Ontology-Based Evaluation of ISO 27001

Danijel Milicevic, Matthias Goeken

Ontology-based Evaluation of ISO 27001

Danijel Milicevic, Matthias Goeken

Frankfurt School of Finance & Management
IT-Governance-Practice-Network
Sonnemannstrasse 9-11
60314 Frankfurt am Main, Germany
{ d.milicevic, m.goeken } @ fs.de

Abstract. Information security risks threaten the ability of organizations of reaching their operational and strategic goals. Increasing diversification of the information security landscapes makes addressing all risks a challenging task. Information security standards have positioned themselves as generic solutions to tackle a broad range of risks and try to guide security managers in their endeavors. However, it is not evident if such standards have the required holistic approach to be a solid foundation. In this paper a metamodel of the ISO 27001 security standard explicating its core concepts is presented. We then compare the constructed metamodel with various information security ontologies and analyze for comprehensiveness. We conclude with a discussion of core concepts in the information security domain.

Keywords: Information Security Management, ISO 27001, Metamodeling, Ontologies, Qualitative Data Analysis (QDA), Grounded Theory

1 Introduction

Regardless if an information system is being planned and used for e-voting, sales via an e-shop or online banking, with all the benefits information systems provide they also come with inherent risks. Information security has gained attention in a number of organizations, be it in the industry or governments. As [2] point out, (exploitable) software vulnerabilities and virus attacks are only two typical threats security managers need to address along with disgruntled employees, social engineering attacks and industrial espionage to name a few. Because security – like a chain – is only as strong as its weakest link, an information security management system requires a holistic approach if one wants to ensure effectiveness [4, 5, 12].

The need for guidance on information security management and common reference points across companies and industries [14] lead to information security standards and best practice frameworks being established. As a collection of best practices on how to deal with most common security risks they provide an overview of the multifaceted information security problem domain [31]. Some researchers have criticized their validity and especially pointed out the lack of depth or content [29]. While depth may be one dimension to scrutinize, we are interested in how comprehensive such information security standards are. To analyze how comprehensive one of the most

prominent standards – ISO 27001 – is, we derive the information security concepts covered in it and compare them with information security ontologies.

The paper is organized as follows. In the next section we introduce metamodels as one central research artifact [18], discuss their application and present the basic ideas of applying qualitative data analysis (QDA). After a brief overview of related work, we elaborate on our findings from the analyzed source documents (ISO 27001) and present a metamodel. Then we compare the elements of our metamodel with a selection of ontologies before we conclude the paper in the final section with a discussion.

2 Research Methodology

2.1 Metamodels as a central artifact of the research approach

In IS research we use *models* as design artifacts [18] to abstract from reality and real world objects, the so called universe of discourse (UoD). If the objects of research are models, and not the real world, we create models of models. Usually a "model of a model" is called metamodel. Going from the instance level (real world, UoD), consisting of instances (M0) to the model level (M1) and further to the metamodel level (M2) signifies the application of abstraction mechanisms. The way of abstraction is guided by a metaization principle (see [15] for a broader discussion).

In order to build a metamodel that is on the same semantic level as ontologies we use the ontological metaization. To model some portion of the world (which might be a model), one needs a language as well as a method with procedures, which supports the identification and representation of relevant objects. The language is considered as the "*way of modeling*", the procedures as the "*way of working*" [34]. In IS research, the emphasis is usually on the way of modeling. Here, we use UML class diagrams. Hence, we focus on the static aspects of the framework. In 2.2 we will focus on the *way of working* in order to better support the construction process of metamodels, by making use of ideas from grounded theory and QDA.

In our research program we are using semi-formal models in order to provide theoretical foundation in different domains (for example IT governance in general and IS security in particular). As metamodels represent the underlying, often implicit structure of the models/standards, they can be used in various ways. On the one hand, they are a methodological support for the construction of company specific extensions/adaptations of known standards/models. If extensions are oriented by both, the company specific needs and the metamodel, it will more likely be consistent with the used model/standard. Further aspects, which take into account the use and application of different models and standards in an enterprise, are the relationships between them. A security model of an enterprise should be linked to and integrated into models used for related tasks and initiatives (e.g. IT governance models like COBIT, ITIL ([15])). This linking can be supported by metamodels because they are useful means to integrate different models. On the other hand, the representation of the standards structure on meta-level supports its deeper evaluation, e.g. for comparing it to other models (e.g. a security ontology). In this respect the motivation is analytic in nature.

