Key Roles in Cross-Organisational Security Settings

Stefan Thalmann
University of Innsbruck
stefan.thalmann@uibk.ac.at

Daniel Bachlechner
University of Innsbruck
daniel.bachlechner@uibk.ac.at

Ronald Maier
University of Innsbruck
ronald.maier@uibk.ac.at

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

Lukas Demetz
University of Innsbruck
lukas.demetz@uibk.ac.at

Abstract

Managing cross-organisational security settings becomes increasingly important with the advent of cloud computing. While there has been a lot of literature on how to organise organisation-internal security management and how to efficiently audit it, little research has been done on the key roles involved in cross-organisational settings at the employee level as well as their responsibilities and interactions. Since considering these aspects is critical for successful management and efficient auditing of cross-organisational security settings, the primary goals of this paper are to investigate these aspects based on a qualitative empirical study with representatives of organisations assuming typical roles in cross-organisational security settings. This paper describes such a setting, the key employee roles involved and their interactions in detail, and discusses implications for managing cross-organisational security settings from the perspective of service providers who need to satisfy the potpourri of security and compliance requirements in such settings as well as from the perspective of auditors who need to efficiently attest compliance of the complex network of service-provider-consumer relationships with security requirements.

Keywords: security management, roles and responsibilities, cloud computing

1. Introduction

Consuming services from external service providers or combining these with services provided organisation-internally becomes increasingly appealing for many organisations as this approach not only promises cost savings and higher flexibility but also lets organisations focus on their core businesses (Takabi et al., 2010; Kaufman, 2009; Wei & Blake, 2010). The attractiveness of this approach crucially depends on the service providers' ability to achieve, maintain and provide evidence for compliance with security requirements so that customers can trust that the suppliers meet their security

requirements and provide justification about their IT, e.g., within the scope of audits. This challenge currently dampens the willingness of many organisations to adopt cloud computing as IT procurement model (Chow et al., 2009). Profound understanding of roles and responsibilities involved in security and compliance activities in cross-organisational security settings, i.e., several organisations jointly achieve and maintain compliance to security requirements (Miede et al., 2010) as well as their interactions is required in order to overcome this challenge. While there has been considerable work on roles and responsibilities in organisation-internal security settings (Bulgurcu et al., 2010), its cross-organisational counterpart has been neglected in the literature. Some research has already been undertaken in this field, e.g., planning of auditing a cloud computing project (Chen et al., 2010) or proposing a framework for secure cloud computing by using IT auditing (Chen & Yoon, 2010). Overall, accountable clouds would be beneficial for both service consumers and service providers (Haeberlen, 2010). Due to the involvement of several organisations in achieving and maintaining security requirements, these constellations are called cross-organisational security settings.

This paper presents the results of a qualitative empirical study focussing on the key employee roles involved in cross-organisational security settings consisting of organisations outsourcing parts of their IT to service providers, i.e., customers, different types of service providers, i.e., suppliers, and auditors. The primary goal is to identify the key roles on the employee level involved in such a setting, to describe them and to investigate their interactions. On the basis of our results, implications for managing such cross-organisational security settings will be discussed.

The next section reviews related work on the analysis of roles and responsibilities in security management. Afterwards, we introduce the investigated cross-organisational security setting. The subsequent sections present the study design and its results, respectively. In conclusion, we discuss implications for security management in cross-organisational security settings and provide a brief outlook on future work.

2. Roles and Responsibilities in Security Management

One research stream focuses on instruments to improve information security management in conjunction with roles and responsibilities. High-level analyses considering security culture (Van Niekerk & Von Solms, 2010), security strategy (LeVeque, 2006), security governance (Moulton & Coles, 2003), security programs (Smedinghoff, 2010) or security policy (Karyda et al., 2005; Kadam, 2007; Bulgurcu et al., 2010) can be found. Furthermore, a range of authors investigated how security standards incorporate roles and responsibilities (Myler & Broadbent, 2006; Höhne & Eloff, 2002).

Another stream of research describes specific roles and responsibilities in security management. 49 roles relevant for security management were identified by a range of authors who developed comprehensive sets of roles with corresponding responsibilities (Wood, 2005; Von Solms, 1998; Paliotta, 2001). Other authors concentrated on one or a few roles and associated responsibilities. 15 roles were identified two of which had not already been described in the lists mentioned above (Ezingeard & Bowen-Schrire, 2007; Whitten, 2008; Chun & Mooney, 2009; Abbot, 2007; Wylder, 2004; LeVeque, 2006).

