Integration of IT-Security Aspects into Information Demand Analysis and Patterns

Kurt Sandkuhl[1], Raimundas Matulevičius[2], Marite Kirikova[3] and Naved Ahmed[2]

[1] University of Rostock, Institute of Computer Science
Chair Business Information Systems, Albert-Einstein-Str. 22, 18059 Rostock, Germany
Kurt.Sandkuhl@uni-rostock.de
[2] Institute of Computer Science, University of Tartu, Estonia
{rma, naved}@ut.ee
[3] Riga Technical University, Riga, Latvia
marite.kirikova@cs.rtu.lv

Abstract. Information logistics in general addresses demand-oriented information supply in organizations. IT-security has not received much attention in information logistics research. However, integration of security aspects into information logistics methods could be useful for application contexts with strong security requirements. As a contribution to this aspect, the paper investigates the possibility to extend information demand patterns (IDP) and information demand analysis (IDA) with security elements. The contributions of this paper are (1) to motivate the integration of security aspects into IDP based on the analysis of three IDPs, (2) the integration of security requirements elicitation from business processes (SREBP) and information demand analysis, and (3) and enhanced representation of IDP including security aspects.

Keywords: information logistics, security requirements elicitation, information demand pattern, information demand analysis

1 Introduction

In the field of information logistics, much research work during the last two decades has been spent on understanding the nature and practices of information demand [1, 5], developing methods and technologies for improving demand-oriented information supply in organizations [2, 4] and implementing evaluating solutions for various application scenarios (see, e.g. [3]). However, IT-security has not received much attention during this period, since IT-security and demand-oriented information supply were viewed as complementary issues: engineering adequate security in organizations has to encompass much more than just the information demand and supply in an organization, i.e., it would be far from sufficient to base IT-security measures only on the needs derived from information flow. Nevertheless, information logistics cannot be considered as completely detached from IT-security concerns as the information still has to be protected against unauthorized access, loss or other security threats. We argue that integration of security aspects into information logistics methods could be useful for application contexts with strong security

requirements. As a contribution to this aspect, the paper investigates the possibility to extend information demand patterns (IDP) and information demand analysis (IDA) with security elements. IDP capture organizational knowledge about the information demand of a role; information demand analysis describes a method how to identify this information demand.

The research question discussed in this paper is "What changes in information demand analysis and information demand patterns need to be incorporated if security requirements are taken into account?" The research approach taken is explorative: using existing IDP and real-world requirements from projects underlying the IDP development, we investigate the need for integrating security requirements. We propose a way to do the integration, apply it in one case and argue that this should be suitable for similar cases. The contributions of this paper are (1) to motivate the integration of security aspects into IDP based on the analysis of three IDPs, (2) the integration of security requirements elicitation from business processes (SREBP) and information demand analysis, and (3) enhanced representation of IDP including security aspects.

The remaining part of the paper is structured as follows: the background for our work from information logistics is described in section 2. Section 3 motivates the need for integrating security aspects by analysing existing demand patterns. Section 4 proposes changes in IDP and IDA based on an integration of an existing method for security requirements elicitation. Section 5 shows an application of this extension and discusses experiences. Conclusions and future work are discussed in Section 6.

2 Background

This section will briefly describe the background for our work from information demand analysis (Section 2.1) and information demand patterns (Section 2.2).

2.1 Information Demand Analysis

Much work in information logistics has been spent on defining and understanding the characteristics of information demand. We will use the results of Lundqvist who defined information demand as follows: "*Information Demand is the constantly changing need for relevant, current, accurate, reliable, and integrated information to support (business) activities, whenever and where ever it is needed.*" [7, p.59]. Furthermore, Lundqvist's work confirmed the conjecture that information demand of a person is based on the roles and tasks this person has: "*Information demand depends on the role and tasks an entity has within a larger organization. If the role and/or the tasks change, so too will the demand".* This role-centric perspective with task and responsibilities as primary characteristics was the starting point for developing a method for information demand analysis. This method consists of several interconnected phases that can be applied in a sequential and iterative manner. The information demand analysis (IDA) method was developed to support this task based

on a well-defined method notion [8]. According to the IDA-method, the process of analysing information demand starts with scoping the area of analysis, includes modelling, analysis and evaluation of information demand context, and concludes in the application of the results in suitable information systems implementation and/or business process reengineering activities. The phases in the IDA process have a clearly defined list of prerequisites and expected outcomes as described in the method handbook [6]. The different phases have the following main characteristics:

