# ALIGNMENT OF REMMO WITH RBAC TO MANAGE ACCESS RIGHTS IN THE FRAME OF ENTERPRISE ARCHITECTURE

CHRISTOPHE FELTUS, ERIC DUBOIS, MICHAËL PETIT

LUXEMBOURG
INSTITUTE
OF SCIENCE
AND TECHNOLOGY

LI
ST

# OVERVIEW

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

- Introduction
- Responsibility metamodel
- ArchiMate extension with Responsibility
- Method for the access rights management
- Conclusions

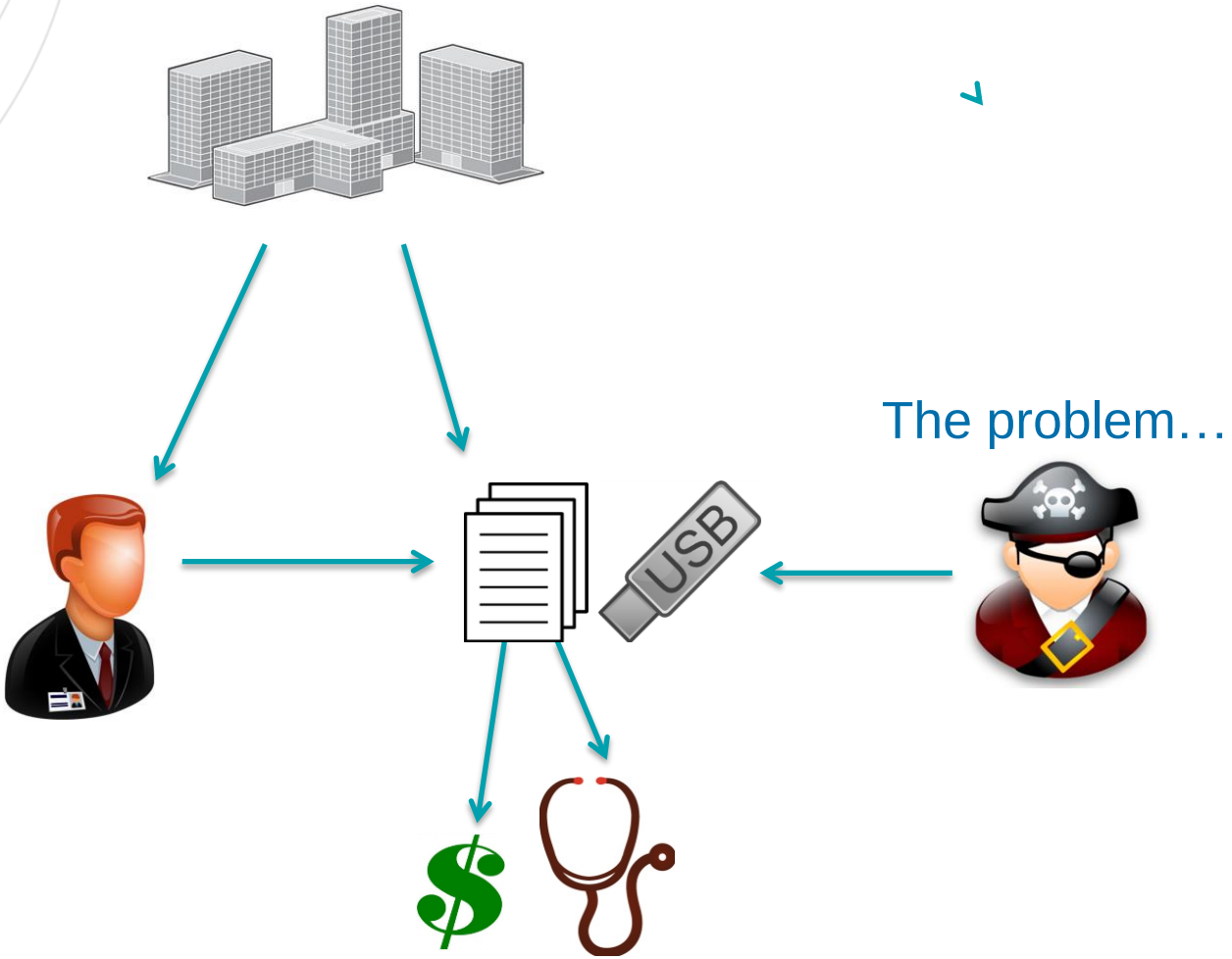
# OVERVIEW

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

- Introduction
- Responsibility metamodel
- ArchiMate extension with Responsibility
- Method for the access rights management
- Conclusions

