Sector-Based Improvement of the Information Security Risk Management Process in the Context of Telecommunications Regulation

Nicolas Mayer[1], Jocelyn Aubert[1], Hervé Cholez[1], Eric Grandry[1]

[1] CRP Henri Tudor, 29 avenue John F. Kennedy, L-1855 Luxembourg, Luxembourg
{nicolas.mayer, jocelyn.aubert, herve.cholez, eric.grandry}@tudor.lu

Abstract. The current European regulation on public communications networks requires today that Telecommunications Service Providers (TSPs) take appropriate technical and organizational measures to manage the risks posed to security of networks and services. However, a key issue in this process is the risk identification activity, which roughly consists in defining what are the relevant risks regarding the business operated and the architecture in place. The same problem appears when selecting relevant security controls. The research question discussed in this paper is: how to adapt generic Information Security Risk Management (ISRM) process and practices to the telecommunications sector? To answer this research question, a four-step research method has been established and is presented in this paper. The outcome is an improved ISRM process in the context of the telecommunications regulation.

1 Introduction

Information systems are everywhere and their roles are central for all organisations because of the increasing amount of information managed during the last decades. Due to the criticality of the information exchanged, more and more supervision is needed and operated by national, European or even international authorities. This supervision and the associated regulations are often defined at a sector-based level. One of the leading sector having adopted such a model is the financial sector, with a National Regulatory Authority (NRA) established in every country and dealing with sector-based regulations, defined at the international and/or national level (e.g., Basel II agreements, the Sarbanes-Oxley Act, etc.). The same approach is currently applied to the telecommunications sector, with a supervision of the Telecommunications Service Providers (TSPs) operated by the NRAs of the different countries, such as ILR (*Institut Luxembourgeois de Régulation*) that is the NRA in Luxembourg.

The recent EU Directive 2009/140/EC [1] amends existing directives on framework (2002/21/EC), authorization (2002/20/EC), and access (2002/19/EC) of electronic communications networks and facilities. This directive should be transposed into a national legislation by all the EU member states and it has been done by the Luxembourg country with the publication of the law of the 27th February 2011 on electronic communications networks and services [2]. The EU Directive

introduces Article 13a on security and integrity of networks and services. This article says that Member States shall ensure that providers of public communications networks "take appropriate technical and organizational measures to appropriately manage the risks posed to security of networks and services" [1]. In addition, the article point out that "these measures shall ensure a level of security appropriate to the risk presented".

In 2010, the European Network and Information Security Agency (ENISA), as the centre of network and information security expertise for the European Union, initiated a series of meetings with the European Commission, Ministries, and Telecommunications NRAs to achieve a harmonized implementation of Article 13a. The result of this work was published in December 2011 in a document entitled "Technical Guideline for Minimum Security Measures" [3]. This document gives guidance to NRAs about the implementation of Article 13a. The starting point of the Minimum Security Measures is to identify, evaluate, and prioritise information security risks by establishing and maintaining an appropriate governance and risk management framework. This document explains also that the telecommunications organisations "should perform risk assessments, specific for their particular setting" [3]. For example, a particular characteristic of the telecommunications sector with regard to risk assessment is that the focus in put on the integrity of the networks and on the continuity of supply of services.

Based on this context, the research question discussed in this paper is: how to adapt generic Information Security Risk Management (ISRM) process and practices to the telecommunications sector? The outcome is a fine-tuned method, supported by a tool, aiming at helping the TSPs to perform efficiently ISRM, in order to be compliant with the European [1] and national [2] regulation. The main contribution of this paper is not on the resulting method (and tool) in itself, but is focussed on the approach followed to improve and fine-tune the ISRM process for our context.

Section 2 is an introduction to ISRM and explains the context of the telecommunications sector. Section 3 presents the research method applied to improve the ISRM process for the telecommunications sector. The two first steps of this research method are about the modelling of the telecommunications services through business processes and a reference architecture and are explained in Section 4. Then, the third step of the research method about the definition of a service-related knowledge base of risks is depicted in Section 5. Finally, Section 6 is about current state of the research work, conclusion and future work.

