Systemic Security Risks in the Telecommunications Sector: An Approach for Security and Integrity of Networks and Services

Nicolas Mayer and Jean-Sébastien Sottet
Luxembourg Institute of Science and Technology, 5, Avenue des Hauts-Fourneaux, L-4362 Esch-sur-Alzette, Luxembourg

Keywords: Information Security, Systemic Risk, Telecommunications, Regulatory Framework, Regtech.

Abstract: A strong emphasis is placed today on the security of Information Systems (IS) and on the management of information security risks. This tendency can be seen in numerous emerging regulations imposing a risk-based approach for IS security on entire economic sectors. However, a major drawback of the methods currently used is that risks are assessed individually by each organization for its own activities, and that no link is established between the risk management results of interacting organizations. In this paper, we propose an approach to deal with systemic risks, i.e. risks propagated from one organization to another due to dependencies between them. This approach is an extension of an existing framework used from 2015 by a European national regulator in the telecommunications sector.

1 INTRODUCTION

In a context of increasing cyberattacks, it is essential to guarantee the resilience of essential services comprising water, energy, health, transport or telecommunications. All of us heard about these massive cyberattacks targeting essential services such as the one in Ukraine in 2015 on the power grid or the WannaCry ransomware having huge consequences especially in the healthcare sector. Therefore, there is nowadays a strong emphasis on the security of information systems and the management of cybersecurity risks. As a consequence, more and more regulations requiring a risk-based approach for information system security are emerging. The Directive on security of network and information systems (the NIS Directive), targeting operators of essential services and digital service providers, or the General Data Protection Regulation (GDPR) are concrete examples of this evolution.

In the telecommunications sector, Article 13a of the EU Directive 2009/140/EC (Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009, 2009), updated in December 2018 as part of the European Electronic Communications Code (Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, 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 research question we already addressed was: how to provide support for both Telecommunications Service Providers (TSPs) and the National Regulatory Authority (NRA) for Article 13a compliance purpose? The major assumptions needed to be taken into account in this context were the limited resources of the NRA and the telecommunications ecosystem, composed of different size companies. The approach adopted, and overviewed in Section 2, was the establishment of a model-based security risk management framework covering the entire regulation cycle. This framework is in production since 2015 and considered by the NRA as the standard approach to comply with the national regulation.

However, a major drawback of the framework currently in place is that risks are assessed individually by each organization for its own activities, and that no link is established between the risk management results of interacting organizations. It is worth to note that the telecommunications services are generally composed of sub-services performed by different service

Mayer, N. and Sottet, J.
Systemic Security Risks in the Telecommunications Sector: An Approach for Security and Integrity of Networks and Services.
DOI: 10.5220/0009352200720079
In *Proceedings of the 5th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS 2020)*, pages 72-79
ISBN: 978-989-758-427-5

operators. It is thus necessary, in order to catch the different risks at the sectoral level, to perform risk management for the whole supply chain. The current situation is thus not sustainable because it is 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 by essence what is targeted by the regulation. The research question addressed in this paper is thus: how to reconcile individual security risk management established by TSPs in order to identify and analyse systemic risks, coming from dependencies between TSPs?

The paper is structured as follows. Section 2 summarises our background work on which our current work is based on. Then, Section 3 presents the problem statement. Section 4 is about related work. Section 5 depicts our proposal for systemic security risk management consisting in a 3-steps method. Finally, Section 6 concludes about our current work and presents our future work.

2 BACKGROUND

As part of the adoption and enforcement of Article 13a of the EU Directive 2009/140/EC at the national level, we developed a project aiming at adapting and facilitating security risk management in the telecommunications sector. The project is composed of two parts. The first one consists in the development of a model-based approach and a tool to support the adoption of the regulation by TSPs at the national level (Mayer et al., 2013). The second one is the development of a framework to analyse the data collected by the NRA through this standard approach (Le Bray et al., 2016).