The approach used in this paper can be integrated into the research streams mentioned above. With respect to the first stream, this paper focuses on policy, security and configuration management and therefore provides a broader view than (Karyda et al., 2005; Kadam, 2007; Bulgurcu et al., 2010) who focused on information security policy only. (Smedinghoff, 2010) proposed to monitor the third-party service provider arrangements within his security program. In contrast to the mentioned streams, this paper focuses on a cross-organisational setting. Thus, it was necessary to investigate the roles relevant to the setting presented within this paper. This process is described in the following section. In general, roles and responsibilities within a specific setting as presented in this work have not been profoundly studied in the literature so far.

3. Study Design

The goals of our study were (1) to identify the most relevant employee roles involved in cross-organisational security management, (2) to investigate the responsibilities of and interdependencies among these roles and (3) to elicit role-specific requirements for the support of cross-organisational security management. The study comprised three phases:

1. *Literature review:* Related literature was analysed with the three study goals in mind. The result was a list of the most important roles for cross-organisational security management. When compiling this list, the perspectives of service providers and auditors were considered.
2. *Key informant interviews:* Two key informants were interviewed. One worked for a service provider, the other one for an auditor. The roles identified within the literature review were discussed with the key informants in the context of their work setting. The result was a refined list of roles important for either both or at least one of the organisations. Furthermore, the primary responsibilities of the identified employee roles were discussed with the key informants. Finally, individuals assuming at least one of the roles were identified and appointments for the role-specific informant interviews were arranged.
3. *Informant interviews:* Eleven informant interviews were conducted with interviewees either working for one of the organisations which participated in the key informant interviews or for one of five other organisations. At least one individual per identified role was interviewed. The structure of the informant interviews and the issues addressed were developed based on the results of the key informant interviews.

Thus, in order to analyse the key employee roles involved in the introduced cross-organisational security setting, we relied on a series of semi-structured interviews. Two key informant interviews in two organisations and eleven informant interviews in those two and five additional organisations were conducted in the first quarter of 2011. The interviewees were from Australia (1), Austria (1), France (3), Germany (6), Switzerland (1) and the US (1). Table 1 shows details with respect to the numbers of interviewees per employee role and their professional experience. Table 2 addresses the organisation types of the organisations the interviewees worked for. All organisations are considered as

large based on the definition of the EU commission[1]. One of the three service providers has no own IT infrastructure and is thus a specialised type of service provider, i.e., a service orchestrator (cf. Figure 1). Many service providers source services from other service providers and therefore also act as service consumers. The three organisations of the type customer are sole service consumers in our setting. From a service procurement perspective, they act similarly to service providers sourcing services from other service providers. While the key informant interviews were conducted face-to-face, the informant interviews were conducted by telephone. Before the informant interviews were carried out, the interview guideline was pre-tested and slightly adapted after one pre-test interview.

Employee Role	**Number of Interviewees**		**Minimum Years of Experience**
	Key Informant Interviews	Informant Interviews	
Security Manager	0	1	11
Compliance Manager	0	2	5
Control Manager	0	3	7
Supplier Relationship Manager	0	1	20
Customer Relationship Manager	1	0	10
Operations Manager	0	2	5
IT Professional	0	1	5
IT Auditor	1	1	6

Table 1 Numbers of interviewees and minimum years of experience per employee role.

Organisation Type	**Number of Organisations**		**Number of Interviewees**	
	Key Informant Interviews	Informant Interviews	Key Informant Interviews	Informant Interviews
Supplier	1	3	1	7
Customer	0	3	0	3
Auditor	1	1	1	1

Table 2 Organisation types of the organisations the interviewees worked for.

The informant interviews took approximately one hour each. They were recorded and transcribed. A template characterising interviewees' roles and their responsibilities was used for data analysis. Within a literature review, comprehensive attributes of employee roles and responsibilities were identified and used to inform the data analysis procedure proposed by (Patton, 2002) which are discussed in the following.

Roles and responsibilities are characterised by several attributes. Openness to communicate with other persons is a characteristic (Stahl, 2004). Furthermore, affinity to action is when an action is conducted and afterwards a role has the responsibility to take

[1] http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm

the consequences (Stahl, 2004; Auhagen, 2001). Hence, suitable attributes identified by the authors are mission statement, communication relationships, ownership of decisions and key activities performed.

