PhD presentation support

Feltus, Christophe

Aligning Access Rights to Governance Needs with the Responsibility MetaModel (ReMMo) in the Frame of Enterprise Architecture

Public Defense
Christophe Feltus

Public Research Centre Henri Tudor, Luxembourg-Kirchberg, Luxembourg
University of Namur, Namur, Belgium
christophe.feltus @tudor.lu

Promotors: Pr. M. Petit et Pr. E. Dubois

March 11th, 2014

Overview

Introduction

State of the art: Access Control Models and Governance needs

Responsibility metamodel

ArchiMate extension with Responsibility

Method for the access rights management

Conclusions

Overview

Introduction
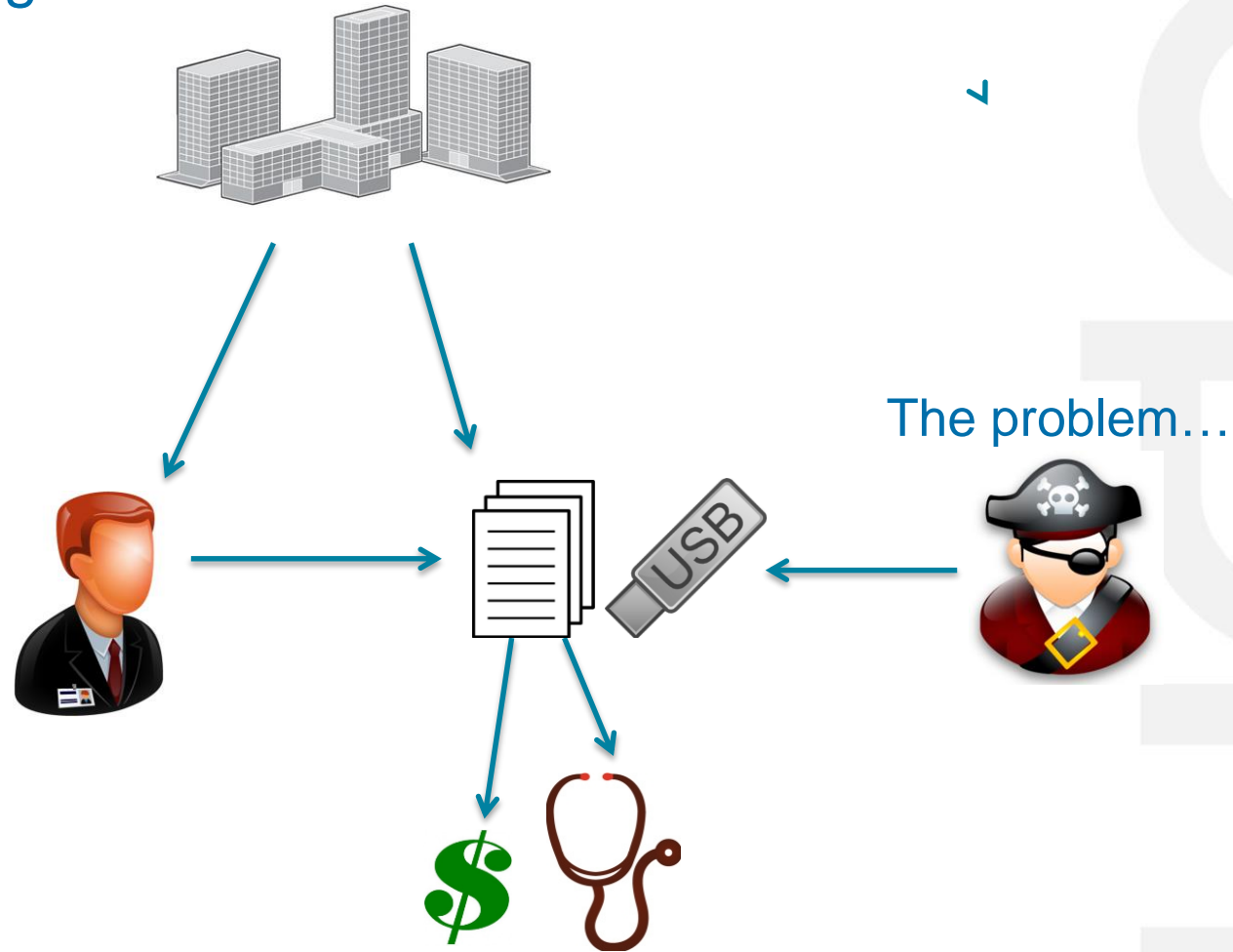
The problem
New challenges

The problem…

The problem
New challenges

ok

USB

Not ok

The problem
New challenges

Roles

ok

Control

Motivations

Enterprise Architecture
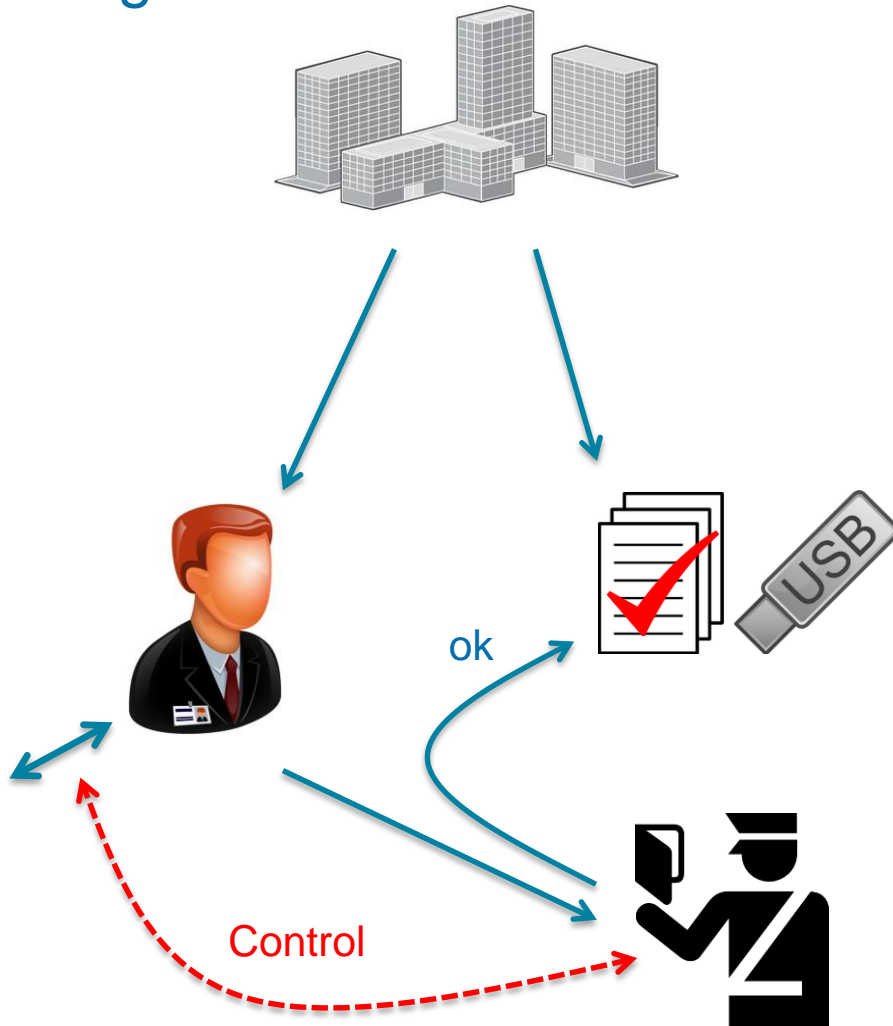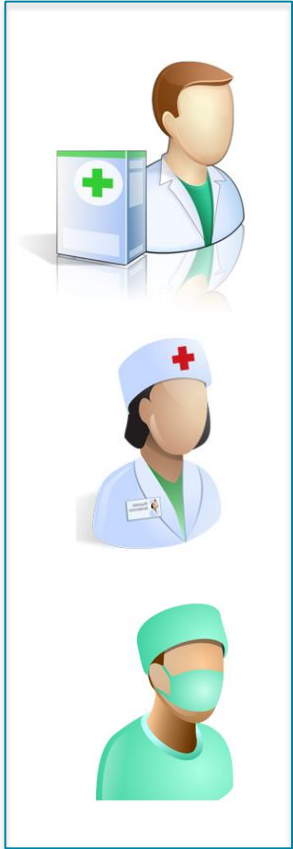
Arising governance needs
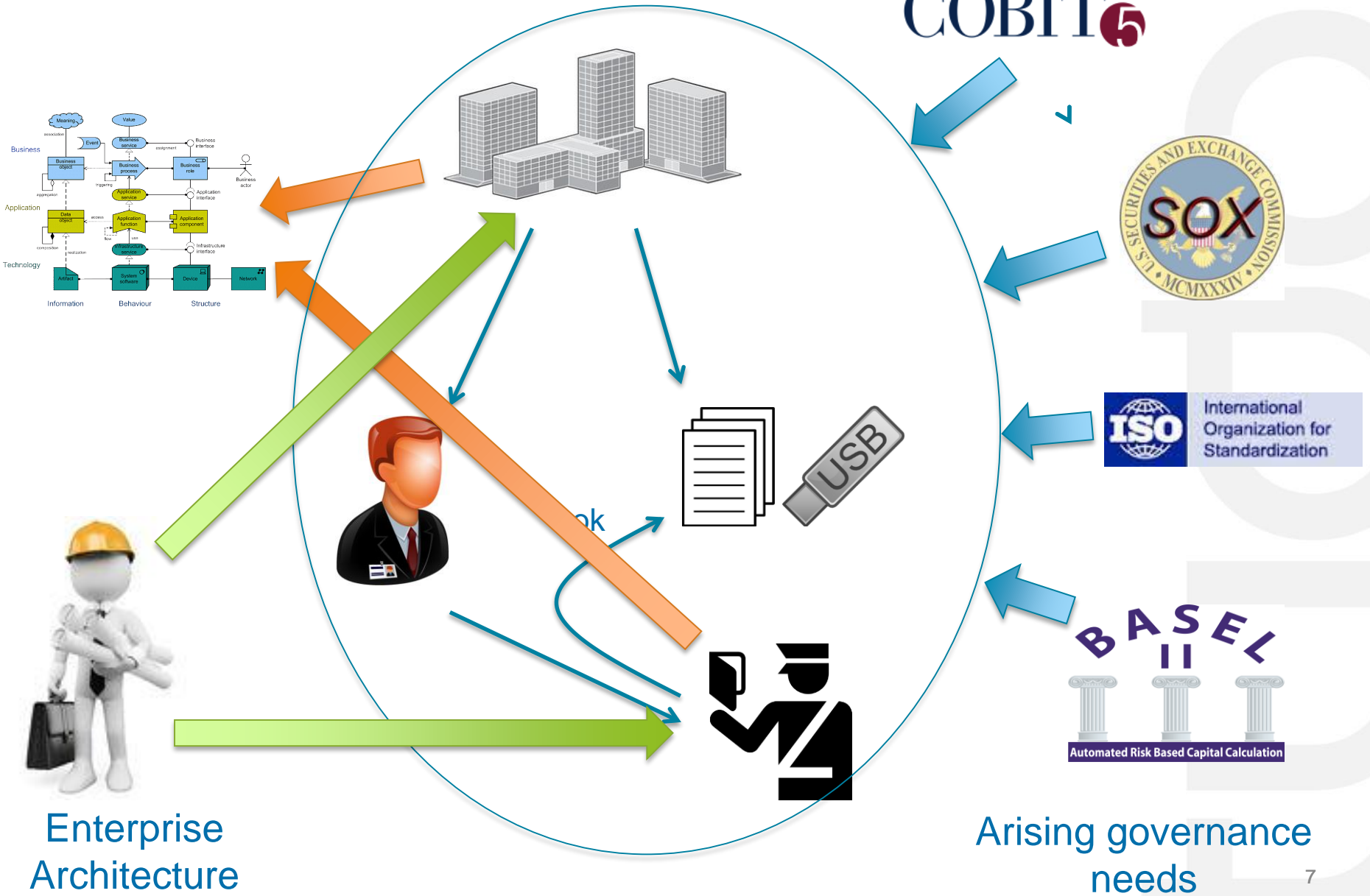
Scope of the research
Targeted companies, type of access rights, case studies

- Targeted companies
  - Highly formalised business and regulated environment
  - Bureaucratic organisations

- Access rights «by design»
  - Necessary to perform operational tasks
  - Accurately and rigorously engineered

- Case studies
  - European Court of Auditors
  - Centre Hospitalier de Luxembourg

