Presentation of RCIS paper

Feltus, Christophe

Publication date:
2015

Document Version
Peer reviewed version

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

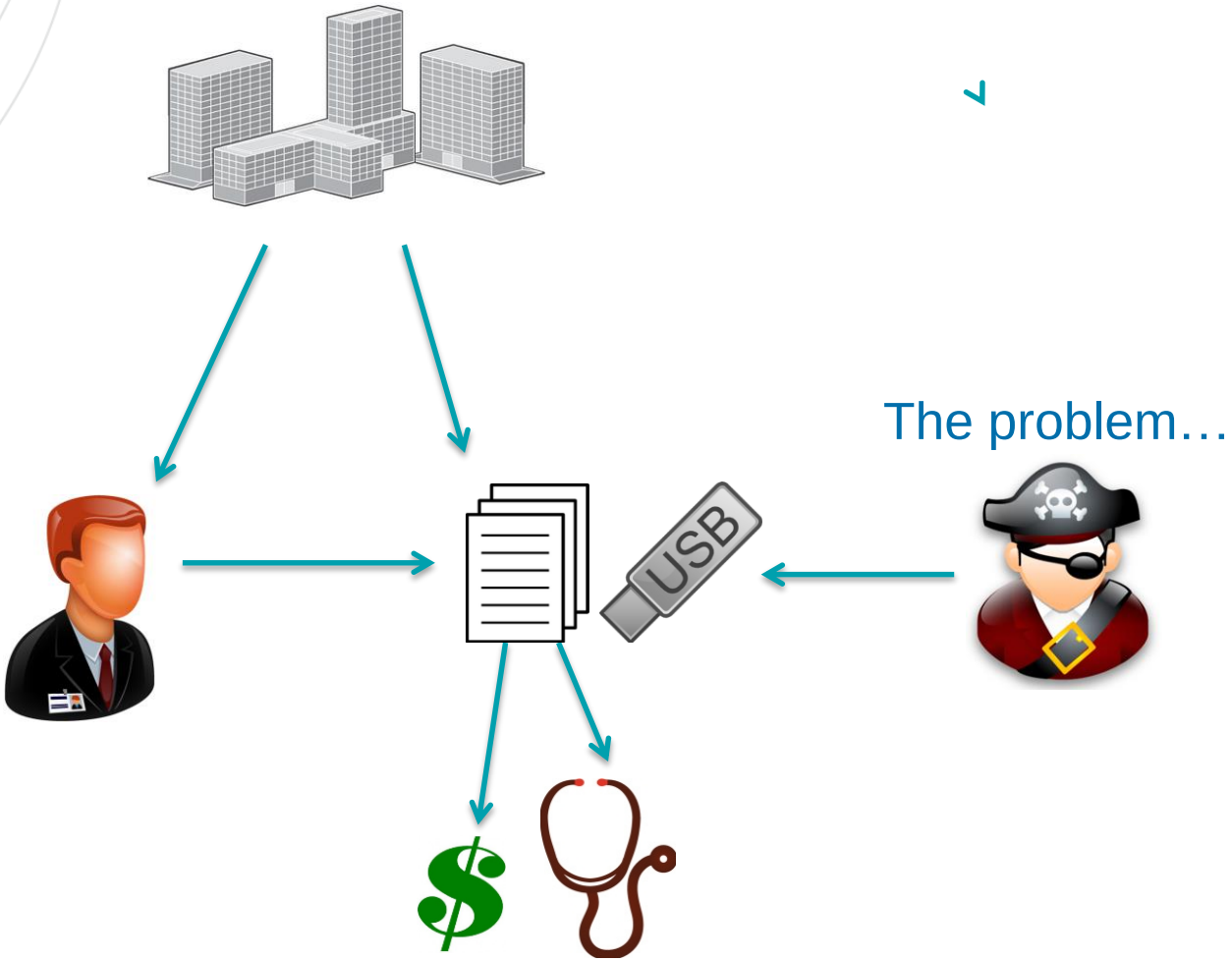
OVERVIEW

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

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

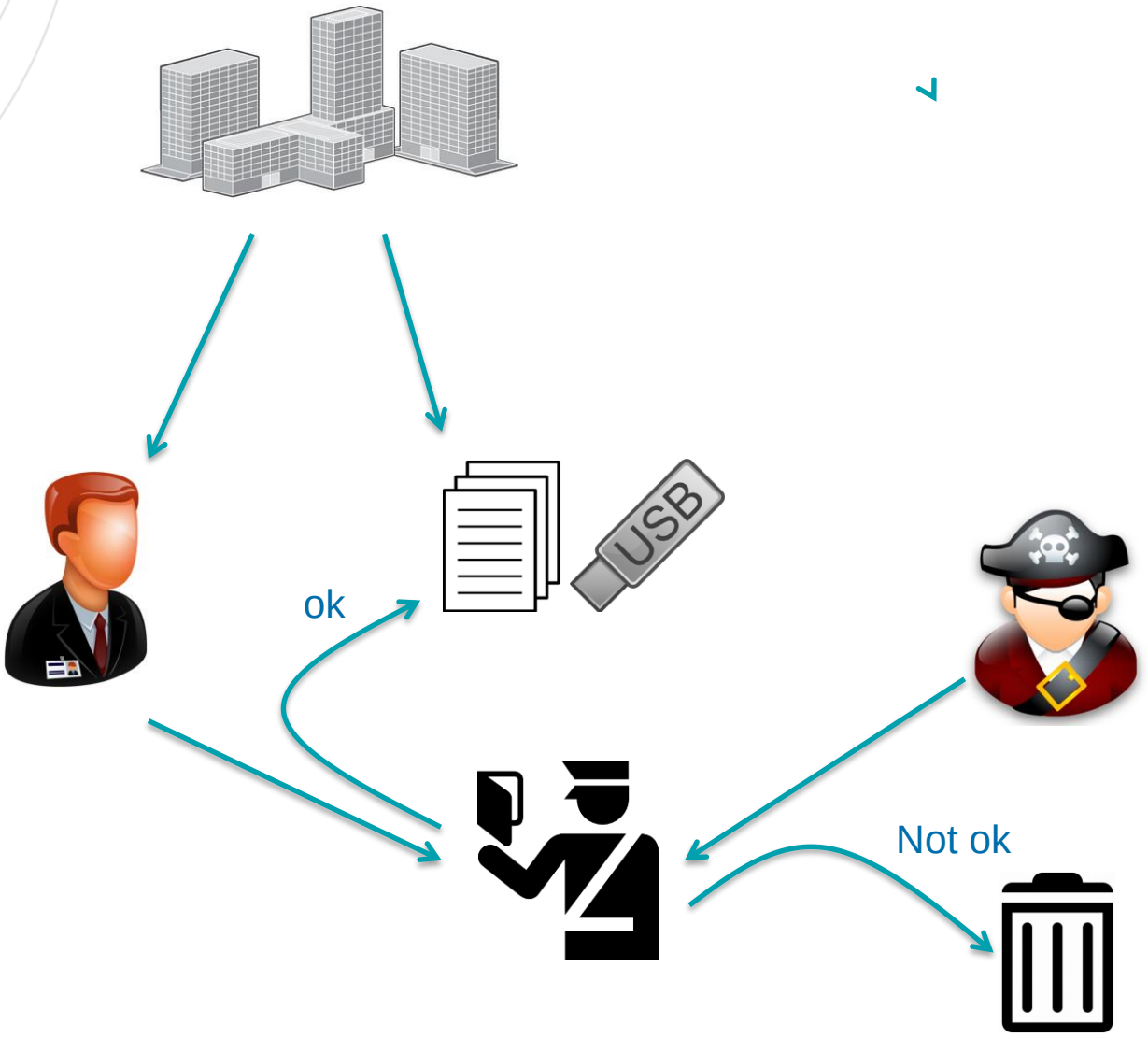
INTRODUCTION

Context



INTRODUCTION

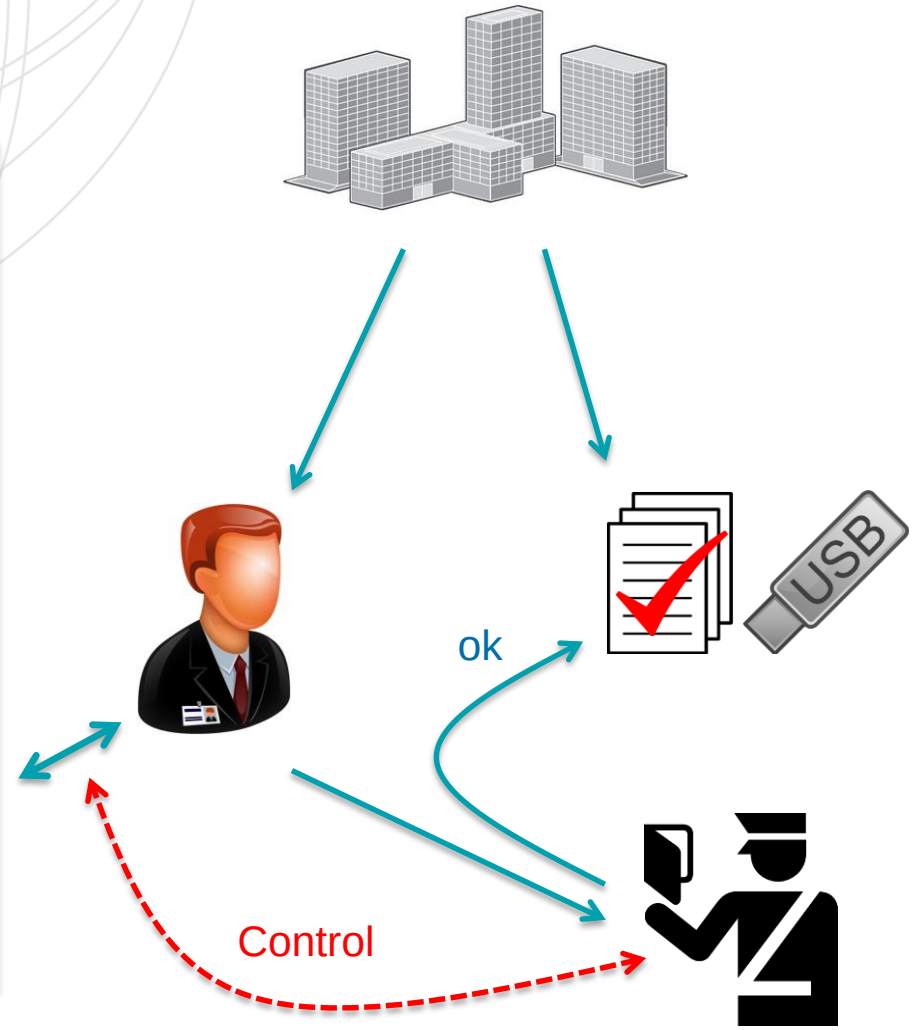
Context



INTRODUCTION

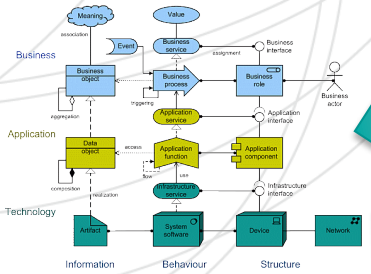
Context

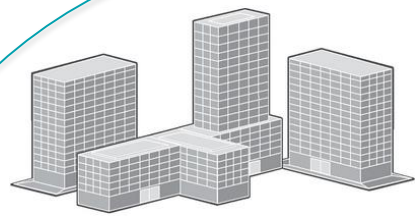
