Sector-Specific Tool for Information Security Risk Management in the Context of Telecommunications Regulation (Tool demo)

Nicolas Mayer
CRP Henri Tudor
L-1855 Luxembourg-Kirchberg
nicolas.mayer@tudor.lu

Jocelyn Aubert
CRP Henri Tudor
L-1855 Luxembourg-Kirchberg
jocelyn.aubert@tudor.lu

ABSTRACT

The current European regulation on public communications networks requires that Telecommunications Service Providers (TSPs) take appropriate technical and organisational measures to manage the risks posed to security of networks and services. After having adapted generic Information Security Risk Management (ISRM) process and practices to the telecommunications sector, these methodological aspects are integrated in a supporting tool dedicated to the TSPs. The objective of this paper is to present the features and our approach for fine-tuning TISRIM, our ISRM tool, to the telecommunications sector.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms

Management, Measurement, Performance, Security.

Keywords

Information Security, Risk Management, Regulation, Telecommunication.

1. INTRODUCTION

Security of information and networks is today a top priority concern for critical sectors such as health, energy or telecommunications. Due to the sensitivity of information exchanged, more and more supervision is needed and operated by national, European or even international authorities. Regarding the telecommunications sector, EU Member States shall ensure that providers of public communications networks manage their risks related to security of networks and services, and take appropriate measures to mitigate these risks, as required in the EU Directive 2009/140/EC [6]. A supervision of the Telecommunications Service Providers (TSPs) is thus required and operated by the National Regulatory Authorities (NRA) of the different countries, such as ILR (*Institut Luxembourgeois de Régulation*) that is the NRA for Luxembourg.

Based on this context, to adapt and facilitate Information Security Risk Management (ISRM) to the telecommunications sector is the topic of a research project developed by our research group and ILR. The research method used and the methodological results obtained were described in a preceding paper [5]. The scope of this paper is the integration of these methodological results into a software tool.

Section 2 presents the regulation context and summarises the domain of ISRM. Section 3 recaps our research approach and the obtained methodological results. Section 4 is about our software tool, entitled TISRIM, and its fine-tuning for ISRM in the telecommunications sector. Finally, Section 5 concludes about current state of the tool and its experimentation by the TSPs.

2. THE REGULATORY CONTEXT AND INFORMATION SECURITY RISK MANAGEMENT

2.1 Regulation on security and integrity of networks and services

The recent EU Directive 2009/140/EC [6] 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 Luxembourg with the publication of the law of the 27th February 2011 on electronic communications networks and services.

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” [6]. In addition, the article points 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 2013 in a document entitled “Technical Guideline on

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
Request permissions from Permissions@acm.org.

SIN '14, September 09 - 11 2014, Glasgow, Scotland Uk
Copyright 2014 ACM 978-1-4503-3033-6/14/09…$15.00.
http://dx.doi.org/10.1145/2659651.2659665

Security Measures" [1]. This document gives guidance to NRAs about the implementation of Article 13a. The starting point of the 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" [1]. An example among others of the sector specificities with regards to information security is that the focus is put on the integrity of the networks and on the continuity of service supply, confidentiality of data and privacy being secondary concerns in the regulation. As a consequence, specific sector-based practices shall be added or adapted to the standard ISRM process, in order to facilitate its use by TSPs.

2.2 Information Security Risk Management in a nutshell

As representative of ISRM activities, Figure 1 represents the ISRM process as defined in the ISO/IEC 27005 standard [3]. This process is composed of steps that are typically found in the different existing methods and standards. The steps can be summarised as follows:

Context establishment: This step consists of precisely defining the scope and boundaries of the study at first. Then, organization for risk management shall be defined, mainly supported by roles and responsibilities definitions. Finally, the set of basic criteria shall be established. Basic criteria are the criteria used to analyse and evaluate risk (*e.g.*, impact criteria, risk evaluation criteria, risk acceptance criteria…). In our context, they are defined under the form of measurement ranges.