The *mission statement* describes the specific overall purpose or goal that an employee role should accomplish. Besides this role-specific view, the alignment of an organisation's mission statement with roles and responsibilities may lead to a better understanding of employees to fulfil their roles and responsibilities (van Hoepen & Verster, 2008). Similar to this argumentation, every department or even group or role within a company may define its specific mission statement (Wood, 2005). However, the authors focus on employee role-specific mission statements, since on this level the attribute ensures an exact distinction between the specific roles and responsibilities.
Communication relationships describe structure and interaction of content including relational message properties, e.g., informality or composure, temporal message patterns, e.g., frequency, symmetry or diversity, and relational perceptions, e.g., dependence, commitment or transferability (Barry & Crant, 2000). Employees need up to date information about how to perform their roles (Aggarwal-Gupta & Kumar, 2010). Adequate communication structures are essential to provide specific roles with relevant information (Dainty et al., 2006).

Since responsibility is the "duty to take ownership for the decisions" (Phillips, 2009), the *ownership of decisions* made by employees characterises the responsibility of the specific roles they occupy (Phillips, 2009; Kloppenborg, 2009).

Furthermore, responsibility related to a specific role can be characterised by the *key activities performed*. According to the (ITGovernanceInstitute, 2007) assignment and communication of unambiguous roles and responsibilities are necessary to execute key activities in an effective and efficient manner.

4. Cross-Organisation Security Setting

Traditionally, organisations operate and maintain their IT infrastructure in-house (Hayes, 2008), that is, they have an organisational unit responsible for the organisation's IT. Auditors requested to audit the IT of such organisations find themselves in the comfortable position that all responsible people are members of the organisation and all necessary information can be found at the auditee's site.

In the hope of improving efficiency and reducing costs, companies started to abandon their traditional way of operating IT in-house and gradually turned their IT over to professional IT service providers, i.e., they outsourced their IT (Ang & Straub, 1998; Levina & Ross, 2003; Hu et al., 1997) or, more recently, adopted cloud computing (Vouk, 2008). This can be seen by the steadily increasing number of businesses consuming services out of the cloud (Kaufman, 2010).

Figure 1 visualises the relationships between organisations participating in the cross-organisational security setting investigated in our empirical study. When taking advantage of cloud computing, organisations no longer operate parts of their IT on their own, but they consume services provided by third parties as customers. Such a third party

may be a supplier offering specific services, e.g., data archiving or signing of invoices, executed on an IT infrastructure operated and maintained fully in-house, i.e. at service providers of type IV, or partly in-house, i.e. service providers of type II or III, or a service orchestrator also offering services, but not operating an own IT infrastructure, i.e. service providers of type I. Services of a network of suppliers, possibly also comprising service orchestrators, are combined in order to provide more comprehensive services.

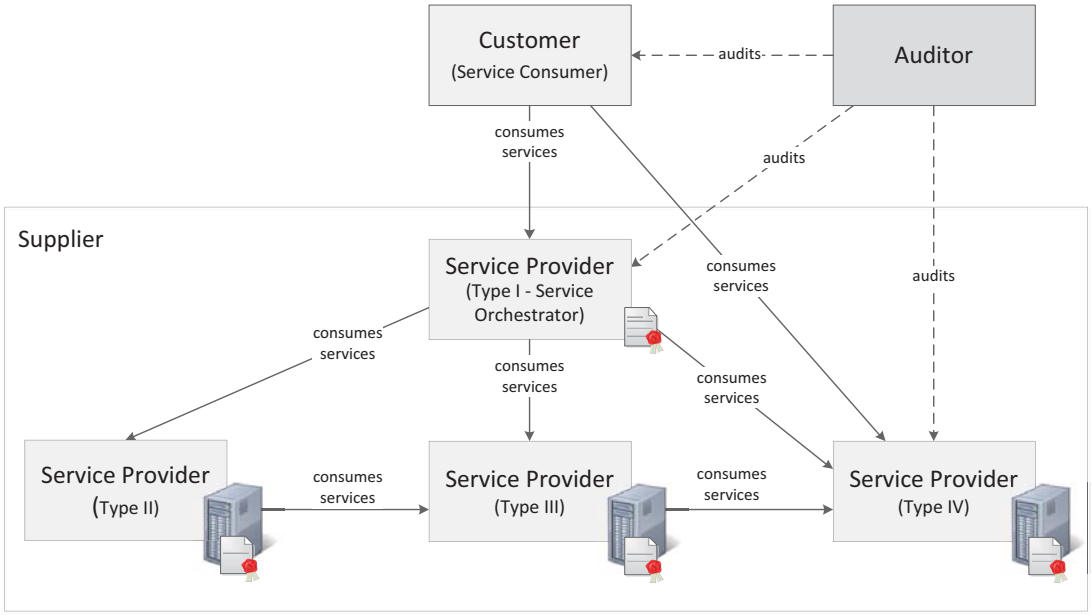

Figure 1 : The investigated cross-organisational security setting

This way of operating IT also changes the way auditors conduct their business. Here, auditors are faced with a different situation as compared to auditing an organisation with in-house IT services since the audited organisation may not be able to provide all necessary information to the auditor. Thus, the auditor needs to request information from third parties, i.e. the network of suppliers, and thus depends on their willingness to provide relevant information. For services provided by a service orchestrator, the situation is even more complicated. Here, information required for an audit cannot be provided by the service orchestrator, but by several subcontracted suppliers whose services are combined and offered to the orchestrator's customer.