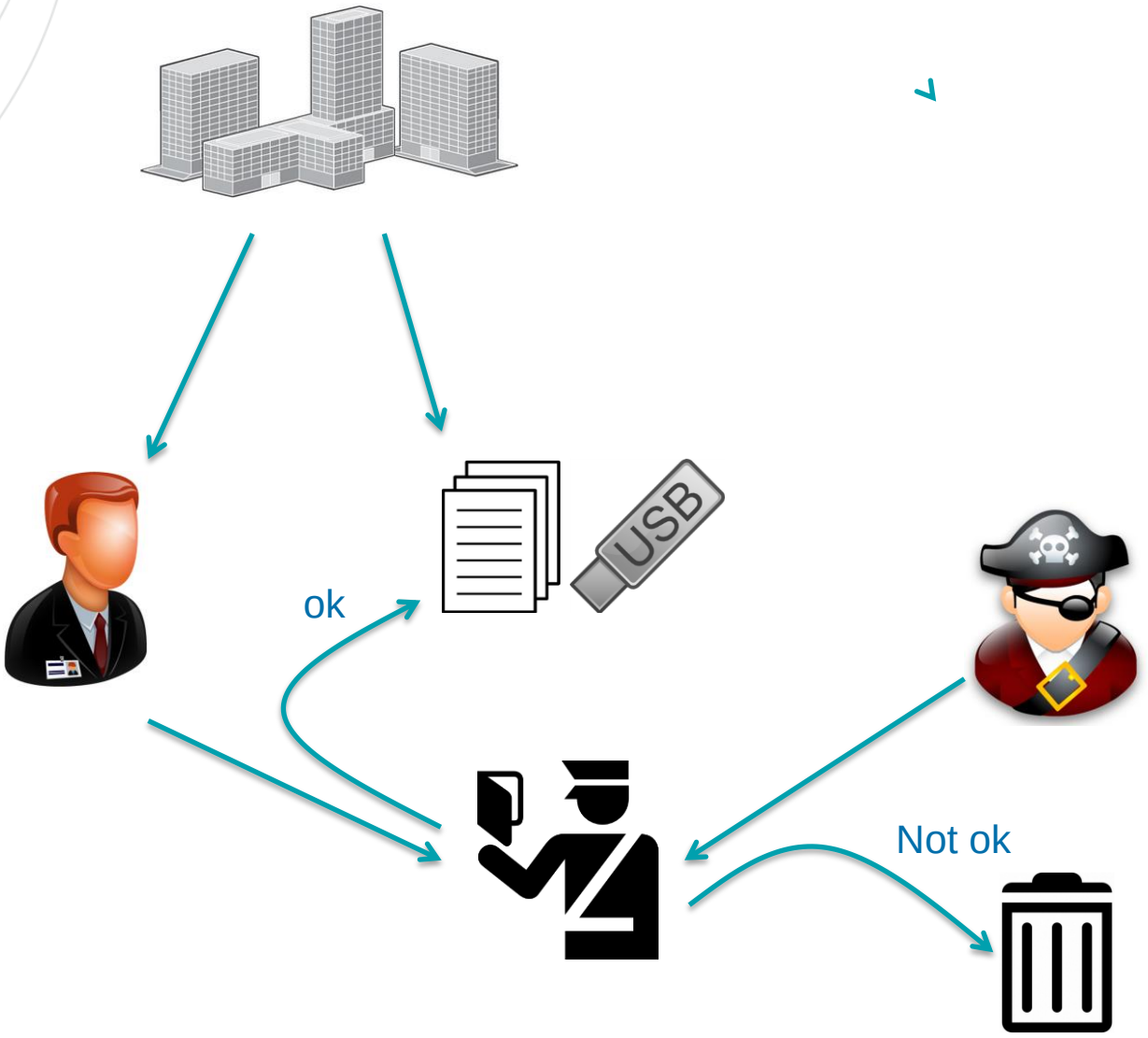
# INTRODUCTION

## Context



# INTRODUCTION

## Context



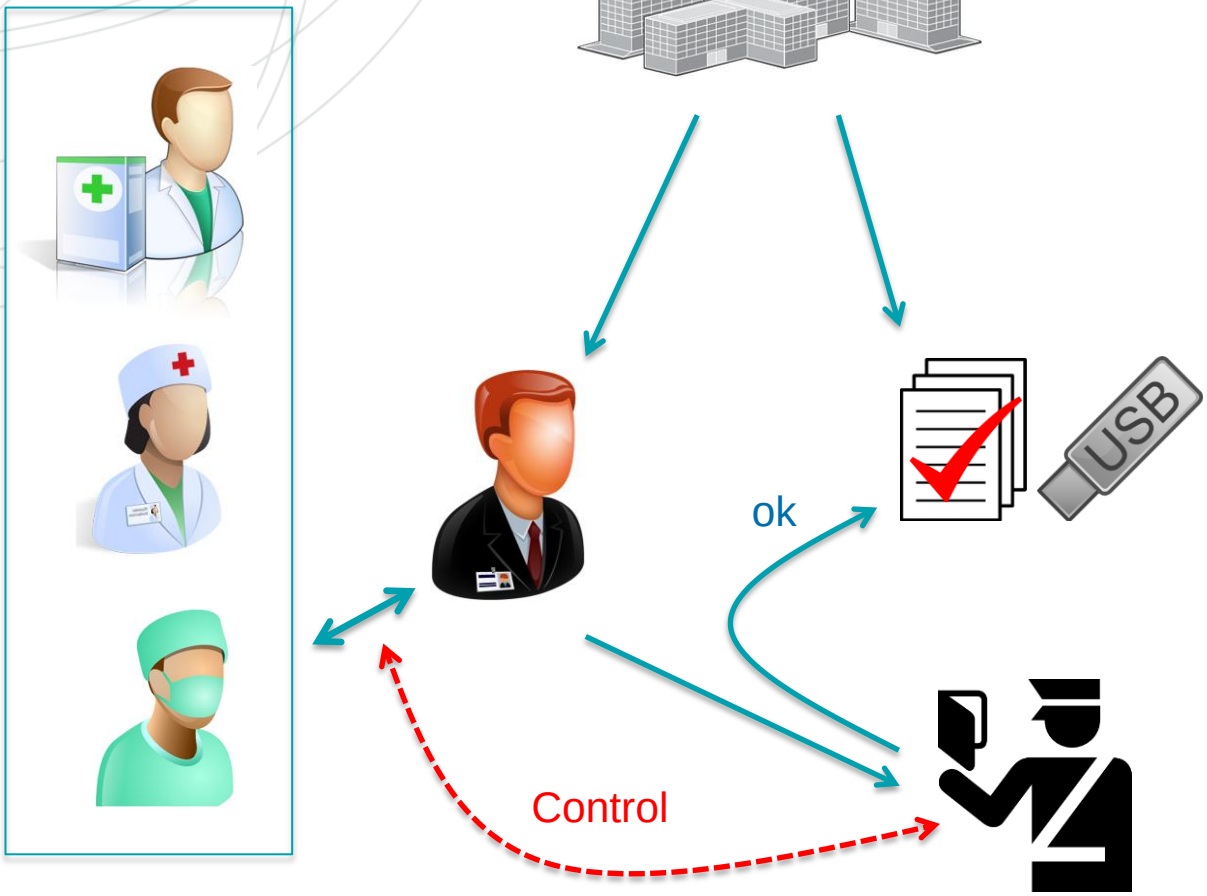
# INTRODUCTION



LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

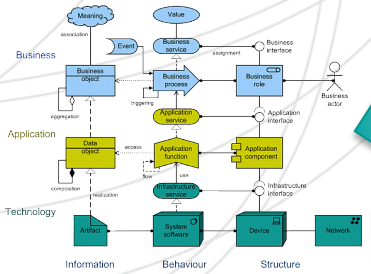
## Context

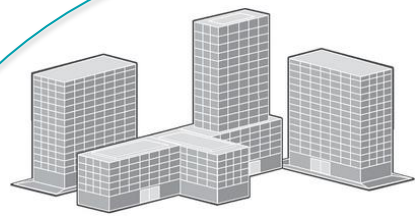
Roles

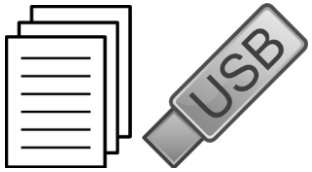


# INTRODUCTION

## Context






Enterprise Architecture

COBIT 5

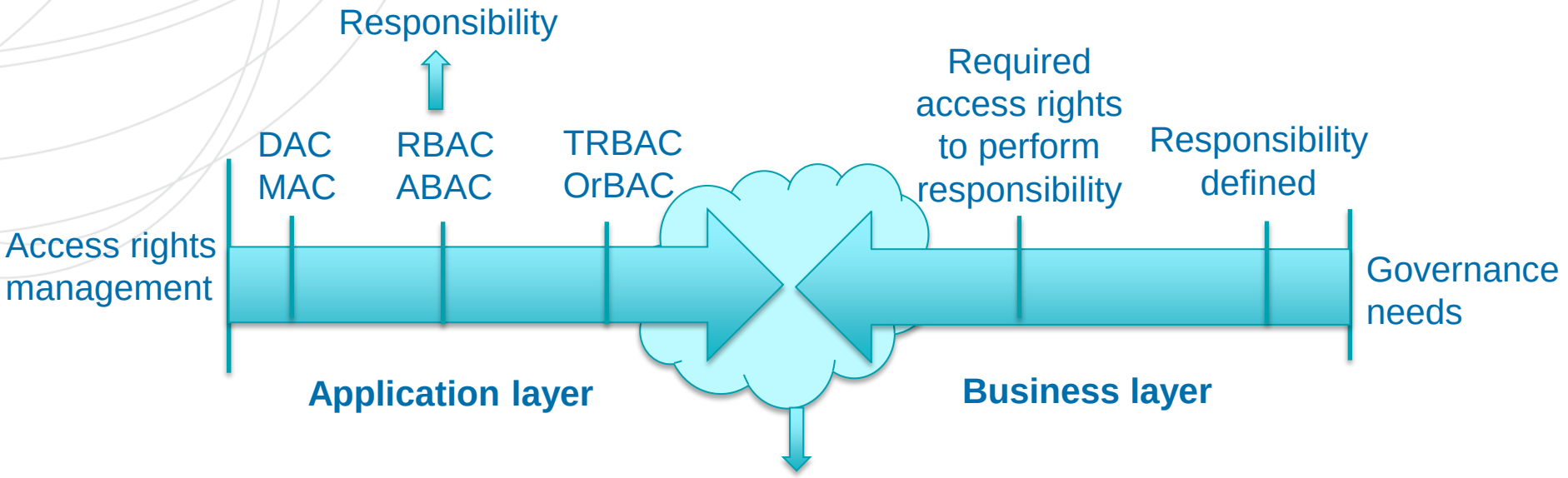
SOX

ISO International Organization for Standardization

BASEL II Automated Risk Based Capital Calculation

# INTRODUCTION

## Responsibility as an hyphen

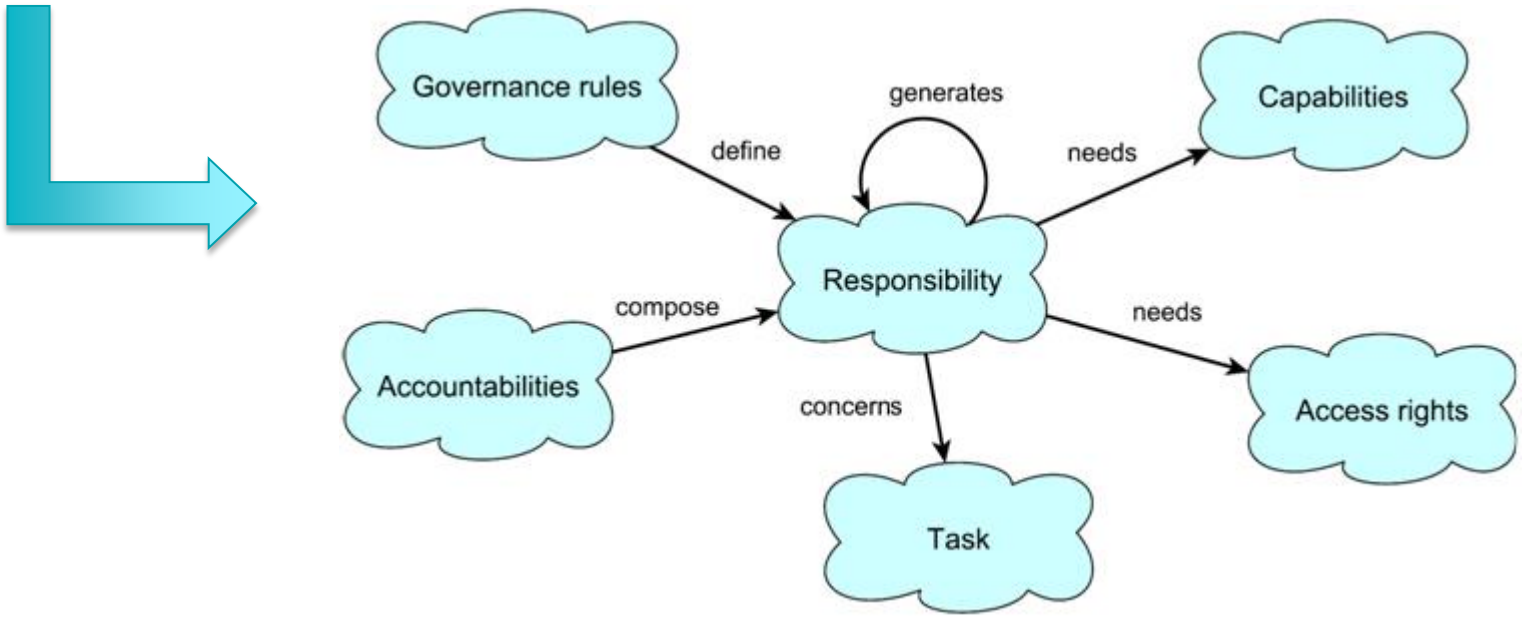



- **Access rights management tends to consider business concepts**
- **Governance needs require to provide accurate access rights**
- **Responsibility is perceived as an hyphen between both worlds**