2.1 Development of a Sector-specific Risk Management Approach and Tool

The development of a sector-specific risk management approach and tool for the telecommunications sector was based on the initial observation that the TSPs in our country have a very different level of expertise in security risk management. Thus, letting them report to the NRA without a strong guidance would have resulted in very different types of reports, with various granularity and quality levels.

In order to build a harmonised reporting approach and to meet the users' needs (i.e. TSPs at the national level), we decided to define both the methodology and its associated tool in collaboration with the TSPs. Furthermore, we established shared business and architecture models supporting the methodology.

Regarding the definition of these sector-specific models, the first task consisted in defining the different processes composing each regulated telecommunications service. Process reference models such as Business Process Framework ("eTOM") of the TMForum (TMForum, n.d.) or the Telecommunications Process Classification Framework of the American Productivity & Quality Center (American Productivity & Quality Center (APQC) & IBM, 2008) were used as input. Then, the second task was to describe the information system supporting each telecommunications service. In this task, the works of The Open Group and TMForum have been specifically analysed and confronted with the state-of-practice of the national TSPs. Finally, we defined for each telecommunications service the (most) relevant threats and vulnerabilities, based on the reference architecture previously defined, and the (most) relevant impacts, based on the business processes previously defined (Mayer et al., 2013).

We have then integrated all of the different models into a software tool. This task was performed through the adaptation of TISRIM, a risk management tool developed in-house, that has been initially released in 2009. TISRIM is currently the tool recommended to the TSPs by our national NRA to comply with the regulation.

2.2 Development of a NRA Data Platform

After having defined and implemented a method to support the adoption of the regulation by TSPs, there was also a strong need to develop a platform in order 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 NRA's trust in TSPs' security, as well as in the whole telecommunications sector. The outcome for the NRA is to be able to provide recommendations to the TSPs and to facilitate policy-making. The first task when defining the measurement framework was to establish a template for the measurement constructs. It was elaborated according to the state-of-the-art, and particularly inspired by the guidelines proposed in ISO/IEC 27004. Then, once the measurement template was established, two types of measurements were defined: on the one hand, compliance measurements, measuring the compliance with regard to requirements imposed by legislation and, on the

other hand, performance measurements, measuring the effectiveness in terms of information system security. The final set obtained was composed of 10 measurements defined for TSPs and 11 measurements defined for the whole telecommunications sector (Le Bray et al., 2016). Finally, the measurements were implemented in a tool named TISRIMonitor.

2.3 Results Achieved

The whole framework has been used since 2015 and four regulation cycles have been performed. In our context, regulation 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. Examples of improvements are, for instance, update of the models, measurement addition, or improvement of the tools and their features.

The framework is considered today by the NRA as the standard approach to follow. The main benefits of the approach for the NRA are:

- The establishment of a risk profile for each TSP based on their individual risk assessment;
- The establishment of a risk profile for the whole sector;
- The capability to benchmark two or more distinct TSPs;
- The generation of individual reports for regulated entities;
- Evolution of the risk assessments' results over the years both at TSP and sectoral level.

3 PROBLEM STATEMENT

As depicted in the previous section, a framework has been developed and is currently running for compliance of TSPs with the national regulation transposing Article 13a of the EU Directive 2009/140/EC (Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009, 2009). This framework is complete in the sense that the entire regulation cycle is covered, from the establishment by TSPs of a risk management report to the feedback provided by the NRA to the TSPs on an individual basis.

However, a major drawback of this framework is that risks are assessed individually by each organization, without taking into account dependencies between them. 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 by 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.

There is thus a strong need for a more customer-centric approach to security risk management. The aim is 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.

The (business) questions the NRA wants now to be able to answer are:

- BQ1: What are the new/emerging risks coming from propagation of risks due to dependencies between TSPs?
- BQ2: Are the risk-related assumptions done by service consumers, especially likelihood of risks, sound with regard to their actual assessment by service providers?
- BQ3: What are the most critical organizations / services / assets in the ecosystem of the sector?

