INSTITUTO SUPERIOR TÉCNICO
Universidade Técnica de Lisboa

MODELLING ACCESS CONTROL MECHANISMS IN ENTERPRISE ARCHITECTURE

Ricardo Alexandre de Almeida Fernandes Martins

Dissertation for the Degree of Master of

Information Systems and Computer Engineering

Jury

President: Prof. Mário Rui Fonseca dos Santos Gomes

Advisor: Prof. Artur Miguel Pereira Alves Caetano

Member: Prof. André Ferreira Ferrão Couto e Vasconcelos

June 2012

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 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 Access 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

SUMÁRIO

Em muitas *frameworks* para a arquitectura empresarial (AE) actualmente existentes, o controlo de acesso não é representado nas camadas de negócio ou processos. Este é composto por três actividades principais: autenticação de utilizadores, autorização para realizar uma certa acção e auditoria das acções realizadas.

Esta tese tem como principal objectivo a realização de um modelo que seja capaz de agregar a informação sobre controlo de acesso aos processos de negócio e aos elementos relacionado com estes. Este modelo irá ser validado e avaliado de três maneiras distintas: um argumento informado, um conjunto de cenários e um caso prático realizado no DIAP.

Também foi realizada uma breve análise de algum trabalho relacionado nas três seguintes áreas: métodos para controlo de acessos, linguagens de modelação de processos de negócio e, por último, algumas *frameworks* para a representação da AE. Os métodos de controlo de acesso estudados foram: MAC; DAC; RBAC (e alguns derivados); TBAC; e ABAC. Seguidamente é feita uma breve descrição do suporte actual para informação sobre segurança em algumas *frameworks* para a AE. As linguagens de modelação de processos de negócio analisadas foram: BPMN e ArchiMate. Esta última também foi analisada na perspectiva de *framework* para a AE em conjunto com o TOGAF ADM e a *Framework* Zachman.

Algumas orientações para o trabalho futuro incluem: a integração total deste modelo em *frameworks* para a AE e em linguagens de modelação de processos de negócio e a geração automática de requisitos de segurança e auditabilidade a partir das regras de negócio.

PALAVRAS-CHAVE

Modelação de processos de negócio, Mecanismos de controlo de acessos, Auditoria, Arquitectura empresarial, Modelação conceptual

ACKNOWLEDGEMENTS

I would like to thank Professor Artur Caetano for advising me on this thesis and all friends, family and colleagues that helped me during its realization.

ADDENDUM

Since the previous delivery of this thesis its language was completely revised and some references were added to it. An acknowledgements section was also added.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF EQUATIONS

LIST OF ACRONYMS

Portuguese		English	
Acronym	**Description**	**Acronym**	**Description**
MP	Ministério Público	PPO	Public Prosecution Office
SIMP-NG	Sistema de informação do Ministério Público – nova geração	PPOIS-NG	Public Prosecution Office information system – new generation
PGR	Procuradoria-Geral da República	PGO	Prosecutor General's Office
DIAP	Departamento de Investigação e Acção penal	DIP	Department of investigation and prosecution
PSP	Polícia de Segurança Pública	PSP	Public Security Police
PJ	Polícia Judiciária	JP	Judicial Police
GNR	Guarda Nacional Republicana	RNG	Republican National Guard

GLOSSARY

Term	Definition
Business Role	A business role is defined as a named specific behaviour of a business actor participating in a particular context (Group, 2009a).
Permission	A permission authorizes a security role or organization to perform a certain action on a business object or on a business process.
Security Requirement	A Security Requirement explains exactly a specific business rule related to security that must be realized when implementing access control on the business layer of the enterprise architecture.
Audit Requirement	An Audit Requirement explains in detail a specific business rule related to auditability of the access control that must be realized when implementing access control on the business layer of the enterprise architecture.
Organization	Organization represents an external or internal group of persons. This concept also applies to external or internal organizations (companies)
Security Role	A security role is defined as the role that a business role may have when interacting with the access control system. This role will contain the permissions that are available to that business role and may belong to certain organizations.
Security Event	A security event is an event that may occur in the Access Control system. Some example of security events are: Read, Write and Execute.
ACECA	Access Control Event-Condition-Action 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.
Restriction	Restrictions are the base of the access control system. They use ACECA to specify when and who can perform a certain action on a business process or a business object.
Access Restriction	An Access Restriction is a special type of Restriction that is only concerned with access control. This is an ACECA only construct.
Organization Rule	An ACECA only construct was created to easily represent restrictions conditions that involve Organizations.
Permission Rule	An ACECA only construct was created to easily represent restrictions conditions that involve Permissions.
Context Rule	An ACECA only construct was created to easily represent restrictions conditions that involve Context.

Term	Definition
Logical Operation	An ACECA only construct that was designed to easily create complex restrictions conditions which involve certain logical operators (AND, OR and NOT)
Business Object	A business object is defined as a unit of information that has relevance from a business perspective (Group, 2009a).
Restriction Log Artefact	A Restriction Log Artefact is an access control log generated by a restriction.
Delegation Restriction	An Access Restriction is a special type of Restriction that is only concerned with the delegation of a certain security role to other security roles. This is an ACECA only construct.
Enterprise Architecture	A coherent whole of principles, methods and models that are used in the design and realization of an enterprise's organizational structure, business processes, information systems and infrastructure (Lankhorst, 2009).
Business Process	A business process is defined as a unit of internal behaviour or collection of causally-related units of internal behaviour intended to produce a defined set of products and services (Group, 2009a).

TERMS USED ON THE META-MODEL FORMALIZATION

Terms	Definition
SR	Security Role
ORG	Organization
R	Restriction
SREQ	Security Requirement
AREQ	Auditability Requirement
SE	Security Event
RLA	Restriction Log Artefact
P	Permission
ACM	Access Control Meta-model

Chapter 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 on the related work chapter (Chapter II).

Access control enables an authority to control access to resources in a given system and in the realm of computer 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) (Sandhu, Ferraiolo, & Kuhn; Sandhu & Samarati, 2002). 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 process 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 (Hevner, March, Park, & Ram, 2004). This evaluation will be made using three methodologies: informed argument, scenarios and a practical case study on the PPOIS-NG.

1 Research Questions

The following research questions are expected to be answered in this dissertation:

Q1. 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.

Q2. 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 Q1 to reach a more dynamic and complete access control system.

Q3. How to define access control authorization on the business layer of the Enterprise Architecture?

Using the concepts and their relationships introduced in questions Q1 and Q2, 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 and extensible access control system.

Q4. 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.

2 Contributions & Results

In this dissertation a set of concepts needed to represent access control in the business process domain are going to be developed to provide a way, in the business process layer of the enterprise architecture, to define how certain elements may be accessed and by whom. Since an access control system is not complete unless it provides a way to verify if a certain restriction was enforced, this dissertation will also propose a set of complementary concepts to provide auditability information to the main concepts.

These concepts will be organized in a meta-model that will be presented in Chapter III section 1, and which will also provide its formalization by using logic rules (Chapter III section 1.4). Also in this chapter, in section 1.5, there will be a complimentary event-condition language to define how the access will be restricted.

In Chapter IV the meta-model will be integrated with an enterprise architecture framework called ArchiMate (Group, 2009a) and a business process modelling language called BPMN (OMG, 2011). It will also be provided some scenarios of common usage of these integrations.

Chapter II
Related Work

In this chapter, 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 and IT Governance; and 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 and IT Governance 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.
In the end of this chapter, a brief discussion about how this related work relates to the thesis problem (introduced in Chapter I) and its questions (Chapter I1) will be made.

1 ACCESS CONTROL METHODS

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

- Mandatory Access Control (MAC) (Sandhu & Samarati, 2002) - 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) (Sandhu & Samarati, 2002) - the user or group privileges are directly associated with specific objects.
- Role based access control (RBAC) (Sandhu et al.) - 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 (Georgiadis, Mavridis, Pangalos, & Thomas, 2001), teams (Thomas, 1997), organizations (Kalam et al., 2003) and delegation (Abdallah & Takabi, 2008; Barka & Sandhu, 2000). It can also be used to implement the DAC and MAC (Osborn, Sandhu, & Munawer, 2000).
- Task based access control (TBAC) (Thomas & Sandhu, 1998) - 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) (Shen & Hong, 2006) - 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 (Wolter, Menzel, & Meinel).

Many of the previous access control models can be applied in workflow systems (Chaari, Biennier, Amar, & Favrel, 2005; Thomas & Sandhu, 1998), but this type of systems represent a new challenge: their dynamic nature and the requirements that arise from that. In many of these systems (Long, Baker, & Fung, 2002), there are serious concerns regarding the separation of duty (Botha & Eloff, 2010) in the tasks to prevent fraud, and the chosen access control method must support this.

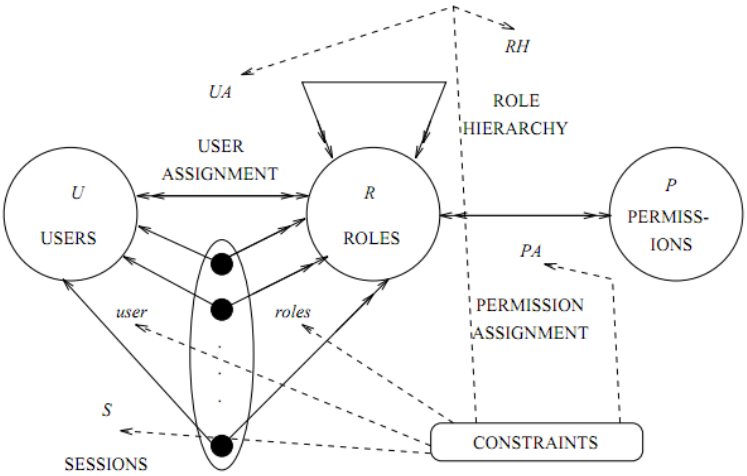

FIGURE 1 - RBAC (TAKEN FROM (RAVI, EDWARD, HAL, & CHARLES, 1996))

2 ENTERPRISE ARCHITECTURE AND IT GOVERNANCE

In this section some common enterprise architecture frameworks will be briefly introduced. Several of them, contain the common concept of viewpoint. A viewpoint (Lankhorst, 2009) 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).

2.1 ZACHMAN FRAMEWORK AND TOGAF ADM

The Zachman Framework (Zachman, 1987) and The Open Group Architecture Framework (TOGAF) (Group, 2009b) 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).

2.2 ARCHIMATE

ArchiMate (Group, 2009a; Lankhorst, 2009) 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.

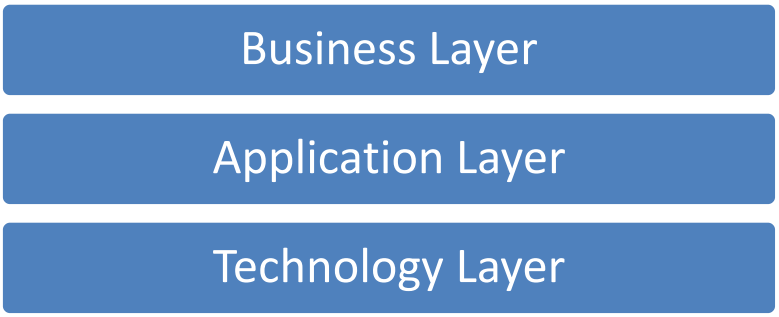

FIGURE 2 - ARCHIMATE LAYERS

Each one of these layers contains structural elements that are categorized according to the three dimensions modelling (Figure 2) that ArchiMate is based upon.

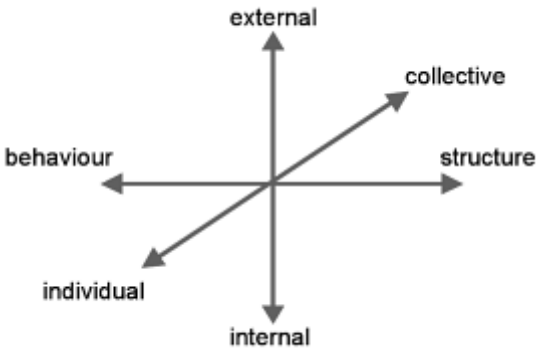

FIGURE 3 - ARCHIMATE THREE DIMENSIONS MODELLING (TAKEN FROM (LANKHORST, 2009))

In the behaviour/structure axis (Figure 3) 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 (Figure 3) 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 (Figure 3), 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.

2.3 SECURITY IN ENTERPRISE ARCHITECTURE

Security in enterprise architecture can be grouped according to some of the layers defined in (Winter & Fischer, 2007):

- 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 0 are normally used in this layer.
- 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 (Wolter et al.) (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 (Group, 2009b).
- ArchiMate doesn't include any object to model security concerns in the business layer (Group, 2009a).
- In the Zachman Framework (Zachman, 1987) access control can be easily integrated into the various perspectives.

2.4 IT GOVERNANCE

According to the IT Governance Institute (ITGI)[1], IT governance is (ITGI, 2003): "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 (Henriques, Tribolet, & Hoogervorst, 2010) enterprise governance is connected with the DEMO (Dietz, 2006) 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) (ISACA, 2010) 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 (ISO/IEC, 2005) 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 (ITGI/OGC, 2008).

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

3 BUSINESS PROCESS MODELLING

Business processes (Lankhorst, 2009; OMG, 2011) 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) (OMG, 2011) 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 swim lanes (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.

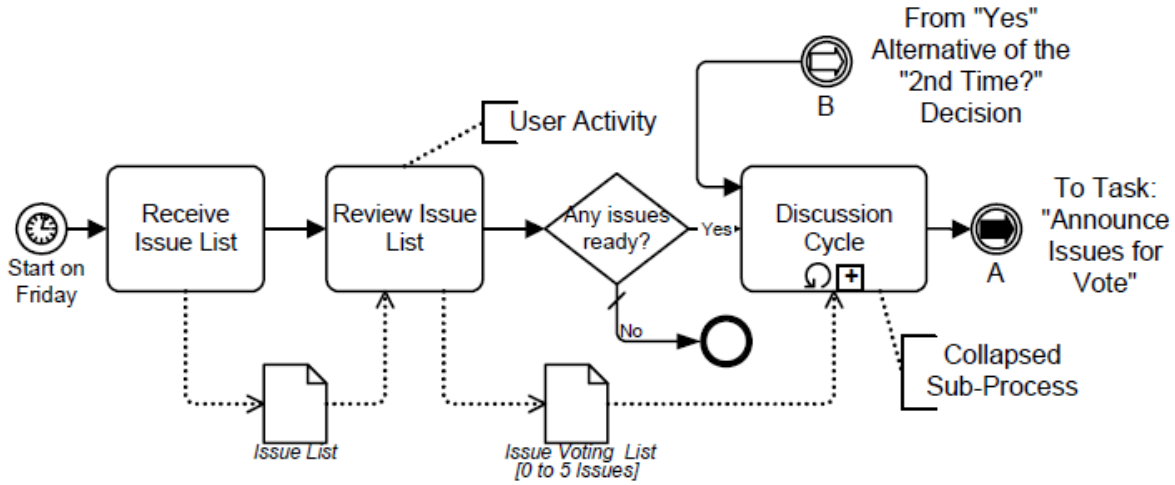

FIGURE 4 - EXAMPLE BPMN BUSINESS PROCESS (WITHOUT SWIM LANES) (TAKEN FROM (OMG, 2009))

In ArchiMate (Group, 2009a) business processes are modelled as a high level concept that realizes business services, use business objects, which are assigned to one business role and are triggered by business behaviours. There is no detailed specification of the business activities that are performed inside each business process (in the core model). One additional feature of ArchiMate is that it allows grouping business processes as business functions. Each ArchiMate business process must be described in detail using another business process language (for example BPMN).

4 DISCUSSION

In this section a brief analysis of the related work introduced in this chapter will be presented. This analysis will start with the explanation of the control method chosen and the reasons behind this choice. Afterwards, a brief discussion behind the current enterprise architecture frameworks and business process modelling will be made.

4.1 ACCESS CONTROL METHODS

The several access control methods introduced in this related work chapter will be compared here, and the reasons for choosing RBAC will be explained.

	Q1	Q2	Q3	Q4
MAC	No	No	Full	No
DAC	Partial	Partial	Full	No
RBAC	Full	Full	Full	No
TBAC	Full	Full	Full	No
ABAC	Full	Full	Full	No

TABLE 1: NO – DOESN'T ANSWER THE QUESTION; PARTIAL – ONLY ANSWERS THE QUESTION IN PART; FULL – ANSWERS THE QUESTION COMPLETELY

Table 1 shows the comparison of the various access control methods studied on the previous section and their relationship with the research questions defined in Chapter I section 1. As can be seen from the table none of the access control methods studied covers the research question Q4 (How to define access control auditability on the business layer of the Enterprise Architecture?), because none of them provide specific constructions to represent it.

Mandatory Access Control method (MAC) can't answer questions Q1 and Q2 (respectively: "Which access control concepts are required in the business process domain?" and "What is the concept structure and what are the relationships between concepts?") because it doesn't support the full set of concepts required by the business process layer. An example of such lack of support is that in this access model the restrictions are applied as a label (e.g. Confidential, Restricted, etc.) to an object and any group of roles may have permissions to access it, becoming impossible to restrict access to an element to a specific role. If, for example, we have three different roles (R1, R2 and R3) and we have three objects (O1, O2 and O3), if those three roles have access to elements marked as "Confidential" and the three objects are also marked as such, we cannot restrict access to O1 just for R1, O2 for R2 and O3 to R2. Even if we assigned different labels to the objects, such as the Confidential1 label to O1 and R1, the Confidential2 label to O2 and R2 and the Confidential3 label to O3 and R3, and since this model only supports multiple hierarchical levels of labels (and all parent labels have access to their child labels), it wouldn't matter how we would arrange the hierarchy (e.g. Confidential1 as the parent label of Confidential2 and Confidential3 as the child of Confidential2), some roles would have access to objects they were not supposed to

The Discretionary Access Control method (DAC) has partial support to the questions Q1 and Q2 because it can restrict access to an element to a specific role (without being inherited by others as in MAC), but it doesn't support other concepts required in the business process layer model such as, for example, a specific context where a permission is valid (even if a role has permission to access a specific element, the modeller may want to restrict its access to a specific business process context where that permission is valid).

Role Based Access Control (RBAC), Task Based Access Control (TBAC) and Attribute Based Access Control (ABAC) fully support all the required features of access control in the business process layer. In this thesis we are going to be focused on the RBAC model because with it we can easily model all the required access control features using the core or extended model.

4.2 Enterprise architecture and IT Governance

In this section the studied enterprise architecture frameworks will be compared. It will also be explained how the previously introduced IT Governance frameworks are related to this thesis.

	Q1	Q2	Q3	Q4
Zachman Framework	No	No	No	No
TOGAF ADM	No	No	No	No
ArchiMate	No	No	No	No

Table 2: No – Doesn't answer the question; Partial – Only answers the question in part; Full – Answers the question completely

As shown in section 2.3 the studied frameworks don't support natively access control artefacts in the business process layer. Although it doesn't provide any access control artefact, TOGAF ADM, states what kind of activities are needed to create a security architecture. Since ArchiMate is an extensible framework, we will use it to show an example of integration of the meta-model that will be created in the Chapter III.

In the context of this thesis, IT Governance is used as an input of the access control policies to be used while modelling the access control artefacts. This thesis will not focus on how these policies are created or how they are transposed to business rules, but it will be an example of a work in this research area (Guerreiro, Vasconcelos, & Tribolet, 2010).

4.3 Business Process Modelling

The support for the research questions introduced in Chapter I section 1 by the studied business process modelling languages is shown in Table 3.

	Q1	Q2	Q3	Q4
ArchiMate	No	No	No	Partial
BPMN	No	No	No	Partial

Table 3: No – Doesn't answer the question; Partial – Only answers the question in part; Full – Answers the question completely

None of languages (BPMN and ArchiMate Business processes) support natively the artefacts which are necessary to represent access control in the Business Process Layer of the Enterprise Architecture. Although both languages don't fully answer question Q4, we can design in them a business process to audit other business processes. In this thesis, BPMN is going to be used to represent business processes and is going to be extended with the artefacts that are needed to represent access control.

Chapter III
Proposal

The artefact that will answer the research questions introduced in Chapter I section 1 will be presented in detail in this chapter. This artefact will consist of a meta-model that covers three main areas: Permissions, Restrictions and Business Rules. 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.

After these concepts are presented, a meta-model mathematical formalization will be made. Since the restrictions introduced in the restrictions meta-model will need an auxiliary language, this will also be presented in this chapter.

1 META-MODEL

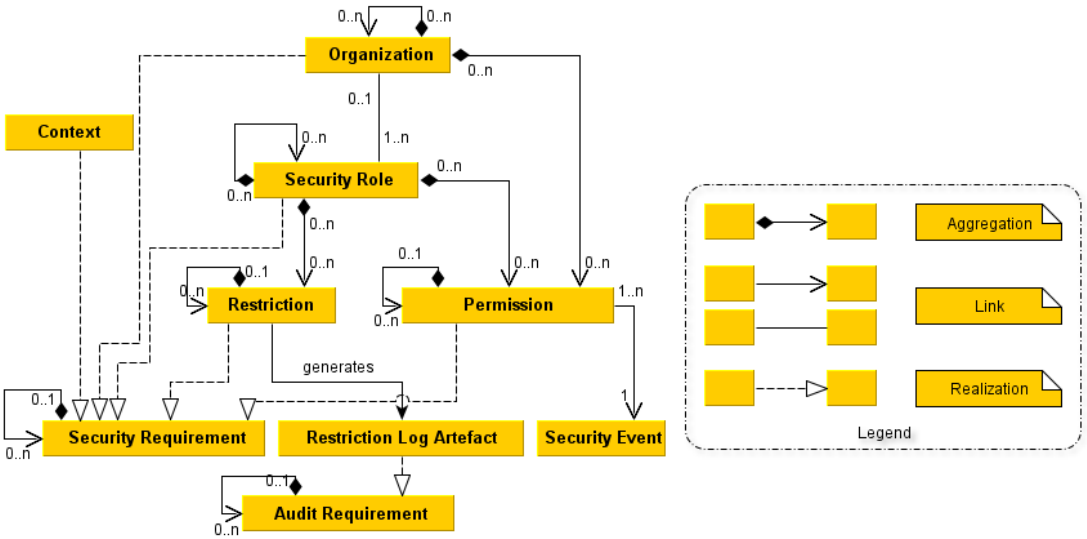

FIGURE 5: PROPOSED META-MODEL

1.1 PERMISSIONS

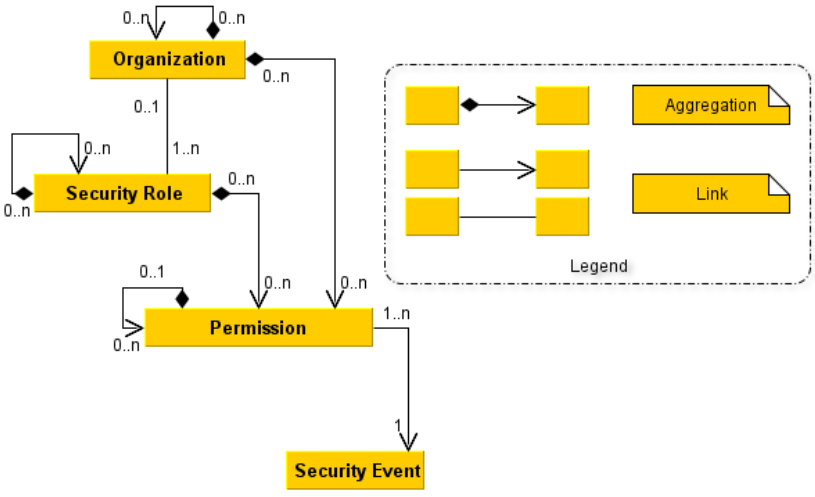

FIGURE 6: PERMISSIONS META-MODEL

The permission meta-model (Figure 6) contains several concepts to represent the permissions associated with a specific security role, and their details.

1.1.1 Security Role

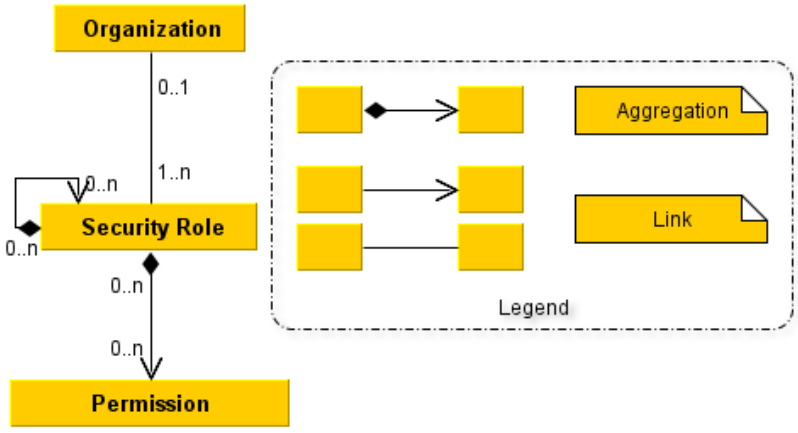

Figure 7: Permission Meta-model - Security Role

With the security role concept (Figure 7), 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.