Roles

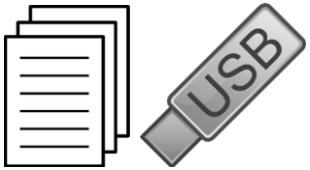


INTRODUCTION

Context







Enterprise Architecture

COBIT 5

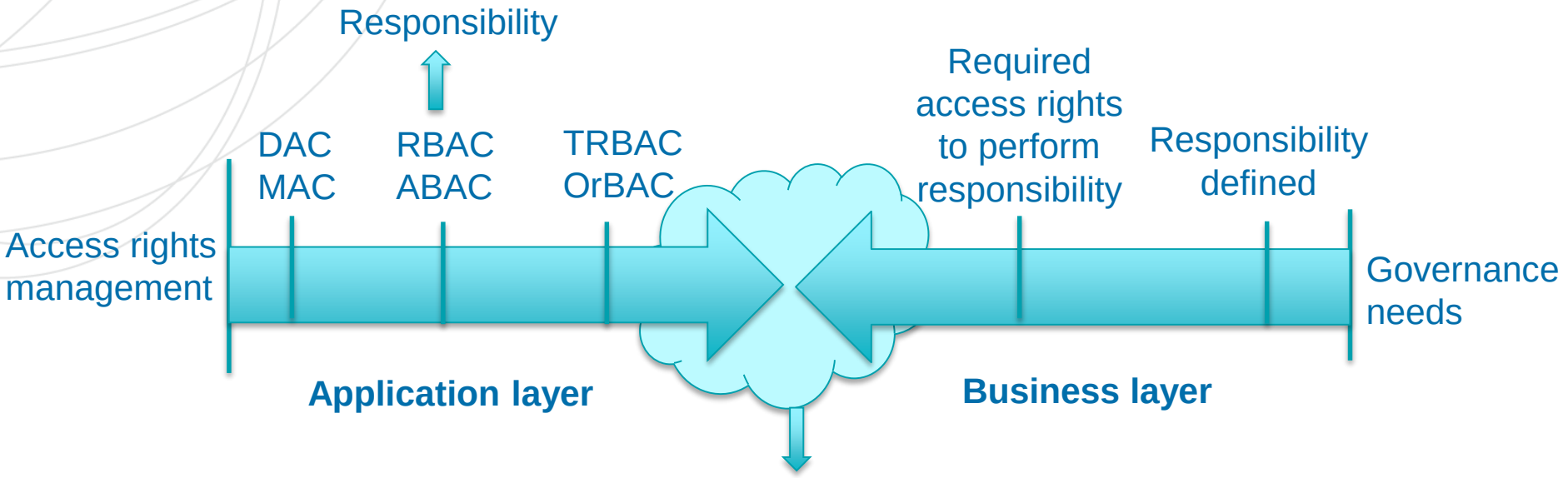
SOX

ISO International Organization for Standardization

BASEL II Automated Risk Based Capital Calculation

INTRODUCTION

Responsibility as an hyphen

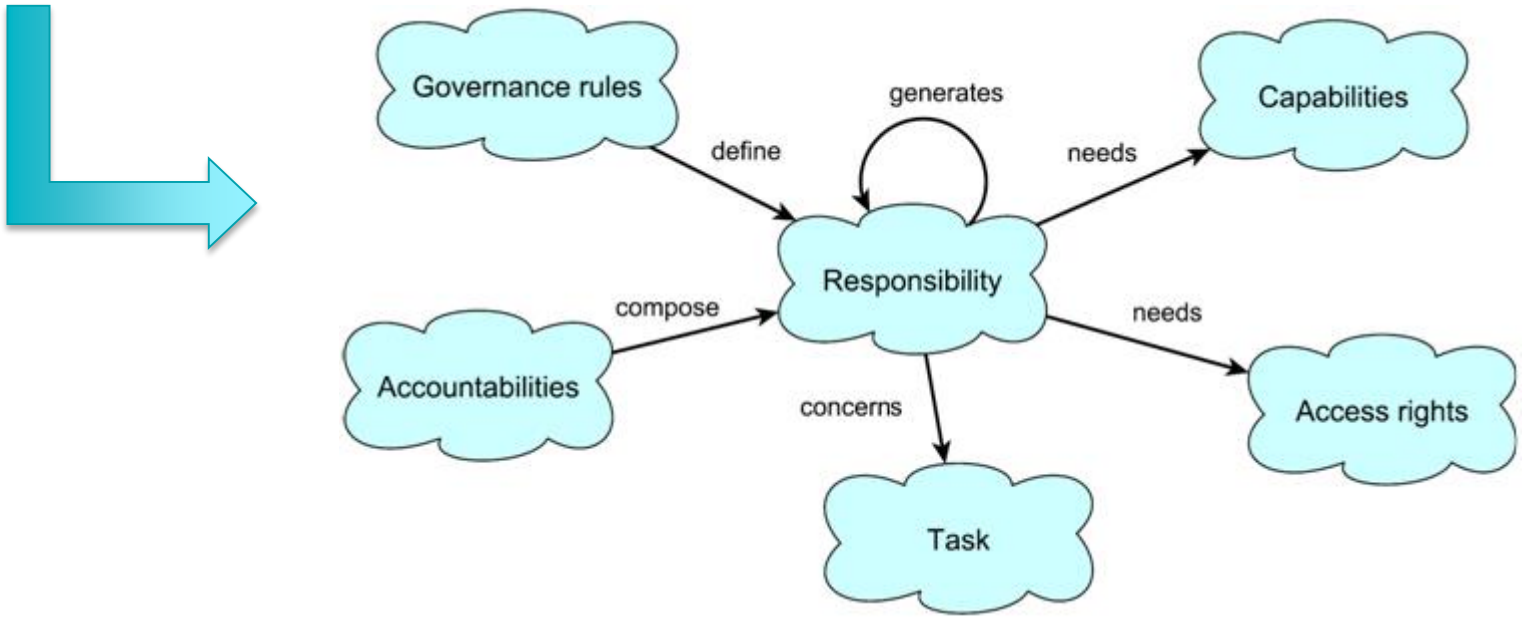


- **Access rights management tends to consider business concepts**
- **Governance needs require to provide accurate access rights**
- **Responsibility is perceived as an hyphen between both worlds**

