

# Defining Measurements for Analyzing Information Security Risk Reports in the Telecommunications Sector

Yves Le Bray, Nicolas Mayer, Jocelyn Aubert

Luxembourg Institute of Science and Technology

5, avenue des Hauts-Fourneaux

L-4362 Esch-sur-Alzette, Luxembourg

{yves.lebray, nicolas.mayer, jocelyn.aubert}@list.lu

## ABSTRACT

It is clearly acknowledged that to consider an Information System (IS) as fully secure, although desirable, this is not achievable. In this context, risk management is becoming both a key aspect and the main trust vector which is particularly included in specific regulations. Our paper is in the context of the telecommunications sector and is about its regulation on security and integrity of networks and services. The objective is to establish a framework to analyse risk-related data collected by the National Regulatory Authority (NRA) through a standard approach they recommend to the Telecommunications Service Providers (TSPs). Our research results are, first, the establishment of the measurement types expected and the definition of a measurement template used as the standard format to define a measurement. Second, we propose a set of measurements to assess the collected, risk-related data, and thus the trust the NRA can have both in a TSP and the entire telecommunications sector. Finally, these measurements are implemented in a tool to be used by the NRA.

## CCS Concepts

• General and reference~Measurement

## Keywords

Information Security, Risk Management, Telecommunications, Regulation, Measurement

## 1. INTRODUCTION

Currently, a strong emphasis is placed on the security of Information Systems (IS) and on the management of security risks. Aside from being an internally adopted steering and governance tool, IS Security Risk Management (ISSRM) is becoming a trust vector included in the standard requirements of organizations. This tendency can be seen in emerging regulations

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

*SAC 2016, April 04-08, 2016, Pisa, Italy*

© 2016 ACM. ISBN 978-1-4503-3739-7/16/04...\$15.00

DOI: <http://dx.doi.org/10.1145/2851613.2851847>

imposing a risk-based approach for IS security on an entire economic sector.

In the telecommunications sector for example, the service providers have to comply with the EU Directive 2009/140/EC [3], whose Article 13a on security and integrity of networks and services constrains Member States to ensure that providers of public communication networks manage the security risks of networks and services. This sectorial approach of ISSRM usually has a shared purpose: to guarantee the trust and sustainability at a sectorial level of provided services, and thus to avoid so-called systemic risks that are threat to the entire sector (e.g., a total breakdown of telecommunications at country level).

Both a methodological approach [1] and a tool [2] have already been developed with our National Regulatory Authority (NRA) to support the adoption of this regulation by companies at the national level. In this context, our objective is to establish a framework to analyse data collected by the NRA through this standard approach. The framework consists in 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 measurement framework shall be in line with state of the art practices of the domain, taking into account the specificity of the regulatory context and the local constraints of the NRA. The outcome for the NRA is to be able to provide recommendations to the Telecommunications Service Providers (TSPs) and to do policy-making.

Section 2 describes in further detail the problem statement and the constraints identified. Section 3 presents the existing background and the state of the art of existing information security measurement standards and approaches. Following that, Section 4 is about the establishment of the different measurement types coming with the measurement template used as the standard format to define a measurement. Section 5 depicts our proposal of a set of measurements adapted to our context and constraints. Section 6 illustrates the implementation of these measurements. Finally, Section 7 concludes the article and proposes potential future work.

## 2. PROBLEM STATEMENT AND APPROACH

In the telecommunications sector, the recent EU Directive 2009/140/EC [3] amends existing directives on framework (2002/21/EC), authorization (2002/20/EC) and access (2002/19/EC) of electronic communications networks and

facilities. This directive should be transposed into a national legislation by all the EU member states. Luxembourg has already begun doing this through publication of the law of 27<sup>th</sup> February 2011 on electronic communications networks and services [4]. The EU Directive introduces Article 13a on 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” [3]. In addition, the article points out that “these measures shall ensure a level of security appropriate to the risk presented”. A supervision of the TSPs is thus required and operated by the NRA of the different countries.

As part of the adoption of this directive at Luxembourg national level, the TSPs are required to send a security risk management report on an annual basis, depicting their perceived security risks related to their so-called level of sophistication for each of the 26 security objectives (SOs) introduced by the Technical Guideline on Security Measures [5] developed by ENISA, the European Network and Information Security Agency. It is recommended (but not mandatory) to follow the approach developed and promoted by the NRA, including a method [1] and a tool [2] compliant with the requirements of the EU Directive and supporting the recommendations established by ENISA.