# INTRODUCTION

## Unrefined picture of zone of concepts

| | COBIT | ISO/IEC 27000 | ISO/IEC 38500 | BASEL II | SOX |
|---|---|---|---|---|---|
| Responsibility needs capabilities | 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 defined by Governance rules | X | | X | X | X |
| Responsibility needs access rights | X | X | | | X |



# INTRODUCTION

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

## Designed artefacts

- 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

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

- Introduction
- Responsibility metamodel
- ArchiMate extension with Responsibility
- Method for the access rights management
- Conclusions

# RESPONSIBILITY METAMODEL

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

## Method and Limitations

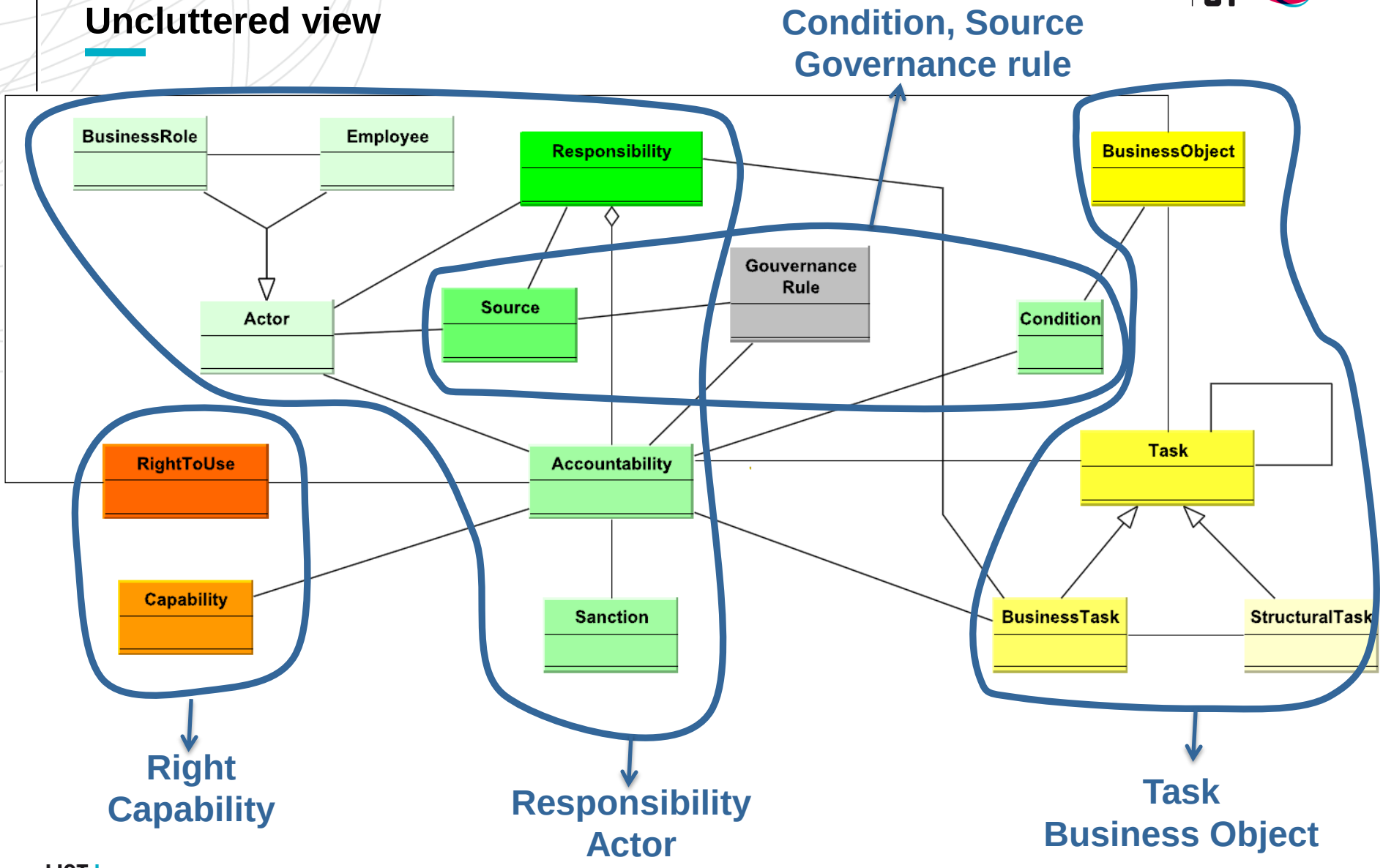
- Method
  - Review of the concepts from the literature
  - Concepts definition
  - Integration in the Responsibility metamodel