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

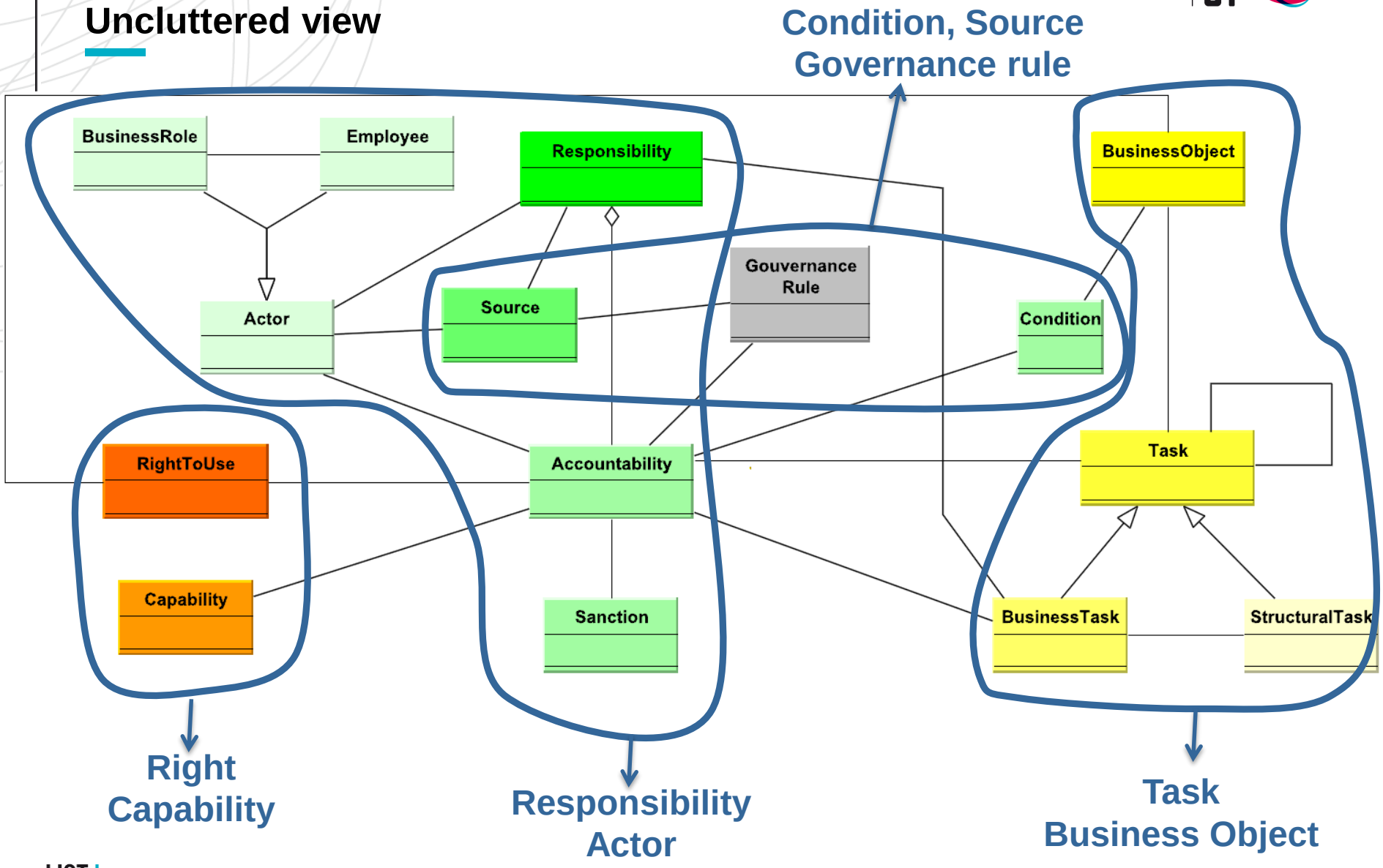
- Method
  - Review of the concepts from the literature
  - Concepts definition
  - Integration in the Responsibility metamodel

- 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

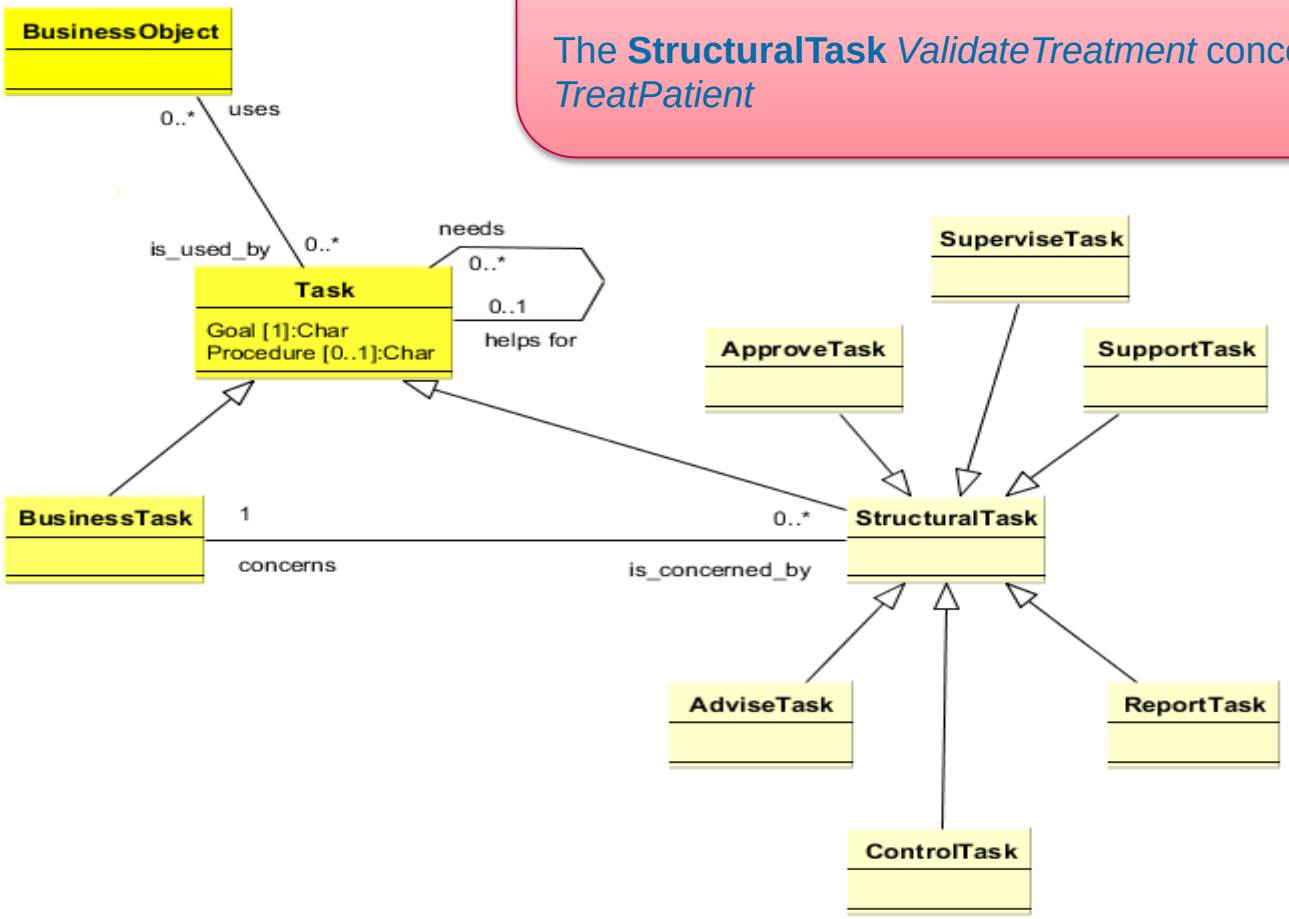
LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

