concepts: Role, User, Permission and Session. The user is associated with one or more roles which in turn are linked to the permissions. When the user wants to start using the system, a session that relates the user with the activated roles (from all the roles that the user is allowed to use) is created. There are several extensions to the base model, amongst others: role hierarchies, restrictions on all the elements, contexts [4], teams [5], organizations [6] and delegation [7, 8]. It can also be used to implement the DAC and MAC [9].
- Task based access control (TBAC) [10] - In this model, when the user reaches a specific task, there are a number of allowed permissions that are checked out when they are needed, if the user tries to execute that specific task more times than allowed, his access will be refused.
- Attribute Based Access Control (ABAC) [11] - Access authorization to a specific resource is given according to the attributes of the requesting entity. Attributes are properties that are associated with specific entities

(Subjects, Resources and Environments). A RBAC model can be partially modelled in ABAC if we consider the roles (or other concepts, like teams) as attributes [12].

Many of the previous access control models can be applied in workflow systems [10, 13], but this type of systems represent a new challenge: their dynamic nature and the requirements that arise from that. In many of these systems [14], there are serious concerns regarding the separation of duty [15] in the tasks to prevent fraud, and the chosen access control method must support this.

B. Enterprise Architecture

In this section some common enterprise architecture frameworks will be briefly introduced. Several of them, contain the common concept of viewpoint. A viewpoint [16] specifies the conventions for constructing and using a view. A view represents the system from the perspective of a related set of concerns (purpose and audience). The studied enterprise architecture frameworks will be:

- Zachman Framework
- TOGAF
- ArchiMate

The Zachman Framework [17] and The Open Group Architecture Framework (TOGAF) [18] don't provide any modelling methodology for constructing an enterprise architecture, but describe how it should be built.

The Zachman Framework using six different perspectives (Scope, Business model, Information system model, Technology model, Detailed description and Actual system) describes the information which is considered essential in an enterprise architecture. These perspectives should be described in six different ways (Data, Function, Network, People, Time and Purpose).

The TOGAF contains an architecture development method (ADM) that describes which steps should be taken to develop an enterprise architecture that has the four architectural domains (Business, Data, Application and Technology).

ArchiMate [16, 19] follows a service oriented layered architecture that consists of:

- Business layer – Describes the products and services offered to external customers which are realised by the business processes.
- Application layer – Describes the application services that will be supporting the business layer. Each one of them is realized by the application components.
- Technology layer – Describes the infrastructure services needed to run applications, realised by devices and software.

Each one of these layers contains structural elements that are categorized according to the three dimensions modelling (Fig. 1) that ArchiMate is based upon.

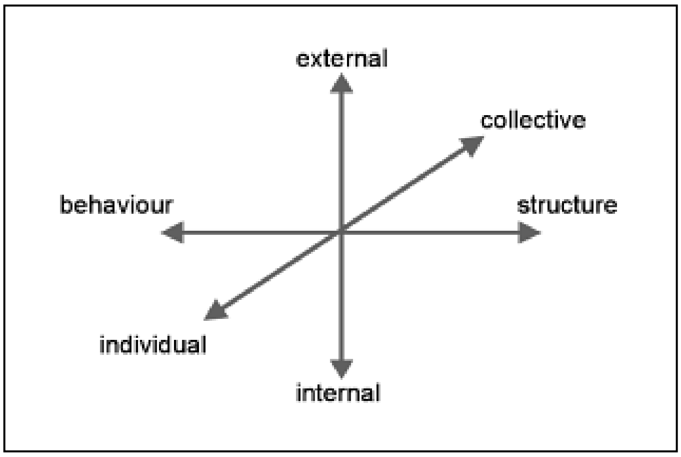

Figure 2. ArchiMate three dimensions modelling (taken from [16])

In the behaviour/structure axis (Fig. 1) there are three categories:

- Passive structure – Structural elements in which behaviour is performed.
- Behaviour – Structural elements that express the behaviour.
- Active structure – Structural elements that display behaviour.

In the internal/external (Fig. 1) there are two categories:

- Internal view – Structural elements that realize the services.
- External view – Functional (Services) and non-functional aspects that are exposed to the environment.

In the last axis, the individual/collective (Fig. 1), are included two categories:

- Individual behaviour – Behaviour that is performed by a single structural element.
- Collective behaviour – Behaviour that is performed by a collaboration of multiple structural elements.

