International Journal of Business and Technology

Volume 1
Issue 2 *Spring 2013*

Article 7

May 2013

# Policy and Security Configuration Management Systems in Cross-Organisational Settings

Sascha Pudenz
*University of Innsbruck*

Markus Manhart
*University of Innsbruck*, markus.manhart@uibk.ac.at

Daniel Bachlechner
*University of Innsbruck*

Stefan Thalmann
*University of Innsbruck*

## Recommended Citation

Pudenz, Sascha; Manhart, Markus; Bachlechner, Daniel; and Thalmann, Stefan (2013) "Policy and Security Configuration Management Systems in Cross-Organisational Settings," *International Journal of Business and Technology*: Vol. 1 : Iss. 2 , Article 7.
DOI: 10.33107/ijbte.2013.1.2.07
Available at: https://knowledgecenter.ubt-uni.net/ijbte/vol1/iss2/7

# Policy and Security Configuration Management Systems in Cross-Organisational Settings:

Sascha Pudenz, Markus Manhart, Daniel Bachlechner,Stefan Thalmann

[1]University of Innsbruck, Department of Information Systems, Production and Logistics Management,
Universitätsstr. 15,6020 Innsbruck, Austria
markus.manhart@uibk.ac.at

**Abstract.** A context of use analysis is an important step in every software engineering project. Comprising the identification of the key system users as well as an analysis of the system environment and the activities supported, this engineering step is crucial for the successful development of information systems. Clarity with respect to the users' demand for system support and their participation in the activities supported by the system is considered particularly important for systems which are critical for organizational continuity and which are used across organizational boundaries. Systems supporting policy and security configuration management in networks of IT service providers, their customers and auditors meet both of these criteria. Within the scope of this article, the context of use of such a system supporting policy and security configuration management is investigated by means of a user-oriented approach. The focus lies on a specific setting being investigated within the scope of an on-going research project. The investigation which was based on a series of qualitative interviews as well as desk research resulted in a comprehensive description of the participation of a set of key system users in activities related to policy and security configuration management as well as their demand for system support. Also the key users and the activities to be supported are discussed within the scope of this article.

## 1. Introduction

The outsourcing of organizational information technology (IT) is driven by the composition of distributed IT services that operate across organizational boundaries. Customers, providers and their suppliers of IT services as well as auditors as the main groups involved in IT outsourcing are, however, increasingly confronted with challenges resulting from the complex and dynamic composition of IT services. For instance, the reconciliation of high-level security and compliance requirements on the one side and low-level configuration settings on the other side often makes a trade-off between profitability, and security and compliance necessary. Tasks such as informing service providers about one's own security and compliance requirements, translating these requirements into concrete configurations and checking if these configurations actually match the security and compliance requirements are not only considered laborious and error-prone but also not adequately supported by tools (Thalmann et al. 2011). Providing adequate system support for policy and security configuration management meeting the demands of the main user groups is thus expected to be beneficial for customers and providers of IT services as well as for auditors involved in IT service provision networks.

The provision of such a system for policy and security configuration management is the main goal of an on-going research project the authors of this article are involved in. The research presented in this article is partially based on preliminary results of this project. Because of the lack of user-focused research on the support of policy and security configuration management through information systems (IS), it is important to apply a profound software engineering procedure. From an IS theory perspective, such systems should not only fulfil functional requirements but also fit the context of use

(Markus et al. 2004). This dual focus is expected to positively affect the adoption of the developed IS by its users. Thus, the success of the policy and security configuration management system depends highly on the quality of both the elicitation of the functional requirements and the context of use analysis. Within the scope of this article, we will concentrate on the context of use analysis, which comprises the identification of the key users of the system, the description of the environment of the system and the investigation of the activities supported by the system.

A user-oriented approach is considered particularly relevant for IT outsourcing settings such as the one we focus on. In view of complex and dynamic networks of IT service suppliers, their customers which may be service

Published by UBT Knowledge Center, 2013

providers themselves, and auditors checking the security and compliance of organizations providing services to others, it is not surprising that organizations regularly face a lack of control (Sherer 2004). Organizations consuming services from IT service providers usually cannot be fully confident, for example, that their suppliers continuously meet all security and compliance requirements as was agreed contractually. At the same time, Internet-facing interfaces that are indispensable if IT services are composed dynamically across organizational boundaries are, despite state-of-the-art security measures, always also serious weak points (Jansen et al. 2011).