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

# RESPONSIBILITY METAMODEL

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

## Uncluttered view



# RESPONSIBILITY METAMODEL

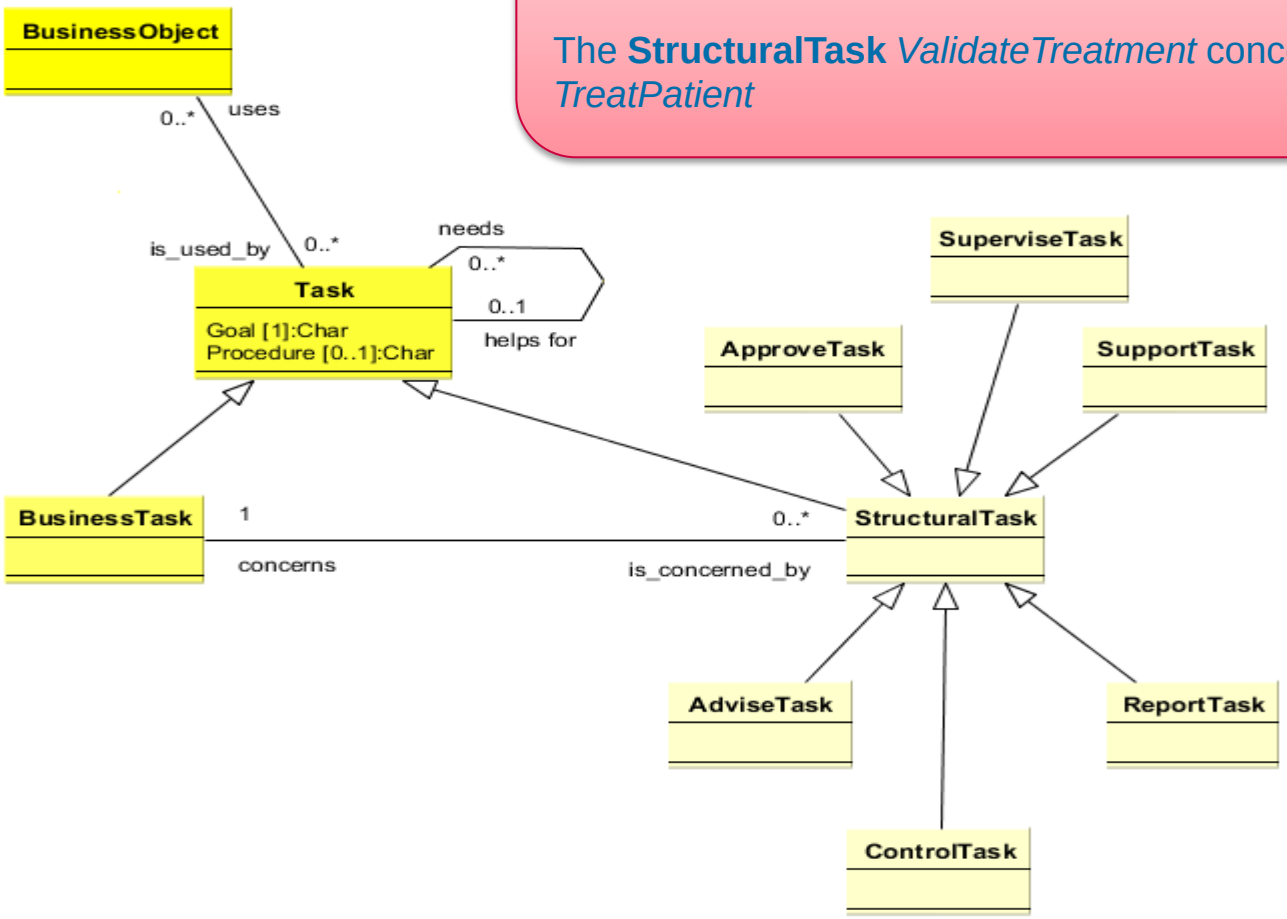
LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

## Task and Business object

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

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

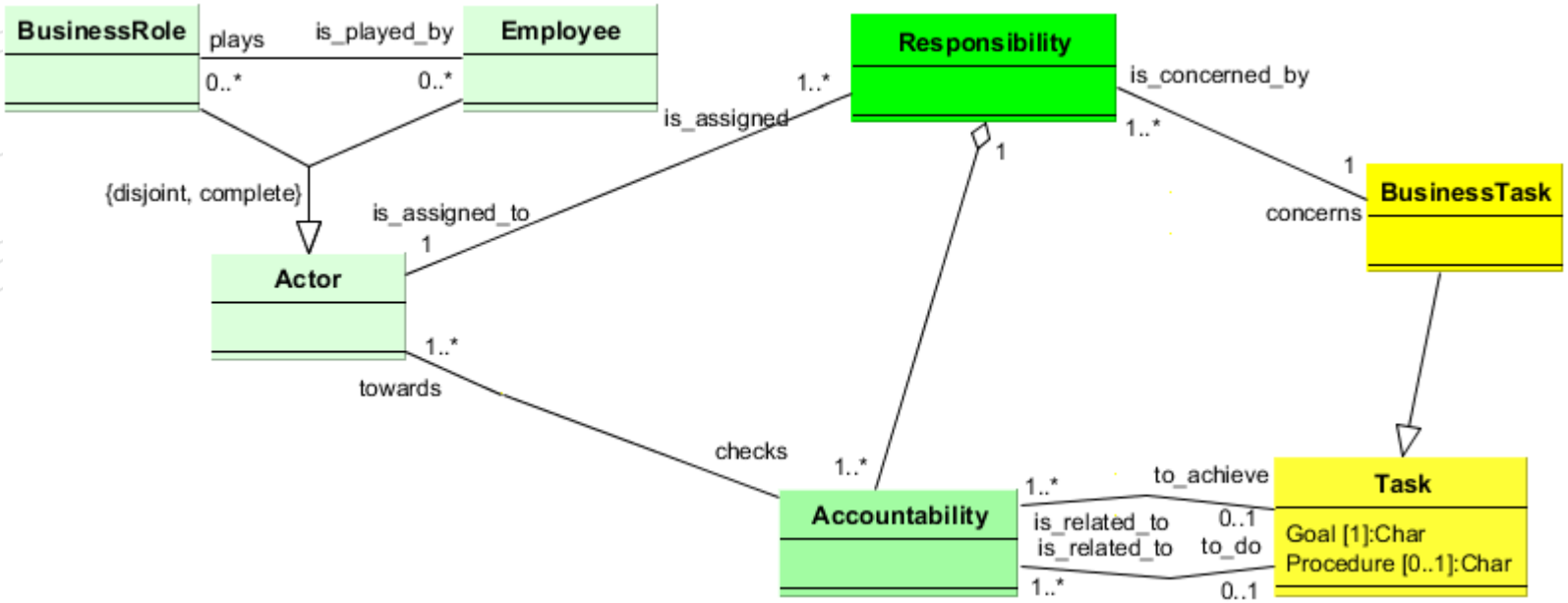
The **StructuralTask** *ValidateTreatment* concerns the **BusinessTask** *TreatPatient*



