Assessing Investments into Enterprise Identity Management (EIdM)

Towards a Decision Support Approach

Denis Royer

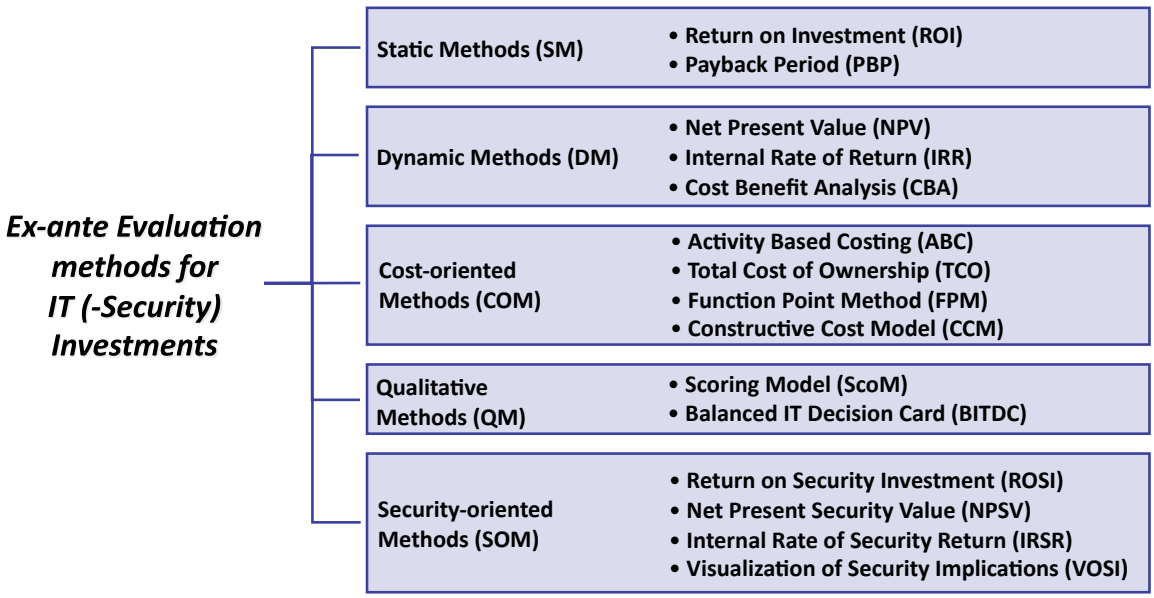
Agenda

- Introduction
  - Research Questions
  - Enterprise Identity Management (EIdM)
- Results
  - Expert Interview Series
  - Derived Theory and Constructs
  - Decision Support Approach
- Decision Support Tool
- Conclusion

Introduction/Motivation

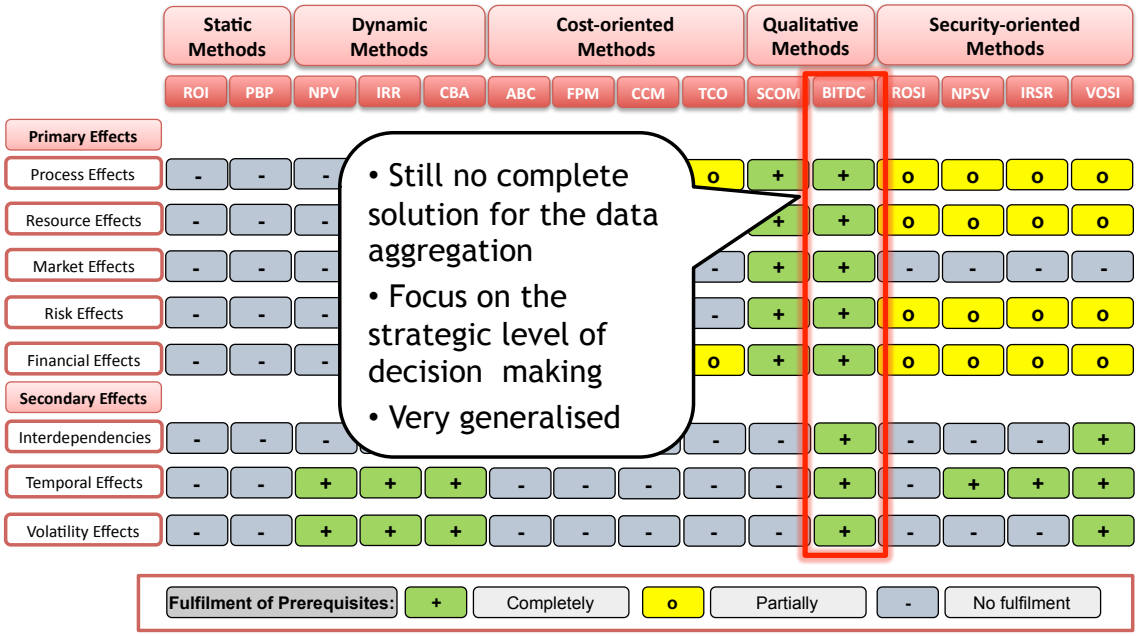
- Problems started with Client/Server applications and distributed computing
  - Segregation of rights
  - Role and permission handling
- Enterprise identity management systems (EIdMS) were introduced to overcome some of the issues
- These “hybrid” IT systems are costly and require comprehensive knowledge about the organisation itself, such processes, technology, and assets.
- Consequently, decision maker cannot decide due to the diverse nature of this technology and the impacts on the organisation itself