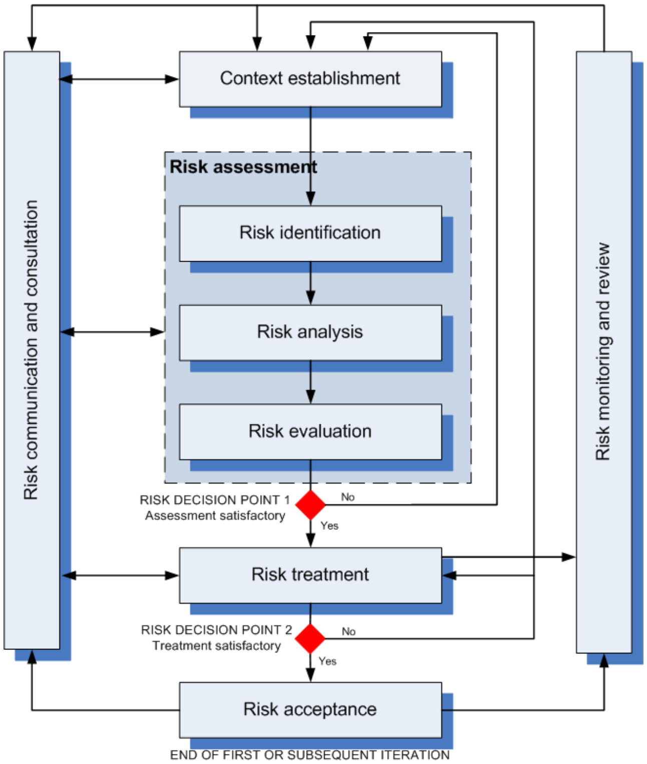

Figure 1. The ISRM process (as depicted in [3])

Risk identification: Risk identification is the process of finding, recognizing, and describing risks. A security risk is usually defined by a threat, exploiting one or several vulnerabilities, and leading to a negative impact on the assets of the organisation. The purpose of this step is to obtain a list of relevant risks, taking into account the context of the organisation.

Risk analysis: Risk analysis is the process of comprehending the nature of risk and determining the level of risk. Basic criteria are used to perform risk analysis. The purpose of this step is to add to the list of relevant risks their magnitude and thus to be able to rank the risks.

Risk evaluation: Risk evaluation is the process of comparing the results of risk analysis with risk (acceptance) criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. The purpose is to assist the risk analyst in its decision about risk treatment.

The reader should note that we mean by "risk assessment" the composition of the 3 preceding steps: risk identification, risk analysis, and risk evaluation.

Risk treatment: Once risk assessment is performed, controls to reduce, retain, avoid, or share the risks should be selected, and a risk treatment plan needs to be defined.

Risk acceptance: Risk acceptance is the activity of explicitly accepting residual risks (*i.e.*, risk remaining after risk treatment) by the managers of the organization.

Risk communication and consultation: Information about risks should be exchanged and/or shared between the decision-maker and other stakeholders all along the different steps of the process.

Risk monitoring and review: Risks and their factors should be continually monitored and reviewed to identify any changes in the context of the organization at an early stage, and to maintain an accurate overview of the complete risk picture.

3. RESEARCH METHOD

The objective of our research project is to adapt the ISRM process (see Section 2.2) and its related practices to the telecommunications sector and its regulatory constraints (see Section 2.1). To reach this objective in a structured way, we defined a four-step research method we then followed [5].

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

Step 2 – *Modelling of the telecommunications services through an information system architecture*: The second step of our research method consisted of 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 was to select the right level of abstraction in the description of the information system, taking into account (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.

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 [3], 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 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, need then to be integrated into a software tool.

The rest of this paper is focused on Step 4 of the research method. The reader should note that this research method and results of Step 1 to Step 3 are described in further details in our preceding paper [5].

4. TISRIM, A SUPPORTING TOOL FOR ISRM IN THE TELECOMMUNICATIONS SECTOR

In this section, the TISRIM tool and its adaptation to the telecommunications sector is presented. The aim of the tool is to provide a support to TSPs in Luxembourg for the compliance with the Article 13a.