Depending on the number of outsourced services consumed by the customer, the audit is prolonged and the costs of an audit may increase. In some cases, it may also be necessary to additionally audit the supplier. This, however, may often not be feasible, e.g., because the auditor has no right to enter the supplier's site. In such cases, the respective supplier could be audited by another auditor of the supplier's choice, or, if available, the supplier could provide existing audit reports to the customer's auditor, indicating the effectiveness and efficiency of its controls and processes and the adherence to specific standards. Consequently, several people are involved in an audit of an organisation outsourcing parts of its IT: (1) employees of the service consumer, i.e., the customer, (2) depending on the number of outsourced services, employees of several service providers which may be of different types, i.e. the suppliers, and (3) employees of the auditor.

Additionally, Figure 1 shows the four approaches with respect to outsourcing strategies of organisations we identified in our study. The different strategies imply different levels of accountability. The first approach is to solely consume services from an audited service provider of type IV which hosts all services in-house. This eases the audit and increases the level of justification of compliance with security requirements for customers. The supplier is assumed to be audited and thus holds an audit report, i.e., an audit certificate (illustrated by a document with a seal in Figure 1). The second approach is to consume services form a service provider of type III which hosts own services and outsources services only to audited suppliers hosting services in-house, i.e. type IV service providers. The third approach is to consume services from a service provider of type II which hosts own services and subcontracts suppliers no matter if they host their services in-house or not. Finally, services from a service orchestrator, a supplier who does not host any IT infrastructure but uses services of other service suppliers, can be consumed. Within the scope of the interviews, we did not identify particularly complex networks of suppliers. However, cross-organisational security settings require a reconsideration of the traditional security roles. Our findings show that the changed model of IT procurement has a strong influence on the roles involved in security and compliance management.

5. Key Roles and Interactions Among Them

In the following, first each of the key roles identified in the interviews is outlined and then the interactions among the key roles are described in the context of all identified key roles. The list of identified roles is based on the literature review and was revised during the two key informant interviews. The first sentence represents the role's mission statement, followed by a description of its key responsibilities and the ownership for decisions. Particular emphasis is put on the primary responsibilities of the roles as learned within the scope of the interviews. In many organisations, several roles are assumed by the same individual. While the roles security manager, compliance manager and control manager are common within our sample of organisations, the roles supplier relationship manager and customer relationship manager are specific to service providers, i.e. types I-III, outsourcing at least parts of their IT. In larger organisations also the operations manager is not uncommon and IT professionals are obviously essential in all organisations operating internal IT, i.e. service providers of types II-IV. All employee roles identified are affiliated to a service provider, except for the IT auditor who is affiliated to an auditor.

The *security manager* maintains an overview of and guides all organisational security activities. He leads the development of the security management strategy and is always involved when the organisational security architecture is to be changed substantially. In such cases, the final responsibility for decisions rests with him. In the context of cross-organisational security management, it becomes particularly important that he coordinates the efforts performed by members of his organisation to satisfy security-related customer requirements. Additionally, he not only defines the general framework for selecting suppliers, he also leads contract negotiations with potential key suppliers.

The *compliance manager* coordinates all efforts made to ensure that compliance requirements are satisfied. The compliance manager is considered particularly important due to his role as an intermediary. He addresses compliance issues in contract negotiations with customers and suppliers. In fulfilment of this task, the compliance manager targets the unrestricted satisfaction of all customer requirements by the network of contracted suppliers. The compliance manager also monitors whether suppliers adhere to contractual agreements. Defining audit scopes is also a responsibility of him. Additionally, he guides the definition of the compliance strategy not only regarding organisational compliance, but also regarding the selection of new and monitoring of contracted suppliers. The final responsibility for selecting new suppliers rests with him.
The *control manager* collects compliance and security requirements from the business perspective and ensures that these requirements are met by the IT landscape by adopting an IT perspective and arranging the implementation of appropriate controls. In this context, he guides the implementation of the controls by IT professionals and ensures that all relevant controls are implemented. Apart from that, the control manager develops the organisational security and compliance framework and coordinates all activities necessary to satisfy security and compliance requirements. Additionally, he is the main contact person for external auditors auditing his organisation's in-house IT. He ensures the audit readiness of the organisation and provides information on processes, identified risks and implemented controls on request.

