# Towards a Systemic Approach for Information Security Risk Management

Yannick Naudet, Nicolas Mayer, Christophe Feltus
IT for Innovative Services (ITIS) department
Luxembourg Institute of Science and Technology
Esch/Alzette, Luxembourg
{yannick.naudet, nicolas.mayer, christophe.feltus}@list.lu

*Abstract*— **Risk management in the field of information security is most often handled individually by enterprises, taking only a limited view on the influential factors coming from their providers, clients or more globally from their environment. This approach becomes less appropriate in the case of networked enterprises, which tend to form ecosystems with complex influence links. A more holistic approach is needed to take these into account, leading to systemic risk management, i.e. risk management on the entire system formed by the networked enterprises, to avoid perturbations of the ecosystem due to local, individual, decision-making. In this paper, we propose a new meta-model for Information System Security Risk Management (ISSRM), comprising systemic elements as defined in the General Systems Theory. We discuss the design of this new model, highlighting in particular how risk management can be related to a problem-solving approach and the important concepts that are instantiated when taking a systemic approach to ISSRM.**

***Keywords-Information security, Risk management, Systemic approach***

## I. INTRODUCTION

Networked enterprises are ecosystems composed of interacting entities which can for most of them be considered as open systems, in permanent relation with their environment. Indeed, aside from communicating with each other's, they are also subjects to regulatory, political or societal rules. Each system of this ecosystem needs to be considered from the system-environment loop perspective, where each system and its environment induce modifications on the other and get also modified by the other in return (mutual influence) (see e.g. [1]). When a change in a system is being investigated, the relations existing between the system and its environment that would be impacted must be identified, and the impact's effect on the environment analysed so as to evaluate the influence feedback that the system would receive. As this feedback might in turn generate new changes in the system having also impacts on the environment, the influence loop needs to be analysed up to a point the last changes in the system do not influence the environment anymore.

Risk management can be seen from a system perspective as a part of a system's decision making process where it is decided how to react to perturbations (internal or induced by the environment) to maintain the system's equilibrium, in a state fulfilling the objective it wants to achieve. Each possible positive feedback loop that causes the system to diverge from its original objective (i.e. identification of a risk) has to be corrected by a negative loop within the control mechanism (i.e. treatment of the risk). Risk management is then related to problem solving, or rather anticipation because problems constituting risks are handled before they occur.

A current drawback of risk management is that it is performed individually by each organisation on its activities, and that no link is established between the risk management results of interacting organisations, particularly in the domain of information security [2]. In this paper, we propose a meta-model to handle Information System Security Risk Management (ISSRM) in a systemic way, i.e. taking a more holistic point of view on services/business ecosystems. To do so, we improve the ISSRM domain model [2], [3], a conceptual model depicting the domain of ISSRM that is part of our previous work, with systemic elements based on former research work on applying the systemic view and the Systems theory to model enterprise interoperability [4]. The regulator's perspective is used as use-case for our approach, regulators being institutions requiring this holistic point of view described above. The resulting model is called *systemic ISSRM* (sISSRM). In this paper, we present this model, the rationale behind it, and a suitable method for systemic risk management. The use of this conceptual model is illustrated in the paper through (basic) instances of the conceptual model. However, it is worth to note that our contribution aims not at introducing a new modelling language, but is focused on defining the conceptual aspects of systemic ISSRM.

Section 2 describes the background of our work through the introduction of the ISSRM domain model. Then, Section 3 summarizes the context and motivation to introduce a systemic ISSRM model. Section 4 is about current state of the art in systemic approaches for risk management and information security. Section 5 is about the integration of the systemic aspects in the ISSRM model, leading to the sISSRM model. Section 6 explains how to use our sISSRM model to deal with systemic risk management at the level of an ecosystem. Section 7 proposes an illustrative example of the approach and, finally, Section 8 is about conclusion and future work.

## II. THE ISSRM DOMAIN MODEL

In our preceding works, the concepts of ISSRM have been represented as a domain model, i.e. a conceptual model depicting the studied domain [3]. The ISSRM domain model was designed from related literature [2]:

risk management standards, security-related standards, security risk management standards and methods, and security requirements engineering frameworks. The ISSRM domain model is composed of 3 groups of concepts: *Asset-related concepts*, *Risk-related concepts*, and *Risk treatment-related concepts*. Each of the concepts of the model has been defined and linked one to the other [2], as illustrated in Fig .2 where ISSRM concepts are represented in light grey.

*Asset-related concepts* describe assets and the criteria which guarantee asset security. An `Asset` is anything that has value to the organisation and is necessary for achieving its objectives. A `Business asset` describes information, processes, capabilities, and skills inherent to the business and core mission of the organisation, having value for it. An `IS asset` is a component of the Information System (IS), supporting business assets like a database where information is stored. In our context, and as described in the ISSRM literature [2], an IS is a composition of hardware, software, network, people and facilities. A `Security criterion` characterises a property or constraint on business assets describing their security needs, usually for confidentiality, integrity and availability. A `Security objective` is the application of a security criterion on a business asset (e.g. the confidentiality of personal information).

*Risk-related concepts* present how the risk itself is defined. A `Risk` is the combination of an event with a negative impact harming the assets. A negative `Impact` describes the potential negative consequence of an event that may harm assets of a system or organisation, when an event causing this impact occurs. As impacts can concern both business and IS assets, we can especially distinguish between Business Impact and IS Impact. An `Event` is the combination of a threat and one or more vulnerabilities. A `Vulnerability` describes a characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw that can be exploited by a threat. A `Threat` characterises a potential attack or incident, which targets one or more IS assets and may lead to the assets being harmed. A threat consists of a threat agent and an attack method. A `Threat agent` is an agent that can potentially cause harm to IS assets. An `Attack method` is a standard means by which a threat agent carries out a threat.

*Risk treatment-related concepts* describe what decisions, requirements and controls should be defined and implemented in order to mitigate possible risks. A `Risk treatment` is an intentional decision to treat identified risks. A `Security requirement` is a desired property of an IS that contributes to a risk treatment. `Controls` (countermeasures or safeguards) are a designed means to improve security, specified by a security requirement, and implemented to comply with it.