As a follow-up of the NRA initiatives, there is a strong need to develop a platform in order to manage the reports that are received annually, and to be able to analyse their content. The key challenge of this part of the work is the development of a measurement framework that is the topic of our article. The purpose is 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.

In this context, in collaboration with the NRA, we have identified the following constraints to be taken into account when developing the measurements:

- Resources allocated by the NRA to the data collection and analysis are limited. It is thus necessary to limit the number of measurements and their management complexity.
- Information available to feed the measurements is limited to the risk management reports and the sophistication levels defined for each SO (i.e., what is required by the tool promoted by the NRA, as described in Section 3.1).
- In order to assess the trust the NRA can have individually in each TSP, as well as the trust it can have in the whole sector, two classes of measurements are expected: measurements related to the individual analysis of each TSP and measurements related to the sector.

### **3. BACKGROUND AND STATE OF THE ART**

#### **3.1 TISRIM: a Sector-Specific Tool for Information Security Risk Management in the Context of Telecommunications Regulation**

TISRIM is a software tool dedicated to ISSRM [2]. The tool has been released in 2009 and about 15 companies, from SMEs to European institutions, have already used it with our support. Initially, it has mainly been used to perform ISSRM in the frame

of Information Security Management System (ISMS) establishments and ISO/IEC 27001 certifications [6].

A new version of the tool, specific for TSPs, has been developed in order to adapt the ISSRM process [7] and its related practices to the telecommunications sector and its regulatory constraints [2]. In this sector-specific version, the main evolutions are:

- Scope limited to the four regulated services, namely: Fixed Voice, Fixed Data, Mobile Voice, Mobile Data;
- Methodological adaptations to be compliant with the regulation [3];
- Introduction of standard and regulated business processes of the sector;
- Catalogue of resources specific to the sector;
- Sector-specific threats, vulnerabilities and impact.

An additional feature has been added to the tool, allowing TSPs to perform a self-assessment towards the 26 SOs introduced by the ENISA Technical Guideline on Security Measures [5]. For each of these objectives, TSPs shall indicate a level of sophistication, the related security measures taken towards achieving the SO, the evidence that could be taken into consideration by an auditor to be assured that the objective is reached, and any useful comment. This self-assessment is particularly complementary with the risk assessment, because it helps to justify the good coverage of risks on the one hand and the identified weaknesses on the other hand. After completing both the risk assessment and the self-assessment, TSPs are able to generate a report in XML format for submission to the NRA.

#### **3.2 Overview of existing information security measurement standards and approaches**

ISO/IEC 27004 [8] is a standard published by the International Organization for Standardization (ISO), providing guidance on the development and use of measures (i.e. a variable to which a value is assigned as the result of measurement [8]) and measurement (i.e. the underlying process and its components [8]) for the management of information security. As an international standard, it is the result of a worldwide consensus between experts. The standard creates a basis for each organization to collect, analyse and report data all along the ISMS lifecycle [9]: identification of needs by defining control objectives (PLAN), measurement of the effectiveness of controls (DO), regular review of results from effectiveness measurement (CHECK), and finally improvement whenever necessary (ACT). With ISO/IEC 27004 being primarily defined to meet the requirements of ISO/IEC 27001 [9], the measurement constructs proposed as examples (around 20) in the annex are strongly related to the assessment of an ISMS (e.g., password quality, ISMS training, etc.).

The Special Publication NIST SP 800-55 [10], published by the National Institute of Standards and Technology (NIST) offers an approach to provide assistance in the development, selection and implementation of performance measures. Originally intended for U.S. government agencies, any organisation can benefit from this document to define measurements. This approach allows the implementation of a full cycle of security measures on several levels, linking security performance and business objectives. The method proposed in the document is based on three types of performance measures: implementation measures to measure execution of security policy, effectiveness/efficiency measures to

measure results of security services delivery and impact measures to measure business or mission consequences of security events. This document is based on a layer (level) approach that allows the organization, when it has reached its highest level of maturity, to make the link between performance and security goals set by the company. As in ISO/IEC 27004, a measurement list is proposed (19) in the annex (e.g., vulnerability management, awareness and training, etc.).