In order to answer the previous business questions, we need to answer the following research questions:

- RQ1: How to model dependencies between regulated entities at the level of services / at the infrastructure level? (contributing to all BQ)
- RQ2: How to cascade risks of service providers to risks on service consumers? (specifically contributing to BQ1)
- RQ3: How to cascade risk assessments of the service providers to (update of) risk assessments on service consumers, in order to reconcile the data? (specifically contributing to BQ2)
- RQ4: How to value the criticality of organizations / services / assets based on security risks? (specifically contributing to BQ3)

As an assumption, our scope is currently focused only on dependencies between TSPs and thus on telecommunications service supply. We are aware that, in the telecommunications sector, a large set of risks also arises from dependencies with other kind of providers, e.g. energy providers, digital service providers, external staff, etc. However, considering the priority established with the NRA, the other dependencies are set aside for now and part of future work.

BQ3 is also set aside in this paper. Expectations and requirements still need to be further elaborated and an iterative approach based on initial results obtained for BQ1 and BQ2 would help to do so.

4 RELATED WORK

The importance of interdependencies between critical infrastructures, including Cyber Interdependency, has been highlighted for years (Rinaldi et al., 2001) and to manage risks coming from these interdependencies is our current research challenge. Therefore, we surveyed systemic risk management related to information systems and critical infrastructures. Systemic risk management in the financial domain is considered here as out of the scope, because based on a completely different paradigm (purely quantitative, mathematical and financial approaches) and a specific background (finance and economy). Moreover, a preliminary survey of systemic risk management in the banking and finance domain has shown that the research questions established in the previous section are completely overlooked.

At the opposite of the banking and finance domain, where the concept of systemic risk is highly prominent, the literature on systemic risk in IT and critical infrastructure is much less prominent (Bartle & Laperrouza, 2009). We agree with Bartle and Laperrouza when they state that systemic risk is only referenced briefly in the literature and not subject to extended and explicit analysis. It is clear today that the domain of security risk management has been extensively studied in the academic and industrial world (Dubois et al., 2010; ENISA (European Network and Information Security Agency), 2006), but the current methods of risk assessment seem not to be fully equipped to deal with the level of complexity inherent to such systems (Zio, 2007) and thus to address systemic risks.

As part of related work, Zimmerman and Restrepo suggest to understand and quantify the cascading effects of risks among interdependent infrastructure systems (Zimmerman & Restrepo, 2006). The scope of risk management is focused on the energy infrastructure context and concerns the risk of power outage. Cascading effect is measured by comparing the duration of the electric power outage with the duration of the infrastructure outage which is a consequence of the electric power outage.

The introduction of systems thinking to risk management is a promising way to address our challenge especially since the literature on systems thinking is prominent (White, 1995). A concrete application of systems thinking to security risk management has been done by Naudet *et al.* who propose a meta-model integrating systemic aspects in the domain of security risk management (Naudet et al., 2016). An application of the meta-model was done in the context of IT service providers of the financial sector.

Ligaarden *et al.* developed an approach to monitor risk in interconnected systems (Ligaarden et al., 2015). More specifically, they propose a method for the capture and monitoring of impact of service dependencies on the quality of provided services. The method is divided into four steps: documentation of interconnected systems, analysis of the impact of service dependencies on risk to quality of provided services, establishment of indicators, and design and deployment of identified indicators. The first step about documentation of interconnected systems is based on the notion of trust between the actors of the network. The risk-based approach we want to design is complementary with this approach, because it could help to formalise and justify this trust level between actors. The modelling language used is CORAS (Lund et al., 2010). A key difference with our context is that in this approach, the risk assessment is performed by one single entity having enough information to analyse the system of systems as a whole. In our context, this approach is not possible, because the infrastructure of each TSP is confidential and known only by them. Our challenge is focused on how to correlate risk assessments established by different actors.