Overview

Introduction

State of the art: Access Control Models and Governance needs

Responsibility metamodel

ArchiMate extension with Responsibility
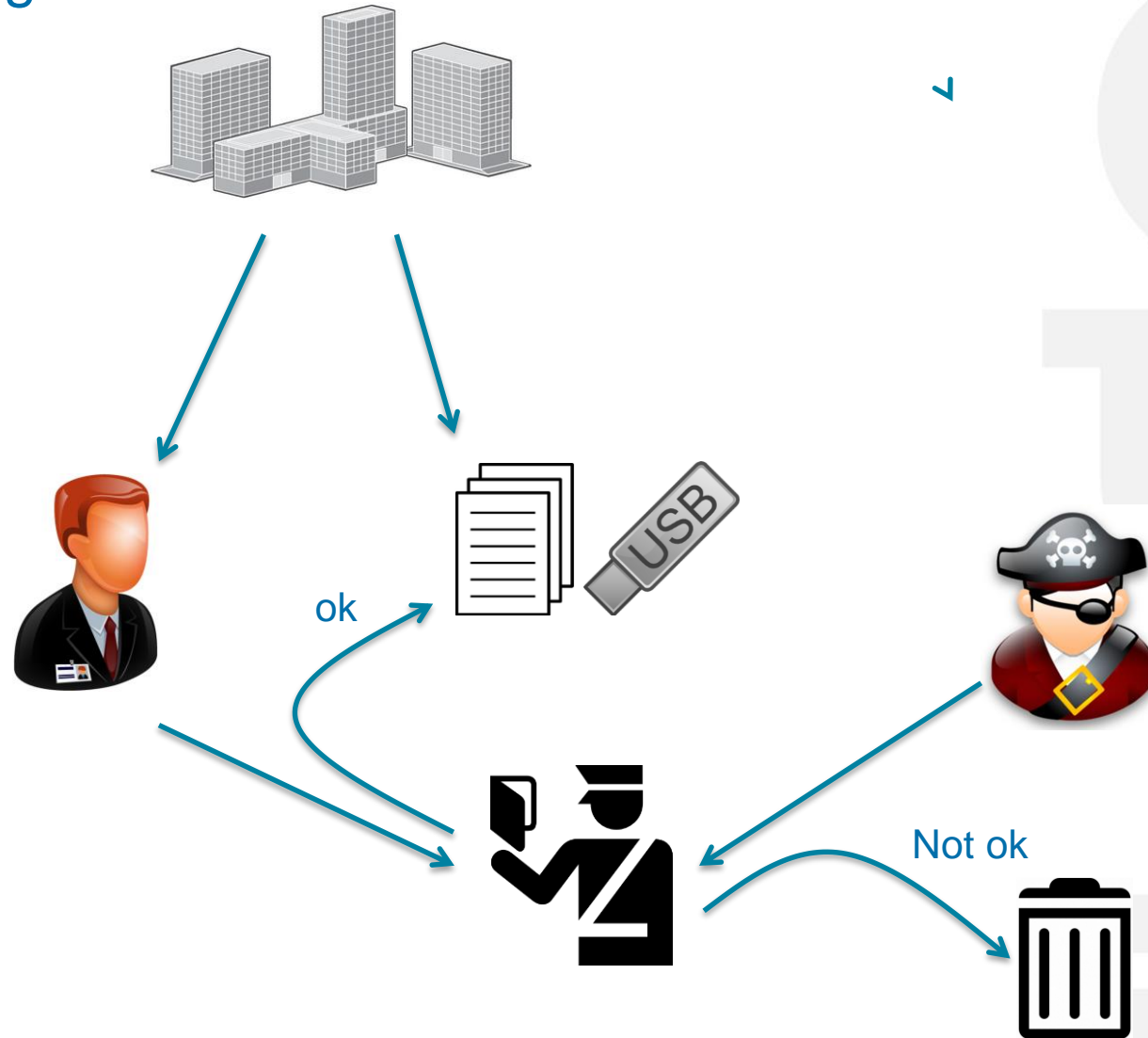
Method for the access rights management

Conclusions

State of the art
Access Control Models and Rights engineering methods

- Objectives of the State of the Art:
  - Figure out the level of integration with the business artefacts
  - Understand the evolution of the models and methods
- Access control models:
  - MAC – DAC – RBAC – ABAC – Others
- Rights engineering methods:
  - R/PAM – ARMF – Uses cases – Scenario-driven

RBAC:

«A role is a job function within the context of an organisation with some associated semantics regarding the authority and the responsibility conferred on the user assigned to the role.»
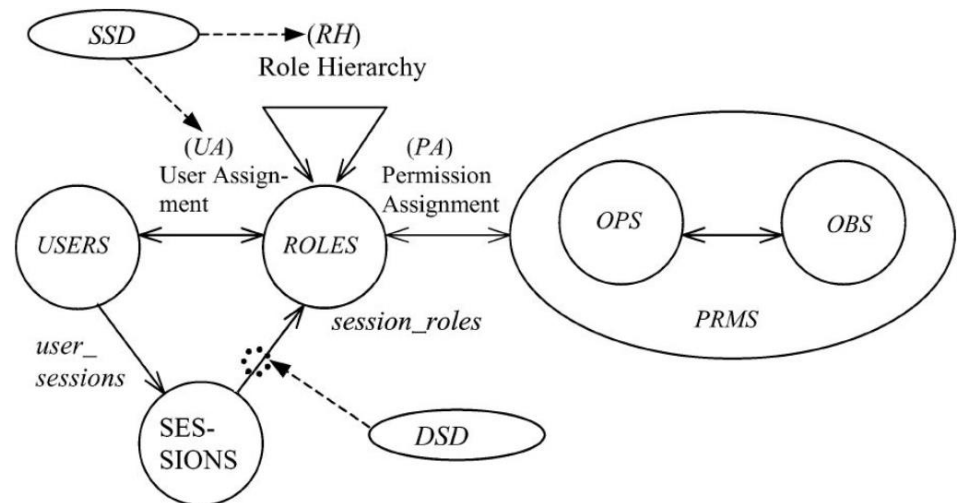
State of the art
Summary

Model	Concepts	Layer of abstraction
MAC	Subject, object, action	Application layer
DAC	Subject, object, action	Application layer
RBAC	User, role, object, action, permission, role hierarchy, SoD, session	Application layer User and role defined at the business layer
ABAC	User, subject, permission, attribute	Application layer User exists at the business layer and is realised by the subject
TRBAC	Task, user, temporal information, role, object	Application layer derived from the business layer
ORBAC	Subject, rights, object, autorisation, obligation, condition, attribute	Concrete layer (application) and Abstract layer (business)

Application Layer

↓

Business Layer

All models and methods mainly aim at supporting IT managers

No model or method allows a full alignment between the business and the application layer

No model or method addresses the access rights management through the responsibility

Governance needs

Definitions

Corporate governance
- Directs, evaluates, monitors the achievement of the business goal
- Dictates the responsibilities of the board

IT governance
- Defines the strategy for using IT
- Provides specific requirements

Business/IT alignment
- Extend to which business and IT strategy are mutually supported
- Use of IT contributes to the performance of the organisation

Governance needs
Analysed frameworks

COBIT 4.1

- 34 IT controls associated to a RACI chart

ISO/IEC 38500:2008

- High level corporate governance of ICT – Principle 1: Responsibility

ISO/IEC 27000 Family

- IT security management and governance – Best practices for access rights management

BASEL II

- Financial system protection – Addresses the responsibilities of the business roles

Sarbanes–Oxley Act

- Financial reporting – Responsibilities of the principal financial officer or officers

Governance needs
Summary

	COBIT	ISO/IEC 27000	ISO/IEC 38500	BASEL II	SOX
Responsibility defined by Governance rules	X		X	X	X
Responsibility generates responsibility	X	X	X	X	
Responsibility composed of accountabilities	X	X	X	X	X
Responsibility concerns tasks	X	X	X	X	X
Responsibility needs capabilities	X		X	X	X
Responsibility needs access rights	X	X			X
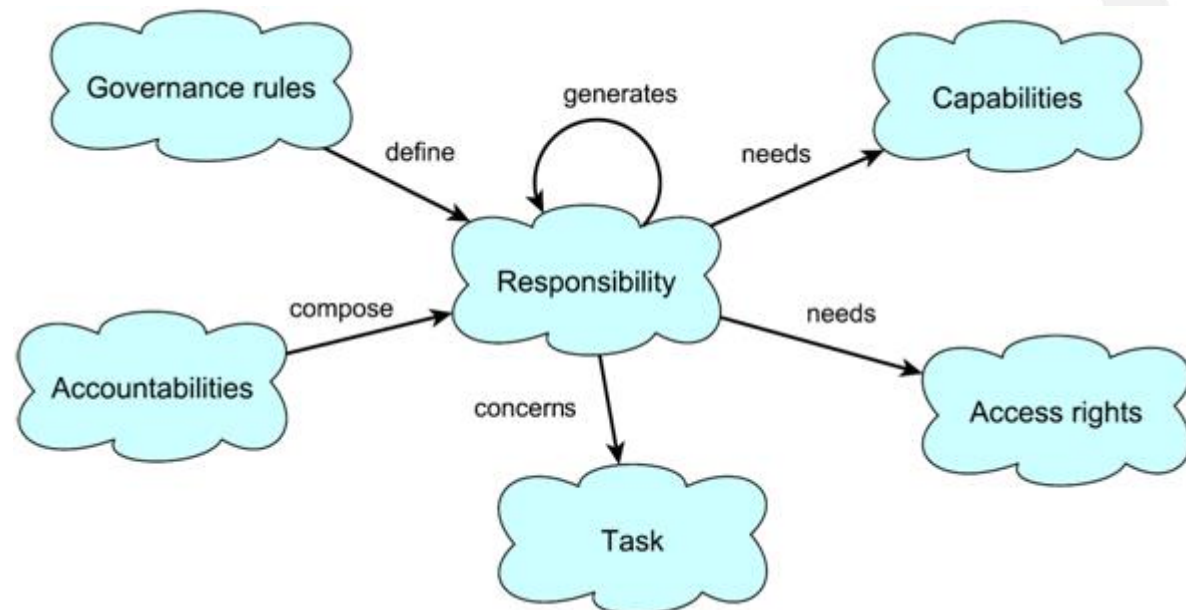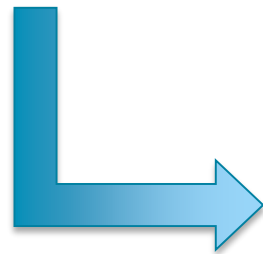
State of the art
Access Control Models and Governance needs
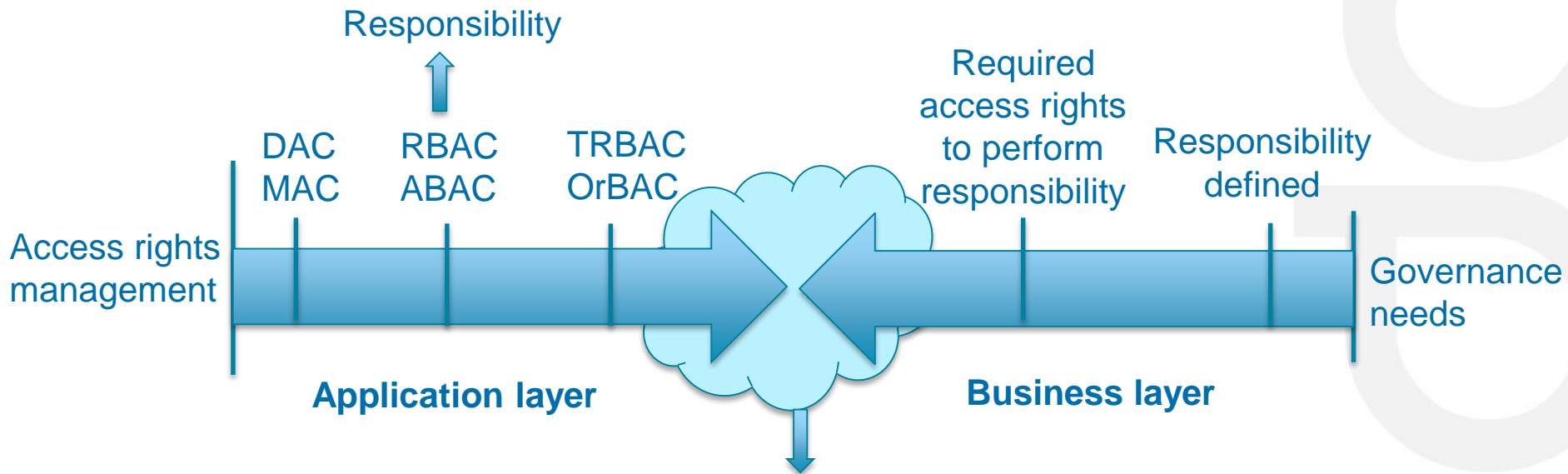
- **Access rights management tends to consider business concepts**
- **Governance needs require to provide accurate access rights**
- **Responsibility is perceived as an hyphen between both worlds**

Research questions and objectives

- Considering the corporate and IT governance needs, what are the concepts which constitute the core of the employee responsibility and how these concepts may be associated in a dedicated Responsibility metamodel?

  → Responsibility metamodel

- How may business/IT alignment be improved considering the responsibility, in the context of enterprise architecture models, and for the field of access rights management?

  → ArchiMate extension with the Responsibility metamodel

- How may responsibility be mapped with the role based access control model and how does this mapping enhances the engineering of roles?

