A system theoretical perspective of IT audits in the financial sector

Bernhard Waltl, 19. May 2014

Software Engineering for Business Information Systems (sebis)
Department of Informatics
Technische Universität München, Germany

wwwmatthes.in.tum.de

Motivation

Basel II: a legal regulation in the financial sector

- Obligatory guidelines for supervision and controlling of banks

*„The supervisory review process of the framework is intended […] to encourage banks to develop and use **better risk management** techniques in monitoring and managing their risks."* [1, §720]

Basel II as a driver for national legal regulations

- The Banking Act (KWG)
- Minimum Requirements for Risk Management (MaRisk)
- Journals of BaFin
  - Federal Financial Supervisory Authority

Risk Management in IT systems

Banking Act

"A proper business organization encompasses, in particular, ***appropriate and effective risk management****, which includes the definition of an adequate contingency plan, especially for IT systems."* [2, §25a.1]

Principle of double proportionality

"The ***risk management structure*** *shall* ***depend*** *on the type, scope, complexity and risk content of the business operations performed."* [2, §25a.1]

Risk management in IT systems

- "appropriate" and "effective"
- Assessment (auditing) as the supervisory measure (BaFin)
- Requirements depend on business operations (e.g. type, scope, complexity etc.)
- Content:
  - Staff
  - Technical-organization equipment
  - Emergency plans

Research Questions

I. What is an appropriate model of a comprehensive assessment process in the IT domain?

II. How can requirements be derived from legal regulations?

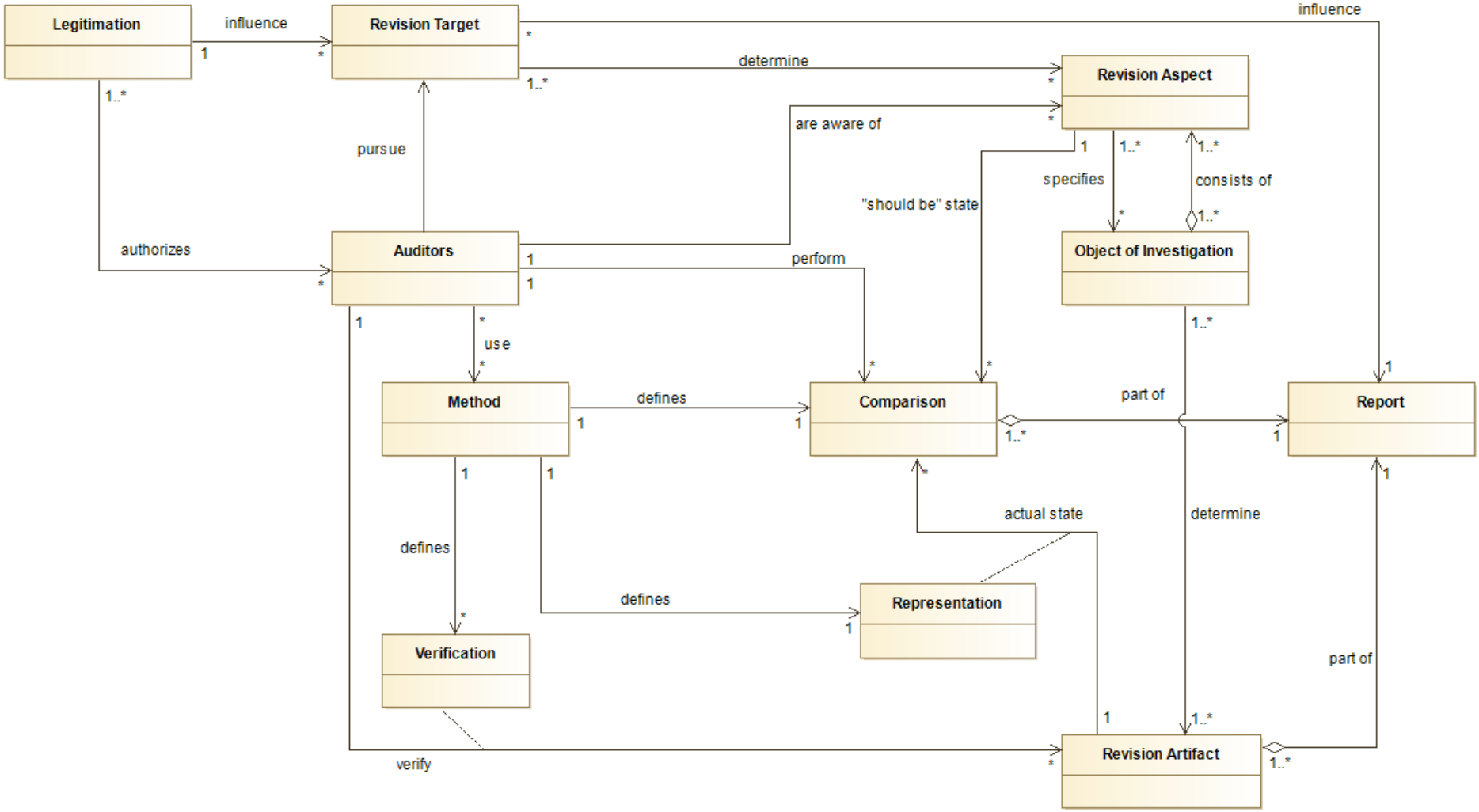
III. What requirements can be derived from legal regulations and how can they be represented?