Ex-ante Evaluation methods for IT (-Security) Investments



own representation based on [Walter and Spitta (2004)]

Ex-ante Evaluation methods for IT (-Security) Investments



[own representation]

Research Question

> **"How can the decision making process concerning investments into EIdM be supported?"**

- Segregated into 4 sub-questions:
  - Which are the methods that can be used to assess investments into EIdM?
  - Which methods are applied in practice (e.g. in the corporate field for decision support) and what are their shortcomings?
  - What are the actual requirements and properties needed to assess investments into EIdM in order to address the shortcomings?
  - How can these requirements and properties be applied into a decision support instrument for the assessment of EIdM and how can the model/method be evaluated?

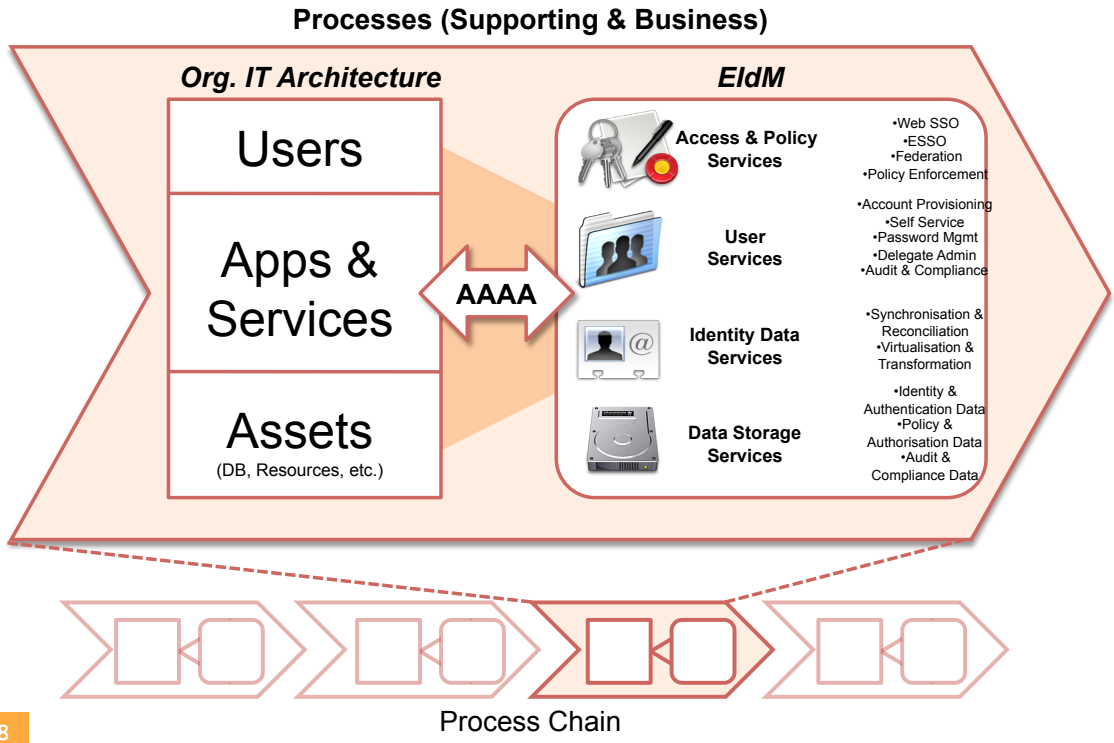
Some Dimensions of EIdM

- **Organisational:** Software systems that help to facilitate one or more of the 4 As: **A**uthorisation, **A**uthentication, **A**dministration, and **A**udit
- **Technological:** Cluster of different technologies,
  - Single/Reduced Sign-On, Meta Directories, PKI, Access Management Systems
  - ➔ EIdM is a framework of different technologies, not a specific product, that serves on the (IT-) infrastructure level of an organisation.
- **Goals:** Amongst a variety of driving factors and reasons for introducing EIdM into an organisation
  - Primary: business-related goals, compliance goals
  - Secondary: risk management / IT security goals, new business opportunities