1.1.2 Organization

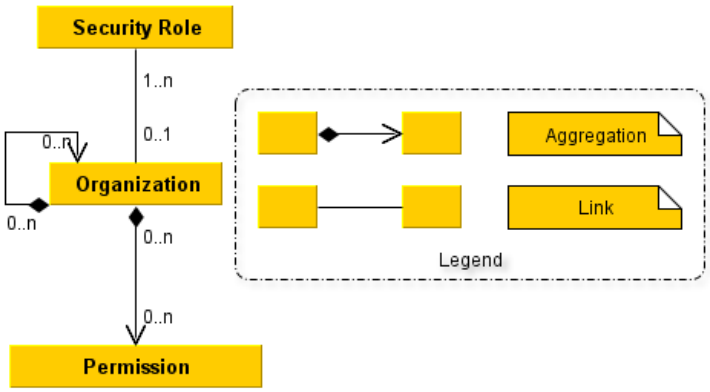

Figure 8: Permission Meta-model – Organization

The organization concept (Figure 8) 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.

1.1.3 Security Event

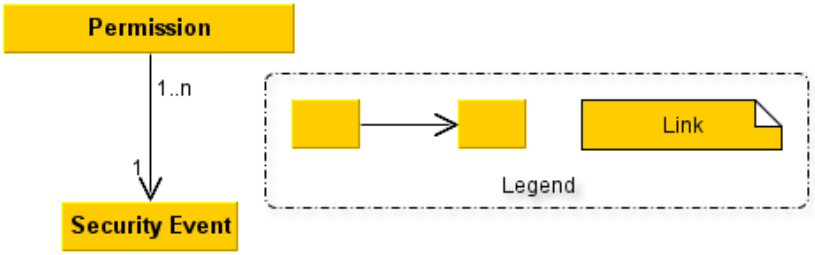

Figure 9: Permission Meta-model - Security Event

The security event concept (Figure 9) specifies the event (e.g. read, write, execute, etc.) where a Permission is valid.

1.1.4 Permission

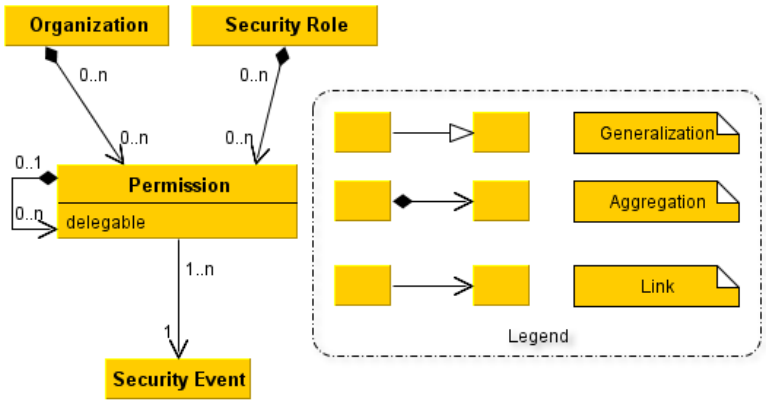

Figure 10: Permission Meta-model – Permission

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) that has a Boolean value (true or false). It indicates if the permission may be delegated when the security role that has it is delegated (see section 1.5.7 for details on delegation).

1.1.5 Example of usage

With the permissions meta-model, a user can model the security roles used to access control to specific elements. These roles have associated with them the permissions needed to perform certain actions that occur when security events are triggered. The organization entity may hold permissions and have security roles connected to it. It is also possible to create complex hierarchies of security roles or organizations that control the permissions which are inherited by each level.

1.2 RESTRICTIONS

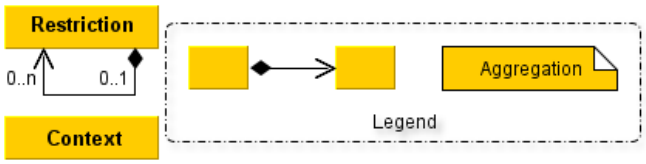

FIGURE 11: RESTRICTIONS META-MODEL

The restrictions meta-model (Figure 11) allows associating with certain business process elements, restrictions regarding access control to them.

1.2.1 CONTEXT

The context concept specifies a certain context in which some elements may or may not be accessed (even if the security role or the organization have permissions to access them). The context is activated and deactivated by certain business process "active" elements, such as activities or a specific action (see section 1.5.5).

1.2.2 RESTRICTION

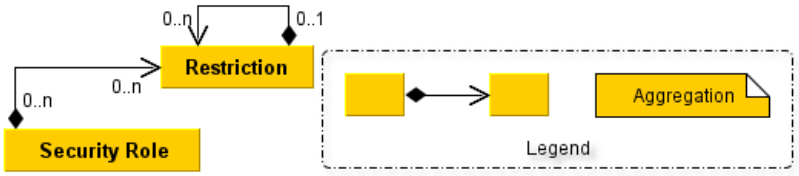

FIGURE 12: RESTRICTION META-MODEL – RESTRICTION

The restrictions are defined using the Access Control Event-Condition-Language (ACECA), which will be described in detail in Section 1.5 of this chapter. There may be restrictions associated with the security roles (these will be related to the delegation of that security role, see section 1.5.7).

A restriction may be decomposed in several sub-restrictions using aggregation. In this case, the interactions between restrictions are defined using the ACECA language.

1.2.3 EXAMPLE OF USAGE

The restrictions are defined using the ACECA language that will be presented later in this chapter (section 1.5) and may be used to restrict access to certain actions that occur during a specific set of security events to authorized security roles or organizations (this will be discussed in detail when the ACECA language is presented). The context concept defines in which context a certain action may be performed even if the required permissions or preconditions are held.

1.3 BUSINESS RULES

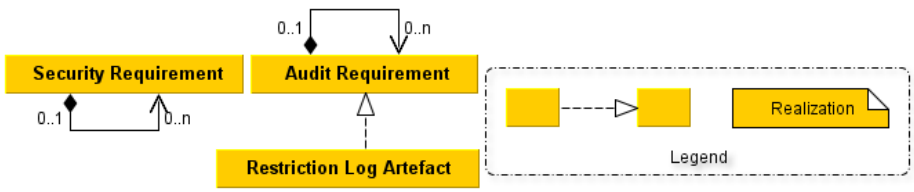

FIGURE 13: BUSINESS LAYER META-MODEL

The business rules meta-model (Figure 13) allows traceability between this meta-model and other parts of the enterprise architecture business layer. By using aggregation the requirements (Audit and Security) can be decomposed in several sub requirements.

1.3.1 Security Requirement

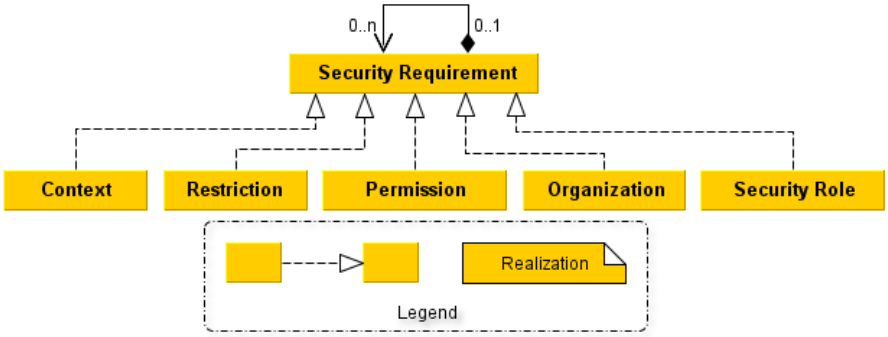

Figure 14: Business Layer Meta-model - Security Requirement

The security requirement (Figure 14) specifies that a certain security requirement regarding access control (taken from other sources) is realized by other meta-model elements.

1.3.2 Audit Requirement

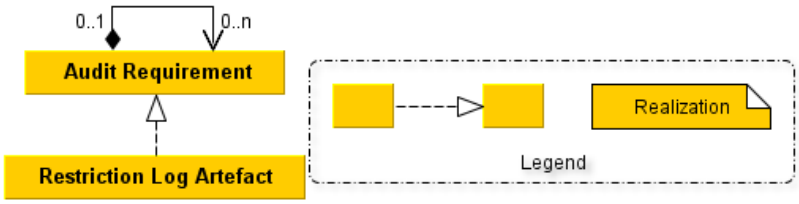

Figure 15: Business Layer Meta-model - Audit Requirement

The audit requirements (Figure 15) allow certain auditability requirements regarding access control to be specified, connecting them with the restriction log artefacts that realize them.

1.3.2.1 Restriction Log Artefact

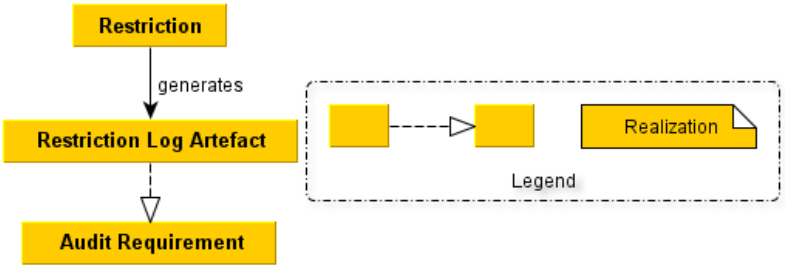

Figure 16: Business Layer Meta-model - Restriction Log Artefact

The restriction log artefact (Figure 16) 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. The generation of this artefact is explained in section 1.5.6.

1.3.3 Example of usage

With the concepts introduced in this section, the user may specify why a certain access control restriction or permission is needed, and how to obey to certain auditability requirements through the generation of log artefacts.

1.4 META-MODEL FORMALIZATION

In this section the meta-model is going to be formalized using a series of definitions.

EQUATION 1: ASR SET

EQUATION 2: AORG SET

EQUATION 3: AR SET

EQUATION 4: ASREQ SET

EQUATION 5: AAREQ SET

EQUATION 6: ASE SET

EQUATION 7: ARLA SET

EQUATION 8: AP SET

The following sets are used in other definitions:

- ASR (Equation 1) – a set containing all security roles (SR).
- AORG (Equation 2) – a set containing all organizations (ORG).
- AR (Equation 3) – a set containing all restrictions (R).
- ASREQ (Equation 4) – a set containing all security requirements (SREQ).
- AAREQ (Equation 5) – a set containing all audit requirements (AREQ).
- ASE (Equation 6) – a set containing all the security events (SE).
- ARLA (Equation 7) – a set containing all the restriction log artefacts (RLA).
- AP (Equation 8) – a set containing all permissions (P).

EQUATION 9: META-MODEL DEFINITION

Equation 9 defines the proposed meta-model as being composed of seven sets: ASR, AORG, AR, ASREQ, AAREQ, ASE and ARLA.

1.4.1 SECURITY ROLES

EQUATION 10: SECURITY ROLES HIERARCHY (SRH IS A PARTIAL ORDERED SET)

SRH (Equation 10) is a set that holds all security role hierarchy in the meta-model.

EQUATION 11: SECURITY ROLES CHILDREN

EQUATION 12: SECURITY ROLES CHILDREN FUNCTION FULL DEFINITION

src (Equation 11) is a function that returns all security roles that are children of the security role given as argument (the function is fully defined in Equation 12).

Equation 13: Security role to permission assignment (many to many)

SRP (Equation 13) is a many to many relation that assigns specific permissions to security roles.

Equation 14: Security role own permissions

Equation 15: Security role own permissions function full definition

srop (Equation 14) is a function that returns all permissions assigned to a specific security role (this function is fully defined in Equation 15). The pc function that is referred in Equation 15 will be defined briefly.

Equation 16: Permissions associated with all children security roles

Equation 17: srcp full function definition

srcp (Equation 16, and fully defined in Equation 17) is a function that returns all permissions associated with child security roles.

Equation 18: All permissions associated with a specific security role

Equation 19: srap function full definition

srap (Equation 19) returns all the permissions associated with a specific security role, whether these are directly associated (using the srop function) or the child permissions (using the srcp function). This function is fully defined in Equation 19.

Equation 20: Assignment of security roles to organizations

Equation 20 introduces the SRO set, which has the assignments of security roles to organizations. The condition present in the equation, state that one security role can only be assigned to one organization.

1.4.2 Organizations

Equation 21: Organizations permissions (many to many)

ORGP (Equation 21) is a set that holds all the permissions that an organization has.

Equation 22: Organizations hierarchy (ORGH is a partially ordered set)

ORGH (Equation 22) is a partially ordered set that holds the organization hierarchy.

Equation 23: orgc function

EQUATION 24: ORGC FUNCTION FULL DEFINITION

orgc (Equation 23 and fully defined in Equation 24) is a function that given a specific organization, returns all child organizations.

EQUATION 25: ORGAP FUNCTION

EQUATION 26: ORGAP FUNCTION FULL DEFINITION

In Equation 25 the function that returns all permissions for a given organization is introduced. Equation 26 shows the full definition of this function.

EQUATION 27: ORGCP FUNCTION

EQUATION 28: ORGCP FUNCTION FULL DEFINITION

orgcp (Equation 27) is a function that returns all the permissions associated with the child organizations of a given organization. The full definition of this function is presented in Equation 28.

EQUATION 29: ORGOP FUNCTION

EQUATION 30: ORGOP FUNCTION FULL DEFINITION

The orgop function (Equation 29, and fully defined in Equation 30) returns all permissions that an organization holds.

1.4.3 SECURITY EVENTS

EQUATION 31: SECURITY EVENT

A security event (Equation 31) is composed of one variable called name that holds the name of this security event.

1.4.4 PERMISSIONS

EQUATION 32: PERMISSION

Equation 32 states that permission has a variable called delegable that can assume one of two values: true or false. This variable defines if permission can be delegated when the owner roles are delegated.

PSE

EQUATION 33: PERMISSION HIERARCHY (PH IS A PARTIALLY ORDERED SET)

PH (Equation 33) is a partially ordered set that holds the permission hierarchy.

EQUATION 34: CP FUNCTION

EQUATION 35: CP FUNCTION FULL DEFINITION

EQUATION 36: PC FUNCTION

EQUATION 37: PC FUNCTION FULL DEFINITION

In Equation 36 the pc function is defined (fully defined in Equation 37) as returning all child permissions of the argument permission. It uses an additional function (cp, defined in Equation 34 and fully defined in Equation 35) that returns only the direct child permissions of a determinate permission.

EQUATION 38: PERMISSIONS TO SECURITY EVENTS ASSIGNMENT

PSE (Equation 38) is a partially ordered set that has all the assignments of permissions to security events. The conditions present in the equation, guarantee that only one security event can be assigned to a specific permission.

1.4.5 RESTRICTIONS

EQUATION 39: RESTRICTIONS HIERARCHY

Equation 39 defines the restriction hierarchy with the condition that one restriction can only have one parent.

EQUATION 40: SECURITY ROLE RESTRICTIONS (MANY TO MANY)

SRR (Equation 40) is a many to many set that stores which restrictions are applied to each security role.

EQUATION 41: RDC FUNCTION

EQUATION 42: RDC FUNCTION FULL DEFINITION

EQUATION 43: RIC FUNCTION

EQUATION 44: RIC FUNCTION FULL DEFINITION

EQUATION 45: RC FUNCTION

EQUATION 46: RC FUNCTION FULL DEFINITION

The function defined in Equation 45, and fully defined in Equation 46, returns all direct (using the rdc function, Equation 41 and Equation 42) and indirect (via the ric, Equation 43 and Equation 44) child restrictions.

1.4.6 SECURITY REQUIREMENTS

EQUATION 47: SECURITY REQUIREMENTS HIERARCHY

SREQH (Equation 47) is a partially ordered set that contains the security requirements hierarchy. It has an additional condition that one security requirement can only have one parent.

EQUATION 48: ELEMENTS THAT MAY REALIZE SECURITY REQUIREMENTS

EQUATION 49: SECURITY REQUIREMENTS REALIZATION

Equation 49 is a many to many set that contains which elements realize the security requirements (these elements where defined in the SREQRE set, see Equation 48).

EQUATION 50: SREQDC FUNCTION

EQUATION 51: SREQDC FUNCTION FULL DEFINITION

EQUATION 52: SREQIC FUNCTION

EQUATION 53: SREQIC FUNCTION FULL DEFINITION

EQUATION 54: SREQC FUNCTION

EQUATION 55: SREQC FUNCTION FULL DEFINITION

sreqc (Equation 54, and fully defined in Equation 55) returns all children of a certain security requirement (whether they are direct, using the function sreqdc introduced in Equation 50 and fully defined in Equation 51, or children of its children using the function sreqic that was presented in Equation 52 and defined in Equation 53).

1.4.7 AUDIT REQUIREMENTS

EQUATION 56: AUDIT REQUIREMENTS HIERARCHY

AREQH (Equation 56) is a partially ordered set that contains the audit requirements hierarchy. It has an additional condition that one audit requirement can only have one parent.

EQUATION 57: AUDIT REQUIREMENTS REALIZATION

Equation 57 is a many to many set that contains which restriction log artefacts realize the audit requirements.

EQUATION 58: AREQDC FUNCTION

EQUATION 59: AREQDC FUNCTION FULL DEFINITION

EQUATION 60: AREQIC FUNCTION

EQUATION 61: AREQIC FUNCTION FULL DEFINITION

EQUATION 62: AREQC FUNCTION

EQUATION 63: AREQC FUNCTION FULL DEFINITION

areqc (Equation 62, and fully defined in Equation 63) returns all child audit requirements of a certain audit requirement (whether they are direct, using the function areqdc introduced in Equation 58 and fully defined in Equation 59, or children of its children using the function areqic that was presented in Equation 60 and defined in Equation 61).

1.5 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.

While explaining the core ACECA constructs, the following writing conventions will be used: **BOLD** to represent keywords or built-in functions and operators and *ITALICS* to represent variable content (like expressions, function arguments, events, etc.).

1.5.1 CONCEPTS

The main core concepts of this language are:

- Security Roles – The security roles that are activated in the current session (see Section 1.1.1).
- Organizations – The organizations that some activated role may belong to (see Section 1.1.2).
- Permissions – The permissions associated with the security roles (see Section 1.1.4).
- Contexts – The contexts that may or may not be active to access a certain business process element (see Section 1.2.1).

1.5.2 SECURITY EVENTS

The events used in this language are described on a per project basis, using the Security Event concept introduced in Section 1.1.3 (with the exception of the delegated event that is part of the core ACECA language delegation features. For more details see section 1.5.7).

The following events are used in the rest of this document:

- access – raised when the business object is accessed.
- modification – triggered when some changes are made to the business object.
- execute – generated when some business process or activity is executed.
- delegated – an event that represents the delegation or sub-delegation of a security role (see Section 1.5.7).

1.5.3 SYNTAX

The ACECA language has a simple pseudo programming language inspired syntax. In this section, the main structural blocks that constitute it are going to be explained in detail.

1.5.3.1 ON BLOCK

The ON block is the main structure of the language and every other block (with the exception of the PRE and POST block, see section 1.5.3.3) is written inside it. It is constructed in the following manner:

ON *event* **THEN**

action

NO

The event that triggers the block is listed between the **ON** keyword and the **THEN** keyword, afterwards the actions that are executed inside the block are presented ending when the **NO** keyword appears.

1.5.3.2 IF EIF BLOCK

The IF EIF block exists to impose certain conditions for the execution of specific actions. It is structured in the following way:

IF *condition* **THEN**

action

EIF *condition* **THEN**

action

ELSE

action

FI

In this block the user may create several conditional execution branches, but only one of them will be executed (or none, if all conditions are evaluated as false. and there is no ELSE branch). To initiate the IF EIF block the **IF** keyword is followed by the condition that is composed using the operators and functions defined in Section 1.5.4. The condition ends when the **THEN** keyword appears and is followed by the actions that will be executed in that conditional branch. To introduce alternate conditional branches one or more EIF branches can be added and they will follow the same structure as the main if branch. When all conditions are evaluated as false, it may exist an ELSE branch that is composed by the **ELSE** keyword followed by the actions. To end the IF EIF block, the FI keyword is used (in the example is after the ELSE branch, but if there is no ELSE branch, it may follow the actions of the EIF block or the IF block).

The IF EIF block is integrated with the ON block in the following way:

ON *event*

IF *condition* **THEN**

action

FI

NO

The **THEN** following the *event* may be omitted in this special case.

1.5.3.3 PRE AND POST BLOCK

The PRE block exists to impose the execution of certain actions, before the execution of the main ON block. The POST block is similar to the PRE block, but the actions are executed after the main ON block. Their structure is:

PRE

action

ERP

POST

action

TSOP

The **PRE** or **POST** keyword is followed by the actions that are going to be performed and the block is terminated using the **ERP** or **TSOP** keyword (respectively).

1.5.4 OPERATORS AND FUNCTIONS

The following section describes the available core operators and functions. They are described using the following structure: operator (type) – brief description.

1.5.4.1 LOGICAL OPERATORS

The available logical operators are:

- AND (binary) –Performs the logical and operation. It returns true if both arguments are true otherwise returns false.
- OR (binary) – Performs the logical or operation. Returns true if one of the arguments is true, otherwise returns false.
- NOT (unary) – Negates the logical value of the argument.

1.5.4.2 ACCESS CONTROL FUNCTIONS

The available access control functions are:

- HAS(expression) – Verifies that the current active security role has the permissions defined in the expression. The expression may be written using a complex rule that uses the logical operators to combine several permissions (e.g. HAS(P1 OR P2) – verifies that the active security role has either P1 or P2; HAS(P1 OR (P2 AND P3) – verifies that the role has the permission P1 or both P2 and P3).
- BELONGS(expression) – verifies that the current active security role belongs to the organization defined in the expression. A complex expression using organizations, similar to the HAS function, may be given as argument.
- IS-ACTIVATED(expression) – Verifies that the context (or contexts) defined in the expression are active. The expression given can have similar rules to the HAS and BELONGS functions.

1.5.5 BUILT-IN ACTIONS

The following list of actions is built-in in the ACECA language and they will be described in a similar way as section 1.5.4:

- ACTIVATE-CONTEXT(context) – Activates the context defined in the argument.
- DEACTIVATE-CONTEXT(context) – Deactivates the context defined in the argument.
- ALLOW (no arguments) – Allows the requested access to the element.
- DENY (no arguments) – Denies the requested access to the element.

1.5.6 RESTRICTION LOG ARTEFACT

The restriction log artefact is generated appending a POST block to any restriction that needs to generate it. The information recorded can be customized on a per project basis. On the remaining of this document the action LOG will be used to store and generate it.

Example ACECA code to generate a restriction log artefact:

ON *event* **THEN**

action

NO

POST

LOG

TSOP

1.5.7 DELEGATION

Delegation of a security role is represented as a special type of event: *delegated*. The delegation model proposed in this document uses a standard ON block but with some extra keywords to deal with delegation and sub-delegation.

The following ACECA code deals with delegation:

ON *delegated* **TO** *roles*

THEN

action

NO

To deal with sub-delegation, the following ACECA code is used:

ON *delegated* **FROM** *role* **TO** *roles*

THEN

action

NO

This block starts with the **ON** keyword followed by the event named *delegated*. When the block refers to sub-delegation, the role that is further delegating the original role is written after the **FROM** keyword. Both variations of this block state which roles may receive the permissions and rights associated with the delegated role, by listing them after the **TO** keyword. The rest of the block is equal to the traditional ON block (see section 1.5.3.1). The role that is being delegated does not need to be specifically stated in the ACECA code, because the restriction that contains it belongs to a specific security role.

1.5.8 COMMON ACECA CONSTRUCTIONS

To minimize coding in ACECA, this section will introduce graphical constructs that are equivalent to some ACECA code.

1.5.8.1 SUPPORT CONSTRUCTS

These constructs are used by the main constructs to represent some specific aspects.

1.5.8.1.1 RESTRICTION RULE

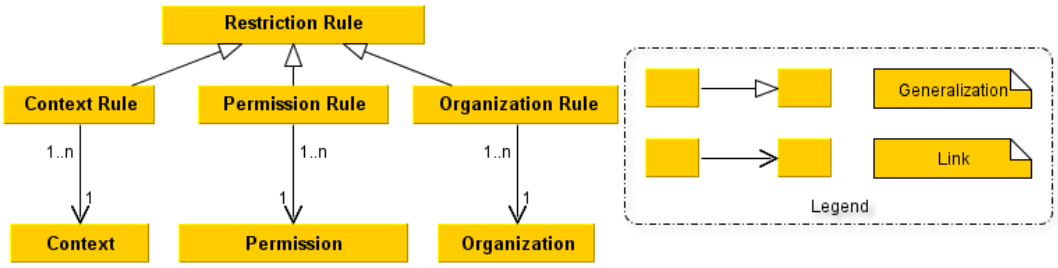

FIGURE 17: RESTRICTION RULE

Figure 17 introduces restriction rules that will be used in other common ACECA constructions in this section. They are the graphical representation of the access control functions presented in section 1.5.4.2 (context rule is the IS-ACTIVATED function, permission rule is the HAS function and the organization rule is the BELONGS function) where the argument is the linked object.

1.5.8.1.2 LOGICAL OPERATOR

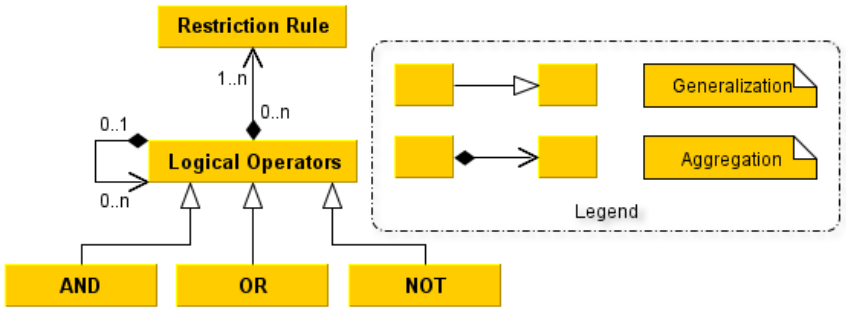

FIGURE 18: LOGICAL OPERATOR

As in the previous section (1.5.8.1.1), these elements (Figure 18) are used in other common ACECA constructions and represent the graphical representation of the logical operators presented in 1.5.4.1. Their arguments are the restriction rules and they may be composed to create more complex expressions.

