UNIVERSITEIT GENT

FACULTY OF ENGINEERING AND ARCHITECTURE

A Quest for Theoretical Foundations of COBIT 5

Jan Devos & Kevin Van de Ginste

Ghent University, Campus Kortrijk, Belgium

Outline

- Problem
- Research Question
- Methodology
- Findings
- Conclusion

Problem

- IT/IS research is **slow** (and a **new**) discipline
- IT/IS has a **practical** kernel which is fast moving where **speed** has won against quality (Cross 2011)
- Practitioners (consultants/large organizations) are developing own methods and frameworks to **evaluate** IT/IS

  e.g. COBIT, ITIL, CMMi, PMBoK, PRINCE2, …
- Not (always) **theoretically** founded (Ridley et al. 2008, Goldschmidt et al. 2009, Choi and Yoo 2009, Chen and Shen 2010)

Problem (cont)

- Hard to **supplant** frameworks and methods to other environments (SMEs, universities, not-for-profit)
- Still a lot of **IT/IS failures** (Avison et al. 2006, Conboy 2010, Dwivedi et al. 2013)
- IT/IS evaluation is under researched

Example: COBIT 5

- COBIT 5 (Control Objectives for Information and Information related Technologies)
- IT governance, management and audit framework well-known in IT/IS practitioners communities (ISACA 2012a)

Domain	Type of Domain	Number of processes
Evaluate, Direct and Monitor (EDM)	Governance	5
Align, Plan and Organize (APO)	Management	13
Build, Acquire and Implement (BAI)	Management	10
Deliver, Service and Support (DSS)	Management	6
Monitor, Evaluate and Assess (MEA)	Management	3

Research Question

Does COBIT have visibly theoretical foundations that can support (some of) the claims made in the framework?

Methodology (cont)

- Reverse Engineering work
- Selection of excising IT/IS theories (not grounded theory method) (Larsen et al. 2014)
- Mapping theoretical propositions to empirical observations (pattern matching) (Yin, 2003, ISO/IEC 15504-2)

Methodology

Which IT/IS theories?

- Truex criteria (Truex et al. 2006)

Preparing the theories

- a classification, an analysis, and a summary of developed components according to Gregor (2006)

	Theories		
Truex criteria	**Stakeholder Theory**	**Principal Agent Theory**	**Technology Acceptance Model**
Fit between theory and phenomenon	SHT fits very well with facts in COBIT. The first key principle of COBIT refers already to the broad phenomenon of stakeholders.	PAT focussed on a fundamental relation between two actors. An information system is a nexus of principal-agent relations: e.g. owner-manager, user-developer, auditor-CIO, …	A substantial critic to COBIT is the 'mechanical' way the framework is constructed and the ignorance of the user as reflective human actor (Hoogervorst 2008). It makes it challenging to investigate how TAM could fit or not with the propositions of COBIT.
Historical context of theory	The concept of stakeholder has gradually grown from shareholder to a general concept of all actors that could have a stake in an artefact or organisation.	PAT is one of the cornerstone theories of organisations.	TAM is one of the only successful IS theories designed from within the IS discipline. Although the theory has been criticized by many, current relevant IS research is still using TAM.
Impact on the research method	SHT is a process theory which is compliant with the basic perspective of our research method (qualitative and a mixture of positivism and interpretivism).	PAT has two streams: positivistic agent theory and principal agent theory. We conducted the last stream (Eisenhardt 1989)	TAM is constructed as a variance theory. However the operationalization of the constructs (acceptance perceived ease of use and usefulness) can be also assessed from a process perspective.
Contribution to cumulative theory	SHT has been used in ten previous works in IS research (Larsen et al. 2014)	PAT has been used in 24 previous works in IS research and has links with other theories used in IS research (Larsen et al. 2014)	TAM is one of the few genuine IS theories, in the sense that the theory is not borrowed from other disciplines. TAM has been used in 64 previous works in IS research and has a profound link with the DeLone & McLean Success Model (Larsen et al. 2014)