The *supplier relationship manager* prepares the selection of new suppliers and monitors them. He serves as an interface to contracted suppliers and monitors the network of suppliers continuously. Particular emphasis is put on monitoring that contracted suppliers adhere to contractual agreements based primarily on customer requirements. When supplier audits are conducted, he is involved in defining the audit scope.

The *customer relationship manager* needs to understand the customer's compliance and security requirements and match them to the organisational capabilities, i.e., in-house as well as outsourced solutions. He serves as an interface to prospects and customers. In order to be able to do that, the customer relationship manager needs to have a basic understanding of how known requirements are typically satisfied. If necessary, he contacts the compliance manager or the security manager to get detailed information about the feasibility of satisfying particular customer requirements. The customer relationship manager is involved in contract negotiations with prospects.

The *operations manager* communicates with prospects and contracted suppliers during contract negotiations. His main target is to clarify whether particular customer requirements can be satisfied by the network of suppliers at reasonable costs. This task is also performed by the customer relationship manager. However, the efficiency aspect is of particular interest for the operations manager. He is mainly in touch with executives at prospect organisations. In case of the development of new business areas or the offering of new services, the operations manager mandates an audit.

The *IT professional* ensures that the controls he is responsible for are implemented effectively. Apart from implementing the controls, the IT professional also monitors the controls continuously.

The *IT auditor* performs IT audits at client organisations which can be service providers as well as their suppliers and customers, and provides consulting services to them. Regarding IT audits, he supports financial auditors by auditing the financial information systems and conducts audits such as SAS 70. Within the scope of the consulting services, the IT auditor primarily helps client organisations to establish a control framework meeting their needs but he also assesses the maturity of selected controls before a certification is carried out. In fulfilment of his consulting tasks, he usually acts as an internal auditor from the perspective of the client organisation.

The main interaction links between the roles described above are presented in Figure . Bold lines indicate strong interaction links between roles, dashed lines weaker, but still clearly recognisable links. Although there are interactions among almost all roles identified, many of them are of limited frequency in the daily routine, but triggered by specific events. Due to the focus of this work on the main interaction links, links of limited relevance are neither shown in the figure nor discussed. The differentiation between types of interaction links is grounded on statements made within the scope of the interviews. The security manager outlines for example that the customer relationship manager creates and maintains profiles for every customer which are discussed on a regular basis and that he is in close contact with the customer relationship manager in order to be informed about the customer requirements. He also meets and communicates with the operations manager occasionally if important security related issues are urgent.