- *Scoping*: Scoping includes definition of the area of analysis and has the purpose of selecting the part of an organization to analyse with respect to the information demand as well as identifying the individuals providing the necessary background information during the continued process of analysing.
- *Information Demand Context Modelling:* The main purpose of this phase is to identify the basic information demands based on the core concept of information demand context, i.e., which role needs to do what tasks and what does this require in terms of resources.
- *ID-Context Analysis and Evaluation:* Once the context related information is gathered this has to be analysed and represented in a format useful for continued work. During this phase a choice has to be made whether or not analysis should be continued and if so what refinements to focus on.
- *Representation and Documentation:* As the different analysis phases produce models and documents expressed in different notations the purpose of this phase is to collect and combine the results into a unified coherent representation that can be used to communicate the information demands as well as utilize them in activities aimed at improving information flow.

2.2 Information Demand Patterns

The basic idea of information demand patterns (IDP) is similar to most pattern developments in computer science: to capture knowledge about proven solutions in order to facilitate reuse of this knowledge. In this paper, the term information demand pattern is defined as follows: *An information demand pattern addresses a recurring information flow problem that arises for specific roles and work situations in an enterprise, and presents a conceptual solution to it* [9]. An information demand pattern consists of different parts (see Section 5 for an example):

- The *pattern name* usually is the name of the role the pattern addresses.
- The *organisational context* explains where the pattern is useful. This context description identifies the application domain or the specific departments or functions in an organisation forming the context for pattern definition.
- The *problems* of a role are identified. The tasks and responsibilities a certain role has are described in order to identify and discuss the challenges and problems, which this role usually faces in the defined organisational context.
- The *conceptual solution* describes how to solve the addressed problem. This includes the i*nformation demand* of the role, which is related to the tasks and responsibilities, a *timeline* indicating the points in time when the information

should be available, and *quality criteria* for the different elements of the information demand. These criteria include the general importance of the information, the importance of receiving the information completely and with high accuracy, and the importance of timely or real-time information supply.

- The *effects* of using the proposed solution are described. If the needed information should arrive too late or is not available at all, this might affect the possibility of the role to complete its task and responsibilities. Information demand patterns include several kinds of effects: potential economic consequences; time/efficiency effects; effects on increasing or reducing the quality of the work results; effects on the motivation of the role responsible; learning and experience effects; effects from a customer perspective.

The above parts of a pattern are described in the *textual description*. Additionally, a pattern can also be represented as a *visual model*, e.g., a kind of enterprise model.

3 Analysis of Selected Information Demand Patterns

Based on three information demand patterns developed during the last years, this section will motivate why it makes sense to integrate security aspects into the process of IDA and the concept of IDP. The three patterns originate from different industrial areas: quote preparation responsible (project management), change administrator (manufacturing) and material responsible (automotive supplier). For each of the three patterns, we will investigate how relevant confidentiality, integrity and availability of the information is. Confidentiality refers to protection against unauthorized disclosure of information; integrity basically means that information cannot be modified in an unauthorized or undetected manner; availability means the information must be available when needed and computing systems or communication channels should be protected accordingly [12].