2 Information Security Risk and the Telecommunications Sector

The complete approach described in this paper is focussed on the concept of service, and more specifically on the concept of telecommunications service. A telecommunications service is a service provided by a TSP and "normally supplied for remuneration, which wholly or mainly provides the conveyance of signals on electronic communications" [4]. The conveyance of signals consists in the transmission, between or among points specified by the user, of information of the user's choosing. The TSP has the responsibility for the acceptance, transmission, and

delivery of the message [5]. Examples of telecommunications services registered and monitored by ILR are: fixed-line telephony service, mobile telephony service, dial-up internet access service, mobile internet access service, etc.

Each service can be decomposed in a set of business processes that are needed to establish and provide the service. Each telecommunications service, and thus each related business process, is realized by the information system of the telecommunications organization. We consider that the information system of a TSP is "a system in which human participants and/or machines perform work (processes and activities) using information, technology, and other resources to produce informational products and/or services for internal or external customers" [6]. The components of the information system are organized so that the system reaches its objectives: this organization is described in the architecture of the system: "an architecture is the fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution" [7]. As the system has the objective of fulfilling the telecommunications services, we will name the architecture that describes the system, the *telecommunications service architecture*. In the TSP sector, there are many types of architecture components, including information, hardware, network components, software, intangibles, but also people and facilities playing a role in the information system and so in its security [7], [8].

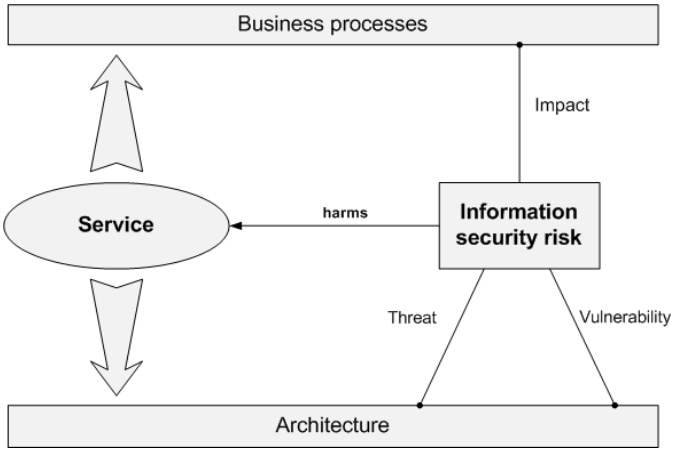

Fig. 1. ISRM in the context of the telecommunications sector

From a security point of view, risks are harming the telecommunications services. An information security risk is defined by three components: Risk = Threat * Vulnerability * Impact. In other words, risk is characterized by the opportunity of a threat targeting components of the architecture, to exploit one or more vulnerabilities originating from the design decisions of the architecture, and leading to an impact on business processes [8]. An example of information security risk is: a thief penetrating a telephone exchange (threat) because of lack of physical access control (vulnerability), stealing cables and thereby provoking loss of availability of the telephony service (impact). Fig. 1 depicts the main components described in this section and their relationships.

3 Research Method

In order to reach our objective of adapting the ISRM process and practices to the telecommunications sector in a structured way, we followed a research method composed of four steps described below. Although the target sector is highly competitive, we made the actors (service providers and the regulator) collaborate in order to co-construct the results of each step of the research method. It is indeed a way to ensure that the results are designed according to the needs and constraints of the actors, and that they are adopted by the end-users when they are rolled out. Workshops have been organised to present the objectives, and then to design and validate the components of the method. A representative panel of TSPs, covering all services, infrastructures and telecommunications media (e.g., optical fibre, satellite, etc.) were appointed by ILR to participate to the workshops. However, all other TSPs were invited to provide information by email through surveys performed before and after the different workshops.

Step 1 – *Modelling of the telecommunications services through business processes*: The first step consists in defining the different processes composing each telecommunications service. A literature review is performed in order to identify relevant documentation about telecommunications processes. Then, based on the literature review, a set of business processes is associated to each telecommunications service.

Step 2 – *Modelling of the telecommunications services through an information system architecture*: The second step of our research method consists in the description of the information system supporting each telecommunications service: listing the components that implement each service permits identifying the relevant threats and vulnerabilities and tracing these back to the actual service. The main challenge in this activity is to select the right level of abstraction in the description of the information system, taking into account the following objectives: (1) we aim at describing the telecommunications information system for the purpose of security risk management; (2) we target a description applicable to all operators providing the selected services in Luxembourg.