Task and Business object

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

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

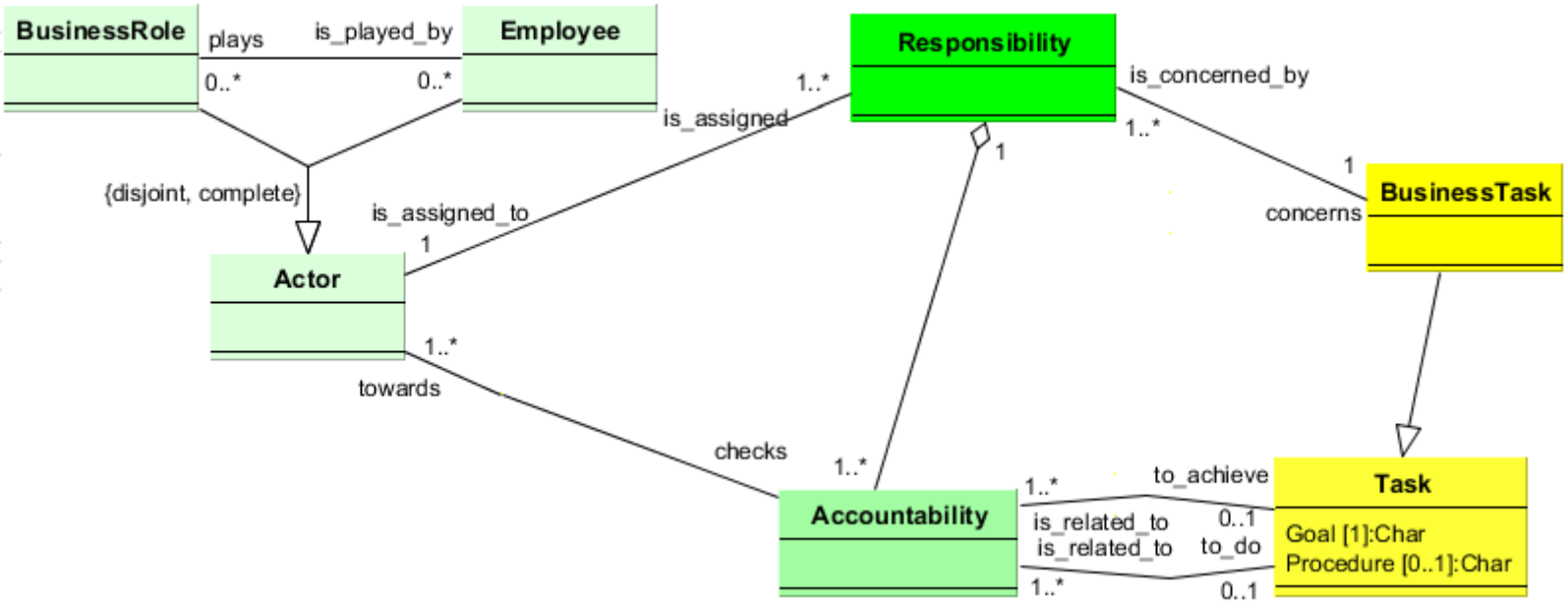
The **StructuralTask** *ValidateTreatment* concerns the **BusinessTask** *TreatPatient*



RESPONSIBILITY METAMODEL

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

Actor, Responsibility, Accountability

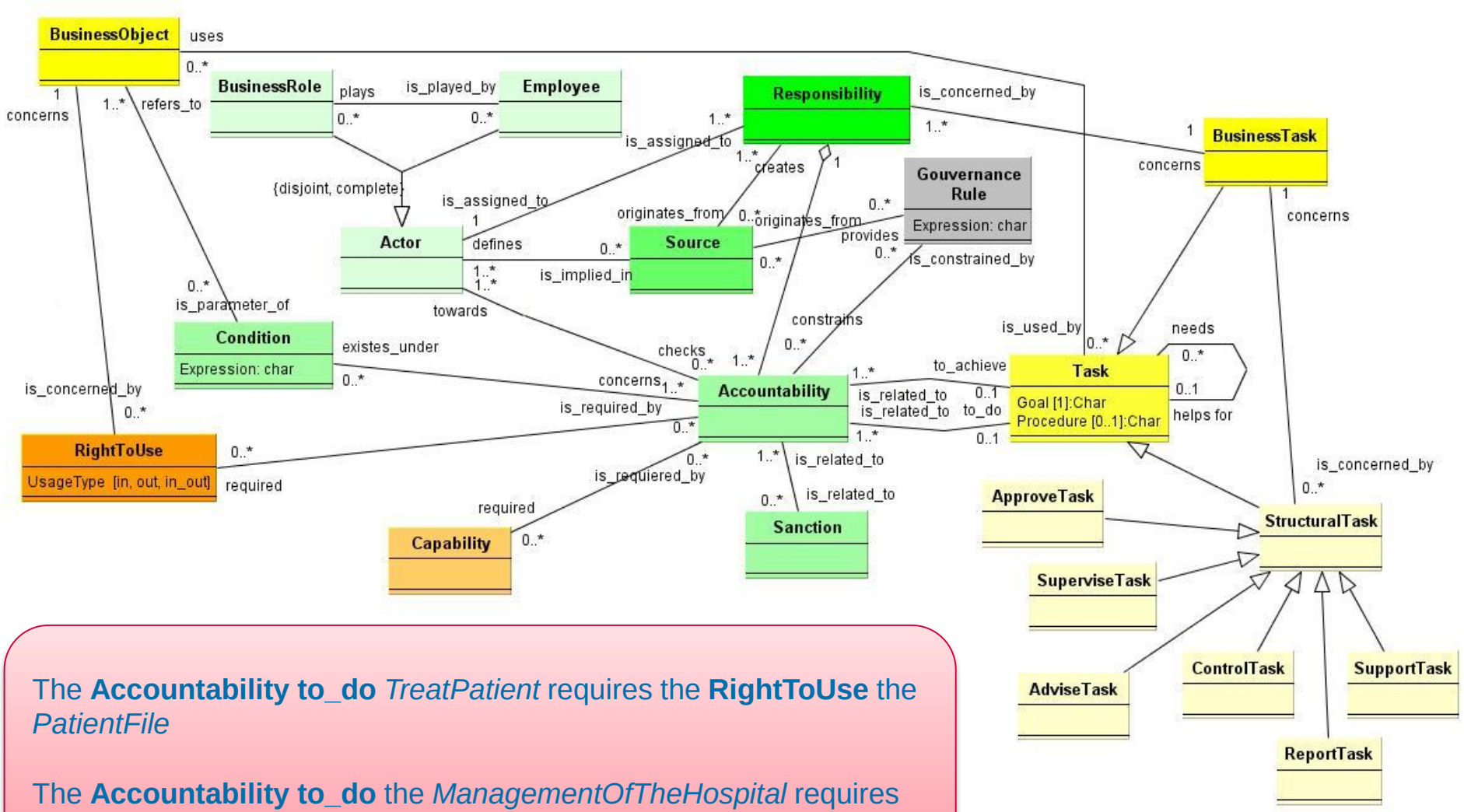


Alice plays the **BusinessRole** of *IT specialist* and is assigned to the **Responsibility** which aggregates the **Accountability to_do** *UpdatePathologyKnowledgeBase*