The "**Quote Responsible**" pattern is presented in detail in [10], which describes "context" and "problem" of the pattern as follows: "*The context for this pattern is manufacturing industries, in particular for built-to-order products. When preparing a quote based on a customer request, usually a team of different competences and disciplines is involved. This team commonly has to produce a quote in a relatively short time frame, i.e. many experiences, best practices and sometimes even "qualified guesses" have to be coordinated in a process with high time pressure. One role in this team is the responsible person for the overall quote. This role requires experience and accurate information about the technical and quality specification for a product, the envisioned logistics and the price levels, which usually originate from different information sources and actors. The pattern describes the information demand typically experienced by the quote responsible for coordinating preparation of a quote. The pattern is supposed to be useful for manufacturing enterprises producing built-to-order products with high demands and short preparation times of quotes developed in teams of engineers. […] The pattern addresses the general problem of submitting quotes of unnecessary low quality, which basically either is reducing the probability of getting the order or creating economic risks for the company. […]*"

The above description shows that the content of a quote is highly confidential during its development. Competitors could have a significant competitive advantage if the information contained in the proposal is disclosed. Furthermore, integrity is important in order to avoid unauthorized modification of essential data in the quote, like, e.g., the overall price for the services in the quote.

The complete description of the "**Change administrator**" pattern is available in [11] and describes "context" and "problem" as follows: *"The context for this pattern is configuration and change management in manufacturing industries, in particular, industry sectors with complex physical products. Changes in products, product parts or installed systems are usually initiated by change reports or enhancements requests. Systematic handling of such requests requires coordination of decision making and implementation, often in a team with members from many different engineering disciplines. The role responsible for coordinating change request for a specific product, product part or system is often called change administrator. […]. The pattern describes the information demand typically experienced by the role "change administrator". The pattern is supposed to be useful for enterprises developing and producing physical products with different variants and various released configurations.. […] The pattern addresses the general problem of delayed decisions, redundant activities and inconsistent data in engineering change management and the resulting product or quality problems […].*

Incidents and problems detected in products might indicate safety issues and vulnerabilities. Disclosure of information could lead to damages of the image of the enterprise even if the safety issue has to be considered as minor. This shows that confidentiality of the information is an issue. Furthermore, availability of information also is crucial as not only the change administrator but also operations in the enterprise might need the information for supporting time-critical problem solving.

The "**Material Responsible**" pattern is presented in detail in [9], which describes "context" and "problem" of the pattern as follows: "*The context for this pattern is manufacturing industries, in particular, automotive industries and automotive suppliers. When developing new products or variants of the existing product families, usually a team of many different engineering disciplines is involved. One role in this team is the material responsible who is supposed to make sure that the applied materials meet the quality requirements of both, the customer of the supplier and the supplier as such. This role requires experience and accurate information about the material characteristics, test results, customer requirements, supplier information etc., which usually originate from different information sources and actors. The pattern describes the information demand typically experienced by the role responsible for contributing to product design processes. The pattern is supposed to be useful for manufacturing enterprises producing products with high demands to material characteristics developed in distributed teams of engineers. […]The pattern addresses the general problem of unnecessary shortcomings, product design or production problems caused by the materials used […].*

The materials used in the product and the production and recycling concepts are part of the enterprise knowledge to be protected. Competitors could gain insight to product variants and specific features of the product line, i.e., the information

included in the material specification should be protected against unauthorized access. Furthermore, the information needs protection against unauthorized modification, as changing material specifications might hamper manufacturability of product features.

The analysis of the above three information demand patterns showed that all three patterns actually showed some information security related issues which motivates to investigate what changes in IDA and IDP are implied by this fact.

4 Integrating Security Aspects into IDA and IDP

The analysis of existing information demand patterns in section 3 showed that there is reason to integrate security aspects into method and technology in information logistics. This section will elaborate on how this integration can be done. For the information demand analysis process we argue that using experiences from existing approach in security engineering is recommendable. Thus, we will first present SREBP (Section 4.1), one of the existing approaches in security requirements elicitation, and afterwards propose its integration with IDA (Section 4.2). Section 4.3 will add an extension of the IDP structure to this discussion.