4.1 TISRIM – Tudor Information Security Risk Management tool

TISRIM is a software tool dedicated to and only focused on ISRM (see Section 2.2). The tool has been released in 2009 and about 15 companies have already used the tool with our support, going from SMEs to European institutions. Until now, it has mainly been used to perform ISRM in the frame of Information Security Management System (ISMS) establishments and ISO/IEC 27001 certifications [4]. In its standard version (*i.e.* not sector-specific), the tool is compliant with international standards (ISO 31000 [2], ISO/IEC 27005 [3]) at the process level, but user-free at the practice level (risk formula, risk evaluation criteria, risk impact criteria, knowledge bases adaptation available for threats, vulnerabilities, impacts, controls…).

4.2 Approach for fine-tuning the tool to the telecommunications sector

4.2.1 Methodological approach

To define a methodology and its associated tool that meet the exact needs of the users (*i.e.* TSPs in Luxembourg), we decided to define both the methodology and tool in collaboration with them. Therefore, we favoured a user-centered design approach. To this end, and in a spirit of cooperative design, we organized a series of workshops or focus groups (around ten sessions took place) with a representative panel of TSPs during which we collected not only the specificities of the sector, but also specified the needs of users and the expectations of both TSPs and the NRA. This phase of co-design enabled the definition of the methodology, the overall design of the tool, and last but not least the establishment of common databases of elements specific to the sector.

The iterative adaptation of TISRIM was able to start early during the phase of co-design, providing flexibility with regards to the functional requirements. As soon as possible (that is to say as soon as the tool proposed features relevant for users), a representative pool of users (different company size, different ISRM knowledge, etc.) was able to test the tool. These tests were designed firstly to ensure the relevance from a functional point of view of the tool (functional testing), but also from a usability point of view (usability testing). Iteratively, tests results allowed improving the tool but also the methodology by a bottom-up approach.

4.2.2 Fine-tuning of the tool

As explained previously, the adaptation of the tool was based on a cooperative design involving both TSPs and the NRA. Such an approach allowed integrating sector-specific knowledge, including knowledge bases and a first level of risk identification (typical services and assets, main threats…), that helps to ease the ISRM process. The major changes and adaptations of the tool are detailed below.

Basic criteria, particularly impact criteria, have been designed with the aim of avoiding duplication of scales, and to facilitate the assessment of impact for a risk scenario. Therefore, it seemed particularly appropriate to adopt scales well known by TSPs, *i.e.* impact scales in terms of percentage of affected customers and of expected unavailability. Indeed, such scales are already used for incident notification, as required by the European and national regulation [6]. The use of common scales for ISRM and incident notification may be worthwhile to formally identify scenarios that may lead to incident declaration, in order to prevent their apparition.

While TSPs shared with us the specificities of their business, in terms of assets location and types, it appeared not appropriate to consider a telecommunications service (primary asset) as a whole. Indeed, telecommunications services are carried out by numerous supporting assets, which are not targeted by the same threats, do not own the same vulnerabilities, etc. So, it became obvious to highlight the technical architecture behind the realisation of these services. In this sense, the notion of “group” was introduced. A group is defined as a collection of supporting assets having the same (geographical) impact, being exposed to the same threats, having the same vulnerabilities, and requiring the same security level. In this way, the definition of groups allows a more efficient and relevant risk assessment of services. In parallel, common infrastructure elements used by all the TSPs to deliver a specific service have been identified. The predefinition of such elements within the knowledge bases of the tool prevents the user to be obliged to key it in.

Knowledge bases of threats and vulnerabilities commonly used in ISRM (extracted for example from [3]) have been refined and tailored to the telecommunications sector. Regarding our scope and our context, a focus was placed on threats harming availability and integrity. 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 and having the same origin (deliberate, accidental, environmental) were checked for being grouped together. At the opposite, some threats were specified to allow a better applicability to the telecommunications sector. A similar work has been done with vulnerabilities in order to be more significant for TSPs. At the same level, when defining risk scenario composed of a threat exploiting one or several vulnerabilities and leading to an impact to the telecommunications service, it is possible for the user to specify the subset of supporting assets directly targeted by the threat (*i.e.* affected assets) in order to obtain a risk scenario as elaborated as possible.

An additional feature has been added to the tool, allowing TSPs to perform a self-assessment towards the 25 security objectives introduced by the ENISA Technical Guideline on Security Measures [1]. For each of these objectives, TSPs can indicate a level of sophistication, the related security measures taken towards achieving the security objective, the evidence that could be taken into consideration by an auditor to be assured that the objective is reached, and any useful comment. This self-assessment is particularly complementary with the risk assessment, because it helps to justify the good coverage of risks on the one hand and the identified weaknesses on the other hand.