The TOGAF ADM and ArchiMate can be used together, since TOGAF doesn't provide much guidance on creating a consistent overall model of the architecture, ArchiMate can complement it by providing a vendor-independent, standardised set of concepts to design a consistent and integrated model.

Security in enterprise architecture can be grouped according to some of the layers defined in [20]:

- Technology architecture – The access control mechanisms focus on the physical and network access to the nodes. It's also in this layer that operating system access controls are contained.
- Software architecture – Any of the access control mechanisms analysed in section A are normally used in this layer.

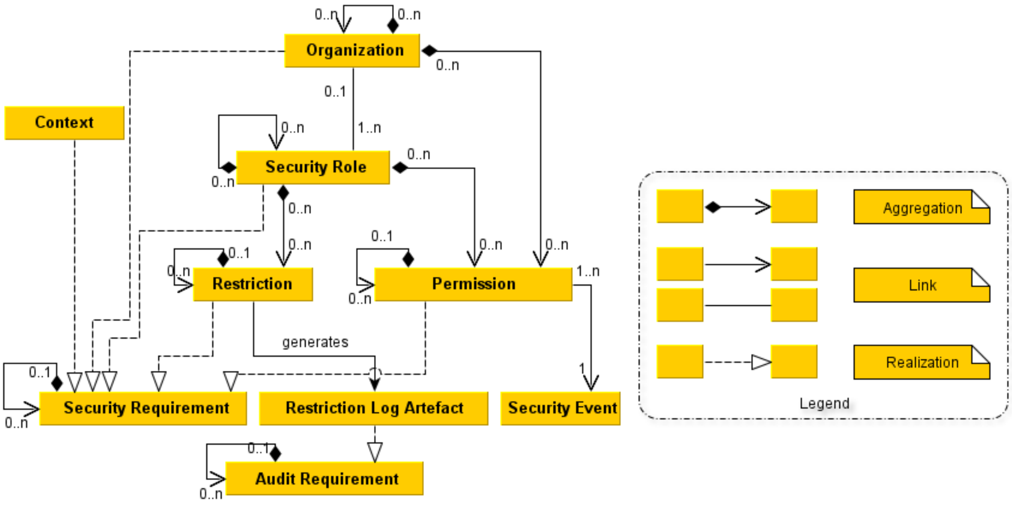

Figure 2. Proposed meta-model

- Integration architecture – In this layer, access control can be defined similarly to the software architecture layer.

In the Process and Business layer, access control is normally not represented in current mainstream enterprise architecture modelling languages, with some exceptions [12] (that use ABAC as the access control mechanism). In the enterprise architectures frameworks introduced in this section:

- TOGAF ADM doesn't include any methodology to create a security architecture but it comprises information on what type of activities it may include [18].
- ArchiMate doesn't include any object to model security concerns in the business layer [19].
- In the Zachman Framework [17] access control can be easily integrated into the various perspectives.

C. *IT Governance*

According to the IT Governance Institute (ITGI)[1], IT governance is [21]: "an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives". Some work has been done to connect governance with current enterprise architecture frameworks, for example, in [22] enterprise governance is connected with the DEMO [23] enterprise ontology framework.

There are several IT Governance frameworks that already have some focus on enterprise security. One of the most known frameworks is the Control Objectives for Information and related Technology (COBIT) [24] which is already in the version 5 and has some internal IT related goals focused on security (for example, the goal, Security of Information, processing Infrastructure and applications). One standard that focus on IT security is the ISO/IEC 2700 [25] which has a practice guide that has an entire chapter dedicated to Access Control. This standard can be mapped with the COBIT framework, just as shown in [26].

D. *Business Process Modelling*

Business processes [16, 27] are detailed descriptions of how an enterprise performs their business activities. They transform an input in an output, through several activities performed by actors (persons, organizations or systems).

The Business process modelling notation (BPMN) [27] is a standard for modelling business processes in a business processes diagram. It contains flow objects (events, activities and gateways) connected by sequence flows, message flows or association flows. The diagram is organized through swimlanes (pools and lanes) that group the activities according to the participant. It can contain artefacts (data objects, groups and annotations) to provide additional information about the business process.