4.1 SREBP Approach

The core components of the security requirements elicitation from business processes (SREBP) method [13] are the *security risk-oriented patterns* [15]. These patterns describe the recurring security problems within the specific security context and propose the solution in terms of the security requirements. Five security risk-oriented patterns for five contextual areas are proposed [15] and summarised in Table 1. The conceptual base of the pattern application is developed from using the domain model [14] for information system security risk management (ISSRM). This domain model differentiates between three major concept groups – asset-related concepts, risk-related concepts and risk treatment-related concepts.

Assets-related concepts describe assets and their security criteria. Here, an *asset* is anything that is valuable and plays a vital role to accomplish organisation's objectives. A *business asset* describes the information, processes, capabilities and skills essential to the business and its core mission. An *IS asset* is the IS component, valuable to the organisation since it supports business assets. A *security criterion* is the property or constraint on business assets describing their security needs, which are, typically, expressed through confidentiality, integrity and availability.

Discussion: in the previously presented ID demand patterns, *content of the quote* (see "Quote Responsibility" pattern) is the business asset is terms of security. Its security criterion is *confidentiality* and *integrity* as defined in the pattern discussion. Similarly, used information (see "Change Administrator" pattern) and the materials and recycling process (see "Material Responsible" pattern) are the business assets. *Confidentiality* and *availability* of the information ("Change Administrator" pattern), and *confidentiality* and *integrity* of the materials and recycling process (see "Material Responsible" patterns) are security criteria in the given context. Hence the *IS systems*

assets in this organisational context could be identified as the technology and software used to input, output, transfer, store and manipulate the identified business assets.

Table 1: Security Risk-oriented Patterns

Contextual area	**Security Risk-oriented Pattern**	**Description**
Access control	Securing data from unauthorized access	This pattern describes how to secure confidential data from unauthorized access by people or devices. The pattern is based on implementation of access control where (stakeholder or device) roles and data are classified to levels of trust and sensitivity.
Communication channel	Securing data that flow between the business entities.	This pattern addresses the electronic transmission of data between two entities, i.e., client (where data is submitted) and business (where data is used).
Input interface	Securing business activity after data is submitted.	This pattern secures the business activity, which is carried out after data has been submitted, and where integrity and availability have to be ensured.
Network infrastructure	Securing business services against DoS attacks.	This pattern addresses the Denial of Service (DoS) attacks and their protection strategies. It helps to protect the business assets in order to guarantee its availability.
Data store	Securing data stored in/retrieved from the data store.	The main goal of this pattern is to prevent the leaking of confidential data from the enterprise's data store.

Risk-related concepts introduce a risk definition. A risk is composed of a *threat* with one or more *vulnerabilities* that leads to a *negative impact* on the assets by harming them. An *impact* is the consequences of an event that negates the security criterion defined for business assets in order to harm assets. Hence the impact harms the business asset and the IS asset which support this business asset. A *vulnerability* is the characteristics of IS assets that expose weakness or flaw. A threat is an incident initiated by a *threat agent* using *attack method* to target one or more IS assets by exploiting their vulnerabilities.

Discussion: We note that the IDP concept *effect* has the direct relationship to the security *impact*. Hence, for example, the *negation of confidentiality or integrity of the content of quote* (see "Quote Responsibility" pattern) will harm the *content of the quote* and IS asset(s) used in the organisations context to support the content of the quote. Here we could also speak bout the malicious role or actor who acts within the context of the information demand; such malicious actor or role could be treated as the threat agent in terms of security. In this light, depending on the IDP organisation context, one could apply the security risk-oriented patterns to identify the targeted security risks in the information demand process.

Risk treatment-related concepts describe the concepts to treat risk. A *risk treatment* is a decision (e.g., avoidance, reduction, retention, or transfer) to treat the identified risk. A *security requirement* is the refinement of a risk treatment decision to mitigate the risks. A *control* designates a means to improve the security by implementing the security requirements.

Discussion: Security requirements mitigate the identified risks. From the perspective of the IDPs, much depends on the organisational context, since this context includes the means and techniques where the implemented security requirements (i.e., controls) should be incorporated.