Of course, a finished metamodel can be used in either way. In the following, we are going to use the metamodel of ISO/IEC 27001 for analytical purpose, e.g. to evaluate for comprehensiveness or completeness.

2.2 Way of working

In order to support the construction process of metamodels, we refer to ideas and methods used in grounded theory and QDA. Due to page restrictions, we are not able to give a broad introduction (please refer to [7, 8]).

The basic idea in grounded theory (as with most QDA methods) is to work with empirical data like transcripts from interviews, protocols and documents a researcher is confronted with in the field. The focus is on inductively developing a theory, which is 'grounded' in the respective empirical data. One central activity is the "coding", which means conceptualizing qualitative data and assigning categories as well as relations between them. The events and instances a researcher is facing in the data are analyzed as potential "indicators of phenomena … which are thereby given conceptual labels" [8, p. 7]. This conceptualization is very similar to the metaization we referred to above. Our approach is discovering the structure in ISO 27001 by identifying relevant categories/concepts as well as their relations.

Furthermore the abstraction mechanisms used to build concepts and categories are, to the best of our knowledge, not subject of discussions in the relevant methodological literature on QDA and grounded theory. Most approaches only stress its inductive nature. In our metamodelling approach applied in the following section we use inductive categorization in order to derive relevant ontological metamodel components for M2 from the ISO/IEC standard, which is located on model level (M1). We furthermore use QDA software (ATLAS.ti) for coding.

3 Related Work

3.1 Information Security Standards

One of the major challenges in managing information security are incomplete information about the risks the information systems are facing as well as available controls to address them [32]. As such, planning models, checklists and guidelines have been and still are popular. As each organization identifies the threats to their information systems and determines suitable countermeasures, a set of best-practice procedures and techniques emerges. In an attempt to standardize efforts in information security, best-practice frameworks and standards have been developed (e.g. ISO 17799, 2700x, NIST). Due to their origin, these vary in scope and purpose. Furthermore, they vary in depth as well as in the level of detail and granularity. We therefore focus our analysis to the meta level M2.

In our selection of a suitable information security standard we have defined two requirements: 1) the chosen standard must aim to be comprehensive and have a wide

scope on information security and 2) the chosen standard should have – even if very limited – a representative character for actual security practice. After considering different standards we chose ISO 27001 [19] for the following reasons: The ISO 27002 standard is the actual guideline on best-practice in information security management. However, as with best practice frameworks in the related field of IT governance, individual controls can be ignored in an attempt to customize the guideline to the actual organizational needs – and in fact this is the common case [24]. By choosing the certification standard ISO 27001 instead, we assume that organizations having completed the certification process accordingly have addressed all concepts incorporated in said standard. Therefore, the chosen standard represents actual security practice in organizations certified based on it. In the next section we will discuss information security ontologies, which will serve as a reference to evaluate our derived metamodel regarding completeness.

3.2 Information Security Ontologies

Ontologies are sets of concepts of a given domain. As explicit specifications of a conceptualization [17] they allow the formalization and transfer of knowledge. This can help to communicate, compare and put in relation to each other the knowledge and findings researchers make. Therefore, defining concepts and the relations between them is one of the primary tasks in any scientific community [5].

Many information security researchers have identified ontologies as a means to structure either the entire information security problem domain or specific subdomains and made contributions (e.g. [1, 10, 23]). In their comparison of thirty security ontologies [6] conclude that the scientific community has not yet reached the goal of establishing a general information security ontology. By building upon an information security standard that is specifically used to certify information security management systems (ISMS) we cannot make the claim to deliver such a contribution either. However, the metamodel of ISO 27001 can serve as a foundation and a starting point to build an information security management ontology which may cover the managerial aspects of information security. After examining several ontologies, we decided to use [12, 21, 23, 25, 27, 33] as reference ontologies based on the shared subject and their broad scope for comparison.