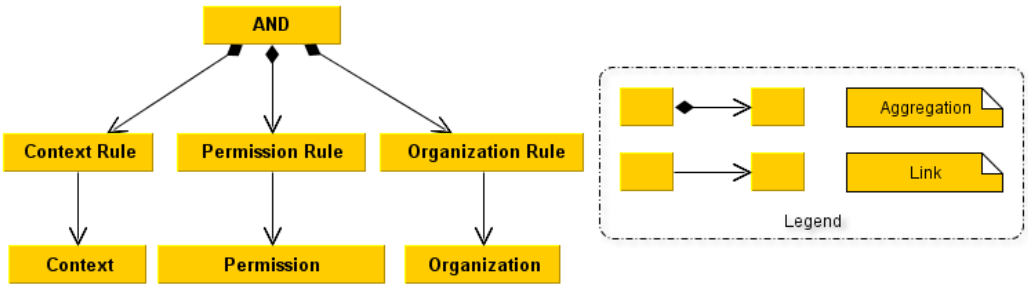

FIGURE 19: RESTRICTION RULES COMPOSITION EXAMPLE

Figure 19 shows an example of a restriction rule composition to create a more complex expression, which is equivalent to the following ACECA expression:

IS-ACTIVATED(*Context*) **AND HAS**(*Permission*) **AND BELONGS**(*Organization*)

1.5.8.1.3 BUILT-IN ACTIONS

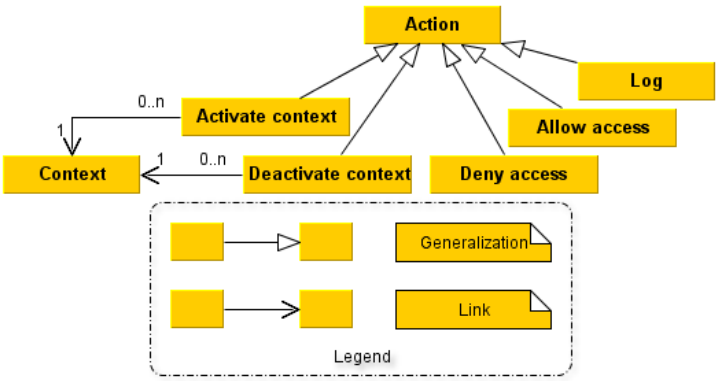

FIGURE 20: BUILT-IN ACTIONS

The elements introduced in Figure 20 are the graphical representations of the built-in actions presented in section 1.5.5, and the log action. The activate context and the deactivate context actions are, respectively, the ACTIVATE-CONTEXT and the DEACTIVATE-CONTEX built-in actions with the linked context as argument. The log action is the built-in action introduced in section 1.5.6 and the allow access and the deny access actions are the ALLOW and DENY built-in actions.

1.5.8.2 MAIN CONSTRUCTS

The main common ACECA constructs represent the access control restrictions that may be applied to the various elements.

1.5.8.2.1 ACCESS RESTRICTION

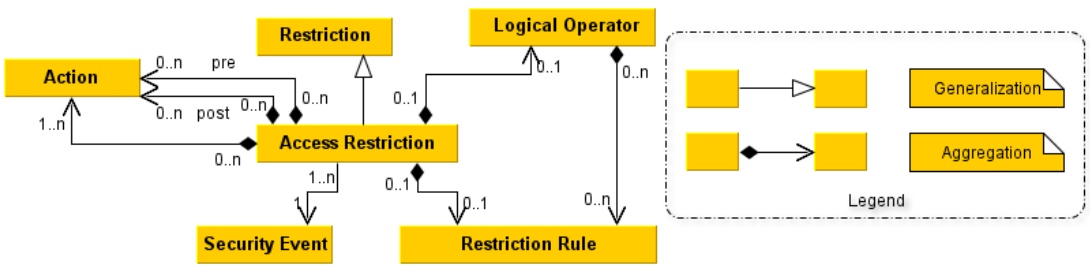

FIGURE 21: ACCESS RESTRICTION

Using the access restriction constructs presented in Figure 21 it is not needed to use directly ACECA code to represent some common access restrictions. An access restriction may be connected to a logical operator, which in turn is connected to the restriction rules, or to one restriction rule (the reason is only one, because it is impossible the composition of restriction rules without logical operators). It may also have associated some pre and post actions (equivalent to the PRE and POST blocks, see section 1.5.3.3), that are represented by the aggregations labelled as pre and post, respectively. The actions that are going to be executed inside the ON block are also linked through an aggregation.

The access restriction generates an ACECA code equivalent to this:

PRE

pre-actions

ERP

ON *event*

IF *expression* **THEN**

actions

FI

NO

POST

post-actions

TSOP

The *event* in this ACECA code will be the security event that is linked by the access restriction, the **IF** block *expression* will be composed using the connected logical operators and restriction rules or, if there is no logical operator, the restriction rule will be directly connected to it. The various actions (*pre-actions*, *post-actions* and *actions*) will be the linked elements previously introduced.

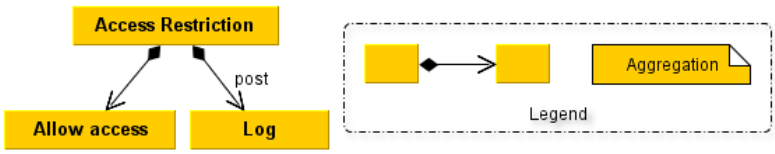

FIGURE 22: ACCESS RESTRICTIONS DEFAULT ACTIONS

The access restriction actions shown in Figure 22, are the default actions for all access restrictions in this document when no other actions are shown.

1.5.8.2.2 DELEGATION RESTRICTION

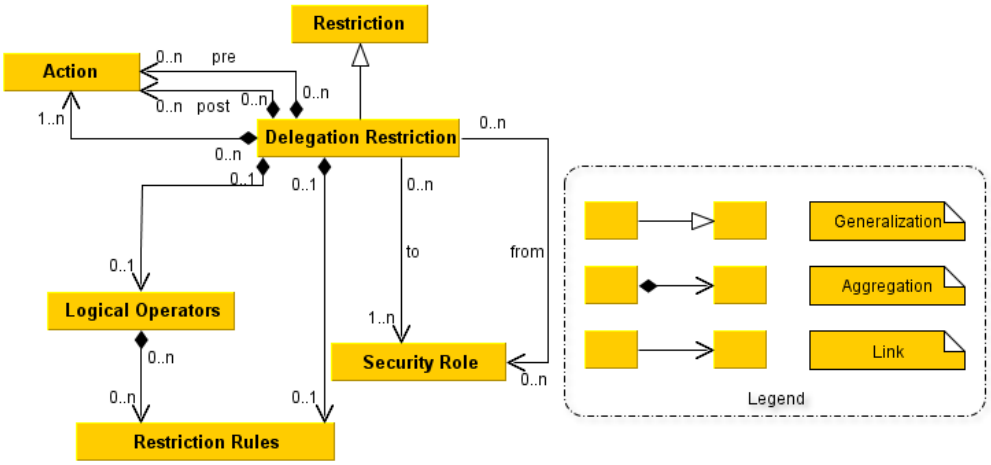

FIGURE 23: DELEGATION RESTRICTION

The delegation restriction construct introduced in Figure 23 allows easy modelling of delegation without using ACECA (presented in section 1.5.7). Each one is connected to the security roles by two links: from and to. They represent the **FROM** and **TO** ACECA keywords that were previously introduced to deal with sub-delegation (FROM) and the roles that will receive the delegation (TO). A delegation restriction may contain one restriction rule or an expression composed of logical operators and restriction rules. As in the access restrictions, the delegation restrictions may have some pre and post actions linked to them, and the actions that will be performed on the ON block are also linked.

This construct is equivalent to the following ACECA code:

PRE

pre-actions

ERP

ON *delegated* **FROM** *role* **TO** *role*

IF *expression* **THEN**

actions

FI

NO

POST

post-actions

TSOP

This restriction is triggered when the *delegated* security event is issued and states the roles that are linked to it by using the **FROM** and **TO** links after the respective keywords. The **IF** expression is constructed using the linked restriction rule or logical operators. The actions that will be executed in the various blocks (the *pre-actions* in the **PRE** block, the *post-actions* in the **POST** block and the *actions* in the **ON** block) will be the previously introduced linked actions.

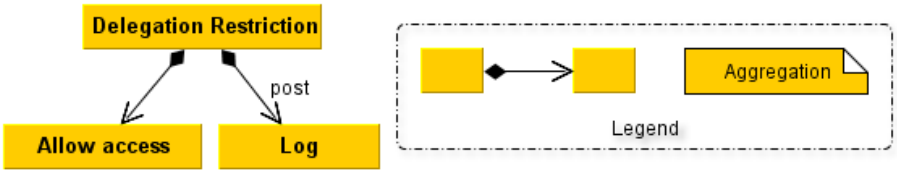

FIGURE 24: DELEGATION RESTRICTIONS DEFAULT ACTIONS

The delegation restriction actions shown in Figure 24, are the default actions for all delegation restrictions in this document when no other actions are shown.

1.5.9 EXAMPLE OF USAGE

With ACECA the user may model in detail how a certain restriction is built and what conditions compose it. The several different language blocks introduced in this section, allow for complex restriction construction. For example, if the user wants to restrict all access to a certain element when a certain security event is triggered, he can construct an ON block with that event and a DENY action on its body. Since the ACECA language is very flexible and expandable any number of examples of increasing complexity may be given with its core elements and future extensions to it. A more complex example of usage is using the ACECA language to define that when a certain security role delegation happens some of its permissions may only be available in certain contexts, or the delegated user must belong to a certain organization to access some specific permissions.

2 SUMMARY

The relationship between the artefacts introduced in this chapter and the research questions introduced in Chapter I section 1 will be presented in Table 4.

	Q1	Q1	Q3	Q4
Organization	R	R	R	
Security Role	R	R	R	
Permission	R	R	R	
Security Event	R	R	R	
Restriction	R	R	R	
Context	R	R	R	
Security Requirement			R	
Auditability Requirement				R
Restriction Log Artefact				R

TABLE 4: META-MODEL ARTEFACTS RESEARCH QUESTIONS REALIZATION (LEGEND: R – REALIZE)

As can be seen from Table 4 the artefacts introduced in this meta-model answer all the research questions proposed in Chapter I section 1. All the artefacts introduced in sections 1.1 and 1.2 (Organization, Security Role, Permission, Security Event, Restriction and Context) answer questions Q1 and Q2 because they introduce represent access control model of this thesis. Additionally they answer question Q3 because they interact with other business process layer elements to provide access control in the business process layer of the enterprise architecture.

The artefacts introduced in section 1.3 (Security Requirement, Auditability Requirement and Restriction Log Artefact) were specifically designed to answer questions Q3 and Q4. With the security requirement artefact in conjunction with the artefacts in sections 1.1 and 1.2 we can answer question Q3 completely, because with this artefact we can connect the business rules with access control. The auditability requirement and the restriction log artefact, allow answering question Q4 completely because, besides connecting with the business rules layer (Auditability Requirement), we provide an artefact that allows for architectural logging of the access control model actions (Restriction Log Artefact).

Chapter IV
Integration and Scenarios

This chapter will show an example of integration of the meta-model introduced in Chapter III section 1 with a chosen enterprise architecture framework (ArchiMate) and a business process modelling language (BPMN). This integration is just an example of how this can be made and its possibilities.

In the end of this chapter a set of scenarios are going to be presented to show how this integration can be used. They will not be exhaustive, as there are many other possible scenarios, but we will try to show the usefulness of this meta-model and some concepts presented on it.

1 ARCHIMATE

1.1 INTEGRATION

ArchiMate (Group, 2009a), as it was introduced in Chapter II section 2.2, is a language for modelling enterprise architectures that has a simple enterprise architecture framework associated with it. Since ArchiMate can be used with TOGAF ADM, the example integration of the previously introduced meta-model (see Chapter III section 1) with ArchiMate can also be used with TOGAF ADM. This integration will be explained in this chapter.

1.1.1 ARCHIMATE BUSINESS LAYER META-MODEL

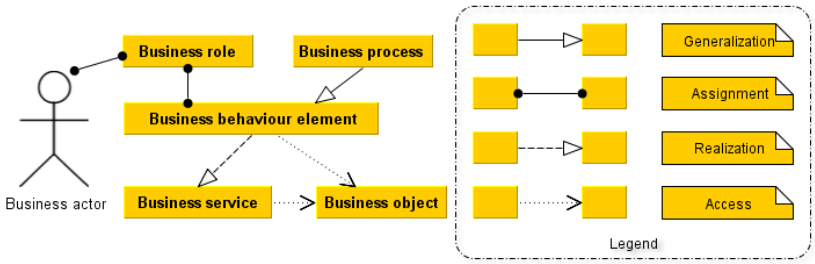

FIGURE 25: ARCHIMATE BUSINESS LAYER META-MODEL (NOT COMPLETE, TAKEN FROM (GROUP, 2009A))

In Figure 25 the ArchiMate Business Layer meta-model (Group, 2009a) is partially represented.

1.1.1.1 ARCHIMATE MOTIVATION EXTENSION

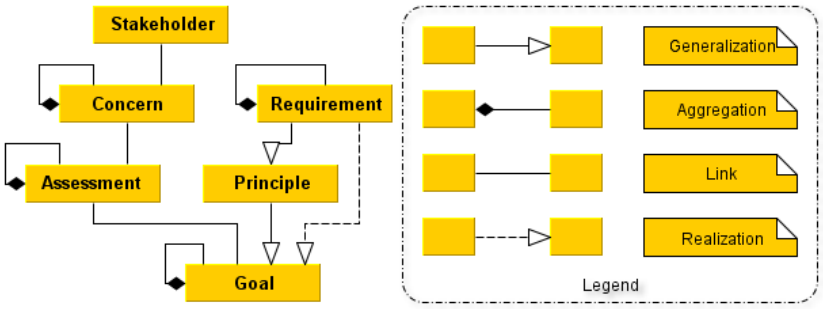

FIGURE 26: ARCHIMATE MOTIVATION EXTENSION (BASED ON (DICK QUARTEL, 2010))

The Extension for Modelling and Managing Motivation, Principles and Requirements in TOGAF (Dick Quartel, 2010) (Figure 26), from now on just referred as ArchiMate Motivation Extension (AME), is used to model some extra business layer concepts that were not available in the core ArchiMate model.

In Figure 27 the connection between the AME meta-model and the core ArchiMate business layer meta-model is shown (the ArchiMate meta-model is not complete, the only elements shown are those that are relevant to this dissertation (Figure 25)).

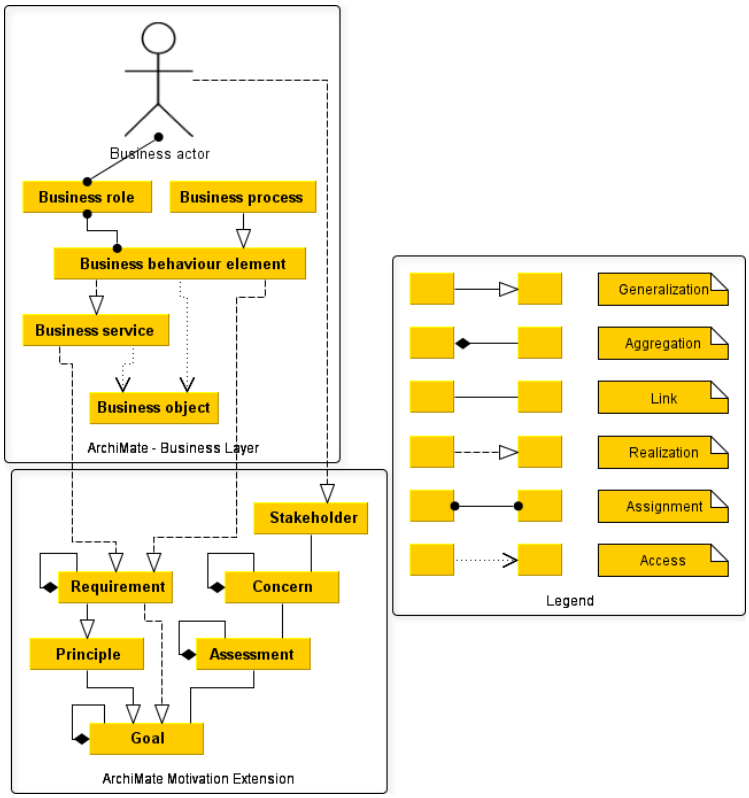

FIGURE 27: INTEGRATION OF ARCHIMATE MOTIVATION EXTENSION WITH THE ARCHIMATE BUSINESS LAYER META-MODEL (BASED ON (GROUP, 2012))

1.1.2 EXAMPLE INTEGRATION

In this section it is shown an example of integration between the ArchiMate and AME meta-models with the meta-model proposed in this thesis (see Chapter III section 1).

1.1.2.1 PERMISSIONS

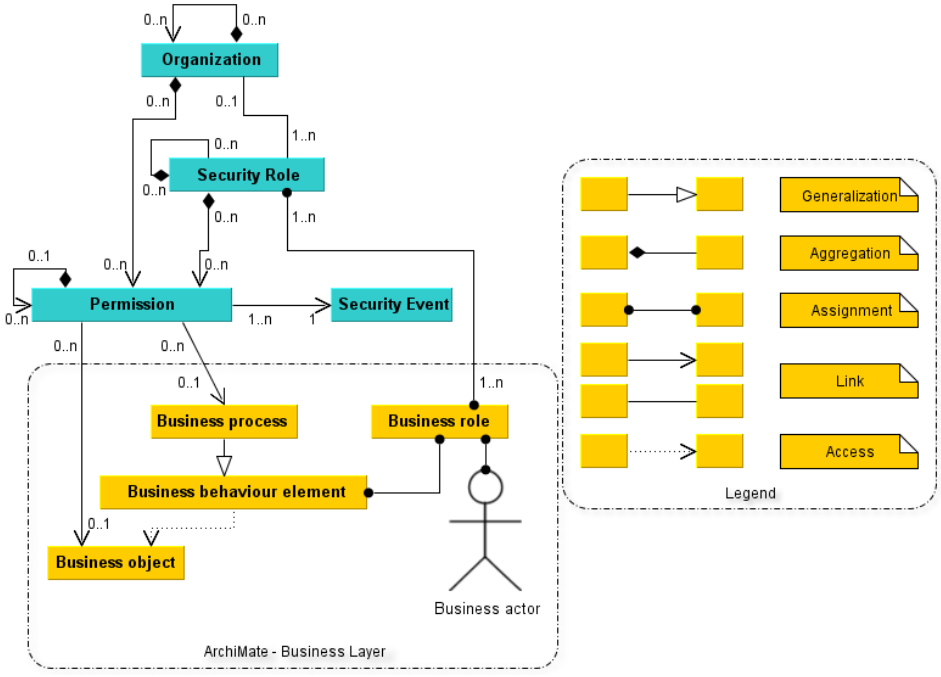

FIGURE 28: INTEGRATION OF THE PERMISSIONS META-MODEL WITH ARCHIMATE

The permissions meta-model concepts (Chapter III section 1.1) are integrated with the ArchiMate meta-model in the following manner (Figure 28):

- The Security role must be assigned with one or more Business roles, and the business roles may be associated with multiple security roles.
- The permissions are associated with only one business process element or only one Business object, although these objects may have associated with them several different permissions.

1.1.2.2 RESTRICTIONS

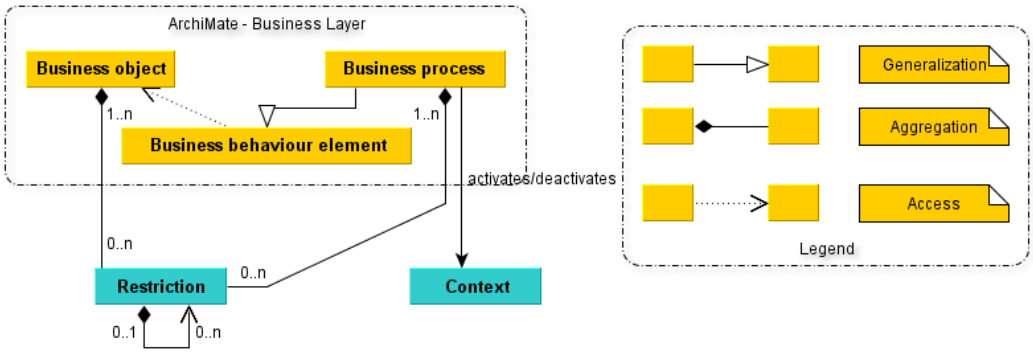

FIGURE 29: INTEGRATION OF THE RESTRICTIONS META-MODEL WITH ARCHIMATE

The concepts that represent restrictions (Chapter III section 1.2) integrate with ArchiMate in the following manner (Figure 29):

- The contexts may be activated or deactivated by the business processes.
- The Business objects and the Business process elements may contain several restrictions.

The extended ACECA constructions presented in Chapter III section 1.5.8.1, can be integrated with ArchiMate as shown in Figure 30:

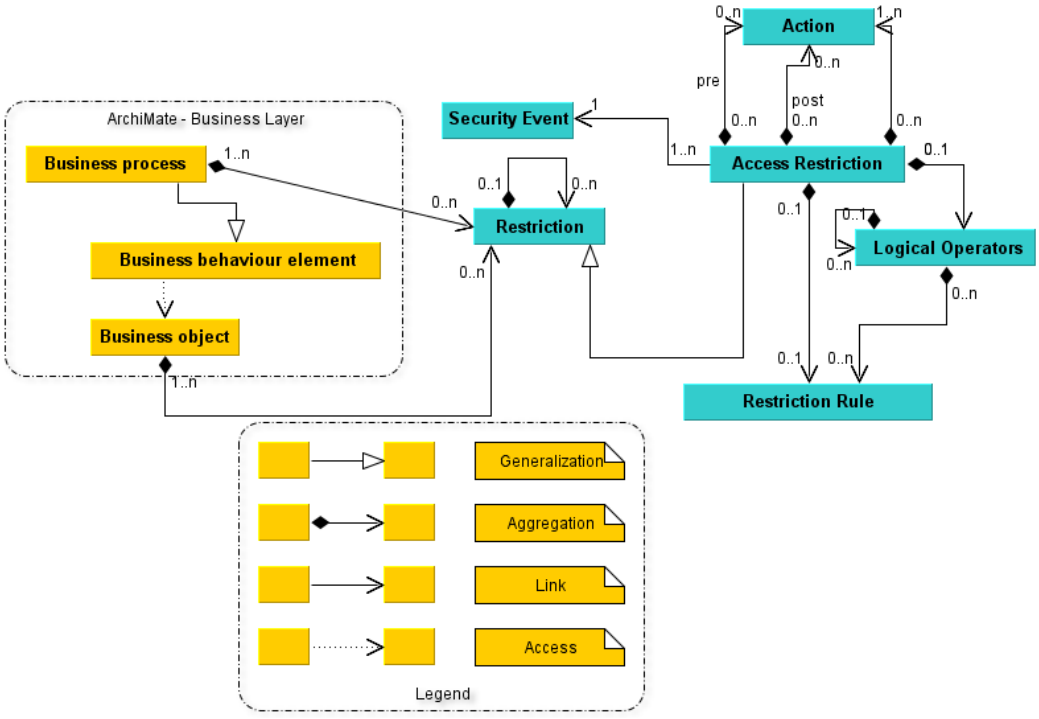

FIGURE 30: ACECA COMMON ACCESS RESTRICTIONS INTEGRATION WITH ARCHIMATE

The delegation restrictions (presented in Chapter III section 1.5.8.2.2) can be integrated with ArchiMate in the following manner (Figure 31):

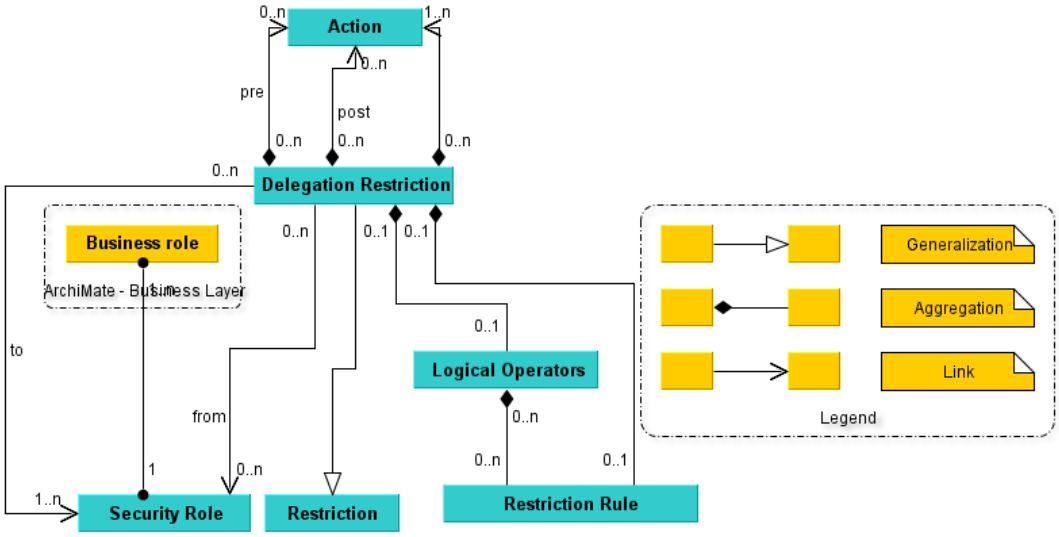

FIGURE 31: ACECA COMMON DELEGATION RESTRICTIONS INTEGRATION WITH ARCHIMATE

1.1.2.3 BUSINESS RULES

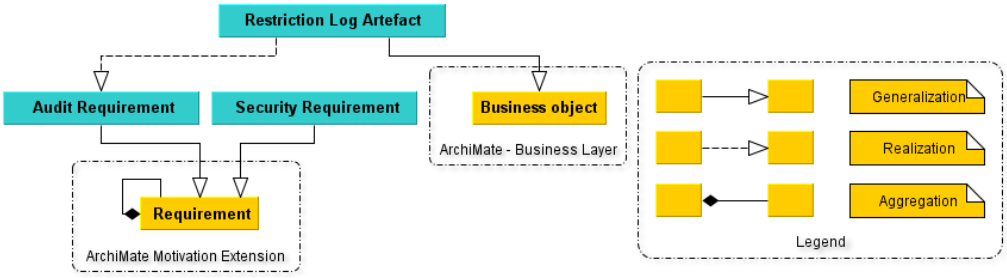

FIGURE 32: INTEGRATION OF THE BUSINESS RULES META-MODEL WITH ARCHIMATE

The business rules concepts (Chapter III section 1.3) are integrated with ArchiMate in the following manner (Figure 32):

- The Audit and Security requirements are a specialization of the Requirement concept of the AME meta-model.
- The Restriction Log Artefact (RLA) (Chapter III section 1.3.2.1) is a specialization of the Business Object concept. This allows associating with RLA permissions or new access restrictions (Sections 1.1.2.1 and 1.1.2.2).