  → Method for the access rights management

Overview

Responsibility metamodel
Introduction

Method

- Review of the concepts from the literature
- Concepts definition
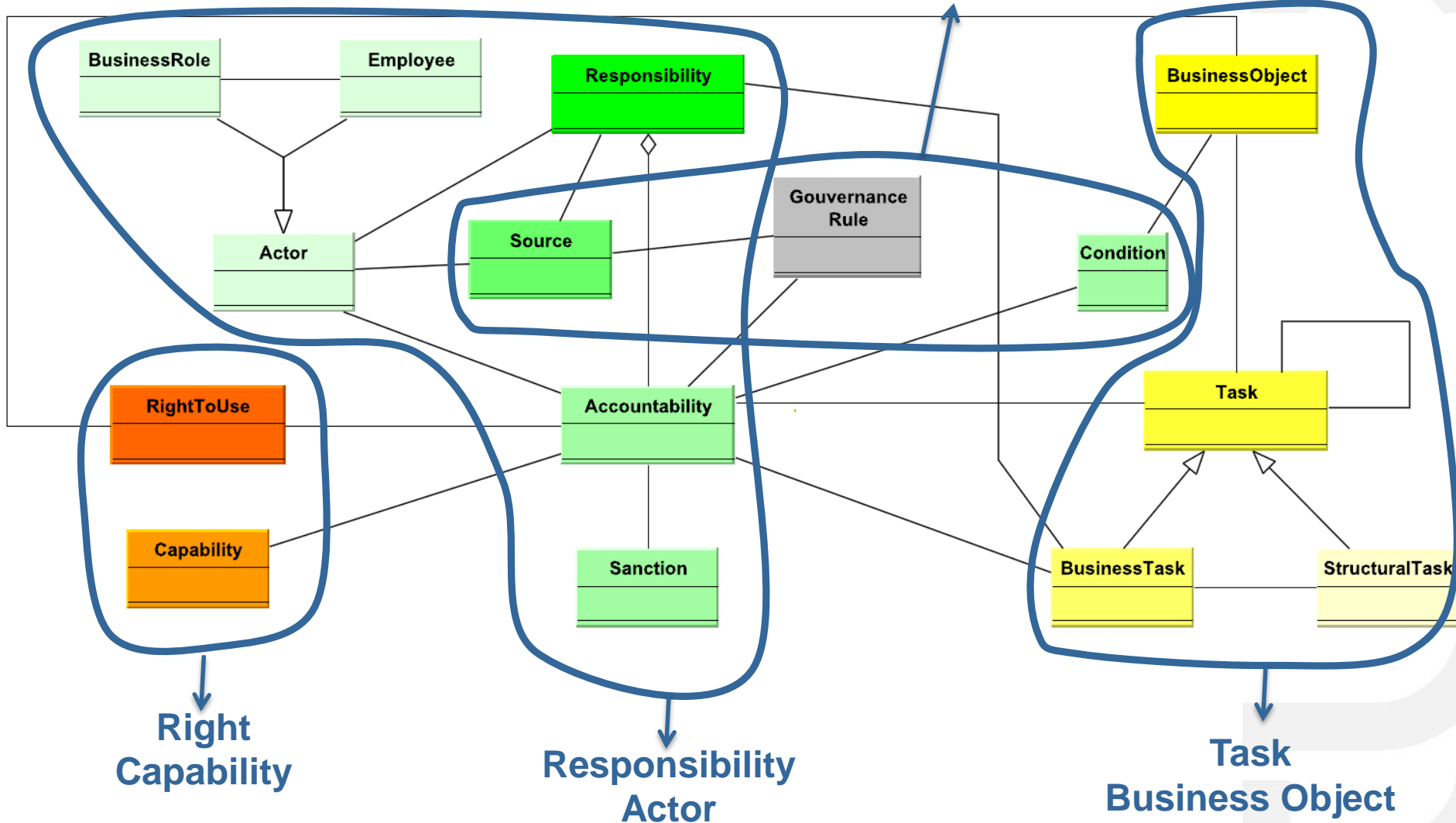- Integration in the Responsibility metamodel

Limitations

- *Responsibility relates to business tasks*
- *Responsibility are those of employees from bureaucratic organisations*
- *Responsibility metamodel kept simple*

Responsibility metamodel

Introduction

Responsibility metamodel
Task and Business object

Task

- Corresponds to a piece of work, or activity
- Contributes to the attainment of a goal
- May be defined through a procedure
- May be decomposed into sub–tasks
- May be of business or structural type
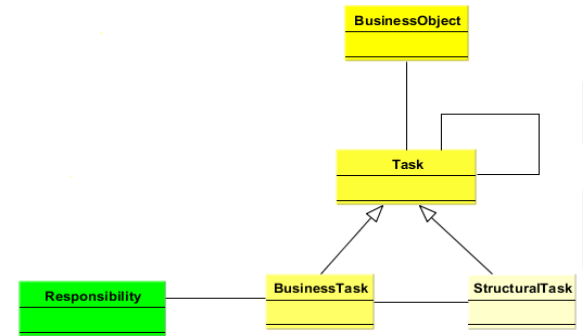
The *Task* is a complete and identifiable piece of work necessary to achieve a goal and which may or may not be defined through a procedure

The *Task* may be either a *business task* if it aims at achieving a business goal or a *structural task* if it aims at achieving a structural goal

Responsibility metamodel
Task and Business object

Business Object

- Is a piece of information or a document
- Is a passive element which has relevance from a business perspective
- Is a representation of organisational concept
- May be accessed by a business process
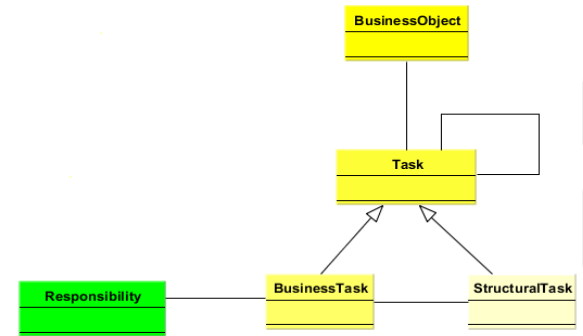
The *Business object* is a passive element (information or document) which has relevance from a business perspective and which may be used by one or many task(s)

Responsibility metamodel
Task and Business object

The **BusinessTask** *TreatPatient* uses the **BusinessObject** *PatientFile*

The **BusinessTask** *SeekInformationAboutPathology* uses the **BusinessObject** *PathologyKnowledgeBase*

The **StructuralTask** *ValidateTreatment* concerns the **BusinessTask** *TreatPatient*
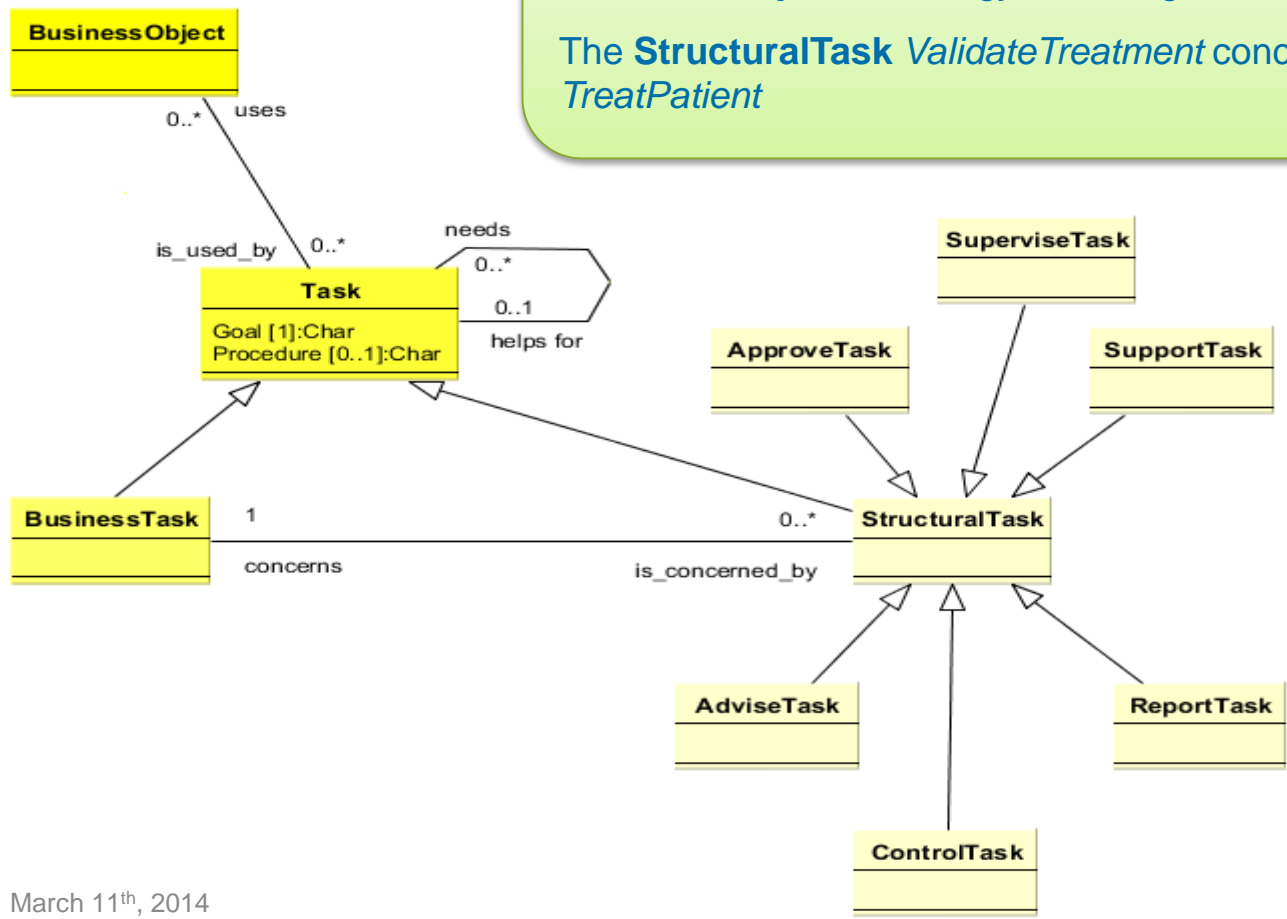
Responsibility metamodel
Responsibility, Accountability, Actor
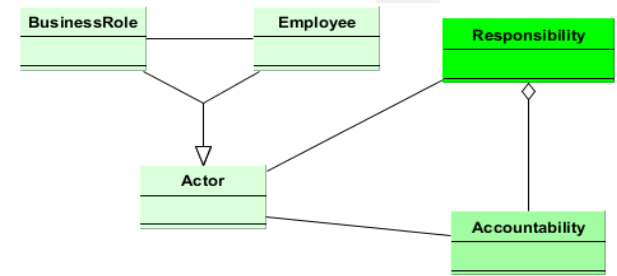
Responsibility

- Confers one or more obligations to an actor
- Provokes a formal duty to justify the performance of the obligation to someone else
- Concerns a task
- May originated from professional norms and frameworks

The *Responsibility* is a charge assigned to a unique actor to signify its accountabilities concerning a unique business task

Responsibility metamodel
Responsibility, Accountability, Actor
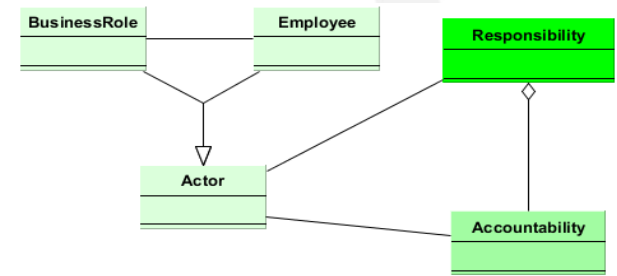
Accountability

- Is related to a task

- Aims to give account to someone else

- May result in sanctions

- May or may not apply under certain conditions

The *Accountability* is an element which is part of a unique responsibility and which represents an obligation of an actor to achieve the goal, or to perform the procedure of a task, and the justification that it is done to someone else, under threat of sanction

Responsibility metamodel
Responsibility, Accountability, Actor

Actor

- Active entity which carries out tasks to achieve goals by exercising its know-how
- May be a business role or an employee (who may play the business role)
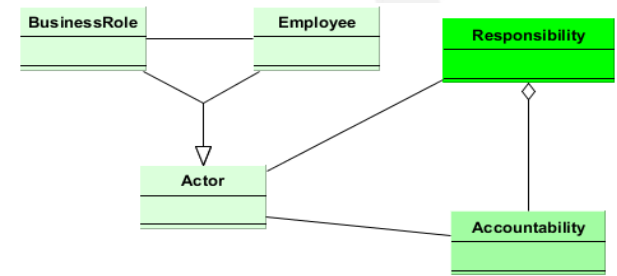
Employee

- Represents human entity

Business role

- Entity which may be associated to the realisation of a behaviour
- Is played by an employee and may be associated to a stuctural position in the organisation

The *Actor* is an active entity which is assigned a set of responsibilities and that may check accountability

- The *Business role* is a type of actor which represents a set of employees who share common characteristics
- The *Employee* is a type of actor which represents a human entity which may or may not play one or more business roles