## III. CONTEXT AND MOTIVATION FOR A SISSRM MODEL

The ISSRM domain model depicts by design the concepts at stake for performing ISSRM in an organisation. However, to be able to assess and manage the security risks taking into account (only) its own IS and its direct environment is often no more sufficient. For example, in the context of the telecommunication sector, the EU Directive 2009/140/EC [5] introduces Article 13a on security and integrity of networks and services. This article says that Member States shall ensure that providers of public communications networks "take appropriate technical and organisational 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". The outcome of Article 13a from the regulator point of view is that the final customer using the service takes as few risks as possible, and that the continuity of the services is assured as much as possible. The same applies in the financial sector, in which a national law requires that the financial service providers perform a "risk-based approach" in order to identify the risks the financial institutions are taking when using their services.

In view of the preceding contexts, and according to the regulators requirements, we observe that it is no more sufficient to perform risk management at the level of the different companies taken individually. The services at stakes are indeed compositions of sub-services performed by different service providers, and it is thus necessary, in order to catch the different risks at the sector level, to perform risk management for the whole supply chain. For example, to come back to the telecommunication sector, a typical case is that the backbone is managed by a company, the local loop by another, and a third one sells packages including prepaid call minutes. All of these actors have their own set of risks coming with their specific impacts. It is thus necessary to connect the different risk assessments in order to catch the risks really taken at the different levels of the supply chain, as well as the risks harming the end-users of the service. To have a systemic view of the service is a must have, and to perform sISSRM is necessary to reach the regulators objectives.

## IV. STATE OF THE ART

Early in 1995, we can find a scientific literature review from Diana White, which focuses on risk management from a system thinking perspective [6]. She reviews different approaches of risk assessment and highlights the underlying theories, stating finally that most frequently used approaches are reductionist in nature. Highlighting the fact that such approaches fail to consider the interactions between parts of a system, emergent properties and environmental effects, the author highlights one approach taking a more holistic perspective, the failures method, which offers a mean to highlight in a global way failures in a system by comparing formal models of the running system to a reference "perfect" model. In this work, the concept of systemic risk is not yet defined, but it highlights the main issues of traditional approaches to risk management.

Systemic risk has first been taken from a broad, societal or environmental perspective. The concept has emerged in 2003 in the Organisation for Economic Co-operation and Development (OECD), targeting risk to human health and the environment, which has to be considered "in a larger context of social, financial and economic risks and opportunities" [7]. The International Risk Governance Council (IRGC), which is focused on systemic risks that may have impacts on human health and safety, environment, economy and society, describes systemic risk as "embedded in the larger context of societal, financial and economic consequences and is at the intersection between natural events, economic, social and technological developments and policy-driven actions" [8]. In this broad context, systemic risks are defined as risks whose consequences are not limited to a primary effect, but rather trigger chained impacts (at least secondary, and tertiary), because they are embedded in a larger context [9].

Systemic approaches to risk management have been proposed in different sectors, taking more narrow perspectives: finance and economy [10]–[13], transport [14], healthcare [15], social systems [16] and project management [17]. Each sector provides its own understanding and definition of systemic risk, which remain however very close. We can quote the finance system perspective, where it is defined as the "risk of the occurrence of an event that threatens the well-functioning of the system of interest (financial, payments, banking, etc.) sometimes to the point of making its operation impossible." It refers also to the risk or probability of breakdown (losses) in the individual parts of components, identified by co-movements (correlation) among most or all parts [18]. From a social system perspective, it is defined in by White as "the possibility that an event will trigger a loss of confidence in a substantial portion of the system serious enough to have adverse consequences on system performance (…) therefore impacting the integrity of the whole system." [6].

Some generic frameworks taking a generic systems perspective are proposed, like in [19], and in [20] for System of Systems. They provide a view that is a priori applicable to any sector. Systemic Risk is defined in [20] by (a) the set of constituents defining each a specific risk category; (b) the dependencies (i.e. risk propagation links) between those constituents; and by (c) the consideration of external elements that can affect the overall risk at the system level. Stating that no common definition exists for systemic risk, Gandhi et al. summarise it as: "Systemic risk is thought of as a risk that originates from multiple sources, affects multiple agents and propagates quickly among individual parts or components of the network" [20]. Importantly, they specify that systemic risk can be understood as a risk affecting the system globally, "characterised by correlations between most of its parts". The definition is then further generalised as: "Systemic risk is a risk that could be greater than the sum of its individual constituent risks".

The most representative definitions of systemic risk highlight important characteristics. In the finance domain, Martinez-Jaramillo et al. states that systemic risk is defined by two components [12]: (a) an initial random shock which affects one or more (here, financial) institutions and (b) a contagion mechanism which transmits the negative effects across the system. From the broader perspective, Klinke and Renn define the following major characteristics of systemic risks: complexity, uncertainty, ambiguity, and ripple effect [7]. Complexity refers to the difficulty of "matching" the plethora of adverse effects with potentially affected parties and objects, as well as deciphering the casual relationships and identifying the feedback loops. Uncertainty refers to the deficiencies of the evidence that ultimately weaken the cause and effect chain. Ambiguity supposes the presence of various legitimate interpretations of the same data set. Finally, "ripple effects" indicate secondary and tertiary effects (in space and time) and is especially representative of systemic risks.

What can be retained from the different perspectives is that systemic risks appear in networked ecosystems, where the individual elements or entities in this ecosystem can influence each other through their relationships. In such a context of a complex system, an issue appearing in one entity can propagate in cascade to other entities (the ripple effect), in sometimes non-linear and unpredictable ways. Systemic risk management is an interdisciplinary field requiring a new form of risk analysis taking a holistic perspective, "to combine the identification of hazards, risk assessment and risk management" [1]. Finally, such a systemic approach means focusing on the interdependencies and relationships between various risk clusters in an ecosystem, in addition to a traditional causes / consequences analysis [1].

In the information security domain, methods traditionally used by organisations to perform ISSRM [2, 3] are lacking the capability to analyse the risks at a systemic level for a whole ecosystem. The main drawback of traditional ISSRM approaches is that risk management methods are designed to be used at the level of the different organisations taken individually, and not for a network of interconnected organisations. This statement has additionally been highlighted at the international level, especially in the 2nd working draft of ISO/IEC 27005 [20] (in the frame of its update), with a specific focus on networked information security risk management.

## V. INTEGRATION OF THE SYSTEMIC ASPECTS IN THE ISSRM MODEL

The following sections first introduce background theory on systemic modelling. Then, the systemic concepts are introduced in the ISSRM domain model to develop the systemic ISSRM (sISSRM) model.

