Formulating the Enterprise Architecture Compliance Problem

Vytautas ČYRAS
Vilnius University
Lithuania
Vytautas.Cyras@mif.vu.lt

Reinhard RIEDL
Bern University of Applied Sciences
Switzerland
Reinhard.Riedl@bfh.ch

Baltic DB&IS 2012, 8-11.07.2012, Vilnius
Bridging enterprise architecture (EA) and law

I know computing!

I know law!

This is similar to Alan Turing’s “Can machines think?”
Systems engineering view on an enterprise system

1. Enterprise business system
   – business actors
   – resources
   – business processes

2. Enterprise information system
   – information processing actors (IPA)
   – Information flows
   – Information processing processes

3. Enterprise application system
   – hardware agents
   – protocols
   – knowledge bases
   – software application programs
"Naïve" approach. Enterprise architects’ views

Purpose:
- transparency optimization in an organisation

Perspectives:
1) business
2) ICT
3) legal perspective
Compliance methodology

Requirements Engineering
Methodological framework for requirements elicitation, e.g. the Sachman framework

Law
“Shared” law

Enterprise architect

Enterprise system

Legal requirements

Methodology for compliance
Law

• Multi-source, evolving, complex regulations
• Which law?
  – Financial reporting
    • Sarbanes-Oxley Act
    • Corporate governance code
  – Data protection
  – Regulatory compliance standards and codes of practice, e.g. COBIT, SCOR
  – Standards
    • ISO 27001 - Security techniques -- Information security management systems
    • Software development
  – …
Compliance problem [Julisch 2008]

Given an IT system $S$ and an externally imposed set $R$ of (legal) requirements

1. make $S$ comply with $R$
2. provide assurance that auditor will accept as evidence of the compliance of $S$ with $R$

1. Formalise $R$
2. Identify which sub-systems of $S$ are affected by $R$
3. Determine what assurance has to be provided to show that $S$ is compliant with $R$
4. Modify $S$ to become compliant with $R$ and to provide the necessary assurance
Machine-based or machine-assisted decision making?

Plaintiff

A case factual situation

Defendant

Judge-machine

Law

No!

Legal decision
“Practical” motivation for academia

- **STORK 2.0 project**
  - Title: Secure idenTity acrOss boRders linKed
  - Big picture:
    - from interoperability to a single identity space for borderless e-business
    - Work package dedicated to legal requirements
  - e-Banking Pilot (10 countries, 4 + n banks)
    - Leaders: ATOS (Spain) + Bern University of Applied Sciences
    - Participation of Lithuania
      - The Ministry of the Interior + “Infostruktūra” + “Ūkio Bankas”
  - Big picture beyond the e-banking pilot project:
    - moving Identity and Access Management out of the core banking IT system
Motivation for academia

• STORK 2.0 use case to check for compliance
  – A company representative with an eID from country X (e.g. Germany), working in a company from country Y (e.g. Switzerland) logs into a banking platform in country Z (e.g. Lithuania)

• Common infrastructure for federated e-government
  – Today’s challenges
    • Organizational & business models
    • Implementation of a government cloud
    • Refinement of the existing enterprise architecture in order to get it “working”
  – Tomorrow’s challenge
    • Enterprise architecture design for the implementation of the Lenk/Schaffroth/Schuppan vision of networked government in Switzerland
  – Future challenge
    • Separation of distribution, execution, and control in order to implement secure service centers for core state tasks
Academia and the compliance problem

- K. Julisch: “sell” compliance, not security
- Academia’s added value?
  - Research on regulatory compliance
- Strengths in academia vs. business
  - Models vs. practices
RE framework

- Zachman framework [1987]
  - architectural [1992]
  - 6 perspectives:
    - planner’s, owner’s, designer’s, builder’s, integrator’s and owner’s
- Čaplinskas [2009]
  - vision driven
  - strategic alignment
    1. business analyst
    2. stakeholder
    3. IS analyst
    4. IS engineer
    5. software analyst
  other views (see textbooks):
    software architect, software engineer, process engineer, tester, etc.
“Naïve” methodology?

Fill in the focus areas (e.g. in Čaplinskas’ framework)

- **Why?** Motivation
  - Vision of the system from the corresponding perspective

- **How?** Service requirements
  - What services are required to support the vision?

- **What?** Objects requirements
  - What kind of objects shall process the system?

- **Who?** Accessibility requirements
  - Who will use the system?

- **Where?** Workplaces requirements
  - What workplaces are required for each “who”?

- **When?** Efficiency requirements
  - What delivery time for each of services?
Holistic approach

Regulation and IT alignment framework [Bonazzi et al. 2009].
http://en.wikipedia.org/wiki/Governance,_Risk_Management,_and_Compliance
Framework vs. procedure

- Framework – static
  - Terminology
  - Formal models
  - In the focus of academia
- Procedure – dynamic
  - Good practices
  - In the focus of business
No silver bullet

• No one-off, best-of-breed solution
• “Hardly any scientific research on GRC” [wikipedia]
• Different levels of capability to understand
  – Compliance maturity models
  – Complex phenomena: EA, law, etc.
Difficulties inherent in law

1. **Abstractness of norms.** Norms are formulated (on purpose) in abstract terms.
2. **Principle vs. rule.** The difference in regulatory philosophy between the US and other countries.
3. **Open texture.** H. L. A. Hart’s example of “Vehicles are forbidden in the park”.
4. **The myriad of regulatory requirements.** Compliance frameworks are multidimensional.
5. **Heuristics.** High level concepts are translated into invented low level ones.
6. **Teleology.** The purpose of a legal norm usually can be achieved by a variety of ways. They need not to be listed in a statute and specified in detail.
7. **Legal interpretation methods.** The meaning of a legal text cannot be extracted from the sole text. Apart from the grammatical interpretation, other methods can be invoked, such as systemic and teleological interpretation.
8. **Consciousness of the society.** Modeling it is a tough task.
Governance, Risk and Compliance

• Financial GRC
  – correct operation of all financial processes

• IT (Information Technology) GRC
  – IT supports business needs
  – complies with IT-related mandates

• Legal GRC
  – via an organization's legal department and Chief Compliance Officer
“GRC is an integrated, holistic approach to organisation-wide governance, risk and compliance ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness."

http://en.wikipedia.org/wiki/Governance,_Risk_Management,_and_Compliance
Conclusions

• Reflections on different issues were presented
• No silver bullet
• Enterprise Architecture Compliance Problem formulation is of theoretical nature