Responsibility metamodel
Responsibility, Accountability, Actor
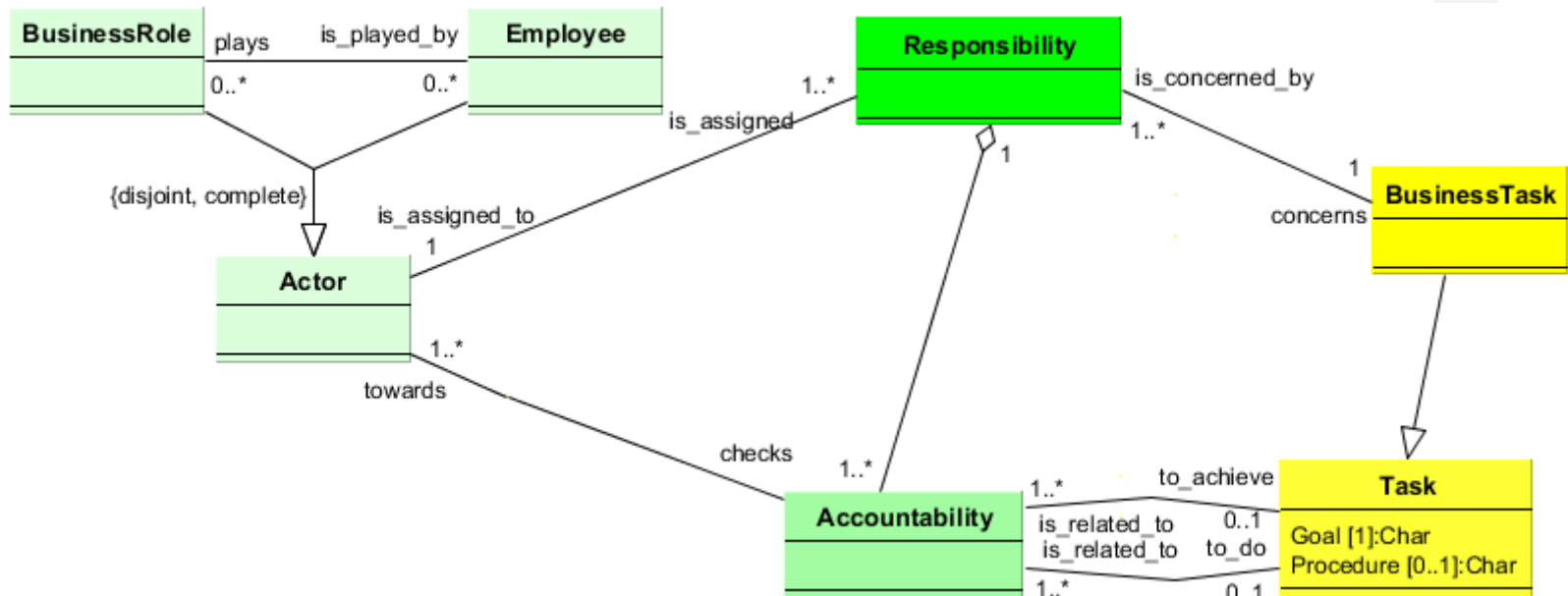
Alice plays the **BusinessRole** of *IT specialist* and is assigned to the **Responsibility** which aggregates the **Accountability to_do** *UpdatePathologyKnowledgeBase*

The *DoctorGeneral* is assigned to the **Responsibility** which aggregates the **Accountability to_achieve** *TreatPatient*

Responsibility metamodel
Capability and Right
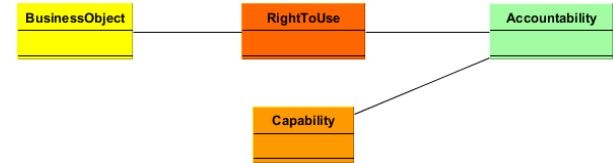
Capability

- Facilities required by an accountability and intrinsic to the actor
- Corresponds to education, experience, knowledge, authority, ability,….

RightToUse

- Facilities required by an accountability and provided by the company
- Corresponds to the permission to access to business object

The *Capability* represents the qualities, the skills or the ressources intrinsic to the actor and which are required to perform one or several accountability(ies)

The *RightToUse represents an authorisation to perform an operation on a business object which is required to perform one or several accountability(ies)*

Responsibility metamodel
Sanction, Condition, Governance rules and Source
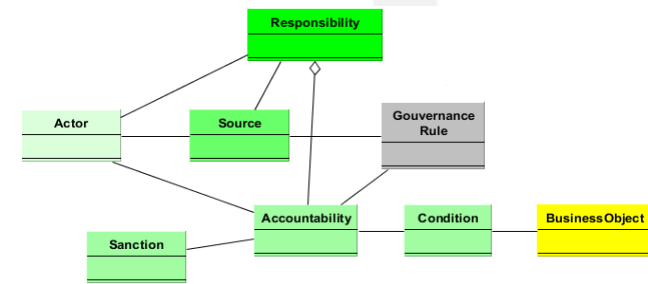
Sanction
- Consequences resulting to the appreciation of the achievement of an accountability
- May be positive or negative

Condition
- Rules which governs the existence of the accountabilities
- Is dependent on the context
- E.g., separation of duties, delegation, Chinese Wall security

Governance rule
- Provides high level rules which impact the elaboration of the responsibilities
- Expresses conditions over the accountability
- E.g., Delegation rule, responsibility to manage responsibilities, etc.

Source
- Formal information
- Generates governance rules, responsibilities, actors

Responsibility metamodel
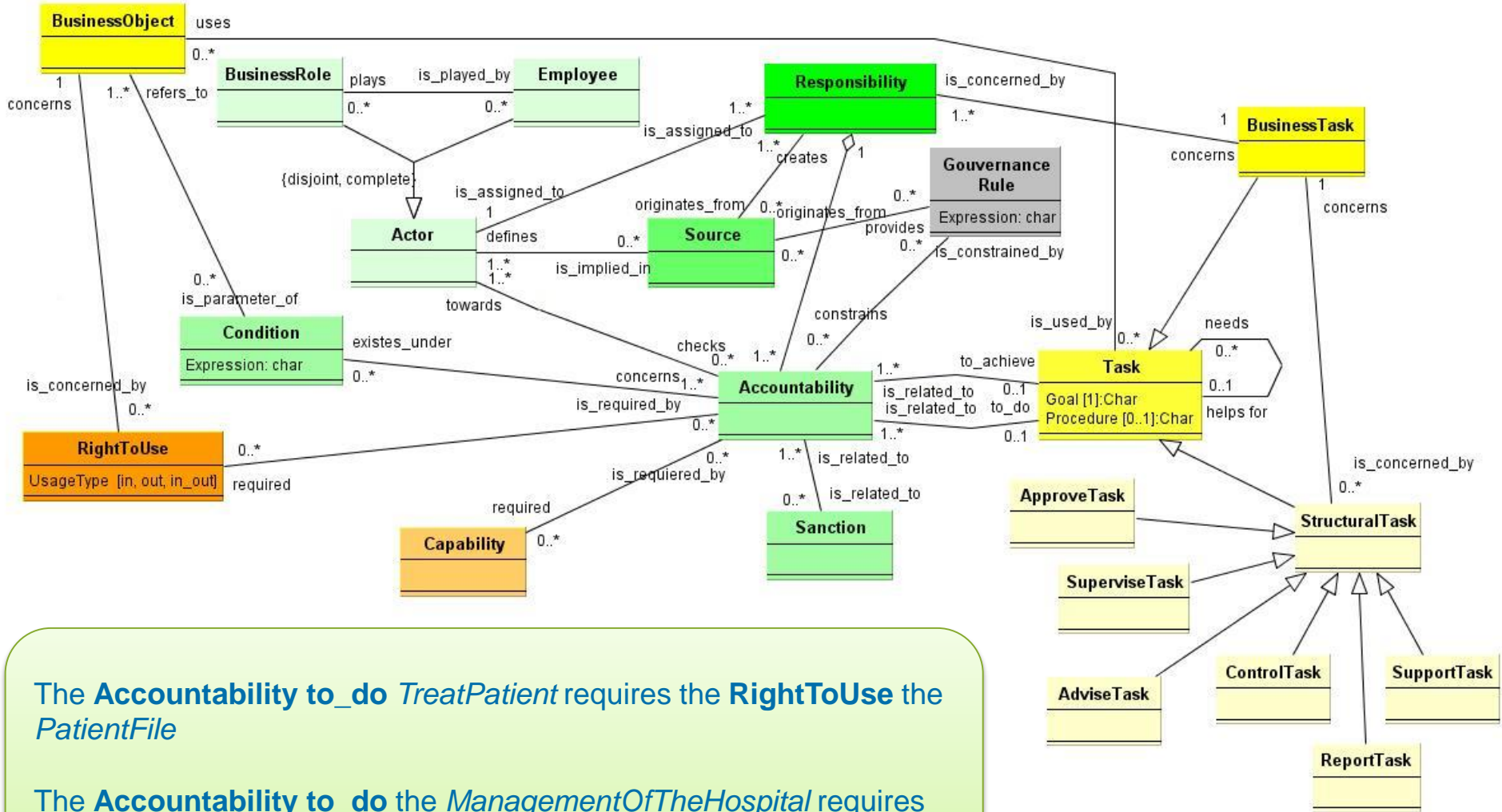
The **Accountability to_do** *TreatPatient* requires the **RightToUse** the *PatientFile*

The **Accountability to_do** the *ManagementOfTheHospital* requires the **Capability** to *Manage a team*

Responsibility metamodel
Healthcare case study
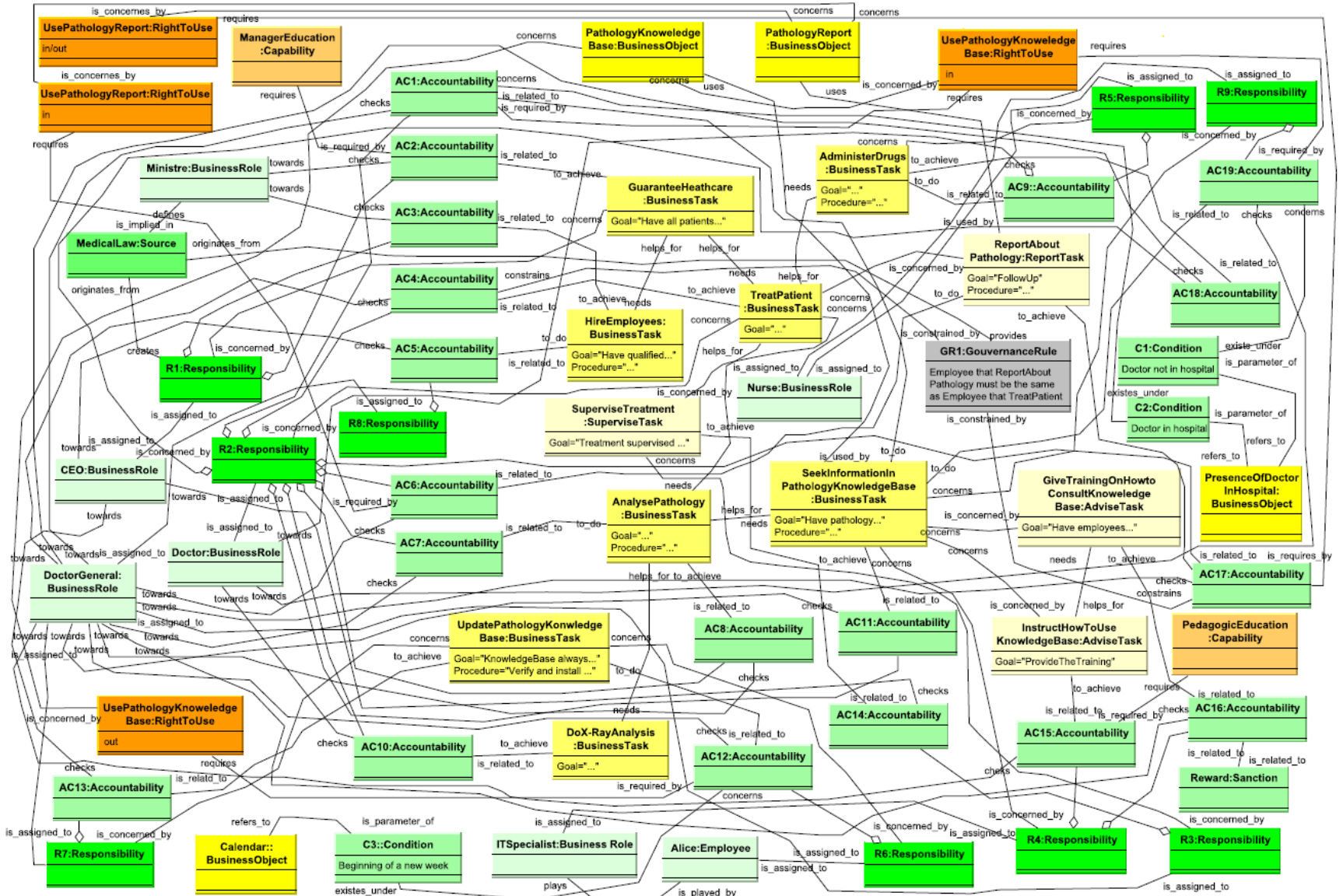
Overview

Responsibility – ArchiMate integration
Introduction

Enterprise Architecture modelling advantages

- Illustrates interrelations between the concepts
- Provides views understandable by all stakeholders
- Supports the decision making

→ Access rights management not yet considered

Objectives

- Enrich the semantics of the ArchiMate business concepts using the responsibility for:
  - Refining the business actor's responsibilities
  - Assigning access rights required to perform the accountabilities
- Support the creation of viewpoints related to the access rights management

Why ArchiMate ?