1.1.2.4 FORMALIZATION

In this section the additional elements that will be added to the formalization presented in Chapter III section 1.4, will be explained.

EQUATION 64: ARCHIMATE BUSINESS ELEMENTS

Equation 64 introduces the ArchiMate business elements that will be used in this formalization, these are: the business processes (BP) and the business objects (BO). Besides this set, there are two additional sets (Equation 65 and Equation 66), that represent all the business objects (ABO) and all the business processes (ABP). The ABE (Equation 67) set represents the union of the two previously presented sets.

EQUATION 65: ABO SET

EQUATION 66: ABP SET

EQUATION 67: ABE SET

EQUATION 68: ABR SET

The ABR set (Equation 68) represents all ArchiMate business roles (BR).

1.1.2.4.1 PERMISSIONS

EQUATION 69: PBE SET (PARTIALLY ORDERED)

The PBE set (Equation 69) is a partially ordered set that contains the business element that a specific permission refers to. The present condition specifies that all permissions must have a business element associated with them.

1.1.2.4.2 SECURITY ROLES

EQUATION 70: ASSIGNMENT OF ARCHIMATE SECURITY ROLES TO ARCHIMATE BUSINESS ROLES

Equation 70 introduces a many to many set called SRBR that has all the assignments of ArchiMate business roles to the security roles.

1.1.2.4.3 RESTRICTIONS

EQUATION 71: RBE SET (PARTIALLY ORDERED)

The RBE set (Equation 71) is a partially ordered set that contains the assignment of restrictions to specific business elements.

1.1.3 VIEWPOINTS

This thesis advises on the creation of several viewpoints (Lankhorst, 2009) that will be described according to the IEEE 1471 Standard (Society, 2000). These viewpoints can be classified according to whether they model the enterprise architecture structure (Passive and Active) or behaviour.

The structural viewpoints are:

- 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.

The behavioural viewpoint is:

- 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.

On the remaining of this section these viewpoints will be described in detail, according to the elements defined in the (Society, 2000), these are:

- Viewpoint name
- List of the stakeholders interested in it
- Concerns that it is trying to answer
- How to model it

1.1.3.1 SECURITY ROLES VIEWPOINT (SRV)

Stakeholders:	Security Architect
Concerns:	• Model the organization and security role structure (hierarchy). • Assign security roles to business roles. • Link organizations with security roles. • Assign permissions to security roles and organizations. • Model the permission structure (hierarchy). • Specify which requirements (security and audit) are realized by the elements present in this viewpoint. • Specify the security role delegation.
How to model:	To construct this viewpoint the security architect must construct the security roles and organizations hierarchy that he wants and then assign the permissions to those roles or organizations. These security roles must also be associated with existing business roles to integrate the access model with the rest of the enterprise architecture. This viewpoint must also contain the permission hierarchy, the various elements connection to the security rules realized by them and also specify, if applicable, the delegation restrictions. The elements that can be used in this viewpoint are: • From the permission meta-model (see section 1.1.2.1): Organization, Permission, Security Role, Security Event and Business Role. • From the restrictions (see section 1.1.2.2): Delegation Restriction. • From the business rules (see section 1.1.2.3): Security Requirement.

1.1.3.2 BUSINESS OBJECTS PERMISSIONS AND RESTRICTIONS VIEWPOINT (BOPRV)

Stakeholders:	Security Architect
Concerns:	• Specify the restrictions that are applicable to a business object. • Specify the restriction structure of those introduced in this viewpoint. • Specify the permissions and the contexts needed to perform a specific restricted operation on a business object. • Specify which requirements (security and audit) are realized by the elements present in this viewpoint. • Specify the log artefacts generated by each restriction (if required).
How to model:	In this viewpoint the security architect must connect the applicable restrictions to each business object and also design those restrictions including their structure, the permissions needed to access those elements, the contexts that need to be activated, the log artefacts generated and the security and audit requirements realized by them. The elements that should be used in this viewpoint are: • From the permission meta-model (see section 1.1.2.1): Permission and Security Event. • From the restrictions (see section 1.1.2.2): Business Object, Restriction and Access Restriction. • From the business rules (see section 1.1.2.3): Security Requirement, Audit Requirement and Restriction Log Artefact.

1.1.3.3 SECURITY AND AUDIT REQUIREMENTS VIEWPOINT (SARV)

Stakeholders:	Security Architect
Concerns:	• Model the security and audit requirements hierarchy.
How to model:	This viewpoint is used by the security architect to specify the hierarchy of the security and audit requirements used in other viewpoints. The elements that should be used are the Security Requirement and Audit Requirement (see section 1.1.2.3).

1.1.3.4 BUSINESS PROCESSES PERMISSIONS AND RESTRICTIONS VIEWPOINT (BPPRV)

Stakeholders:	Security Architect
Concerns:	• Specify the restrictions that are applicable to a business process and/or its activities. • Specify the restriction structure of those introduced to this viewpoint. • Specify the permissions and the context needed to perform a specific restricted operation on a business process. • Specify which requirements (security and audit) are realized by the elements present to this viewpoint. • Specify when a context is activated and deactivated.
How to model:	Since this viewpoint is very similar to the BOPRV, the instructions to model it are equivalent, but instead of using business objects, business processes are used. One additional concern that this viewpoint and that the security architect must specify is when some context is activated and deactivated. The elements used in this viewpoint are the same as the BOPRV, but instead of using a Business Object (from the restrictions in section 1.1.2.2), a Business Process is used (from the same section).

1.2 EXAMPLES

To demonstrate the integration presented to the previous section, some examples are going to be introduced. In all the diagrams that are presented, the yellow elements will be core ArchiMate elements, and the blue ones will be elements proposed on this thesis.

1.2.1 SECURITY ROLES VIEWPOINT (SRV)

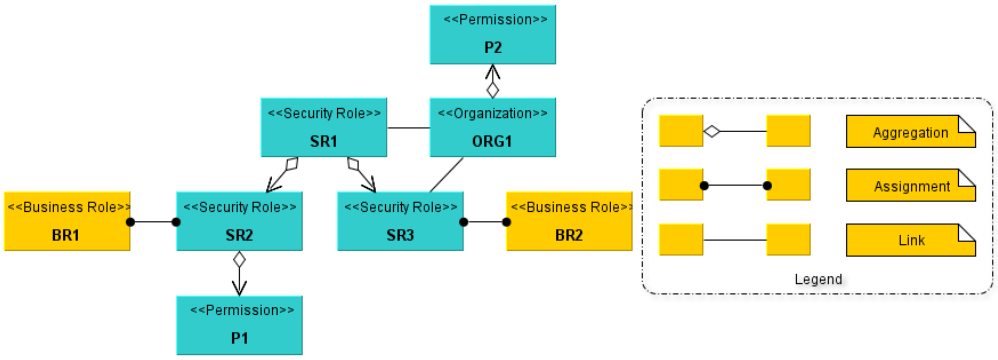

FIGURE 33: EXAMPLE ARCHIMATE SRV (SECTION 1.1.3.1)

In this example (Figure 33), there are two business roles (BR1 and BR2) that are associated with two different security roles (SR2 and SR3, respectively). These two security roles belong to a hierarchy where they have a common parent security role (SR1), which will aggregate all permissions that they have. There is a permission associated directly with a security role (P1) and one (P2) that is associated with an organization (ORG1), where all security roles that belong to it (SR1 and SR3) will also have it.

1.2.2 Business Objects Permissions and Restrictions Viewpoint (BOPRV)

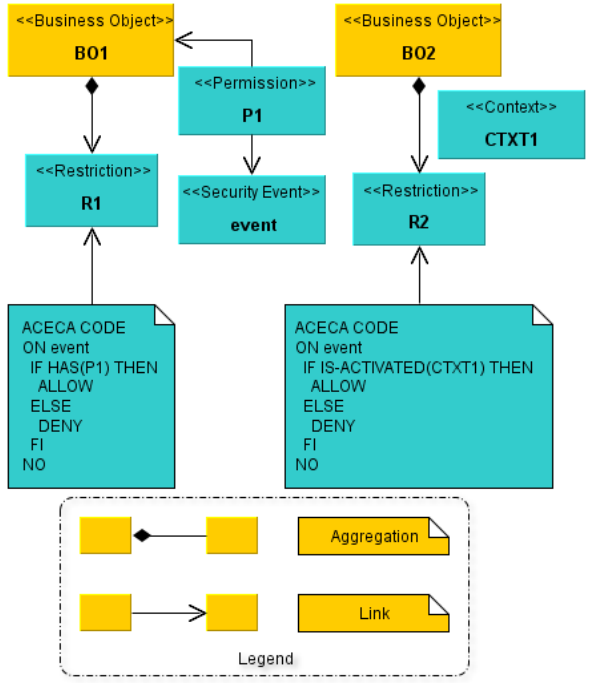

Figure 34: Example ArchiMate BOPRV (Section 1.1.3.2)

In this example there are two ArchiMate Business Objects (BO1 and BO2) that have restrictions associated with them (R1 and R2, respectively). The ACECA code of those restrictions, which allows access only to the role that have the necessary permissions (P1 on R1) or if a specific context is activated (CTXT1 on R2), is displayed in the notes linked to them. The security event that triggers both of these restrictions is also displayed (event).

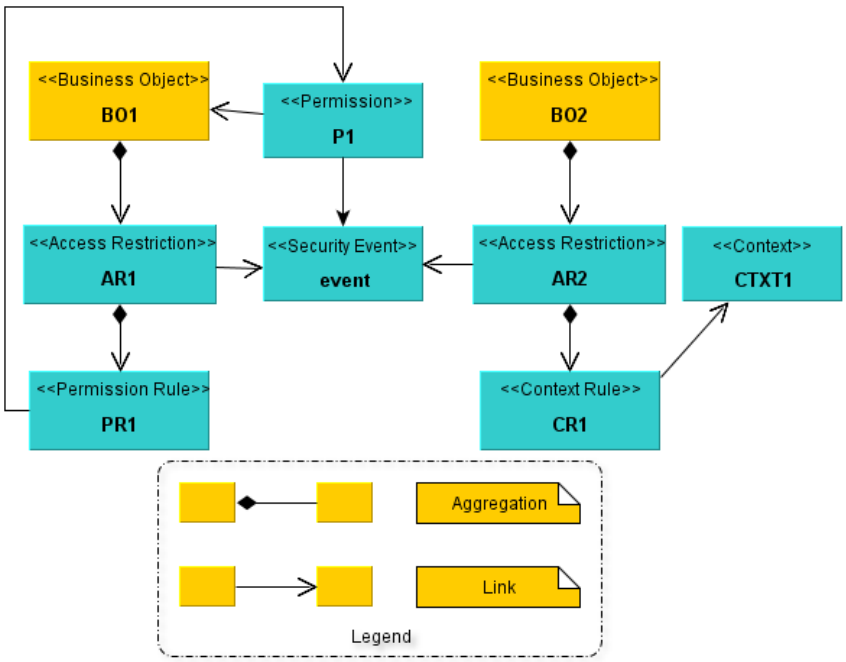

Figure 35: Example ArchiMate BOPVR using the extended common ACECA constructions presented on Chapter III section 1.5.8.2.1

The example introduced in Figure 34 may be simplified by using the extended ACECA access restrictions which were introduced in section 1.1.2.2, as shown in Figure 35.

1.2.3 Business Process Permissions and Restrictions Viewpoint (BPPRV)

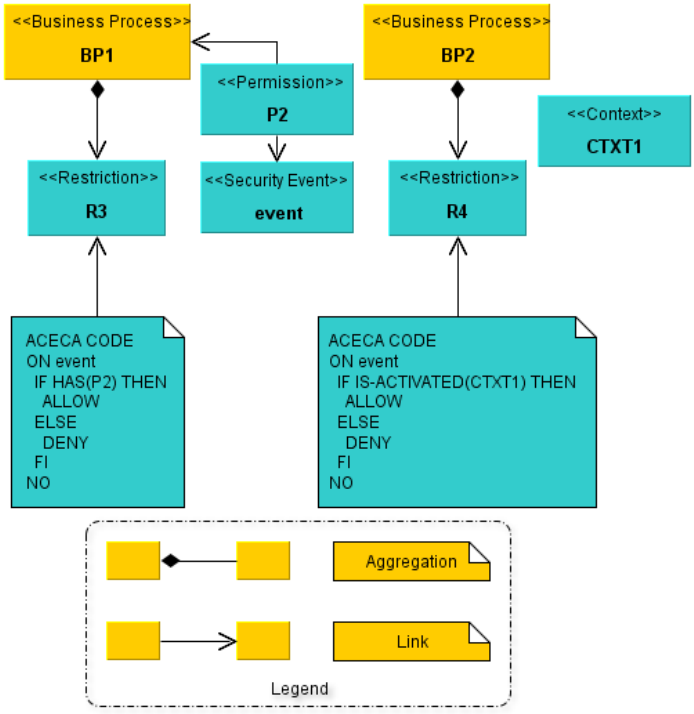

Figure 36: Example ArchiMate BPPRV (section 1.1.3.4)

In this figure an example BPPRV is shown, where two ArchiMate Business Processes (BP1 and BP2) have restrictions associated with them (R3 and R4, respectively) that are triggered by a specific security event (event). In the linked notes the ACECA code needed to restrict access to users that have a certain permission (P2 on R3) or if a certain context is activated (CTXT1 on R4) is shown.

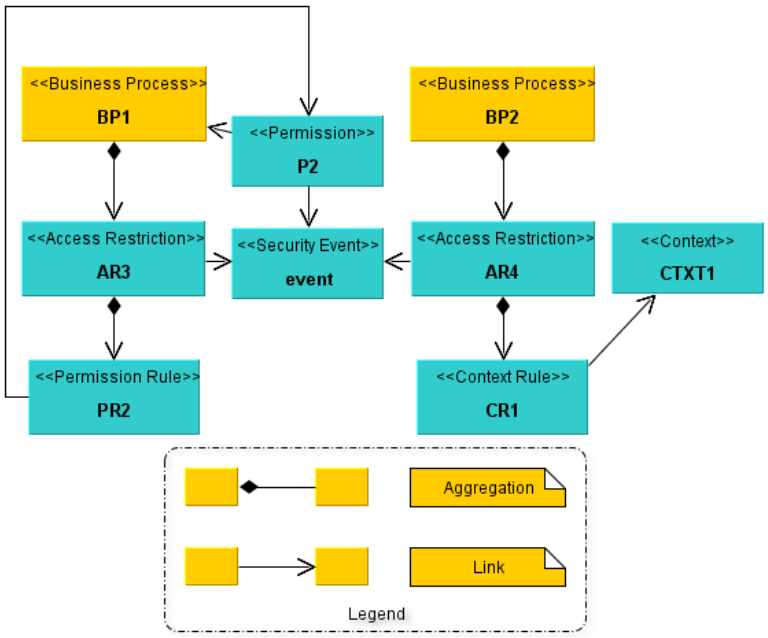

Figure 37: Example ArchiMate BPPVR using the extended common ACECA constructions presented on Chapter III section 1.5.8.2.1

The example that was previously introduced (in Figure 36) can be further simplified when the extended ACECA access restrictions introduced in section 1.1.2.2 are used, as shown in Figure 37.

1.2.4 Security and Audit Requirements Viewpoint (SARV)

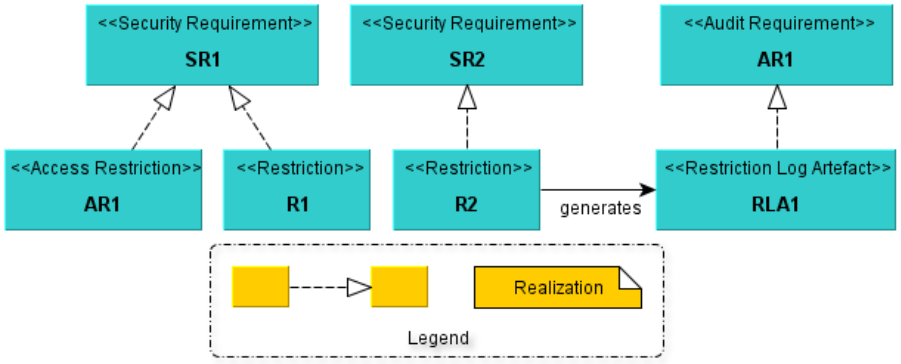

Figure 38: Example ArchiMate SARV (1.1.3.3)

In this example (Figure 38) there are two security requirements (SR1 and SR2) that are realized by several different restrictions (AR1, R1 and R2). The restriction R2 also generates a Restriction log Artefact (RLA1) (Chapter III section 1.3.2.1) that realizes an audit requirement (AR1). The ACECA code needed to generate this RLA is omitted but an example of it may be seen in Chapter III section 1.5.6.

2 BPMN

In this section it is introduced an example of integration of the meta-model which was presented in Chapter III section 1 with the Business Process Model and Notation (BPMN) v2.0 Process Diagram (OMG, 2011) meta-model.

2.1 Integration

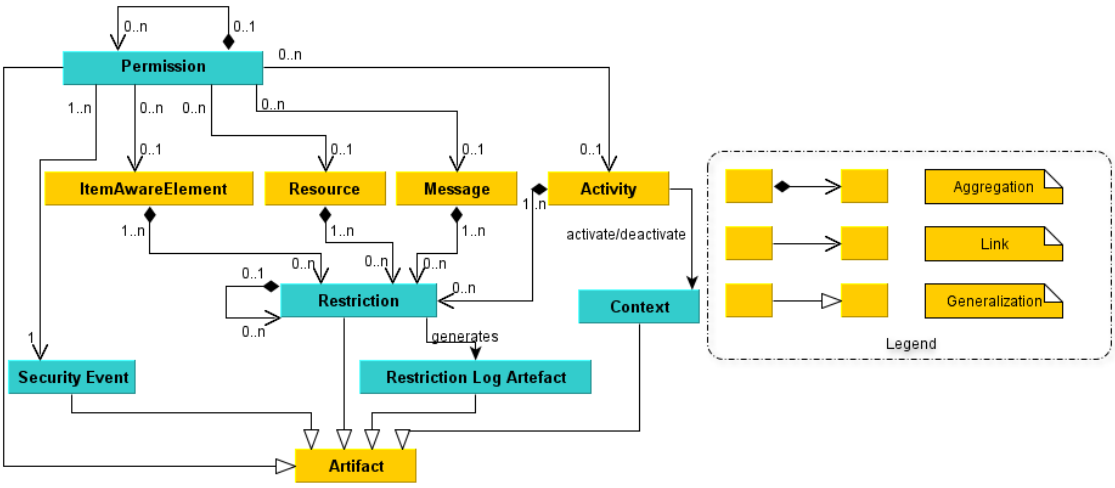

Figure 39: BPMN 2.0 meta-model with some of the security concepts introduced on the proposal (Chapter III section 1) (yellow elements are BPMN Elements, Blue are the new elements proposed)

The integration with BPMN presented in this chapter is not complete. For modelling the complete access control meta-model presented on Chapter III, the user needs to use other modelling languages (like ArchiMate, which has a sample integration presented on Section 1).

2.1.1 Restriction

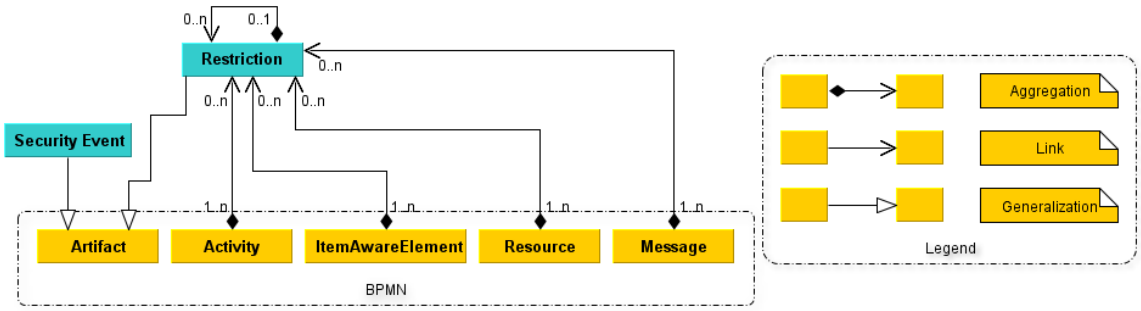

Figure 40: BPMN Meta-model integration with the restrictions meta-model

Figure 40 introduces the integration of the BPMN 2 Process Diagram meta-model with the restriction meta-model (Chapter III section 1.2.2). There are four BPMN elements that may have restrictions associated with them: Activity, ItemAwareElement, Resource and Message.

A restriction is a type of a BPMN artefact and is defined by using the ACECA language (Chapter III section 1.5). The access rules restrictions (Chapter III section 1.5.8.2.1) may be used in BPMN, but to fully represent them and other restrictions aspects fully (like permissions, organizations, etc.) other diagram types must be used (for example ArchiMate, see Section 1 of this chapter).

2.1.2 Restriction Log Artefact

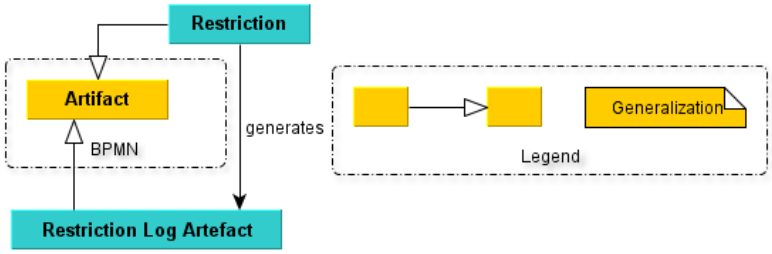

Figure 41: Restriction Log Artefact integrated with BPMN

A Restriction Log Artefact (RLA) (Chapter III section 1.3.2.1) is a type of a BPMN Artefact and is generated by the restrictions.

2.1.3 Context

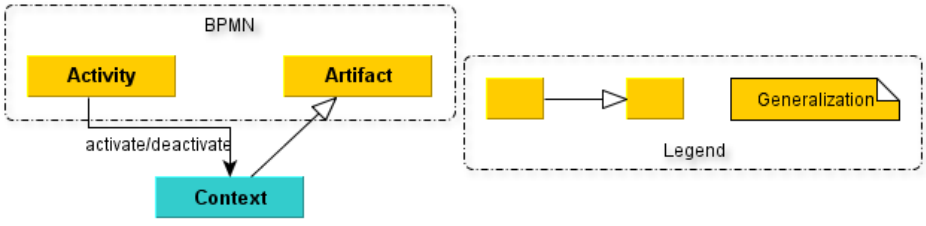

Figure 42: Context integrated with BPMN

The context (Chapter III section 1.2.1) is a type of a BPMN Artefact and is activated and deactivated by the Activity BPMN element.

2.1.4 PERMISSION

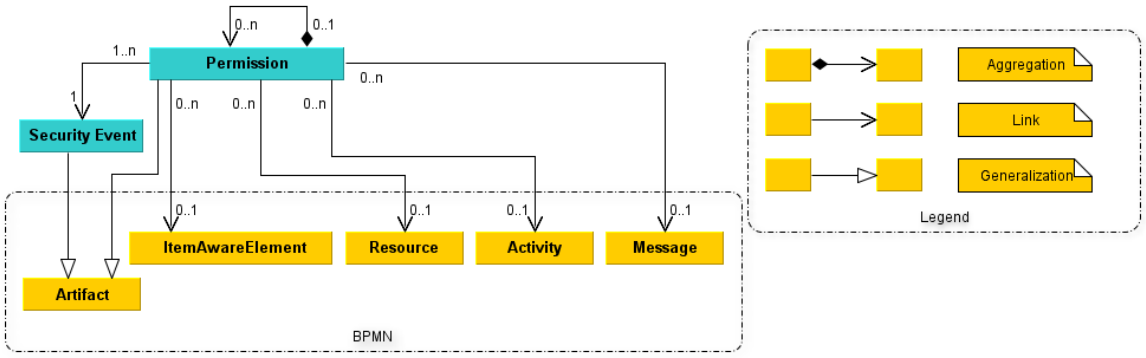

FIGURE 43: PERMISSION INTEGRATED WITH BPMN

The permissions (Chapter III section 1.1.4) are BPMN Artifacts and may be associated with the same elements as the restrictions (see section 2.1.1).