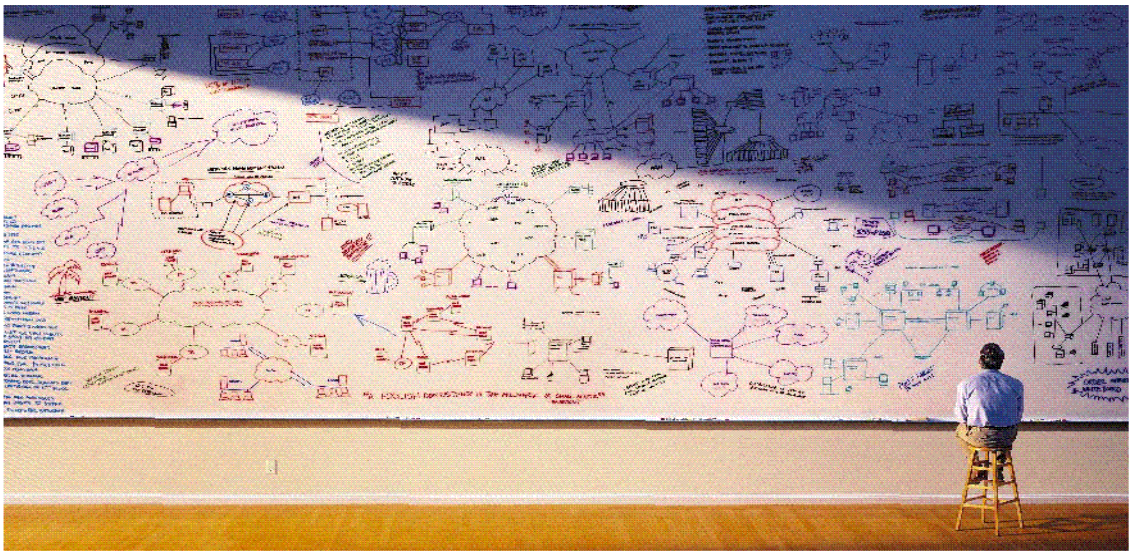
➔ The goals itself are not mutually exclusive – however, there are overlaps.

- ➔ EIdM projects are no ends in themselves → They are introduced to obtain a specific goal.

EIdM in Business Processes



Identity Management…



…if it only was easy…

Preliminary Assessment: So… What's the Problem?

- **EIdM projects are complex:**
  - EIdM is an architectural IT building block, offering a communication infrastructure for the "4As" between different systems/services and the management of the Id-Lifecycle.
  - Also, EIdM is more process-oriented than an issue of technology
- **They have various effects on the organisation:**
  - Processes, people, politics, [price]…
  - Derivation of the optimal level of investment into IS security is difficult
- **Available evaluation approaches for IT and IT security investments are to narrow:**
  - No approach is yet capable of capturing the potential benefits form the introduction of EIdMS
  - Data collection puts high demands on decision makers (how to collect what data and where, required accuracy, comparability of results)

Expert Interviews: Overview

- 11 people interviewed experts in the field of integrators, vendors, and users
  - Sample: 5 integrators, 2 vendors, and 4 users
  - Between 8 to 15 years of experience in the field of EIdM

- ***Language community:*** foundation for communication with shared symbols, concepts, and terminology already existed within the group (cf. Holten 2007, p. 3).

- Material was analysed, using the Qualitative Content Analysis for deriving patterns from the statements made by the interviewees.

Expert Interview: Goals for EIdM Projects

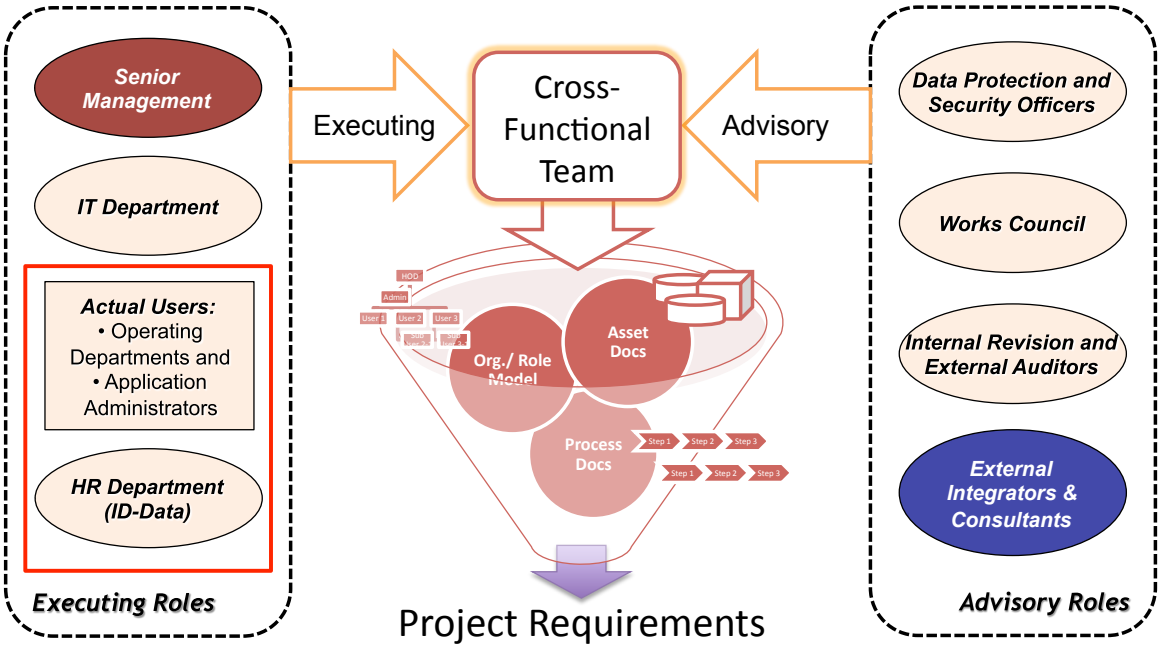
- EIdM projects are no ends in themselves → They are introduced to obtain a specific goal.
- Amongst a variety of driving factors and reasons for introducing EIdM into an organisation, the most prevalent are:
  - Primary goals:
    - Business-related goals (e.g. efficiency, automation of processes, general cost reduction, accounting for IT costs)
    - Compliance goals (constraint for organisations)
  - Secondary goals:
    - Risk management / IT security goals
    - Enabler for new business opportunities