One may ask if ontologies and models can be compared the way we propose. Due to different notions of both, it is impossible to clearly separate ‘ontology’ and ‘model’ [3]. E. g. ontologies in literature differ in notation, axiomatic richness and the levels of formality (graphical vs. logic based language; lightweight vs. heavyweight ontologies; machine-readable vs. machine-interpretable); similarly, conceptual modelling languages differ in modelling concepts and their external notation as well as in operators or rules of inference and in their integrity rules. In his ontology spectrum [26] views conceptual models (like the object oriented models of UML) as a kind of ontology, having a medium level of structure and formalization. Partially in contrast, [3] consider every ontology a model. We therefore see our metamodels as comparable to ontologies as long as both are on the same level of abstraction.

4 Metamodeling of the Information Security Standard ISO 27001

Based on our selection of the certification standard ISO 27001 for information security management systems the primary document was defined. We additionally narrowed the QDA approach down to its Annex A, which contains the actual objectives and controls. In order to reduce a potential linguistic bias of the researcher (preferences for certain words), we used in-vivo coding which uses the quoted term itself as code label. By doing this, we have generated 153 codes, which were grounded in 275 quotations. We call this set of codes our base set. Figure 1 shows the steps of our process and the resulting sets of codes.

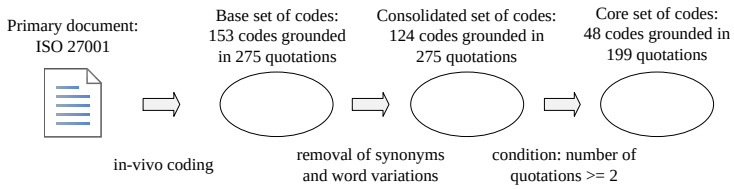

Fig. 1. Inductive Categorization Process.

The codes stem from the ISO standard and therefore reside on the M1 level. In a next step we have merged codes based on synonyms and word variations. This way we reduced the number of codes to 124, our so-called consolidated set of codes. During an examination of the remaining codes we noticed that most codes that were grounded only in a single quotation would be considered attributes under a modeling aspect. For example the codes 'information in transit' and 'stored information' embody two states of 'information'. Using the condition of grounding in at least 2 quotations we finalized 48 codes as the foundation for our metaization effort. Once a first version of our metamodel, containing the core set of codes, is established, the excluded 76 codes with singular grounding are re-evaluated and included as either concepts on their own, subconcepts, attributes or ultimately dismissed.

We derive concepts using inductive ontological metaization. These concepts therefore reside on the level M2. We define core concepts as concepts that are not types or subconcepts of other concepts. Amongst the 48 codes we identified the following concepts to be as such: 'asset', 'threat', 'control', 'requirement' and 'role'. The first three concepts did not come as a surprise. Assets represent a value that is deserving of protection for the organization, while threats are the concept that endangers this value and controls (synonymous to countermeasures) are the means to achieve said protection. All three are often cited in security requirements engineering (e.g. [13, 28]).

The concept 'requirements' is represented by three subconcepts we identified in the standard: 1) security requirements, 2) legal requirements and 3) business requirements. These distinctions indicate potential aspects or layers of information security management, as suggested by many information security researchers (see [9]). Figure 2 shows the metamodel of the ISO 27001 standard based on our findings.

In comparison to the other core concepts 'rule' has relatively weak grounding based on the in-vivo coding. However, with 10 quotations the code 'responsibility' is one of the more predominant ones and represents the relation between 'role' and other concepts, mainly 'asset'. To include this emphasis on an ownership-type paradigm we

decided to include role as a (supporting) core concept. The relationships among concepts have been derived by analyzing quotations.

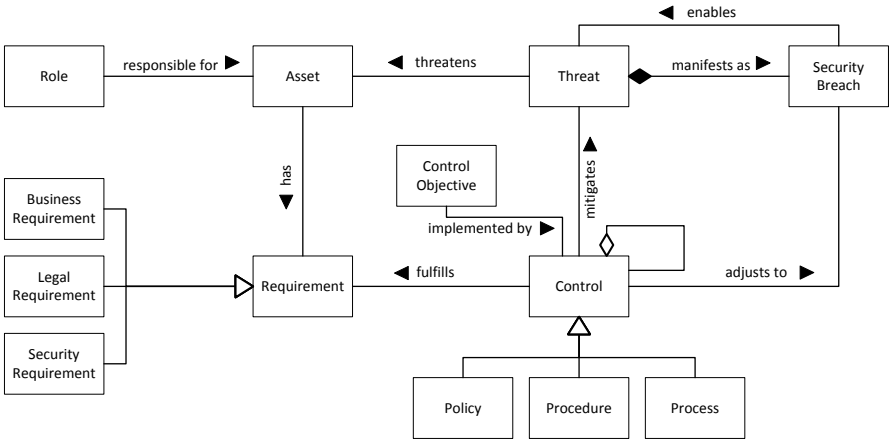

Fig. 2. ISO 27001 Metamodel.