IV. Can modeling support the audit process and how can normative models look like?

Idea

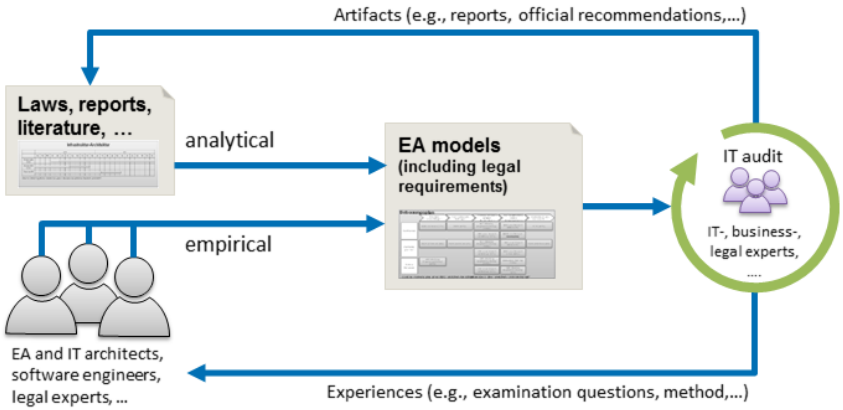
- Analyzing the assessment of IT systems and architectures
- Extracting requirements arising from legal obligations
- Associating legal requirements with concrete IT objects
  - Create a common language by harmonizing terms from the legal domain with the terms from the IT domain
  - Support the audit process (auditor and auditee) by providing normative models representing the „should-be“ state
    - „blueprints“
- Supporting the implementation of compliant risk management processes in the financial sector

IT Audit Meta Model (ITAMM)



Identification of IT requirements

- Identification is challenging
  - Legal texts lack concreteness and interpretation is not uncontroversial
  - Principle of **double proportionality**
- IT audit and requirements within the assessment as information source



- **Analytical**: Objective artifacts (e.g. legal texts, books, reports etc.)
- **Empirical**: Subjective experiences (e.g. interviews, examination questions etc.)

➔ Enhancement of existing EA models with legal requirements

What is the right modeling language?