### *A. Background on systemic modelling*

Systems or systemic theories, as we understand it usually, originate all from the General System Theory (GST) of von Bertalanffy [1] whose underlying idea was first presented in 1937 [24]. Based on observation of living organisms, it is a theory about organised complexity that promotes a holistic approach on the exploration of phenomena and exceeds the limits of

classical theories in tackling complex problems. Systemic thinking is recognised as the main form of analysis allowing systemic modelling. While traditional reductionist approaches focus on the individual parts of a system, systemic thinking focuses on the interactions between parts [25]. In preceding works on Enterprise Interoperability, we have formalized a systemic meta-model, based on a definition adapted from the GST: *A system is a bounded set of inter-connected elements forming a whole that functions for a specific finality in an environment, from which it is dissociable and with which it exchanges through interfaces* [4].

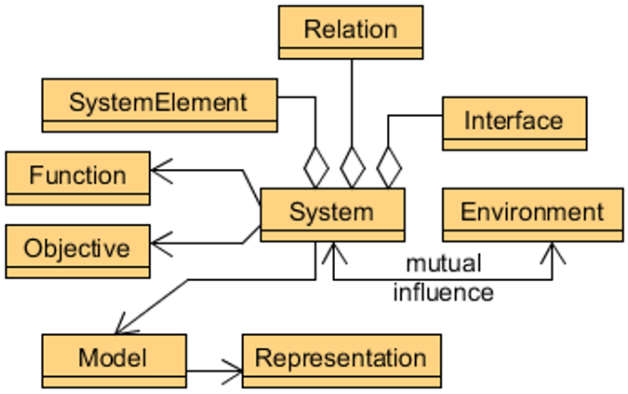


Figure 1. A systemic meta-model

As illustrated in Fig. 1 (based on [20] and extending to further research results), the systemic meta-model we have developed formalises the main concepts characterising a system. It provides a basis to formalise the structure and behaviour of a system, and the relationships between its composing elements. While it is not represented in Fig. 1 for sake of readability, we will use in the remainder of the paper the `sys:` namespace to denote systemic concepts and distinguish them from the other concepts pertaining to the ISSRM domain. A `sys:System` is by definition composed by instances of `sys:SystemElement` (identifiable elements of the system), `sys:Relation` (links between at least two elements or an element and the system) and `sys:Interface` (the gateway through which exchanges between system and environment occur). It is further characterised by: `sys:Objective` (the system's finality); `sys:Function` (set of executable actions to reach the system's objective) and `sys:Environment` (any kind of environment, influencing the system and being influenced by it). This is further completed by `sys:Model` (representing views on the system) and `sys:Representation` (the model syntax).

### *B. sISSRM: the systemic adaptation of the ISSRM model*

Managing risks at a systemic level requires taking a holistic view on the system concerned by the risk management process, together with the ecosystem in which it evolves. The elements to consider are then: the system, its components, its environment (being itself composed of interconnected systems), and the interactions between those elements. Interactions are the key to systemic ISSRM since they are vectors of risk propagation across entities in an ecosystem. Elaborated originally for modelling risks in a single organisation, the ISSRM domain model does not permit to model such propagation elements. Extending it with systemic concepts allows its use at the ecosystem level, or at single organisation's level, taking into account explicitly the mutual influence with their environment.

As a complement to the systemic meta-model presented in the previous section, we introduce the concepts of `sys:SystemComponent` and `sys:SystemicElement` (see Fig. 2). The latter represents from a generic point of view the core elements of a systemic model as just cited. We have respectively for these elements: `sys:System` ⊑ `sys:SystemicElement`, `sys:SystemComponent` ⊑ `sys:SystemicElement`, and `sys:Environment` ⊑ `sys:SystemicElement`. The former represents the components of a system: subsystems or non-system elements (e.g. resources) composing it; the relation links between those components; and the interfaces through which the component interacts or with which the system interacts with its inner component or its environment. According to [6], we have respectively: `sys:SystemElement` ⊑ `sys:SystemComponent`, `sys:Relation` ⊑ `sys:SystemComponent`, and `sys:Interface` ⊑ `sys:SystemComponent`. The original definition of `sys:SystemElement` is extended here to elements that are not systems themselves.

Risk management can be seen easily from a problem solving perspective, as was taken in our research on systemic-grounded interoperability [8]. The risk, as defined in the ISSRM domain model, can be seen as a problem to solve, whose solution is given by the specific treatment: `Risk` ⊑ `sys:Problem`, and `Risk Treatment` ⊑ `sys:Solution`. Then, we have to introduce the notion of `sys:Solution Implementation`, to distinguish between a solution *per se* and its actual implementation. This is formalized by: `implements(Solution Implementation, Solution)`. In ISSRM, the actual implementation of the solution is represented by the `Control` class: `Control` ⊑ `sys:Solution Implementation`. It implements a specific formalisation of the solution that is constituted of the security requirements derived from the chosen risk treatment. The problem-solving perspective is implicitly taken in risk management. Linking specific concepts of ISSRM to generic problem-solving concepts allows in particular to model the modifications on assets (i.e. system components) induced by the implementation of any risk mitigation (control) solution. Although we did not investigate in this direction so far, such modifications potentially impact connected assets and contribute to risk propagation.

As said in Section 3, the principal elements concerned by risk management are the assets. When links exist between assets of different organisations, a door is open to risk propagation. This can be modelled naturally with systemic concepts: *system elements*, *environment* and *influence* relations. As part of the system, assets are system components. This is formalised by: `Asset` ⊑ `sys:SystemComponent`. We then distinguish between IS and business kind, renaming the corresponding asset

classes of ISSRM into respectively `IS Component` and `Business Component`. As an asset is a system component, it can influence or be influenced by the system's environment. The `influences` link between `sys:Environment` and `sys:System` propagates to `sys:SystemComponent` through the composition relation existing between these two classes. Practically, this allows to formally model links between assets, inside and outside an organisation. Technically, `influence` links are materialised by connections between interfaces (`sys:Interface`). However, in ISSRM, only interfaces of IS components should be represented. The relation `hasInterface (IS Component, sys:Interface)` can be further specialised into more precise relations to express the semantics of the link (e.g. "calls" link; see Section VII).