2.1.5 SECURITY EVENT

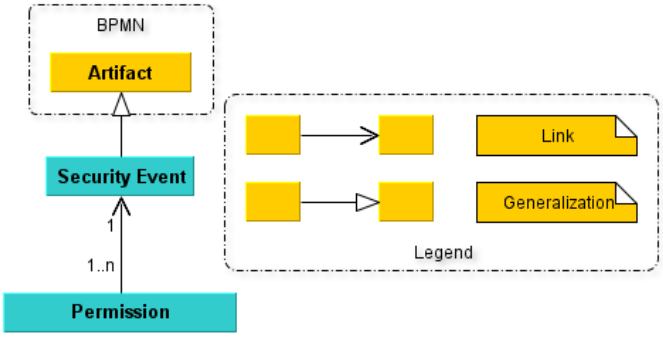

FIGURE 44: SECURITY EVENT INTEGRATED WITH BPMN

The security event (Chapter III section 1.1.3) is a type of a BPMN Artefact and is used in permissions to define which event they refer to.

2.1.6 FORMALIZATION

As in section 1.1.2.4 it will be now presented additional formal elements to the already presented elements in Chapter III1.4.

EQUATION 72: BPMN BUSINESS ELEMENTS

This formalization is similar to the one presented for ArchiMate (see 1.1.2.4). The BE set that was presented, on BPMN has different elements: the ItemAwareElement (IAE), Resource (RSRC), Activity (ACT) and Message (MSG).

EQUATION 73: AIAE SET

EQUATION 74: ARSRC SET

EQUATION 75: AACT SET

EQUATION 76: AMSG SET

There are also sets that represent all elements of a certain type:

- AIAE (Equation 73) – all ItemAwareElements (IAE).
- ARSRC (Equation 74) – all resources (RSRC).
- AACT (Equation 75) – all activities (ACT).
- AMSG (Equation 76) – all messages (MSG).

The rest of this formalization is equal to the ArchiMate one, although the presented security roles formalization is not applicable to BPMN (since that element is not integrated with BPMN)..

2.1.7 Viewpoints

Two of the viewpoints, Business Objects Permissions and Restrictions Viewpoint (BOPRV) (Section 1.1.3.2) and Business Processes Permissions and Restrictions Viewpoint (BPPRV) (Section 1.1.3.4), described in the ArchiMate integration can also be used in the BPMN integration. The BOPRV can be used with the following BPMN elements: ItemAwareElement, Resource and Message, while the BPPRV is used with the Activity element.

2.2 Examples

In this section some examples of the BPMN integration proposed in the previous section are going to be introduced. The yellow elements will be core BPMN elements and the blue elements will be the proposed extension.

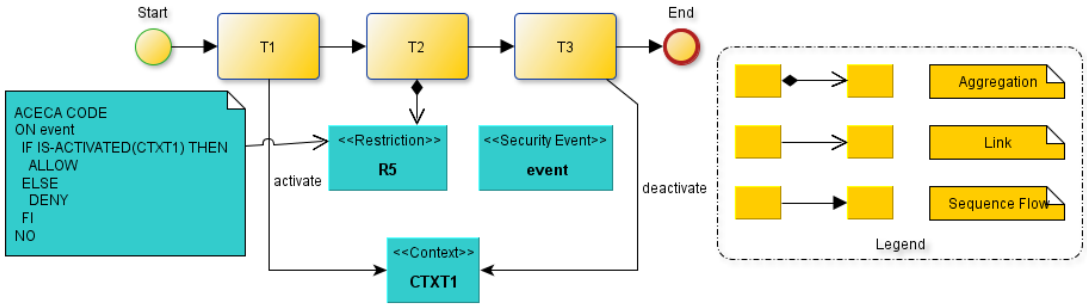

Figure 45: BPMN example

In this example (Figure 45), there are three Tasks (T1, T2 and T3) and one of them has a restriction (R5 on T2) that is triggered by the security event (event). The ACECA code of this restriction (shown in the linked note) requires that a specific context is active (CTXT1) to allow access. This context was activated on T1 and will be deactivated on T3.

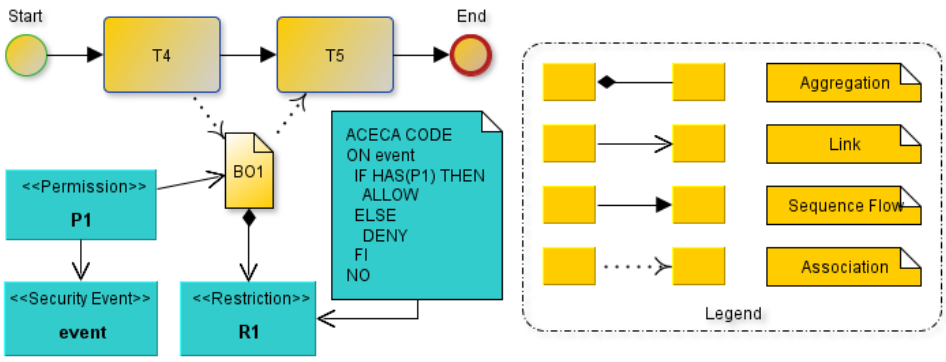

Figure 46: BPMN Example with some ArchiMate Elements

This example (Figure 46) shows how some external elements (from the ArchiMate proposed extension described in Section 1.1) can be integrated with a BPMN diagram to model some specific restrictions. The tasks T4 and T5 use some specific Business Object (BO1) (since this is a BPMN diagram, that object is modelled as a BPMN Data Object) that was introduced in the example regarding the BOPRV (see Section 1.2.2) as well as the restriction, security event and permission associated with it.

3 SCENARIOS

In this section some example scenarios that use both the ArchiMate and BPMN integrations presented in the previous sections (Sections 1 and 2) are going to be introduced. When useful the common ACECA constructions presented in Chapter III section 1.5.8 will be used instead of using the equivalent ACECA code.

The structure of this chapter will be the same for all scenarios, first the audit and security requirements will be presented along the original business processes and other relevant models. After that, it is presented the proposed solution using the concepts that were previously introduced.

3.1 SIMPLE SCENARIO

3.1.1 ORIGINAL DIAGRAMS AND SECURITY REQUIREMENTS

The following ArchiMate diagram (Figure 47) models the business roles structure and its assignment to specific business actors.

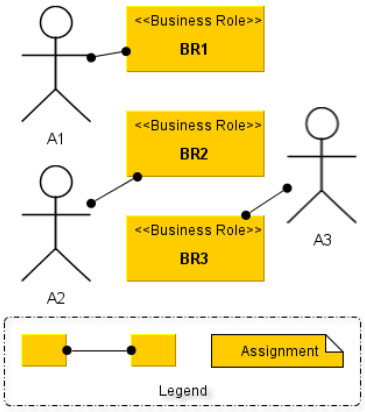

FIGURE 47: EASY SCENARIO BUSINESS ROLE ACTOR ASSIGNMENT

The next two diagrams describe in detail the two business processes present in this scenario (BP1 and BP2) and using the BPMN language

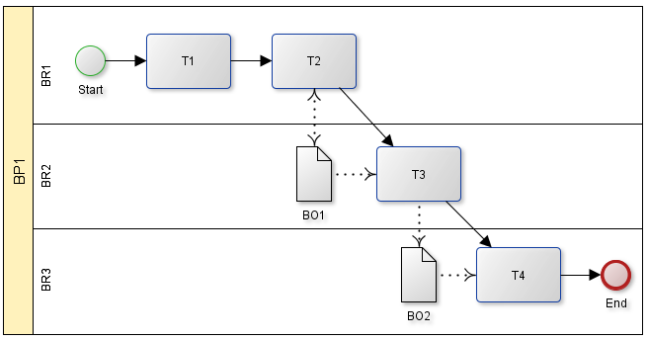

FIGURE 48: BUSINESS PROCESS BP1 (DETAIL MODELLED WITH BPMN)

Figure 48 shows in detail which tasks are performed by each Business Role (T1 and T2 by BR1, T3 by BR2 and T4 by BR3), and where the Business Objects (BO1 accessed in T2 and T3 and modified in T2. BO2 is modified in T3 and accessed in T4) are used.

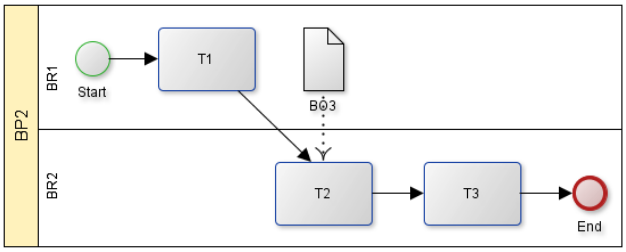

FIGURE 49: BUSINESS PROCESS BP2 (DETAIL MODELLED WITH BPMN)

Figure 49 shows the detailed modelling of BP2 as in Figure 48 the tasks each business roles performs (T1 by BR1 and T2 and T3 by BR2) and where the business object (BO3 is accessed on T2) is used is shown.

The security rules that will be applied to these models are:

SReq1) BO1 may be accessed by BR1 and BR2 but may only be modified by BR1. These operations must occur only in a context specific to BP1.

SReq2) BO2 may only be modified in a context specific to BP1 by BR2 and may be accessed by BR3 and BR2 (even if not in the BP1 context).

SReq3) BO3 may only be accessed in a context specific to BP2 and only by BR2.

SReq4) The following BP1 tasks can only be executed in a context specific to this business process and by these specific roles: T2 by BR1 and T3 by BR2. This context must be activated by T1 and deactivated by T4.

SReq5) BP2 T2 Task may only be executed by BR2 in a context specific to BP2 that is activated in T1 and deactivated in T3.

These security rules may be further decomposed:

SReq1) BO1 may be accessed by BR1 and BR2 but may only be modified by BR1. These operations must occur only in a context specific to BP1.

SReq1.1) BO1 may be accessed by BR1 and BR2.

SReq1.2) BO1 may be modified by BR1.

SReq1.3) Any operation on BO1 must occur in a context specific to BP1.

SReq2) BO2 may only be modified in a context specific to BP1 by BR2 and may be accessed by BR3 and BR2 (even if not in the BP1 context).

SReq2.1) BO2 may be accessed by BR2 and BR3.

SReq2.2) BO2 may only be modified by BR2 in a context specific to BP1.

SReq3) BO3 may only be accessed in a context specific to BP2 and only by BR2.

SReq4) The following BP1 tasks can only be executed in a context specific to this business process and by these specific roles: T2 by BR1 and T3 by BR2. This context must be activated by T1 and deactivated by T4.

SReq4.1) The BP1 specific context must be activated by T1 and deactivated by T4.

SReq4.2) The BP1 tasks T2 and T3 must only be executed in a context specific to BP1.

SReq4.3) The BP1 task T2 may only be executed by BR1.

SReq4.4) The BP1 task T3 may only be executed by BR2.

SReq5) BP2 T2 Task may only be executed by BR2 in a context specific to BP2 that is activated in T1 and deactivated in T3.

SReq5.1) The BP2 task T2 must only be executed in a context specific to BP2.

SReq5.2) The BP2 specific context is activated in BP2 T1 and deactivated in BP2 T3.

3.1.2 PROPOSED SOLUTION

3.1.2.1 SARV

The following SARV (Chapter IV section 1.1.3.3) is created with these rules:

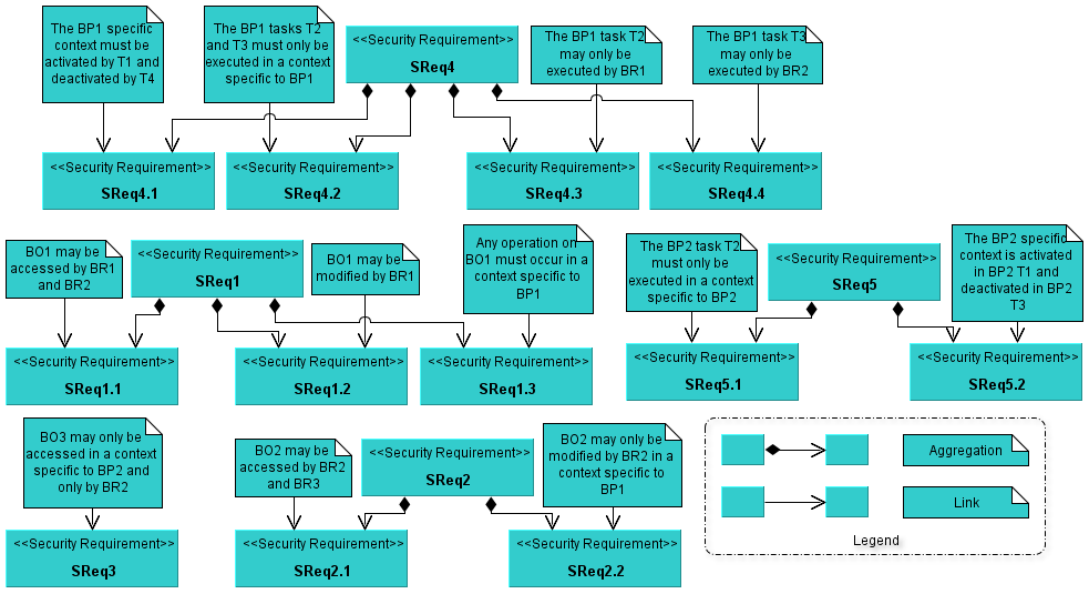

FIGURE 50: EASY SCENARION SARV (CHAPTER IV SECTION 1.1.3.3)

3.1.2.2 SRV

The following diagram (Figure 51) shows the SRV (Chapter IV section 1.1.3.1) for this scenario. The permissions shown will be explained in detail in other diagrams. The rationale for creating a security role in this diagram was simply to minimize the number of security roles present:

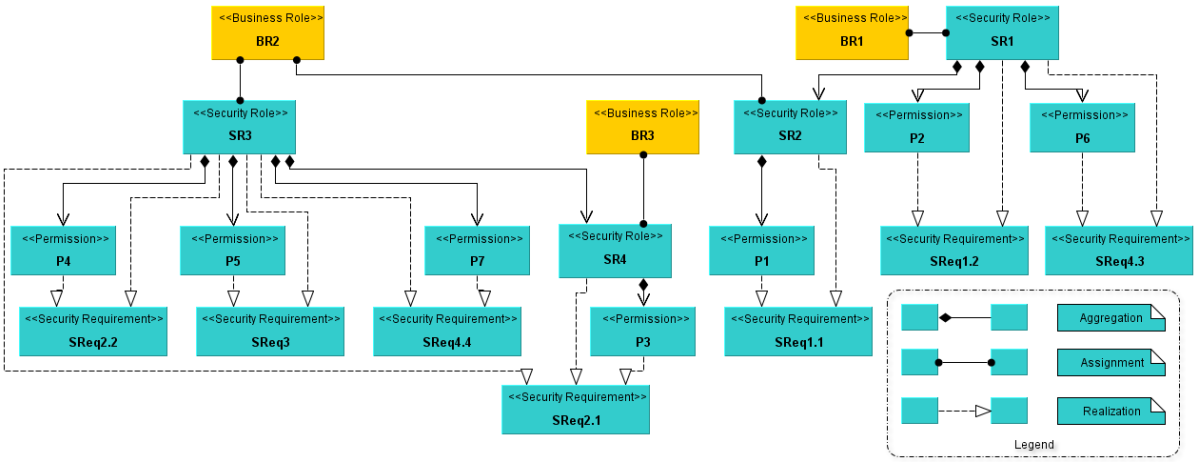

FIGURE 51: EASY SCENARIO SRV (CHAPTER IV SECTION 1.1.3.1)

3.1.2.3 BOPRV

The next diagrams show the BOPRV (Chapter IV section 1.1.3.2) for each business object in this scenario.

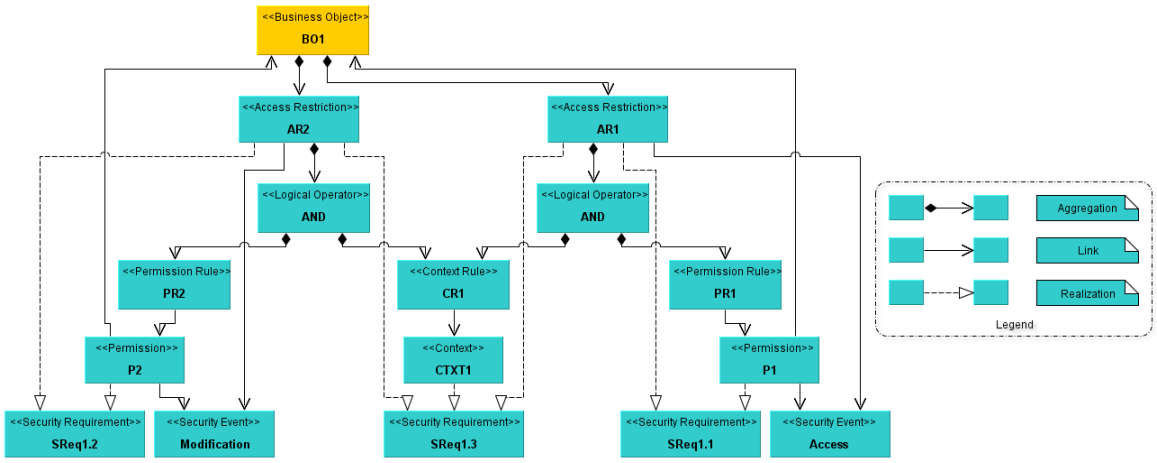

FIGURE 52: EASY SCENARIO BO1 BOPRV (CHAPTER IV SECTION 1.1.3.2)

BO1 has two restrictions applied to it AR1 and AR2, that occur in two distinct security events: Access and Modification, respectively. AR1 only allows access to the element if the CR1 rule (only true if the context CTXT1 is activated) and PR1 rule (only true if the active role accessing the object has the P1 permission) are both true. AR2 only allows modifications to the object if both the CR1 rule (same rule as the AR1) and PR2 rule (only true if the active role accessing the object has the P2 permission) are true.

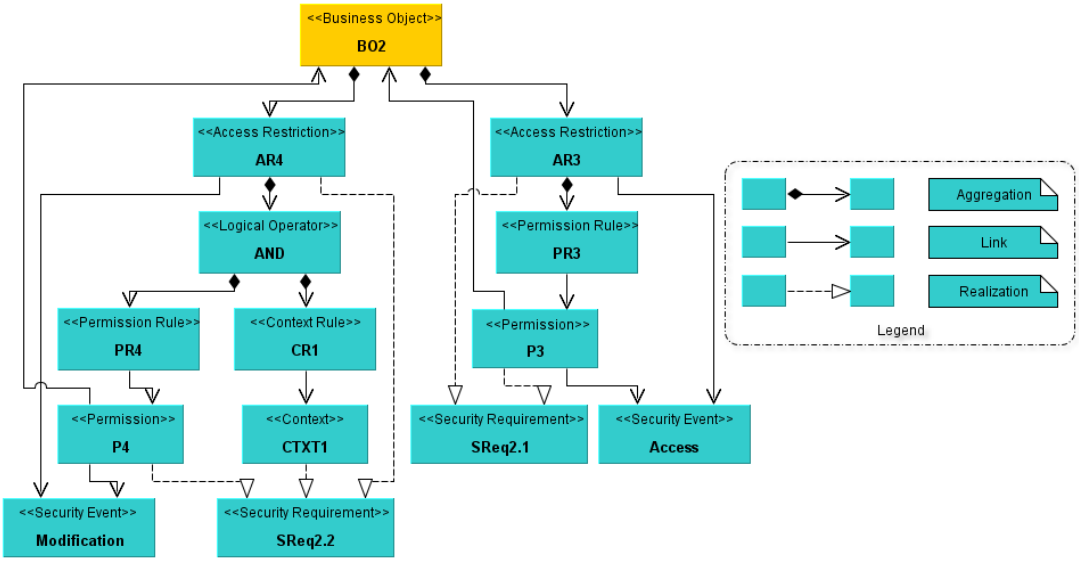

FIGURE 53: EASY SCENARIO BO2 BOPRV (CHAPTER IV SECTION 1.1.3.2)

Has in BO1 (Figure 52), BO2 has two access restrictions applied to it that are similar to those of the BO1. AR4, that is triggered when someone tries to modify the object, is similar to both AR1 and AR2 in the sense that it restricts access if both the permission rule PR4 (only true if the active role has the permission P4) and the context rule CR1 (only true if the context CTXT1 is activated) are true. When someone or something tries to access the object, AR3 comes in effect, only allowing access if the permission rule PR3 (true if the active role has the P3 permission) is true.

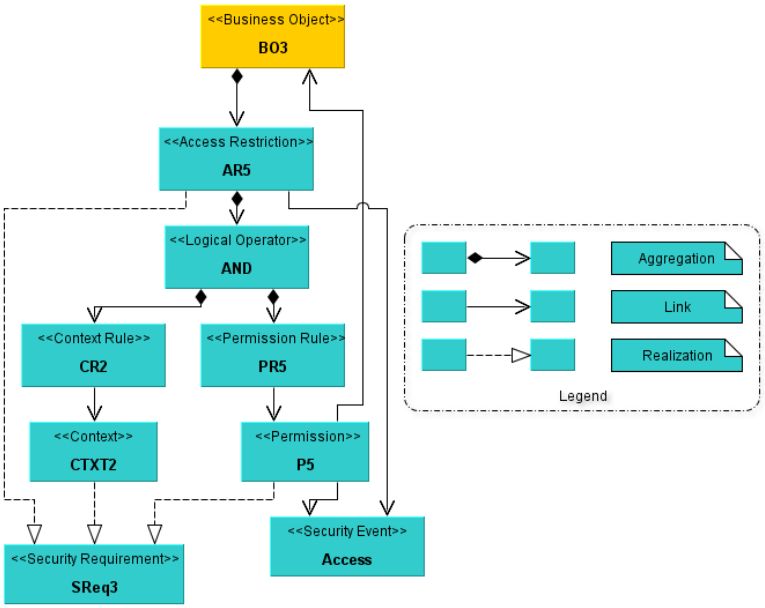

FIGURE 54: EASY SCENARIO BO3 BOPRV (CHAPTER IV SECTION 1.1.3.2)

The access restriction present in Figure 54 (AR5), that is applied when the object is accessed, is equivalent to some access restrictions presented earlier (AR1, AR2 and AR4), that is, only allows access if both the context rule CR2 (true if the context CTXT2 is activated) and the permission rule PR5 (true if the active role has the permission P5) are true.

3.1.2.4 BPPRV

The next diagrams show the BPPRV (Chapter IV section 1.1.3.4) for each relevant task:

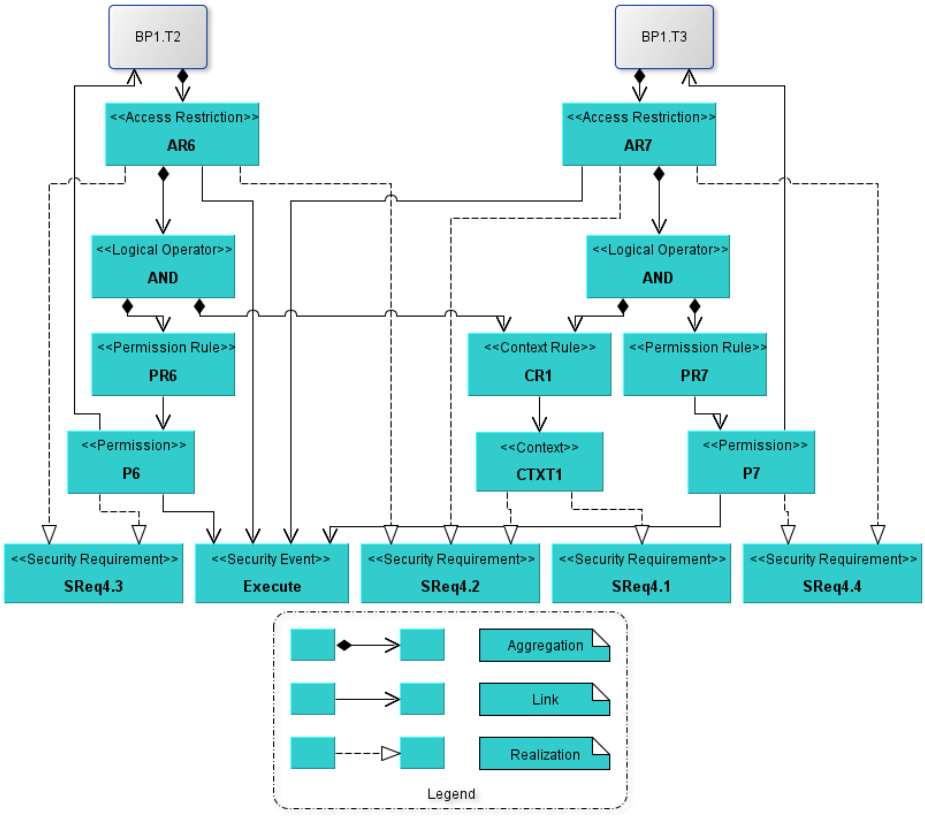

FIGURE 55: BPPRV (CHAPTER IV SECTION 1.1.3.4) FOR THE BP1 TASKS

In this figure (Figure 55) there are two similar access restrictions (AR6 and AR7) that restrict the execution of a business process task (T2 and T3). In AR6 access is allowed if both the permission rule PR6 (only true if the active role has the P6 permission) and the context rule CR1 (true if the context CTXT1 is activated) are both true. The AR7 is similar but instead of the permission rule PR6 has the PR7 (true if the active role has the P7 permission).