IV. PROPOSAL

The artefact (Fig. 2) that will answer the proposed research questions will be presented in detail in this section and it is based on the RBAC access control model presented on the previous section. This artefact will consist of a meta-model that covers three main areas: Permissions, Restrictions and Business Rules. The three main areas will focus on different concept areas to add access control to business processes: the permissions meta-model will add concepts which are needed to represent permissions and authorized users; the restrictions meta-model will focus on how to represent access control restrictions to specific elements and the business rules meta-model will specify how to connect the previously presented concepts with the enterprise architecture business layer.

[1] http://www.itgi.org/

A. *Permission meta-model*

The permission meta-model (Fig. 3) contains several concepts to represent the permissions associated with a specific security role, and their details.

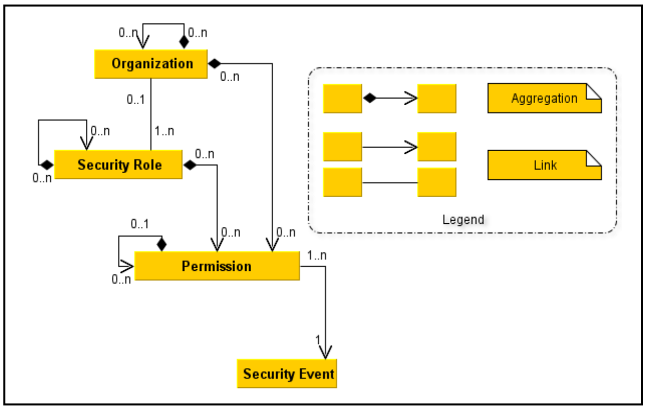

Figure 3. Permission meta-model

The several concepts included in this meta-model are:

- Security Role - With the security role concept, is possible to model the roles that are associated with a specific business actor, and the permissions associated with it. It is also possible to create a hierarchy of security roles, where the parent role aggregates all permissions of the child role.
- Organization - The organization concept allows an organization to be associated with specific security roles, and gives all these roles the extra permissions connected with that organization. It is possible to create a hierarchy of organizations where the parent organizations have all the permissions associated with their children.
- Security Event - The security event concept specifies the event (e.g. read, write, execute, etc.) where Permission is valid..
- Permission – In order to get an easier modelling, the permissions may be decomposed,. This leads to a tree hierarchy (where the topmost permissions aggregate all child permissions). They belong to specific security roles or organizations, where all roles belonging to that organization have the extra organization permissions because they were directly associated with the organization. The permissions may have an attribute (delegable), which has a Boolean value (true or false). It indicates if it the permission may be delegated when the security role that has it, is delegated.

B. *Restrictions meta-model*

The restrictions meta-model (Fig. 4) allows associating with certain business process elements, restrictions regarding access control to them.

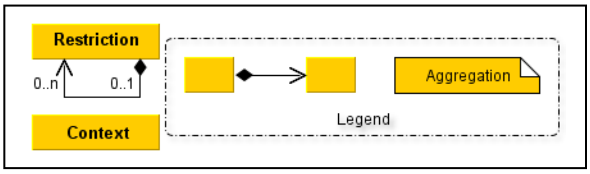

Figure 4. Restrictions meta-model

The two concepts included in this meta-model are:

- Restriction – The restrictions are defined using the Access Control Event-Condition-Language (ACECA), which will be described briefly. There may be restrictions associated with the security roles (these will be related to the delegation of that security role). A restriction may be decomposed in several sub-restrictions using aggregation. In this case, the interactions between restrictions are defined using the ACECA language.
- Context - The context concept specifies a certain context in which some elements may or may not be accessed (even if the security role or organization has permissions to access them). The context is activated and deactivated by certain business process "active" elements, such as activities or a specific action.

C. *Business Rules meta-model*

The business rules meta-model (Fig. 5) allows traceability between this meta-model and other parts of the enterprise architecture business layer. By using the requirements (Audit and Security) can be decomposed in several sub requirements using aggregation.

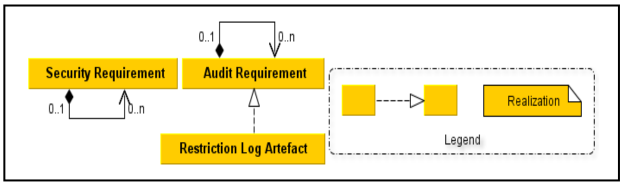

Figure 5. Business Rules meta-model

The three concepts included in this meta-model are:

- Security Requirement – The security requirement specifies that a certain requirement (taken from other sources) is realized by other meta-model elements.
- Audit Requirement – The audit requirements allow certain auditability requirements regarding access control to be specified, connecting them with the restriction log artefacts that realize them.
- Restriction Log Artefact – The restriction log artefact is generated by a restriction (when it is being enforced), and contains information about what access control element was enforced, when and by whom (and in which context, if that information is available). This artefact allows posterior auditability to the enforcement of the access control meta-model.

