



A risk management framework for security and integrity of networks and services

Nicolas Mayer & Jocelyn Aubert

To cite this article: Nicolas Mayer & Jocelyn Aubert (2020): A risk management framework for security and integrity of networks and services, Journal of Risk Research, DOI: [10.1080/13669877.2020.1779786](https://doi.org/10.1080/13669877.2020.1779786)

To link to this article: <https://doi.org/10.1080/13669877.2020.1779786>



© 2020 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 24 Jun 2020.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)

A risk management framework for security and integrity of networks and services

Nicolas Mayer  and Jocelyn Aubert

IT for Innovative Services, Luxembourg Institute of Science and Technology, Esch-sur-Alzette, Luxembourg

ABSTRACT

It is clearly acknowledged that, in complex sectors like telecommunications, to consider an infrastructure as fully secure, although desirable, is not realistic. The current European regulation on public communications networks is aware of this assumption and currently requires that Telecommunications Service Providers (TSPs) take appropriate technical and organizational measures to manage the risks posed to the security of networks and services. In this context, risk management has become both a key aspect for dealing with security and a main trust vector included particularly in regulations. In this context, our paper concerns the establishment of a national security risk management framework to comply with national and European regulations for TSPs. This framework is composed of two parts: a security risk management tool to be used by the TSPs and an analysis tool to be used by the regulatory authority to gather and assess the risk management reports from the TSPs. The latter is specifically used to benchmark the security level of TSPs and the security of the sector as a whole. This paper reports on the design of this framework and the challenges emerging after an entire regulatory cycle.

ARTICLE HISTORY

Received 21 June 2019

Accepted 16 April 2020



KEYWORDS

Information security;
telecommunications;
regulatory frame-
work; regtech

Introduction

Nowadays, there is a strong emphasis on the security of information systems and the management of cybersecurity risks. Numerous regulations are emerging that impose a risk-based approach on entire economic sectors for information system security. Compliance with these regulations concerning innovative regulatory technologies, also known as ‘RegTech’, is currently a challenge for organizations.

In the telecommunications sector, Article 13a of the EU Directive 2009/140/EC (Official Journal of the European Union 2009), updated in December 2018 as part of the European Electronic Communications Code (Official Journal of the European Union 2018), concerns the security and integrity of networks and services. This article states 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’. In addition, the article points out that ‘these measures shall ensure a level of security appropriate to the risk

CONTACT Nicolas Mayer  nicolas.mayer@list.lu  Luxembourg Institute of Science and Technology, Esch-sur-Alzette, Luxembourg

© 2020 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

presented'. As part of the adoption of this directive at the national level, the main research question is how to provide support to both Telecommunications Service Providers (TSPs) and the National Regulatory Authority (NRA) in Luxembourg for Article 13a compliance purposes, taking into account the limited resources of the NRA and the telecommunications ecosystem, composed of different size companies. The approach adopted is the establishment of a security risk management framework covering the entire regulatory cycle. In our context, regulatory cycle means three successive steps: the processing of security risk management by the regulated entities (the TSPs), the gathering and analysis of risk-related data by the NRA, and finally, improvements for the next cycle of the whole framework based on lessons learned from the previous steps.

This paper covers these three steps and their current integration. One paper has already been published on the development of models supporting the regulated entities (Mayer et al. 2013) and another on the definition of measurements for the NRA (Le Bray, Mayer, and Aubert 2016). The objective of this paper is to report on our approach as a whole, and to highlight the lessons learned and the improvements expected after the first regulatory cycle. The contribution of the paper is twofold: first, it suggests an innovative approach to designing a security risk management framework covering an entire regulatory cycle, and second, it sets out limitations of and research agenda for its application in the telecommunications sector. It is also worth noting that the risk management reports established by TSPs and the assessment performed by the NRA are confidential. They are thus outside the scope of this paper, which focuses only on the design of the framework and the conclusions drawn following the first regulatory cycle.

The paper is structured as follows. The next section concerns related work. Then, Section 3 presents our security risk management framework as a whole, comprising the risk management approach and tool (also called the regulated entities part), and the NRA data platform. Section 4 reports on lessons learned after the processing of the framework and highlights its current limitations. Section 5 presents the different measures established to address these limitations. Finally, Section 6 concludes and introduces future work.

Related work

The International Organization for Standardization (ISO) defines risk management as the 'coordinated activities to direct and control an organization with regard to risk' (ISO/IEC Guide 73:2009 73:2009 2009). In other words, as explained by the European Network and Information Security Agency (ENISA), risk management is the 'process of identifying, quantifying and managing the risks that an organization faces'. In the field of information security, a risk-based approach is favoured by all stakeholders and has therefore become unavoidable. As a result, many standards and methods for managing security risks exist. Among these references, ISO 31000 introduces a generic risk management cycle applicable to any kind of risk, including security risks, but without offering specific recommendations for information security (ISO 31000:2018 31000:2018 2018). For this purpose, ISO/IEC 27005 (ISO/IEC 27005:2018 27005:2018 2018) was published with specific guidelines for security risk assessment and treatment, (e.g., identification of assets, threats, and vulnerabilities, assessment of consequences and probabilities, risk evaluation, etc.) Furthermore, the National Institute of Standards and Technology (NIST) published the SP 800-39 providing guidance for managing security risks (Joint Task Force Transformation Initiative 2011). It uses a multi-tiered approach (organizational, business process, and information systems) and describes the security risk management cycle, whose parts are addressed in dedicated NIST documents, including the SP 800-30, which provides guidance for conducting risk assessments (Joint Task Force Transformation Initiative 2012). Although these documents provide guidelines for security risk management, they do not provide a specific method to follow. In this sense, different methods have been developed. It would be unrealistic to establish an exhaustive

list here. However, among the most recognized and widely used methods, we can mention: CRAMM (CCTA Risk Analysis and Management Method) (Insight Consulting 2003) created by the Central Computer and Telecommunications Agency (CCTA), a UK government agency, EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) (ANSSI 2010) developed and supported by the French National Cyber Security Agency (ANSSI), IT-Grundschutz (IT Baseline Protection Manual) (Bundesamt für Sicherheit in der Informationstechnik 2005) developed by the German Federal Office for Information Security (BSI), MAGERIT (Ministerio de Hacienda y Administraciones Públicas 2012) supported by the Spanish Ministry for Public Administrations, OCTAVE (Operationally Critical, Threat, Asset and Vulnerability Evaluation) (Alberts and Dorofee 2001) developed by the Software Engineering Institute at Carnegie Mellon University, and CORAS, developed as a visual risk-management framework for security-critical systems, especially IT systems (Fredriksen et al. 2002). The standards and methods mentioned above are intended to be generic and applicable in any organization, regardless of its type, size or nature. Although they can obviously be applied in a telecommunications context, they do not fit our purpose and context of establishing a security risk management framework specifically designed for TSPs and their regulated services, taking into account the low maturity and expertise of most of those in the field.

Methods or guidelines dedicated to security and risk management in the telecommunications sector are much less widely developed. Among those most used by TSPs, the standard ISO/IEC 27011 (ISO/IEC 27011:2016 27011:2016 2016) is an implementation guide for the telecommunications industry proposing guidelines and general principles for initiating, implementing, maintaining and improving information security controls. As it is not a specific risk management standard, it does not propose a dedicated process per se; thereby, some elements can be used for risk management purposes (e.g., threats, security controls, etc.). These elements are sometimes also augmented with elements from ITU X.805 (ITU (International Telecommunication Union)) 2003). ENISA published the Technical Guidelines on Security Measures (Dekker and Karsberg 2014) to assist NRAs in the implementation of Article 13a of EU Directive 2009/140/EC, in particular by listing security measures they should take into account when evaluating the compliance of public communications network and service providers. As a result, TSPs can rely on these guidelines when implementing these measures. Raster (Risk Assessment by Stepwise Refinement) (Vriezekolk, Wieringa, and Etalle 2012) is a risk assessment method for making telecommunications services aware of availability risks. Based on graphs, it focuses only on the availability criteria, and does not claim to be used in the context of security and integrity of networks and services.

A security risk management framework covering the entire regulatory cycle

In order to answer our research question, it is necessary to develop tools supporting the entire regulatory cycle, thus satisfying the requirements of the TSPs and NRA. In the first step of the regulatory cycle, TSPs need to perform a security risk assessment and establish associated risk treatments as part of the security risk management process. The results obtained need to be reported to the NRA before a fixed annual deadline. In the second step, the NRA gathers the risk management reports and analyses their content. Individual reports are then established by the NRA and communicated to each TSP depicting the current status of the TSP, as well as indicators for the sector as a whole. Finally, based on the modifications envisaged by the NRA and the feedback provided by the TSPs, the regulation framework is improved and transmitted to the TSPs who then start a new regulatory cycle by performing the security risk management tasks again. Our research results are thus composed of two main artefacts: a security risk management tool to be used by the TSPs and a data platform used by the NRA to gather and assess the risk management reports from the TSPs and benchmark their security level and the security of the

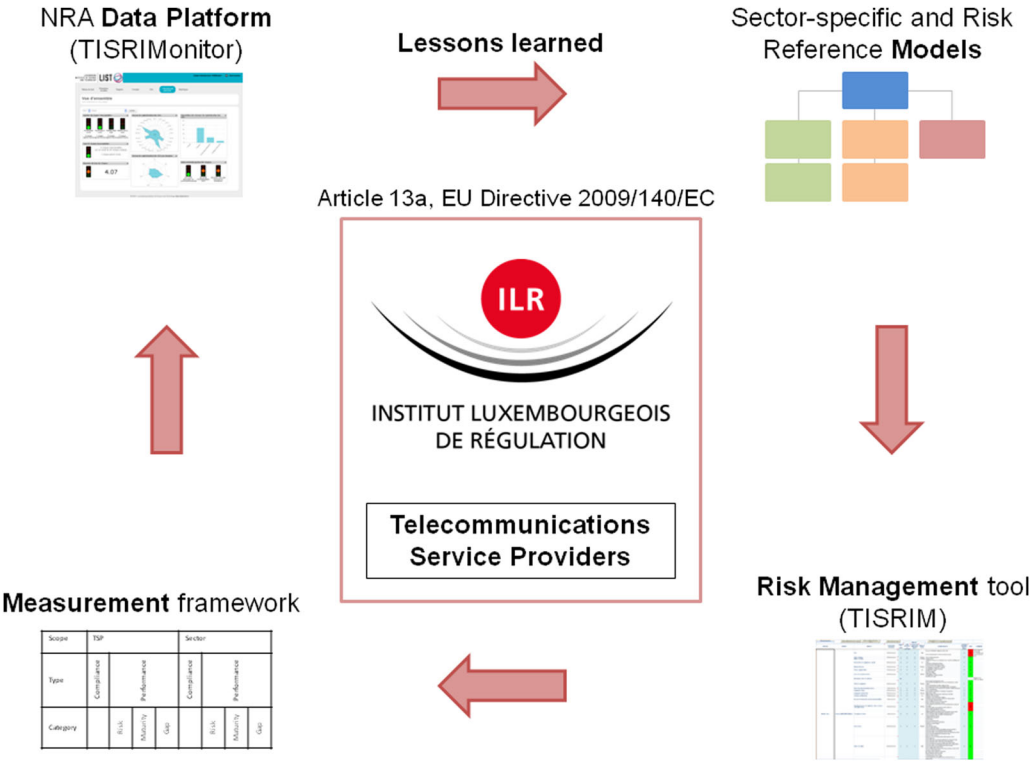


Figure 1. Artefacts designed to support the regulatory cycle.

sector as a whole. Our framework is based on these two software tools, with reference models for the former, and a set of measurements for the latter, as illustrated in Figure 1.

To this end, the project consists of two parts. In the first part (regulated entities), we have developed a model-based approach and a tool to support the adoption of this regulation by Telecommunications Service Providers (TSPs) at the national level, as discussed in Section 3.1. The second part (NRA) involves developing a framework to analyse the data collected by the NRA through this standard approach and is depicted in Section 3.2.

Both regulated entities and NRA parts have been tested in a regulatory cycle involving a risk assessment performed by each TSP followed by the gathering and analysis of data by the NRA.

Development of a sector-specific risk management approach and tool

For the first part of this project, the starting point of our analysis is the different levels of expertise in security risk management of TSPs in Luxembourg. Thus, letting them report to the NRA without strong guidance would have resulted in very different types of reports and quality levels. Here, we wanted to address the question of how to adapt standard security risk management processes and practices to the telecommunications sector and its national specificities.

To answer this question and meet the specific needs of the users (i.e. TSPs in Luxembourg), we decided to define both the methodology and its associated tool in collaboration with them. Therefore, we favoured a user-centred design approach. To this end, and in a spirit of cooperative design, we organized a series of workshops or focus groups (10 sessions took place) with a panel of TSPs (represented by the person expected to perform the required security risk management tasks), selected for their representativeness, as well as their diversity in terms of size, specificities, etc. However, all other TSPs were invited to provide information by email through surveys

before and after the different workshops. During the workshops, we collected not only the specificities of the sector, but also the needs of users and the expectations of both TSPs and the NRA. To facilitate the work of the NRA, it was necessary to adopt a homogeneous, standard and easy-to-compare and analyse risk assessment process. Then, to facilitate the work of the TSPs, we decided to integrate sector-specific models as well as a first selection of risks considered mandatory to be assessed to guarantee the quality of the results and have a fine-tuned tool adapted to TSPs. In the end, this phase of co-design enabled the definition of the methodology (aligned with ISO 31000 (ISO 31000:2018 31000:2018 [2018](#))), the overall design of the tool and the establishment of shared business and architecture models supporting the methodology.

Regarding the definition of these sector-specific models, the first task consisted of defining the different processes of each regulated telecommunications service. Process reference models such as the Business Process Framework ('eTOM') of the TMForum (TMForum 2018) or the Telecommunications Process Classification Framework of the American Productivity & Quality Center (American Productivity & Quality Center (APQC) and IBM [2008](#)) were used as input. Then, the second task was to describe the infrastructure supporting each telecommunications service. The work of The Open Group (The Open Group [2011](#)) and the one of TMForum (TMForum [2011](#)) have been specifically analysed and confronted with the state-of-practice of the national TSPs. Both processes and infrastructure aspects were represented in ArchiMate: an Enterprise Architecture modelling language (The Open Group [2016](#)). Finally, we defined the (most) relevant threats and vulnerabilities for each telecommunications service, based on the reference infrastructures previously defined, and the (most) relevant impacts, based on the business processes previously defined. To do so, we extended ArchiMate with the appropriate concepts from the security risk management domain (Mayer et al. [2019](#)).

All of the different models established, including and linking the business, infrastructure and risk-related elements, were then integrated into a software tool. This was done by adapting TISRIM, a security risk management tool developed in-house, that was initially released in 2009. TISRIM is the tool currently recommended to the TSPs by our national NRA to comply with the regulation. More information about this can be found in (Mayer et al. [2013](#)).

Development of an NRA data platform

This part of the project aims to establish a platform to manage the reports received annually by the NRA, and to be able to efficiently analyse their contents. The purpose was therefore to define a set of measurements depicting the trust the NRA can have in the security of telecommunications companies, as well as in the whole telecommunications sector. The outcome for the NRA is to be able to provide recommendations to the TSPs and facilitate policy-making. The question addressed here was: with available information restricted to risk management reports, how can we depict the trust the NRA can have in the security of telecommunications companies, as well as in the telecommunications sector as a whole?

The first task when defining the measurement framework was to establish a template for the measurement constructs, inspired by the state of the art, and in particular the recommendations suggested by ISO/IEC 27004 (ISO/IEC 27004:2009. 27004:2009 [2009](#)). Then, once the measurement template was established, two types of measurements were defined: compliance measurements, measuring compliance with requirements imposed by legislation, and effectiveness measurements, measuring the effectiveness of risk management and security, and classified in three main categories, namely:

- **Risk Effectiveness:** measuring the security risk management effectiveness;
- **Security Maturity:** measuring the information security maturity, relying on the sophistication levels proposed by ENISA (Dekker and Karsberg [2014](#));

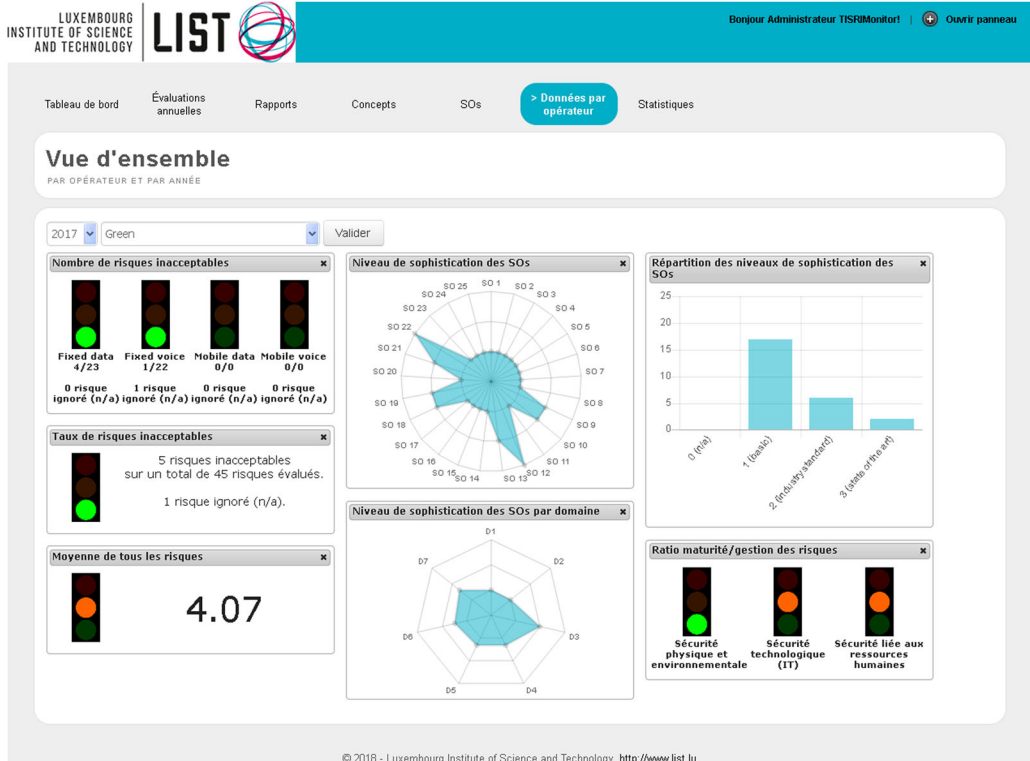


Figure 2. Screenshots of TISRIMonitor, the NRA data platform.

- **Risk-Maturity Gap:** comparing Risk Effectiveness with Security Maturity, in order to assess the consistency of the risk management activities compared to the security maturity stated.

The final set obtained is composed of 10 measurements defined for TSPs and 11 measurements defined for the whole telecommunications sector. More information about this part and a complete list of the measurements can be found in (Le Bray, Mayer, and Aubert 2016).

The set of measurements was then implemented in a tool named TISRIMonitor (presented in Figure 2), which has been made available to the NRA. Such a tool accepts individual risk management reports in the form of XML files and allows the generation of:

- A global risk profile for each TSP based on their individual risk assessment (thanks to the measurements for TSP);
- A risk profile for the whole sector either for all the telecommunications services or for each individual telecommunications service (thanks to the measurements for the telecommunications sector);
- Benchmarks between two or more distinct TSPs, either for a specific service or globally.

Beyond these functionalities related to the analysis of risk profiles, the tool also provides:

- Consolidated lists of the concepts used by the TSPs in their risk assessment, in particular threats, vulnerabilities, supporting assets and controls. These data are particularly relevant for the update and improvement of the knowledge bases included in the TISRIM tool;

- Statistical data of the yearly risk assessment results for the whole sector including a ranking of the highest risks, a summary of the risk levels, a ranking of the most sensitive assets, a list of the most implemented security measures, etc.;
- An automatic generation of individual reports aimed at TSPs. Such reports, which put into perspective individual TSP risk assessment results with consolidated data of the entire sector, enable TSPs to position themselves in relation to the other market players.

Last but not least, the tool provides a first view on the evolution of the risk assessment results over the years both at TSP and sector level. This last feature allows the measurements for a specific TSP or for the whole sector to be put into perspective and the evolution of the impact of the regulation on the global security level of the telecommunications sector to be assessed.

Using this tool, the NRA was able to successfully analyse and get an overview of all the risk management reports for the first regulatory cycle. Still supported by the tool, the NRA generated a digest of the whole sector status for presentation to the TSPs (in particular thanks to statistical data). Following this first cycle, and based on the NRA feedback, we have many opportunities for improvement related to additional relevant measurements (both for the NRA and TSPs), as well as to additional features, especially related to the evolution of the risk assessment results over time.

Emerging challenges after the first regulatory cycle

Regulated entities and NRA parts have been tested through a regulatory cycle involving a risk assessment performed by each TSP from December 2015 to July 2016. Then, data was gathered and analysed by the NRA over several months. The TSPs sent 33 reports, which were then analysed by the NRA. Based on these data, feedback on the results (in the form of a summary presentation for the sector, as well as a personalized positioning report for each individual TSP) was provided in March 2017.

In light of the feedback following this regulatory cycle from both the regulated entities and the NRA, steps have been taken to facilitate and improve the quality of the risk management process performed by the regulated entities on one hand and to improve the governance of the regulation by the NRA on the other. Three limitations have been highlighted and identified as improvement opportunities.

Limitation 1: Lack of support for the security risk management process for the regulated entities

As part of the security risk management tool currently provided to the regulated entities, a set of predefined information is included in the existing framework (infrastructure components, standard threats and vulnerabilities, etc.) This set was considered useful for the initial regulatory cycle; however, it has some limitations in terms of completeness and usability. First, the information systems of TSPs are more and more complex with an increasing number of threats to be managed, and lists of assets/risk components are not able to tackle this complexity alone. Second, as soon as advanced features are envisaged (e.g., linking risk management with incident notification which is the other facet of Article 13a, or even bridging different regulations such as the GDPR (Official Journal of the European Union 2016) also concerning TSPs), it is necessary to further support regulated entities with more specific models.

Limitation 2: No link established between the risk management results of interacting organizations

The main drawback of the security risk management approach currently applied by the TSPs is that risks are managed individually by each organization for its activities, and that no link is established between the risk management results of interacting organizations. The consequence is that it is currently not possible for the NRA to be aware of the actual risks harming the end-user (i.e. to have a customer-centric risk approach), which is in essence what is targeted by the regulation. The aim of the regulation is indeed to try to minimize as much as possible risks taken by the end-users related to a lack of security and integrity of networks and services, and avoid critical situations such as, e.g., the incapacity to make a phone call in case of emergencies (fire, dizzy feeling, etc.) There is thus a strong need for a more customer-centric approach to security risk management and to be able to assess risks at the level of the network of companies providing the telecommunications service to the end-user. For example, a typical case for interacting TSPs providing a fixed-line telephony service is that the backbone is managed by one company, the local loop by another, and a third one sells packages including prepaid call minutes to the end-user. All of these actors have their own set of risks with their own specific consequences. It is thus necessary to connect the different risk assessments in order to identify the risks taken at the different levels of the supply chain, as well as the risks harming the end-users of the service.

Limitation 3: Limited data analytics framework in place (only) for the NRA

Current implemented measurements for data analytics are of two types: compliance measurements, measuring the compliance to requirements imposed by legislation, and effectiveness measurements, measuring the effectiveness of implemented security. These measurements, which are intended exclusively for the NRA, make it possible to have statistics for each individually regulated entity and then for the sector (taking into account the statistics of all regulated entities). However, the fact remains that these measurements are limited and could be improved in order to enable decision-making by the NRA (recommendations, carry out an audit, etc.), as well as provide a better governance of the sector through the regulations. In more detail, the measurements currently in place only provide snapshot views; evolution and trend over time are not taken into account at all. Moreover, they propose a biased picture of reality, since each TSP is considered in the same way regardless of its size, its importance within the sector, its market share, etc. The previous limitation is also echoed here, since data taken into account for the establishment of measurements are only data at the individual level of each TSP, there is therefore no holistic view of the situation of the sector as a whole. Last but not least, current measurements are only intended for the NRA. Regulated entities could also benefit from relevant measurements and associated indicators, as stated in the feedback they provided to the NRA, which could also further transform a regulatory constraint into an opportunity for improvement at their level.

A research agenda

To address the limitations identified, we have developed a research agenda made up of the three following parts:

Compliance models and reference architectures supporting TSPs' regulations

The research question addressed here is: what are the relevant models and reference architectures we can establish to standardize and support compliance concerns as much as possible (especially Article 13a) of the TSPs?

In order to tackle the complexity of the telecommunications sector while improving guidance for regulated entities, models and reference architectures should be established and allow multiple applications. To this end, we will proceed in three main steps.

First, based on data collected in previous regulatory cycles, a comprehensive analysis of the relevant elements for integration and/or consolidation will be performed. In other words, elements missing in the predefined information, which would have been added by a significant number of regulated entities, or on the contrary, elements that are little or not used, thus seeming irrelevant, will be identified. The supporting models will then be produced in the form of enterprise architecture models conforming to the integrated conceptual model for Enterprise Architecture Management and Information System Security Risk Management (EAM-ISSRM). Experiments have been done with this kind of model and it is considered usable and useful for performing security risk management [6].

Second, these consolidated and completed models will then be extended to support other types of compliance concerns. In particular, a first extension will consist of establishing a strong link between risk management and incident notification, both of which are part of Article 13a of the EU Directive 2009/140/EC [1]. Indeed, these activities, although independent may have repercussions on each other: an identified risk can potentially lead to an incident, and conversely a proven incident may suggest a previously unidentified risk.

Third, multi-regulation models will be developed. In particular, we plan to develop an integrated model for the joint assessment of compliance to the 'Technical Guidelines on Security Measures' [9] and the GDPR [4].

Customer-centric and systemic risk assessment

Based on a state-of-the-art we recently performed (Naudet, Mayer, and Feltus 2016), methods traditionally used by organizations to perform security risk management lack the capability to analyse risks at a systemic level for a whole ecosystem. The main drawback of traditional approaches is that risk management methods are designed to be used at the level of the different organizations individually, and not for a network of interconnected organizations (ANSSI 2010; Ministerio de Hacienda y Administraciones Públicas 2012; Insight Consulting 2003; Bundesamt für Sicherheit in der Informationstechnik 2005; Alberts and Dorofee 2001; Fredriksen et al. 2002).

The research question addressed here is: how to perform systemic security risk management, i.e. security risk management performed at the level of a system composed of different interconnected organizations to provide a service to the end-users? To answer this question, we will develop an approach allowing the NRA to connect risk-related results from different TSPs in order to assess actual risks taken by the end-user. The development of this approach will be based on an initial model we established (Naudet, Mayer, and Feltus 2016). This model, called systemic Information System Security Risk Management (sISSRM), is a conceptual model merging Systems theory with the domain of Information System Security Risk Management (ISSRM). From our generic sISSRM model, it will be necessary to determine how the risk models and reference architectures of the different TSPs can be connected from the NRA perspective. To do this, we will first develop a conceptual model, inspired by our initial sISSRM model, but specific to the TSP context, taking care of the data available to the NRA. Then we will define which measurements, methods and algorithms we can apply to perform systemic security risk management.

Data analytics for both the NRA and the regulated entities

The research question addressed here is: how to perform relevant data analytics for both the NRA and the regulated entities? By relevant, we mean data analytics driven by the needs and expectations of the NRA and the regulated entities.

To answer this question, we will proceed in two steps. First, a preliminary study and review of the literature concerning TSP measurements will be carried out. Secondly, a 'Goal, Question, Metric' (GQM) approach is envisaged with the basic idea of deriving metrics from measurement questions and goals (Basili, Caldiera, and Rombach 1994). GQM is based upon the assumption that, for an organization to measure efficiently, it must specify the goals for itself and its projects first, then trace those goals to the questions intended to operationalize them. The application of the GQM approach will result in the definition of the measurement system targeting a particular set of issues.

This complementary approach will therefore be applied on the one hand to the identification of metrics for the NRA and on the other hand to the regulated entities. Concerning the NRA, expectations and needs have already been identified (or at least to a large extent) based on initial joint brainstorming sessions, but still need to be refined. They concern mainly the need (1) to represent the evolution of the results over several years for a given TSP, a given telecommunications service or even for the sector as a whole, (2) to weight TSPs according to their market share in terms of the number of customers potentially impacted, types of customers, etc., and (3) to move from an individual TSP view towards a holistic view based on a systemic approach.

Conversely, the needs and expectations of regulated entities are still to be determined. We plan to organize different working sessions with TSPs to identify their needs, determine with them how they could be translated into measurements and finally present a consolidated set of measurements and validate their relevance and adequacy with their needs.

Conclusions and future work

In this paper, we reported on the design of a security risk management framework to comply with national and European regulations for the security and integrity of networks and services of TSPs. The first part of the framework comprises a risk management approach and tool, which includes sector-specific models to provide support to the TSPs on the methodological aspects. The second part is a platform used by the regulator to gather and analyse the reports established by the TSPs, supported by a set of measurements allowing TSPs to be benchmarked both at the individual level and as a sector as a whole. Both parts were processed through a regulatory cycle consisting of the establishment of risk management reports by the TSPs and their analysis by the NRA. Following this cycle, limitations to our current framework have been highlighted, and a research agenda has been defined to improve the framework on three specific aspects: improvement of the supporting models for the TSPs, the introduction of a customer-centric and systemic risk assessment, and the improvement of data analytics features for both regulated entities and the NRA.

Regarding future work, we first plan to address the research questions that emerged after the regulatory cycle and undertake the associated tasks. Then, we plan to extend our approach to other regulations and concerns, such as Directive 2008/114/EC on the identification and designation of critical European infrastructures and the assessment of the need to improve their protection (Official Journal of the European Union 2008) or the business continuity of TSP services (ISO 22301:2012 22301:2012 2012). In this context, a key challenge will be to develop a multi-regulation risk management tool, allowing TSPs to meet the specific requirements of different regulations by performing one integrated risk assessment and treatment.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

Supported by the National Research Fund (FNR), Luxembourg, and the Luxembourg Regulatory Institute, and financed by the RegTech4ILR project (PUBLIC2-17/IS/11816300).

ORCID

Nicolas Mayer  <http://orcid.org/0000-0002-6021-3660>

References

- Alberts, Christopher J., and Audrey J. Dorofee. 2001. *OCTAVE Method Implementation Guide Version 2.0*. Pittsburgh, Pennsylvania: Carnegie Mellon University—Software Engineering Institute.
- American Productivity & Quality Center (APQC) and IBM. 2008. *Telecommunication Process Classification Framework*.
- ANSSI. 2010. *EBIOS 2010-Expression of Needs and Identification of Security Objectives*. France: <https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/>.
- Basili, Victor R., Gianluigi Caldiera, and H. Dieter Rombach. 1994. "The Goal Question Metric Approach." In *Encyclopedia of Software Engineering*, 532–538. John Wiley & Sons, Inc.
- Bundesamt für Sicherheit in der Informationstechnik. 2005. *BSI Standard 100-3: Risk Analysis Based on IT-Grundschutz*.
- Dekker, Marnix, and Christoffer Karsberg. 2014. *Technical Guideline on Security Measures—Technical Guidance on the Security Measures in Article 13a*. Athens, Greece: ENISA (The European Network and Information Security Agency).
- Fredriksen, Rune, Monica Kristiansen, Bjørn Axel Gran, Ketil Stølen, Tom Arthur Oppervud, and Theodosios Dimitrakos. 2002. "The CORAS Framework for a Model-Based Risk Management Process." In *Proceedings of the 21st International Conference on Computer Safety, Reliability and Security (SAFECOMP '02)*, 94–105. Springer-Verlag.
- Insight Consulting. 2003. *CRAMM (CTTA Risk Analysis and Management Method) User Guide Version 5.0*. United Kingdom: SIEMENS.
- ISO 22301:2012. 2012. *Societal Security—Business Continuity Management Systems—Requirements*. Geneva: International Organization for Standardization.
- ISO 31000:2018. 2018. *Risk Management—Guidelines*. Geneva: International Organization for Standardization.
- ISO/IEC 27004:2009. 2009. *Information Technology—Security Techniques—Measurement*. Geneva: International Organization for Standardization.
- ISO/IEC 27005:2018. 2018. *Information Technology—Security Techniques—Information Security Risk Management*. Geneva: International Organization for Standardization.
- ISO/IEC 27011:2016. 2016. *Information Technology—Security Techniques—Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Telecommunications Organizations*. Geneva: International Organization for Standardization.
- ISO/IEC Guide 73:2009. 2009. *Risk Management—Vocabulary*. Geneva: International Organization for Standardization.
- ITU (International Telecommunication Union). 2003. *ITU-T X.805: Security Architecture for Systems Providing End-to-End Communications*. Geneva: International Telecommunication Union.
- Joint Task Force Transformation Initiative. 2011. *SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View*. Gaithersburg, MD, United States: National Institute of Standards & Technology.
- Joint Task Force Transformation Initiative. 2012. *SP 800-30 Rev. 1. Guide for Conducting Risk Assessments*. Gaithersburg, MD, United States: National Institute of Standards & Technology.
- Le Bray, Yves, Nicolas Mayer, and Jocelyn Aubert. 2016. "Defining Measurements for Analyzing Information Security Risk Reports in the Telecommunications Sector." In *Proceedings of the 31th Annual ACM Symposium on Applied Computing*, ACM. doi:[10.1145/2851613.2851847](https://doi.org/10.1145/2851613.2851847).
- Mayer, Nicolas, Jocelyn Aubert, Hervé Cholez, and Eric Grandry. 2013. "Sector-Based Improvement of the Information Security Risk Management Process in the Context of Telecommunications Regulation." In *Systems, Software and Services Process Improvement*, edited by Fergal McCaffery, Rory V. O'Connor, and Richard Messnarz, 13–24. Communications in Computer and Information Science 364. Berlin Heidelberg: Springer. http://link.springer.com.proxy.bnl.lu/chapter/10.1007/978-3-642-39179-8_2.

- Mayer, Nicolas, Jocelyn Aubert, Eric Grandry, Christophe Feltus, Elio Goettelmann, and Roel Wieringa. 2019. "An Integrated Conceptual Model for Information System Security Risk Management Supported by Enterprise Architecture Management." *Software & Systems Modeling* 18 (3): 2285–2228. doi:10.1007/s10270-018-0661-x.
- Ministerio de Hacienda y Administraciones Públicas. 2012. *MAGERIT—versión 3.0—Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información—Libro II: Catálogo de Elementos*. http://administracionelectronica.gob.es/recursos/pae_000021965.pdf.
- Naudet, Y., N. Mayer, and C. Feltus. 2016. "Towards a Systemic Approach for Information Security Risk Management." In 2016 11th International Conference on Availability, Reliability and Security (ARES), 177–186. doi:10.1109/ARES.2016.76.
- Official Journal of the European Union. 2008. *Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection*.
- Official Journal of the European Union. 2009. *Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009*.
- Official Journal of the European Union. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council*.
- Official Journal of the European Union. 2018. *"Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 Establishing the European Electronic Communications Code"*.
- The Open Group. 2011. *TOGAF Version 9.1*. The Netherlands: Van Haren Publishing. <https://www2.opengroup.org/ogsys/catalog/g116>.
- The Open Group. 2016. *Archimate 3.0 Specification*. The Netherlands: Van Haren Publishing.
- TMForum. 2011. *TMForum Framework—SID Service Overview*. Report GB922-450.
- TMForum. 2018. "TM Forum—ETOM Business Process Framework". Accessed April 11 2018. <https://www.tmforum.org/business-process-framework/>.
- Vriezekolk, E., Roelf J. Wieringa, and Sandro Etalle. 2012. "Design and Initial Validation of the Raster Method for Telecom Service Availability Risk Assessment." Proceedings of the 9th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2012), April. <https://research.utwente.nl/en/publications/design-and-initial-validation-of-the-raster-method-for-telecom-se>.