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

RESPONSIBILITY METAMODEL

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY



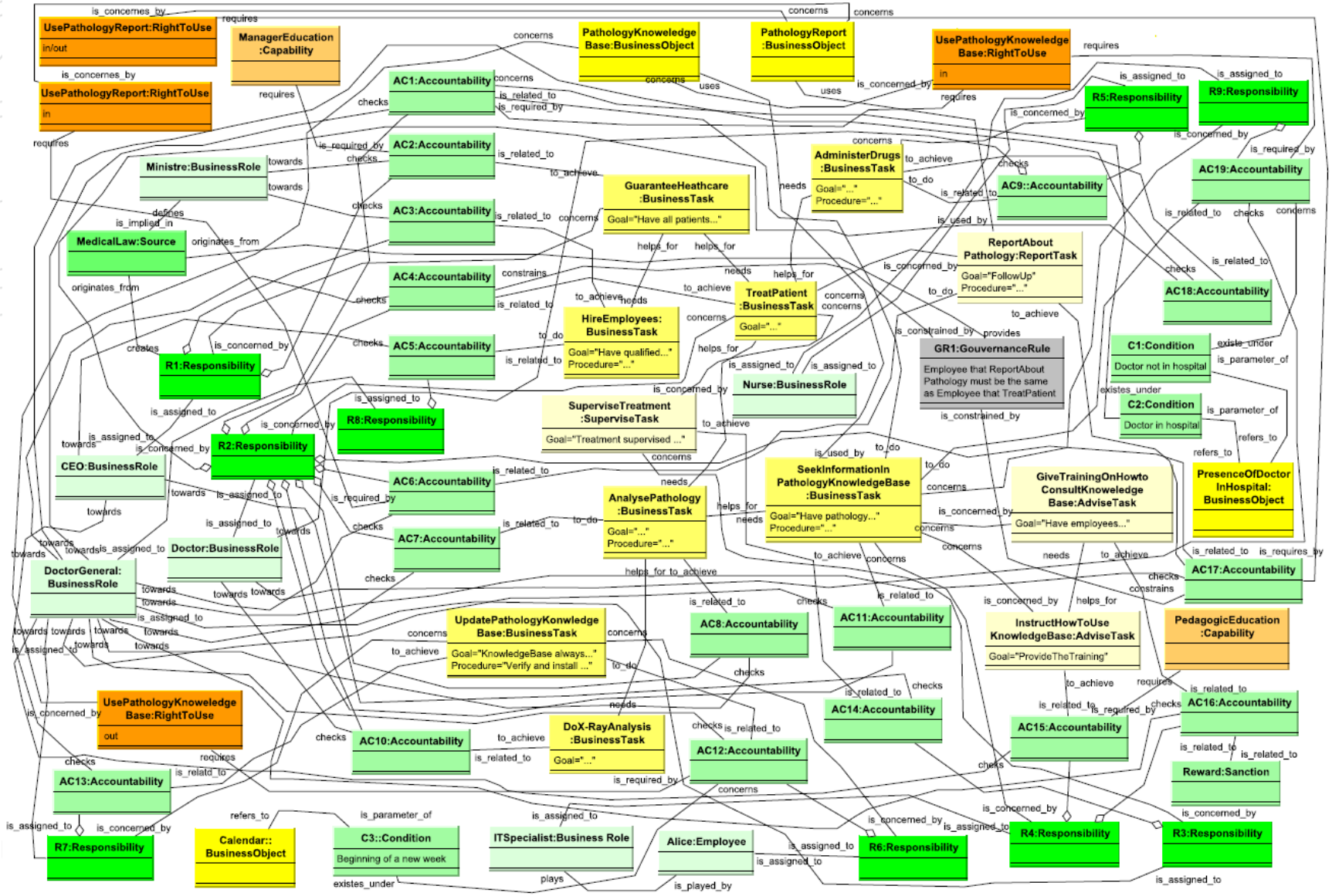
The **Accountability to_do** *TreatPatient* requires the **RightToUse** the *PatientFile*