➔ The goals itself are not mutually exclusive – however, there are overlaps.

Expert Interview: Which are the Problem Fields?

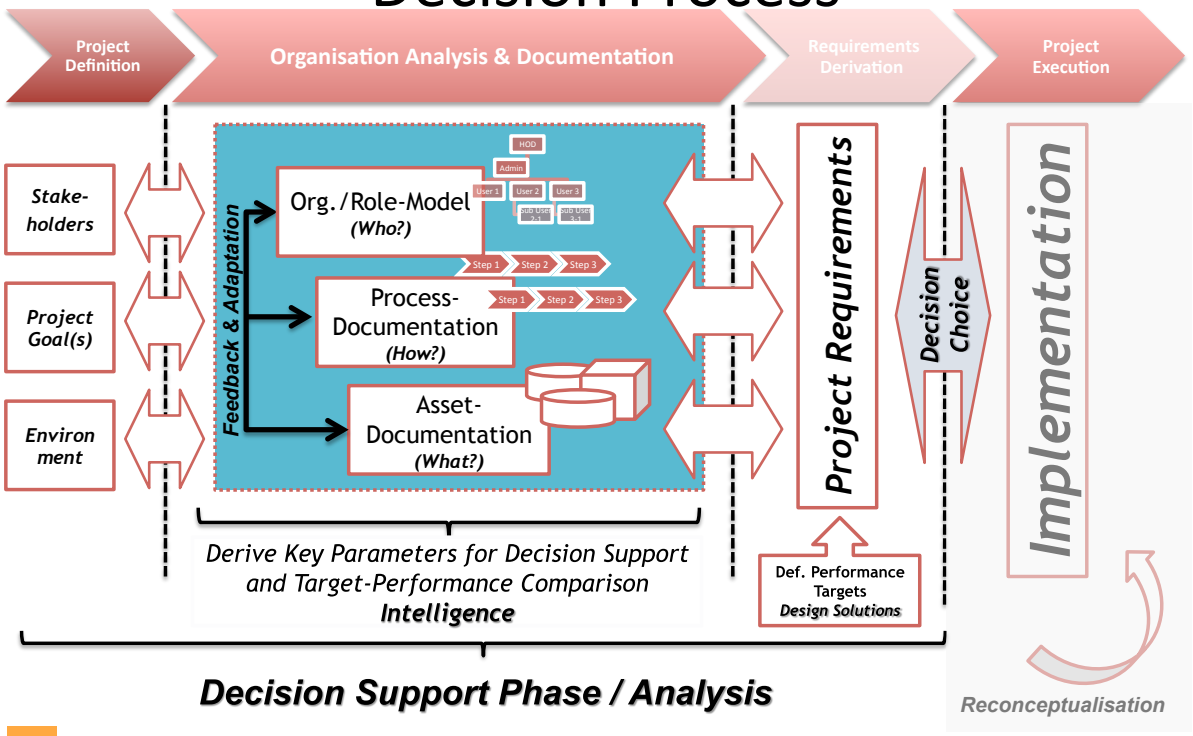
- ***Organisational factors***
  - Goal of an EIdM Project
  - Stakeholders
    - Sponsorship of a project
    - Enforcement of an EIdM project in an organisation
    - Responsibilities for the EIdM
  - Identification of topologies, roles, permissions, etc. (role-mining, data quality)
  - Delivery of ID data
  - Knowledge and analysis of the processes (EIdM and business) and their maturity
  - Political decisions (favored vendors, changes of the org. culture, etc.)
- ***Complexity of technical systems***
  - Heterogeneity of the systems and the infrastructure in an organisation
  - Availability of systems
- ***Operationalisation of projects***
- ***Description and knowledge about the implication of EIdM at the decider's level***

Stakeholder Model for EIdM Model



[own representation]