Harm caused by impact on asset (`harms(Impact, Asset)`) can be propagated to the environment. In the other way around, it might happen that the environment influences the harm on an asset, however this is taken into account when evaluating a risk's impact. If changes occur in the environmental factors affecting an impact, they might however lead to re-evaluate the impact level. Propagation of impacts occurring in a system, to its environment, can be modelled by the relation `generates(Impact(`*S1*`), Threat(`*S2*`))`, *S1* ≠ *S2*, which is valid only if the system *S1* where the impact occurs is different from the system *S2* where a new threat is generated. The resulting sISSRM model is presented in Fig. 2 where main systemic concepts are linked to concepts of the ISSRM domain model, to form the systemic version of the latter. In this figure, light grey concepts belong to the original ISSRM model, while dark grey are new ones, necessary to extend ISSRM with a systemic approach. Concepts labelled with the *sys:* namespace belong to the systemic meta-model (see Fig. 1). Links in bold line represent essential relations for implementing systemic risk management.

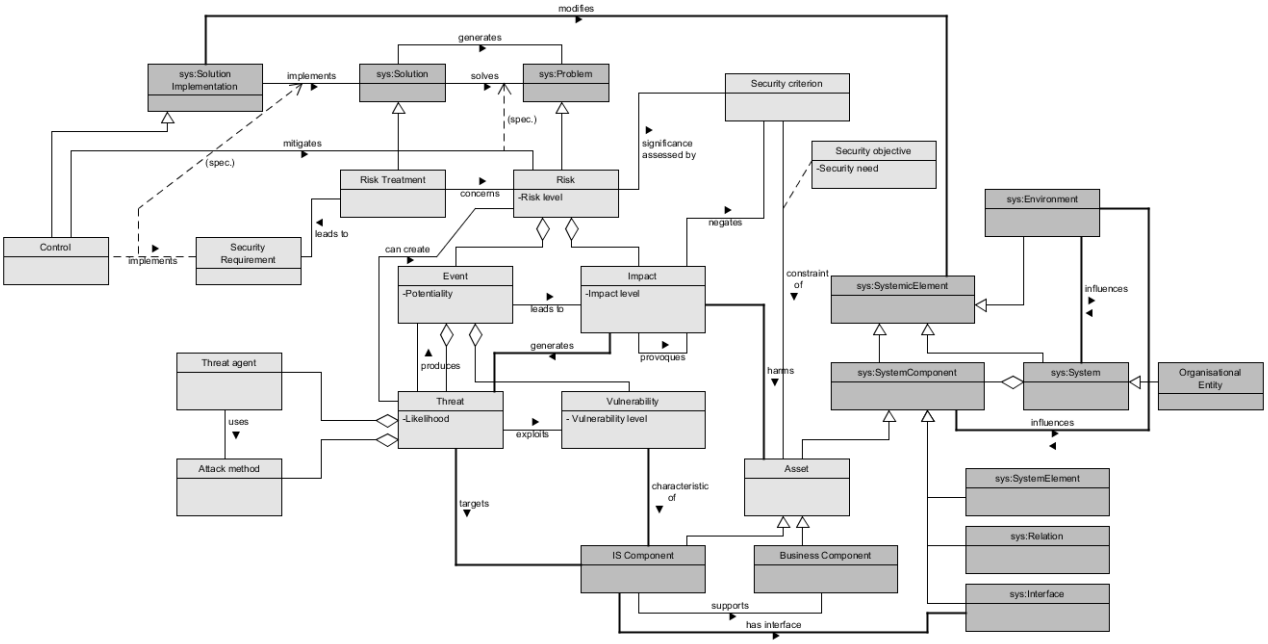


Figure 2. The sISSRM meta-model

## VI. sISSRM TO MODEL SYSTEMIC RISKS

Identifying systemic risks starts by knowing the ecosystem's structure, i.e. the relationships that exist between the entities composing it. The sISSRM meta-model allows formalising the relationships between entities through the *influences* link, which represents at a very abstract level a relationship between a system or a system component and its environment. In an ecosystem, each organisational entity (each system) having an asset in contact with other elements of the ecosystem (i.e. the entity's environment), can influence or be influenced by the element with which it is in contact. This is true whatever the kind of link. Systemic risk management is about identifying those influence links, between assets belonging to different entities in a same ecosystem, which can propagate impacts of risks for one entity to another entity.

Relationships between different entities are materialised by influence links at two levels: (1) between their respective business assets; and (2) physically implemented by corresponding links between interfaces linked to IS assets. Influence links are formalised as specialisations of the *influences* relationship (see relationship between `sys:Environment` and `sys:System` in Fig. 2), with directed links bearing a more precise semantics. This can be, e.g., "uses", "refers to", or "relies on" at the business level, or "calls" at the IS level. Finally, at the risk description level, influence links are materialised by chains of <*Impact*-*Threat*> couples, where an impact in one entity generates a threat for another entity with which it is linked. This can formally

be modelled by the relation `generates(Impact, Threat)`, where the impact belongs to an entity e1 and the threat belongs to an entity e2<>e1. As said before in Section 2, impacts can be related to IS assets and to business assets, leading respectively to IS impacts (the impact at the level of the IS, i.e. related to hardware, software, network, people or facilities) or business impacts (the impact at the business level, i.e. related to business functions or information). For sake of readability, the corresponding concepts have been omitted in the meta-model presented in Figure 2. However, this will be further illustrated in the example described in next section.

## VII. ILLUSTRATIVE EXAMPLE OF USE OF THE sISSRM MODEL

To illustrate the use of the sISSRM model, we focus on a national regulation from our financial National Regulatory Authority (NRA) entitled "*Circulaire CSSF 12/544*" [26]. It requires that each financial service provider uses a "risk-based approach" in order to identify the risks the financial institutions are taking when using their services. The risk management reports are sent annually to the NRA. The analysis of these reports performed by the NRA in 2014 has shown that the providers were generally able to assess the consequences of risks on their own business, but they were unable to propagate them on their clients. However, from the regulator point of view, considering risks taken individually by each organisation is no more sufficient, and it is necessary to have a systemic view of the services provided, highlighting in particular the dependencies between services provided by different organisations. This view should provide a detailed view of the ecosystem, comprising enough information to be able to understand and manage risk propagation.