D. Access Control Event-Condition-Language (ACECA)

The Access Control Event-Condition-Language (ACECA) is a simple and extensible Event-Condition-Language that was created to represent the restrictions that may affect a specific business process element.

In the dissertation this language is explained in detail, but due to space constraints of this paper we cannot enter in detailed explanations of the various constructs contained in it. But there are several constructs and built-in actions that cover the basic access control mechanisms and some advanced topics (like delegation).

Also present in the main text of this dissertation there are several additional constructs that are based on some ACECA code to ease the use of this language.

V. Results

In the main text of this dissertation there are two integrations of the proposed meta-model with one business process modelling language (BPMN) and one enterprise architecture framework (ArchiMate). These integrations were used in the construction of several synthetic scenarios and in the case study to demonstrate the utility of this meta-model.

In the synthetic scenarios it is shown that this meta-model is able to answer all the proposed research questions and effectively add access control artefacts to the business process layer of the enterprise architecture. The case study shows how this meta-model can be used in a real world solution to solve real world problems.

To better group the concepts in a real world usage and integrate them with existing enterprise architecture frameworks several viewpoints were created:

- Security Roles Viewpoint (SRV) – models the structure of the security roles and organizations (and the business roles associated with them). This viewpoint also has information about the permissions owned by each security role or organization.
- Security and Audit Requirements Viewpoint (SARV) – the audit and security requirements that will be realized by the elements defined in other viewpoints will be modelled here.
- Business Objects Permissions and Restrictions Viewpoint (BOPRV) – Associates with each business object the permissions and the restrictions that affect them, along with the relevant contexts. There is also information about which elements realize the requirements defined in the SARV.
- Business Processes Permissions and Restrictions Viewpoint (BPPRV) – All restrictions that affect some business processes will be represented here along with the relevant permissions and contexts. In this viewpoint it is also shown which elements realize the requirements defined in the SARV.

For further details on the specific concerns of these viewpoints and a definition of them, according to the elements defined in [28], please see the full dissertation text.

VI. Evaluation

This thesis was evaluated and validated by following some of the guidelines introduced in [3]. These are:

- Design as an artefact – The artefact that was developed during this thesis was the meta-model to integrate access control and auditability in the business process layer of the enterprise architecture.
- Problem relevance – The research questions relevance was used to determine the problem relevance.
- Design evaluation – Three methodologies were used to evaluate the model: Informed argument, scenarios and a case study.

VII. Conclusion and Future Work

The main objective of this thesis was to create a meta-model that was extensible and its core features were able to provide effective access control design in the business process layer of the enterprise architecture. The extensibility objective was achieved by using the ACECA language to specify the restrictions. In this manner an architect may add new actions and conditions without needing to modify the core meta-model. The access control on the business layer objective was achieved as it is shown in the various scenarios presented and the case study.

Some future work on this area may be focused on expanding the ACECA language and the core model to include additional features. The integrations introduced in the thesis (ArchiMate and BPMN) are just examples of how an integration of this meta-model with existing modelling languages and frameworks can be made, they are not extensive and some future work may be focused on improving them or integrating this meta-model with other languages and frameworks.

There is also an additional research question that was not focused on this thesis but it also may be a future related work area: “How can access control be derived from business rules?”. Work on this area may automate or improve how the security and audit requirements are created and connected with this meta-model.

References

1 Sandhu, R., Ferraiolo, D., and Kuhn, R.: ‘The NIST Model for Role-Based Access Control: Towards A Unified Standard’

2 Sandhu, R., and Samarati, P.: ‘Access control: principle and practice’, Communications Magazine, IEEE, 2002, 32, (9), pp. 40-48

3 Hevner, A., March, S., Park, J., and Ram, S.: ‘Design science in information systems research’, Mis Quarterly, 2004, 28, (1), pp. 75-105

4 Georgiadis, C., Mavridis, I., Pangalos, G., and Thomas, R.: 'Flexible team-based access control using contexts', in Editor (Ed.)^(Eds.): 'Book Flexible team-based access control using contexts' (ACM, 2001, edn.), pp. 21-27

