Complex Systems Informatics and Modeling Quarterly
CSIMQ, Issue 10, March/April 2017, Pages 75–99
Published online by RTU Press, https://csimq-journals.rtu.lv
https://doi.org/10.7250/csimq.2017-10.05
ISSN: 2255-9922 online

Capability-Driven Design of Business Service Ecosystem to Support Risk Governance in Regulatory Ecosystems

Christophe Feltus[1*], Eric Grandry[1*] and François-Xavier Fontaine[2]

[1] Luxembourg Institute of Science and Technology, 5 avenue des Hauts-Fourneaux, 4362 Esch-sur-Alzette, Luxembourg
[2] Fonction Publique, 4 Place de l'Europe, 1499, Luxembourg

christophe.feltus@list.lu (orcid.org/0000-0002-7182-8185),
eric.grandry@list.lu (orcid.org/0000-0003-3553-8460),
francois-xavier.fontaine@tr.etat.lu (orcid.org/0000-0001-5196-916X)

Abstract. Risk-based regulation and risk governance gain momentum in most sectorial ecosystems, should they be the finance, the healthcare or the telecommunications ecosystems. Although there is a profusion of tools to address this issue at the corporate level, worth is to note that no solution fulfils this function at the ecosystem level yet. Therefore, in this article, the Business Service Ecosystem (BSE) metamodel is semantically extended, considering the Capability as a Service (CaaS) theory, in order to raise the enterprise risk management from the enterprise level up to the ecosystem level. This extension allows defining a concrete ecosystem metamodel which is afterwards mapped with an information system risk management model to support risk governance at the ecosystem level. This mapping is illustrated and validated on the basis of an application case for the Luxembourgish financial sector applied to the most important concepts from the BSE: capability, resource, service and goal.
Keywords: Service, capability, resource, ecosystem, information security, risk, risk management, risk governance, systemic governance.

1 Introduction

Business Service Ecosystems (BSE) are types of enterprise networks which gather enterprises that collaborate to achieve a common systemic goal. These systems are, according to [1], relatively self-contained, self-adjusting systems of mostly loosely coupled social and economic (resource integrating) actors connected by shared institutional logics and mutual value creation through service exchange. Moreover, BSE acts for a business purpose which is composed of business entities that are subject to regulation [2]. The latter is enforced by a regulation body (government agency or public authority) which exercises autonomous authority over some area. In Luxembourg, the ILR (Institut Luxembourgeois de Régulation, Luxemburgish Regulation

*Corresponding author

Reference: C. Feltus, E. Grandry and F.-X. Fontaine, "Capability-Driven Design of Business Service Ecosystem to Support Risk Governance in Regulatory Ecosystems," Complex Systems Informatics and Modeling Quarterly, CSIMQ, no. 10, pp. 75–99, 2017. Available: https://doi.org/10.7250/csimq.2017-10.05

Institute) is the regulation body for the telecommunication service providers, while the CSSF (Commission de Surveillance du Secteur Financier) regulates the financial institutions. In an attempt to optimise the use of resources, the regulation bodies are increasingly adopting a risk-based approach to regulations: assessing the risks to which the market is subject, allows the regulation body to give higher priority to higher risks.

A risk is defined as the consequences of an (adverse) event on the objectives of an organisation [3]. In practice, we have observed, in [4] and [5] that the management of the risk in an ecosystem happens at different levels. At the ecosystem level, the risk management is concerned with the objectives of the ecosystem, while at the enterprise level the risk management is concerned with the objectives of the enterprise. At the ecosystem level, the survival of one enterprise of the system is not the priority, unless it has negative impacts on the ecosystem's objectives: in some cases, it might be better to have an enterprise go bankruptcy and save the overall system.

The risk management at the enterprise level is already well tooled. There exist a plethora of solutions, models, frameworks, and methods to address it [6]. Most of the risks management methods relay on a fair knowledge of the structure and organisation of the enterprise, from many perspectives (strategic, operational, and financial). Acquiring the appropriate knowledge, in the enterprise, to perform this task, is realistic and within range of a risk management team.