Responsibility – ArchiMate integration
ArchiMate and ArchiMate motivation extension

3 aspects:
Information – Behaviour – Structure

Business Layer

© The Open Group
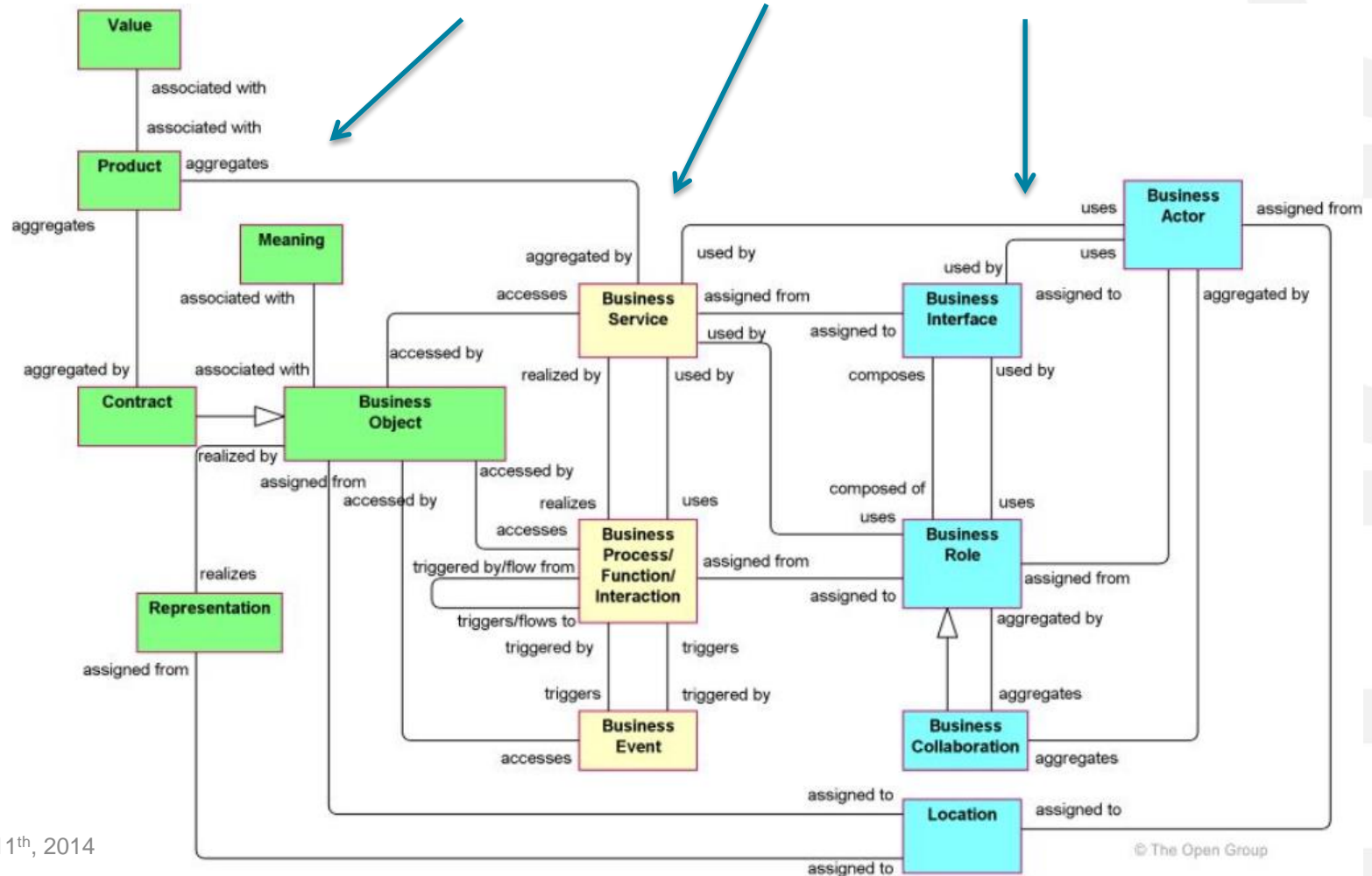
Responsibility – ArchiMate integration
ArchiMate and ArchiMate motivation extension
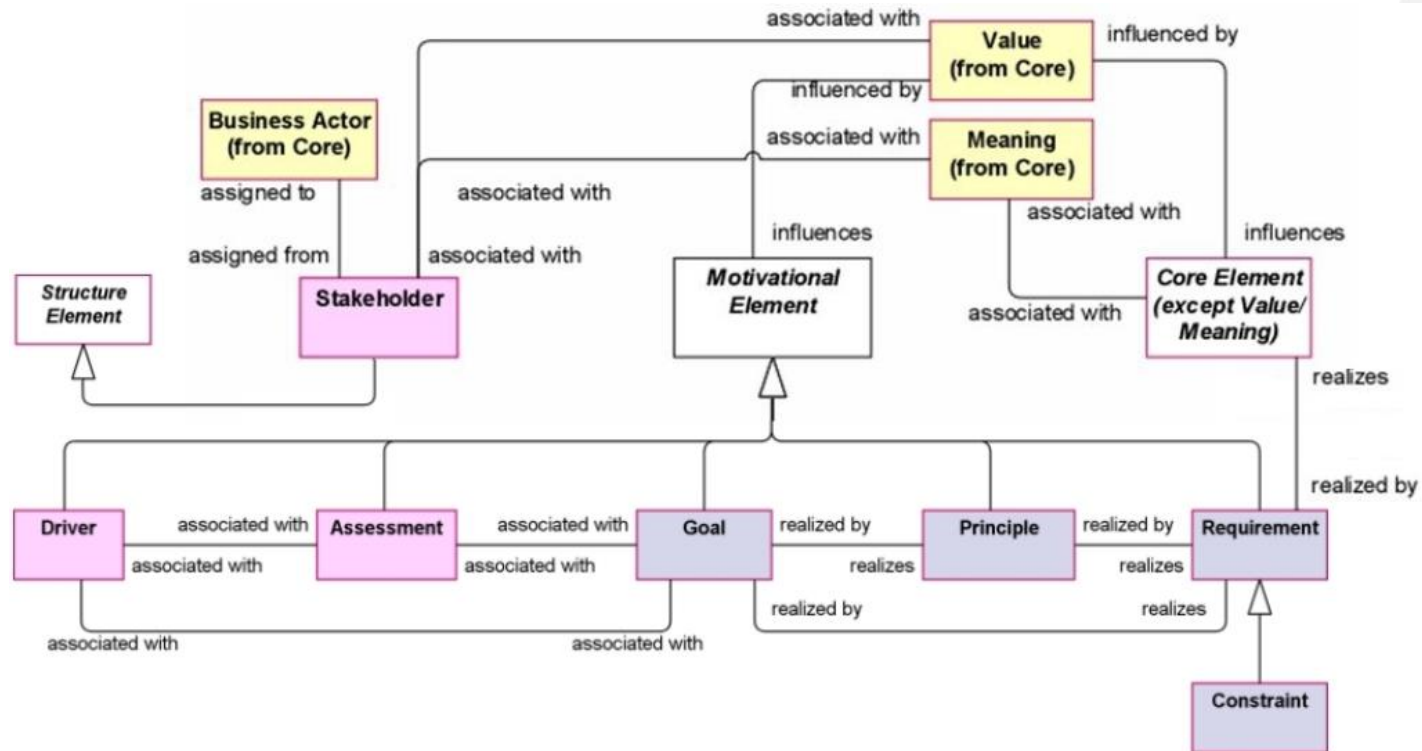
The motivation model allows expressing that:

- a motivation element influences the value concept associated to a core element
- a motivation element of type requirement must be realised by a core concept

Responsibility – ArchiMate integration

ArchiMate metamodel
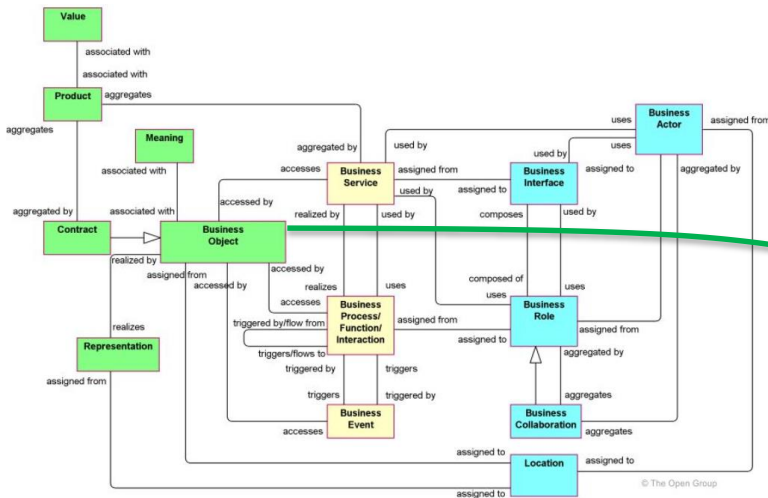
Responsibility metamodel

n-m mapping

1-1 mapping

No mapping
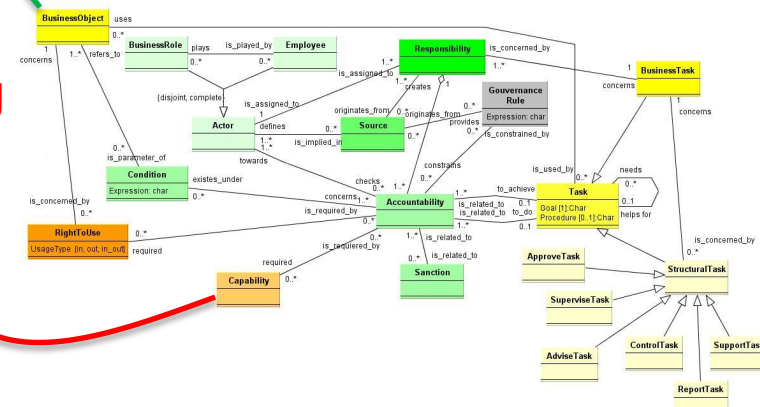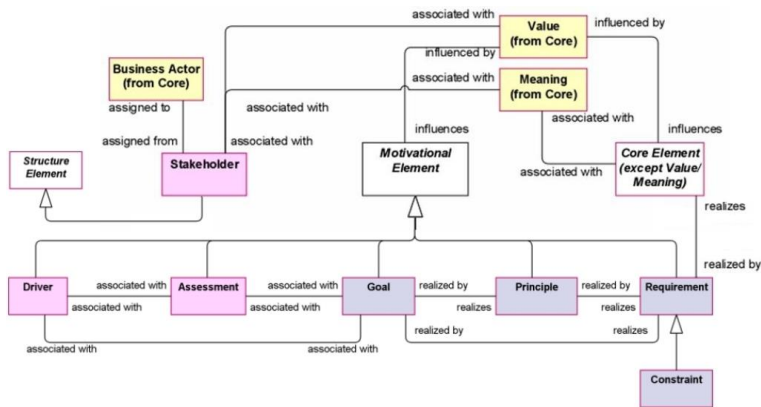
Responsibility – ArchiMate integration