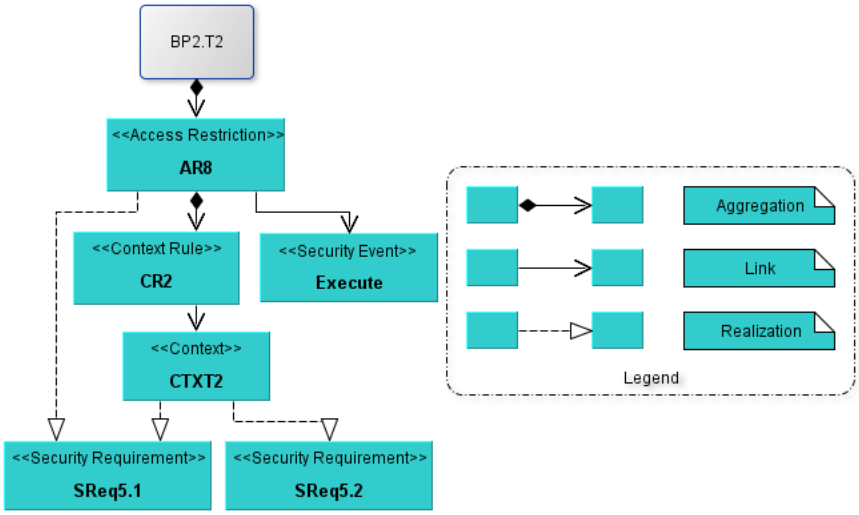

FIGURE 56: BPPRV (CHAPTER IV SECTION 1.1.3.4) FOR THE BP2 TASKS

The access restriction (AR8) shown in Figure 56, allows the task T2 be executed if the context rule CR2 is true (true if the CTXT2 is activated).

3.1.2.5 BPMN DIAGRAMS

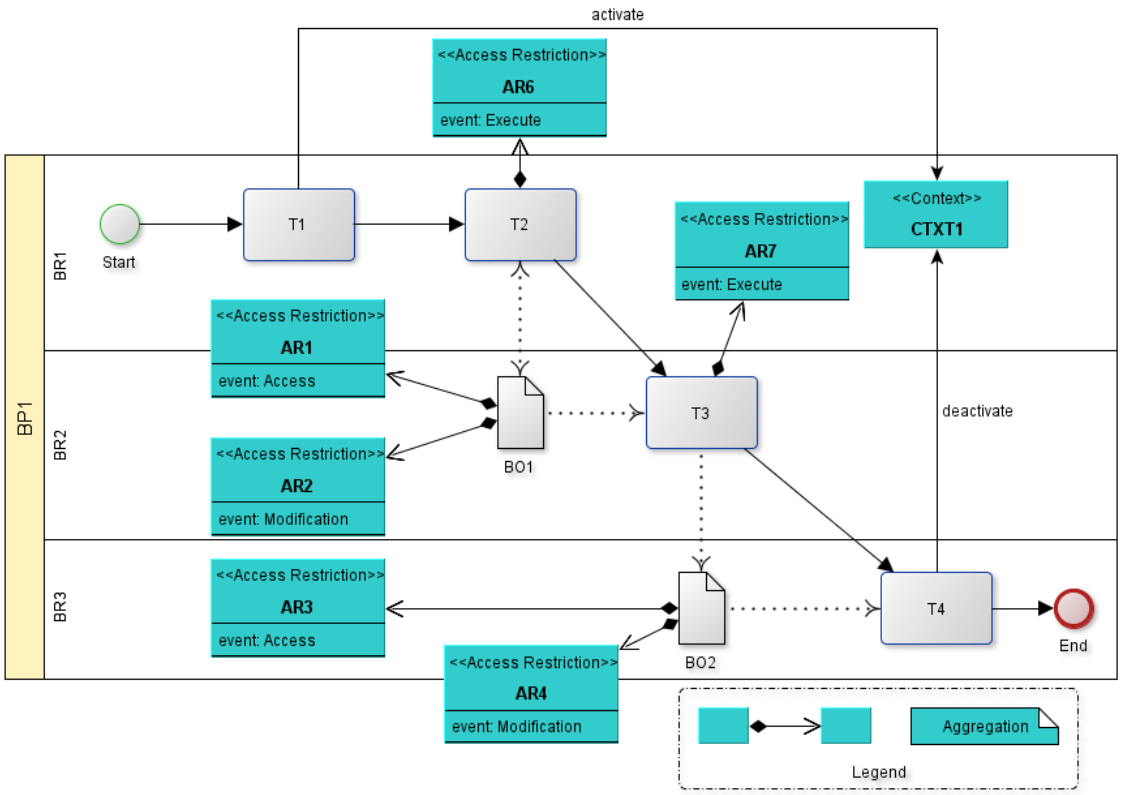

FIGURE 57: BP1 BPMN DIAGRAM WITH THE SECURITY ARTEFACTS

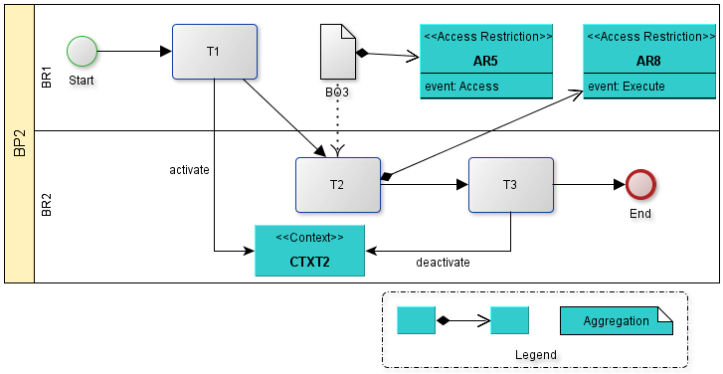

FIGURE 58: BP2 BPMN DIAGRAM WITH THE SECURITY ARTEFACTS

Figure 57 and Figure 58 show the BPMN diagrams of the BP1 and BP2 business processes with the security artefacts included. These artefacts were explained in detail in other viewpoints.

3.1.2.6 SECURITY REQUIREMENTS REALIZATION

	SReq 1.1	SReq 1.2	SReq 1.3	SReq 2.1	SReq 2.2	SReq 3	SReq 4.1	SReq 4.2	SReq 4.3	SReq 4.4	SReq 5.1	SReq 5.2
AR1	R		R									
AR2		R	R									
AR3				R								
AR4					R							
AR5						R						
AR6									R			
AR7								R		R		
AR8											R	
P1	R											
P2		R										
P3				R								
P4					R							
P5						R						
P6									R			
P7										R		
SR1		R							R			
SR2	R											
SR3				R	R	R				R		
SR4				R								
CTXT1			R		R		R	R				
CTXT2						R					R	R

TABLE 5: EASY SCENARIO SECURITY REQUIREMENTS REALIZATION(R - REALIZED, EMPTY - NOT REALIZED)

Table 5 summarizes which elements realize the security requirements presented in section 3.1.1. As can be seen in the table, all elements can be connected to, at least, one requirement and none are left to be realized (the proposed solution, satisfies the imposed requirements).

3.2 SIMPLE SCENARIO WITH ORGANIZATIONS

If we say that in the previous scenario the BO3, that was accessed in the task T2 of the business process BP2 is an object created by an external organization, we add the previously presented R3 security requirement is changed to:

SReq3) BO3 may only be accessed in a context specific to BP2 and only by BR2, but may be modified by the organization ORG1, even if not in the context.

It may be further decomposed to:

SReq3.1) BO3 may only be accessed by BR2 in a context specific to BP2

SReq3.2) BO3 may be modified, even if not in the BP2 specific context, by a role belonging to the organization ORG1,

3.2.1 PROPOSED SOLUTION

3.2.1.1 SARV

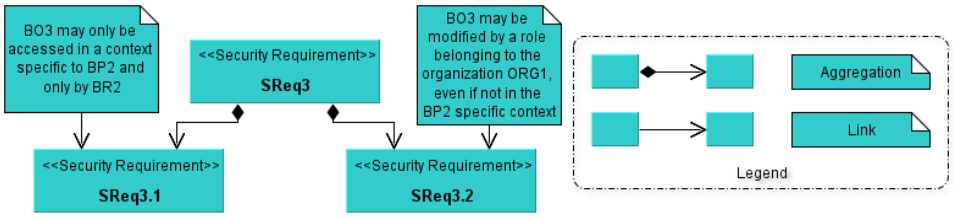

FIGURE 59: EASY SCENARIO WITH ORGANIZATIONS SARV (CHAPTER IV SECTION 1.1.3.3)

In Figure 59 the changes that need to be made to the previously presented SARV are shown.

3.2.1.2 SRV

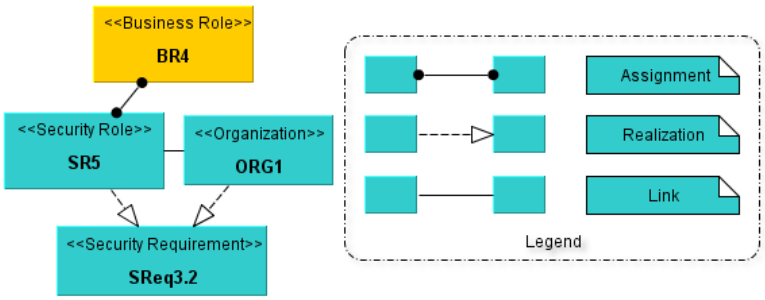

FIGURE 60: EASY SCENARIO WITH ORGANIZATIONS SRV (CHAPTER IV SECTION 1.1.3.1)

This image (Figure 60) shows the additional SRV for this scenario, although it was not specifically required, is included here for completeness. There are some new additional elements to the solution that was previously presented: a new business role (BR4) that is assigned to a new security role (SR5), which represents the actors that belong to the organization ORG1.

3.2.1.3 BOPRV

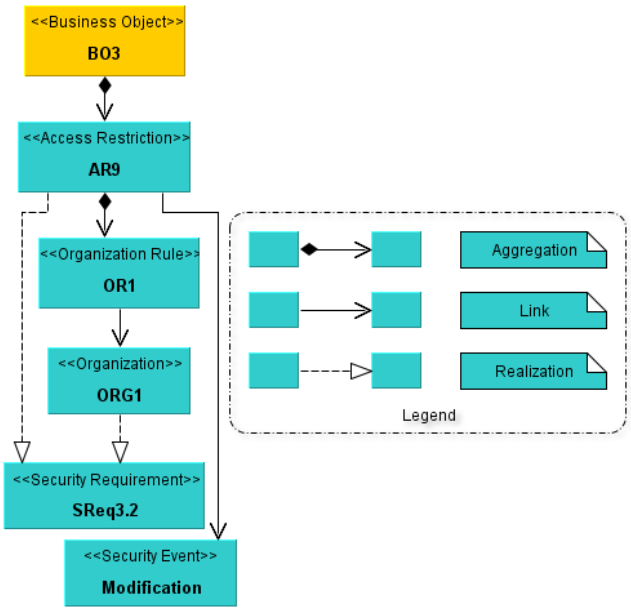

FIGURE 61: EASY SCENARIO WITH ORGANIZATIONS BO3 BOPRV (CHAPTER IV SECTION 1.1.3.2)

Figure 61 shows the access restriction (AR9) that needs to be applied to the business object BO3. It will allow modification of the object if the organization rule OR1 is true (true if the active security role belongs to the organization ORG1).

3.2.1.4 SECURITY REQUIREMENTS REALIZATION

	SReq3.1	SReq3.2
AR5	R	
AR9		R
P5	R	
SR3	R	
SR4		R
CTXT2	R	
ORG1		R

TABLE 6: EASY SCENARIO WITH ORGANIZATIONS SECURITY REQUIREMENTS REALIZATION(R - REALIZED, EMPTY - NOT REALIZED)

Table 6 shows in this scenario the realization of certain security requirements by the elements that were added. The security requirement SReq3.1 column here is equal to the SReq3 column on Table 5.

3.3 SIMPLE SCENARIO WITH AUDITABILITY REQUIREMENTS

In this scenario some auditability requirements will be imposed to the simple scenario presented in Section 3.1. The following two auditability requirements are introduced in this scenario:

AReq1) The restrictions imposed on the business objects that are used or modified during the business process BP1 must generate log artefacts.

AReq2) The restrictions imposed on the tasks of the business process BP1 must generate log artefacts.

These requirements may be further decomposed:

AReq1) The restrictions imposed on the business objects that are used or modified during the business process BP1 must generate log artefacts.

AReq1.1) The restrictions imposed when the business object BO1 is accessed or modified must generate a log artefact.

AReq1.1.1) The restriction imposed when the business object BO1 is accessed must generate a log artefact.

AReq1.1.2) The restriction imposed when the business object BO1 is modified must generate a log artefact.

AReq1.2) The restrictions imposed when the business object BO2 is accessed or modified must generate a log artefact.

AReq1.2.1) The restriction imposed when the business object BO2 is accessed must generate a log artefact.

AReq1.2.2) The restriction imposed when the business object BO2 is modified must generate a log artefact.

AReq2) The restrictions imposed on the tasks of the business process BP1 must generate log artefacts.

AReq2.1) The restriction imposed on the execution of the task T2 of the business process BP1 must generate a log artefact.

AReq2.2) The restriction imposed on the execution of the task T3 of the business process BP1 must generate a log artefact.

3.3.1 PROPOSED SOLUTION

3.3.1.1 SARV

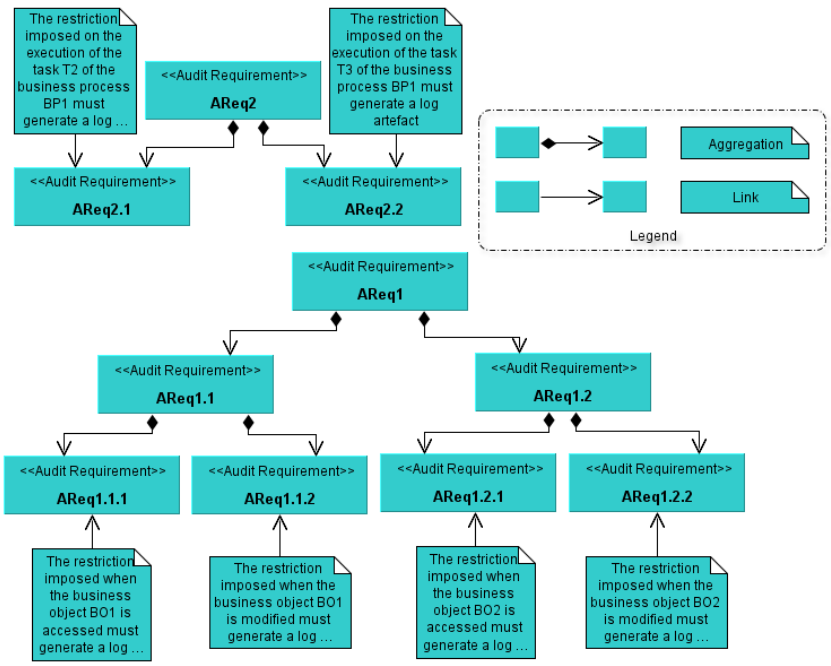

FIGURE 62: EASY SCENARIO WITH AUDIT REQUIREMENTS SARV (CHAPTER IV SECTION 1.1.3.3)

Figure 62 shows the SARV for the easy scenario with audit requirements (this SARV here presented is added to the previously presented SARV on section 3.1.2.1).

3.3.1.2 BOPRV

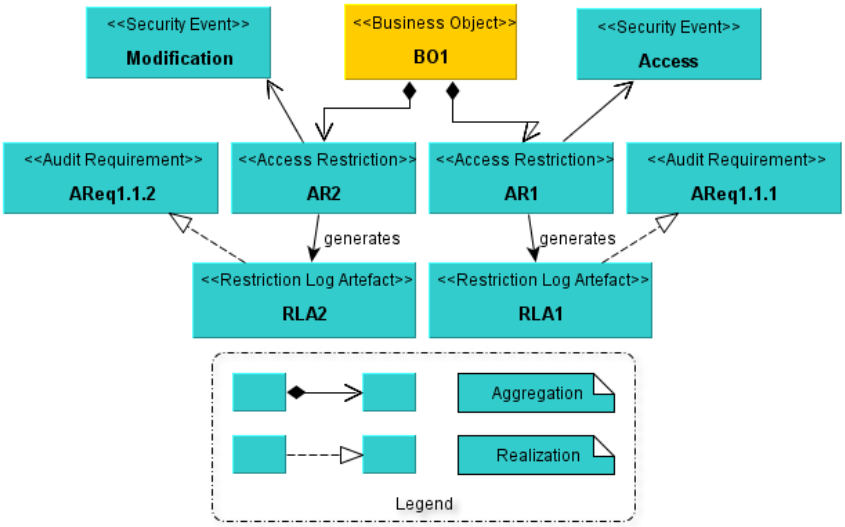

FIGURE 63: EASY SCENARIO WITH AUDIT REQUIREMENTS BO1 BOPRV (CHAPTER IV SECTION 1.1.3.2)

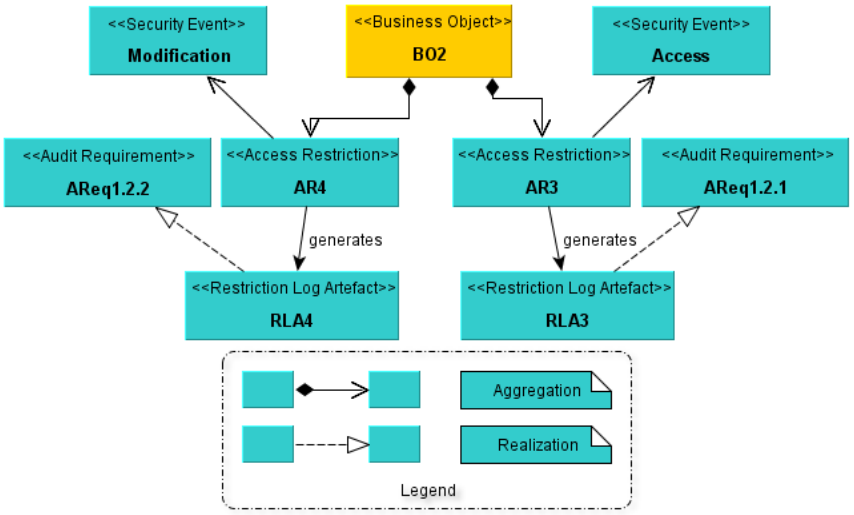

FIGURE 64: EASY SCENARIO WITH AUDIT REQUIREMENTS BO2 BOPRV (CHAPTER IV SECTION 1.1.3.2)

The previous two images (Figure 63 and Figure 64) show which restrictions generate each restriction log artefacts (AR1 generates RLA1, AR2 generates RLA2, AR3 generates RLA3 and AR4 generates RLA4). To ease the explanation of the new elements the full BOPRV (see Figure 52 for BO1 and Figure 53 for BO2) for each business object is not repeated here.

3.3.1.3 BPPRV

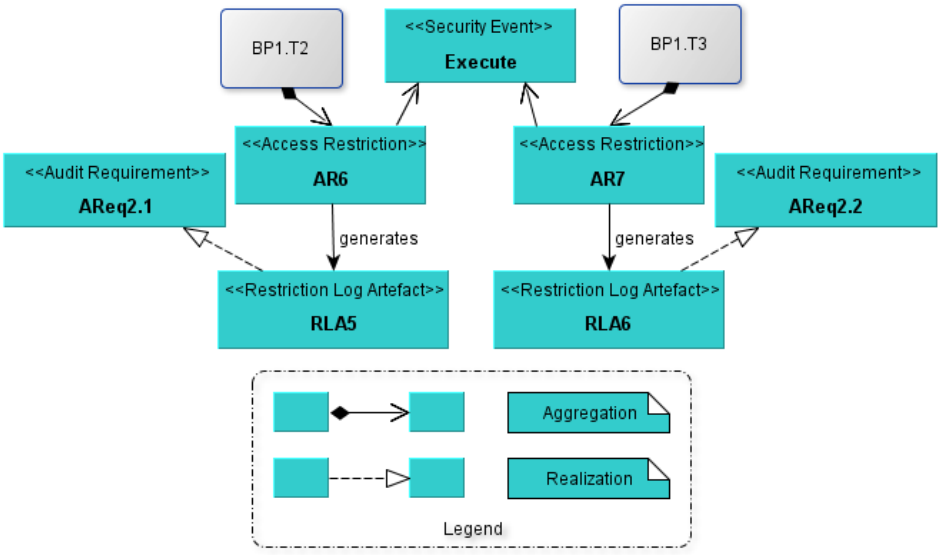

FIGURE 65: EASY SCENARIO WITH AUDIT REQUIREMENTS BPPRV FOR THE BP1 TASKS

As in the BOPRV presented in the section 3.3.1.2, Figure 65 shows the additional elements that will be added to the previously presented BPPRV (Figure 55). The access restriction AR6 generates the restriction log artefact RLA5 and AR7 generates the RLA6.

3.3.1.4 AUDIT REQUIREMENTS REALIZATION

	AReq1.1.1	AReq1.1.2	AReq1.2.1	AReq1.2.2	AReq2.1	AReq2.2
RLA1	R					
RLA2		R				
RLA3			R			
RLA4				R		
RLA5					R	
RLA6						R

TABLE 7: EASY SCENARIO AUDIT REQUIREMENTS REALIZATION(R - REALIZED, EMPTY - NOT REALIZED)

Table 7 summarizes which new elements realize the audit requirements imposed on this scenario.

3.4 SIMPLE SCENARIO WITH ORGANIZATIONS AND SECURITY AND AUDIT REQUIREMENTS

If we take the scenario introduced in section 3.2 and add the following additional audit requirements:

AReq3) Any restriction applied on the business object BO3 must generate a log artefact.

AReq3.1) The restriction applied on the modification of the business object BO3 must generate a log artefact.

AReq3.2) The restriction applied on the access of the business object BO3 must generate a log artefact.

And the following additional security requirements to be applied to the log artefact which was generated by the previous auditability requirements:

SReq6) The log artefact generated by the modification of the business object BO3 must only be accessed by a role that belongs to the organization ORG1.

SReq7) The log artefact generated by the access of the business object BO3 may be accessed by roles belonging to the organization ORG or by the business role BR5.

3.4.1 Proposed solution

3.4.1.1 SARV

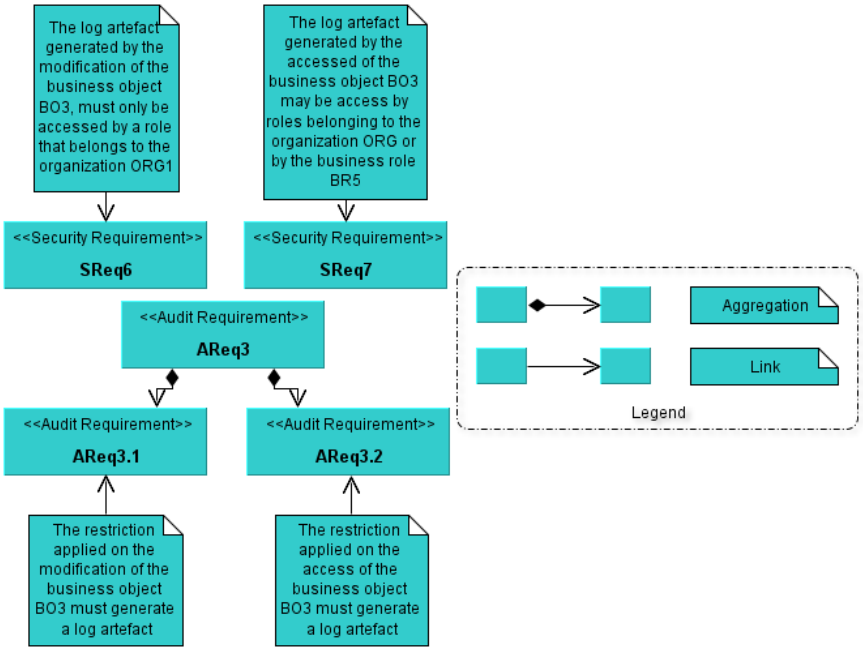

Figure 66: Easy Scenario with organization and audit and security requirements SARV (Chapter IV section 1.1.3.3)

Figure 66 shows the SARV for this scenario with the added security and audit requirements.

3.4.1.2 SRV

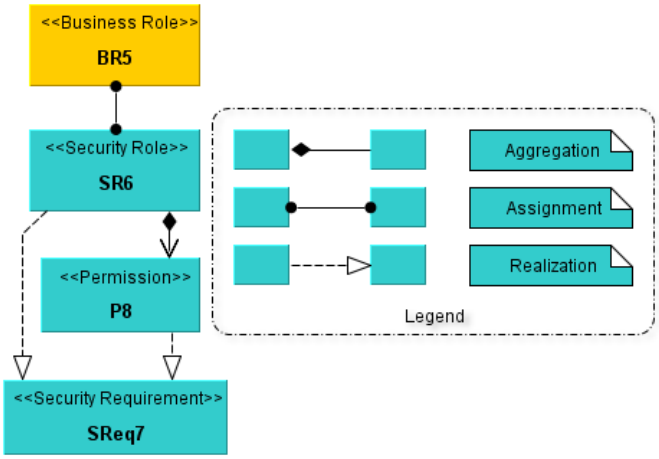

Figure 67: Easy scenario with organizations and audit and security requirements SRV (Chapter IV section 1.1.3.1)

In Figure 67 the SRV for this scenario is shown. The new business role BR5 is assigned to an also new security role (SR6), this role has a permission associated with it (P8).