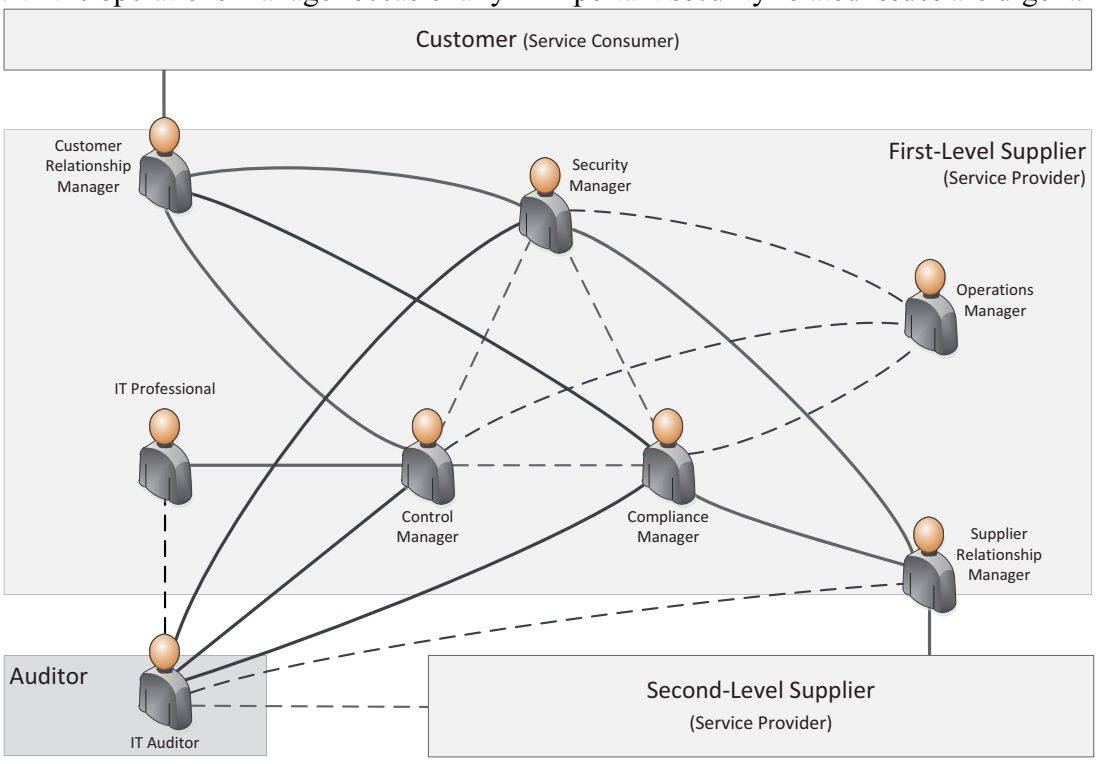

Figure 2: Interaction of employee roles across the different types of organisations.

We start the description of the interaction links at the interface to the customer where requirements are gathered. The key role at this interface between a customer and supplier is the customer relationship manager. He interacts with prospects to improve his understanding of their requirements and serves as a contact person for prospects and customers. He maintains a close relationship with customers and forwards gathered requirements to the security as well as the compliance manager. If necessary, he requests clarification concerning the satisfaction of customer requirements from the security manager, the control manager or the compliance manager.

The customer requirements not only have to be satisfied by the supplier itself, but also by further subcontracted suppliers (e.g., second-level suppliers) in case services are outsourced. The supplier relationship manager serves as interface to the network of subcontracted suppliers, maintains a close relationship with the network and assesses the suppliers' trustworthiness. He reports the current status of subcontracted suppliers, e.g., the degree to which security and compliance requirements are satisfied, and the status of contract negotiations with new suppliers to the security as well as the compliance manager. The supplier relationship manager discusses the fulfilment of customer requirements with the compliance and the security manager. Finally, he also communicates with auditors auditing new as well as subcontracted suppliers to get assurance about their fulfilment of security and compliance requirements. The supplier relationship manager is particularly involved in the scoping phase of such supplier audits. Both, customer relationship and supplier relationship manager are in close contact with the security and the compliance manager who maintain an overview of all organisational security and compliance activities, respectively. They work in close coordination as they clarify feasibility and costs of satisfying customer requirements.

The security and the compliance manager receive customer requirements from the customer relationship manager, match them to the organisational security and compliance strategy and, in case the IT required to satisfy customer requirements is outsourced, forward their results to the supplier relationship manager. In case the IT required to satisfy the customer requirements is operated internally, the control manager mandates IT professionals to address security and compliance requirements by implementing appropriate controls. The IT professionals implement the controls, monitor them continuously and report the status of the controls periodically or on request to the control manager. The control manager also interacts with business units and other specialists having detailed knowledge about processes, with the intent of gathering their security and compliance requirements and the peculiarities of their processes. The control manager reports the status of the controls to the security as well as to the compliance manager and, if requested, to the customer relationship manager.

The control manager is also the main contact person for auditors and typically maintains an overview of the internal controls and thus is able to provide the information usually requested by auditors. However, in case of very specific questions, auditors also interact directly with IT professionals.

The security and the compliance manager coordinate their decisions with the operations manager when new suppliers are selected and when contract negotiations with important prospects take place. Apart from that, the operations manager is also involved in decisions concerning the security and compliance strategy. For all aspects targeting the in-house IT, he is in contact with the control manager. Both, the security and the compliance manager engage auditors to audit subcontracted suppliers. Furthermore, they are also contact persons for auditors.

6. Managerial Implications

In the following, we present several managerial implications we concluded based on the results of the interviews reflecting key aspects of development relevant for organisations involved in cross-organisational security settings.

Standards for security requirements: A standardised way for describing security and compliance requirements seems useful, such as a model-based approach (Breu et al., 2008). Firstly, this would allow the development of an automated detection of conflicts and decision support tools for resolving conflicts in security and compliance requirements, e.g., between contradictory customer requirements. As a consequence, the requirement negotiations between customer and supplier would be shortened. Secondly, such a standard would help to unify the terminologies on requirements into a coherent one which would be again beneficial for requirements negotiations reducing the coordination loops needed. Thirdly, standardised descriptions would enable standardised reporting showing how security requirements are satisfied by controls which is essential information to be transferred to customers. Finally, such standardised requirement descriptions also seem to be beneficial for auditors and could help to improve the company's audit readiness.

Process definition: We identified one dominant and critical path of interaction links from customers via customer relationship manager, security manager or compliance manager and supplier relationship manager to subcontracted suppliers. In cases where the entire IT infrastructure is run in-house, however, this path is not or only to some extent organised. Because of its criticality, particular attention has to be paid for instance with respect to the definition of related processes as well as the description of goals, key activities, decisions and related rights for each role involved. Again, a standardised description of requirements is helpful for the information exchange between the processes.