- **Requirements**
  1. Modeling enterprise architecture [9] (Ia – Ie)
  2. Modeling of legal obligations (intentions, constraints, requirements) [8] (II)
  3. Active Community (III)
  4. Tool support (IV)

- Choosing from a set of possible modeling languages [10]:
  - ArchiMate, BPMN, i*, Tropos, UML

Requirement	ArchiMate	BPMN	i*	Tropos	UML
Ia	++	++	+	o	+
Ib	++	+	o	o	++
Ic	++	o	+	+	+
Id	++	++	o	o	++
Ie	+	++	+	o	++
II	++	o	++	++	o
III	+	++	o	o	++
IV	+	++	+	+	++

Modeling IT architecture and legal requirements

ArchiMate 2.1 [7]

- Open and independent **modeling languages for enterprise architectures**
  - **Business objects** (process, role, service etc.)
  - **Application objects** (interface, component, data object etc.)
  - **Technology objects** (artifact, system software, device etc.)

- Provides a **motivation extension**
  - Requirements, principles and goals representing the intentions of the model
  - Can be used for modeling risks and counter-measures [5]

- **Tool-support**: Archi –The Free ArchiMate Modelling Tool, Version: 2.7.1

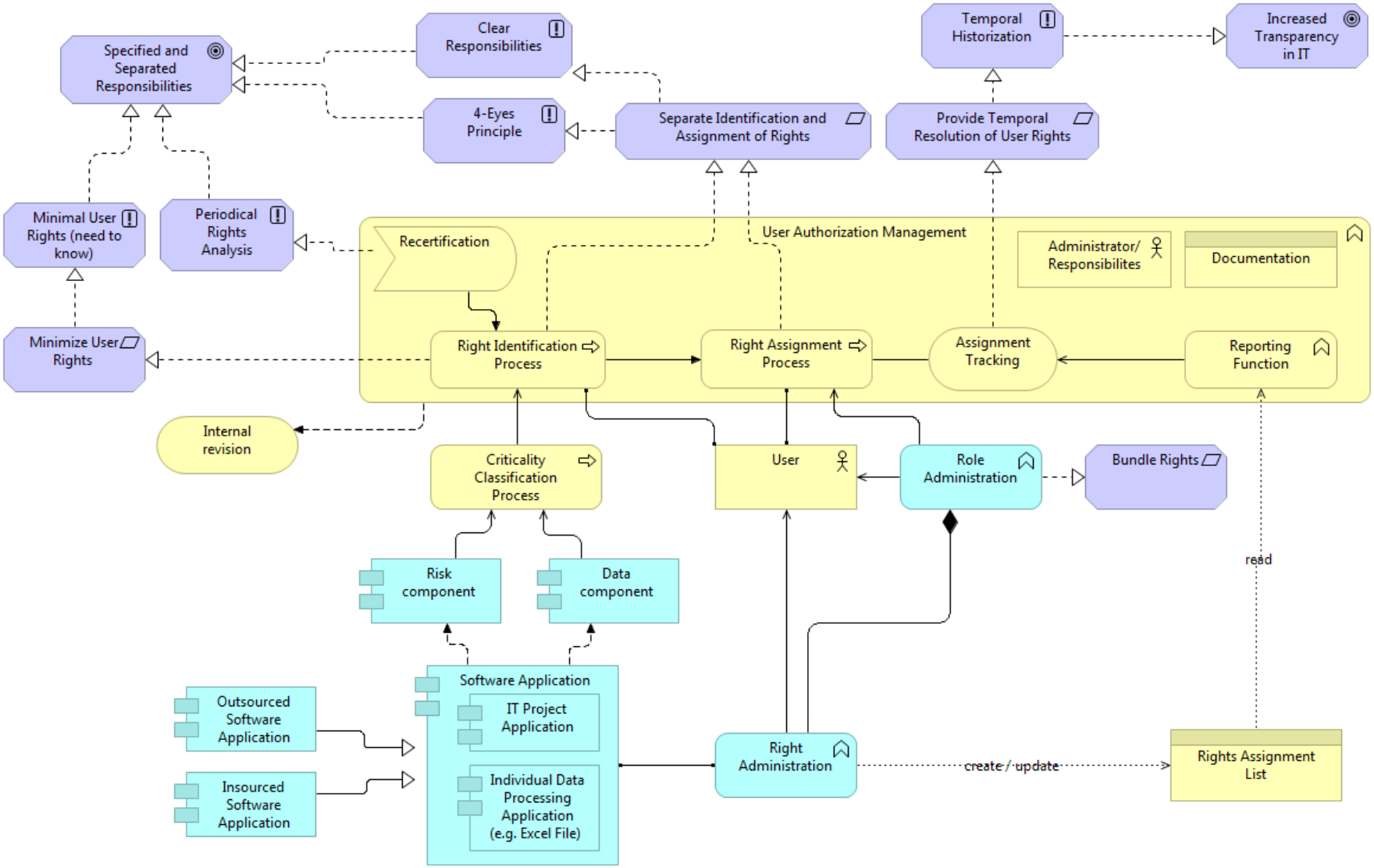
- **Negative aspects:**
  - Not that easy to understand (variety of different elements, colors and arrows)
  - Not very common in the IT of financial industry
  - Not used by auditors