3.4.1.3 BOPRV

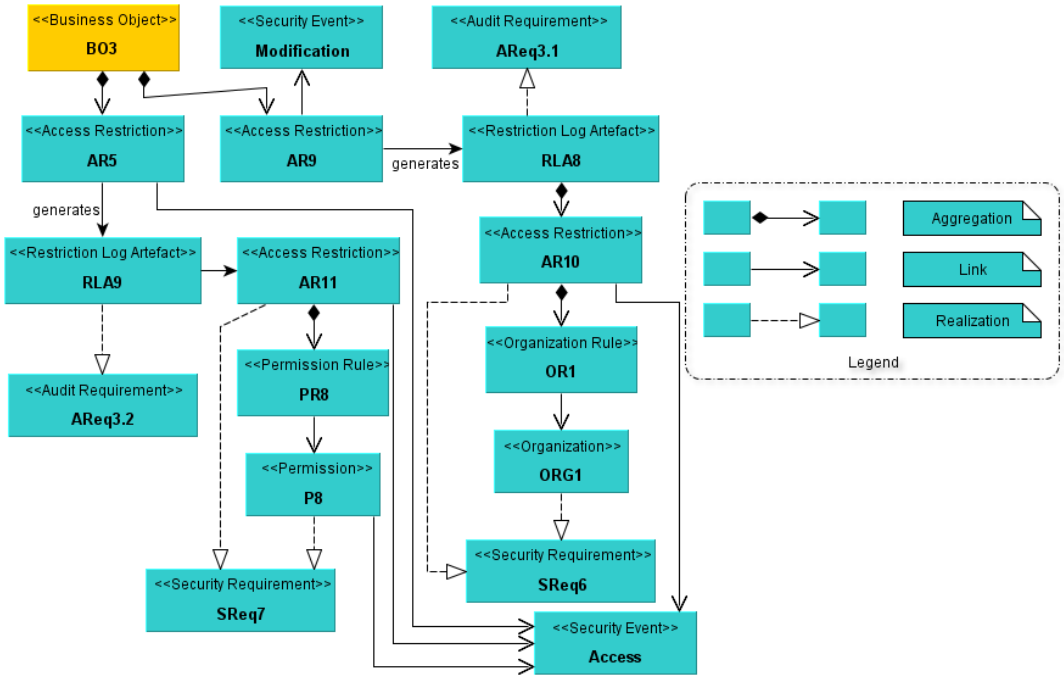

FIGURE 68: EASY SCENARIO WITH ORGANIZATIONS AND AUDIT AND SECURITY REQUIREMENTS BO3 BOPRV (CHAPTER IV SECTION 1.1.3.2)

The BOPRV presented in Figure 68 shows how the existing access restrictions will generate the restriction log artefacts (AR5 generates RLA9 and AR9 generates RLA8) and what restrictions these elements will have (RLA8 is restricted by AR10 and RLA9 by AR11). The access restriction AR10 will allow access to the element if the organization rule OR1 is true (true if the active role belongs to the organization ORG1) and AR11 if the permission rule PR8 is true (only true if the active role has the permission P8).

3.4.1.4 SECURITY AND AUDIT REQUIREMENTS REALIZATION

	SReq6	SReq7	AReq3.1	AReq3.2
RLA8			R	
RLA9				R
AR10	R			
AR11		R		
ORG1	R			
P8		R		
SR6		R		

TABLE 8: EASY SCENARIO AUDIT AND SECURITY REQUIREMENTS REALIZATION(R - REALIZED, EMPTY - NOT REALIZED)

Table 8 shows how each security and audit requirements are realized by the new elements introduced in this scenario.

3.5 SIMPLE SCENARIO WITH DELEGATION

If we add to the simple scenario introduced in section 3.1 the following security requirement regarding delegation:

SReq8) The business role BR1 may delegate the permissions needed to execute the tasks and access the business objects that are used or modified during the business process BP1 to the business role BR2. This delegation may only occur during the execution context specific to BP1.

3.5.1 PROPOSED SOLUTION

3.5.1.1 SARV

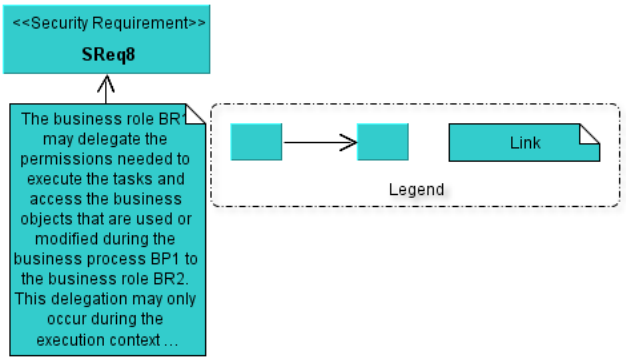

FIGURE 69: EASY SCENARIO WITH DELEGATION SARV (CHAPTER IV SECTION 1.1.3.3)

In Figure 69 the SARV for this scenario is shown.

3.5.1.2 SRV

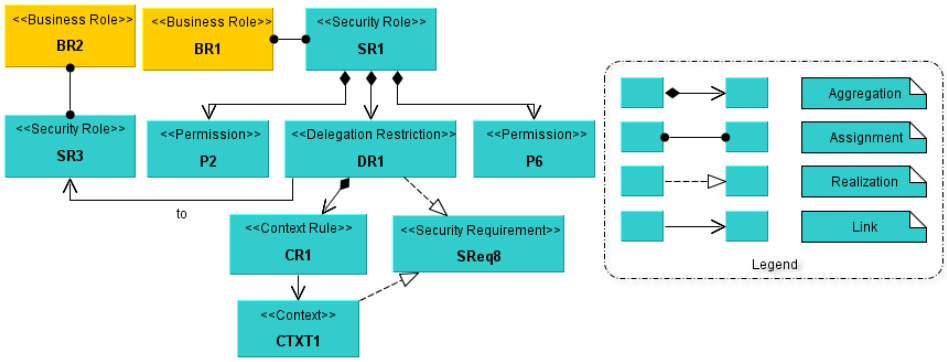

FIGURE 70: EASY SCENARIO WITH DELEGATION SRV (CHAPTER IV SECTION 1.1.3.1)

Figure 70 shows the delegation restriction (DR1) needed in this scenario and the permissions associated with the delegated security role (P2 is needed to modify the business object BO1 and P6 is needed to execute the task T2 of the BP1 business process). The delegation of the security role SR1 to the SR3 will only happen if the context rule CR1 is true (true if the context CTXT1 is activated).

3.5.1.3 SECURITY REQUIREMENTS REALIZATION

	SReq8
DR1	R
CTXT1	R

TABLE 9: EASY SCENARIO SECURITY REQUIREMENTS REALIZATION(R - REALIZED)

Table 9 shows that the security requirement SReq8 is realized by the new element DR1 and by one existing element CTXT1.

4 SUMMARY

In this chapter we have shown how the meta-model introduced in Chapter III can be integrated with an enterprise architecture framework (ArchiMate) and a Business Process modelling language (BPMN). Examples of how it can be used with them are also shown.

To demonstrate how to use the introduced meta-model in a practical case there are also five synthetic scenarios that use the ArchiMate and BPMN integrations. These scenarios were not exhaustive but had the main intention of showing that an enterprise architect can use this proposal to model Access Control in the Business Process layer of the enterprise Architecture.

Chapter V
Case Study

This chapter will present the case study that was realized to demonstrate how this thesis concepts and models can be used in a real situation. To construct it, documentation provided by the INESC[2] and ITIJ[3] was used.

The Portuguese PPO is (quote taken from the GPO site[4]): "the organ that represents the state and defends the interests determined by law, and, under the law, participates in the implementation of the criminal policy as defined by the organs of sovereignty".

To support many of the activities currently executed by the PPO and other entities directly connected to it (such as the courts and the criminal police), a new information system called PPOIS-NG is being implemented. An excerpt of the PPO organizational architecture, with only the organizations that are directly or indirectly referred to.in this case study, is shown in Figure 71.

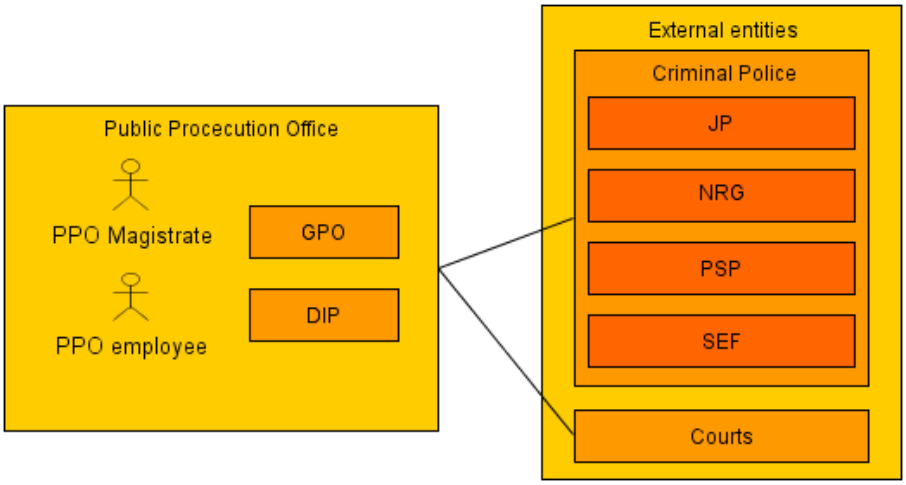

FIGURE 71: PPO ORGANIZATIONAL ARCHITECTURE (ADAPTED FROM (INOV, 2009A))

The PPO employs its own magistrates and employees and is composed of several organizations, among these organizations, the two that are going to be referred in this case study are the the DIP and the GPO. This last one manages the PPOIS-NG and is also the highest authority inside the PPO. This case study will use business processes taken from the Lisbon DIP, which has its own organizational architecture presented in Figure 72.

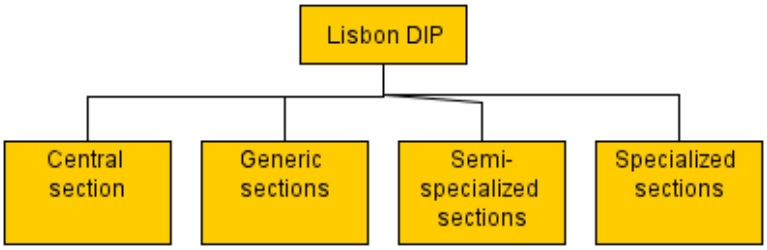

FIGURE 72: DIP ORGANIZATIONAL ARCHITECTURE (ADAPTED FROM (INOV, 2009B))

DIP is (quote taken from the DIP site[5]): "the organ responsible for coordinating and directing the judicial inquests and also for preventing the violent, highly organized or highly complex criminality".

[2] http://www.inesc.pt
[3] http://www.itij.mj.pt/PT/Paginas/Default.aspx
[4] http://www.pgr.pt/grupo_pgr/indice.html
[5] http://www.pgr.pt/grupo_pgr/DCIAP.html

1 PROBLEM

The PPOIS-NG has the following proposed institutional architecture:

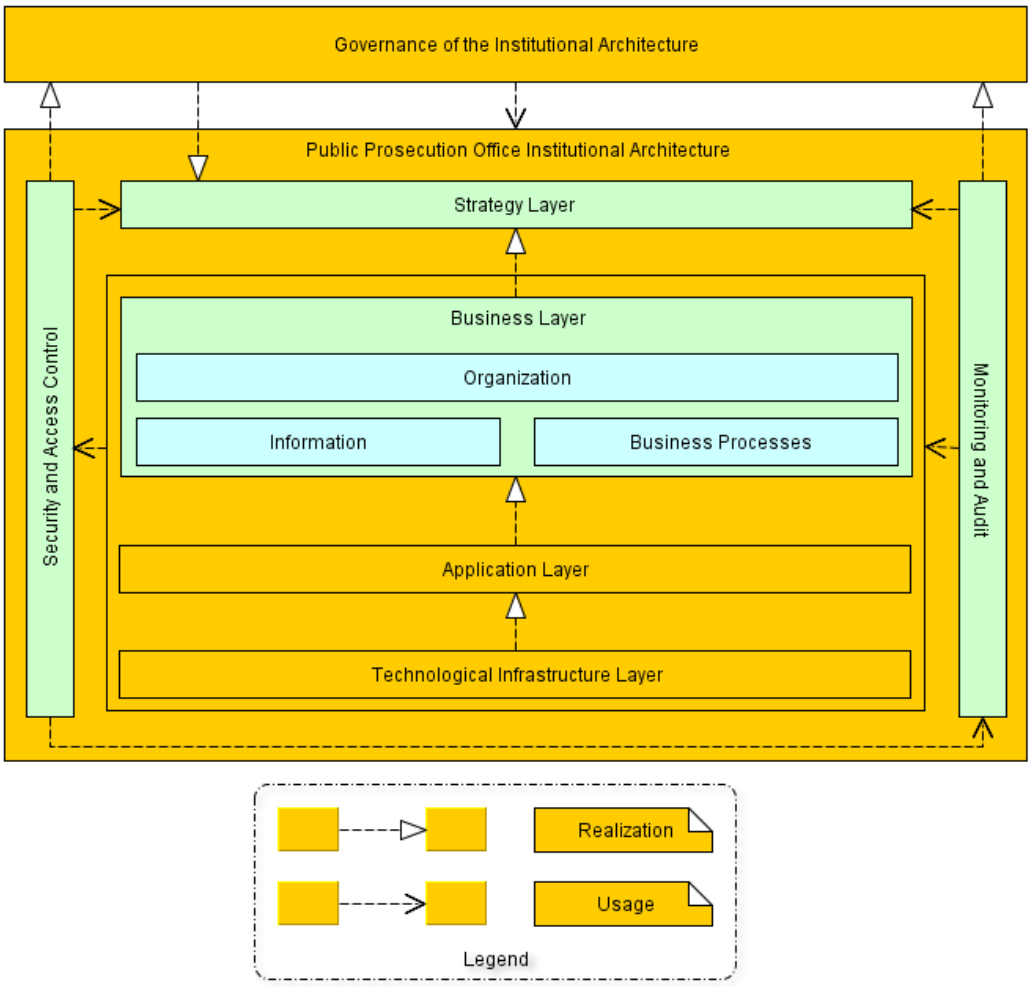

FIGURE 73: PPO INSTITUTIONAL ARCHITECTURE (ADAPTED FROM (INOV, 2009B))

The PPO institutional architecture (Figure 73) is composed of four layers:

- Strategy – Describes the strategy, business objectives, business rules and regulations that define the PPO as organization.
- Business – Describes how the PPO conducts its business and it can be further decomposed in the following parts:
  - Organization – Shows the PPO organizational structure.
  - Information – Describes the information architecture that will produce the business objects used in the business processes.
  - Business Processes – Specifies the PPO business processes, showing how the PPO really works.
- Application – Identifies the applications and services that they provide for the business processes.
- Technology infrastructure – Shows how the applications are made.

There are two layers that transverse all the previous layers, these are:

- Security and Access Control – Describes the access control requirements that all elements present in the institutional architecture must comply.
- Monitoring and Audit – Specifies the requirements that guarantee the auditability of the institutional architecture elements through application of independent monitoring.

The PPO institutional architecture is managed by governance mechanisms that will define the teams, the responsibilities and the processes that will manage, plan, instantiate and update it.

The PPOIS-NG requirement documents define that the access control and auditability in this project must be applied in two different moments:

- Ex-ante – These types of controls are designed during the modelling of the enterprise architecture and define who has access to what elements. Most of the artefacts that will be proposed in the solution are of this type.
- Ex-post – Elements and information that will say who has accessed an element and when to verify if the ex-ante security controls are effective. Each restriction included in the solution will generate a log artefact to help other with this aspect.

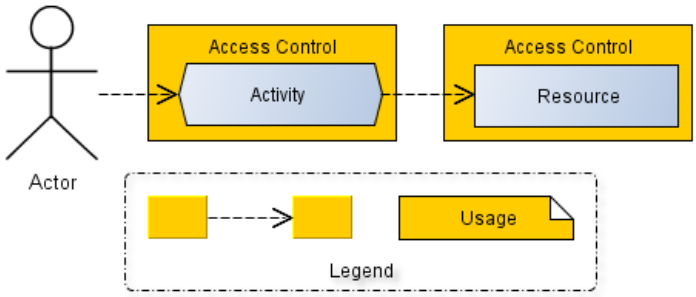

FIGURE 74: ACCESS CONTROL APPLIED TO ACTIVITIES AND RESOURCES (TAKEN FROM (INOV, 2009A))

Figure 74 shows how the ex-ante access controls must be applied (in a business process context) to the activities and resources, where they must be independent (the user must be authorized to execute an activity and then it must gain an independent authorization for the resources that are used).

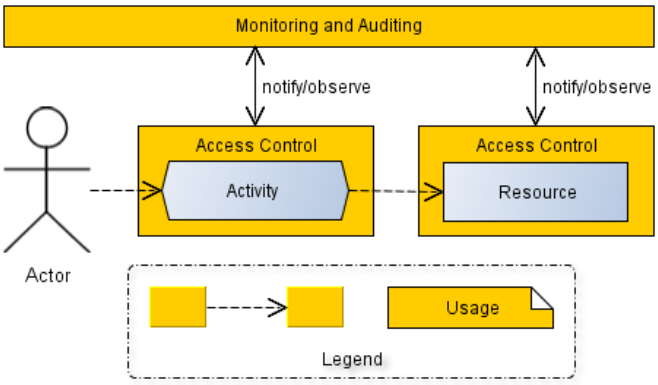

FIGURE 75: ACCESS CONTROL AUDITING (ADAPTED FROM (INOV, 2009A))

In Figure 75 is shown how the ex-post security methods of monitoring and auditing use information provided by the access control.

There are two general security requirements that are imposed by the requirements document (INOV, 2009b):

SReq1) The actor must first request an authorization to execute the activity and only after that is given, he can request a new authorization to access the resources used on it. Those resources can only be accessed in that activity specific context.

SReq2) The auditability registries generated by the access control elements can't be modified or deleted.

And one auditability requirement is imposed:

AReq1) Any action performed by the access control system must provide auditability information, and the access to this information must itself generate new auditability information.

2 SOLUTION

In this section, a possible solution to the previously presented problems is introduced. Due to space constraints, only one business process (taken from the Lisbon DIP) is going to be considered.

2.1 REQUIREMENTS AND SARV

The following security requirements (already decomposed) will guide the rest of this implementation:

SReq1) The actor must have permissions to execute an activity and access the resources used on it. Those resources can only be accessed or modified in an activity specific context. Besides these restrictions, the actor must belong to the organizational unit or organization where that activity is being executed or the resources are being accessed.

SReq1.1) The actor must have permissions to execute a business process activity.

SReq1.2) The actor must have permissions to access the resources used in a business process activity.

SReq1.3) The resources used in an activity can only be accessed or modified in a context specific to it.

SReq1.4) The actor must belong to the organization where the resources or activities are being accessed or executed.

SReq2) The auditability registries generated by the access control elements can't be modified or deleted.

SReq2.1) Any auditability registry can't be modified.

SReq2.2) Any auditability registry can't be deleted.

SReq3) Only actors that are involved in a specific business process can execute its activities and access the various resources used by them.

SReq3.1) A business process activity can only be executed by the actors that are involved in that business process.

SReq3.2) A business process resource can only be accessed by the actors that are involved in that business process.

The following auditability requirements are going to be followed:

AReq1) Any action performed by the access control system must provide auditability information, and the access to this information must itself generate new auditability information.

AReq1.1) Any action performed by the access control system must provide auditability information.

AReq1.2) Any access to auditability information must generate new auditability information.

The security requirement SReq1 was modified from the one present in section 0, in order to add some extra conditions when accessing or executing the business process elements.

The following simplified SARV (Chapter IV section 1.1.3.3) is generated with some of the previously presented security and audit requirements:

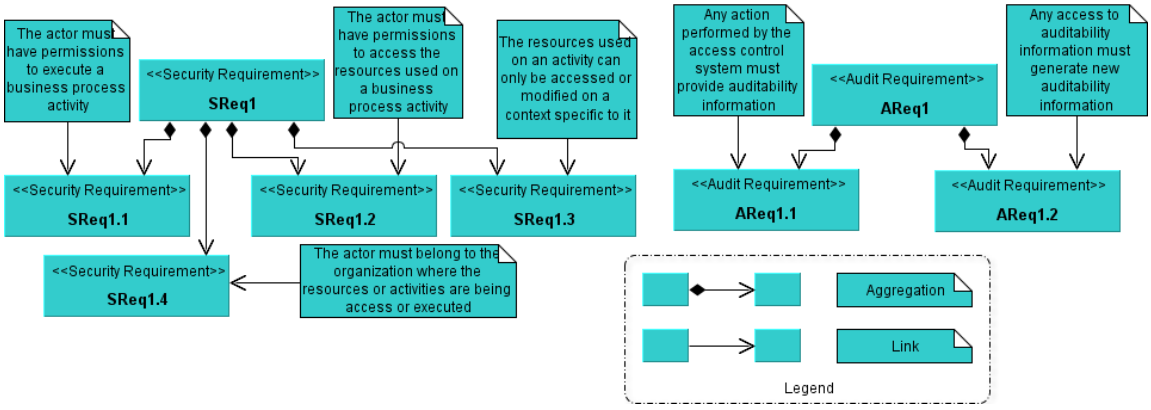

FIGURE 76: CASE STUDY SARV

2.2 SECURITY EVENTS AND BPPRV

The following security events are going to be considered in the rest of this section:

- Read – The read event is going to be applied when an actor tries to read a business object.
- Modify – When a user tries to modify a business object, this event is triggered.
- Execute – Before the execution of any task, the execute event is triggered.
- Post-Execute – The post-execute event is going to be triggered after the execution of a certain activity.

The reason behind the two events related to the execution of an activity (executes and post-execute) is the security requirement 1.3 (see section 2.1). It is stated in it that the user needs to be in an activity specific context to access any resource that is used on it. So that this happens, a context specific to a task is going to be activated on the execute event restriction (if the user is authorized) and that context is going to be deactivated after the task executed on the post-execution restriction.

The original business process diagram (ITIJ) is shown in Annex A in Figure 83 and the information about which objects are used in each task and how they are used is present in Table 11 (also in Annex A). With this information, the business process diagram shown in Figure 78 was constructed.

The following diagram represents the SRV (Chapter IV section 1.1.3.1) for this case study (it is only a partial model because the full model with the permissions associated with each security role will be presented soon):

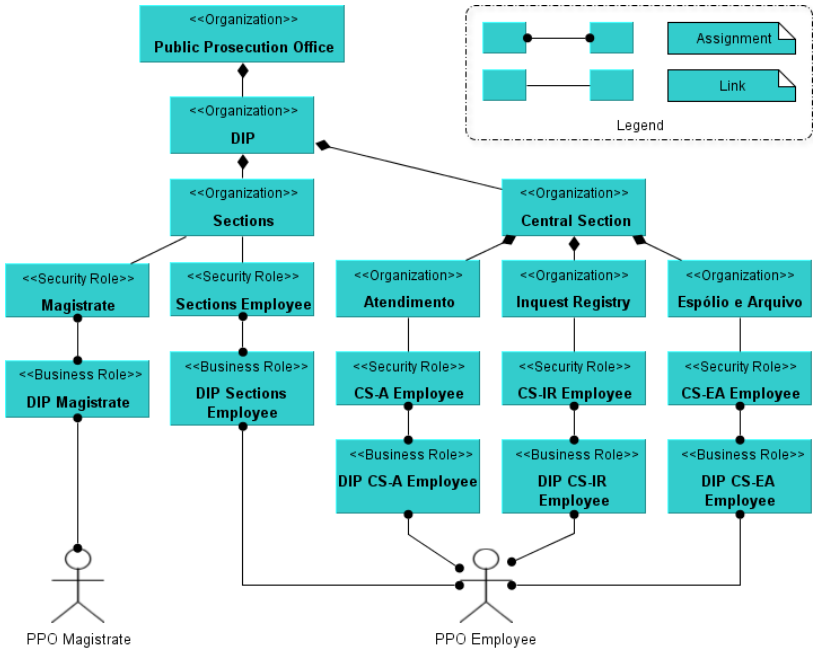

FIGURE 77: SRV FOR THE CASE STUDY (NOT COMPLETE)

In Figure 77, there are several different actors associated with the business roles that will perform the activities present in Figure 78. These are associated with security roles that are linked with the organizations that represent the organizational units of DIP.