Very close to our concerns, Bernardini *et al.* have developed a tool for a system approach to risk management in mission critical systems (Bernardini et al., 2013). The paper depicts the conceptual and functional model of the tool and reports on its application in the healthcare sector. However, no information is given on our key research questions such as how to model dependencies or how risks are cascaded.

The Preliminary Interdependency Analysis (PIA) is a tool-supported methodology for analysing interdependencies between critical infrastructure

(Bloomfield et al., 2017). The method proposed starts with a qualitative phase and may be evolved into a quantitative method for assessing the risk due to interdependencies between critical infrastructure. The different entities are modelled by state machines and probability distributions of failure determine the next state of modelled entity during simulation. This approach is relevant for risk cascading but the necessity to have probability distribution for risks to be analysed is a limitation to our concerns.

5 A SYSTEMIC APPROACH TO SECURITY RISK MANAGEMENT

In this section, we will present our approach to manage systemic risks in our context, which is based on an existing risk management framework (see Section 2) built on top of the legislation. First, we will present the method we suggest to perform systemic risk management. Then we will detail the different steps by making first a focus on dependency modelling and second on risk propagation and systemic risk analysis by the regulator.

5.1 Systemic Risk Management Method

According to our background (Section 2) and the challenges we want to address (Section 3), our proposal is a method composed of three sequential steps. The goal of the method is to allow reconciling the risk assessments coming from different TSPs in order to evaluate systemic risks.

Step 1: Dependency modelling. The dependency modelling is performed based on dependency statements established by the TSPs. At the end of this step, a model for the ecosystem at stake is available.

Step 2: Risk propagation and systemic risk analysis. For each risk targeting an asset / function / service used by a service consumer, the resulting risk generated at the level of the service consumer is identified and its level analysed.

Step 3: Systemic risk evaluation. With the help of the dependency model and the associated propagation of risks, the regulator will be able to evaluate systemic risks at two different levels. First, a consolidation at the risk identification level will be possible, i.e. the regulator will verify if the threats generated by the propagation of risks have all been identified and addressed by the related TSPs in their report. This tasks allows answering BQ1. Second, a consolidation at the risk analysis level will be done, i.e. the regulator will verify if the likelihoods associated to the propagated threats are relevant with regard to the risk levels of the original risks of the provider. This task allows answering BQ2. At the opposite of Step 1 and 2, this step is not further detailed later in this section, because dependent on policy-making strategy of the NRA.

5.2 Dependency Modelling

As depicted in Section 2.1, as part of our current framework, we established shared business and architecture models for the sector. In order to build a model of the ecosystem, which is the goal of this task, an improvement and a better formalisation of these models is necessary. To do so, a sectoral reference model was thus established as a specialisation of an enterprise architecture model and written in the ArchiMate language (Lankhorst et al., 2009). We reused and adapted the ArchiMate language to use it as a reference architecture, selecting a specific subset of the language that is relevant for risk management purpose. We especially completed our previous work by specifying the potential dependency links between TSPs at the ecosystem level. Notably, we are now able to depict the contracts between TSPs concerning resources, people, devices or capabilities. We also depict shared resources (e.g., shared antenna) or shared location or infrastructure (e.g., different enterprises sharing the same building). In other words, we define the viewpoint from which the NRA wants to see the dependencies between TSPs.

From the regulated entity point of view, in addition to the current information needed to be reported by the TSPs (i.e., services, architecture, risks, etc.), each TSP is asked about the actual relations they have with the others TSPs: contracts and resource sharing conforming to the sectoral reference model. Then, after the gathering of all TSP's reports by the NRA, we can build the ecosystem model that represents the holistic sectoral view. This ecosystem model contains the individual models of each TSP, as well as a reconciled view highlighting the dependencies between every TSPs (Sottet et al., 2018). It is an aggregation of models and bridges (i.e., dependencies) between TSP's models plus the actual risk-related information (threats, vulnerabilities, impacts, controls). Thus, it contains all the necessary information to be processed during the risk propagation step.