To describe the information system, we adopt the ISO/IEC 42010:2007 standard [7], which defines that a system (our telecommunications information system) has an architecture described by an architectural description. More important, the standard acknowledges that the architecture can be described from multiple viewpoints according to the specific concerns of the stakeholders. The scope of the second step of our research method is to build the architectural view that supports the management of information security risks for the telecommunication organisations in Luxembourg: we abstract away both the details that do not pertain to the domain of security risk management, and the specificities of each organisation. Building this telecommunication service architectural view can also be seen as building an industry architecture dedicated to security risk management in telecommunications according to the TOGAF architecture continuum [9]: this architecture is indeed a reference model for each TSP having the objective of managing information security risks.

Step 3 – *Definition of the service-related knowledge base of risks*: A key issue in ISRM is the risk identification activity, which roughly consists in defining what are the relevant risks, and thus the relevant threats, vulnerabilities and impacts, regarding the business operated and the architecture in place. Some generic knowledge bases already exist [10], [11], helping the analyst in the risk identification phase. However, it is generally difficult for non-experienced people to deal with such a knowledge base and determine what are the relevant sets of risk they need to consider. The same problem appears during the risk treatment phase and the security controls selection [10], [12]. The objective of this step is to predefine for each telecommunications service the (most) relevant threats and vulnerabilities, based on the reference architecture defined during step 2 and the (most) relevant impacts based on the business processes defined during step 1.

Step 4 – *Integration of the results in a software tool and experimentation*: The different models established during step 1 and step 2, as well as the risk and control knowledge bases established during step 3, are then integrated into a software tool already used to do ISRM in the frame of Information Security Management System (ISMS) establishment [13]. This tool needs to be validated by the NRA of Luxembourg, and then distributed to the TSPs as a support to fulfil their regulatory requirements related to ISRM.

4 Modelling of the telecommunications services through business processes and an information system architecture

The two first steps of the research method are about the modelling of the telecommunications services through business processes (step 1) and through an information system architecture (step 2). This section presents these two first and related steps, illustrated and summarised by Fig. 2.

4.1 Business process modelling

Step 1 of our research method consists in defining the different processes composing each telecommunications service. This step is crucial to understand the TSP activities and to propose a concrete business process framework understandable and meaningful for the TSPs.

As a first stage (**step 1.1**), a literature review was performed in order to identify relevant documentation about telecommunications processes. Several models and documents were studied and analysed. Finally, we mainly focussed on two well-established and well-accepted process models: the Business Process Framework ("eTOM") of the TMForum [14] and the Telecommunications Process Classification Framework of IBM and the American Productivity & Quality Center (APQC) [15]. These two models were widely known by Luxembourgish TSP and sometimes already used. Based on these models, we wanted to establish a customized process

model not to give priority to one specific model, and mainly to have a model really adapted to our needs.

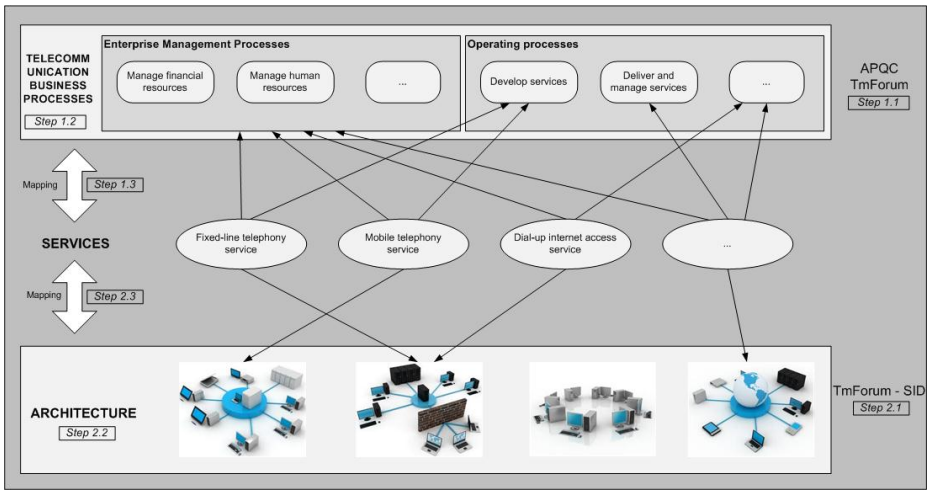

Fig. 2. Modelling of the telecommunications services through business processes and an information system architecture