Overview of Stakeholder Theory (SHT)	
SHT is a management theory that identifies groups and individuals that have a stake in an organisation (Frooman 1999). The theory helps to identify, understand and use in a strategic way stakeholders in an organisation. SHT explains how stakeholders can affect the organization. SHT gives answers to three key questions: 1) Who are the stakeholders (Mitchell et al. 1997), 2) What do the stakeholders want? and 3) How do stakeholders influence?	
Theory Component	Instantiation
Means of representation	Words, lists, tables and diagrams
Primary constructs	Questions, groups and individuals
Statements of relationships	Relations between the stakeholders and the organization
Scope	The relations of an organization
Causal explanations	SHT explains the relation between stakeholders and organization by stating how stakeholders will impose their will.
Testable propositions	Questions can be composted and tested by interviews
Prescriptive statements	Only for the questions 1 and 3

Methodology

Principles

1: Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single, Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management

Goals (BSC)

- 02 IT compliance and support for business compliance with external laws and regulations
- 07 Delivery of IT services in line with business requirements
- 10 Security of information, processing infrastructure and applications
- 16 Competent and motivated business and IT personnel

Processes (security oriented)

- APO13 Manage Security,
- BAI06 Manage Change,
- DSS05 Manage Security Services
- EDM03 Ensure Risk Optimisation
- MEA03Monitor, Evaluate and Assess Compliance with external Requirements

Methodology

- **Score N**: (Not Present) There are no propositions, keywords or statements in COBIT that can be matched with components of one of the selected theories.
- **Score P**: (Present) There is a least one proposition, keyword or statement in COBIT that can be matched with one components of one or more of the selected theories.
- **Score L**: (Largely present) There is more than one proposition, keyword or statement in COBIT that can be matched with one theory.
- **Score F**: (Fully present) There is a strong match of several (more than two) COBIT propositions, keywords or statements with one theory.

FINDINGS	SHT	PAT	TAM
Meeting Stakeholder Needs	LP	LP	N
Covering the enterprise End-to-End	LP	LP	N
Applying a Single Integrated Framework	P	P	N
Enabling a Holistic Approach	N	N	N
Separating Governance From Management	LP	F	N
APO13 Manage Security	LP	LP	P
BAI06 Manage Change	P	LP	P
DSS05 Manage Security Services	LP	LP	N
MEA03 Monitor, Evaluate and Assess Compliance with external Requirements	LP	LP	N
EDM03 Ensure Risk Optimisation	LP	F	P
Goal 2 - IT compliance and support for business compliance with external laws and regulations	P	LP	N
Goal 7 - Delivery of IT services in line with business requirements	N	N	P
Goal 10 - Security of information, processing infrastructure and applications	P	LP	N
Goal 16 - Competent and motivated business and IT personnel	N	N	P

Findings

- The strongest theoretical foundations in COBIT are coming for **PAT**. PAT is a theory that is often used to explains elements of control in a governance versus management setting
- There is also coupling in appearance between **PAT** and **SHT**
- TAM is less present in COBIT. This can be due to the fact that TAM is a higher type of theory, with strong causal relations
- IT-related goals can strongly determine the presence of a theory. **This is the way around**, a framework should be designed with a theoretical stance in the first place

Findings

e.g.

- IT-related goal 07 (Delivery of IT services in line with business requirements) suggest to be based on TAM and brings the theory into the process BAI06 Manage Change.
- IT-related goals 02 (IT compliance and support for business compliance with external laws and regulations) and 10 (Security of information, processing infrastructure and applications) bring in PAT in APO13 Manage Security and DSS05 Manage Security Services.

Conclusions

- The strong appearance of **PAT** and **SHT** in COBIT is probably due to the fact that both theories are lower types of theories Gregor (2006).
- COBIT was originally build as an IT audit guideline, so control (PAT) and stakeholders (SHT) are key elements there.
- Only prescriptive statements from SHT are (limited) present. To fully implement SHT one could use the findings of Mitchell et al. (1997) to assess the **influence** of each stakeholder. Together with the findings of Frooman (1999) the framework could be enriched with the way **how** stakeholders try to execute their influence. This could lead to better or more fine-tuned metrics.

Conclusions

- COBIT did not took off from a **clear** theoretical starting position
- Derived theoretical propositions from the selected theories are **present** in the framework, albeit not always complete (e.g. SHT)
- Primary constructs, scope and statements of relationship of the theories are often found, but causal explanations are often absent
- Some theories do not have very clear causal explanations, so type I and type II theories have a higher likelihood to be supportive for COBIT. (e.g. PAT).

Conclusions

- What other theories are present in COBIT? (e.g;. Resource Based Theory, Transaction Economics, and Structuration Theory)
- The assessment model of scoring the presence of a theory in COBIT can be more ine-tuned.