# RESPONSIBILITY METAMODEL

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

## Actor, Responsibility, Accountability

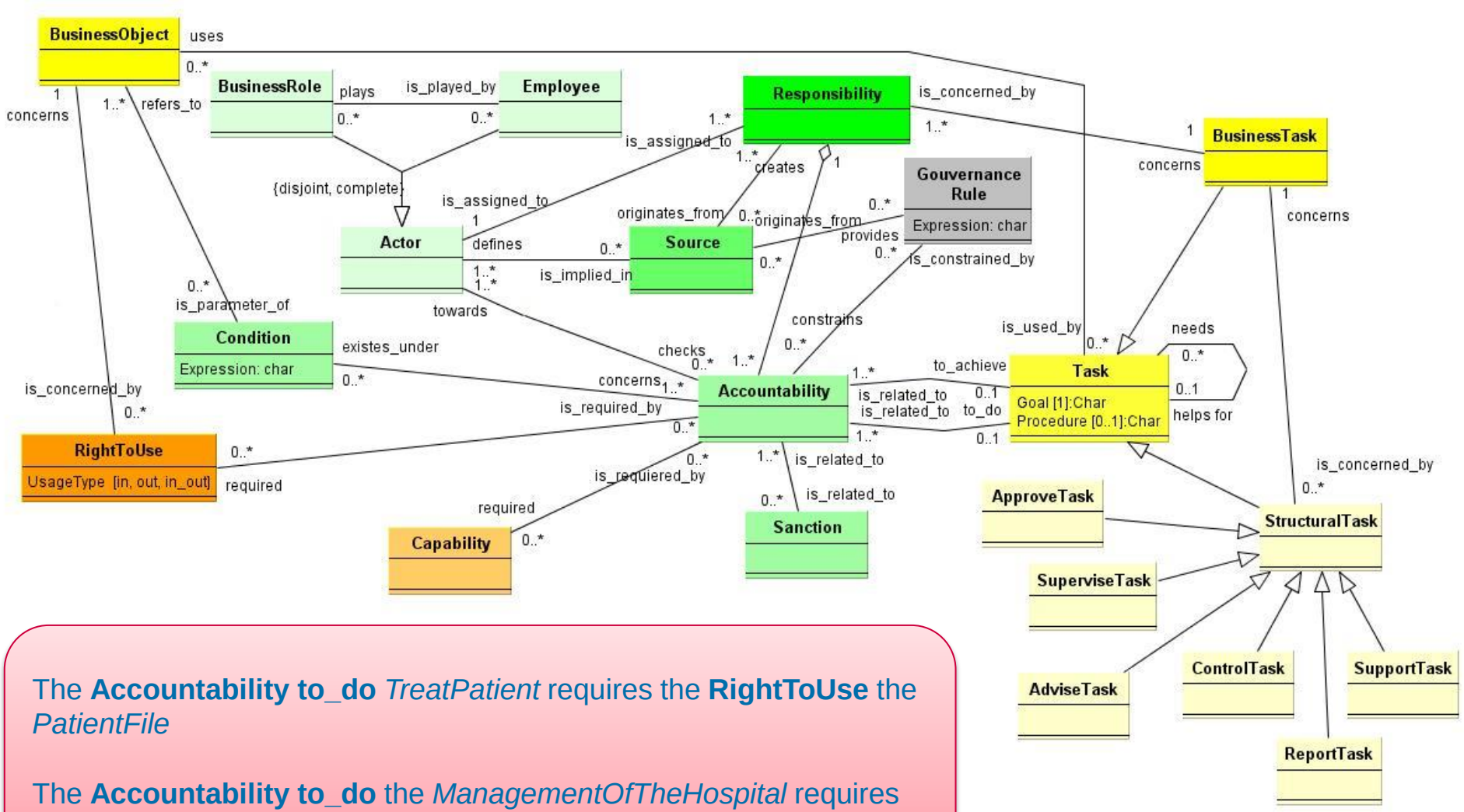



*Alice* plays the **BusinessRole** of *IT specialist* and is assigned to the **Responsibility** which aggregates the **Accountability to_do** *UpdatePathologyKnowledgeBase*

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

# RESPONSIBILITY METAMODEL

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY



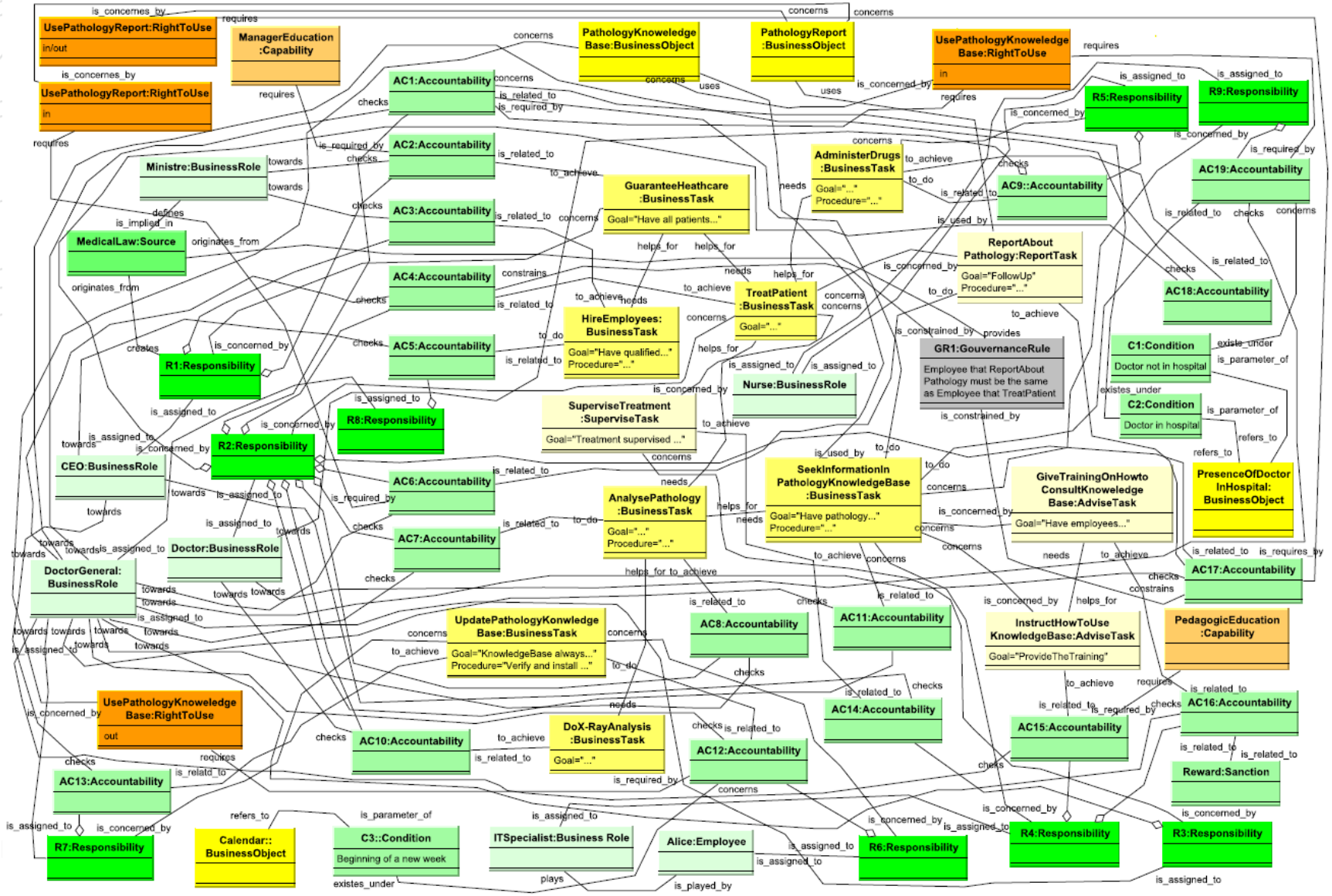

The **Accountability to_do** *TreatPatient* requires the **RightToUse** the *PatientFile*

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

# RESPONSIBILITY METAMODEL

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

## Healthcare case study



# OVERVIEW

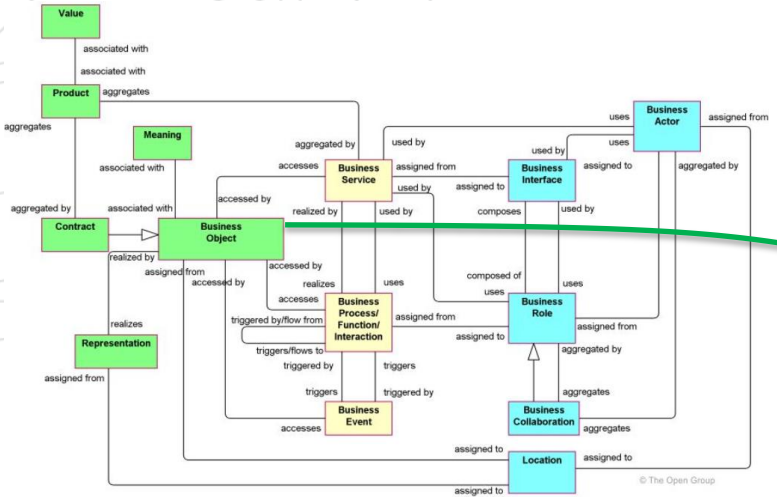
LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

- Introduction
- Responsibility metamodel
- ArchiMate extension with Responsibility
- Method for the access rights management
- Conclusions