After completing both the risk assessment and the self-assessment of the Guideline, TSPs are able to generate a report in XML format for submission to the NRA. The choice of such a language both human-readable and machine-readable was guided by the need for interoperability (between future versions of the tool, but also to allow any TSP to generate such report without the use of the tool) and the need for the NRA to be able to exploit such results in a simplified and efficient way.

4.3 The different steps defined in the tool

The TISRIM tool is actually a Microsoft Excel workbook, with different macros written in Visual Basic for Applications (VBA), and whose operation is totally different from a simple spreadsheet file. Indeed, most of the interactions are realized using wizards developed for this purpose. Moreover, user entries are restricted by data validation. Users are thus step-by-step guided following the methodology and cannot theoretically enter inappropriate information.

TISRIM takes advantage of the notion of sheet of a workbook, as it is organised by sheet; each sheet providing a particular feature. Below, descriptions of each sheet are detailed.

4.3.1 Basic criteria

This sheet displays the basic criteria used for the risk assessment, namely impact criteria, risk evaluation criteria (for threat and vulnerability) and risk acceptance criteria. Since the scales are established by the NRA and shared by the whole sector, this sheet is for information purpose only and does not offer any interaction.

4.3.2 Services

This sheet allows listing and managing (*i.e.* adding, modifying and deleting) the electronic telecommunications services (a.k.a. primary assets) and their supporting assets, organised by group.

4.3.3 Supporting assets

This sheet allows listing and deleting the supporting assets considered in the risk assessment. Their selection is performed in the preceding step, when defining services.

4.3.4 Mapping

This sheet displays which supporting assets are used to provide an electronic telecommunications service. It allows to generate a report about primary assets and their mapping with supporting assets. It is a summary of the service selection and definition step.

4.3.5 Risk assessment

This sheet allows to identify threats, affected assets and vulnerabilities; to assess the levels of threat, impact and vulnerabilities (current and residual); to define a treatment for each identified risk; and finally to define control(s) to mitigate risks whose treatment requires control implementation.

4.3.6 Technical Guideline

This sheet allows assessing high-level security objectives issued from the Technical Guideline on Security Measures [1].

5. CONCLUSIONS AND CURRENT STATE

The tool is now fully functional and has been distributed to all the TSPs established in Luxembourg wishing to use it. To this end, several training sessions about the method and the related use of the tool have been carried out; over 25 TSPs were trained. In this way, they will be able to use TISRIM to meet the regulatory requirements, which requires them to perform ISRM and provide the results to the NRA. Thanks to another dedicated tool (currently under development) the results will be processed and the NRA will thus be able to exploit such an amount of data thanks to generated reports and statistics.

In parallel with this specific development of TISRIM for the telecommunications sector, other adaptations of the tool are already planned or in progress; especially for the health sector and the financial sector, but also to include a systemic approach in ISRM (moving from one identified entity to a complete service supply chain).

Finally, aware of the intrinsic limitations of a spreadsheet file, we are considering the feasibility of moving to a more scalable and maintainable format (*i.e.* SaaS solution), taking into consideration issues related to the confidentiality of data processed.

6. ACKNOWLEDGMENTS

Thanks to ILR, the NRA of Luxembourg.

7. REFERENCES

[1] Dekker, M. and Karsberg, C. 2013. *Technical Guideline on Security Measures - Technical guidance on the security measures in Article 13a*. ENISA (The European Network and Information Security Agency).

[2] ISO 31000 2009. *Risk management – Principles and guidelines*. International Organization for Standardization.

[3] ISO/IEC 27005 2011. *Information technology – Security techniques – Information security risk management*. International Organization for Standardization.

[4] Mayer, N. A Cluster Approach to Security Improvement according to ISO/IEC 27001.

[5] Mayer, N. et al. 2013. Sector-Based Improvement of the Information Security Risk Management Process in the Context of Telecommunications Regulation. *Systems, Software and Services Process Improvement*. F. McCaffery et al., eds. Springer Berlin Heidelberg. 13–24.

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