4.2 Integration of SREBP and IDA

Both IDA and SREBP are approaches that apply patterns. All patterns of IDA have the same representational structure. The number of patterns can be equal to the number of roles in the enterprise. Each SREBP pattern has its specific representational structure which is expressed in terms of a fragment of a business process model. Currently the number of SREBP patterns is limited to 5 patterns briefly described in Table 1.

The integration of both approaches is quite straight-forward because they have several things in common, namely, both approaches consider roles, activities, and information, which is needed for the role to fulfil its responsibilities (particular information demand in IDA corresponds to particular data input in SREBP). IDA approach indirectly addresses also the information produced by the role performing the activity. Consideration of such information would extend integration possibilities of both approaches, however this aspect of integration is beyond the scope of this paper. Thus further in this sub-section the discussion is limited only to those SREBP patterns which directly represent and analyze data inputs of activities.

There are three ways how to practically integrate the approaches:

- Start with IDP of the roles; for each activity and corresponding information demand then analyze all processes where the activities and their inputs corresponding to the information demand might be involved. This approach prescribes that business processes, in the form where the SREBP patterns can be discovered, are modelled after the application of IDP.
- Start with SREBP approach and analyze security aspects for information demand of each role represented in the business process if its IDP is available. Here the IDP can be applied only to those roles, which are represented in the business process model and included in SREBP patterns focused on data inputs of activities.
- Apply IDP and discover SREBP patterns in business processes in parallel; then try to establish mappings between the patterns of both approaches in terms of activities and information demands and data inputs.

In the first two cases integration of approaches is easier, as one approach is applied on the basis of another one. However this can introduce a kind of stereotypical thinking in the analysis of information demands and security threats and thus leave some issues un-attended. The third approach is stereotype free. However it has to overcome challenges that are caused by different levels of detail and abstraction in which the patterns of IDA and SREBP might be presented. Furthermore, in the first case, SREBP can be considered as additional method component in the IDA framework which is applied after business process modelling.

4.3 Extension of the IDP Structure

In order to accommodate the security-related information in the IDP structure introduced in section 2.2, there are two possibilities: extending existing elements or adding new elements. In the following, both options will be discussed separately.

A) Extension of existing elements in the IDP structure: As security aspects do not change the context of the IDP or the problem addressed, these two elements of the IDP structure are no candidates for extensions. The same is true for the actual information demand contained in the pattern and for the timeline. However, for the tasks and responsibilities of a role, it might be useful to add what parts of the tasks or responsibilities are related to confidential information or integrity and availability demands. The quality criteria for each information demand would be a candidate for extension. Here we could add confidentiality, integrity and availability as additional quality criteria. However, this would require another classification as the one used for the quality criteria regarding completeness, accuracy and timeliness of information. The same applies for the effects of not receiving the demanded information: we could consider security effects as additional aspect, but for security the classification of low / moderate / high would not be suitable.

B) Add new elements in the IDP structure: The above discussion regarding the extension of existing elements shows that there is no obvious way how to do this. Hence, we propose to add two new elements expressing the security aspects:

- Security demands: for the information demands in an IDP, the demands regarding confidentiality, integrity and availability have to stated separately for each information demand. As an IDP does not aim at providing actual solutions how to implement information supply, even the security demands should only indicate whether security-related issues regarding each information demand exist or not.
- Security-related effects: for each information demand it should be made clear what effects non-implementation of the security requirements could have. The effects should be distinguished into economic effects, violation of laws and regulations, effects on customers, regulations and image or publicity effects.

Both additional elements are optional for an IDP. An example is shown in Sec. 5.

5 Example of a Security-enhanced IDP

In order to illustrate the extension of the IDP structure proposed in Section 4.3, the information demand pattern "Quote Responsible" was selected. The pattern follows the structure introduced in Section 2.2 and was presented in detail in [10]; "context" and part of "problem" are included in section 3 of this paper when discussing the need for security extensions of the IDP structure. For brevity reasons, this section will only include the actual "information demand" part of the IDP, and the "security demand" and "security-related effects" extensions.