# ARCHIMATE EXTENSION

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

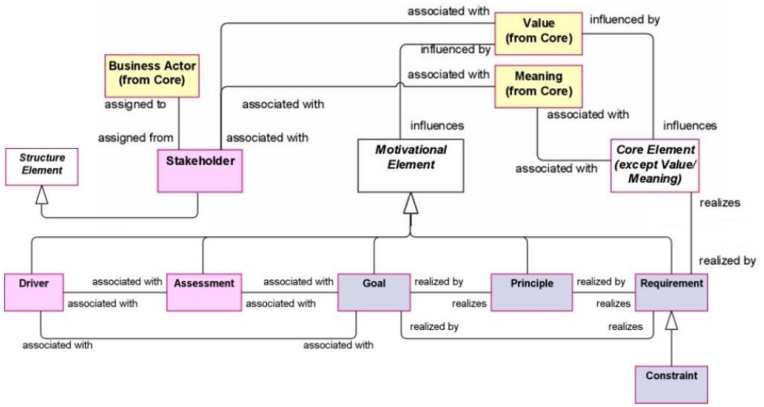
## Type of mappings

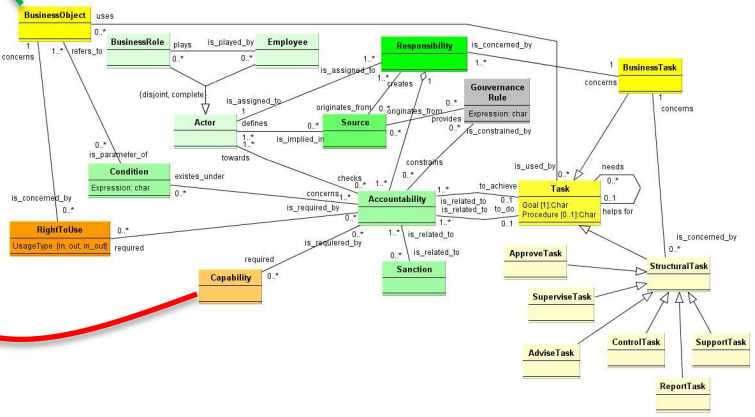



n-m mapping

1-1 mapping

No mapping

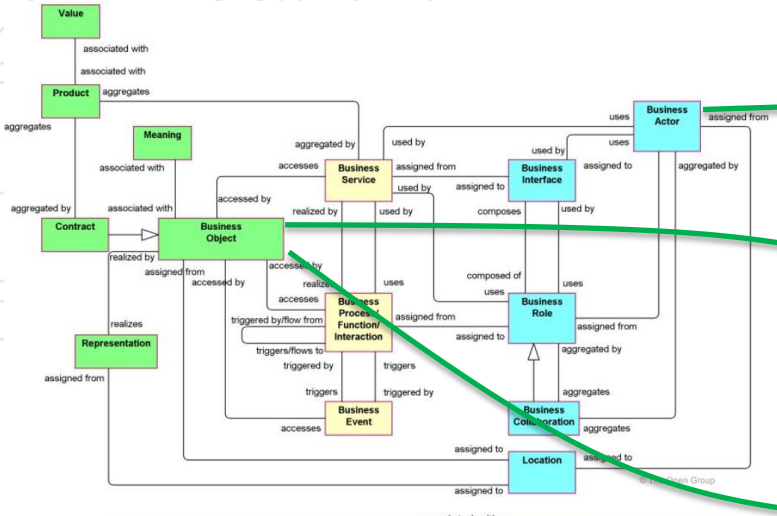


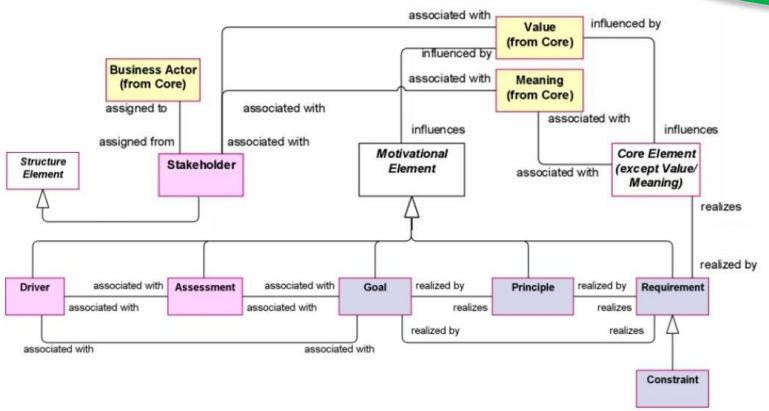



# ARCHIMATE EXTENSION

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

## Metamodel Integration

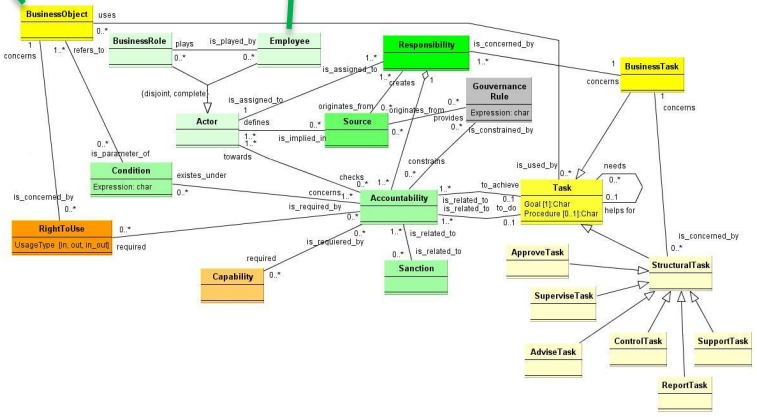



specialisation

1-1 mapping

merge



# ARCHIMATE EXTENSION

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

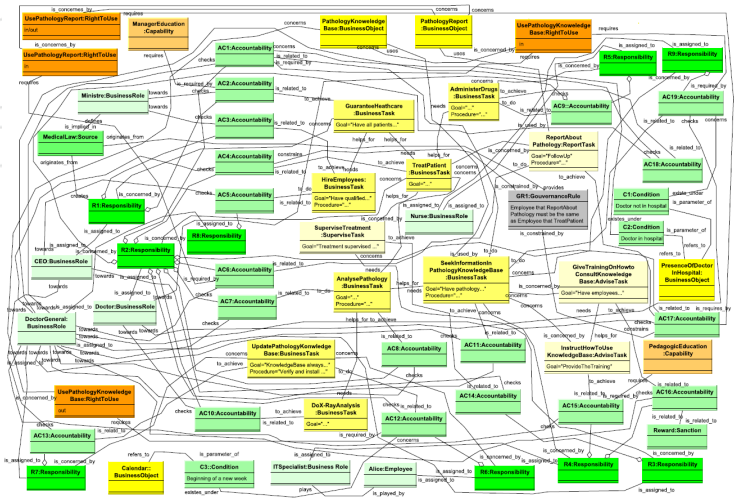
## Result

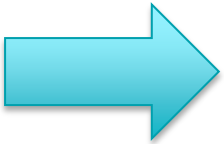
| Responsibility element | ArchiMate element | Mapping | Integration rule | Integrated element |
|---|---|---|---|---|
| Business Object | Business Object | 1:1 | Merge | Business Object |
| Task | Business Process | 1:1 | Specialisation | <<Task>> |
| R_Business Role | Business Role | 1:1 | Specialisation | <<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>> |