Expert Interview: EIdM Project Decision Process



Parameter Categories

	Parameter Category	Response Frequency	Specific Topic Areas

1	**Process**	**(N=11)**	• Documentation (also as target-performance comparisons):
			  ○ Inventory of processes identified with regard to EIdM
			  ○ Number of process steps
			  ○ Number of process exceptions
			  ○ Number of media breaks in processes
			• Ratio integrated vs. not integrated processes
			• Target-performance comparison of the cycle time for EIdM processes (e.g. provisioning, change of attributes)
			• Process maturity level (e.g. based on the capability maturity model)

2	**Monetary aspects**	**(N=11)**	• Project costs
			  ○ Organisational and process analysis
			  ○ Integration of EIdM solution and costs per integration / degree of customisation
			  ○ Costs for running the EIdMS
			• General operational costs of the organisation currently, based on the actual processes – e.g. as costs per incident or costs per person
			• Costs savings with regard to software licences, help-desk-calls, etc.
			• Budgets

3	**Quality**	**(N=11)**	• Overall quality of the organisational documentation • Quality of available ID data (e.g. as scoring) • Number of variations in target-performance comparisons

Parameter Categories (cont'd)

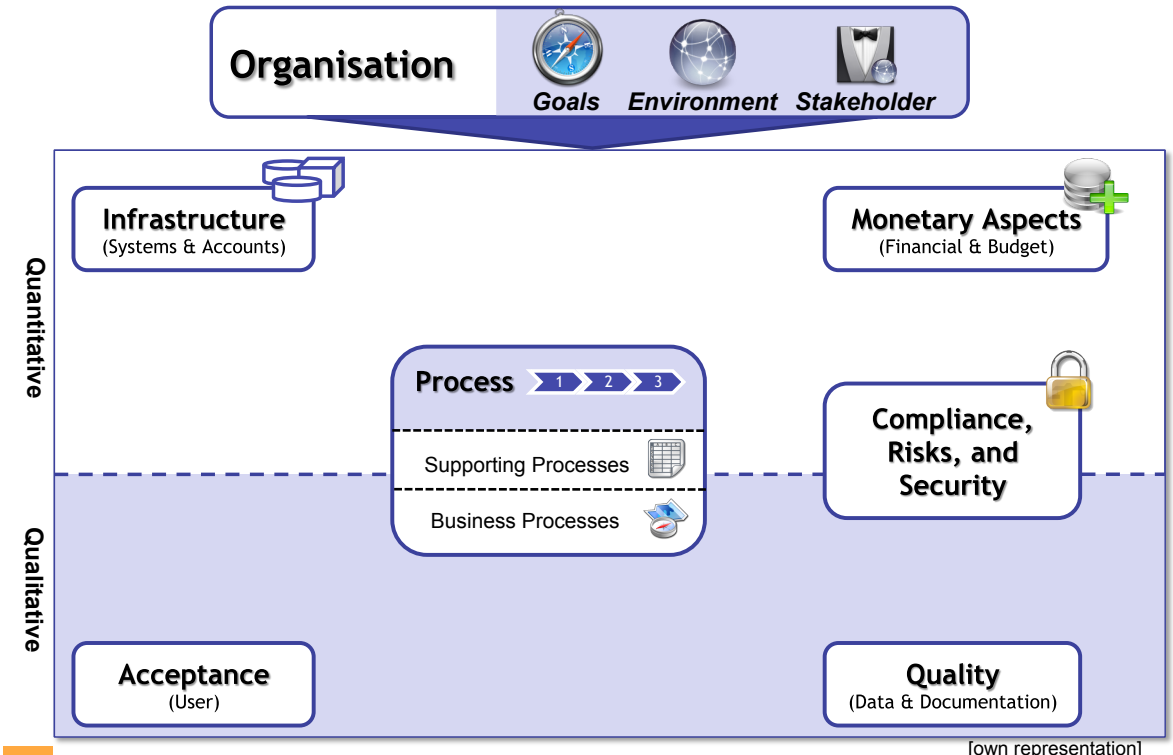
	Parameter Category	Response Frequency	Specific Topic Areas

4	**Infrastructure**	**(N=8)**	• Existing Systems
			  ○ Number of systems / coverage
			  ○ Priority/Importance of integration
			  ○ Number of existing platforms (operating systems)
			  ○ System owner
			  ○ Number of identified shadow-IT
			  ○ Number of interfaces between systems
			• Number of users / Accounts
			  ○ Mapping of Users/Accounts
			  ○ Number of issued credentials (per user/system)
			  ○ Number of Software packages used per user