The **information demand** of a quote responsible is based on tasks and responsibilities of this role within the organisation. This part of the ISP is shown in Table 2.

The **security demand** includes confidentiality, integrity and availability demand as introduced in Section 3 and uses two levels, which have to be defined for each information demand:

- Protect: the information set available for meeting this information demand has to be protected with appropriate measures

- Open: the information set available for meeting this information demand does not need any specific protection

Within an IDP the security demands are visualized in a table, which includes the information demand (left column), and the confidentiality, integrity and availability demand. Table 3 shows the security demand summary for the example pattern:

Table 2: Information Demand part of IDP "Quote Responsible" (from [10])

The **tasks and responsibilities** of the role responsible for a quote include • The preparation of a competitive, complete and high quality content of the quote (technical specification, quality characteristics, physical & administrative logistics) • The preparation of an accurate, complete and consistent economic part of the quote • Team management, i.e. coordination of all contributions from participating team • On-time submission of the quote with all needed attachments, information and signatures
The **information demand** of the role responsible for a proposal consists of: • Call for tender / terms and conditions from the customer side • Technical specification of the requested product from customer side • Available capacity, production resources and competences at the own enterprise • market information • own records about customer relation (previous orders, complaints, financial issues) • applicable standards and norms in the domain • […]

Table 3: Security Demand part of IDP "Quote Responsible"

Information Demand	Confidentiality	Integrity	Availability
Call for tender / terms and conditions	Open	Open	Open
Technical specification	Protect	Protect	Open
Own capacity, resources, competences	Protect	Protect	Open
Market information	Protect	Protect	Open
Own customer records	Protect	Protect	Open
Domain standards	Open	Open	Open

Table 4: Textual Description (excerpt) of Security-related Effects for IDP "Quote Responsible"

Economic effect: • Disclosure of information about the capacity might give competitors an advantage in the actual quote as they will understand the limitations of the company's ability **Customer effects:** • If the customers get to know that information about them has been disclosed to third parties, this might corrupt customer loyalty **Regulation and law effects:** • For this example, no effects are expected **Image and publicity effects**: • Publication of customer records or information derived from these costumer records will cause damage to the image of the company

Security-related effects: the effects of not implementing the security demands shown in table 2 are described in writing and visualized in a table. We will only include an excerpt of this text (Table 4) and table (Table 5) due to space limitations:

The tabular description uses three levels for classifying the effects:

- Not applicable (n/a): this level is used in case the information does not need any protection (see table 2) or if no effects are expected
- Task level: the impact of not protecting the information against security threats is limited to the actual task at hand. For the example of "Quote Responsible" this means that the impact is limited to the actual quote.
- Enterprise level: not protecting the information against security threats has an impact on the overall enterprise. For the example of "quote responsible" this means that the impact is not limited to the quote under preparation but will affect the whole enterprise.

Table 5: Tabular description (excerpt) of security-related effects for IDP "Quote Responsible"

	Economic effect	***Customer effects***	***Regulation & law effect***	***Publicity / image effects***
Call for tender, terms condition	*n/a*	*n/a*	*n/a*	*n/a*
Technical specification	*Enterprise level*	*n/a*	*n/a*	*n/a*
Own capacity, resources, competences	*Task level*	*Task level]*	*n/a*	*n/a*
Market information	*Task level*	*n/a*	*n/a*	*Enterprise level*
[…]				

6 Summary and Future Work

Based on three existing IDP, this work motivated the integration of security-related aspects into information demand analysis and patterns. With an integration of SREBP as a method component into the IDA pattern, the paper demonstrated how a light-weight security requirements elicitation approach can be a complementary method component for IDA. The structure of IDP was extended by the two elements of security demand and security-related effects in order to accommodate security-related issues in IDP. The biggest limitation of the work so far is that it is purely conceptual, i.e. the proposed changes in IDP and IDA only have been designed on paper but not be applied in practice.