The goal of this article is to describe the procedure and results of a context of use analysis concentrating on a policy and security configuration management systems in cross-organizational settings. Therefore, we (1) identify the main activities to be supported by such a policy and security configuration management system, (2) analyze the participation of key system users in these activities and (3) explore the actual user demand for such a system.

The remainder of this paper will be structured as follows: Section 2 provides further information about the investigated cross-organizational settings, introduces user-oriented software engineering and highlights the cornerstones of context of use analyses. The procedure chosen for the presented context of use analysis concentrating on a policy and security configuration management system is described in section 3. In section 4, the results are presented. Apart from introducing the main activities to be supported by the system, for each user group the participation in the activities as well as their actual demands are described. The results of the context of use analysis are discussed in section 5. Finally, section 6 summarizes the key findings and provides an outlook on future work.

## 2. Foundations

The outsourcing of IT has its origins in the 1960s but became a more and more important alternative to in-house IT over the decades (Lee et al. 2003). With the advent of concepts such as SaaS, IaaS and PaaS, companies have numerous potential possibilities to outsource IT services (Vouk 2008).

The distribution of data across organizational boundaries coming with the outsourcing of IT services leads to risks to security and compliance (Thalmann et al. 2012). People are traditionally considered the weakest link in organizations with respect to information security and unfavourably designed IS, particularly if they are directly related to security management, thus make organizations even more vulnerable (Edwards et al. 2008). The policy and security configuration management system is intended to be used in a cross-organisational setting as illustrated in Fig 1...

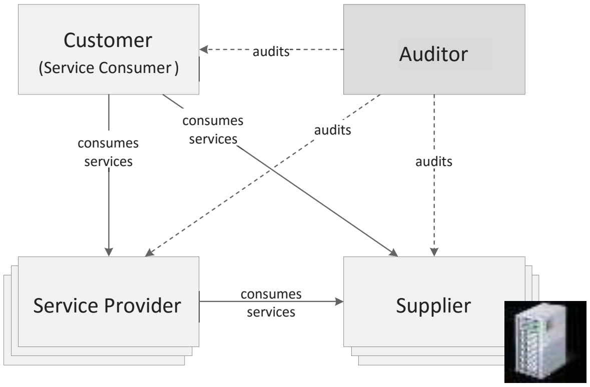

**Fig. 1.** Cross-organizational security setting (Thalmann et al. 2011)

Fig 1. illustrates the relationships between organizations involved in cross-organizational security settings (Thalmann et al. 2012). Suppliers offer specific IT services executed on an infrastructure operated and maintained at their own sites. Service providers might operate their own IT infrastructures but can also consume services from different service suppliers and orchestrate them according to their customers' requirements.

High-level security and compliance requirements, IT policies and low-level configuration settings are characterized by various different standards, best practices and frameworks such as ISO 27001, ITIL or COBIT. Some governance, risk and compliance (GRC) tools support the handling of highlevel requirements. Different low-level configuration settings are, if at all supported by IS, maintained in separated configuration management systems or configuration management databases. Furthermore, a seamless exchange of security and compliance requirements between business partners is usually not supported by existing IS (Thalmann et al. 2012). Thus, the

DOI: 10.33107/ijbte.2013.1.2.07

development of an integrated policy and configuration management system for cross-organizational settings can be considered innovative. Is goes considerably beyond the improvement of existing solutions. Supporting complex and dynamic networks of IT service providers, their customers and auditors though an IS requires a well-considered software engineering procedure matching the specific characteristics of the system itself and its context of use. One of the key success factors of IS is the involvement of system users during the software engineering processes (Ferré 2003; Markus et al. 2004; Nielsen 1993). Thus, a human-centered, i.e. user-oriented, design approach is considered appropriate.