The process model was established in **step 1.2**. In order to be accurate and avoid a cumbersome model, we defined the scope of the ISRM to focus only on the core business of TSPs. Thus, we selected only the relevant processes which can have a negative impact on the security or continuity of services provided over the networks. The selection of processes was done by comparing and bringing together processes of the different models. In our scope, the processes of different models were fairly similar, and then the process selection was straightforward. Only some processes were grouped together to avoid complexity and some others were divided to be more significant and relevant for ISRM. Two groups of processes were defined to separate (1) all processes related to the "Enterprise Management Processes" including support processes, strategy processes, etc., and (2) all "Operating Processes" that are directly related to the telecommunications service management. This separation in two groups is particularly useful since TSPs often manage several different services, and to perform ISRM on a high number of processes is a complex and substantial work. Our model allows performing the ISRM process on the "Enterprise Management Processes" only once, independently of the number of services managed by the TSP, because the activities performed in this group of processes are common to all delivered services. Then, the ISRM process is performed on each "Operating Processes" of each telecommunications service, the operating processes being clearly different from one service to another (i.e. involving different architecture components and pursuing different business objectives). In a nutshell, for a TSP with n services, the ISRM process is applied on the following number of processes: (1 * "Enterprise Management Processes") + (n * "Operating Processes").

Finally, in **step 1.3**, after having been co-designed by ILR and several TSPs, the process model was submitted to and validated by them. In this final version, the group "Enterprise Management Processes" contains 5 processes:

1.1 Develop vision and strategy,
1.2 Manage financial resources,
1.3 Manage human resources,
1.4 Manage knowledge, research, and change,
1.5 Manage stakeholder and external relationships.

In the second group, "Operating Processes", there are 6 processes:

2.1 Develop and acquire resources (application, computing, and network),
2.2 Manage resources (application, computing, and network),
2.3 Develop services,
2.4 Market & sell services,
2.5 Deliver and manage services,
2.6 Manage supplier/partner relationship.

4.2 Architecture modelling

In this second step, we aim at producing the description of the Telecommunications Service Architecture. This modelling activity was performed iteratively, each iteration dealing with a specific registered service. This guarantees that the scope of the modelling exercise is better managed and that the experience gained in the first iterations is injected in the next ones.

The first stage (**step 2.1**) of this activity aims at proposing a model of the concepts that are relevant in this specific view of the system. We reviewed the literature and the industry standards in order to identify enterprise architecture models of reference for telecommunication. The works of The Open Group and TMForum have been specifically analysed and confronted to the state-of-practice of the national TSPs, and we finally selected the Information Framework (SID) from the TMForum [16]. This model suits well our needs as it is centred on the concept of service, and it describes the relations between service and resource (i.e. architecture components).

As illustrated in Fig. 3, we adopted a layered architecture organised according to the SID model. The Customer Facing Service layer encompasses the services registered at ILR (fixed and mobile phone and data services). The Resource Facing Service layer represents the functional blocks of the architecture: this layer has been omitted at the beginning of the modelling exercise and introduced later for sake of reuse across services. The Resources layer contains all the resources that implement the services. Several classifications of resources (logical vs. physical, asset classification from ITU-T [17]) have been considered, but without actually bringing differentiating value at this stage. Finally, we extended the model with the Facility layer in order to capture the fact that resources are physically localised in facilities.

The second stage (**step 2.2**) of this activity was to identify the resources that are meaningful in the scope of ISRM. Information about the implemented architecture was collected from the TSPs, and the resources were selected according to the abstraction principles described in the approach: is this resource meaningful for all operators, is this resource relevant to identify risks on the services managed by the

regulator, etc. This modelling exercise was collaboratively conducted: the active participation of both the operators and the regulator is indeed required in order to reach the objective in the abstraction process. At the end of this stage, we had a list of resources for each telecommunications service.