We assume that each entity belonging to the ecosystem has provided a detailed formalisation of its risk analysis to the regulator. Identifying risks locally is not the focus of systemic risk management. However, the way local risks are managed plays a central role because it influences risk propagation across the ecosystem. For each entity, the regulator has access especially to the following information: assets, threats to which the assets are susceptible to, coming with associated vulnerabilities, and impacts linked to threats. Vulnerabilities, impacts and the number of assets targeted will be used in particular to assess the importance of threats.

A model-based approach [27] is used to perform and to represent the different steps of the risk management process [21]. The models designed at each step are obtained based on the regulator own knowledge (i.e. its understanding of the ecosystem) and the risk management reports gathered from all the entities. To illustrate the ecosystem and the related systemic risk management, we propose a case study where a financial institution is in network with three service providers. Fig. 3 illustrates the business relationships between the entities in this case study. First, the Financial institution archives business data with the support of an Archiving company, second it subcontracts financial brokerage activities to a Brokerage company and third it clears trades with other financial institutions to a Clearing company. The Clearing company makes also clearing for the Brokerage company. Finally, the Datacenter company archives data for the Brokerage company and stores data for the Archiving company, the Brokerage company and the Clearing company.

### A. *Step 1- Business graph of the ecosystem.*

The first step consists in building a global view of the ecosystem, representing all the organisations that are part of the ecosystem, and the business relationships among them. This can be formalised by a graph, where nodes representing entities are connected by one or multiple arcs representing business relationships (other representations may also be used). This is a first specialisation of the *influences* link (see Fig. 2), at the business level, which will be connected to entities' IS components in Step 2. At this stage, it is already possible to identify nodes having a high number of connections, and thus potentially involved in several systemic risks of the ecosystem. In our example (see Fig. 3), the Financial institution has many outgoing connections provided that it uses several services from other entities. Thus, it relies on a good risk management of others in order to secure the activities partially or totally outsourced. At the opposite, the Datacenter company, as a service provider, has many ingoing connections. It thus concentrates a lot of activities potentially critical for the ecosystem and can thus become a single point of failure.

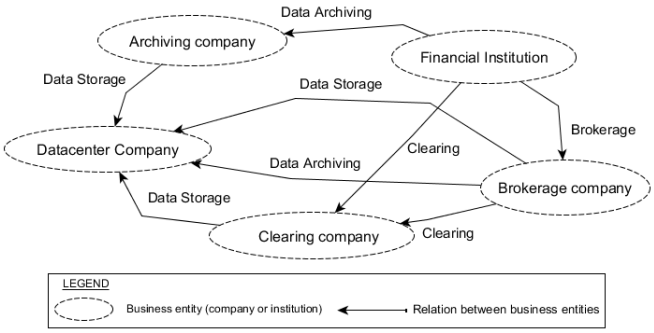


Figure 3. Business graph of the ecosystem

### B. *Step 2 - sISSRM model of the ecosystem.*

Once the high-level formalisation of the ecosystem highlighting the business relationships between entities is done, the second step consists in formalising entities and relationships among them according to sISSRM. This gives a more detailed (and low-level) view of the ecosystem, providing specialisations to the *influence*s link at business and IS levels. Although this is not mandatory, this formalisation can be divided into different steps, as described above.

#### 1) *Step 2.1 - Business and IS model*

First model concerns the assets within each entity of the ecosystem and their relationships at the business and IS level. At this stage, the sISSRM model of the ecosystem conforms to the following requirements:

Requirement 1: At the business level, influence links existing between business assets of different entities are identified and formalised with a suitable semantic (as specialised sub-relationships of the *influences* link): e.g., the customer account management of Financial institution *uses* the archiving service of Archiving company, as represented in Fig. 4.

Requirement 2: At the IS level, IS assets linked to the previously identified business assets are identified and formalised: e.g. Archiving UI (User Interface) of Financial institution and Archiving Management software of Archiving company in our case. It is important to note that each business relationship identified and represented in the business graph maps to one or multiple links between IS assets at the IS level, representative of the way the business aspects are implemented in the IS. Each link between a couple of IS assets starts and ends by interfaces elements ("Int" blocks in Fig. 4), which can be kept abstract or be more detailed to provide further information about the link. Identifying the interfaces brings here a more granular view allowing to identify more precisely the targets impacted by risks. Such interfaces are specific system components (see Fig. 1) ensuring a relation between two elements. In other words, interfaces are the specific parts of assets or assets themselves, which are dedicated to communication with other assets. In the context of two different entities like illustrated in Fig. 4, it is particularly important to identify them, because they are the vectors of risk propagation.

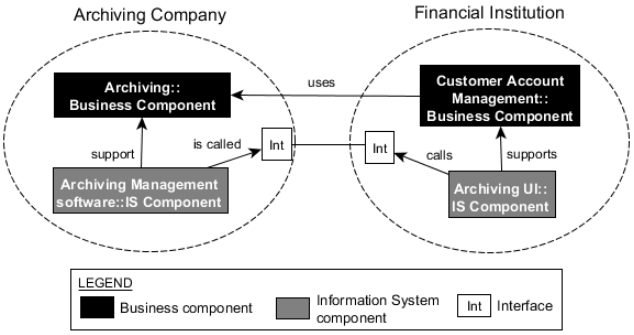


Figure 4. Model of business and IS components

*2) Step 2.2 - Risk modelling, using local risk analysis*

The second step in modelling the ecosystem consists in populating the risk layer, using the information provided by the local risk analysis performed by each entity.

The model (Fig. 4) is thus completed with risk-related aspects, modelling threats, vulnerabilities, events and impacts. Coming back to our example, at the Financial institution level (Fig. 5), the archiving software can be taken over (threat). Combined with the absence of redundancy of the archiving application (vulnerability), it becomes a potential security event "Archiving is taken over" and leads to corrupted software (IS impact) that arms the archiving UI and provokes service archiving unavailability (business impact), both business and IS impact being specialisation of the `impact` class from the meta-model presented in Figure 2.