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

RESPONSIBILITY METAMODEL

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

Healthcare case study



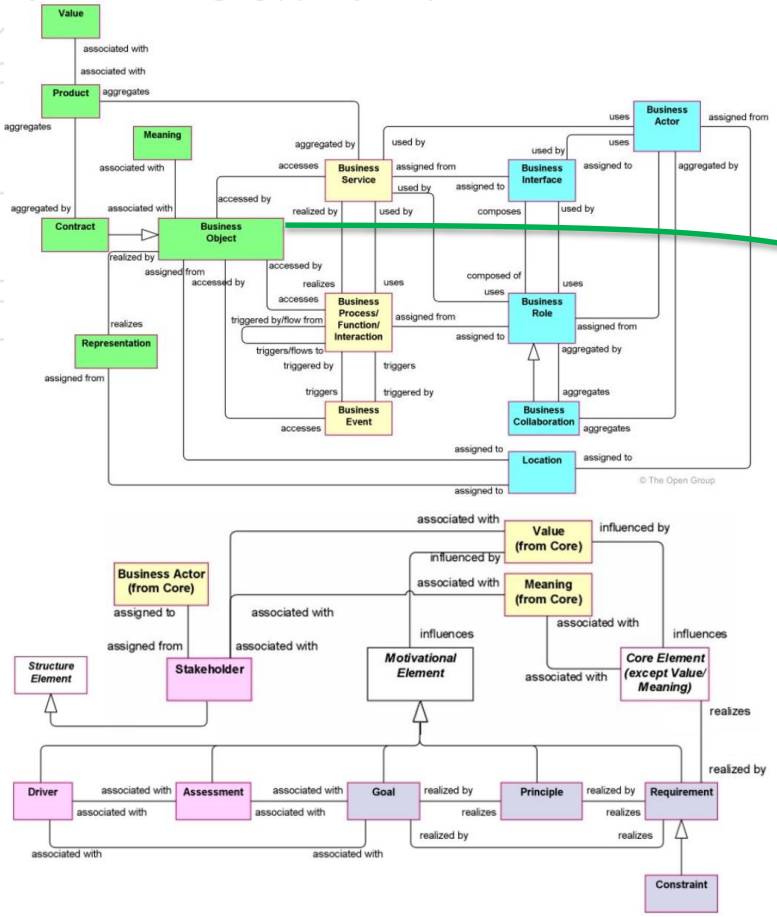
OVERVIEW

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

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

ARCHIMATE EXTENSION

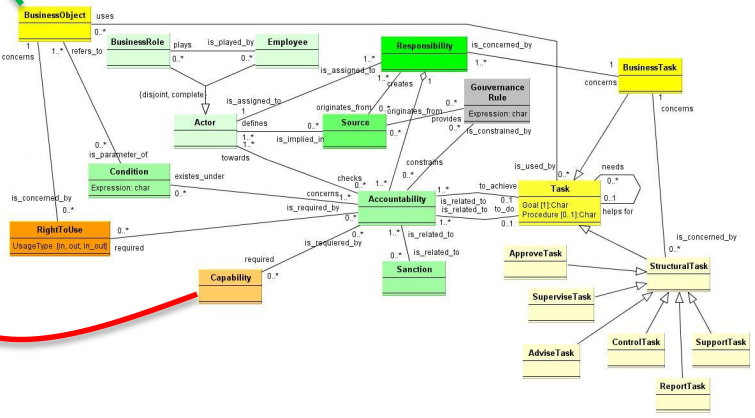
Type of mappings



n-m mapping

1-1 mapping

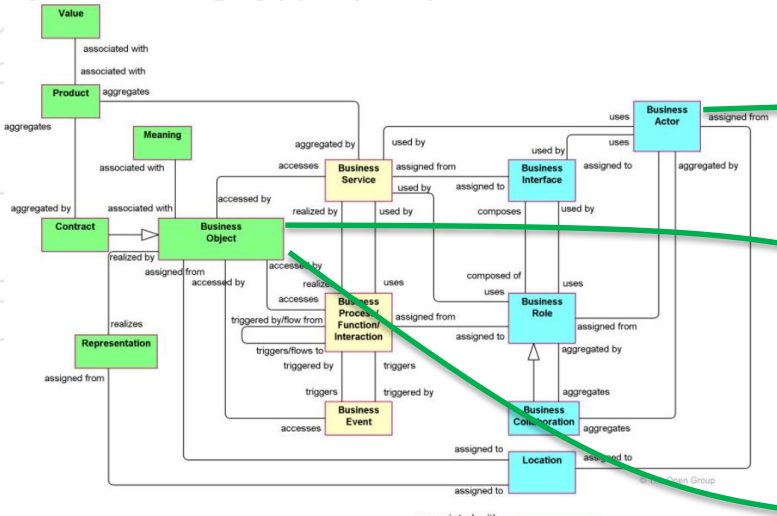
No mapping

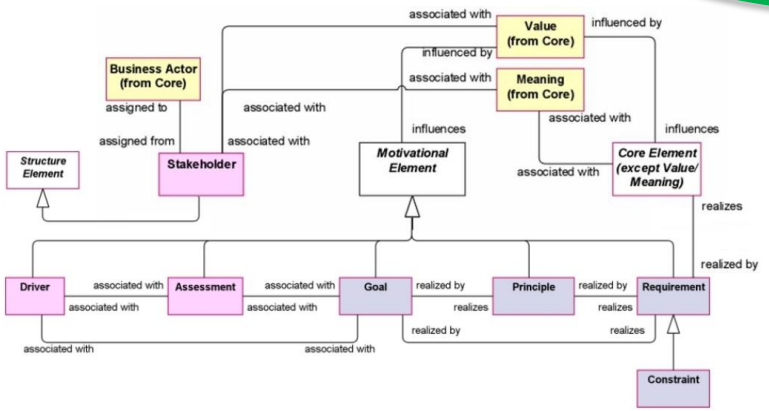


ARCHIMATE EXTENSION

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

Metamodel Integration

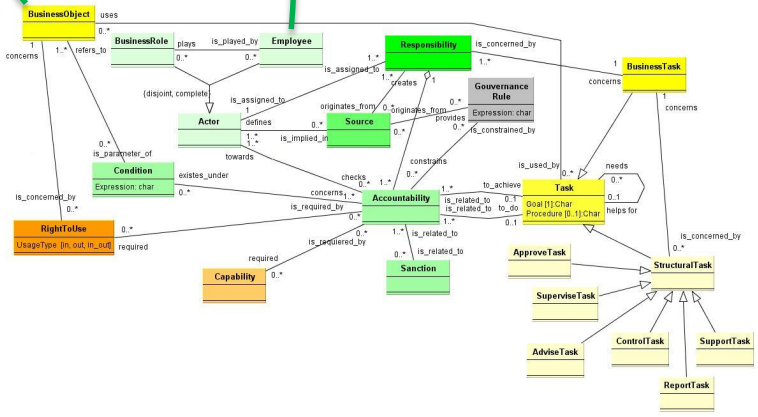




specialisation

1-1 mapping

merge



ARCHIMATE EXTENSION

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

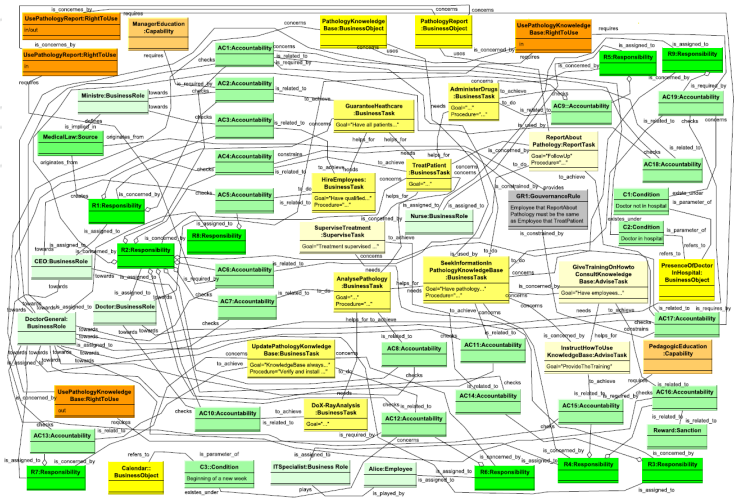
Result

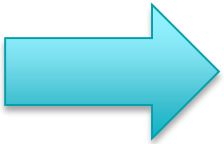
Responsibility element	ArchiMate element	Mapping	Integration rule	Integrated element
Business Object	Business Object	1:1	Merge	Business Object
Task	Business Process	1:1	Specialisation	<<Task>>
R_Business Role	Business Role	1:1	Specialisation	<<R_BusinessRole>>
Responsibility	Business Role	1:1	Specialisation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

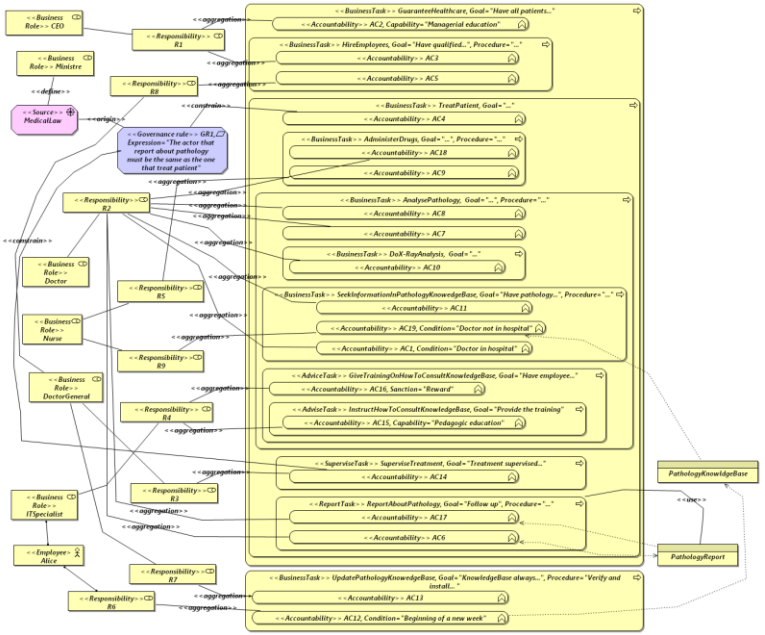
ARCHIMATE EXTENSION

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

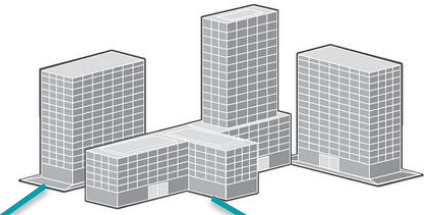
AR MANAGEMENT METHOD

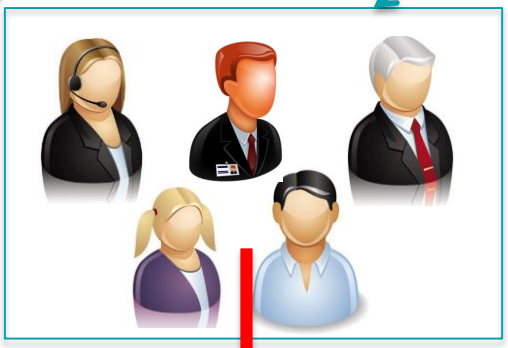
LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