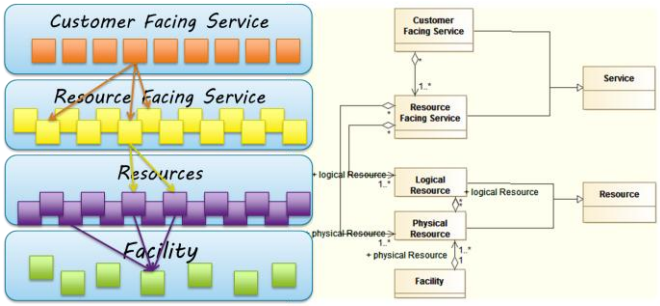

Fig. 3. Telecommunications Service Architecture metamodel

The last stage (**step 2.3**) was the actual production of the telecommunications service architecture. The resources listed in step 2.2 were put in the context of the services they implement, and the reference model selected in step 2.1 was instantiated. During this modelling activity, the participants naturally grouped the resources according to some shared functions commonly accepted in the industry (Access, Core, Transmission, Business Support, Infrastructure, Security, Devices) leading to the emergence of the Resource Facing Service layer of the service architecture. An architectural description can be represented in multiple forms, from a formal model to a totally informal drawing. In this project, it was decided to represent the architecture as a catalogue of resources implementing each service. This catalogue is currently described in an Excel sheet, although it can later be transformed into a relational database accessible through a web application, or into any other technological form. The most important aspect is that the model (whatever the form of representation) respects the metamodel of the architecture: all elements are instances of the concepts and relate to other elements according to the metamodel.

The outcome of step 2 of the research method is thus a catalogue of resources, implementing each registered service, and thus composing the telecommunications service architecture.

5 Definition of the service-related knowledge base of risks

The third step of the method, illustrated by Fig. 4, aims at defining a service-related knowledge base of risks specially tuned for TSPs. By service-related knowledge base of risks, we mean a set of threats, vulnerabilities and impacts specifically targeting elements of the architecture modelled in the previous step. In addition, with the aim of simplifying and focussing on the telecommunications sector, we strive to simplify the base as much as possible, and to propose to this extent only elements relevant for

TSPs. Wherever possible, threats and vulnerabilities are associated to generic elements of architecture, to automatically provide TSPs with possible threats and exploited vulnerabilities. In the frame of their ISRM process, for a given service, TSPs will mainly have to indicate if (pre-selected) threats apply or not, and how their system is vulnerable. It is however important for each TSP to think also about its specificities (at the business or architecture level) potentially implying specific risks, involving non-pre-selected threats/vulnerabilities.

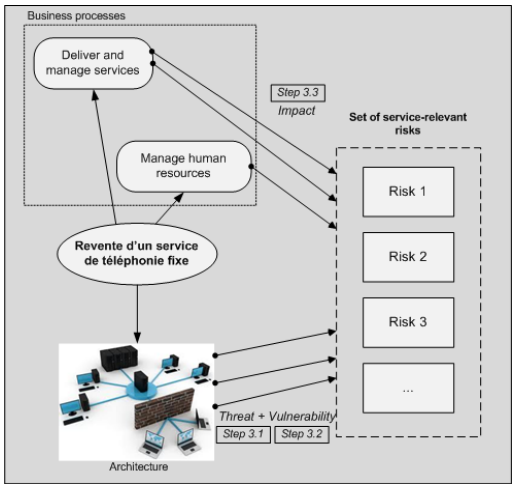

Fig. 4. Definition of the service-related knowledge base of risks

As a first stage (**step 3.1**), an inventory of standards and references proposing knowledge bases of threats was made. Various documents were studied, including documents proposing generic approaches for risk assessment [10], [11], [18]–[22] as well as documents targeting specifically telecommunications-related risk assessment [20], [23], [24]. Threats were analysed and selected to propose a subset of threats focussing essentially (as pointed out by the law) on those harming availability of services and integrity of networks. To avoid duplicates, same threats issued from different documents were selected only once. When applicable, with the intention of simplifying threat selection, threats were grouped as far as possible: for example threats targeting the same type of components, having very close impact, having the same origin (deliberate, accidental, environmental), were checked for being grouped together. In this way, as an example, the following threats, issued from [10], *Climatic phenomenon*, *Seismic phenomenon*, *Volcanic phenomenon*, *Meteorological phenomenon* and *Flood* were grouped into a new threat called *Natural Disaster* since they generally target facilities, have environmental origin and harm integrity and/or availability. On the contrary, some threats were specified, to allow a better applicability to the telecommunications sector. This is, for example, the case of the threat *Theft of equipment* specified by *Theft of cable* meaningful for TSPs. This step led us to identify twenty-two threats. Finally, each threat is associated with generic elements of architecture (defined in step 2) that may be impacted.