At the ecosystem level, risk management is still a recent and rather unexplored domain. Practically, this activity is generally handled by the ecosystem regulators, as owners of the stability and development of the latter. The access to the relevant information required to perform risk assessment is guaranteed as it requires knowing the structure and organisation of the entities of the sector, and knowing the cross-entities relationships. In this context, managing the ecosystemic risk appears to be a challenging activity which calls upon knowledge from different fields amongst which we identify risk management and enterprise modeling.

This article aims to pave the way for the reconciliation of these fields in order to evolve to an integrated approach for ecosystemic risks management. This evolution relies on the idea that it is necessary to delimitate the border of the ecosystem to the right level of granularity. In that regard, in our previous work, we have initiated the modeling of the core business of the ecosystem considering the ecosystem components (enterprises composing the ecosystem and the services and capabilities they make available for the ecosystem) through the Capability as a Service (CaaS) concepts and approach [5]. Accordingly, we have proposed a capability-based model of Business Service Ecosystem (BSE), which consists in a specialisation and extension of the CaaS for capturing system and ecosystem goals, services, capabilities, and resources. The value of the BSE is that it not only abstracts the ecosystem at a manageable level, but also identifies the service as the interface between the ecosystem and its composing entities: in a service ecosystem, the service that an enterprise provides is a resource used to deliver the capabilities required to meet the goals of the ecosystem.

The first objective of this article is to extend the BSE metamodel with additional concepts extracted from CaaS and therefore support the variability and contextual aspects of the ecosystem and its composed entities. The extension, as a result, does not aim at representing the elements required to realise the capabilities but focusses on the context that motivates the latter's existence. The research associated with this first objective is described in Section 2 (background research in the domain of capability-based enterprise modeling) and Section 3 (extended business service ecosystem model).

The second objective of this article is to make use of the extended business service ecosystem and support the regulation of the ecosystem, more specifically through a risk-based approach. The research associated with this second objective is described in Section 4 (background research in the domain of risk-based regulation and risk governance) and Section 5 (risk governance in business service ecosystems).

The third and last objective of this article is to introduce a language for expressing the model of risk governance in business service ecosystems. The language relies on the ArchiMate enterprise architecture framework and is described in Section 6.

In Section 7 the achievements of this research are reviewed, and the perspectives that emerge from the model integration are further elaborated by addressing two separate concerns: what the model allows to capture (modeling concern), and how the model can be used (methodological concern).

The outcomes of these research topics have been validated with an application case in the domain of regulation in the financial sector. The application case is used for illustration purpose in this article, at every stage of the research, and more specifically in Section 3 (instance of the extended BSE), Section 5 (instance of the risk governance in the BSE), and in Section 6 (use of the modeling language). The application case itself is therefore described in this section.

2 Capability-Based Enterprise Modeling

Strategic sourcing is the essence of the capability theory. It requires the right capability to be delivered at the right cost from the right source and right shore [8]. The CaaS project has defined a Capability metamodel [9], [10], [11], [12] gathering elements from three perspectives, each of them having a precise semantics (Figure 1): the enterprise modeling elements, the reuse and variability elements, and the contextual elements. The capability is a cornerstone which allows connecting these three perspectives [11].