Principle

Business Layer

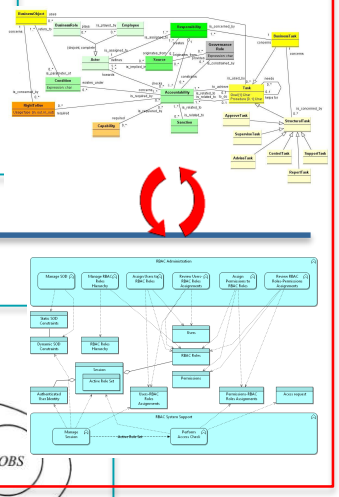
Application Layer

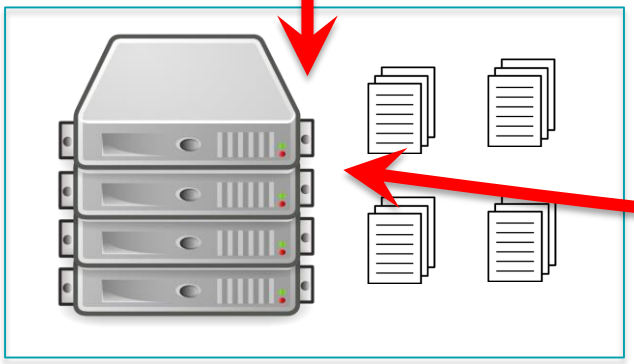


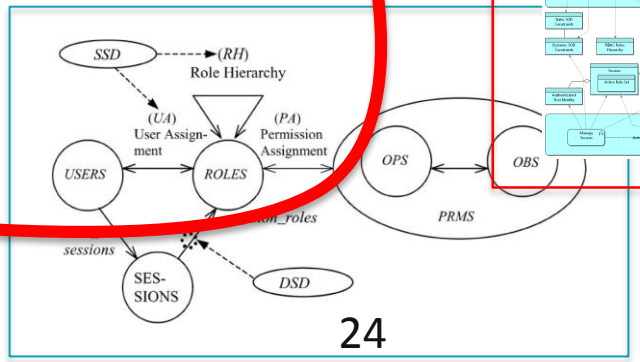


Responsibilities
Responsibilities
Responsibilities
Responsibilities

ArchiMate



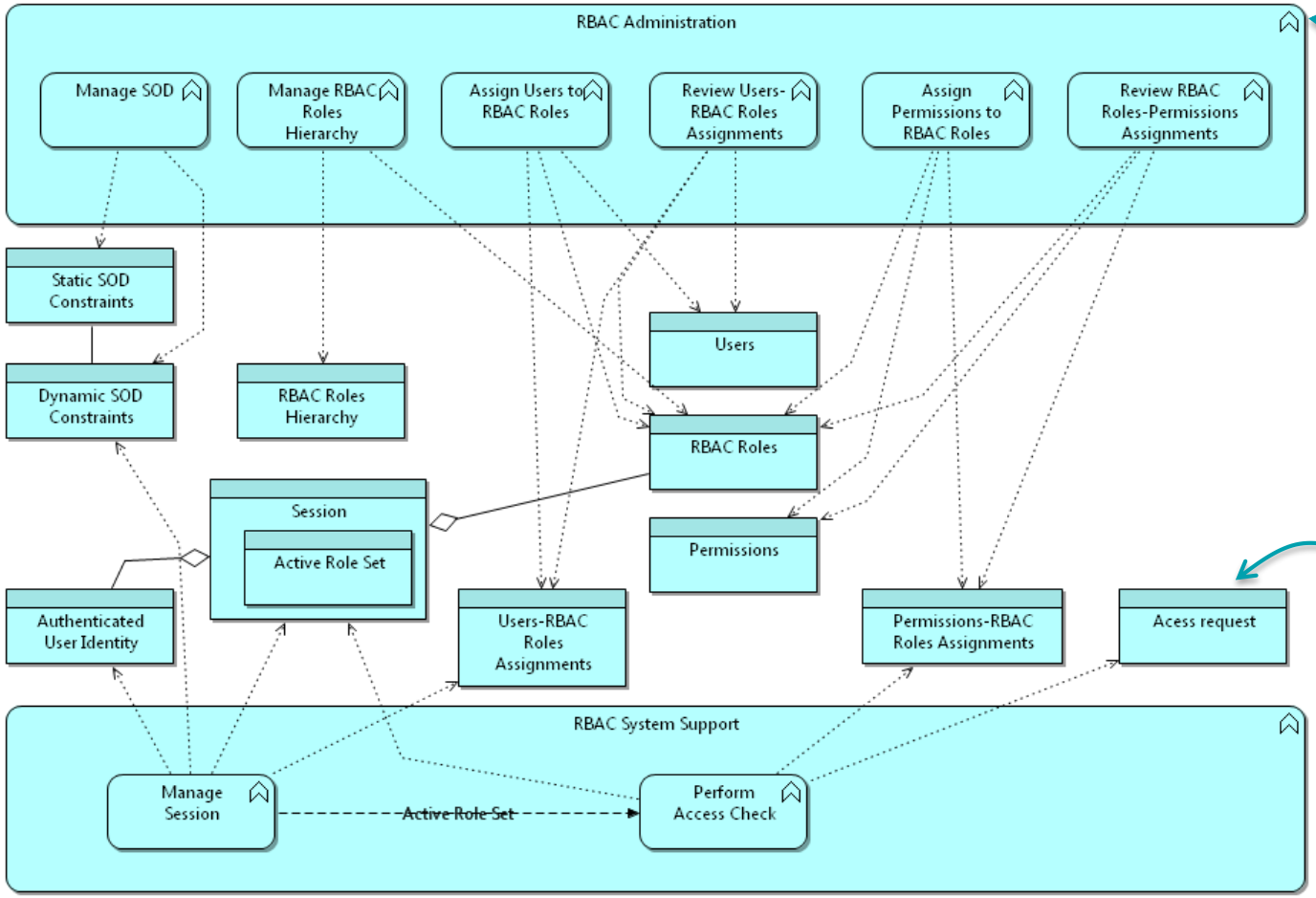




AR MANAGEMENT METHOD

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

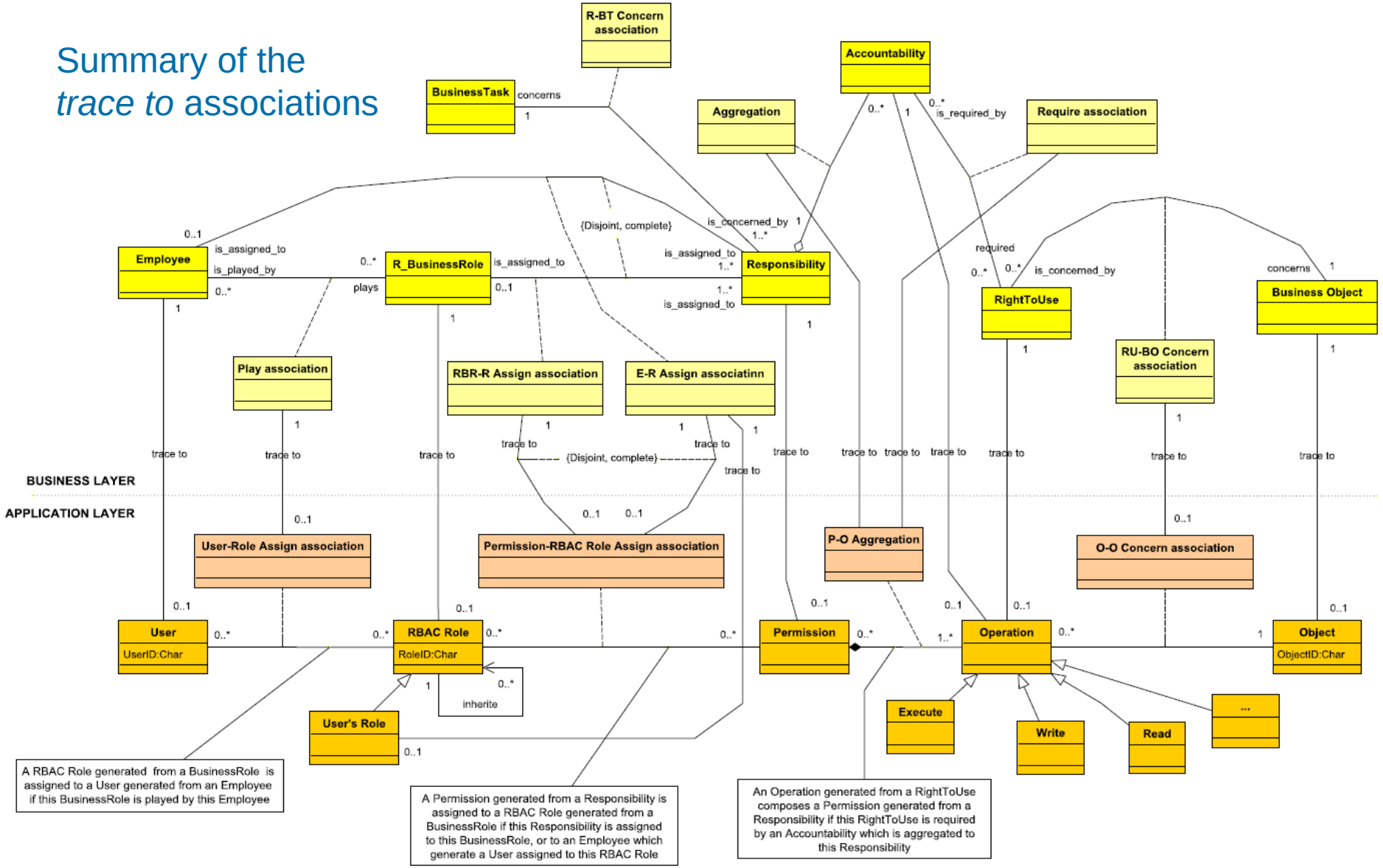
Data object: represents a passive element suitable for automated processing