Throughout a guide [11] and a practical example of application [12] published in 2004, the *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI), the French Network and Information Security Agency, offers a methodology for building IS security dashboards. These documents present the definition of three different views of dashboard (management, operational, strategic) according to the needs and objectives of an organisation. Thus, a five-step methodology is introduced, each step being illustrated with a descriptive sheet presenting the expected input and output elements. This methodology clearly focuses on the definition of security objectives, used by the results of a risk assessment. Thereafter, the methodology proposes the definition of measurable objectives by setting targets and thresholds expected for the constitution of the final dashboard. The last two phases aim at defining the measurements based on the collected data and at providing a representation via a dedicated measure. Its generic nature allows this method to be adapted to any type of organization, whatever its purpose. The procedural form of sheets can be adopted in the context of a large security project.

The ENISA proposes an overview of existing approaches about measurement frameworks and metrics for resilient networks and services within a technical report [13]. This report represents an attempt to create a single source of information on security measurement methods. It references approaches about the construction of measurements in the information security domain, including some of which are already described in this section (e.g., NIST SP 800-55). The document, which is based on different inputs, offers 30 measures specific to the electronic communications sector, and which are mainly centred on resilience such as the mean time to incident discovery.

As a conclusion, the measurement templates proposed in the different references studied are generally of high interest with regard to our objectives. The different proposed templates have a relatively similar design; defining the different elements required for the construction of a measurement (e.g., definition of the measurable objective, measure construction, decision criteria, etc.). Our measurement template will be inspired by these different proposals, especially the one from ISO/IEC 27004, which has the most detailed model.

However, regarding the set of measurements proposed as examples in the studied references, they are generally not relevant to our context. They are in fact focused on an organization's information security, and more specifically on its ISMS. Coming back to our scope, we are focusing (only) on risk management aspects of information security at the level of an individual organization, but also at the level of the entire national sector. The set of suggested measures are thus out of scope and not adapted to our context.

## 4. ESTABLISHMENT OF THE MEASUREMENT TYPES AND TEMPLATE

### 4.1 Measurement types

Inspired by existing information security measurement standards and approaches, a measurement taxonomy has been defined, as illustrated in Table 1. Considering the context, and especially the fact that measures shall allow the NRA to assess the trust it can have both at individual TSP level and at the whole sector level, it is necessary to address two classes of measurements, namely *TSP* and *Sector*. This is what we call the measurement scope. Beyond the scope distinction, measurements are classified by type. Two types of measurements have been identified based on the state-of-the-art:

- **Compliance:** measuring the compliance with regard to requirements imposed by legislation;
- **Performance:** measuring the effectiveness in terms of IS security.

Finally, Performance measurements are classified in three main categories, namely:

- **Performance-Risk:** measuring the risk management effectiveness;
- **Performance-Maturity:** measuring the information security maturity, relying on the sophistication levels proposed by ENISA;
- **Performance-Gap:** comparing Performance-Risk with Performance-Maturity, in order to assess the consistency of the risk management activities compared to the maturity stated.

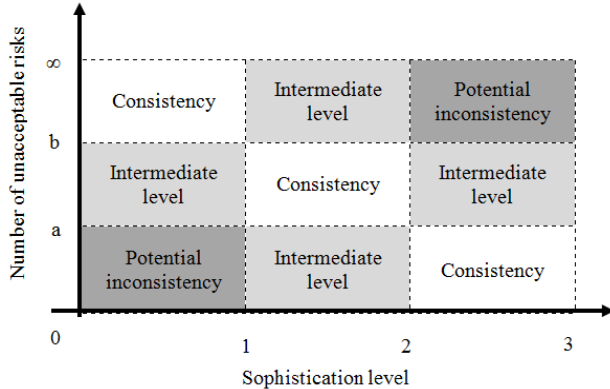
**Table 1: Measurement taxonomy**

Scope	TSP			Sector			
Type	Compliance	Performance		Compliance	Performance		
Category		Risk	Maturity	Gap	Risk	Maturity	Gap

It is worth noting that measurements related to an individual TSP provide not only a view for the TSP itself, but also contribute to the establishment of the sectorial measurements, providing the global view.