The main subject of future work will have to be (a) to apply the extended version of the IDP structure in real-world projects for validation purposes and in order to gain experiences regarding its utility and practical use and (b) to provide guidelines for how security demands can be implemented in practice and anticipated effects can be minimized or avoided. In particular for the second work, continuation of the cooperation with security experts that led to this paper is essential.

Acknowledgements

The paper presents the results of an international project involving Estonian, German and Latvian teams. This research project of the Baltic-German University Liaison Office is supported by the German Academic Exchange Service (DAAD) with funds from the Foreign Office of the Federal Republic Germany.

References

1. Dinter B., Winter R.:. *Information Logistics Strategy-Analysis of Current Practices and Proposal of a Framework*. in *Proceedings of the 42nd Hawaii International Conference on System Sciences*. Los Alamitos: IEEE Computer Society, (2009)
2. Lin F., Sandkuhl K.: *A New Expanding Tree Ontology Matching Method*. in *On the move to meaningful internet systems. OTM 2007 Workshops*. Berlin: Springer (2007)
3. Meister S., Stahlmann V.: *Telemedial ILOG Listeners. Information Logistics Processing of Telemedical Values Using CEP and HL7*. in *Ambient Assisted Living*. 2012. Berlin Heidelberg: Springer (2007)
4. Billig A., Blomqvist E. and Lin. F.: *Semantic Matching based on Enterprise Ontologies*. In *Proceedings of the 6th International Conference on Ontologies, DataBases, and Applications of Semantics*.. Berlin Heidelberg: Springer, (2007)
5. Lundqvist M.; Holmquist, E.; Sandkuhl, K.; Seigerroth, U., & Strandesjö, J. Information Demand Context Modelling for Improved Information Flow: Experiences and Practices. In IFIP Working Conference PoEM, The Practices of Enterprise Modelling, 2 (pp. 8 - 22). LNBIP 39, Springer Verlag, (2009)
6. Lundqvist M.: Handbook for Information Demand Analysis. Version 1.0, Deliverable 4 of the infoFLOW project, April 2010, Jönköping University, School of Engineering, (2010)
7. Lundqvist M.: *Information Demand and Use: Improving Information Flow within Small-scale Business Contexts*. Licentiate Thesis, Dept of Computer and Information Science, Linköping University, Linköping, Sweden, ISSN 0280-7971, (2007)
8. Lundqvist M., Sandkuhl K., Seigerroth U.: Modelling Information Demand in an Enterprise Context: Method, Notation and Lessons Learned. International Journal Systems Modeling and Design, Vol. 3 (1), IGI Publishing. (2011).
9. Sandkuhl K.: Information Demand Patterns. Proc. PATTERNS 2011, The Third International Conferences on Pervasive Patterns and Applications, pp. 1-6. September 25-30, 2011; Rome, Italy. ISBN: 978-1-61208-158-8 (2011)
10. Sandkuhl K.: Improving Quote Preparation in Project Management with Information Demand Patterns. Perspectives in Business Informatics Research - 11th International Conference, BIR 2012, Nizhny Novgorod, Russia, September 24-26, 2012. Proceedings. LNBIP 128, pp. 41-53. Springer, ISBN 978-3-642-33280-7 (2012)
11. Sandkuhl K.: Improving Engineering Change Management with Information Demand Patterns. Product Lifecycle Management: Virtual Product Lifecycles for Green Products and Services. Proc. PLM11, Eindhoven, The Netherlands, pp. 47 - 58. Inderscience Enterprises Ltd. 2013. ISBN 978 90 79182 26 8. (2013)
12. ISO/IEC 27000:2009 (E). (2009). Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC.
13. Ahmed N.: Deriving Security Requirements from Business Process Models, PhD thesis, University of Tartu, 2015
14. Dubois E., Heymans P., Mayer N., Matulevičius R.: A Systematic Approach to Define the Domain of Information System Security Risk Management. In: Intentional Perspectives on Information Systems Eng., pp. 289–306. Springer (2010)
15. Ahmed N., Matulevičius R.: Securing Business Processes Using Security Risk-oriented Patterns. Computer Standards and Interfaces 36(4), 723–733 (2014)