Integrated tool supporting all key roles: We found only scattered tool support in the cross-organisational security settings we studied. A variety of tools exists for specialised tasks, especially in the domain of control monitoring. According to our interviewees, all roles develop tools on their own, mainly spread sheet based, to solve everyday problems specific to their field of duties. The output of these tools is usually a document which is used to communicate with customers or subcontracted suppliers. Data from such tools, however, cannot, or only to a limited extent, be reused in other applications. As a consequence, additional coordination effort arises. Due to the scattered usage of individual tools, an aggregated status is neither available on the current IT landscape across suppliers nor on the fulfilment of security and compliance requirements. This missing overview renders management of cross-organisational security settings and the

work of auditors less efficient. A promising approach would be an integrated tool supporting the key roles identified in this paper as desired by interviewees.

Reliability of audit reports: The efficiency of implementing security and compliance requirements is considered a key weakness in cross-organisational security settings. Since auditing service providers is costly and auditing subcontracted suppliers is difficult to realise from a legal point of view, customers as well as suppliers with at least partly outsourced IT. i.e. service providers of type I-III, rely on audit reports. These reports are often issued by different auditors and the details with respect to scoping and sampling decisions are often unknown. The level of uncertainty increases with a more comprehensive network of suppliers. In order to overcome this issue, supplier relationship managers maintain a close relationship to the network aiming at getting assurance that outsourced services satisfy all contractual agreements. The same principle holds for customer relationship managers who are in close contact with customers. We recognised a lack of specific guidance for customer relationship managers as well as supplier relationship managers. Thus, detailed guidelines and defined procedures could be beneficial in order to systematise actions in cases of uncertainty.

7. Conclusion

Based on a series of interviews conducted with professionals having long-standing experience with a number of relevant roles in several organisations, we introduced a setting which our interviewees deem typical for describing the main roles involved in cross-organisational security management. Most of the roles described are common in organisations providing services to other organisations. Attention has to be paid to cases in which service providers themselves source services from suppliers. In this context, service orchestrators that do not operate an IT infrastructure are extreme examples of organisational relationships in a cloud computing setting. In such cases, the role of the control manager loses importance and the role of the supplier relationship manager becomes increasingly important. Service providers typically have several customers imposing potentially different security and compliance requirements on them. Both satisfying such a potpourri of requirements and justifying correct implementation to customers in the scope of audits becomes more and more challenging as the complexity of networks of customers and suppliers get more comprehensive and opaque in the cloud.
Our analysis of key roles, their links of interaction as well as our interpretation of key requirements towards tools that can support these roles and their interactions support understanding of cross-organisational security management which has been neglected so far in the literature. The results suggest developing standards for security requirements, tools for visualising and coordinating the information exchange between the involved parties as well as organising and guiding primary processes coordinating interactions between the key roles involved in cross-organisational security management. Based on these results, several avenues for future research can be seen, e.g., reviewing standard definitions of roles and responsibilities in security management which have a long tradition, but are limited to organisation-internal settings, reviewing auditing practices and developing instruments that render IT audits in cross-organisational security settings more efficient or, last but not least, developing tools that help exchange information on

security and compliance between key roles interacting with each other across organisational boundaries.

Acknowledgments
The research leading to these results was partially funded by the European Union 7th Framework Programme (FP7) through the PoSecCo project (project no. 257129) and through the COSEMA project which is sponsored by the Tyrolean business development agency as part of the Translational Research program.

References

Abbot LJ (2007) Corporate Governance, Audit Quality, and the Sarbanes-Oxley Act: Evidence from Internal Audit Outsourcing. THE ACCOUNTING REVIEW 82(4), 23.

Aggarwal-Gupta M and Kumar R (2010) Look Who's Talking! Impact of Communication Relationship Satisfaction on Justice Perceptions. VIKALPA-The Journal for Decision Makers 35(3), 11.

Ang S and Straub DW (1998) Production and Transaction Economies and Is Outsourcing: A Study of the U.S. Banking Industry. MIS Quarterly 22(4), 535-552.

Auhagen AE (2001) Responsibility in Everyday Life. In Responsibility: The Many Faces of a Social Phenomenon (Auhagen AE and Bierhoff HW, Eds), pp 61-79, Routledge.

Barry B and Crant MJ (2000) Dyadic Communication Relationships in Organizations: An Attribution/ Expectancy Approach. Organization Science 11(6), 17.

Bulgurcu B, et al. (2010) Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. Management Information Systems Quarterly 34(3), 25.