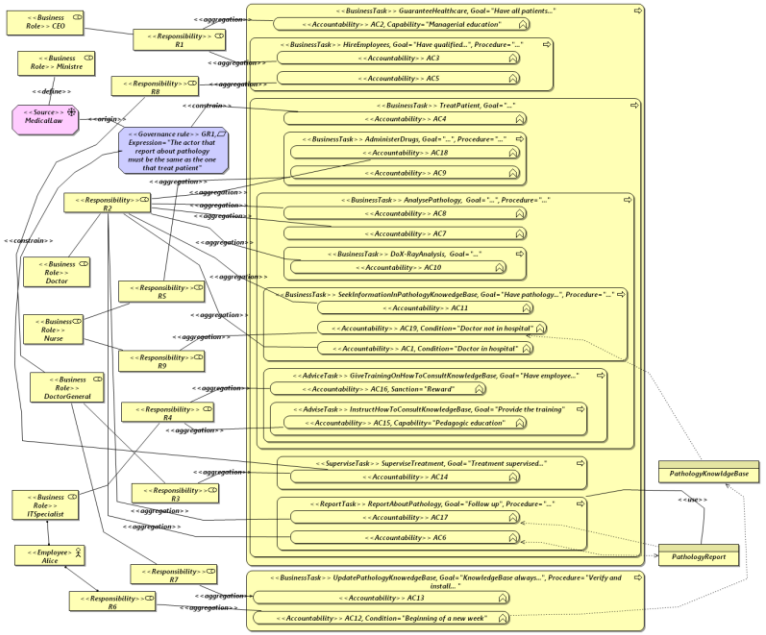
# ARCHIMATE EXTENSION

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

## Illustration







# OVERVIEW

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

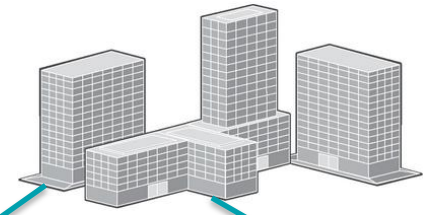
- Introduction
- Responsibility metamodel
- ArchiMate extension with Responsibility
- Method for the access rights management
- Conclusions

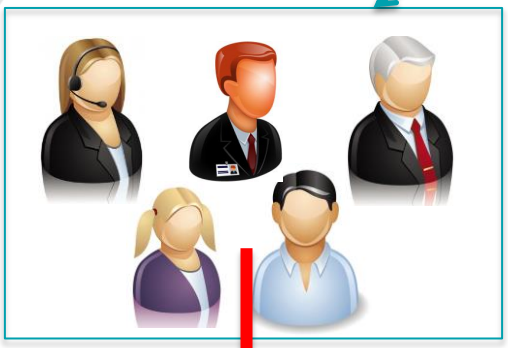
# AR MANAGEMENT METHOD

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

## Principle

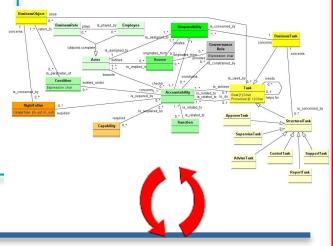
Business Layer

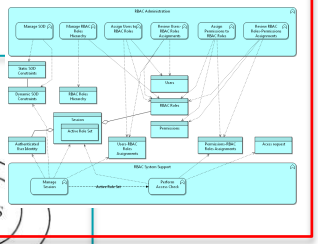




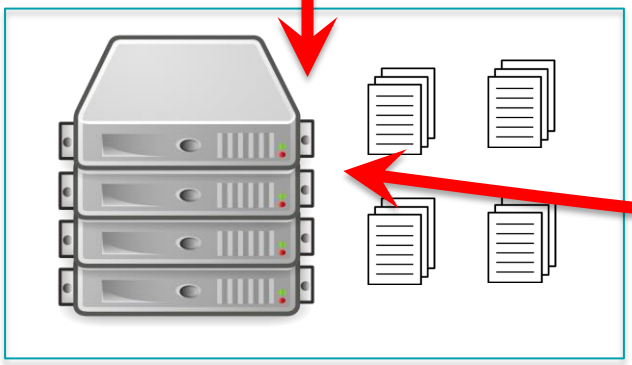
Responsibilities
Responsibilities
Responsibilities
Responsibilities