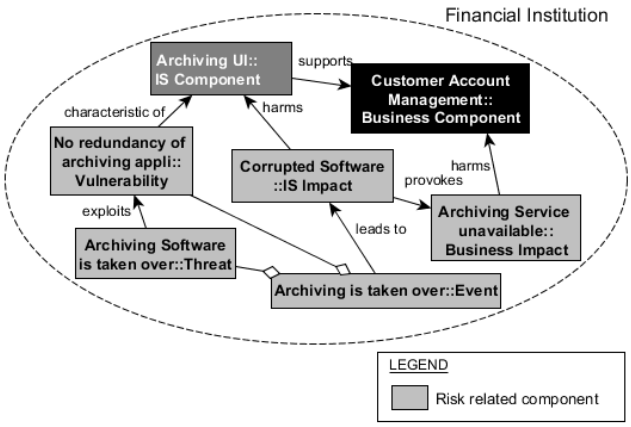


Figure 5. Risk layer model illustration

*3) Step 2.3 Inter-entities links model, using the regulator knowledge*

Then, based on the local risk analysis results, it is possible to link the risks between the entities. More specifically, we formalise <*Impact-Threat*> links between entities, using the regulator knowledge about the ecosystem and the business graph established in Step 1. An IS impact in one entity can indeed lead to a threat in another, if there is a dependency of the latter entity to the IS component harmed in the former. Thus, it links local risk models of entities obtained from Step 2.2, by specialising the *influences* links between them. In order to do this, it is assumed that the regulator is aware of a list of typical and well known IS impacts that can affect entities, and the threats these impacts can generate for other entities. In its simplest form this list contains <*Impact-Threat*> couples and is still in progress.

The identification of relevant <*Impact-Threat*> couples is done for each interface between entities identified in the model. Impacts to consider are those that harms an IS component at the interface between two entities, and threats generated by these impacts are those that target an interface or an IS component depending on it. A *generates* link (see Fig. 2) is added to the model for each couple (dashed link in Fig. 6), which we will name "risk propagation link" in the remainder of the document. For example, "Tampering with software" related to the archiving management software at the Archiving company level leads to "Corrupted software" (IS impact). This IS impact is afterwards propagated at the Financial institution level as the "Archiving software is taken over" threat (see Fig. 6).

At this stage, a complete sISSRM model of the ecosystem is available. At a systemic level, it highlights the influence links between entities in the Business and IS layers, and the <*Impact-Threat*> links across entities. Once the sISSRM model of the ecosystem built, the work of the regulator is to identify systemic risks, i.e. risk generated by <*Impact-Threat*> couples that can be problematic (i.e. generating non-acceptable risks). This is the case, for example, when the local moderation of the risk(s) is relevant at the individual level of an entity, but not sufficient regarding the ecosystem's objectives,

because it is involved in a risk chain leading to inacceptable impacts (i.e. the residual risk whatever small it is, can lead by propagation to an instability in a part or in the entire ecosystem). A risk considered as weak by an entity can induce a strong risk to another entity it is linked to, directly or not, and especially when combined with other small risks (amplification phenomenon [10]).

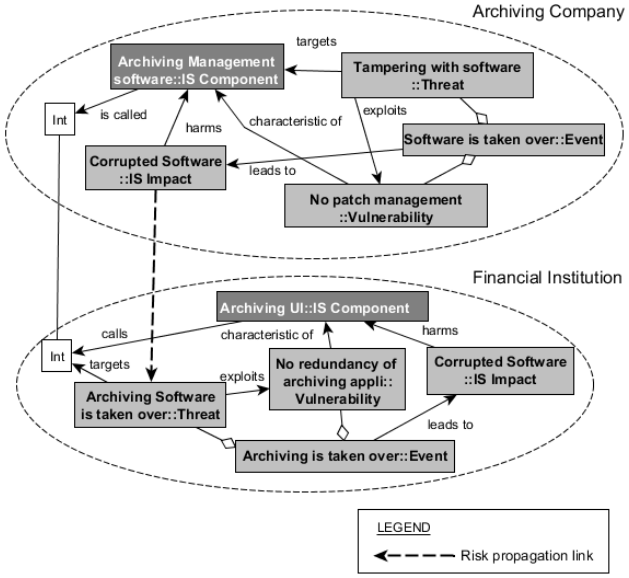


Figure 6. Inter-entities links model illustration

### C. *Step 3 - Systemic risk analysis*

Once inter-entities links have been formalised, the regulator has a complete view of its ecosystems and the possible risk propagation paths between entities. Then, it can analyse those paths to evaluate the importance of the risks.

The regulator has specific objectives regarding the management and control of the ecosystem, keeping stability and sustainability of the ecosystem being probably the most important ones. From a systemic perspective, these can be extrapolated to the objectives of the ecosystem itself, of which the regulator is responsible. The ecosystem is susceptible to potential threats affecting its functions and objectives, for which global system-level risk policies will be applied. It is important to remind that the ecosystem is not simply the sum of the entities composing it. Its assets are not only those entities, but also the relationships between them. We understand here the importance of the different system components of the systemic model, i.e. which comprise those specific elements that are relations and interfaces in addition to other systems and resources (elements that are not systems).

Different aspects have to be handled during systemic risk management:

- *Risk propagation analysis*

The *risk propagation* links represented in the sISSRM model of the ecosystem (see Step 2.3) are the vectors of new risk generation. As already explained, a risk can propagate from one entity to another, from an IS impact harming an IS component of an entity, whether another entity relies on this IS component to perform its activities. The IS impact on the IS component creates a threat in this other entity, which can then constitute a risk for this entity. Resulting impacts can in turn generate other threats in other entities and generate instabilities in the ecosystem through accumulation. For example, in Fig. 6, "Corrupted software" IS impact in the Archiving company is propagated as a threat ("Archiving software is taken over") for the Financial institution.

The regulator has to analyse the system after having identified the risk propagation links. He has to identify critical systemic risks (by systemic risks we mean risks coming from propagation links), which can make the ecosystem dysfunction if one or several elements of a chain are weak. Weakness in this case means that a risk's local regulation is not sufficient to avoid a systemic risk. Further work on risk metrics and associated propagation algorithms needs to be performed to deal with this issue.

- *Identification of critical nodes*

Critical nodes are entities that generate a risk for the ecosystem by the way they are connected to others in the latter. Such nodes are more susceptible to generate weak elements of a risk propagation chain. Two kinds of critical nodes must be identified by the regulator, because it needs to ensure that the risk local regulation for these nodes are strong enough to sustain the system (and thus the systemic objectives): nodes that constitute single points of failure because they provide services to multiple other nodes; and nodes concentrating risk propagation chains usually because they use services from other nodes. For example, within the Datacenter company, "Data storage software unavailable" is an IS impact that generates threats to many network partners (i.e. the Archiving company, the Brokerage company and the Clearing company). The "Datacenter company" is thus a critical node for the whole system (see Fig. 7).