If the development of Performance-Risk and Performance-Maturity measurements seem quite trivial (measure and then comparison with a threshold value), the Performance-Gap measurements are more elaborated. Indeed, they are always composed of two measures - the aim being to compare a risk management level with a security maturity level. To do so, a specific analytical model and its interpretation have been defined (see Figure 1). While the sophistication levels from ENISA (see Section 3.1) have been used for the scale related to the security maturity, the number of related risks considered as unacceptable has been selected as the measure for the risk management scale. The threshold values for the number of unacceptable risks (denoted "a" and "b" in Figure 1) shall be set by the NRA based on its expectations and its strategic policy. By doing the comparison between the sophistication level and the number of unacceptable risks, three interpretations are possible: Consistency

of the results, Intermediate level, and Potential inconsistency. Figure 1 depicts these different levels.



**Figure 1: Analytical model & interpretation for Performance-Gap measurements**

The risks identified by a TSP are split into 3 categories, compliant with families of threats established in ISO/IEC 27005 [7]:

- Physical/Environmental risk (e.g., water damage, fire etc.)
- Technological risk (e.g., equipment failure, loss of essential services, or similar)
- Human risk (e.g., breach of staff availability, theft of equipment etc.)

Three different Performance-Gap measurements, corresponding to risk categories, are thus defined. To do so, these risk categories have been mapped with the different SOs defined by ENISA [13] and used in our risk management tool [2] (e.g., a SO dedicated to the security building is mapped with the physical/environmental family of risks). During this mapping, SOs that are generic (i.e. helping to deal with risks from all three categories) are intentionally set aside (e.g., Information security policy, Business continuity management, etc.). As the measurement method used for each Performance-Gap measurement, the number of unacceptable risks of a category is compared to the average sophistication level of related SOs.

## 4.2 Measurement template

Once the measurement types are established, and in order to gather all related information of the measurements, a template for a measurement construct has been established, inspired by the state-of-the art (see Section 3.2), and in particular the template proposed in ISO/IEC 27004. This proposal is in fact the most detailed and well-known by practitioners.


The template we have defined includes four distinct blocks, as illustrated in Table 2, namely: Identification, Measurement construct, Measurement specification and Measurement results. Each block is composed by several elements detailing the components used during a measurement process.

**Identification:** defines the measurement name (e.g. “Unacceptable risk rate”), the measurement scope (*TSP* or *Sector*), the measurement type (*Compliance* or *Performance*), and the measurable objective (e.g. “To know the number of unacceptable risks compared to the total number of risks”).

**Measurement construct:** indicates first the source (object and attribute) providing the measurement data; in our context the

object specifies a tab within the TISRIM tool (e.g. “*Tab Risk Assessment*”) while the attribute specifies our concern in this tab (e.g. “*Column Risk*”). Then, it also defines the measurement method (i.e. a logical sequence of operations used to compute the numerical value of the measure).

**Table 2: Example of measurement**

Field	Description
<i>Identification</i>	
Name / ID	Unacceptable risk rate
Type & target measurement	Compliance: <input type="checkbox"/> Performance: <input type="checkbox"/> Risk: <input checked="" type="checkbox"/> Maturity: <input type="checkbox"/> Gap: <input type="checkbox"/> TSP: <input checked="" type="checkbox"/> Sector: <input type="checkbox"/>
Measurable objective	To know the number of unacceptable risks compared to the total number of risks
<i>Measurement construct</i>	
Objet	Tab “Risk Assessment” (TISRIM)
Attribute	Column “Risk” (TISRIM)
Measurement method	X = total number of risks resulting from the risk assessment Y = number of unacceptable risks identified during the risk assessment R = number of unacceptable risks compared to the total of risks, expressed as a percentage: $R = \frac{Y}{X} * 100$
<i>Measurement specification</i>	
Analytical model & interpretation	Target value: 0% Thresholds value: If $R \geq 20\%$ then “unsatisfactory” If $9\% \leq R \leq 19\%$ then “room for improvement” If $R \leq 8\%$ then “satisfactory”
Decision criteria	If “satisfactory” then do nothing If “room for improvement” then a review is nice to have If “unsatisfactory” then a review is mandatory
<i>Measurement result</i>	
Reporting format	The result is represented in the form of a “traffic light” as follows: <ul style="list-style-type: none"> <li>- Red = unsatisfactory</li> <li>- Orange = room for improvement</li> <li>- Green = satisfactory</li> </ul> 