Chen J, et al. (2010) Understanding the Approach for Auditing of Cloud Computing System. In Proceedings of the 2010 Second International Conference on Information Technology and Computer Science (ITCS), pp 581-583.

Chen Z and Yoon J (2010) It Auditing to Assure a Secure Cloud Computing. In Proceedings of 2010 IEEE 6th World Congress on Services, pp 253-259.

Chow R, et al. (2009) Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. Proceedings of the 2009 ACM workshop on Cloud computing security, ACM, Chicago, Illinois, USA, pp 85-90.

Chun M and Mooney J (2009) Cio Roles and Responsibilities: Twenty-Five Years of Evolution and Change. Information & Management 46(6), 323-334.

Dainty A, et al. (2006) Communication in Construction- Theory and Practice. Taylor & Francis.

Ezingeard J-N and Bowen-Schrire M (2007) Triggers of Change in Information Security Management Practices. Journal of General Management 32(4), 19.

Haeberlen A (2010) A Case for the Accountable Cloud. SIGOPS Oper. Syst. Rev. 44(2), 52-57.

Hayes B (2008) Cloud Computing. Communications of the ACM 51(7), 9-11.

Höhne K and Eloff JHP (2002) Information Security Policy- What Do International Information Security Standards Say? Computers & Security 21(5), 7.

Hu Q, et al. (1997) Research Report: Diffusion of Information Systems Outsourcing: A Reevaluation of Influence Sources. Information Systems Research 8(3), 288.

ITGovernanceInstitute (2007) Cobit 4.1.

Kadam A (2007) Information Security Policy Development and Implementation. Information Systems Security 16(5), 246-256.

Karyda M, et al. (2005) Information Systems Security Policies: A Contextual Perspective. Computers & Security 24(3), 246-260.

Kaufman LM (2009) Data Security in the World of Cloud Computing. IEEE Security and Privacy 7(4), 61-64.

Kaufman LM (2010) Can Public-Cloud Security Meet Its Unique Challenges? Security & Privacy, IEEE 8(4), 55-57.
Kloppenborg TJ (2009) Contemporary Project Management- Organize/Plan/Perform. South-Western Cengage Learning.
LeVeque V (2006) Information Security: A Strategic Approach. Wiley- Interscience.
Levina N and Ross JW (2003) From the Vendor's Perspective: Exploring the Value Proposition in Information Technology Outsourcing. MIS Quarterly 27(3), 331-364.
Miede A, et al. (2010) Cross-Organizational Security – the Service-Oriented Difference ICSOC/ServiceWave 2009, Springer Lecture Notes in Computer Science, 2010, Volume 6275/2010, Stockholm, Sweden, pp 72-81.
Moulton R and Coles RS (2003) Applying Information Security Governance. Computers & Security 22(7), 580-584.
Myler E and Broadbent G (2006) Iso 17799: Standard for Security. Information Management Journal 40(6), 43-52.
Paliotta AR (2001) Beyond the Maginot-Line Mentality: A Total-Process View of Information Security Risk Management. Information Systems Security 22(7), 4.
Patton MQ (2002) Qualitative Research & Evaluation Methods. Sage, Thousand Oaks.
Phillips J (2009) Pgmp- Programme Management Professional. McGraw-Hill.
Smedinghoff TJ (2010) Developing a Comprehensive Written Information Security Program. The Computer & Internet Lawyer 27(11), 15.
Stahl B (2004) Responsible Management of Information Systems. Idea Group Publishing.
Takabi H, et al. (2010) Security and Privacy Challenges in Cloud Computing Environments. IEEE Security & Privacy November/December, 24-31.
van Hoepen L and Verster V (2008) Client Services and Human Relations- Level 2. Pearson.
Van Niekerk JF and Von Solms R (2010) Information Security Culture: A Management Perspective. Computers & Security 29(4), 476-486.
Von Solms R (1998) Information Security Management (2):Guidelines to the Management of Information Technology Security (Gmits). Information Management & Computer Security 6(5), 3.
Vouk MA (2008) Cloud Computing: Issues, Research and Implementations. Journal of Computing and Information Technology 16(4), 235-246.
Wei Y and Blake MB (2010) Service-Oriented Computing and Cloud Computing: Challenges and Opportunities. IEEE Internet Computing November/December, 72-75.
Whitten D (2008) The Chief Information Security Officer: An Analysis of the Skills Required for Success. Journal of Computer Information Systems 48(3), 5.
Wood CC (2005) Information Security Roles & Responsibilities Made Easy. Information Shield.
Wylder J (2004) Strategic Information Security. Auerbach Publications.