ArchiMate metamodel

Responsibility metamodel
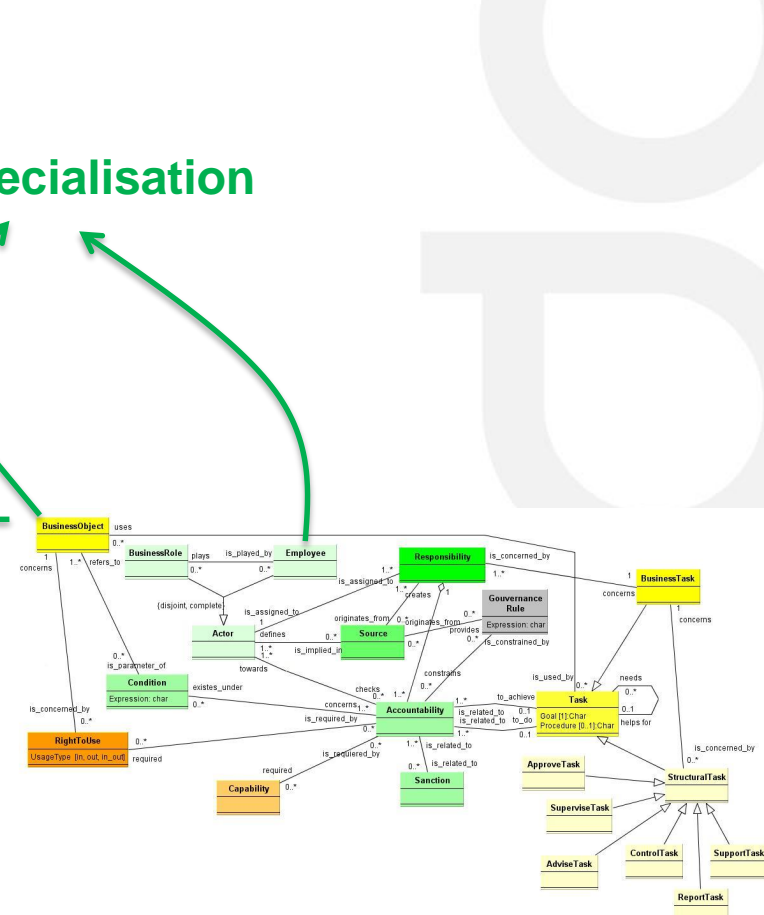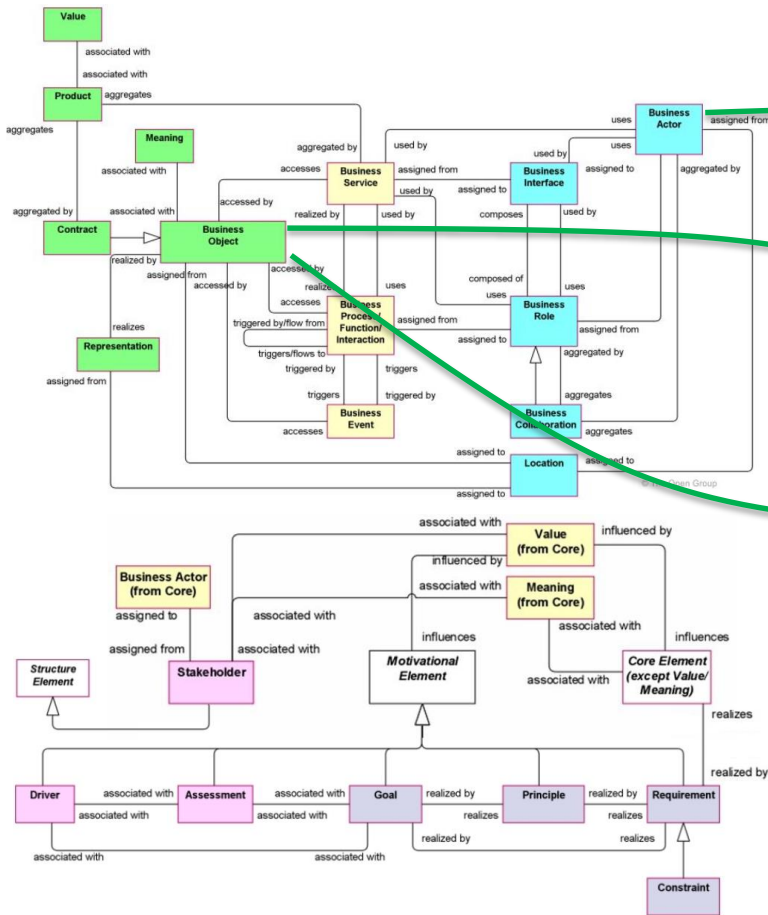
specialisation

1-1 mapping

merge

Responsibility – ArchiMate integration
Example of mapping and integration

Responsibility – Business role

- *Responsibility* **is a charge assigned to a unique actor** *to signify its accountability concerning a unique business task*

- *Business role corresponds to the* **responsibility for performing specific behaviour, to which** *an* **actor can be assigned**

→ 1:1 mapping with conflict between both concepts such that the responsibility is a specialisation of the business role

ReMMo Business Object – ArchiMate Business Object

- *The ReMMo business object is* **a passive element** *(information or document) which has* **relevance from a business perspective** *and which may be used by one or many task(s).*

- *The ArchiMate business object is defined* **as a passive element that has relevance from a** **business perspective**

→ 1:1 mapping without conflict between both concepts such that both concepts of business object are merge in a single one in the integrated metamodel

Responsibility – ArchiMate integration
Mapping and integration summary

Responsibility element	ArchiMate element	Mapping	Integration rule	Integrated element
Business Object	Business Object	1:1	Merge	Business Object
Task	Business Process	1:1	Specialisation	<<Task>>
R_Business Role	Business Role	1:1	Specialisation	<<R_BusinessRole>>
Responsibility	Business Role	1:1	Specialisation	<<Responsibility>>
Employee	Business Actor	1:1	Specialisation	<<Employee>>
Accountability	Business Function	1:1	Specialisation	<<Accountability>>
Right To Use	Access association	1:1	Specialisation	<<RightToUse>>
Sanction	-	-	Addition of attribute	<<Accountability>>, Sanction: Sanction description
Condition	-	-	Addition of attribute	<<Accountability>>, Condition: Condition description
Capability	-	-	Addition of attribute	<<Accountability>>, Capability: Capability description
Source	Driver	1:1	Specialisation	<<Source>
Governance Rule	Requirement	1:1	Specialisation	<<Governance Rule>>

Reminder: Healthcare case study
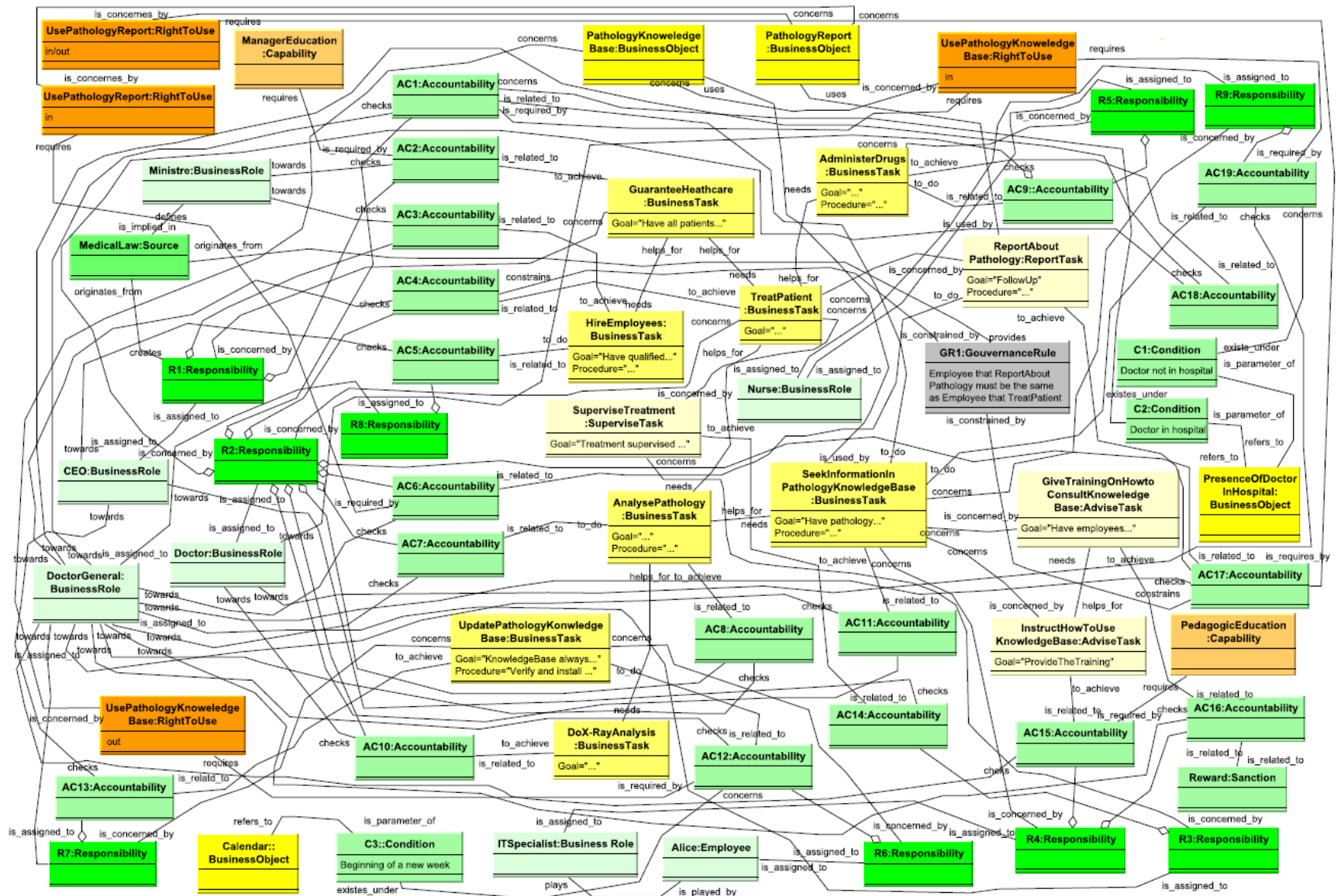
After integration with ArchiMate:
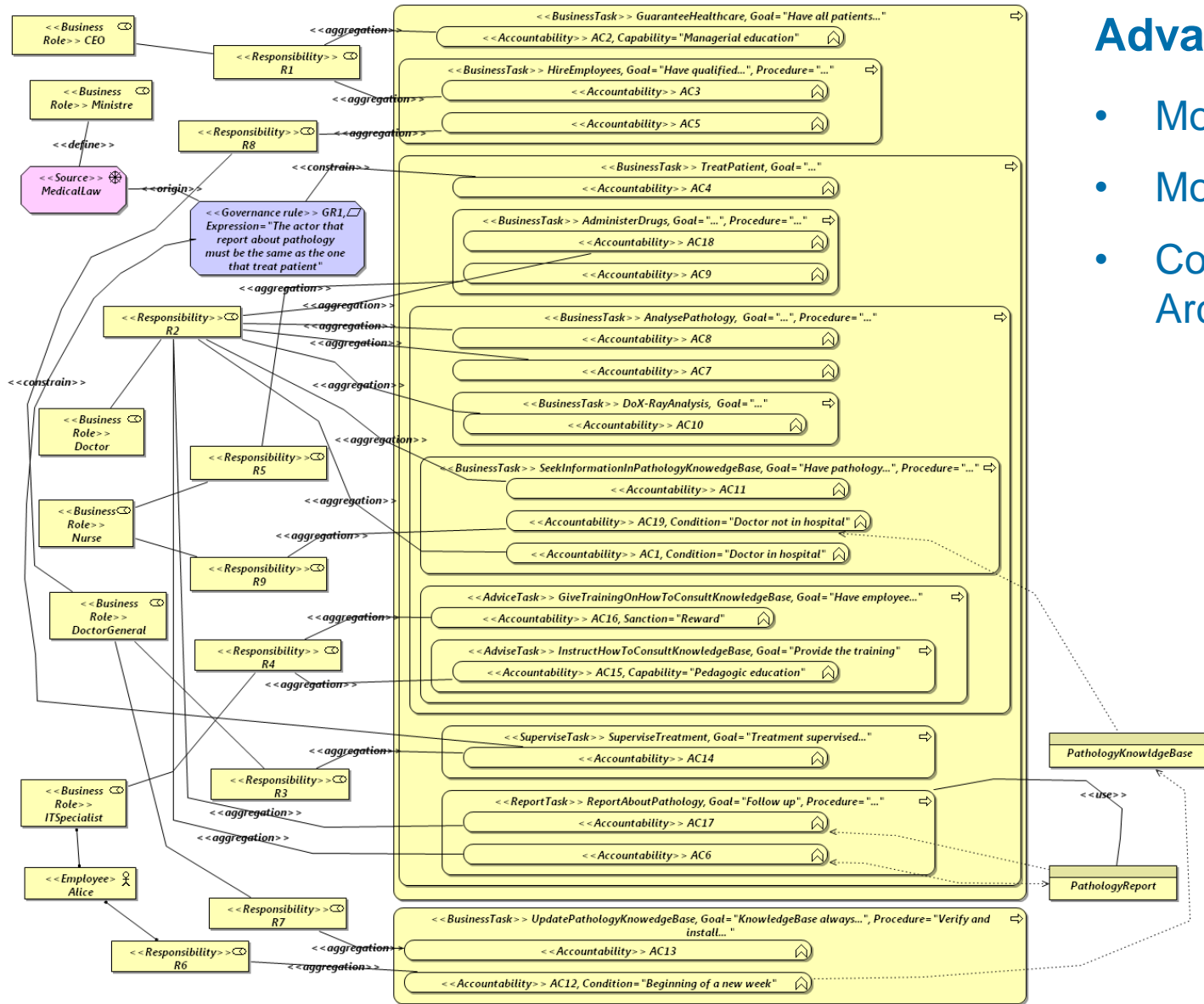
Advantages:

- More easily readable

- More comprehensible

- Conforming with ArchiMate formalism

Responsibility – ArchiMate integration
Case study at the Centre Hospitalier de Luxembourg (1)

Objectives of the case study:

- Evaluate the expressiveness of the Responsibility metamodel
- Illustrate how the integration of the Responsibility with the ArchiMate metamodel may be instantiated to a real case

Context

- Activity to provision the access rights to the patient's record according to the employee's role and the hospital specific access control model

Steps of the case study

- Analysis of the context and the scenarii for the access rights management
- Modelling of the tasks, responsibilities and roles following the scenarii
- Modelling of the scenarii using ArchiMate extended with the responsibility

Responsibility – ArchiMate integration
Case study at the Centre Hospitalier de Luxembourg (1)

Case study figures

- From January 2011 to January 2012
- 8 meetings of 2 hours with the Manager for the Application Support

Case study results

- 10 roles, 22 tasks, 27 responsibilities
- Possiblity to use ArchiMate extended with the Responsibility to model the solution designed by the hospital to access the patient's record