As described in ISO 13407 (ISO-13407 1999), a human-centered design cycle comprises several steps of engineering, which are given by:

1) Planning: Plan the human-centred process
2) Context of use: Understand and specify the context of use
3) Requirements: Specify the user- and organizational requirements
4) Design: Produce design solutions
5) Evaluation: Evaluate designs against requirements

As the research presented in this article focuses on the second step, the context of use, it is necessary to identify the key system users, to specify in which environment the system will be used and to investigate the activities for which the systems is used (ISO-13407 1999). The identification of the key system users has already been presented in related work (Thalmann et al. 2011). Within the scope of this article, we focus on the identification of activities to be addressed by the policy and security configuration management system and on the investigation of how the identified key users are involved in those activities. Additionally, we investigate the user demand for such a system. Assessing and understanding user attitude towards a system is considered an important factor for successful system implementation (Hecht et al. 2011). Although user-oriented system development is addressed in several IS theories (Davis 1989; DeLone et al. 1992; Markus et al. 2004; Spears et al. 2010), we found no work that focuses on the context of use analysis for systems to support policy and security configuration management.

The importance of a profound context of use analysis is underlined in the IS user-participation theory. Markus and Mao (Markus et al. 2004) state that a system is inconclusively successful if it fits its functional specifications (what the system should do). An important side-factor, however, which highly influences the successful adoption of the system, is the system's fit with respect to issues such as task routines, usability criteria or the social environment. Therefore, a system that also fits its context of use is more likely to be adopted by its users than a system that only addresses the functional requirements (Markus et al. 2004).

## 3 Procedure

The online version of the volume will be available in LNCS Online. Members of institutes subscribing to the Lecture Notes in Computer Science series have access to all the pdfs of all the online publications. Non-subscribers can only read as far as the abstracts. If they try to go beyond this point, they are automatically asked, whether they would like to order the pdf, and are given instructions as to how to do so.

In the following, the procedure applied for the context of use analysis is presented in detail. After an initial phase of desk research, we conducted a series of semi-structured interviews. This approach seemed appropriate taking the innovativeness of the system and the cross-organizational distribution of potential system users into account [2, 16]. Within the scope of the interviewing phase, we first conducted face-to-face interviews with key informants which took approximately 120 minutes each. Building on the gathered results, informant interviews were conducted by telephone that took approximately 60 minutes each. Overall, fourteen informant interviews were recorded and transcribed. In case of two informant interviews, the interviewers took notes and produced a written summary right after conducting the interviews.

The primary goals of the series of interviews were (1) the identification of the specific policy and security configuration management activities to be supported by the system, (2) the investigation of the main users' participation in these activities, and (3) the elicitation of their actual demand for system support. We followed an explorative approach and intended to portray insights by means of original voice rather than to be representative. The overall procedure comprised the following phases:

1) *State-of-the-art description*: One expert of both an auditor and a service provider were asked to describe their typical work processes related to policy and security configuration management in written form. These descriptions served as input for the subsequent desk research and interviews.

2) *Desk study on system users*: Literature on users of cross-organizational IS was analysed with the study goals in mind. The result was a list of about 80 potential users relevant for the investigated cross-organisational security setting.
3) *Key informant interviews*: Two key informants, one working for a service provider and one working for an auditor, were interviewed. The provided descriptions of work processes were discussed and the state-of-the-art descriptions were refined. The result was a list of the main activities of security and policy configuration management. Also the users identified in the desk study were discussed with the key informants to identify the users that participate in the main activities and to clarify their participation. Furthermore, for each user at least one interview partner for more detailed interviews was identified. The key informants were asked to select individuals having sufficient experience with respect to the topic in order to provide valuable insights only.
4) *Informant interviews*: In the first quarter of 2011, 14 semi-structured informant interviews were conducted with individuals from eight organizations. The interviewees were from Australia, Austria, France, Germany, Switzerland and the US. At least one individual was interviewed per identified key user. All interviewees had a profound security management background. They had between three and 15 years of experience in the field (about five years on average). At the time of the interviews, nearly all interviewees were employed in a leading position of IT security management or related departments. Within the scope of the informant interviews the main activities, the users' participation in these activities, and their demand for system support were addressed once again but in more detail and with a clear focus on the respective interviewees user group.
5) *Evaluation of data*: In the last step of our procedure, we analysed the data gathered through the interviews. The interview transcripts were investigated by applying a qualitative data analysis method (Miles et al. 1994; Patton 2002). Within the scope of this step, we refined the set of policy and security configuration management activities to be supported by the system. Apart from that, the users' participation in the activities and their demand for system support was analysed.

During the interviews, we asked directly for the participation in the activities to be supported.