After adding the five mentioned core concepts and branching 'requirement' and 'control' into subconcepts, we re-evaluated prior excluded codes with singular occurrences. By doing so we identified three codes that had a semantic similarity: 'security event', 'security incident' and 'security breach'. While interpretation allows to distinct them by varying levels of severity, we decided to merge them together add them as one core concept ('security breach') as an analysis of quotations for the 'control' and 'threat' concept showed that this element played an important part for the control objectives A.8.2, A.10.10 and A.13.2. Additionally we added 'control objective', as it is an important structural element in the standard which groups controls and elaborates on their common purpose.

It is notable, that in the part of the ISO 27001 standard we used for our analysis, measures are not included systematically, even though in the rest of the standard they are mentioned frequently. Furthermore, there is no strong evidence that roles and responsibilities might be assigned to controls or control objectives. From a governance point of view, it would be of central importance to define accountability and decision rights during the implementation of a security standard.

5 Comparison and Findings

To evaluate ISO 27001 using our metamodel we compare it with selected information security ontologies to find out how our identified concepts relate to different sets (e.g. be a super set, subset or an intersection with other sets of concepts). Table 1 shows the security concepts and their correlation to our core concepts of the metamodel. We are aware that it is not possible to evaluate for completeness, but we consider a set of ontologies to be a good proxy evaluating for comprehensiveness.

A review of the selected ontologies shows that the *way of working* differs from our inductive approach, which may be one reason for differences in concepts found. For

example [12] identify concepts using a deductive categorization. By surveying existing literature they derive a structure which they fill using multiple source documents such as ontologies of security subdomains (e.g. cryptology) and standards.

Lee et al. [23]	Karyda et al. [21]	Tsoumas et al. [33]	Fenz et al. [12]	Mouratidis et al. [25]	Raskin et al. [27]	ISO 27001 Metamodel
Asset	Asset	Asset	Asset	Sec. Entities	Object	Asset
Countermeasure	Countermeasure	Countermeasure/Control	Control			Control
Criticality			Rating			
		Impact				
Goal	Objective					Control Objective
			Organization			
		Risk				
Sec. Requirement			Attribute	Security Constraint	Property	Requirement
Source			Location			
Stakeholder	Person	Stakeholder / Threat Agent	Person			Role
Threat	Threat	Threat	Threat			Threat
		Attack/Unwanted Incident			Event	Security Breach
Vulnerability		Vulnerability	Vulnerability			

Table 1. Comparison of information security concepts.

Comparing these concepts we can find 'asset', 'threat' and 'control' either verbatim in the selected ontologies or in the case of control as a synonym of 'countermeasure'. As we have pointed out before, these concepts are also predominant in security engineering literature and probably can be considered authentic core concepts of the information security discipline. For our 'role' concept we see a semantic equivalent in the two concepts 'organization' and 'person', as well as 'stakeholder' and contextualized in the threat scenario 'threat agent'. Finally, despite its strong grounding in our analysis of the ISO 27001 standard, the 'requirement' concept does not seem to be part of many other ontologies. At best we can find semantic equivalents in the concepts 'security constraints', 'attribute' and 'property'.

One possible reason for this discrepancy might be the difference in the way of working. By building an ontology using a deductive categorization process, the theoretical foundation can pre-determine (bias) elements of the ontology and lead to a different result compared to an inductive process. In their description of the 'attribute' concept [12] describe 'security attributes' as a subconcept, which has e.g. availability or confidentiality as instances – terms that we'd associate with the 'security requirements' subconcept in our metamodel.

Based on the weak grounding of codes like 'internal user' and 'external threat' we did not subsume such codes into a 'source' concept. However, based on its importance in distinguishing threats (by origin) we agree that such an aspect is vital for a comprehensive information security management system. However, it is unclear if 'source' (or 'location') is a concept, a criterion to create subconcepts (e.g. 'internal threat' and 'external threat') or if it is an attribute or property of the 'threat' concept.