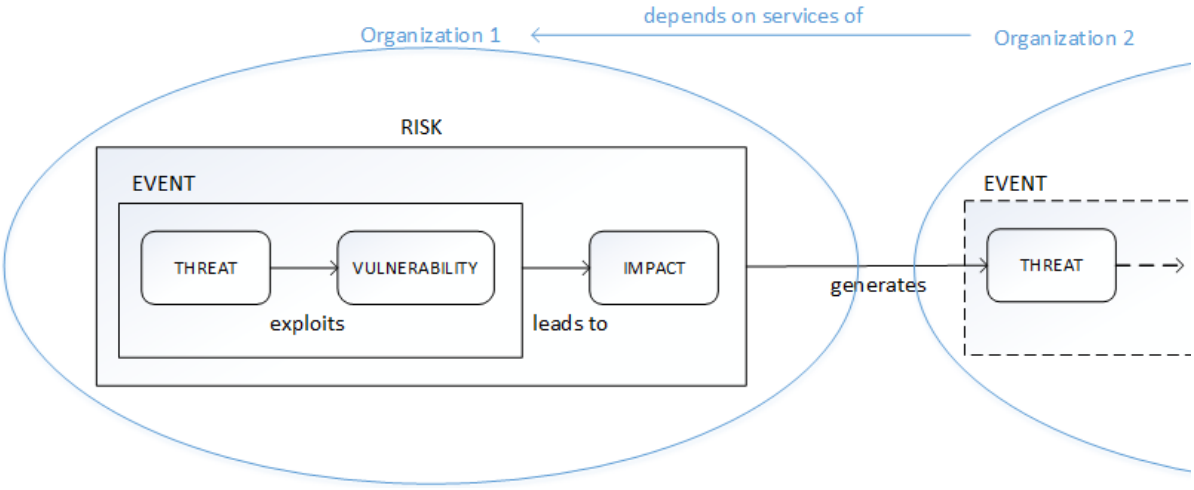

Figure 1: Propagation of a security risk.

5.3 Risk Propagation and Systemic Risk Analysis

Before suggesting a risk propagation approach, it is necessary to have in mind the definition of a security risk and what the components of a security risk are. According to the literature, a security risk can be defined as 'the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization' (ISO/IEC 27000:2018, 2018). A risk is therefore often defined as the composition of a threat exploiting one or more vulnerabilities (also called an event) and leading to a negative impact harming some assets (Dubois et al., 2010).

As a consequence, the propagation of a risk from TSP1 to TSP2 leads to the generation of a new threat in TSP2, which is the source of risk (see Figure 1). This emerging risk needs then to be identified (what are the associated vulnerabilities and impacts) and analysed (what is the likelihood of the event and the magnitude of the impact). As an example, TSP1 identified the risk of cut of a buried communications cable (threat), because this cable is in an area currently under work (vulnerability), leading thus to potential stop of the transmissions (impact). If TSP2 relies on the communications cables of TSP1 to provide its fixed voice service, the previous risk generates the threat of 'loss of telecommunications services' for TSP2. Indeed, at the level of TSP2, the root cause of the risk (e.g., human error, accident, theft of equipment, etc.) is out of its control (its management is under the responsibility of TSP1) and probably unknown. At its level, the risk needing to be managed by TSP2 is a 'loss of service', that can be mitigated through redundancy, taking an insurance, etc.

The generated threat can be determined based on the characteristics of the original risk and the characteristics of the provided service. In the telecommunications sector, the provided services can be 'passive' or 'active'. Passive infrastructure includes all the civil engineering and non-electronic elements of infrastructure, such as physical sites, poles and ducts (and also power supplies). Data and their transmission are out of the scope of the provided service, only the physical infrastructure is provided. Active infrastructure covers all the electronic telecommunication elements of infrastructure like lit fibre, access node switches, and broadband remote access servers. Data and their transmission are in this case in the scope of the provided service. A special kind of passive service is 'co-location'. It is special in the sense that the infrastructure (and thus the set of related risks) is shared (and not fully managed by only one actor) leading thus to a sharing of risks (See Table 1) that are targeting the shared infrastructure (typically an equipment room such as a POP (Point Of Presence) or a PABX (Private Automatic Branch Exchange)).