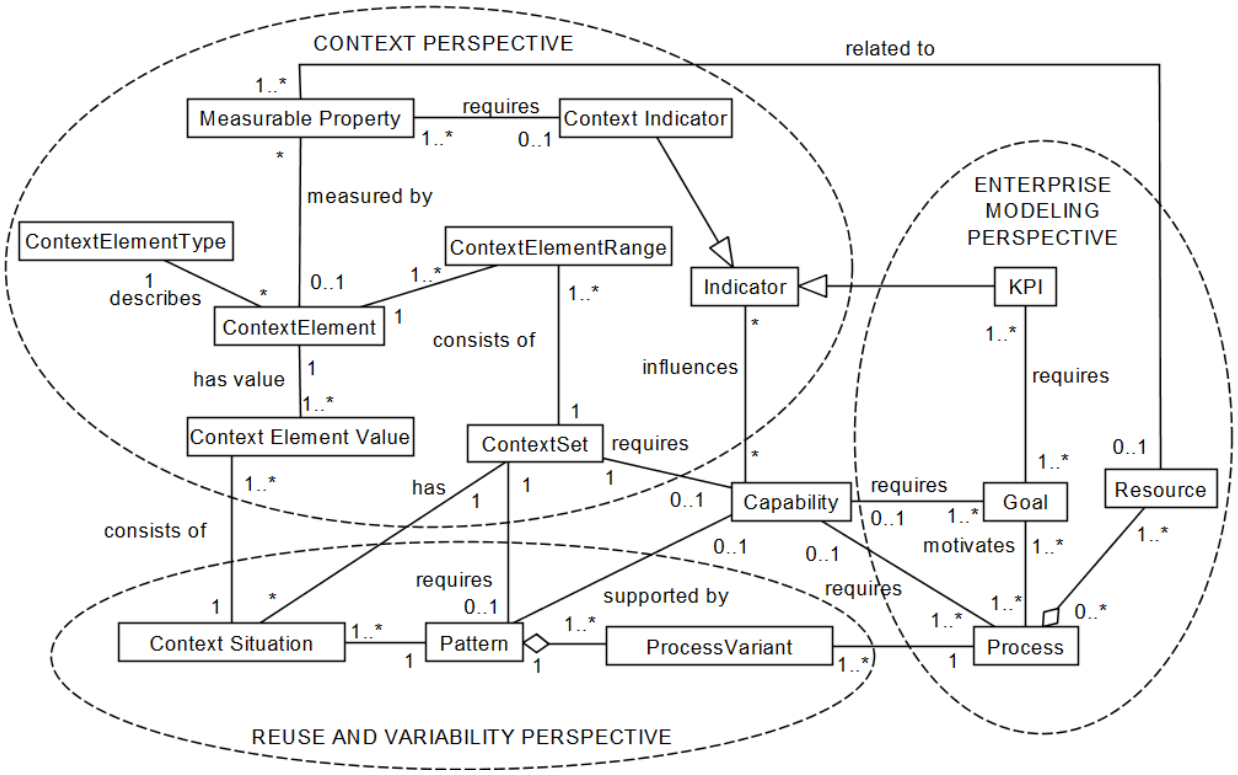


Figure 1. Uncluttered CaaS metamodel and semantic perspectives (remodeled from [12])

The Capability can be seen as the abstraction linking the use of resources and the goals to achieve [13]. It is indeed defined by Henkel et al., as *the ability of an organisation to manage its resources to accomplish a task* [14] (focus on the resources), and by Stirna et al., as *the ability and capacity that enables an enterprise to achieve a business goal in a certain context* [12] (focus on the goal). According to España et al., the context is *the characterisation of a solution in which the capability should be provided* [9]. Consequently, the context is used to evaluate and

adjust the pattern that must be applied to deliver capabilities and represents a reusable solution in terms of business process, roles, supporting IT and resources.

The definition of the capability from CaaS covers both the organisation capability (enabling a firm to make a living in the present [15] and the dynamic capability (enabling a firm adaption to rapidly and discontinuously changing external environments [16]. Helfat et al. [15] addresses this distinction between dynamic and operational (or ordinary) capability. The latter represents what is used and what enables a firm to extend or modify what brings it to live. The organisational capability implies that the organisation has the capacity to perform a particular activity in a reliable and at least minimally satisfactory manner. This organisational capability is equivalent to the main capability as expressed by Henkel et al. [14].

The goal (that requires capabilities in order to be met), as defined in CaaS, may be of five types according to España et al. [9]: *Strategic, Business, Technical, Design time and Run-time.* It can be achieved by dynamic or organisational capabilities. Rosen considers that a capability is composed of capacity [17]: resources (e.g. money, time, staff, tools) for delivering the capability, and ability: competence (e.g. talent, intelligence and disposition), skills, processes. For Rosen, capabilities are of three types: *strategic, value-added, commodity*. According to Taking Service Forward, the capability is *an ability to perform* that requires *investment of time and effort*. Taking Service Forward [18] also considers the resources as an element which *can be bought* or *easily acquired*. An explanation of resource is proposed by Rafati et al. [8] which consider it as the *assets that organisation has or can call upon*. In order to procure competitive advantage to the enterprise, it must be – as far as possible – *Rare, Valuable, Inimitable* and *Non-substitutable* (VRIN) [19].