- *Systemic objectives*

As a system, the ecosystem in which the organisational entities evolve has its own objectives. The regulator acts as a controller element in this system, and is in charge of ensuring the system is stable, functions correctly and is healthy enough to reach its objectives. Examples of security-related objectives can be, for example, to guarantee the sustainability of the system or to avoid data leakage in order to support the reputation of the sector. These objectives can be translated in terms of risk-related rules, globally for the whole system (e.g. no risk having a level above a given threshold), or locally targeting one or multiple particular system's element(s), i.e., in particular entities or relations (e.g. an entity identified as particularly critical shall not have more than N risk having a level above a given threshold).

To optimise its objectives knowing the corresponding rules, the regulator may indicate to concerned entities exactly which impact needs to be better handled and at which level. For example in the case of a risk propagation chain, if only one link leads to a better fulfilment of a system objective, only this particular link should be better

handled. If the regulator refers simply to the global objective asking the concerned entity to enhance e.g. its confidentiality level (if this is the objective pursued), this might end up with this entity acting on an impact that has other consequences on the system, leading to benefits for the whole ecosystem

- *Systemic (influence) graphs of the ecosystem*

The last task in systemic risk analysis is to build influence graphs ***for each ecosystem's objective***. These are sub-graphs of the business graph (see Fig. 3), where business links are replaced by oriented arcs representing the influence materialised by risk propagation links identified before, and formalising systemic risk propagation chains. Weights are associated to arcs, representing the importance of the influence regarding the objective's rules (this part is still in progress). Those importance weights are a function of the importance value associated locally by the different entities involved in a propagation link, and of the structure of the entities network. The latter concerns the critical nodes and the paths of the causal effects in risk propagation chains.

With these influence graphs, the regulator can then give further recommendations to entities, in order to ensure the system stability, giving them the indication of which risk to better handle, together with indications on the kind and importance of external impacts that needs to be considered. At this point, it is important to note that dependency between objectives is of primary importance, since each time dependent objectives exist, the influence graphs have to be integrated and a best compromise has to be found regarding the importance weights given to arcs. This is typically a multi-criteria optimisation problem, which we will not detail here, but requires future focused work.

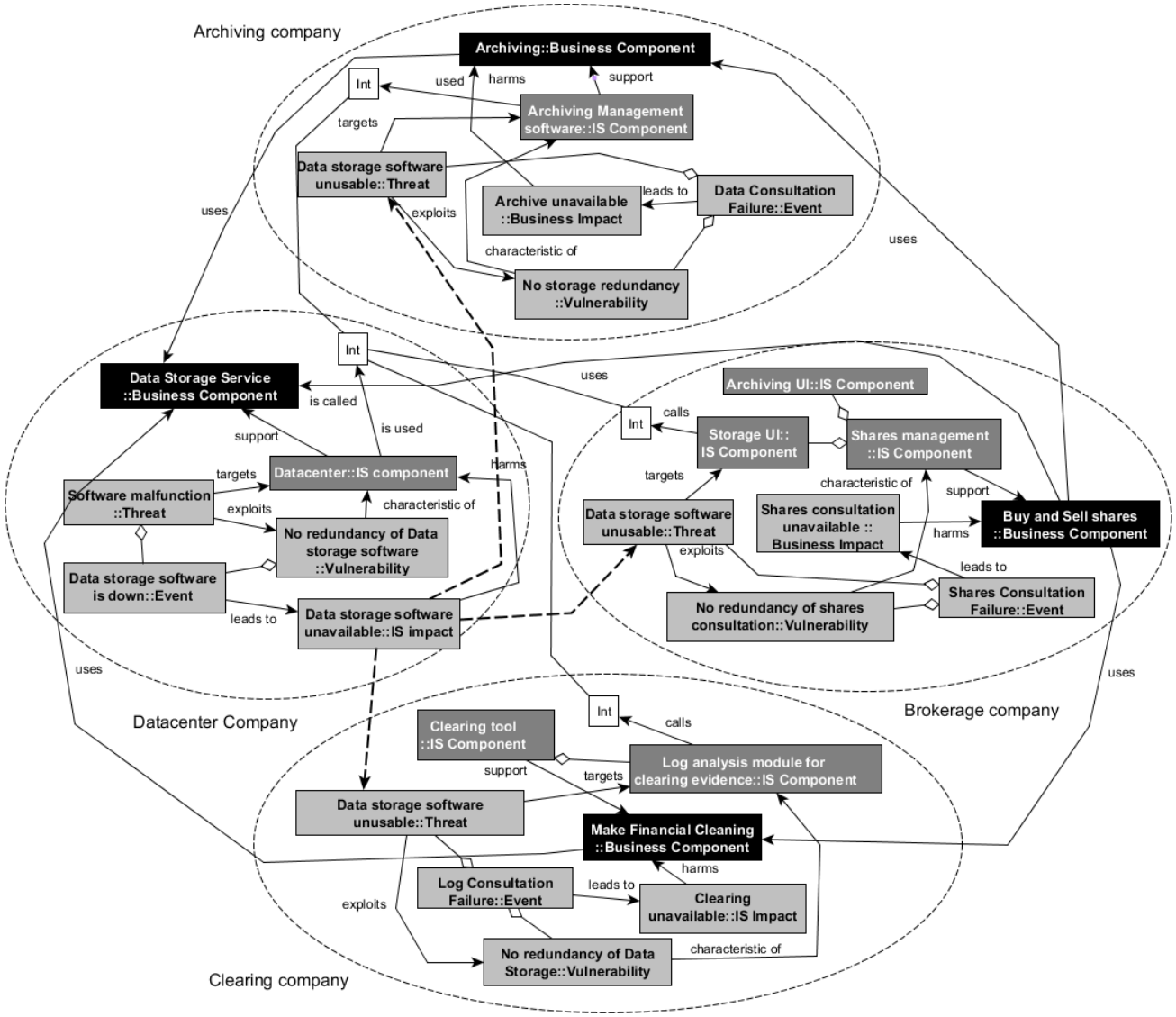


Figure 7. Identification of critical nodes

## VIII. CONCLUSION AND FUTURE WORK

In this paper, we have proposed to integrate systemic elements, as defined in the General System Theory [1], into the ISSRM domain model [2], [3], a conceptual model depicting the domain of ISSRM. First we have introduced the ISSRM domain model as our background work and have exposed the context and our motivation to introduce systemic concepts in the ISSRM domain model. Then, after having reviewed the state-of-the-art, the so-called sISSRM model has been established as a proposal of model integrating systemic aspects within the ISSRM domain model. The application of such a model on an illustrative example has been used to illustrate the approach to be followed in order to identify systemic risks from local and individual risk analysis performed by the entities composing the ecosystem.