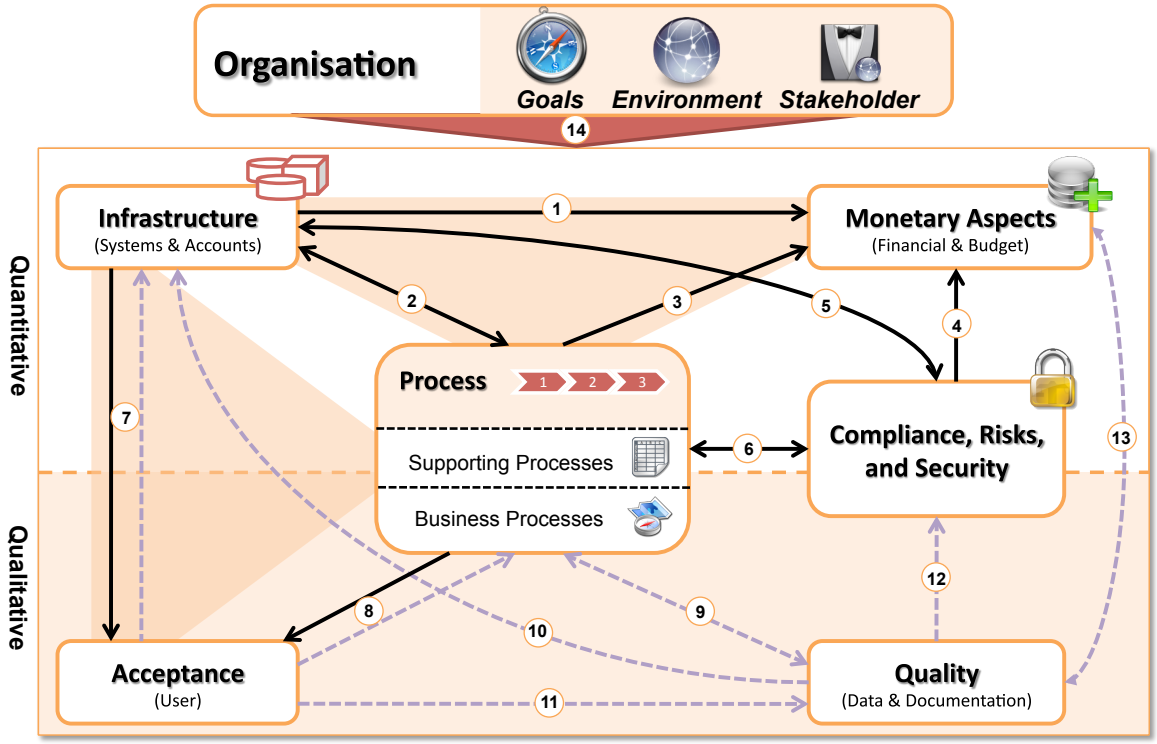
5	**Compliance, Risks, and Security**	**(N=8)**	• Documentation and assessment of risks/risk classes
			  ○ Costs per incident
			  ○ Probability of incidents
			  ○ Importance of affected processes
			  ○ Protection requirements for systems
			• Compliance specifications
			• Deposit of capital for compliance incidents
			• Number of incidents
			• Number of rules, roles, and permissions

6	**Acceptance**	**(N=3)**	• General acceptance of EIdM systems by users (surveys)

Derived Model



[own representation]