Responses such as *"I assess how well designed security controls are and if they are implemented"* or *"this is not related to my field"* allowed drawing conclusions with respect to the type of participation in the activities for each user group. In order to assess the actual demand for system support, we also asked directly. Examples for relevant statements of the informants are *"the visualization of the security design is very interesting and would be used, especially in the sales process"* and *"to define an audit scope, a supporting tool would be interesting"*. The level of detail provided with respect to the demand for system support differed considerably from one interview to another. Nevertheless, we gathered all information that was provided by the interviewees. Some interviewees also stated that there is no demand for system support regarding specific activities. Due to the exploratory character of the study and the small sample size, we had to live with missing information with respect to some user groups.

**Table 5.** Policy and security configuration management activities

| Abbrev. | Activity description |
|---|---|
| A | *Achieving and maintaining a control design satisfying the control objectives:*<br>The activity focuses on the continuous optimization of the set of controls taking the requirements as well the current landscape into account. It ranges from the identification of conflicting control objectives and the creation of the control design to the anticipation of the impact of modifications. |
| B | *Monitoring of mismatches between the control objectives and the actual implementation of controls:*<br>The activity focuses on the detection of security misconfigurations by comparing the actual configuration of the landscape and the configuration specified by the set of security and compliance requirements. |
| C | *Verifying if a potential service provider satisfies the required control objectives:*<br>The activity focuses on the verification if specified control objectives can be fulfilled by a potential service provider. It is performed before a contract is concluded and takes requirements as well as the landscape into account. |

D *Providing audit evidence to be evaluated by the auditor of customers:*

The activity focuses on the provision of audit evidence. Such audit evidence is usually requested by auditors on behalf of customer to be able to audit its client's service landscape including outsourced parts.

E *Defining an audit scope:*

This activity focuses on the selection of business units, activities and services to be audited and the identification of the respective control objectives.

F *Verifying if the control design and implementation meets the control objectives:*

This activity focuses on the verification if controls meet control objectives and if they are implemented effectively. It includes the check of equivalent controls.

In the following, we describe the system users' participation in these activities as well as their demand for system support in detail**.** summarizes the findings. The columns represent the activities to be supported and the rows the key system users. Empty cells indicate that there was no information available.

## A. Security Manager

**User participation.** In order to achieve a control design satisfying the control objectives (activity A), the security manager evaluates whether a provider is able to fulfil certain requirements. One security manager stated "I am responsible to check whether the hosting partner is able to be compliant to the security requirements". The security manager is, for instance, involved in questions regarding authentication mechanisms or how access rights management should look like. With respect to the verification if a potential service provider satisfies the required control objectives (C), the security manager contacts the security manager of the service provider "to gather more detailed information concerning the implementation of security policies". This communication takes place when detailed information beyond SAS70 reports is needed (SSAE16 will displace SAS70 in the future, however, at the time we conducted the interviews, the interviewees mentioned SAS70 as auditing standard).

**Demand for system support.** Mainly, system support is demanded by the security manager in the form of a central database to collect the customers' requirements to "have a quick opportunity to check the requirements of a considered service customer". This would facilitate the verification of potential service providers (C). However, generally, the interest in system support is rather low, since the security manager is not heavily involved in these activities. Every kind of visualization of the control design is considered very useful. Generally, the security manager is interested in transparency of processes and activities.

## B. Compliance Manager

**User participation.** The compliance manager is directly involved in the development of the control design (A). One compliance manager stated that "process owners usually propose security controls which they discuss with me". Additionally, the compliance manager performs reviews at the service provider's site together with auditors. In the course of service provider audits, the compliance manager demands the results of the audits to monitor mismatches between control objectives and the implementation of controls (B). A compliance manager mentioned, "I generally try to establish and maintain audit readiness throughout the organization." The compliance manager is also involved in verifying if a potential service provider satisfies specific control objectives (C). On the one hand, by checking the service provider's compliance to standards and the presence of certifications, and on the other hand by testing how the reporting to 3rd-party providers is practiced. Providing audit evidence (D) lies also in the responsibility of the compliance manager, who acts here as a coordinator. One compliance manager mentioned, "Generally, I coordinate people that should hand log-files to me and communicate the results to auditors." With respect to the definition of the scope of provider audits (E), the compliance manager usually plans the audit together with an auditor who actually performs the audit and is heavily involved into the definition of what business processes are audited or which tests are conducted.