For the concepts 'criticality', 'impact', 'organization' and 'risk' we did not find sufficient quotations to derive respective concepts, nor were those concepts found in many of the analyzed ontologies. Contrary the 'vulnerability' concept plays a vital

role in the operationalization of ontologies like [12, 33] and should be considered for adoption in a more general metamodel of the information security domain.

6 Conclusion and Future Research

In this paper we attempted to identify relevant concepts in the information security management standard ISO 27001 in order to achieved insight into its structure. As a methodological foundation we applied QDA to enhance transparency and traceability of the metamodeling procedure and, furthermore, showed that metamodels can assist in the analysis and comparison with multiple ontologies.

In their comparison of security ontologies [6] focused on ontological metrics and evaluated essentially the structure of the proposed ontologies, not their content. We contributed by comparing a selection of ontologies and the constructed metamodel based on the concepts therein. Hereby, core concepts in the sense of an intersection of said ontologies could be derived and compared with our findings.

In an extension of the presented research we also see the need to examine the depth (search for instances on meta level M0) and comparison with additional ontologies, which is where e. g. the 'vulnerability' concept may play a crucial role.

We assume that an extended ontology can contribute significantly to the building of a theory core for IS security research. There is a dominance of subjective-argumentative research in information security research, which – according to [30] – indicates that the discipline is still on its way to establish a theory core. We believe that by establishing an ontology not only ambiguity in terminology can be reduced or eliminated, but that ontologies can also serve as a framework for a theory core in the discipline. This consideration is mainly based on the view of theory as "a lens for viewing or explaining the world" [16]. In this respect, the goal of theory is to provide a description of the phenomena of interest, analysis of relationships among concepts, and the definition of constraints. Based on correspondence as well as consensus theory of truth, it could be possible to derive one integrated and reconciled ontology/model which could serve as a theory core for IS security research.

References

1. Amaral, F. d. N., Bazilio, C., Silva, G. M. H. d., Rademaker, A. and Haeusler, E. H. (2006) An Ontology-based Approach to the Formalization of Information Security Policies, *Proc. of the 10th IEEE on International Enterprise Distributed Object Computing Conference Workshops EDOCW '06*, IEEE Computer Society.
2. Arief, B., Besnard, D. (2003) Technical and human issues in computer-based systems security. *Report No. CS-TR 790*, University of Newcastle, UK.
3. Atkinson, C., Gutheil, M. and Kiko, K. (2006) On the relationship of Ontologies and Models, *Second Workshop on Meta-Modelling (WoMM 2006)*, October 2006.

4. Baker, W. H. and Wallace, L. (2007) Is Information Security Under Control?: Investigating Quality in Information Security Management, *IEEE Security and Privacy*, 5, 1, 36-44.
5. Bishop, M. (2003) What Is Computer Security?, *IEEE Sec. & Privacy*, 1, 67-69.
6. Blanco, C., Lasheras, J., Valencia-Garcia, R., Fernandez-Medina, E., Toval, A. and Piattini, M. (2008) A Systematic Review and Comparison of Security Ontologies, *Proc. of the Third International Conference on Availability, Reliability and Security*, 813-819.
7. Bryant, A., Charmaz, K. (Eds) (2007) The SAGE Handbook of Grounded Theory, Sage, London.
8. Corbin, J. M. and Strauss, A. (1990) Grounded theory research: Procedures, canons, and evaluative criteria, *Qualitative Sociology*, 13, 1, 3-21.
9. Dhillon, G. and Backhouse, J. (2001) Current directions in IS security research: towards socio-organizational perspectives, *In. Systems Journal*, 11 127-153.
10. Donner, M. (2003) Toward a Security Ontology, *IEEE Sec. & Privacy*, 1, 3, 6-7.
11. Eloff, J. H. P., Eloff, M. (2003) Information security management: a new paradigm, in: Proc. of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology, 130 – 136.
12. Fenz, S., Ekelhart, A. (2009) Formalizing information security knowledge, Proc. of the 4th International Symposium on Information, Computer, and Communications Security, 183-194.
13. Flechais, I., Mascolo, C. and Sasse, M. A. (2007) Integrating security and usability into the requirements and design process, *Int. Journal of Electronic Security and Digital Forensics*, 1, 1, 12-16.
14. Fomin, V., Vries, H.J. de and Barlette, Y. (2008) ISO/IEC 27001: Exploring the reasons for low adoption, *Proc. EUROMOT 2008*, Nice / Sophia Antipolis.
15. Goeken, M., Alter, S. (2009) Towards Conceptual Metamodelling of IT Governance Frameworks. Approach - Use – Benefits. *Proc. of the 42nd Annual Hawaii Int. Conference on System Sciences*, Hawaii.
16. Gregor, S. (2006) The nature of theory in information systems, *MISQ* 3, 491-506.
17. Grubner, T. R. (1995) Towards principles for the design of ontologies used for knowledge sharing, *Int. Journal of Human-Computer Studies*, 43, 5, 907-928.
18. Hevner, A. R., March, S. T., Park, J., Ram, S. (2004) Design Science in Information Systems Research, *MISQ*, 28, 2, 75-105.
19. International Organization for Standardization and International Electrotechnical Commission (2005) ISO/IEC 27001:2005, information technology - security techniques - information security management systems- requirements.
20. Kankanhalli, A., Teo, H., Tan, B. and Wei, K. (2003) An integrative study of information systems security effectiveness, *Int. Journal of Information Management*, 23, 2, 139-154.