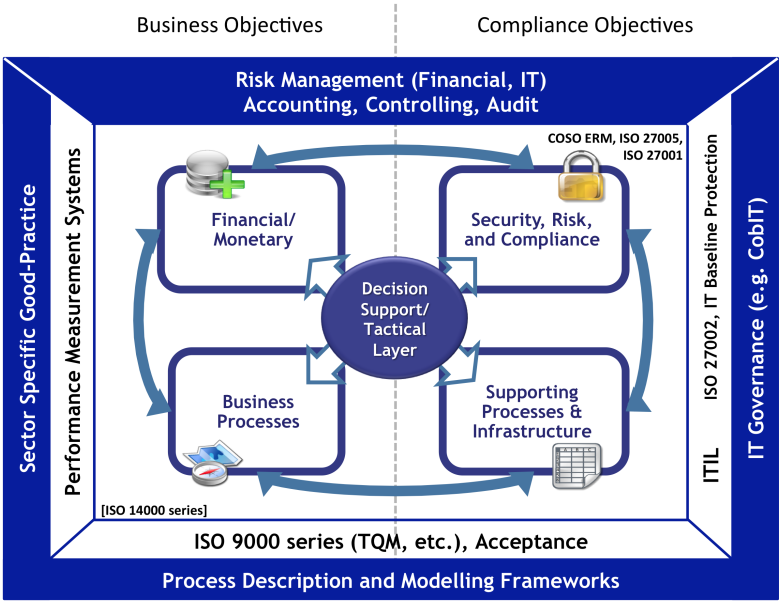


Expert Survey → Validation of the Model

19 Anzahl

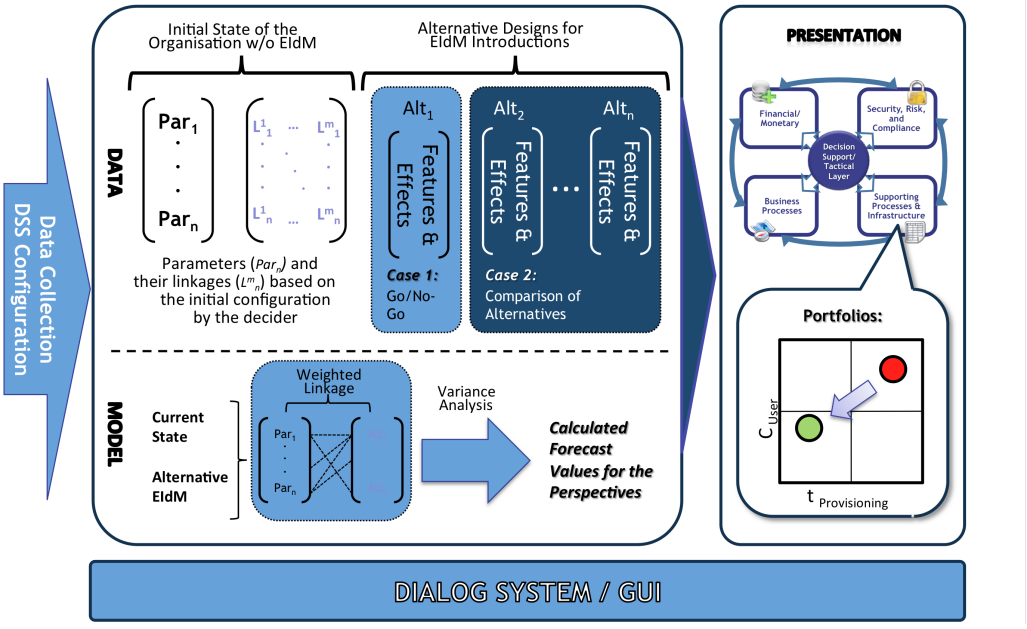
		Already Interviewed Experts							External Experts											Analysis				
		Int 1: 1-I-2002	Int 2: 2-I-2005	Int 3: 4-V-0506	Int 4: 6-U-2106	Int 5: 8-U-2706	Int 6: 10-I-1108	Int 7: 11-I-2209	Ext 1	Ext 2	Ext 3	Ext 4	Ext 5	Ext 6	Ext 7	Ext 8	Ext 9	Ext 10	Ext 11	Ext 12	Comment (o)	Yes (y)	No (n)	Full Agreement	Partial + Full Agreement
Constructs																								
A	Procsess (P)	y	y	y	y	y	y	o	y	y	y	y	y	y	y	y	y	y	y	y	1	18	0	95%	100%
B	Monetary (M)	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	0	19	0	100%	100%
C	Quality (Q)	y	y	y	y	y	n	y	y	y	y	y	y	y	y	y	y	y	y	y	0	18	1	95%	95%
D	Infrastructure (IS)	y	y	y	y	y	y	y	y	y	y	y	y	y	o	y	y	y	y	y	1	18	0	95%	100%
E	CRS	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	0	19	0	100%	100%
F	Acceptance (A)	y	y	y	y	y	y	y	y	o	y	y	y	y	o	y	y	y	y	y	2	17	0	89%	100%
Linkages																									
1.	Environment	y	y	y	y	y	o	y	y	y	y	y	y	y	y	y	y	y	y	y	1	18	0	95%	100%
2.	IS → M	y	y	y	y	y	y	o	y	y	y	y	y	y	y	y	y	y	y	y	1	18	0	95%	100%
3.	IS↔ P	y	y	y	y	y	y	y	y	y	y	y	y	y	y	o	y	y	y	y	1	18	0	95%	100%
4.	CRS → P	y	y	y	y	y	y	o	y	y	y	y	y	y	y	n	y	y	y	y	1	17	1	89%	95%
5.	CRS → M	y	y	y	y	y	o	o	o	y	n	y	y	y	y	n	y	y	y	y	3	14	2	74%	89%
6.	CRS ↔ (IS & P)	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	y	0	19	0	100%	100%
7.	IS ↔ A	y	y	y	y	y	y	y	o	y	y	y	y	y	y	y	y	y	y	y	1	18	0	95%	100%
8.	P ↔ A	y	y	y	y	y	y	y	o	y	y	y	y	y	y	y	y	y	y	y	1	18	0	95%	100%
9.	Q ↔ P	y	y	y	y	y	o	y	y	y	y	y	y	y	y	n	y	y	y	y	1	17	1	89%	95%
10.	Q ↔ IS	y	y	y	y	y	y	y	y	o	y	y	y	y	y	y	y	y	y	y	1	18	0	95%	100%
11.	A → Q	y	y	y	y	y	y	o	y	o	y	y	y	y	y	n	y	y	y	y	2	16	1	84%	95%
12.	Q → CRS	y	y	y	y	y	y	y	y	o	y	y	y	y	y	n	y	y	y	y	1	17	1	89%	95%
13.	Q → M	y	y	y	y	y	y	o	y	y	y	y	y	y	y	y	y	y	y	y	1	18	0	95%	100%