**Demand for system support.** The compliance manager has a high interest in the support of the control design (A) and the monitoring of mismatches (B). Bad performance or a delegation of responsibilities could easily lead to a lack in trust and the loss of certifications. With respect to the monitoring of mismatches (B), the compliance manager wants to establish that processes and services are continuously auditable. Ideally, the monitoring should be fully automated. Furthermore, the risk assessment should be facilitated as well as the assignment of control incidents to responsible persons. In case of cloud computing, the compliance manager states that it is difficult to provide audit evidence (D) due to the high amount of user accounts and customer systems. One compliance manager stated that “such an all-rounder tool would be very interesting although it might be hard to implement”.

### C. Operations Manager

**User participation**. The operations manager is directly involved in the achievement and maintenance of the control design (A). During contract negotiations, the operations manager discusses with executives of the customer if his or her organization is generally able to meet the customers’ requirements. It is more important for the operations manager to know whether the requirements can be fulfilled or not rather than to know any other contractual details. According to that, an operations manager stated: “I confer with my team to discuss whether we can be compliant to the customers’ security requirements.” The identification and monitoring of mismatches (B) is “only relevant for if it appears as a finding in an audit report”. Thus, the operations manager is a consumer of the outcome of this activity. Furthermore, an operations manager stated: “of course, I am involved in strategic negotiations with potential providers”, consuming the information gained from the verification of a potential service provider (C), and using the information for contract negotiations, renegotiations, but also for yearly provider audits.

**Demand for system support.** With respect to the achievement and maintenance of the control design (A), the operations manager is rather interested in yes/no decisions – if the company is able to be compliant with a potential customer’s requirements or not – than in detailed information. The operations manager demands system support regarding the automation of procedures described in SAS70 reports or ISO 27001. The main goal is to be able to conduct ad-hoc compliance checks. The operations manager is interested in the support of compliance checks of potential providers (C), however, would primarily be a consumer of compliance reports. A concrete example for system support would be a database where internal security requirements could be matched to potential providers in order to identify those with the highest degree of compliance. With respect to the provision of audit evidence (D), the operations manager requests for system support to increase efficiency. One mentioned critical factor of such a system is the security of the system itself, i.e. “that no data is lost via security-bridges.”

### D. Supplier Relationship Manager

**User participation.** The supplier relationship manager checks against ISO standards if a potential service provider (C) is able to be compliant to the control objectives defined by his organization. Upon this check, the supplier relationship manager predicts the suitability of a service provider from a security perspective. One supplier relationship manager stated: “In case of a large contract, I get an external auditor on board to get a neutral assessment of the supplier.” After contracting, the supplier relationship manager monitors the provider´s compliance. The supplier relationship manager has a controlling function with respect to the definition of an audit scope (E), checking if the scope that has been defined is actually audited by the auditor and poses questions in case of ambiguity.

**Demand for system support.** With respect to the verification of a potential service provider (C), the supplier relationship manager needs information if the provider is able to be compliant. However, the supplier relationship manager states that this activity is supported well enough through control mechanisms, i.e. norms and standards which would leave no leeway for a potential system. Scepticism was expressed by the supplier relationship manager that the system might take up his or her job taking a supportive role. With respect to the definition of an audit scope (E), the supplier relationship manager demands transparency how the audits are conducted and a clear definition of the audit scope. In general, the statement of one supplier relationship manager saying that “the [security and policy configuration management] topic is too specific to make use of a superficial tool” indicates that there is a demand for a specified comprehensive system, although its implementation is seen as challenging.

### E. Control Manager

**User participation.** With respect to the achievement and maintenance of the control design (A), the control manager is involved, assessing if the controls are well designed and if they are implemented. The monitoring of mismatches (B) is only possible on the data level. The control manager uses reports to check reliability of data. In the definition of an audit scope (E) the control manager is directly involved, selecting critical business activities, defining entities, risks, controls that should be covered by an internal audit. Further, the control manager is involved in the verification if the control design meets the control objectives and the verification if it is implemented effectively (F) in the scope of internal revisions and internal control system.

**Demand for system support.** The control manager states that the achievement and maintenance of the control design (A) is relevant but highlights that only to be a user of the outcome. The verification of the control design (F) is considered as an interesting aspect where system support could make sense, although it is stated that

DOI: 10.33107/ijbte.2013.1.2.07

"project-specific characteristics might complicate the verification and only approximately about 30 per cent of all control designs could be verified with the support of a system", which is, nevertheless, still seen as useful. Thereby, platform independent support or a partly automated report generation would make sense for the control manager. With respect to this certain activity (F), the support of the activity would ease work; although only a small part of the transactions might be automatable.