AR MANAGEMENT METHOD

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

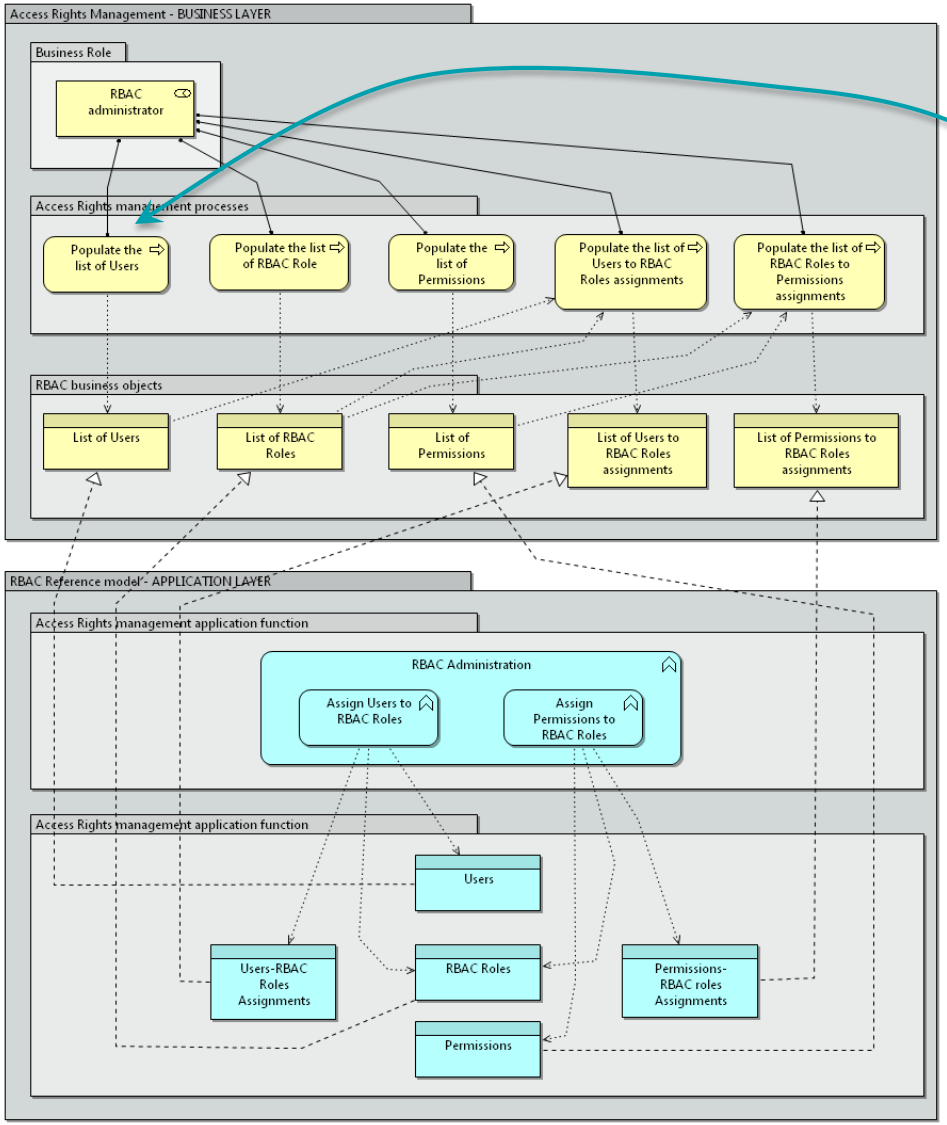
Responsibility-RBAC alignment

Summary of the *trace to* associations



AR MANAGEMENT METHOD

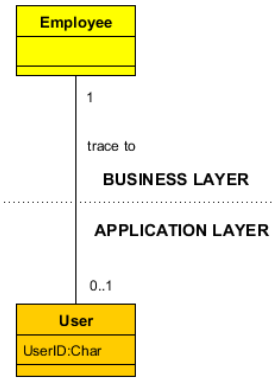
AR Management Reference Model



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

REFERENCES

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY

References

- Feltus, C. Aligning access rights to governance needs with the responsibility metamodel (ReMMo) in the frame of enterprise architecture, 2014, University of Namur, Belgium
- Sein, M.K., Henfridsson, O., Purao, S., Rossi, M., and Lindgren, R. Action design research. MIS Q., 35(1):37-56, March 2011.
- Petit, M., Feltus, C.,Vernadat, F. Enterprise Architecture Enhanced with Responsibility to Manage Access Rights - Case Study in an EU Institution, PoEM 2012, Rostock, Germany.
- Eric S.K.Y. Towards modeling and reasoning support for early-phase requirements engineering. RE '97, Washington, DC, USA, 1997. IEEE.
- Amyot, D., Horkoff, J., Gross, D., and Mussbacher, G. A lightweight GRL profilefor i* modeling. ER 2009 Workshops on Advances in Conceptual Modeling – Challenging Perspectives, Berlin, Heidelberg, 2009.
- Vernadat, F. Enterprise modelling and integration. In ICEIMT, pages 25-33. 2002.
- Parent, C. and Spaccapietra, S. Database integration: The key to data interoperability. Advances in Object-Oriented Data Modeling, 2000.
- Zivkovic, S., Kühn, H., and Karagiannis, D. Facilitate modelling using method integration: An approach using mappings and integration rules. ECIS 2007, pages 2038-2049. University of St. Gallen.
- The Open Group. ArchiMate® 2.1 Specification. Van Haren Publishing, The Netherlands. 2012-2013.
- Band, I. Modeling rbac with sabsa, togaf and archimate. In The Open Group Conference, Austin, Texas. 2011.
- Gaaloul, K. and Proper, H.A.E. An access control model for organisational management in enterprise architecture. In Proceedings of the 9th International Conference on Semantics, Knowledge and Grids. 2013.
- Cenys, A. Normantas, A., and Radvilavicius, L. Designing role-based access control policies with uml. Journal of Engineering Science and Technology Review, 2(1), 2009.
- Shin, M.E., and Ahn, G.-J. Uml-based representation of role-based access control, WETICE '00, pages 195-200, Washington, DC, USA, 2000.
- Ray, I., Li, N., France, R., and Kim, D.K., Using uml to visualize role-based access control constraints. SACMAT '04, NY, USA, 2004. ACM.
- Kim, D.K., Ray, I., France, R., and Li, N. Modeling role-based access control using parameterized uml models. FASE, vol. 2984. Springer, 2004.
- Anderson, A. Xacml profile for role based access control (rbac). Technical Report Draft 1, OASIS, February 2004.
- Object Management Group (OMG). Uml 2.4.1 superstructure specification. 2011.
- Storer, T., Lock, R. Modelling responsibility. Project working paper 7, indeed project. 2008.
- Sommerville, I. Models for responsibility assignment. Responsibility and Dependable Systems 165-186, Springer. 2007.
- Strens, R., and Dobson, J. How responsibility modelling leads to security requirements. NSPW, 143-149, NY, USA. 1993, 143-149.
- Feltus, C., Petit, M. and Dubois, E. Strengthening employee's responsibility to enhance governance of IT: COBIT RACI chart case study. WISG '09. ACM, New York, NY, USA, 23-32.
- Blind, P.K. Accountability in public service delivery: A multidisciplinary review of the concept. Vienna, Austria. 2001.
- Bovens, M. Two concepts of accountability: Accountability as a virtue and as a mechanism. West European Politics, 33(5):946-967. 2010.
- Dubnick, M.J. Situating accountability: Seeking salvation for the core concept of modern governance. TR, University of New Hampshire. 2007.
- White, S.A., Business process modeling notation v1.0. Technical report. 2004.
- Katranuschkov, P., Gehre, A., Scherer, R.J., Reusable process patterns for collaborative work environments in AEC. 13th ICE, Nottingham, UK. 2007.
- Fox, J.A. The uncertain relationship between transparency and accountability. Development in Practice, 17(4):663-671. 2007.
- Karp, A.H., Haury, H., Davis, M.H. From ABAC to ZBAC: The Evolution of Access Control Models, Information Systems Security Assoc. J., 2010.
- Pete A. Epstein. Engineering of role/permission assignments. PhD thesis, Fairfax, VA, USA, 2002.
- H Roeckle, G. Schimpf, and R. Weidinger. Process-oriented approach for role-finding to implement role-based security administration in a large industrial organization. In RBAC '00: 5th ACM WS on RBAC, 2000.
- R. Crook, D. Ince, and B. Nuseibeh. Modelling access policies using roles in requirements engineering. Information and Software Technology, 45(14):979-991, 2003.
- R. Crook, D. Ince, and B.Nuseibeh. On modelling access policies: Relating roles to their organisational context. RE'05, pp 157-166, 2005.
- R. Chandramouli. A framework for multiple authorization types in a healthcare application system. 17th Annual Computer Security Applications Conference, ACSAC '01, Washington, DC, USA, 2001.
- E. B. Fernandez and J. C. Hawkins. Determining role rights from use cases. Second ACM WS on Role-based access control, NY, USA, 1997.
- G.Neumann and M. Strembeck. A scenario-driven role engineering process for functional rbac roles. SACMAT '02, New York, NY, USA, 2002
- A. Kern, M. Kuhlmann, A. Schaad, and J. Moffett. Observations on the role life-cycle in the context of enterprise security management. SACMAT '02, New York, NY, USA, 2002.
- J. Vaidya, V. Atluri, and Q. Guo. The role mining problem: Finding a minimal descriptive set of roles. SACMAT '07, NY, USA, 2007.
- Ferraiolo, D.., et al. "Proposed NIST standard for role-based access control." ACM TISSEC, 4.3 (2001): 224-274.
- Ferraiolo, David, Janet Cugini, and D. Richard Kuhn. "Role-based access control (RBAC): Features and motivations." 11th ACSAC. 1995.
- Feltus, C., Petit, M., Dubois, E. ReMoLa: Responsibility model language to align access rights with business process requirements. In Research Challenges in Information Science (RCIS), 2011. IEEE.