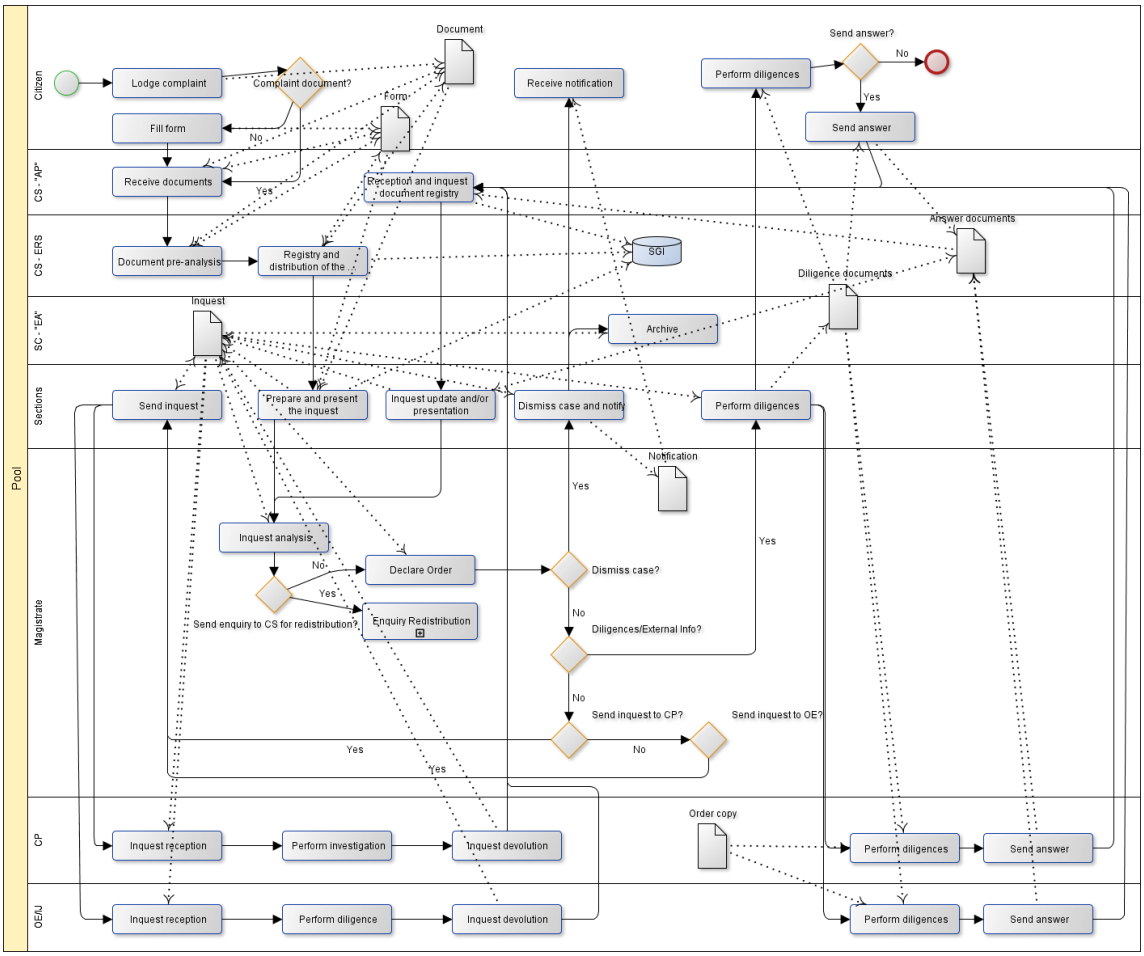

FIGURE 78: DIP COMPLAINT LODGING WITH INFORMATION

To construct the restrictions that are going to be applied to each task, the following rules were followed:

1. The actor that is referenced on the lane where it is located is the only one who can execute it. In some cases, where there is no specific actor only an organizational unit or an organization, it is considered that the task is executed by an employee of that organization.
2. There is a global business process context that has to be activated so that it can be executed (SReq3.1).
3. All the restrictions will generate a log artefact (AReq1.1).
4. If some resource is read or modified, a task specific context is activated on the execute restriction and deactivated on the post-execute restriction (SReq1.2).
5. The actor must belong to the organization referenced on the lane, or in the magistrate's case, belong to the sections (SReq1.4).

With these rules in mind, a BPPRV (Chapter IV section 1.1.3.4) diagram was created. Due to space constraints and since the restrictions applied to each activity are very similar, only one diagram will be presented here.

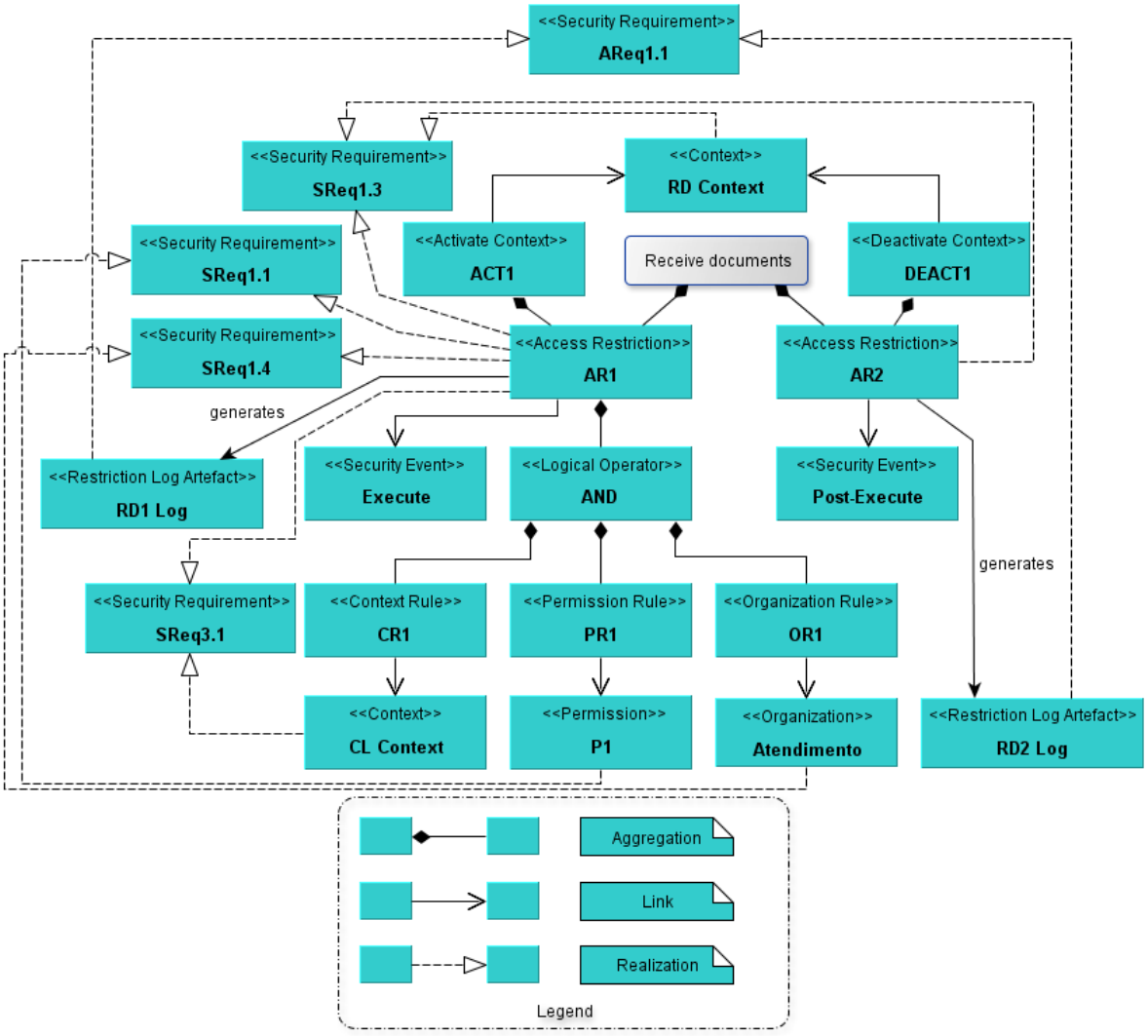

FIGURE 79: RECEIVE DOCUMENTS ACCESS RESTRICTIONS

The diagram shown in Figure 79 has:

- Two access restrictions associated with the activity (AR1 and AR2);
- An activity specific context that is activated and deactivated on the restriction associated with the activity (RD Context).
- A restriction that only allows access if these three rules are true:
  - The business process context is activated (CL Context);
  - The active security role has a specific permission (P1).
  - The active security role belongs to a specific organization (Atendimento).
- The restriction generates log artefacts (AR1 generates RD1 Log and AR2 generates RD2 Log).

2.3 BOPRV

The following rules were used during the construction of the restrictions applicable to the business objects:

1. The complaint lodging global business process specific context (CL Context) has to be activated (SReq3.2).
2. The actor must have permissions to access or modify the resource (SReq1.2).
3. The task specific context, where the resource is accessed or modified, must be activated (SReq1.3).
4. The actor must belong to the organizations referenced on the lane, or in some cases, like the magistrate, belong to the sections (SReq1.4).
5. All the restrictions will generate a log artefact (AReq1.1).
6. If the business object is a restriction log artefact, it can't be modified (SReq2.1) or deleted (SReq2.2) and any access to it must generate new auditability information (AReq1.2).

Since there are many business objects in this case study and due to space constraints, it will only be shown here the BOPRV (Chapter IV section 1.1.3.2) regarding the read (access) event restriction for the inquest object (Figure 80) and one restriction log artefact (Figure 81).

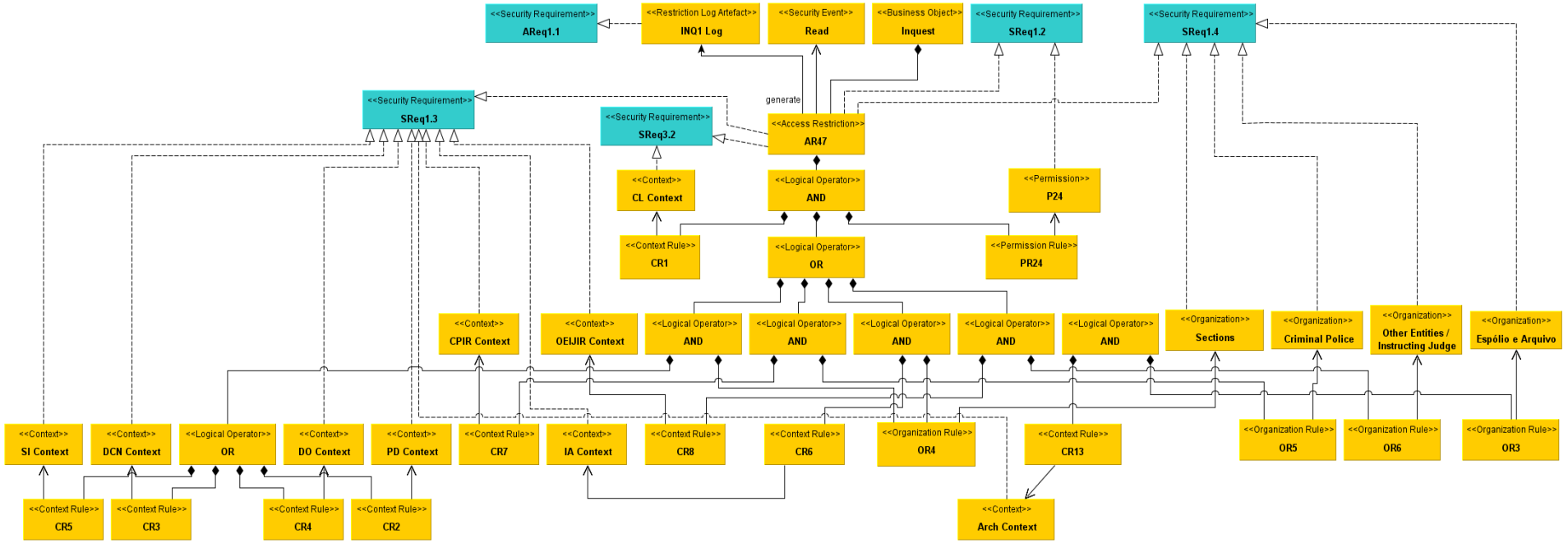

FIGURE 80: INQUEST OBJECT READ RESTRICTIONS

In Figure 80 the access restriction applicable to the inquest object is shown, and has the following characteristics:

- The business process context (CL Context) has to be active (CR1).
- The actor has to have permission (P24) to access the object (PR24).
- The actor has to belong (e.g. OR4) to an organization or organizational unit (e.g. Sections) that has access.
- The activity specific context (e.g. SI Context) has to be active (e.g. CR5).

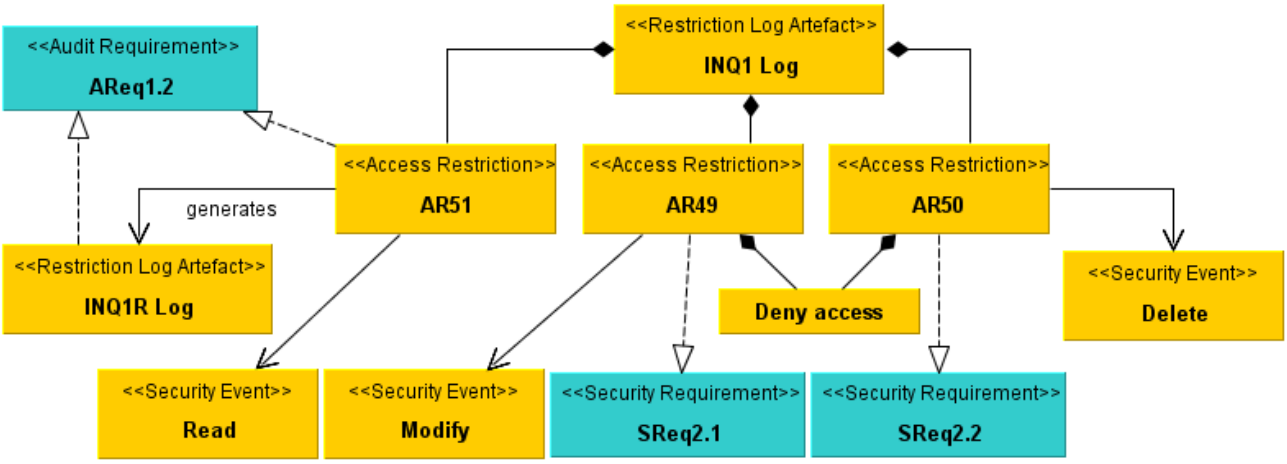

FIGURE 81: INQ1 RESTRICTION LOG ARTEFACT RESTRICTIONS

Figure 81 shows the access restrictions (AR49, AR50 and AR51) that the restriction log artefact (INQ1 Log) has. AR49 and AR50 deny any modification or deletion and AR51 states that any access to the INQ1 Log object generates a new log artefact (INQ1R Log).

2.4 SRV

In this section, the SRV (Chapter IV section 1.1.3.1) for the PPO Magistrate actor is going to be shown.

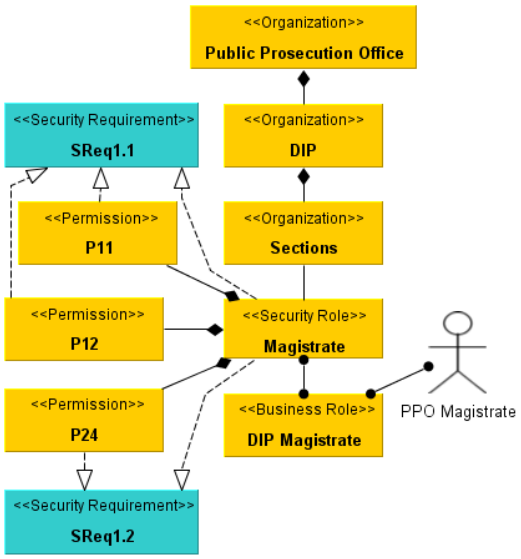

FIGURE 82: SRV FOR THE MAGISTRATE

In Figure 82, the security role magistrate has three permissions associated with it (P11, P12 and P24), they allow, respectively, to execute the inquest analysis and the declare order activities and to access (read) the inquest object.

2.5 SECURITY AND AUDIT REQUIREMENTS REALIZATION

	SReq1.1	SReq1.2	SReq1.3	SReq1.4	SReq2.1	SReq2.2	SReq3.1	SReq3.2	AReq1.1	AReq1.2
AR1	R		R	R			R			
AR2			R							
AR47		R	R	R				R		
AR49					R					
AR50						R				
AR51		R								
P1	R									
P11	R									
P12	R									
P24		R								
CL Context							R			
RD Context			R							
Atendi-mento				R						
RD1 Log									R	
RD2 Log									R	
INQ1 Log									R	
INQ1R Log										R
Magistrate	R	R								

TABLE 10: CASE STUDY SECURITY AND AUDIT REQUIREMENTS REALIZATION

Table 10 shows the security and audit requirements realization with some of the presented elements (due to the space constraints, the only elements shown here are from: Figure 79, Figure 81, Figure 82 and some elements were taken from Figure 80).

Chapter VI
Analysis and Conclusions

1.1 EVALUATION

This thesis was evaluated and validated by following some of the guidelines introduced in (Hevner et al., 2004). 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 (presented through the text of this thesis), Scenarios (presented in Chapter IV) and a Case study (presented in Chapter V).

1.2 ANALYSIS AND CONCLUSIONS

The meta-model presented in Chapter III answers all the research questions proposed in Chapter I section 1 while the integrations with ArchiMate and BPMN introduced in Chapter IV sections 1 and 2 allow enterprise architects to use this meta-model for modelling access control.

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 in the case study.

1.3 FUTURE WORK

Some future work on this area may be focused on expanding the ACECA language and the core model to include additional features. The integrations presented in this 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.

BIBLIOGRAPHY

Abdallah, A. E., & Takabi, H. (2008). *Integrating delegation with the formal core RBAC model*.

Barka, E., & Sandhu, R. (2000). *A role-based delegation model and some extensions*.

Botha, R., & Eloff, J. (2010). Separation of duties for access control enforcement in workflow environments. *IBM SYSTEMS JOURNAL, 40*(3), 666-682.

Chaari, S., Biennier, F., Amar, B., & Favrel, J. (2005). *An authorization and access control model for workflow*.

Dick Quartel, W. E., Henk Jonkers. (2010). ArchiMate Extension for Modeling and Managing Motivation, Principles and Requirements in TOGAF.

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

Georgiadis, C., Mavridis, I., Pangalos, G., & Thomas, R. (2001). *Flexible team-based access control using contexts*.

Group, T. O. (2009a). ArchiMate 1.0 Specification Retrieved 8/12/2010, 2010, from http://www.opengroup.org/archimate/doc/ts_archimate/

Group, T. O. (2009b). TOGAF Version 9 Retrieved 14/12/2010, from http://www.opengroup.org/architecture/togaf9-doc/arch/

Group, T. O. (2012). ArchiMate 2.0 Specification, from http://pubs.opengroup.org/architecture/archimate2-doc/

Guerreiro, S., Vasconcelos, A., & Tribolet, J. (2010). Adaptive Access Control Modes Enforcement in Organizations

ENTERprise Information Systems. In J. E. Quintela Varajão, M. M. Cruz-Cunha, G. D. Putnik & A. Trigo (Eds.), (Vol. 110, pp. 283-294): Springer Berlin Heidelberg.

Henriques, M., Tribolet, J., & Hoogervorst, J. (2010). *Enterprise Governance and DEMO.* Master Thesis, Department of Computer Science and Engineering, Technical University of Lisboa, Instituto Superior Técnico, Lisboa.

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design science in information systems research. *Mis Quarterly, 28*(1), 75-105.

INOV, I. (2009a). Arquitectura Empresarial para o SIMP.

INOV, I. (2009b). Requisitos técnicos para o SIMP-NG. Retrieved from

ISACA. (2010). *COBIT 5*.

ISO/IEC. (2005). ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security management.

ITGI. (2003). Board Briefing on IT Governance (pp. 10).

ITGI/OGC. (2008). Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit ITGI (Ed.)

ITIJ. Levantamento de processos e análise funcional.

Kalam, A., Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., . . . Trouessin, G. (2003). *Organization based access control*.

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

Long, D., Baker, J., & Fung, F. (2002). *A prototype secure workflow server*.

OMG. (2009). Business Process Model And Notation (BPMN) Retrieved 7/12/2010, from http://www.omg.org/spec/BPMN/

OMG. (2011). Business Process Model And Notation (BPMN) v2.0 Retrieved 1/02/2011, from http://www.omg.org/spec/BPMN/2.0/

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

Ravi, S., Edward, J., Hal, L., & Charles, E. (1996). Role-based access control models. *IEEE Computer, 29*(2), 38-47.

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

Sandhu, R., & Samarati, P. (2002). Access control: principle and practice. *Communications Magazine, IEEE, 32*(9), 40-48.

Shen, H., & Hong, F. (2006). *An attribute-based access control model for web services*.

Society, I. C. (2000). IEEE Std 1471-2000: IEEE Recommended Practice for Architectural Description of Software-Intensive Systems. New York: IEEE.

Thomas, R. (1997). *Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments*.

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

Winter, R., & Fischer, R. (2007). Essential Layers, Artifacts, and Dependencies of Enterprise Architecture. *Journal of Enterprise Architecture–May*, 1.

Wolter, C., Menzel, M., & Meinel, C. Modelling security goals in business processes. *Modellierung 2008, 127*, 201–216.

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

Annex A CASE STUDY ADDITIONAL DIAGRAMS AND TABLES

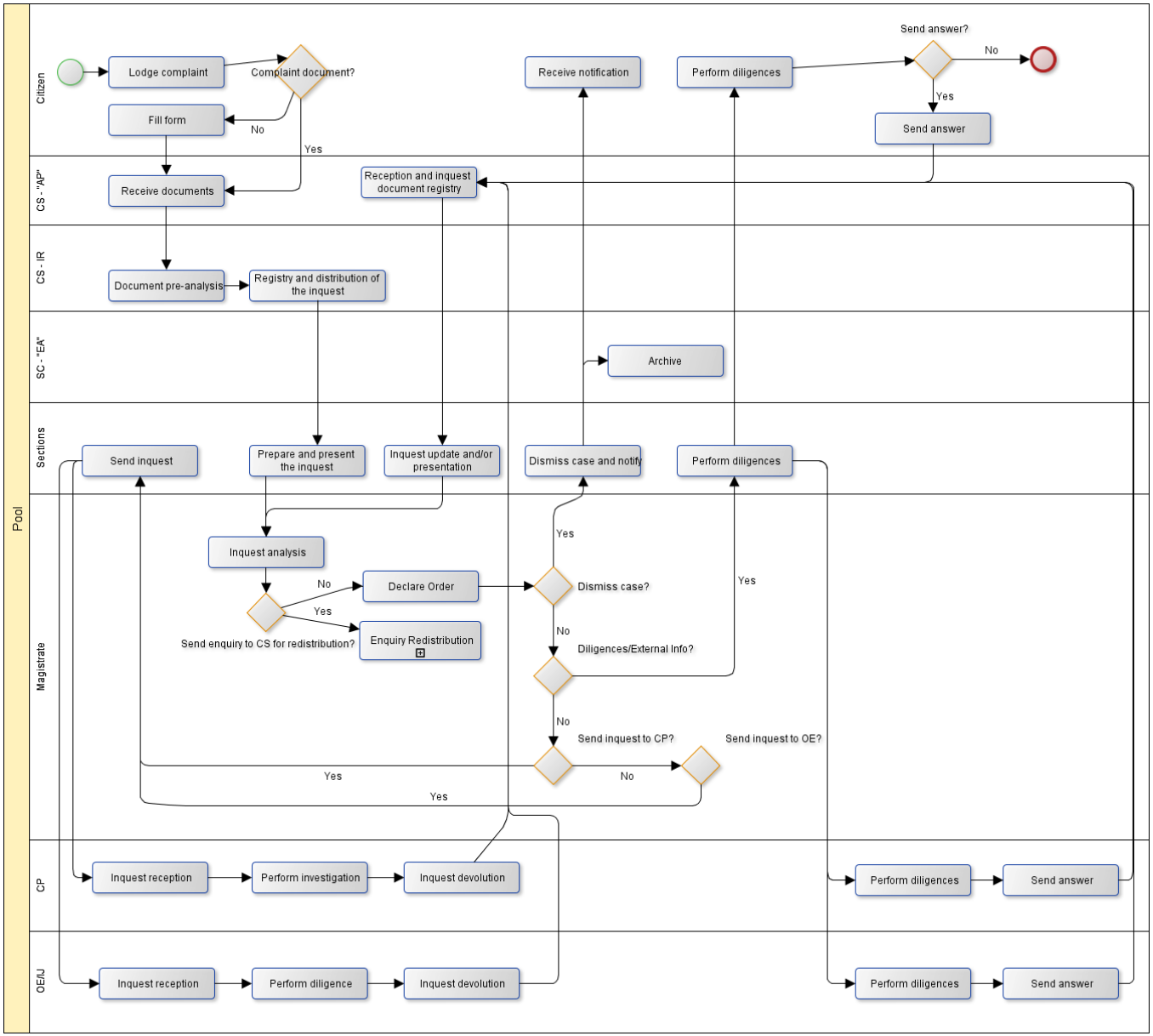

FIGURE 83: COMPLAINT LODGING DIAP (TAKEN FROM (ITIJ))

Organizational unit	Activity	Input	Output
Citizen	Lodge complaint		Documents
	Fill form		Form
Central section (CS) – "Atendimento"	Receive documents	Form or documents	Form or documents
CS - Inquest registry	Document pre-analysis	Form or documents	Form or documents
	Registry and distribution of the inquest	Form or documents	Form or documents and SGI registry
Sections	Prepare and present the inquest	Form or documents	Inquest
Magistrate	Inquest analysis	Inquest	
	Declare order	Inquest	Inquest
Section	Dismiss case and notify	Inquest	Inquest and Notifications
CS – "Espólio e arquivo"	Archive	Inquest	(Optional)Inquest
Citizen	Receive notification	Notification	
Sections	Perform diligences	Inquest	Inquest and Documents
Citizen	Perform diligences	Specific document	
	Send answer	Specific document	Answer document
CS – "Atendimento"	Reception and inquest document registry	Answer documents	Answer documents and SGI registry
Sections	Inquest update and/or presentation	Answer documents	Inquest and/or answer document
	Send inquest	Inquest	Magistrate inquest
Criminal Police (CP)	Inquest reception	Inquest	
	Perform investigation		
	Inquest devolution		Documents and Inquest
Other entities (OE) / Instructing Judge (IJ)	Inquest reception	Inquest	
	Perform diligences		
	Inquest devolution		Documents and Inquest
CP	Perform diligences	Documents and order copy	
	Send answer		Answer documents
OE / IJ	Perform diligences	Documents and order copy	
	Send answer		Answer documents

TABLE 11: COMPLAINT LODGING DIAP – ACTIVITY INPUTS AND OUTPUTS (TAKEN FROM (ITIJ))