### F. IT Professional

**User participation.** The IT professional monitors mismatches between control objectives (B) and the actual implementation of the respective controls. To achieve this, one IT professional stated, "we make use of secondary controls that are used to check whether to implemented key controls work correctly." The criteria for the tests are provided by the company based on legal obligations and recommendations from audits. In providing audit evidence (D) the IT professional has to "provide the necessary data to auditors."

**Demand for system support.** With respect to the achievement and maintenance of the control design (A), a system support that gives an overview over possible control design problems is considered as interesting and it is stated that "this kind of tool that provides the overview over potential bottlenecks is hard to find on the market". Additionally, the IT professional considers the visualization of the control design as crucial.

### G. IT Auditor

**User participation.** Generally, the IT auditor is "involved in helping organizations to create and maintain the control design as risks are moving permanently and a major challenge is to follow and anticipate them". In other words, IT auditors encourage their clients to build a control framework (A) which is flexible enough to be adapted to changing risks. Further, the IT auditor is involved in the monitoring of mismatches (B). More detailed, one IT auditor stated that a responsibility is to "assesses the maturity of internal controls before the actual audit or certification is conducted". This task is a kind of testing or preparation before the audit. The IT auditor is also involved in identifying exceptions to the control objectives and the communication what has to be improved to gain a certification at a later point in time. The IT auditor is involved in providing audit evidence (D) through "guiding the client before an audit in order to receive the right sample". In case that a client has outsourced parts of its IT, the provider provides audit samples. The IT auditor is responsible for the definition of audit scopes (E). In general, an IT manager and a financial manager from the client side as well as the service customer, who wants to have a service provider being audited, are involved in this activity. Verifying if a control design is implemented effectively and if it meets a set of control objectives (F) is "the main responsibility of an IT auditor".

**Demand for system support.** The achievement and maintenance of the control design (A) is important for the IT auditor as well as the visualization of the control design. The interviewee stated that small company-internally developed applications are "more used like guidelines, not really like automated tools" since it is "quite difficult to adapt these tools to specific client context". Thus, one can see that, currently, there is no system that currently addresses adequately the described activities.

Table 6. **Participation and demand for system support of system users**

| Participation .<br>System Demand | | **A**-control design | **B**-Monitor mismatches | **C**-Verify control objectives | **D**-Provide audit evidence | **E**-Define audit scope | **F**-Verify control implementation |
|---|---|---|---|---|---|---|---|
| Service Provider | Security Manager | Evaluates supplier compliance | | Contacts suppliers' security manager | | | |
| | | | ICT support Transparency | Central security database | | | ICT support Automation |
| | Compliance Manager | Involved in development of control design | Consumes reports & establishes audit readiness | Checks service provider's compliance, certificates & reporting | Responsible for providing reports & coordinating parties | Coordination with IT auditor | |
| | | Delegation of responsibilities | Full automation | | ICT support | | |
| | Operations Manager | Direct involvement in control design | Intervenes if thresholds are passed | Participates in strategic negotiations | | | Assists auditors |
| | | Support control design Automation | Report of results Automation | ICT support for compliance checks | ICT support | | |
| | Supplier Relationship Manager | | | Predicts suitability of providers | | Definition of focus areas | |
| | | | | ICT Support Neutral Assessment | | Transparent scope definition | |
| | Control Manager | Assess controls | Checks data reliability | | | | Responsible for internal revisions |
| | | | | | | | |
| | IT Professional | | Responsible for this activity | | Provides accessible data | Responsible in case of internal audits | |
| | | Visualization | | | | | |
| Auditor | IT Auditor | Guides suppliers and customers | | Guiding during sampling | | Coordination with compliance manager | Responsible & accountable for the activity |
| | | Visualization | | | | | |

## 4 Discussion

Six main activities could be identified within the context of use analysis of an IS supporting policy and security configuration management in cross-organizational settings. Four different organizational perspectives are relevant when discussing the activities: (1) the perspective of a service provider delivering IT services and providing them to their customers, (2) the perspective of a service suppliers hosting IT services for the service provider (note that the service supplier is also a service provider), (3) the service customer consuming IT services from the service provider and (4) the auditor checking the service provider's compliance with security and compliance requirements which partially result from a contract with the service customer. The identified activities and their relationships are illustrated in an aggregated form in Fig.2.