Henkel et al. in [14] proposed a capability-based approach to support business transformations. It assumes that an enterprise consists in any organisation that generates operation activities funded by stakeholders that do not work for the enterprise. This organisation has the capability to produce value for external entities (like customers in case of private organisations or citizens in the case of public ones) in exchange of money. In this context, Henkel et al. suggest structuring the organisations as a recursive structure of capability and resources, and using a set of transformation patterns. The (main) capability that produces value for which external stakeholders are ready to pay are supported by resources, themselves supported by supporting capabilities, and called sub-capabilities. To uncover the structure of an organisation regarding these capability-resource pair, Henkel et al. have introduced the capability resource type that helps identifying the resources which constitute a particular capability and the capability sub-type to explore the capability that is needed by the resources which constitute the (main) capability.

The recurring repetition of capability-resource pairs constitutes a fractal organisation which supports the achievement of organisational and dynamic goals from the business layer of the organisation down to the supporting layers. According to Sandkuhl et al. [10], these pairs also aggregate process variants, which are themselves specialisations of processes. The variability in capability modeling allows facing the rapidly changing environment in companies. Therefore Sandkuhl et al. suggests to introduce the variation aspects as the cause of a variation and the variation points as the locations of variation in the elements that compose the business service.

3 Towards a Capability-Based Business Service Ecosystem Model

The concept of business ecosystem has already been identified in the 90's, suggesting that a company can be viewed as part of a business ecosystem that crosses a variety of industries [20]. In today's service dominant logic (SD-logic) economy, a business service ecosystem is a business ecosystem oriented towards the exchange of service for service between natural or legal persons to deliver valuable services [21].

The ecosystem services aim to achieve ecosystem goals (like defining the required level of security of the information in the financial sector) and they represent a high value for the beneficiaries of the ecosystem (state or private companies) that are generally willing to pay for it.

Henkel et al. [14] consider that *any organisation where the operational activities of which are financed by external stakeholder* may be considered as an enterprise. Based on this statement, we assume that an ecosystem may be perceived as a specialisation of an enterprise, provided that this ecosystem has specified goals. To achieve its goals, the ecosystem is actually financed by stakeholders (e.g. the customers paying for the financial products, states injecting public money to stabilise the financial system). In return, the ecosystem produces high value to its beneficiaries (such as guaranteeing the performance and stability of the financial activities at the national level). In a service economy, the enterprise can be viewed as a set of service systems, delivering value to its customers through business service, defined as *acts performed for other entities, including the provision of resources that other entities will use* [22]. From the same perspective, the ecosystem can be viewed as a value constellation, defined as a set of complementary service systems, and is named a Business Service Ecosystem (BSE).

The business service ecosystem delivers the ecosystem services through the use of ecosystem capabilities. In a regulated ecosystem, these capabilities are not only the actual core activities of the sector, but also the ability and capacity to regulate the system by governing the business and operational risks.

Given the similarity between the enterprise structure and the ecosystem structure, we propose to extend the fractal organisation approach proposed by Henkel et al. and generalise the capability-resource pair from the enterprise level (fraction B of Figure 2) up to the ecosystem level (fraction A). This allows elaborating what we have named the Business Service Ecosystem Metamodel where the (main) capabilities of the entire system are the ecosystem capability and where the resources of the ecosystem are derived from the capabilities provided by the entities of the ecosystem (the enterprises). Moreover, acknowledging that during an economic exchange, one system benefits from another system due to the application of resources [23], at the BSE level, a service offered by an enterprise must also be considered as a type of ecosystem resource to be applied to realize ecosystem services. Additionally, although an enterprise capabilities generate enterprise services [21], these capabilities, according to the SD-logic, must always be exchanged by the intermediary of the service.