Core examination areas as normative models

- According to BaFin **seven examination areas** are of significant relevance during the IT assessment [8]:
  I. IT strategy
  II. IT risk management
  III. IT revision
  IV. IT outsourcing
  V. Emergency management
  VI. Application development
  VII. User authorization

- **Analysis** of **laws** and **texts** lead to legal obligations
  - **Implicit**: EA objects (processes, functions etc.) as demanded
  - **Explicit**: concrete requirement as „requirement“, „principle“ and „goal“ element

User Authorization Management



Critical remarks

1. Provision of normative models for IT assessments may be irritating
   - **No blueprint** of the „correct“ solution
   - Companies try to pass the examination with minimal effort

2. Modeling with respect to the right **level of granularity** is „impossible“
   - At which stage should the modelling end?
   - E.g. User Authorization
     - No operational user should have root rights!
     - How could this be prevented?

3. **Compliance** is a **process** (according to BaFin)
   - **Static models** as snapshots may impose the opposite
   - Risk management and compliance as business targets

Conclusion

- The method received **positive feedback from practitioners** (IT auditors and banks), however the main remarks concern
  - the level of granularity provided by normative models
  - the blueprint character of the models
  - the compliance as process not as static state

- **Interpreting legal texts** and **associating** obligations **with real-world objects** is a relevant problem (not only for the financial sector!)

- **Legal audits** can serve as an **information source** for concretization of requirements based on legal texts
  - Requirements can either be **analytically** or **empirically** derived
  - **Existing EA models** can be **enhanced** with proper elements and objects

Thank you for your attention!

Bernhard Waltl

Technische Universität München
Department of Informatics
Chair of Software Engineering for
Business Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289.17124
Fax +49.89.289.17136

b.waltl@tum.de
wwwmatthes.in.tum.de

References

[1] Basel Committee on Banking Supervision. International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version, June 2006.

[2] Deutsche Bundesbank. Banking Act, 2009.

[3] Federal Financial Supervisory Institution. Minimum requirements for risk management (MaRisk). 2012.

[4] Klaus Schmidt and Dirk Brand. IT-Revision in der Praxis: Nach den Grundsätzen einer ordnungsgemäßen IT. Carl-Hanser Verlag, Munich, 2011.

[5] Gerben Wierda. Mastering ArchiMate: A serious introduction to the ArchiMate Enterprise Architecture Modeling Language. R&A, Heerlen, 2012

[7] The Open Group. ArchiMate 2.1 Specification. 2013.

[8] Jörg Bretz. Prüfung IT im Fokus von MaRisk und Bundesbank: Verstärkter IT-Fokus in Sonderprüfungen. Finanz Colloquium Heidelberg, 2012.

[9] Marc Lankhorst. Enterprise Architecture at Work: Modelling, Communication, and Analysis, Berlin, Springer 2005.

[10] Eric Yu, Markus Strohmaier, and Xiaoxue Deng. Exploring Intentional Modeling and Analysis for Enterprise Architecture. 10th IEEE International Enterprise Distributed ObjectComputing Conference Workshops, 2006.