DOI: 10.33107/ijbte.2013.1.2.07

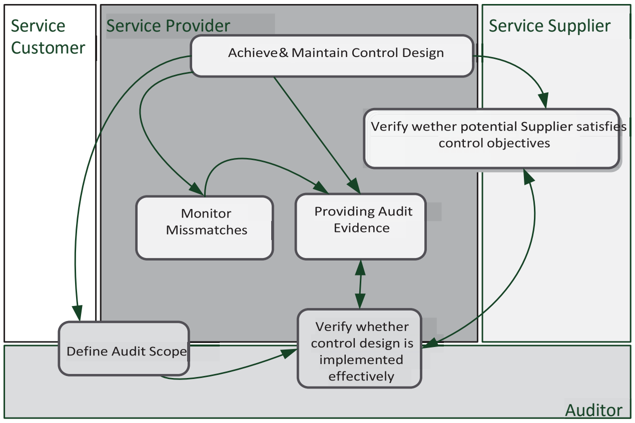
Service Customer
Service Provider
Service Supplier
Achieve& Maintain Control Design
Verify wether potential Supplier satisfies control objectives
Monitor Missmatches
Providing Audit Evidence
Verify whether control design is implemented effectively
Define Audit Scope
Auditor

**Fig. 2** Aggregated view on activities

The basis is the formalization of the control framework during the achievement and maintenance of the control design. This serves as input for the monitoring of mismatches, the verification of suppliers, the provision of audit evidence and the definition of the audit scope. The definition of the audit scope can be initiated by customers and is performed by auditors taking the service providers landscape, the defined control framework as well as defined security requirements into account. Building on the audit scope, IT auditors request evidence from the service provider as well as from the service supplier in case of outsourced services. The provision of audit evidence requires input from the monitoring of mismatches.

The aggregated view on the activities and the involved organizations shows that the intended policy and security configuration management system has interfaces to all four types of participating organizations. During the performed context of use analysis the main system users, their participation and their demand for system support could be identified. The insight with respect to the demand for system support serves as input for the planning of the requirements engineering being conducted after the context of use analysis. Furthermore, the actual software engineering phase can also benefit from the results of a human-centered context of use analysis. These findings are in line with research by Damodaran (Damodaran 1996) and the user-participation theory by Markus and Mao (Markus et al. 2004) who stated that the quality of surveyed user requirements in large measure determines the quality of an IS.

One main insight of this investigation is that an IS needs to be integrated to address all the interdependencies between the activities which are illustrated in **Error! Reference source not found.**. Thereby, it seems promising to operate the IS at the service providers' sites and to integrate tailored interfaces for customers, auditors and service suppliers. Our investigation shows that all organizations involved would clearly benefit from such an integrated solution.

Another main insight of our investigation is that the formulation of security requirements needs to be standardized (1) to facilitate the exchange between many interacting stakeholders from different organizations and (2) to allow the automation of integrity tests, conflict detections or even an automated translation of policies to configuration settings. In this regard, a model-driven approach as proposed by Breu et al (Breu et al. 2008) seems very promising. Again, all involved stakeholder groups would benefit from such a standardized approach of formulating security requirements, supplier relationship managers and auditors in particular.

The applied procedure was useful for the specification of the context of use of a system that acts in a cross-organizational setting in a very complex domain, which is currently inadequately supported by IS. Due to the applied user-oriented approach, information regarding activities, which should be supported by the system, the participation of key system users in those activities and their demand for such a system could be identified and a differentiated picture of the system's context of use could be drawn. The consideration of different perspectives on the system support should enhance the quality of the system as well as user adoption.

## 5 Conclusion & Outlook

Our investigations gathered information about the context of use of a policy and security configuration management system used in a cross-organizational setting. The applied user-oriented approach comprised the application of semi-structured interviews with key system users to identify the main activities for which the system will be used and to identify the demand for such a system.

The results of our study build a basis for follow-up actions regarding system design and are highly important for a successful system implementation.