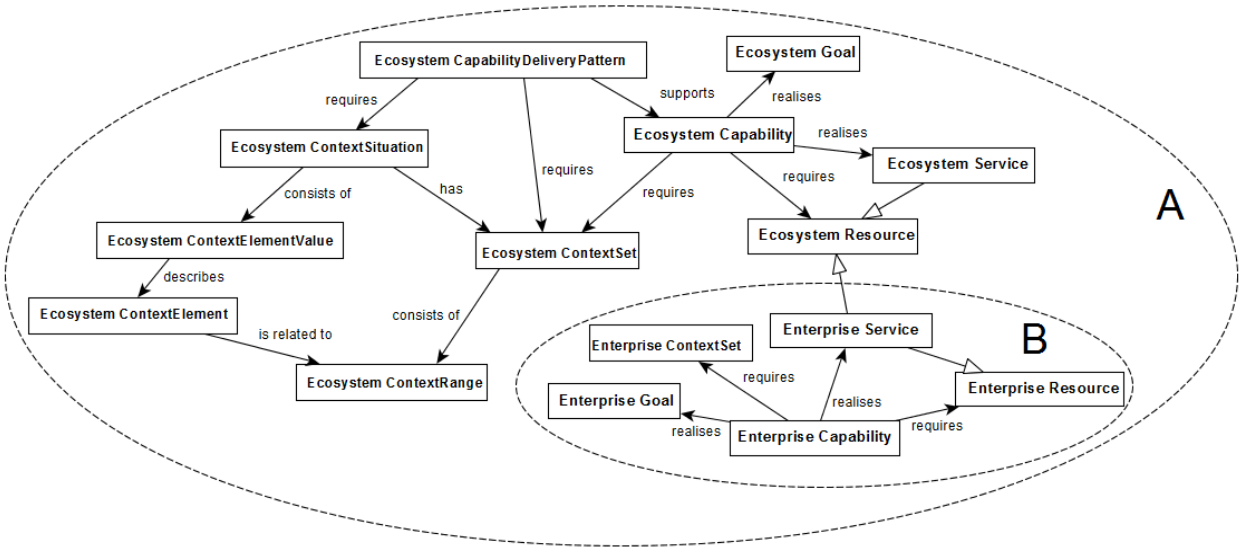


Figure 2. Extended Business Service Ecosystem metamodel

Accordingly, the first version of the BSE was presented in [5], structured around the most significant enterprise modeling concepts from the CaaS metamodel: our primary objective at that time was indeed to capture the architecture of the ecosystem focusing on the relationships

between the enterprise elements and the ecosystem elements. In this article, we further analyse the relevance of additional elements from the CaaS Metamodel (Enterprise Modeling zone Context perspective, and Reuse and Variability perspective) to enrich the fraction of the BSE dedicated to the comprehension of the ecosystem (diagram fraction A). Hence, the scope of the BSE extension is to provide a model for the representation of the risk governance, but not a framework for managing it.

3.1 Concepts From the Enterprise Modeling Perspective

The Business Service Ecosystem metamodel relies on three concepts extracted from CaaS: resource, capability, and goal. We have adopted the CaaS definitions associated with these concepts.

The Capability is *the ability and capacity that enable an enterprise to achieve a business goal in a certain context* [12]. Capability formulates the requirements for the ability of accomplishing a business goal, realised by applying a solution described by a capability delivery Pattern. Given diagram fractions A and B, we distinguish the ecosystem capability from the enterprise capability. The ecosystem capability in the financial sector is for instance the ability to regulate the system, at the national level. At the enterprise level, for instance, it is the capacity to provide financial advice to the customers.

The Resource is *an asset that an organisation has or can call upon* [8]. Resource describes material, staff and other assets that are needed to ensure the Capability delivery. At the enterprise level, a resource could consist in a financial asset management software. There is no actual resource at the ecosystem level, as the entities of the ecosystem provide the required resources as a service.