**Measurement specification:** consists of an analytical model in the form of an algorithm for measure interpretation, with the aim of determining if the measure obtained is satisfactory or not. This

interpretation is framed by a target value (theoretical value for an ideal) indicating a potential security objective to reach. Then, threshold values are used to decide whether the measure is considered as satisfactory or not. Finally, decision criteria indicate if the NRA should take actions, depending on the obtained results. These criteria and actions need obviously to be specified by the NRA.

**Measurement result:** proposes reporting format depicting in verbal and/or visual form (e.g., curve, radar, traffic light, etc.) the result of the measurement.

Compared to the template provided in ISO/IEC 27004, assuming that the risk management reports are sent annually to the regulator, data collection frequency is an element that was voluntarily ignored, because already fixed in the regulation. The same applies to the responsibility part, which is usually included in traditional measurement templates. Unlike the proposed template in the other references, the context is completely different here, without any need to dispatch the measurement responsibilities among the different roles in an organization. The NRA, as an external party, is responsible for data collection and communication.

## 5. PROPOSAL OF A SET OF MEASUREMENTS

Based on the measurement types and the context, we have established two sets of measurements, identified by their names and types in Table 3. The first part is composed of measurements for individual TSPs and the second one is focused on the whole

sector. All measurements are obviously further defined following the measurement template (see Section 4.2), but for the sake of brevity, only a summary table is presented in this paper. It is worth noticing that very few measurements of Compliance type have been identified (one per set). The TISRIM tool suggested by the NRA to the TSPs is in fact already aligned with the regulation, and encompassing features checking the compliance of the required risk management tasks.

Performance-Risk measurements are mainly based on the number of unacceptable risks. For example, the rate of unacceptable risks for each regulated service (e.g., Fixed Voice, Mobile Data, etc.) of each TSP is estimated. At sector level, knowing the most sensitive regulated service is of interest for the NRA. The rate of unacceptable risks at sector level for each regulated service is thus also calculated. Furthermore, a focus is placed on the most critical threats at sector level. Both the top 5 threats causing the highest risks and the most sensitive assets (at the service level and in general) are tracked. These types of measurement allow the NRA to establish relevant recommendations based on the obtained results.

Performance-Maturity measurements are defined at different levels: SO, Domain (the 26 SOs of ENISA are grouped in 7 Domains), and TSP. They allow identifying the security level of a TSP at several granularity levels.

Finally, Performance-Gap measurements, as explained in Section 4, give a trend of the results' consistency provided by a TSP, by comparing risk-related results and sophistication levels.

**Table 3: Set of measurements established for TSPs and for the telecommunications sector**

	Measurement name	Type
TSP	Risk management performed annually for each regulated service	Compliance
	Unacceptable risk rate for each regulated service	Performance-Risk
	Unacceptable risk rate compared to the total number of risks	Performance-Risk
	Average level of all risks	Performance-Risk
	Sophistication level for each Security Objective	Performance-Maturity
	Sophistication level for each Domain	Performance-Maturity
	Average level of sophistication for a TSP	Performance-Maturity
	Consistency in terms of governance in the field of physical and environmental threats	Performance-Gap
	Consistency in terms of governance in the field of technological threats	Performance-Gap
Consistency in terms of governance in the field of human threats	Performance Gap	
Telecommunications sector	Risk management rate performed once a year in time	Compliance
	Unacceptable risk rate for each regulated service	Performance-Risk
	Unacceptable risk rate compared to the total number of risks	Performance-Risk
	Average level of all risks	Performance-Risk
	Top 5 threats causing the highest risks for each regulated service	Performance-Risk
	Top 5 threats causing the highest risks for the sector	Performance-Risk
	Most sensitive assets by regulated service	Performance-Risk
	Most sensitive assets for the sector	Performance-Risk
	Sophistication level for each Security Objective	Performance-Maturity
	Sophistication level for each Domain	Performance-Maturity
	Average level of sophistication for the sector	Performance-Maturity

## 6. MEASUREMENTS IMPLEMENTATION

Once the set of measurements defined, the measurements have been implemented within a web-based tool helping the NRA to manage TSPs reports. Such a tool - illustrated in Figure 2 - accepts individual reports in the form of XML files and allows not

only displaying data from each TSP's risk assessment, providing an overview for each TSP (thanks to the measurements for TSP) and for the whole sector (thanks to the measurements for the electronic communications sector) but also benchmarking two or more distinct TSPs, either for a specific service or globally.