Similarly, in **step 3.2**, an inventory of standards and references proposing knowledge bases of vulnerabilities was made [10], [11], [19], [20], [24].

Vulnerabilities potentially exploitable by the threats selected during the previous step were selected. As in Annex D of ISO/IEC 27005 [10], examples of threats that might exploit these vulnerabilities are associated with each vulnerability. In the case of relatively close vulnerabilities issued from different sources, when relevant, an effort of reconciliation has been made. In some cases, vulnerabilities are specified, in order to be more significant for TSPs; this is, for example, the case for the vulnerability *Bad configuration* specified by *Badly configured network routers, gateways or firewalls*. This step led us to identify more than ninety vulnerabilities.

In **step 3.3**, an impact scale was defined. Such scale will be used by TSPs to qualify the effects of a threat exploiting one or more vulnerabilities on the targeted process(es). To that purpose, we rely on the scale provided by ILR for the notification of any breach of security or loss of integrity which is (1) *Between 1% and 2% of customers are affected for at least 3 hours*, (2) *Between 2% and 5% of customers are affected for at least 2 hours*, (3) *Between 5% and 10% of customers are affected for at least 1 hour* and (4) *More than 10% of customers are affected regardless of the length*. Taking into account the possible consequence of a given threat regarding the actual vulnerabilities, TSPs will have to estimate the impact using this scale. Reusing a scale already used by ILR and TSPs should facilitate its acceptance and common understanding.

Finally in **step 3.4** (currently planned), the service-related knowledge base of risks composed of threats, vulnerabilities and impacts is submitted to ILR and to several TSPs of Luxembourg during a workshop in order to collect their feedback and suggestions for improvement. This step is part of an iterative process; threats, vulnerabilities and impacts can be improved following the TSPs comments. The overall idea behind this approach is to reach a consensus, and provide a common reference basis allowing TSPs to perform risk assessment and ILR to more easily compare the results.

6 Current state, conclusion and future work

6.1 Current state of the research work

Today, we have established and validated the telecommunications business process model (**step 1**). We have also identified the architecture components used in each telecommunications service (**step 2**). Some enhancements can still be brought like finer classification of services and resources in the architectural description: although we initially prevented from introducing details of technical implementation in the service layers (e.g., phone VoIP vs. PSTN), it might be useful to introduce this separation when specific risks only affect a specific technology; in the same way, a classification of resources according to some model might be useful when identifying generic threats and vulnerabilities. We however have to balance between complexity of the classification and level of reuse. The definition of the service-related knowledge base of risks is not currently finished (**step 3**) and the integration of the results in a software tool and experimentation (**step 4**) is still work in progress. The

different threats, vulnerabilities, and impacts on services are defined, but further validation needs to be done. In the same manner, the software tool integrates all current results and the development of the first usable version is complete, but some tests by the future users should be done to adapt the tool to theirs needs and requirements. The final version of the software tool is expected in a few months.

After these last validations, the main next step is to experiment the method and the tool on TSPs providing different services and being of different size and maturity level. A presentation of the results and training sessions are also planned to support them during the ISRM process.

6.2 Conclusion and future work

In this paper, we have presented our approach to establish an improved process to deal with information security risks in the telecommunications sector. After having detailed our context, i.e. the telecommunications sector in Luxembourg, and our scope, i.e. what we mean by information security risk, the four-step research method we defined and applied is presented. Then, the way we performed these four steps and the results obtained are presented.

As explained in the section dedicated to the current state of the work, we know that our results are still subject to validation, because most of the experimentation work is still to be done. We expect to analyse the quality and relevance of the risk management results of the TSPs, and thus to be able to validate the quality of our improved process. The ease of understanding of the process and the efficiency of the work that will be performed by the TSPs during their ISRM activities are also key indicators of the quality of our results. Finally, the use of a co-design approach, involving the different stakeholders from the beginning of the work, seems to us a key asset to quickly reach an optimized process.