Then, the generated threat is defined based on two characteristics of the original risk. First, it is necessary to know the security criteria harmed by the cascaded risk. By security criteria harmed we mean which criteria among integrity or availability (the confidentiality being out of the scope of the EU directive we want to address) is harmed by the studied risk. For example, a risk initiated by a threat of 'fire' will potentially harm both the integrity and availability of the supported service. At the opposite, a 'power supply failure' will only harm availability and 'corruption of data' will only harm the integrity criteria. Our proposal is that basically a risk from

TSP1 harming integrity generates the threat 'transmission and communication errors' to TSP2 and a risk from TSP1 harming availability generates the threat 'loss of essential services' to TSP2.

A second characteristic, used only in the case of a risk targeting an active telecommunications service, is if the original risk has a deliberate or an accidental cause. Indeed, according to the risk taxonomy available, a risk with an accidental cause will still lead to a 'transmission and communication error' but a risk with a deliberate cause will lead to a 'corruption of data' (see Table 1). These characteristics of threats are extracted from and documented in standards and will be reused here (ISO/IEC 27005:2018, 2018).

Table 1: Generated threats based on original risk and service.

	Threat leading to loss of Integrity	Threat leading to loss of Availability
Active service	Transmission and communication errors (accidental cause) Corruption of data (deliberate cause)	Loss of essential services
Passive service	Transmission and communication errors	Loss of essential services
Co-location	*Same threat as initial threat*	*Same threat as initial threat*

6 CONCLUSIONS AND FUTURE WORK

In this paper, we suggested an approach to deal with systemic security risks in the telecommunications sector. Systemic security risks are risks that are not only occurring locally, by an actor of the ecosystem, but are cascaded from an actor to another due to dependencies between these actors. The approach proposed is a method composed of three steps: modelling of the ecosystem and the dependencies between the actors, risk propagation and systemic risk analysis and, finally, systemic risk evaluation by the NRA. The main constraint of our work was to propose an approach that is suited to the risk management framework currently in place, which was developed to support TSPs to comply with the legislation.

Regarding future work, we need to experiment and validate the approach. To do this, we plan first to demonstrate the applicability of our approach on an illustrative example currently in progress. This illustrative example will be inspired by real data and focused on the 'fixed voice' service, where the dependencies between telecommunications actors are well known and standardised. In a second step, we will experiment the approach with real data collected by the NRA and extend the scope to the four telecommunications services that are regulated in the legislation. Finally, a software module will be developed to implement our approach. This software module will be an extension of the NRA software tool used to analyse the TSPs reports.

ACKNOWLEDGEMENTS

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

REFERENCES

American Productivity & Quality Center (APQC), & IBM. (2008). *Telecommunication Process Classification Framework*.

Bartle, I., & Laperrouza, M. (Eds.). (2009). Systemic risk in the network industries: is there a governance gap? In *5th ECPR Conference*.

Bernardini, G., Paganelli, F., Manetti, M., Fantechi, A., & Iadanza, E. (2013). SYRMA: A Tool for a System Approach to Risk Management in Mission Critical Systems. *Int. J. Bus. Inf. Syst.*, *13*(1), 21–44. https://doi.org/10.1504/IJBIS.2013.054166

Bloomfield, R. E., Popov, P., Salako, K., Stankovic, V., & Wright, D. (2017). Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment. *Reliability Engineering & System Safety*, *167*, 198–217. https://doi.org/10.1016/j.ress.2017.05.030

Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. (2010). A Systematic Approach to Define the Domain of Information System Security Risk Management. In S. Nurcan, C. Salinesi, C. Souveyet, & J. Ralyté (Eds.), *Intentional Perspectives on Information Systems Engineering* (pp. 289–306). Springer Berlin Heidelberg. http://link.springer.com.proxy.bnl.lu/content/pdf/10.1007%2F978-3-642-12544-7_16?pds=412013102713342426306690521769 99

ENISA (European Network and Information Security Agency). (2006). *Inventory of risk assessment and risk management methods*.