Figure 2: Dashboard of measurements

Last but not least, the tool provides a view on the evolution of the risk assessments' results over the years both at TSP and sector level. This last feature allows putting in perspective the measurements for a specific TSP or for the whole sector and assessing the evolution of the impact of the regulation on the global security level of the telecommunications sector.

## 7. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a set of measurements dedicated to the analysis of the risk management reports of TSPs by the national NRA in Luxembourg. This set of measurements comes with the establishment of the measurement types that are relevant to our context, as well as with a measurement template used as the standard format to define a measurement. The final result consists in 10 measurements defined for TSPs and 11 measurements defined for the telecommunications sector.

Our work has been intentionally driven by information security measurement standards and references (see Section 3.2). We acknowledge that this approach is incomplete and that it is necessary to compare and challenge the results that were obtained with other related research results. However, to the best of our knowledge, no other work has been performed in a so specific context (i.e., a sector-based regulation context, in which measurements deal only with risk management results), thus not allowing a direct comparison of our set of measurements with another one.

Regarding future work, it is now necessary to experiment our results in a real-world context. Before doing so, a final specification of some of the measurements' components we have defined is necessary to be performed by the NRA (especially regarding the analytical models and the decision criteria). Such an experiment will provide us feedback regarding the relevance of the different measurements, which is still uncertain. A key aspect of this relevance will be based on the capability of the NRA to provide recommendations to the TSPs and to do policy-making, based on the measures performed. Another outcome of the project is to use this approach as a pilot project for other national regulators (financial regulator, privacy regulator, etc.). To apply

the same method to define measurements for other NRA is part of our future work.

## 8. ACKNOWLEDGMENTS

Thanks to *Institut Luxembourgeois de Régulation* (ILR), the NRA of Luxembourg.

## 9. REFERENCES

- [1] N. Mayer, J. Aubert, H. Cholez, and E. Grandry, "Sector-Based Improvement of the Information Security Risk Management Process in the Context of Telecommunications Regulation," in *Systems, Software and Services Process Improvement*, F. McCaffery, R. V. O'Connor, and R. Messnarz, Eds. Springer Berlin Heidelberg, 2013, pp. 13–24.
- [2] N. Mayer and J. Aubert, "Sector-Specific Tool for Information Security Risk Management in the Context of Telecommunications Regulation (Tool Demo)," in *Proceedings of the 7th International Conference on Security of Information and Networks*, New York, NY, USA, 2014, pp. 85:85–85:88.
- [3] Official Journal of the European Union, *Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009*. 2009.
- [4] Journal Officiel du Grand-Duché de Luxembourg, *Loi du 27 février 2011 sur les réseaux et les services de communications électroniques*.
- [5] M. Dekker and C. Karsberg, "Technical Guideline on Security Measures - Technical guidance on the security measures in Article 13a," ENISA (The European Network and Information Security Agency), Nov. 2013.
- [6] N. Mayer, "A Cluster Approach to Security Improvement according to ISO/IEC 27001," in *Software Process Improvement, 17th European Conference, EuroSPI 2010*.
- [7] ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management*. Geneva: International Organization for Standardization, 2011.
- [8] ISO/IEC 27004:2009, *Information technology – Security techniques – Measurement*. Geneva: International Organization for Standardization, 2009.
- [9] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*. Geneva: International Organization for Standardization, 2013.
- [10] National Institute of Standards and Technology, "NIST SP 800-55 Revision 1 Measurement Guide for Information Security," Jul. 2008.
- [11] ANSSI, "Élaboration de tableaux de bord SSI - TDBSSI - Section 1: Méthodologie," February 2004.
- [12] ANSSI, "Élaboration de tableaux de bord SSI - TDBSSI - Exemple d'application," February 2004.
- [13] ENISA, "Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report," Discussion draft, Feb. 2011.