Feed-back from the Manager for the Applications Support

According to him, considering the concept of Responsibility:

- Could enhance the performance of the hospital
- Is appropriate to perform business/IT alignment

Overview

Responsibility alignment with RBAC
Method

Business Layer
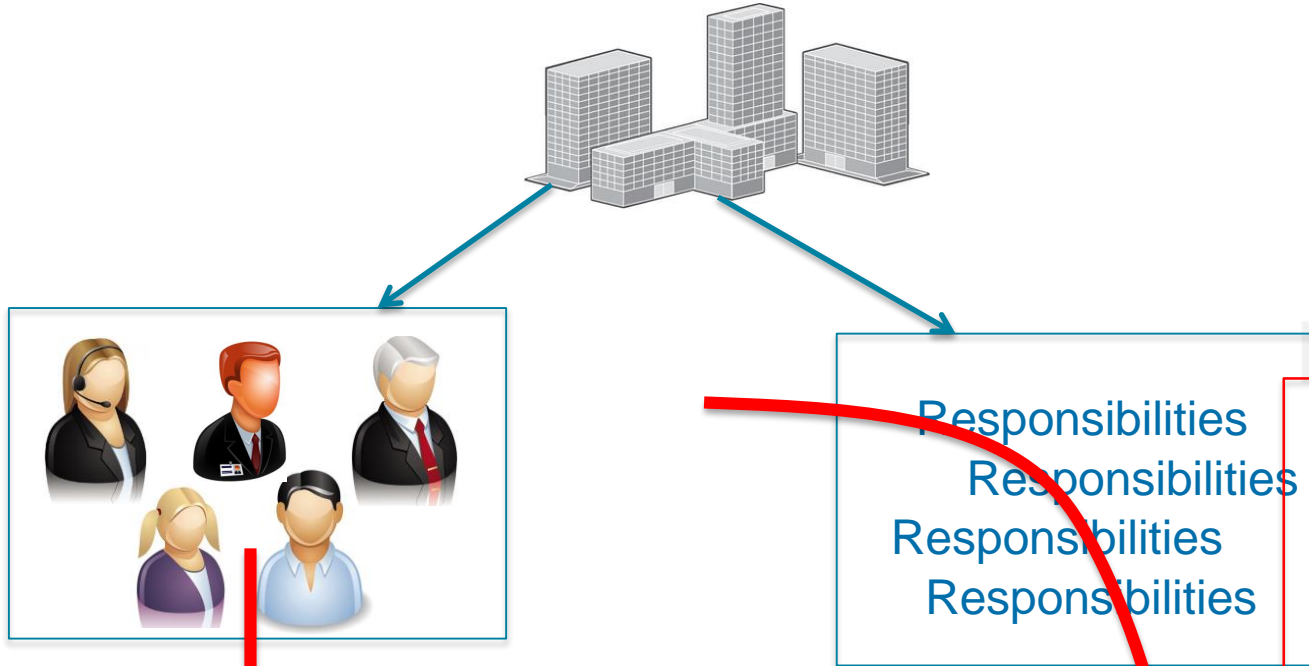
Application Layer

Responsibilities
Responsibilities
Responsibilities
Responsibilities
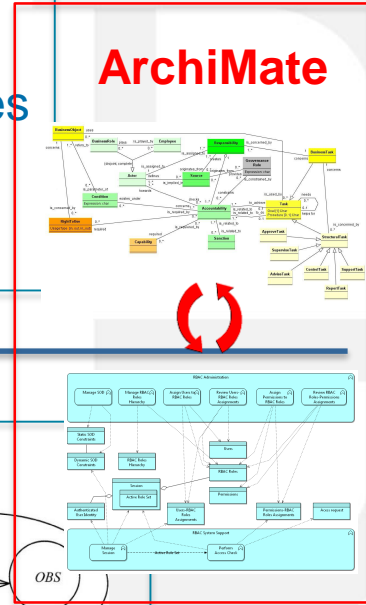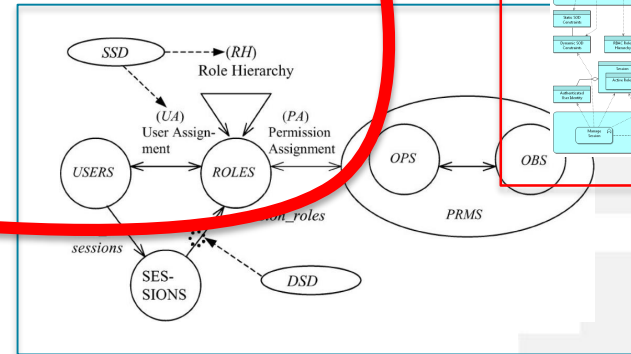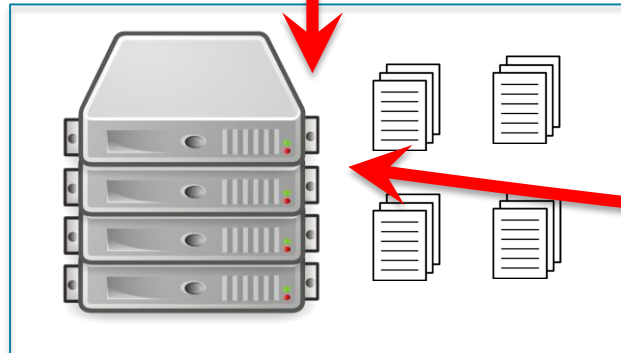
ArchiMate

Responsibility ArchiMate with RBAC
Existing *RBAC reference model* in ArchiMate (*Band (2011)*)
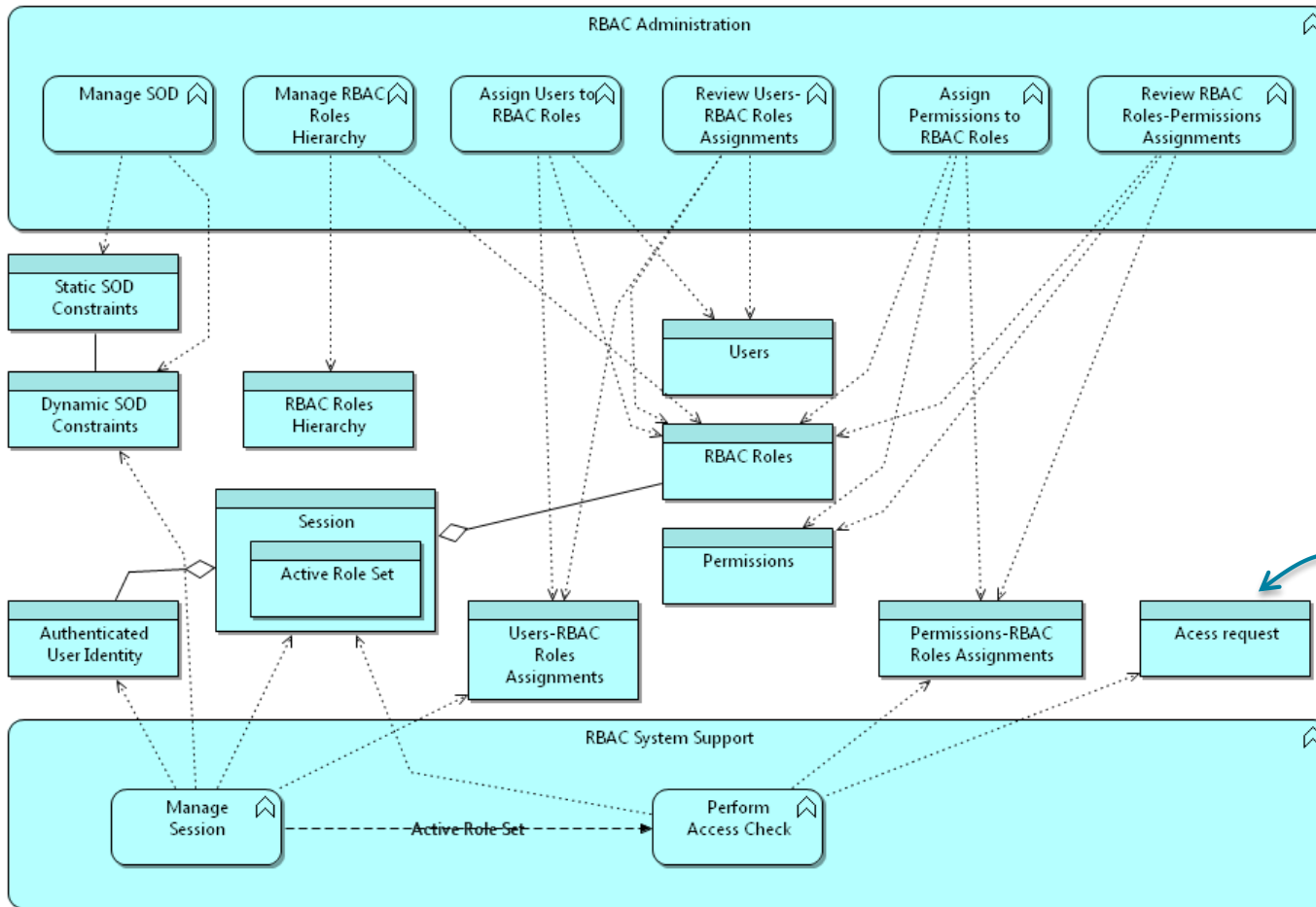
Application function: represents a behaviour element that groups automated behaviour which can be performed by an application component

Data object: represents a passive element suitable for automated processing

Responsibility ArchiMate with RBAC
Alignment between RBAC and the Responsibility metamodel

Summary of the
trace to associations
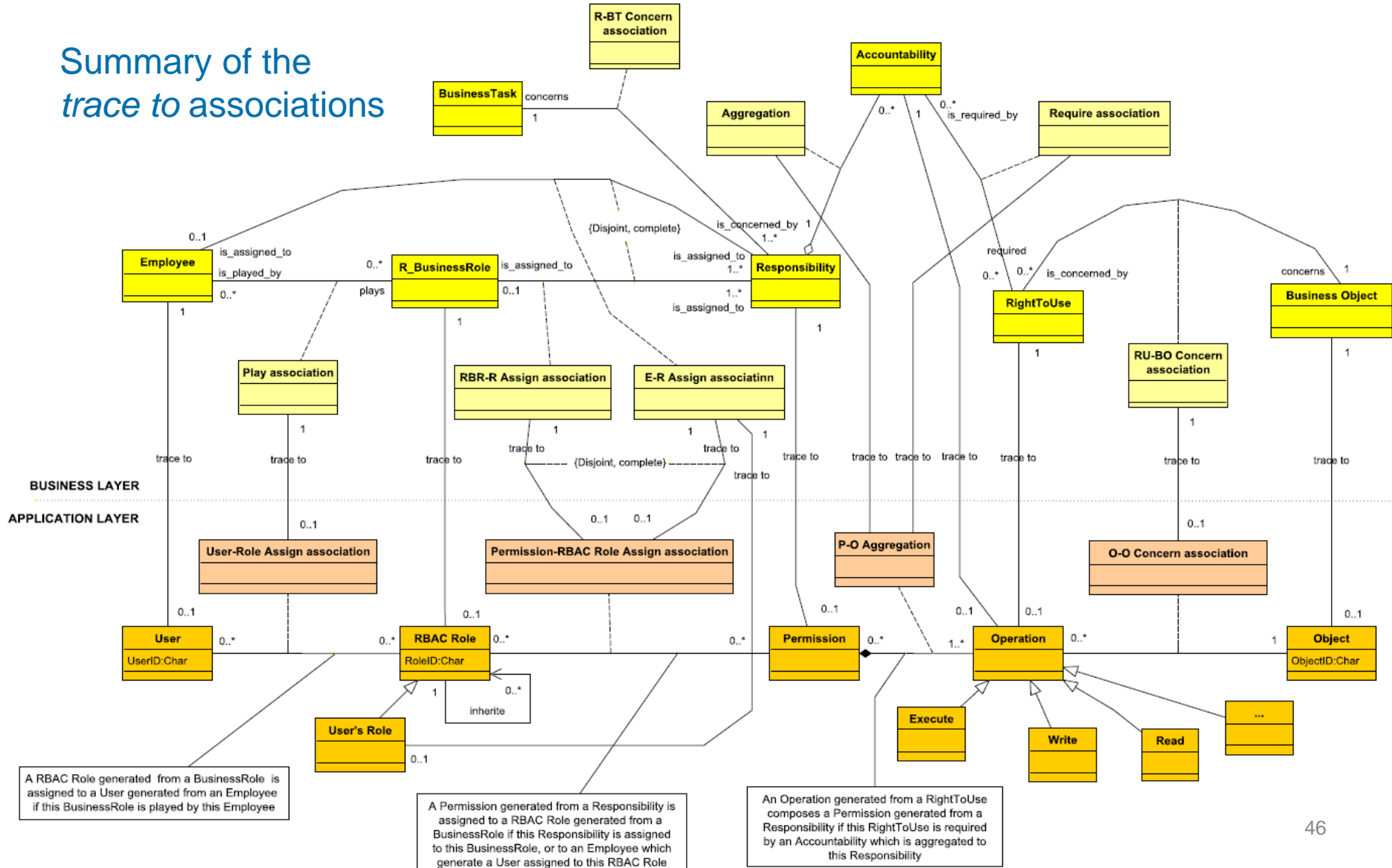
Responsibility ArchiMate with RBAC
Method to populate RBAC
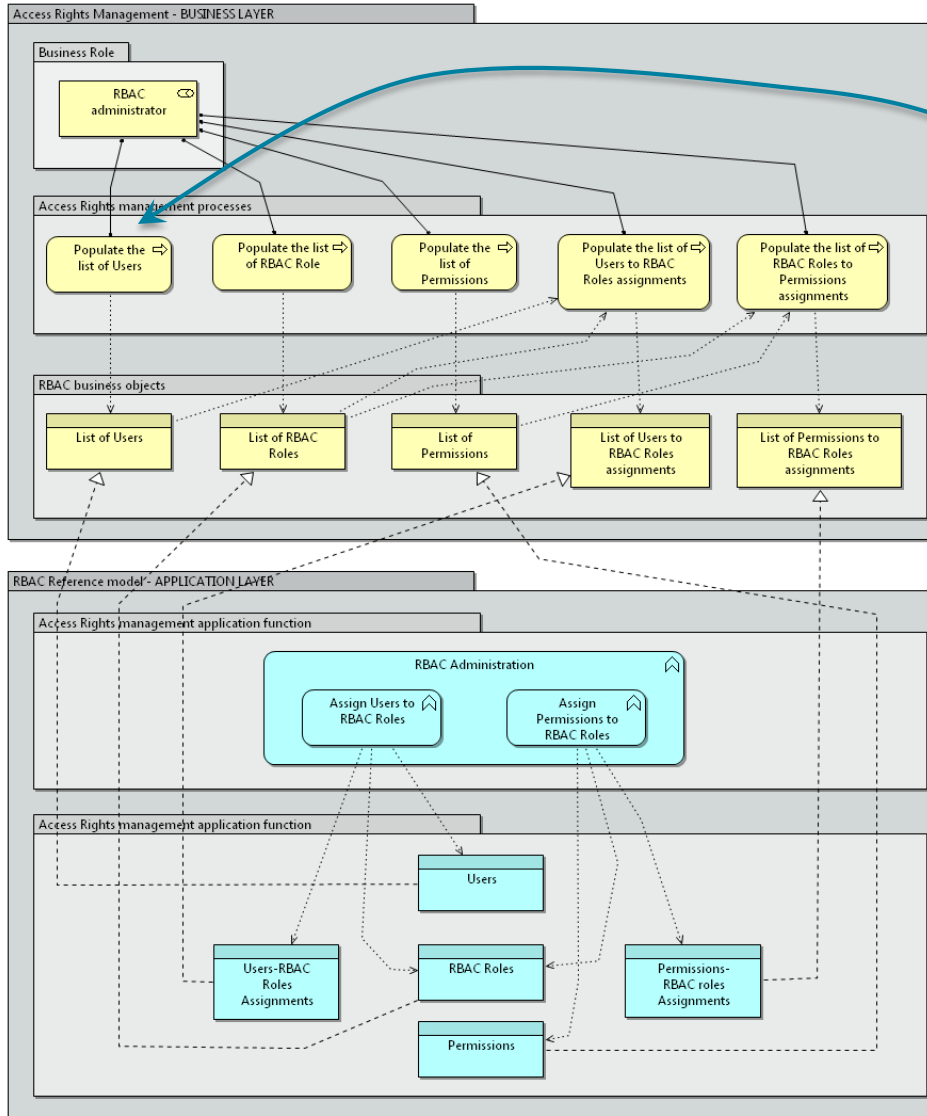
Business role: RBAC administrator