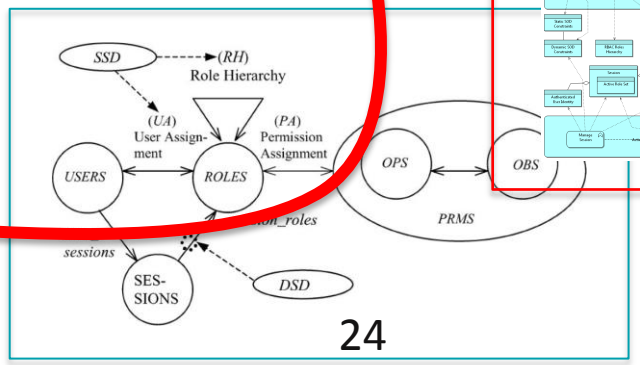
**ArchiMate**





Application Layer

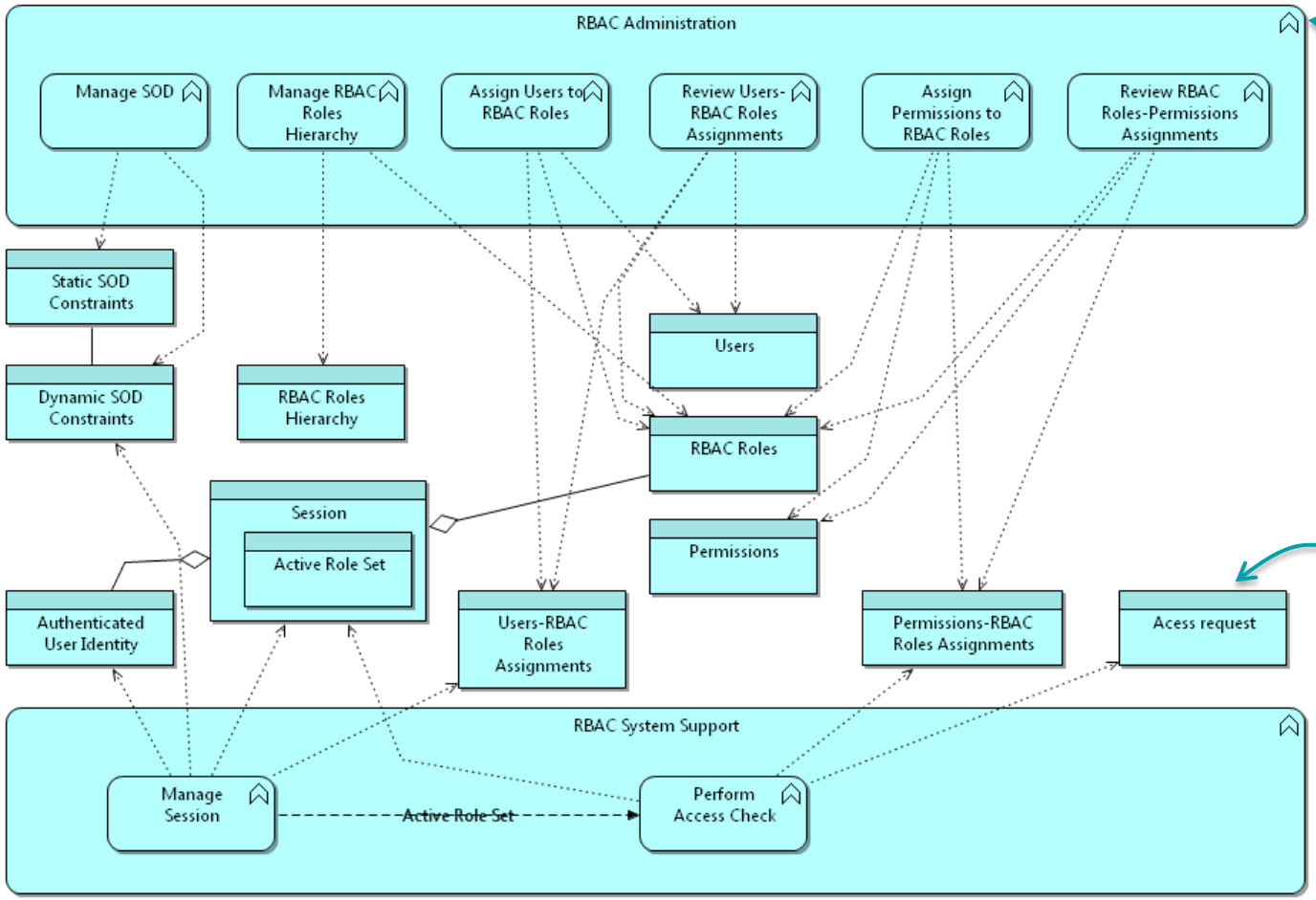




# AR MANAGEMENT METHOD

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

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

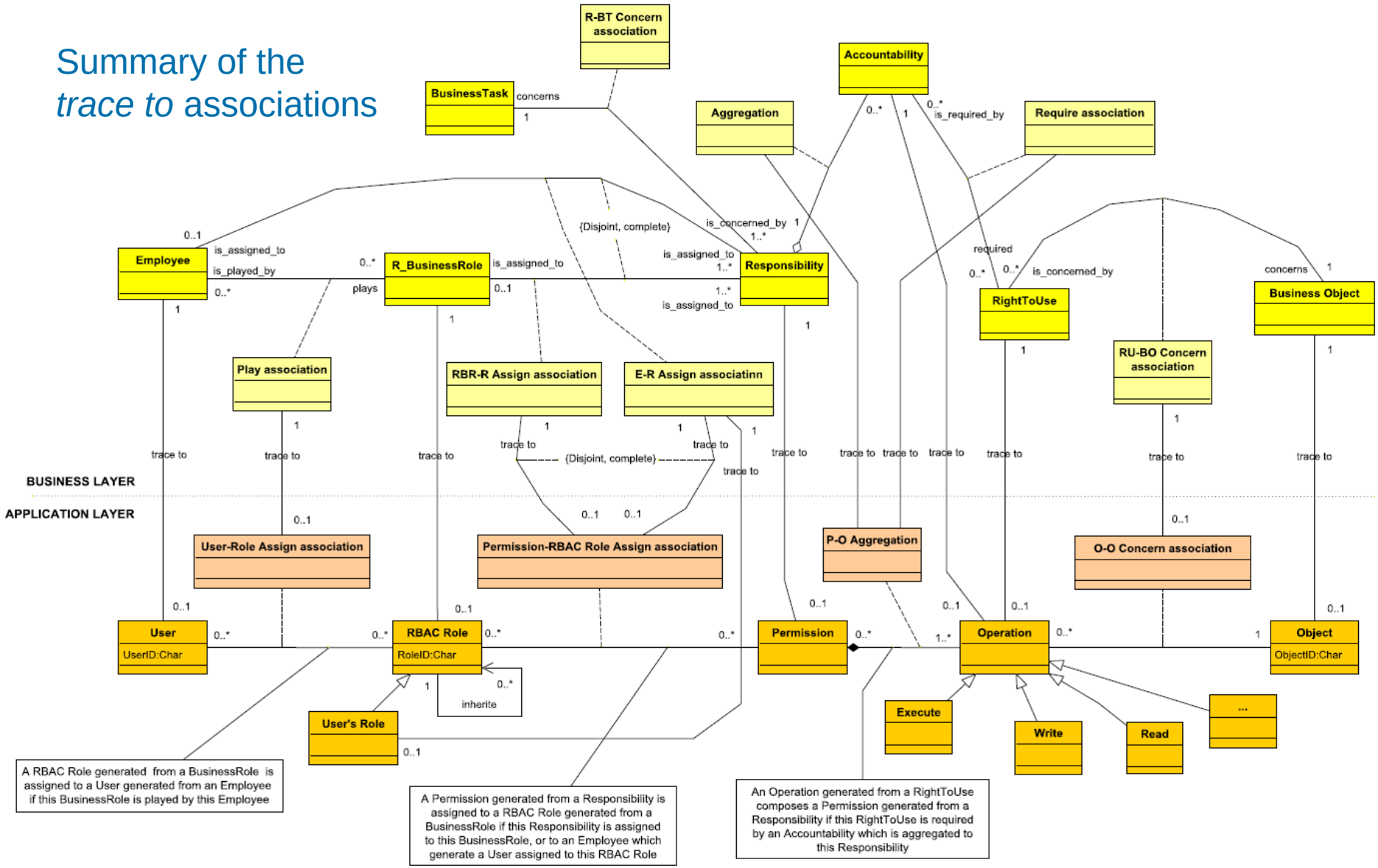
**Data object**: represents a passive element suitable for automated processing

# AR MANAGEMENT METHOD

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

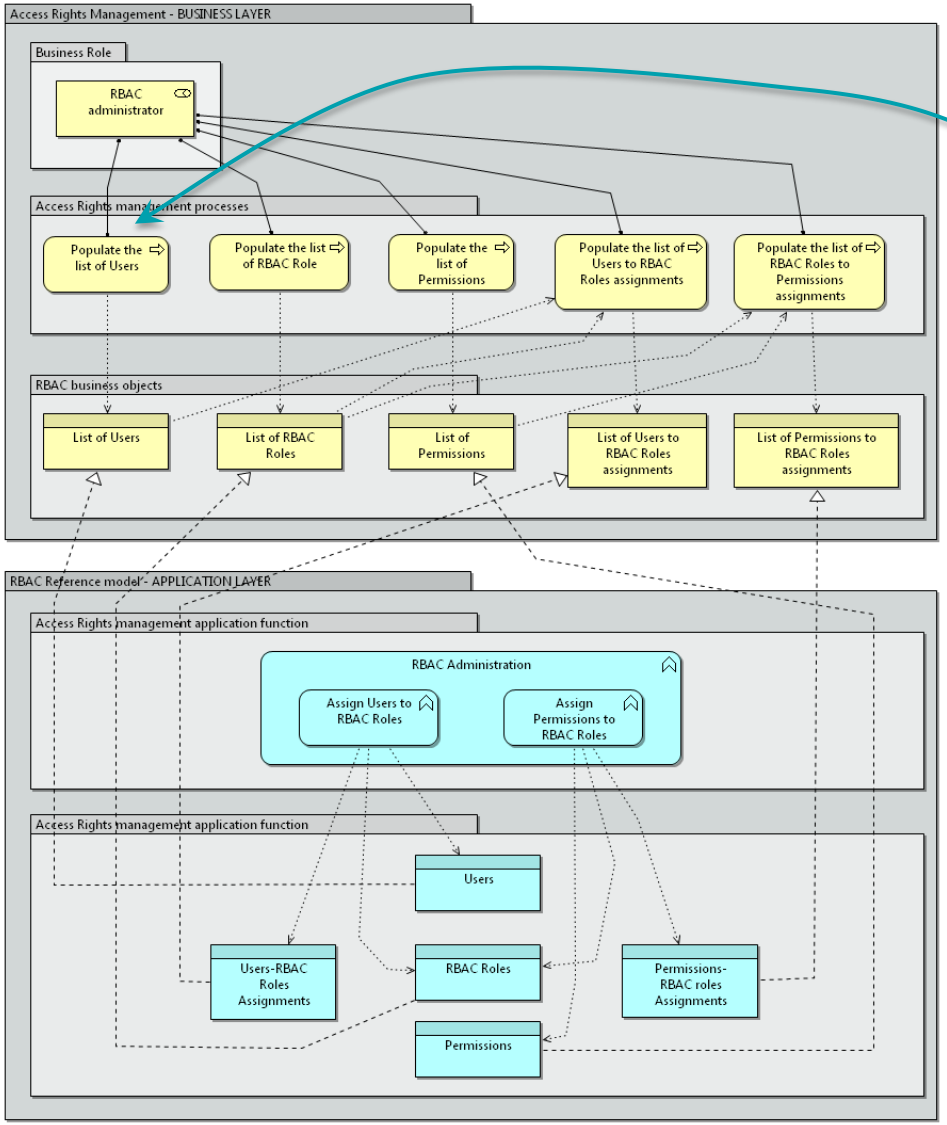
## Responsibility-RBAC alignment

Summary of the *trace to* associations



# AR MANAGEMENT METHOD

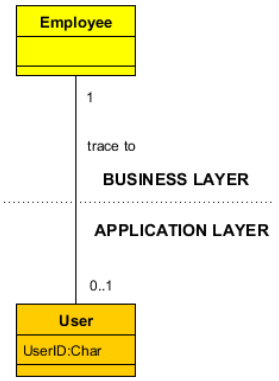
## AR Management Reference Model




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*

# OVERVIEW

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

- Introduction
- Responsibility metamodel
- ArchiMate extension with Responsibility
- Method for the access rights management
- Conclusions

# CONCLUSIONS

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

- 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

# THANK YOU ! QUESTIONS ?

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY