ISSN: 2181-3906 2023

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 2 / ISSUE 12 / UIF:8.2 / MODERNSCIENCE.UZ

A RISK MANAGEMENT FRAMEWORK FOR SECURITY AND INTEGRITY OF NETWORKS AND SERVICES

Turobova Gulnoza Orif qizi
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, assistant teacher of the Faculty of Cyber Security, Information Security
Mehmonxo'jayev Azizbek
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, 4th year student of the Faculty of Cyber Security, Information Security
Kamolitdinov Ulug'bek Jamolitdin ugli
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, 4th year student of the Faculty of Cyber Security, Information Security
Sahaddinov Muzaffar
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, 4th year student of the Faculty of Cyber Security, Information Security

https://doi.org/10.5281/zenodo.10394811

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.*

Keywords: *Information security, telecommunications, regulatory framework, regtech.*

СИСТЕМА УПРАВЛЕНИЯ РИСКАМИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ЦЕЛОСТНОСТИ СЕТЕЙ И УСЛУГ.

Аннотация. *Совершенно очевидно, что в таких сложных секторах, как телекоммуникации, считать инфраструктуру полностью безопасной, хотя и желательно, но нереалистично. Действующее европейское регулирование сетей связи общего пользования учитывает это предположение и в настоящее время требует, чтобы поставщики телекоммуникационных услуг (TSP) принимали соответствующие технические и организационные меры для управления рисками, связанными с*

безопасностью сетей и услуг. В этом контексте управление рисками стало одновременно ключевым аспектом обеспечения безопасности и основным вектором доверия, включенным, в частности, в нормативные акты. В этом контексте наш документ касается создания системы управления рисками национальной безопасности для соответствия национальным и европейским нормам для TSP. Эта структура состоит из двух частей: инструмента управления рисками безопасности, который будет использоваться TSP, и инструмента анализа, который будет использоваться регулирующим органом для сбора и оценки отчетов по управлению рисками от TSP. Последний специально используется для оценки уровня безопасности TSP и безопасности сектора в целом. В настоящем документе сообщается о разработке этой структуры и проблемах, возникающих после завершения всего цикла регулирования.

Ключевые слова: *Информационная безопасность, телекоммуникации, нормативная база, регтех.*

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 Citation 2009), updated in December 2018 as part of the European Electronic Communications Code (Official Journal of the European Union Citation 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 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. Citation2013) and another on the definition of measurements for the NRA (Le Bray, Mayer, and Aubert Citation2016). 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 Citation2009). 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 Citation2018).

For this purpose, ISO/IEC 27005 (ISO/IEC 27005:2018 27005:2018 Citation2018) 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 Citation2011). 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 Citation2012). 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 Citation2003) created by the Central Computer and Telecommunications Agency (CCTA), a UK government agency, EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) (ANSSI Citation2010) developed and supported by the French National Cyber Security Agency (ANSSI), IT-Grundschutz (IT Baseline Protection Manual) (Bundesamt für Sicherheit in der Informationstechnik Citation2005)

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 Citation2001) 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. Citation2002).

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 Citation2016) 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)) Citation2003).

ENISA published the Technical Guidelines on Security Measures (Dekker and Karsberg Citation2014) 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 Citation2012) 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

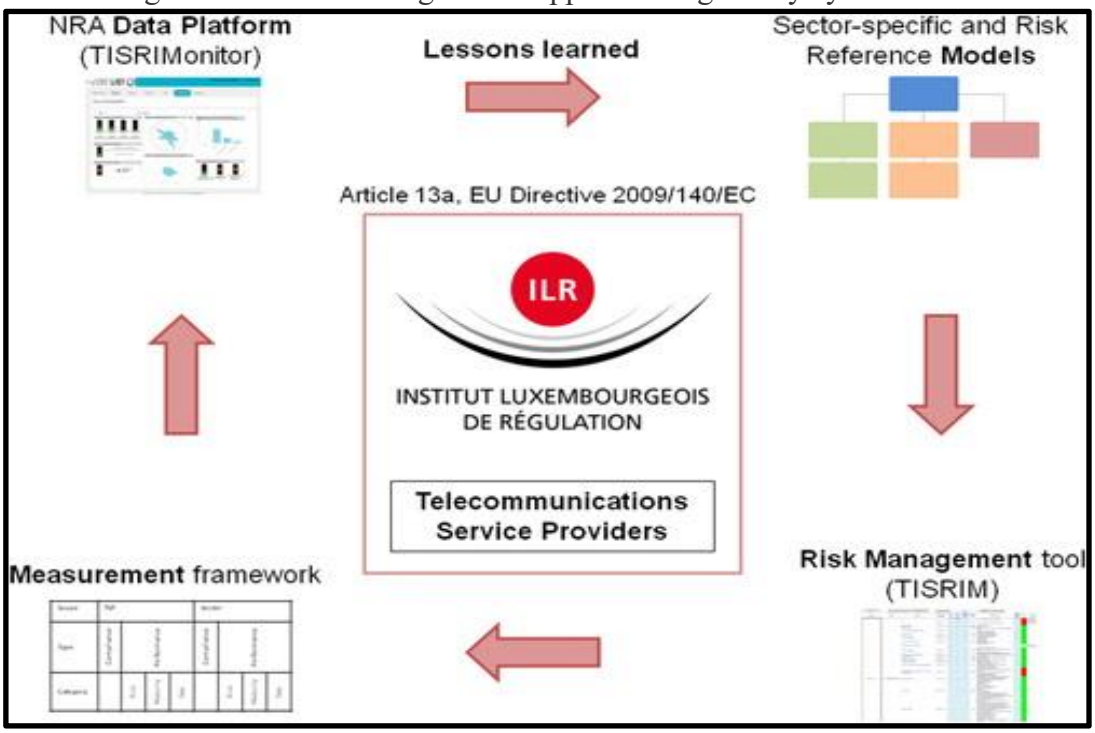
In order to answer our research question, it is necessary to develop tools supporting the entire regulatory cycle, thus satisfying the requirements of the TSPs and NRA. In the first step of the regulatory cycle, TSPs need to perform a security risk assessment and establish associated risk treatments 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.

ISSN: 2181-3906 2023

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 2 / ISSUE 12 / UIF:8.2 / MODERNSCIENCE.UZ

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 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.

Figure 1. Artefacts designed to support the regulatory cycle



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 Citation2018)), 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 Citation2008) 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 Citation2011) and the one of TMForum (TMForum Citation2011) 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 Citation2016). 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. Citation2019).

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. Citation2013).

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?

ISSN: 2181-3906 2023

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 2 / ISSUE 12 / UIF:8.2 / MODERNSCIENCE.UZ

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 Citation2009). 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;

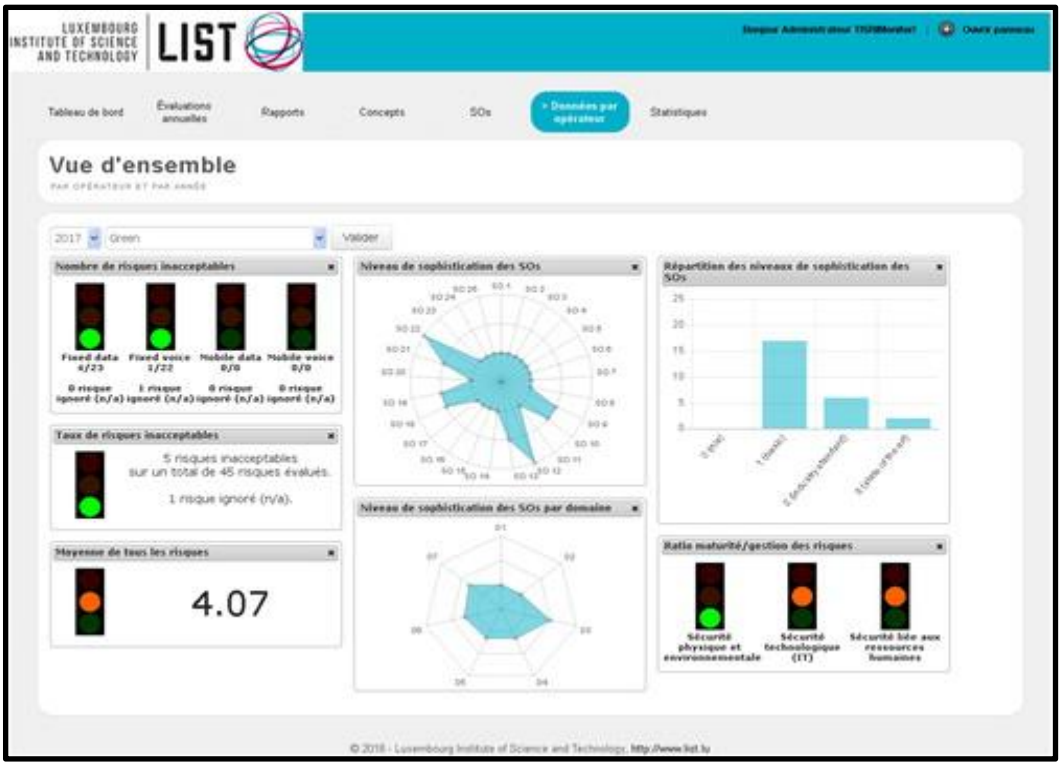
Security Maturity: measuring the information security maturity, relying on the sophistication levels proposed by ENISA (Dekker and Karsberg Citation2014);

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 Citation2016).

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:

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



- 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 Citation 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.

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) or the business continuity of TSP services (ISO 22301:2012). 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.

REFERENCES

1. Alberts, Christopher J., and Audrey J. Dorofee. 2001. *OCTAVE Method Implementation Guide Version 2.0*. Pittsburgh, Pennsylvania: Carnegie Mellon University—Software Engineering Institute. [Crossref], [Google Scholar]
2. American Productivity & Quality Center (APQC) and IBM. 2008. Telecommunication Process Classification Framework. [Google Scholar]
3. 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/. [Google Scholar]
4. 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. [Google Scholar]
5. Bundesamt für Sicherheit in der Informationstechnik. 2005. BSI Standard 100-3: Risk Analysis Based on IT-Grundschutz. [Google Scholar]

ISSN:
2181-3906
2023

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 2 / ISSUE 12 / UIF:8.2 / MODERNSCIENCE.UZ