Follow-up research could be seen in verifying the gathered information about activities, participations and demands of certain users by generalizing the insights through an additional quantitative study. Considering future system development steps, the outcomes of our study can be used as a direct input for other system design methods. Particularly, usability engineering methods, such as Personas (Cooper 2004; Maguire 2001), can benefit from our results. Hence, a more human-centered design, which is emphasized as an important style of system engineering (Nielsen 1993), would get a higher priority, if demands and participations of important system users are considered and used for further steps of system development. This fact is especially important for the next engineering phases which are, firstly, the requirements engineering phase in which the user- and organizational requirements are specified in more detail and, secondly, the implementation phase and, thirdly, the evaluation phase in which the implemented system is tested against the specified requirements. All phases can benefit from the outcomes of our context of use analysis since the key system users and the activities, which should be supported by the system, have been identified.

The Lecture Notes in Computer Science volumes are sent to ISI for inclusion in their Science Citation Index Expanded.

## References

1. Breu, R., Hafner, M., Innerhofer-Oberperfler, F., and Wozak, F. 2008. "Model-driven security engineering of service oriented systems," *Information Systems and e-Business Technologies*), pp 59-71.
2. Cooper, A. 2004. *The inmates are running the asylum: Why high tech products drive us crazy and how to restore the sanity*, (Pearson Higher Education.
3. Damodaran, L. 1996. "User involvement in the systems design process-a practical guide for users," *Behaviour & Information Technology* (15:6), pp 363-377.
4. Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:3), pp 319-340.
5. DeLone, W. H., and McLean, E. R. 1992. "Information systems success: The quest for the dependent variable," *Information Systems Research* (3:1), pp 60-95.
6. Edwards, W. K., Poole, E. S., and Stoll, J. 2008. "Security automation considered harmful?," in *Proceedings of the 2007 Workshop on New Security Paradigms*, ACM: New Hampshire, pp. 33-42.
7. Ferré, X. 2003. "Integration of Usability Techniques into the Software Development Process," in *Proceedings of the 28th international conference on Software engineering*: Shanghai, China, pp. 28-35.
8. Hecht, M., and Waldhart, G. Year. "Fostering adoption, acceptance, and assimilation in knowledge management system design," ACM2011, p. 7.
9. ISO-13407 1999. "ISO 13407," in *Human-centered design processes for interactive system*.
10. Jansen, W., and Grance, T. 2011. "Guidelines on Security and Privacy in Public Cloud Computing," in *800144*, National Institute of Standards and Technology, pp. 1-60.
11. Lee, J. N., Huynh, M. Q., Kwok, R. C. W., and Pi, S. M. 2003. "IT outsourcing evolution---: past, present, and future," *Communications of the ACM* (46:5), pp 84-89.
12. Maguire, M. 2001. "Methods to support human-centred design," *International journal of human-computer studies* (55:4), pp 587-634.
13. Markus, M. L., and Mao, J. Y. 2004. "Participation in development and implementation-updating an old, tired concept for today's IS contexts," *Journal of the Association for Information Systems* (5:11), p 1.
14. Miles, M. B., and Huberman, A. M. 1994. *Qualitative data analysis: An expanded sourcebook*, (SAGE publications, Inc.
15. Nielsen, J. 1993. *Usability engineering*, (Academic Press: Boston.
16. Patton, M. Q. 2002. *Qualitative Research & Evaluation Methods*, (3th ed.) Sage: Thousand Oaks.
17. Sherer, S. A. 2004. "Managing risk beyond the control of IS managers: the role of business management," in *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, IEEE Computer Society: Hawaii, pp. 1-10.
18. Spears, J. L., and Barki, H. 2010. "User participation in information systems security risk management," *MIS Quarterly* (34:3), p 503.

DOI: 10.33107/ijbte.2013.1.2.07

19. Thalmann, S., Bachlechner, D., Demetz, L., and Maier, R. 2012. "Challenges in Cross-Organizational Security Management," in *Proceedings of the 45th Hawaii International Conference on System Sciences*: Hawaii, pp. 5480-5489.
20. Thalmann, S., Bachlechner, D., Maier, R., Manhart, M., and Demetz, L. Year. "Key Roles in crossorganizational security settings," The 2011 European Security Conference Örebro, 2011.
21. Vouk, M. A. 2008. "Cloud computing: Issues, research and implementations," *Journal of Computing and Information Technology* (16:4), pp 235-246.