We consider the sISSRM model as a promising proposal to be able to deal with the complexity of ISSRM in a context of networked organisations and services shared between several organisations. First, we need to develop metrics to be used in the different modelling steps in order to perform systemic risk analysis, i.e. estimating newly generated risks. Then, the next step of our research work is to validate this proposal by instantiating it on a case. After validation, we plan to perform implementation by applying our research results at a whole sector level, in collaboration with a national regulator, such as the financial or telecommunication regulator with which we have tight collaborations. In the frame of this implementation, a tool support is expected to be able to deal with the complexity of the underlying IS and the huge number of risk-related data.

## ACKNOWLEDGMENT

This work has been funded with the support of *Fonds européen de développement régional* (FEDER).

## REFERENCES

[1] L. Von Bertalanffy, *General System Theory: Foundations, Development, Applications*. New York, USA: Georges Braziller, Inc., 1993.

[2] N. Mayer, "Model-based Management of Information System Security Risk," University of Namur, 2009.

[3] E. Dubois, P. Heymans, N. Mayer, and R. Matulevičius, "A Systematic Approach to Define the Domain of Information System Security Risk Management," in *Intentional Perspectives on Information Systems Engineering*, S. Nurcan, C. Salinesi, C. Souveyet, and J. Ralyté, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 289–306.

[4] Y. Naudet, T. Latour, W. Guedria, and D. Chen, "Towards a systemic formalisation of interoperability," *Computers in Industry*, vol. 61, no. 2, pp. 176–185, Feb. 2010.

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

[6] D. White, "Application of systems thinking to risk management: a review of the literature," *Management Decision*, vol. 33, no. 10, pp. 35–45, 1995.

[7] O. Renn and A. Klinke, "Systemic risks: a new challenge for risk management," *EMBO Reports*, vol. 5, no. Suppl 1, pp. S41–S46, Oct. 2004.

[8] C. Bunting, O. Renn, and M. V. Florin, "Introduction to the IRGC risk governance framework," *The John Liner Review*, vol. 21, no. 2, pp. 7–26, 2007.

[9] A. Klinke and O. Renn, "Systemic Risks as Challenge for Policy Making in Risk Governance," *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, vol. 7, no. 1, Jan. 2006.

[10] I. Anabtawi and S. L. Schwarcz, "Regulating Systemic Risk: Towards an Analytical Framework," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 1735025, Oct. 2011.

[11] H. Cholez and C. Feltus, "Towards an Innovative Systemic Approach of Risk Management," in *Proceedings of the 7th International Conference on Security of Information and Networks*, New York, NY, USA, 2014, pp. 61:61–61:64.

[12] S. Martínez-Jaramillo, O. P. Pérez, F. A. Embriz, and F. L. G. Dey, "Systemic risk, financial contagion and financial fragility," *Journal of Economic Dynamics and Control*, vol. 34, no. 11, pp. 2358–2374, Nov. 2010.

[13] K. Ye, J. Yan, S. Wang, H. Wang, and B. Miao, "Knowledge level modeling for systemic risk management in financial institutions," *Expert Systems with Applications*, vol. 38, no. 4, pp. 3528–3538, Apr. 2011.

[14] E. Fielding, A. W. Lo, and J. H. Yang, "The National Transportation Safety Board: A Model for Systemic Risk Management," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 1695781, Nov. 2010.

[15] A. C. Cagliano, S. Grimaldi, and C. Rafele, "A systemic methodology for risk management in healthcare sector," *Safety Science*, vol. 49, no. 5, pp. 695–708, Jun. 2011.

[16] A. Namatame and T. Komatsu, "Management of systemic risks and cascade failures in a networked society," *Information, Knowledge, Systems Management*, vol. 10, no. 1–4, pp. 111–133, 2011.

[17] T. Vinnakota, "Systemic assessment of risks for projects: A systems and Cybernetics approach," in *2011 IEEE International Conference on Quality and Reliability (ICQR)*, 2011, pp. 376–380.

[18] G. G. Kaufman, "Banking and Currency Crises and Systemic Risk: A Taxonomy and Review," Netherlands Central Bank, DNB Staff Reports (discontinued) 48, 2000.

[19] G. Bernardini, F. Paganelli, M. Manetti, A. Fantechi, and E. Iadanza, "SYRMA: A Tool for a System Approach to Risk Management in Mission Critical Systems," *Int. J. Bus. Inf. Syst.*, vol. 13, no. 1, pp. 21–44, May 2013.

[20] S. J. Gandhi, A. Gorod, and B. Sauser, "A systemic approach to managing risks of SoS," in *Systems Conference (SysCon), 2011 IEEE International*, 2011, pp. 412–416.

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

[22] ANSSI, *EBIOS 2010 - Expression of Needs and Identification of Security Objectives*. France: http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html, 2010.

[23] ISO/IEC WD 27005.2, *Information technology – Security techniques – Information security risk management*. Geneva: International Organization for Standardization, 2014.

[24] E. Laszlo, "Systems theories: Their origins, foundations and development," in *In*, 1998, pp. 47–74.

[25] J. P. Monat and T. F. Gannon, "What is Systems Thinking? A Review of Selected Literature Plus Recommendations," *American Journal of Systems Science*, vol. 4, no. 1, pp. 11–26, 2015.

[26] CSSF, "Circulaire CSSF 12/544 - Optimisation par une approche par les risques de la surveillance exercée sur les 'PSF de support,'" 2012.

[27] N. Mayer, E. Grandry, C. Feltus, and E. Goettelmann, "Towards the ENTRI Framework: Security Risk Management enhanced by the use of Enterprise Architectures," in *Advanced Information Systems Engineering Workshops*, Springer International Publishing, 2015.