21. Karyda, M., Balopoulos, T., Dritsas, S., Gymnopoulos, L., Kokolakis, S., Lambrinoudakis, C., Gritzalis, S. (2006) An ontology for security e-government applications, *Proc. of the First Int. Conference on Availability, Reliability and Security 2006*, 1033-1037.
22. Kim, A., Luo, J. and Kang, M. (2005) Security Ontology for Annotating Resources, *Proc. of the 4th Int. Conference on Ontologies, Databases, and Applications*, Agia Napa, Cyprus.
23. Lee, S.-W., Gandhi, R., Muthurajan, D., Yavagal, D. and Ahn, G.-J. (2006) Building problem domain ontology from security requirements in regulatory documents, *Proc. of the 2006 international workshop on Software engineering for secure systems*, ACM, Shanghai.
24. Looso, S. and Goeken, M. (2010) Application of Best-Practice Reference Models of IT Governance, *Proc. of European Conference on Inf. Systems (ECIS) 2010,*.
25. Mouratidis, H., Giorgini, P., Manson, G. (2003) An Ontology for Modelling Security: The Tropos Approach, In: Palade, V., Howlett, R. J., Jain, V. (eds) *Knowledge-Based Intelligent Information and Engineering Systems*, Lecture Notes in Artificial Intelligence, Springer-Verlag, 1387-1394.
26. Obrst, L. (2003) Ontologies for Semantically Interoperable Systems. Proceedings of the Twelfth International Conference on Information and Knowledge Management, 366-369.
27. Raskin, V., Hempelmann, C. F., Triezenberg, K. E., Nirenburg, S. (2001) Ontology in information security: a useful theoretical foundation and methodological tool, *Proc. of the 2001 workshop on New security paradigms*.
28. Sindre, G., Opdahl, A. L. (2005) Eliciting security requirements with misuse cases, *Requirements Engineering*, 10, 1, 34-44.
29. Siponen, M. and Willison, R. (2009) Information security management standards: Problems and solutions, *Information & Management*, 46, 267-270.
30. Siponen, M., Willison, R. and Baskerville, R. (2008) Power and Practice in Information Systems Security Research, *Proc. of the Int. Conference on Information Systems (ICIS) 2008*.
31. Solms, S.H., Solms, R. (2009) Information Security Governance, New York.
32. Straub, D. W. and Welke, R. J. (1998) Coping with Systems Risk: Security Planning Models for Management Decision Making, *MIS Quarterly*, 22, 441-469.
33. Tsoumas, B., Gritzalis, D. (2006) Towards an Ontology-based Security Management, *Proc. of the 20th Int. Conference on Advanced Information Networking and Applications*, 1, 985-992.
34. Verhoef, T.F., Hofstede, A.H.M.T., and Wijers, G.M. (1991) Structuring Modelling Knowledge for CASE Shells, in Andersen, R. et al. (Eds.): *Proc. of the third international Conference CAiSE'91 on Advanced Information Systems Engineering*, 502-524.