ISO/IEC 27000:2018. (2018). *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. International Organization for Standardization.

ISO/IEC 27005:2018. (2018). *Information technology – Security techniques – Information security risk management*. International Organization for Standardization.

Lankhorst, M. M., Proper, H. A., & Jonkers, H. (2009). The Architecture of the ArchiMate Language. In T. Halpin, J. Krogstie, S. Nurcan, E. Proper, R. Schmidt, P. Soffer, & R. Ukor (Eds.), *Enterprise, Business-Process and Information Systems Modeling* (pp. 367–380). Springer Berlin Heidelberg.

Le Bray, Y., Mayer, N., & Aubert, J. (2016). Defining Measurements for Analyzing Information Security Risk Reports in the Telecommunications Sector. *Proceedings of the 31th Annual ACM Symposium on Applied Computing*.

Ligaarden, O. S., Refsdal, A., & Stølen, K. (2015). Using Indicators to Monitor Security Risk in Systems of Systems: How to Capture and Measure the Impact of Service Dependencies on the Security of Provided Services. *Transportation Systems and Engineering: Concepts, Methodologies, Tools, and Applications*, 1342–1377. https://doi.org/10.4018/978-1-4666-8473-7.ch068

Lund, M. S., Solhaug, B., & Stolen, K. (2010). *Model-Driven Risk Analysis: The CORAS Approach*. Springer-Verlag Berlin and Heidelberg GmbH & Co. K.

Mayer, N., Aubert, J., Cholez, H., & Grandry, E. (2013). Sector-Based Improvement of the Information Security Risk Management Process in the Context of Telecommunications Regulation. In F. McCaffery, R. V. O'Connor, & R. Messnarz (Eds.), *Systems, Software and Services Process Improvement* (pp. 13–24). Springer Berlin Heidelberg. http://link.springer.com.proxy.bnl.lu/chapter/10.1007/978-3-642-39179-8_2

Naudet, Y., Mayer, N., & Feltus, C. (2016). Towards a Systemic Approach for Information Security Risk Management. *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 177–186. https://doi.org/10.1109/ARES.2016.76

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009, Pub. L. No. Directive 2009/140/EC (2009).

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, Pub. L. No. Directive (EU) 2018/1972 (2018).

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11–25. https://doi.org/10.1109/37.969131

Sottet, J., Grandry, E., & Bjekovic, M. (2018). Managing Regulatory System with Megamodelling. *2018 IEEE 20th Conference on Business Informatics (CBI)*, *02*, 1–10. https://doi.org/10.1109/CBI.2018.10041

TMForum. (n.d.). *TM Forum - eTOM Business Process Framework*. Retrieved 11 April 2018, from https://www.tmforum.org/business-process-framework/

White, D. (1995). Application of systems thinking to risk management: a review of the literature. *Management Decision*, *33*(10), 35–45. https://doi.org/10.1108/EUM0000000003918

Zimmerman, R., & Restrepo, C. E. (2006). The next step: quantifying infrastructure interdependencies to improve security. *International Journal of Critical Infrastructures*, *2*(2/3), 215. https://doi.org/10.1504/IJCIS.2006.009439

Zio, E. (2007). From complexity science to reliability efficiency: a new way of looking at complex network systems and critical infrastructures. *International Journal of Critical Infrastructures*, *3*(3/4), 488. https://doi.org/10.1504/IJCIS.2007.014122