Business processes:

- *Populate the list of Users*
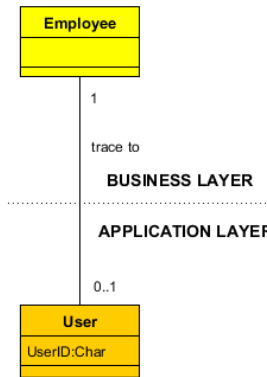
  - Collects the list of employees who need to access the information *system*
  - *From the responsibilities model in ArchiMate*
  - Output: Business object «*List of Users*»
  - List of users realized by data object *«Users»*

- *Populate the list of RBAC Roles*

- *Populate the list of Permissions*

- *Populate the list of Users to RBAC Roles assignments*

- *Populate the list of RBAC Roles to Permissions assignments*

Responsibility ArchiMate with RBAC
Case study at the Centre Hospitalier de Luxembourg (2)

Objectives of the case study:

- Evaluate how the integration of ArchiMate with the Responsibility metamodel enhances the definition of the access rights
- Evaluate how the responsibilities may be used to generate the RBAC roles and permissions

Context

- Definition of the permissions to be provisioned to the roles from the hospital reception

Steps of the case study

- Analysis of the existing access rights management in the hospital
- Engineering of the access rights really required by the business roles
- Analysis of the difference between the existing and the engineered rights.

Responsibility – ArchiMate integration
Case study at the Centre Hospitalier de Luxembourg (2)

Case study figures:

- From February to March 2012
- 4 meetings of 2 hours with the Manager of the Reception and the Competence manager

Case study results:

- 8 RBAC roles, 16 permissions, and 28 *assignements of permissions to RBAC roles*
- 7 over 8 business roles are assigned to not required permissions

Feed-back from the Department manager and the Competence manager

- The solution is accurate and suitable to align the access rights provided to the employees according to their real activities
- The usage of the Responsibility metamodel could be extended to other domains such as the alignment of the competences required to perform activities

Overview

Introduction

State of the art: Access Control Models and Governance needs

Responsibility metamodel

ArchiMate extension with Responsibility

Responsibility alignment with RBAC

Conclusions

Conclusions
Summary

- State of the art: Access Control Models and Governance needs
  - Access rights models/methods tend to consider business concepts (responsibility)
  - Governance requires the definition of responsibilities and associated access rights
  - 3 main designed artefacts:

1. **Responsibility metamodel**
2. **Responsibility extension of ArchiMate Business layer**
3. **Method for access rights management based on the Responsibility alignment with RBAC**

- Limitations
  - Evaluation mainly performed with case studies
  - Alignment only with RBAC model

Conclusions
Future works

Service system modelling

- Sustain the interoperability between access rights management solutions of services system

Agent's responsibility

- Agent's responsibility to be assigned dynamically depending on the agents capability and simultaneous assignments of access rights

ArchiMate evolution

- Continuation the integration of the Responsibility in next versions of ArchiMate
- Exploring the definition of the concept of capability in ArchiMate

Responsibility management tool

- Supporting tool for the management of the access rights using the method based on the Responsibility and the RBAC reference model

Thank you !

Questions ?

References

Feltus, C. (2008) , Preliminary Literature Review of Policy Engineering Methods - Toward Responsibility Concept, ICTTA 2008, Damascus, Syria.

Feltus, C., Petit, M., Building a Responsibility Model Including Accountability, Capability and Commitment, Fourth International Conference on Availability, Reliability and Security, 2009, Fukuoka, Japan

Feltus, C., Petit, M., Vernadat, F., Enhancement of CIMOSA with Responsibility Concept to Conform to Principles of Corporate Governance of IT, 13th IFAC Symposium on Information Control Problems in Manufacturing, 3-5/6/2009, Moscow, Russia.

C. Feltus, M. Petit, and E. Dubois, Strengthening employee's responsibility to enhance governance of IT: COBIT RACI chart case study. 1st ACM Workshop on Information Security Governance. ACM, New York, NY.

C. Feltus, M. Petit, and M. Sloman, Enhancement of Business IT Alignment by Including Responsibility Components in RBAC, 5 th Busital workshop, 2010, Hammamet, Tunisia.

Feltus, C., Petit, M., Vernadat, F., Refining the Notion of Responsibility in Enterprise Engineering to Support Corporate Governance of IT, 13th IFAC Symposium on Information Control Problems in Manufacturing, 3-5/6/2009, Moscow, Russia.

Feltus, Christophe. Aligning access rights to governance needs with the responsibility metamodel (ReMMo) in the frame of enterprise architecture.   Prom. : Petit, Michaël ; Dubois, Eric

Christophe Feltus, Eris Dubois, Michaël Petit, Conceptualizing a Responsibility based Approach for Elaborating and Verifying RBAC Policies Conforming with CobiT Framework Requirements, in Proceedings of the 3th International Workshop on Requirements Engineering and Law (RELAW10), Sydney, Australia. 2010. IEEE.

Christophe Feltus, Michaël Petit, Eric Dubois, ReMoLa: Responsibility Model Language to Align Access Rights with Business Process Requirements, in Proceedings of the 5th International Conference on Research Challenges in Information Science (RCIS), Guadeloupe – French West Indies, France. 2011. IEEE.

Cédric Bonhomme, Christophe Feltus, Michaël Petit, Dynamic Responsibilities Assignment in Critical Electronic Institutions - A Context-Aware Solution for in Crisis Access Right Management, in Proceedings of the 6th International Conference on Availability, Reliability and Security (ARES), Vienna, Austria. 2011. IEEE.

Christophe Feltus, Abdelasis Khadraoui, Anastasiya Yurchyshyna, Michel Leonard, Eric Dubois, Responsibility aspects in service engineering for eGovernment, in Proceedings of the Workshop of the 6th Interoperability for Enterprise Systems and Applications conference (I-ESA), Service Science and the next wave in Enterprise Interoperability, Valencia, Spain. 2012.

Michaël Petit, Christophe Feltus, François Vernadat, Enterprise Architecture Enhanced with Responsibility to Manage Access Rights - Case Study in an EU Institution, in Proceedings of The Practice of Enterprise Modeling - 5th IFIP WG 8.1 Working Conference (PoEM), Rostock, Germany. 2012.

Christophe Feltus, Eric Dubois, Erik Proper, Iver Band, Michaël Petit, Enhancing the ArchiMate® Standard with a Responsibility Modeling Language for Access Rights Management, in Proceedings of the 5th International Conference on Security of Information and Networks (SIN), Jaipur, Rajastan, India. 2012. ACM.

André Rifaut, Christophe Feltus, Improving Operational Risk Management Systems by Formalizing the Basel II Regulation with Goal Models and the ISO/IEC 15504 Approach, Regulations Modelling and their Validation & Verification (REMO2V'2006), an International Workshop of the 18th Conference on Advanced Information Systems Engineering (CAISE2006), pp. 831-837, 2006, Luxembourg, Grand-Duchy of Luxembourg.

Christophe Feltus, André Rifaut, *An Ontology for Requirements Analysis of Managers' Policies in Financial Institutions,* Interoperability for Enterprise & Software Applications (I-ESA2007), 2007, Madeira, Portugal.

Christophe Feltus, Michaël Petit, Georges Ataya, *Definition and Validation of a Business IT Alignment Method for Enterprise Governance Improvement in the Context of Processes Based Organizations*, 2008 Corporate Governance of IT International Conference, 1-2/12/2008,Wellington, New Zealand. Ed. Dr Brian Cusack, ISBN 978-1-877314-73-5.

Christophe Feltus, Christophe Incoul, Jocelyn Aubert, Benjamin Gâteau , Who Govern my Responsibilities? SIM: a Methodology to Align Business and IT Policies in the Industrial Field, 13th IFAC Symposium on Information Control Problems in Manufacturing, 2009, Moscow, Russia.

Christophe Feltus, Christophe Incoul, Jocelyn Aubert, Benjamin Gâteau, André Adelsbach, and Marc Camy, Methodology to Align Business and IT Policies: Use case from an IT Company, 1st International Workshop on Organizational Security Aspects (OSA 2009), an International Workshop of the Fourth International Conference on Availability, Reliability and Security ("ARES 2009 – The International Dependability Conference") IEEE, 2009, Fukuoka, Japan.

Abdelaziz Khadraoui, Christophe Feltus, Services Specification and Services Compliance, How to Consider the Responsibility Dimension?, in Journal of Service Science Research - "Challenges and Advances on Service Quality Aspects", Springer, volume 4, issue 1, pp. 123-142.

Benjamin Gâteau, Moussa Ouedraogo, Christophe Feltus, Guy Guemkam, Gregoire Danoy, Marcin Seredinsky, Samee U. Khan, Djamel Khadraoui, Pascal Bouvry, Adopting Trust and Assurance as indicators for the reassignment of responsibilities in Multi-agent Systems, Special issue "Intelligent Computing in Large-Scale Environments", The Knowledge Engineering Review (KER), Cambridge University Press (CUP), ISSN: 0269-8889, volume 30, issue 2.

Abdelaziz Khadraoui, Damien Nicolas, Christophe Feltus, Prosumer's Responsibilities?... On Stage to a Dedicated Framework for Services Sharing and Compliance in the Healthcare Domain. In Frameworks of IT Prosumption for Business Development, Ed. Małgorzata Pańkowska, 73-84 (2014), accessed August 12, 2013. doi:10.4018/978-1-4666-4313-0.ch006

B. Gâteau, C. Feltus, J. Aubert, C. Incoul, An Agent-based Framework for Identity Management: The Unsuspected Relation with ISO/IEC 15504, IEEE RCIS 2008, 3-6/6/2008, Marrakech, Morocco.