5 Thomas, R.: 'Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments', in Editor (Ed.)^(Eds.): 'Book Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments' (ACM, 1997, edn.), pp. 13-19

6 Kalam, A., Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C., and Trouessin, G.: 'Organization based access control', in Editor (Ed.)^(Eds.): 'Book Organization based access control' (IEEE, 2003, edn.), pp. 120-131

7 Barka, E., and Sandhu, R.: 'A role-based delegation model and some extensions', in Editor (Ed.)^(Eds.): 'Book A role-based delegation model and some extensions' (Citeseer, 2000, edn.), pp. 49-58

8 Abdallah, A.E., and Takabi, H.: 'Integrating delegation with the formal core RBAC model', in Editor (Ed.)^(Eds.): 'Book Integrating delegation with the formal core RBAC model' (IEEE, 2008, edn.), pp. 33-36

9 Osborn, S., Sandhu, R., and Munawer, Q.: 'Configuring role-based access control to enforce mandatory and discretionary access control policies', ACM Transactions on Information and System Security (TISSEC), 2000, 3, (2), pp. 85-106

10 Thomas, R., and Sandhu, R.: 'Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management', Database Security, 1998, 11, pp. 166-181

11 Shen, H., and Hong, F.: 'An attribute-based access control model for web services', in Editor (Ed.)^(Eds.): 'Book An attribute-based access control model for web services' (IEEE, 2006, edn.), pp. 74-79

12 Wolter, C., Menzel, M., and Meinel, C.: 'Modelling security goals in business processes', Modellierung 2008, 127, pp. 201–216

13 Chaari, S., Biennier, F., Amar, B., and Favrel, J.: 'An authorization and access control model for workflow', in Editor (Ed.)^(Eds.): 'Book An authorization and access control model for workflow' (IEEE, 2005, edn.), pp. 141-148

14 Long, D., Baker, J., and Fung, F.: 'A prototype secure workflow server', in Editor (Ed.)^(Eds.): 'Book A prototype secure workflow server' (IEEE, 2002, edn.), pp. 129-133

15 Botha, R., and Eloff, J.: 'Separation of duties for access control enforcement in workflow environments', IBM SYSTEMS JOURNAL, 2010, 40, (3), pp. 666-682

16 Lankhorst, M.: 'Enterprise architecture at work: Modelling, communication and analysis' (Springer-Verlag New York Inc, 2009), pp. 57,85-119

17 Zachman, J.: 'A framework for information systems architecture', IBM SYSTEMS JOURNAL, 1987, 26, (3)

18 http://www.opengroup.org/architecture/togaf9-doc/arch/, accessed 14/12/2010

19 http://www.opengroup.org/archimate/doc/ts_archimate/, accessed 8/12/2010 2010

20 Winter, R., and Fischer, R.: 'Essential Layers, Artifacts, and Dependencies of Enterprise Architecture', Journal of Enterprise Architecture–May, 2007, pp. 1

21 ITGI: 'Board Briefing on IT Governance', in Editor (Ed.)^(Eds.): 'Book Board Briefing on IT Governance' (IT Governance Institute, 2003, 2 edn.), pp. 10

22 Henriques, M., Tribolet, J., and Hoogervorst, J.: 'Enterprise Governance and DEMO', Master Thesis, Department of Computer Science and Engineering, Technical University of Lisboa, Instituto Superior Técnico, Lisboa, 2010

23 Dietz, J.: 'Enterprise ontology: theory and methodology' (Springer Verlag, 2006), pp. 139-158,170,173-184

24 ISACA: 'COBIT 5' (2010. 2010)

25 ISO/IEC: 'ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security management', in Editor (Ed.)^(Eds.): 'Book ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security management' (2005, edn.), pp.

26 ITGI/OGC: 'Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit', in Editor (Ed.)^(Eds.): 'Book Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit' (2008, edn.), pp.

27 http://www.omg.org/spec/BPMN/2.0/, accessed 1/02/2011

28 Society, I.C.: 'IEEE Std 1471-2000: IEEE Recommended Practice for Architectural Description of Software-Intensive Systems', in Editor (Ed.)^(Eds.): 'Book IEEE Std 1471-2000: IEEE Recommended Practice for Architectural Description of Software-Intensive Systems' (IEEE, 2000, edn.), pp.