EIdM Balanced Scorecard

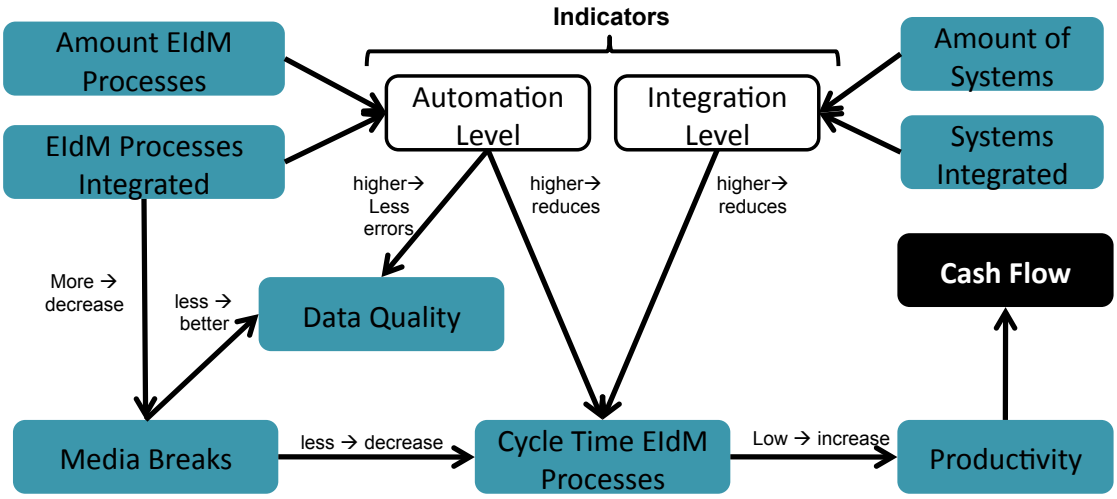


[own representation]

Building a Decision Support System



Exemplary Indicator Pattern: Integration-Automation Level

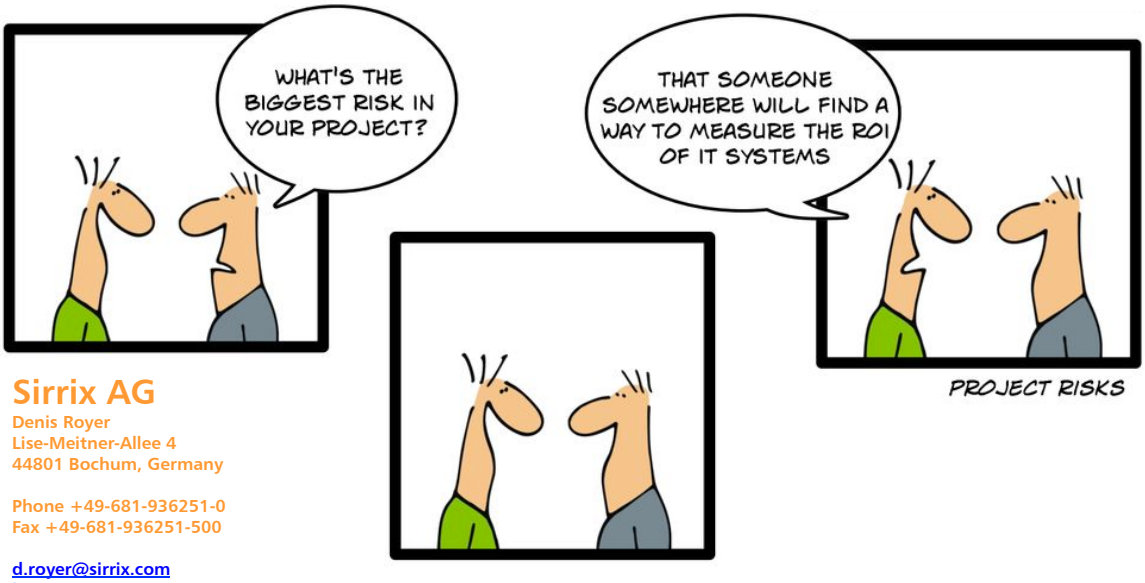


Summary: Core Results & Research Contribution

- Core results of the research:
  - The result is a model (the artefact) for decision making whether organisations should invest into the introduction of an EIdM solution or not.
- Research contribution - esp. design foundations for analysing EIdM projects:
  - Identification of the relevant problem areas and ”stumbling blocks” when introducing EIdM (e.g. relevant stakeholders, collection of data, and their aggregation).
  - Identification of the relevant constructs and decision parameters for the introduction of EIdM solutions into an organisation (What matters?).
  - Understanding of the interdependencies and the effects between the constructs and the relevant decision parameters

[Hevner et al. (2004)] and [Gregor, S. (2006)]

It’s your turn now . . .



Sirrix AG
Denis Royer
Lise-Meitner-Allee 4
44801 Bochum, Germany

Phone +49-681-936251-0
Fax +49-681-936251-500

d.royer@sirrix.com
http://www.sirrix.com