Regarding future work, our results can be disseminated at the European level and other countries may use them in order to comply with the European legislation. We are currently discussing and presenting our research work to the European telecommunications regulator. Another natural way of extension would be to apply the same research method to other sectors in Luxembourg having defined sector-based regulations, such as the financial sector or the records management sector.

Acknowledgments. Thanks to ILR, the NRA of Luxembourg.

References

[1] Official Journal of the European Union, *Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009*. 2009.

[2] Journal Officiel du Grand-Duché de Luxembourg, *Loi du 27 février 2011 sur les réseaux et les services de communications électroniques*. .

[3] M. Dekker, D. Liveri, D. Catteddu, and L. Dupré, “Technical Guideline for Minimum Security Measures - Guidance on the security measures in Article 13a,” ENISA (The European Network and Information Security Agency), Dec. 2011.

[4] Official Journal of the European Communities, *Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)*. 2002.
[5] Federal Communications Commission, *Telecommunications Act of 1996*. .
[6] S. Alter, "Defining Information Systems as Work Systems: Implications for the IS," *European Journal of Information Systems*, vol. 17, no. 5, pp. 448–469, 2008.
[7] ISO/IEC 42010, *Systems and software engineering -- Recommended practice for architectural description of software-intensive systems*. Geneva: International Organization for Standardization, 2007.
[8] É. Dubois, P. Heymans, N. Mayer, and R. Matulevičius, "A Systematic Approach to Define the Domain of Information System Security Risk Management," in *Intentional Perspectives on Information Systems Engineering*, S. Nurcan, C. Salinesi, C. Souveyet, and J. Ralyté, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 289–306.
[9] The Open Group, *TOGAF Version 9.1*. Van Haren Publishing, The Netherlands, 2011.
[10] ISO/IEC 27005, *Information technology – Security techniques – Information security risk management*. Geneva: International Organization for Standardization, 2011.
[11] ANSSI, *EBIOS 2010 - Expression of Needs and Identification of Security Objectives*. France: http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html, 2010.
[12] ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security management*. Geneva: International Organization for Standardization, 2005.
[13] N. Mayer, "A Cluster Approach to Security Improvement according to ISO/IEC 27001," presented at the Software Process Improvement, 17th European Conference, EuroSPI 2010.
[14] TMForum, "TM Forum - eTOM Business Process Framework." [Online]. Available: http://www.tmforum.org/BusinessProcessFramework/1647/home.html. [Accessed: 11-Feb-2013].
[15] American Productivity & Quality Center (APQC) and IBM, "Telecommunication Process Classification Framework," Nov. 2008.
[16] TMForum, "TMForum Frameworx - SID Service Overview," GB922-4SO, 2011.
[17] ITU (International Telecommunication Union), "ITU-T X.1057 Asset Management Guidelines in Telecommunication Organizations," Recommendation ITU-T X.1057, 2011.
[18] L. Marinos and A. Sfakianakis, "ENISA Threat Landscape - Responding to the Evolving Threat Environment," ENISA (The European Network and Information Security Agency), Sep. 2012.
[19] Ministerio de Hacienda y Administraciones Públicas, "MAGERIT - versión 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro II: Catálogo de Elementos," Oct. 2012.
[20] National Institute of Standards and Technology, "NIST Special Publication 800-30 Guide for Conducing Risk Assessments," Sep. 2012.
[21] C. Alberts and A. Dorofee, "OCTAVE Threat Profiles," Software Engineering Institute, Carnegie Mellon University, White paper.
[22] Bundesamt für Sicherheit in der Informationstechnik, "Supplement to BSI-Standard 100-3, Version 2.5 - Application of the Elementary Threats from the IT-Grundschutz Catalogues for Performing Risk Analyses," Federal Office for Information Security, Bonn, Germany, Aug. 2011.
[23] M. D. Collier, "Enterprise Telecom Security Threats," 2004.
[24] ITU (International Telecommunication Union), "ITU-T X.1055 - Risk management and risk profile guidelines for telecommunication organizations," Nov. 2008.