The goal is a *desired state of affairs that needs to be obtained* [9]. Goal describes the vision of the organisation, what it wants to achieve or avoid. Goal achievement requires Capabilities. At the ecosystem level, a goal could be to guarantee the delivery of secure financial services to customers, although it could be to make profits for a private financial institution.

The BSE metamodel also introduces the concept of Enterprise Service: an Enterprise Service is a business service that an enterprise provides. According the business service's partial definition introduced by Alter et al. [22] (*acts performed for other entities*), we can say that business service provisioning requires enterprise capabilities (*ability and capacity to act for other entities*). Moreover, according to the second part of the business service definition (*including the provision of resources that other entities will use*), an enterprise service can be viewed as resources' provision, justifying the specialisation relationship introduced: an Enterprise Service is a type of Resource that can be used when delivering a Capability. The Enterprise Service is therefore a type of behaviour that allows an enterprise's goal to be realised and that requires enterprise's capability to exist. For instance, the analysis of the level of risk regarding certain financial assets is a service provided by a unit of the bank which also constitutes a resource for analysing the customer risk profile by the customer service unit.

Postulated that the capabilities consist in elements that require a set of resources (enterprise human resources, software, material, processes, etc.) from the enterprise [18], they may hardly be directly exploited by the ecosystem. For instance, the financial asset management software is resource owned by a company and it may not be directly exploited without agreement for delivering ecosystem capabilities. As a consequence, the enterprise resources are provisioned to the ecosystem as enterprise services, which constitute a hyphen between the enterprise capability and the ecosystem resource and hence, a common element to both fractions A and B. At the ecosystem level, this enterprise service may be considered as a type of resource that is required by an ecosystem capability or by any other enterprise capability. For instance, the service of risk analysis associated to certain financial assets may be sold outside the institution to analyse, e.g. the risk associated to the ecosystem assets, or required by the institution to analyse, e.g. the average risk associated to all the assets managed by this institution.

The two last elements from the Enterprise Modeling perspective are the Key Performance Indicator (KPI) and the process. KPIs are *performance measurements used for monitoring goal fulfilment* [2]. Berzisa et al. explain that, in order *to provide a fit between required resources and available resources, KPIs for monitoring capability delivery quality are defined in accordance with organisation's goal* [2]. They are also used to select the most suitable pattern for capability delivery, according to España et al. [6]. The BSE metamodel has an objective to represent the structural elements of an ecosystem, as well as the relationships among them, and does not include at this stage the measurement framework associated with the dynamics of the system. Therefore, elements related to resource availability indicators are currently not included. The realisation of a capability requires (business) processes that use a set of resources.

The processes are directly related to the capability, are affected from the change in the context Sandkuhl et al. [19] and must be designed in *a way to be adjusted quickly*. The relation between the three concepts has been further analysed in Sandkuhl et al. [19]. Alike KPI, processes are related rather to operational aspects than to architecture representation. Hence, the concept of process will not be considered for the extension of the BSE at this stage.

3.2 Concepts From the Context Perspective

The part of the metamodel dedicated to the context is composed of the Measurable Property, the Context Indicator, the Context Element, the Context Element Range, the Context Element Value and the Context Set. The Context Set is the central concept of the context perspective. According to Berzisa et al. [24], it *denotes a set of circumstances, such as geographical location, platforms and device used, as well as business conditions and environment*. It describes the set of Context Elements that are relevant for describing run time context and representing information that can be used to characterise the situation of an entity [25] and for the delivery of a specific Capability accordingly. The Context Set defines relevant ContextSituations: a Capability is designed to be adequate for the certain instance of the context situations that only exist at run time and are represented by a Context Set.

The Context Set is described by Context Elements which are valid in certain Context Element Range. Context Element is any information that is relevant to capability design, delivery, and pattern application. Context Elements can be described by Context Element Type, e.g. static context, dynamic context, social context. Context Element Type supports finding the most appropriate pattern for a certain context situation, and defining relevant contexts during capability design. The Context Element may be, for instance, the legislation that applies for a specific sector. The Context Element only defines the context conceptually, the run time values are represented by Context Element Value – that has only instance at run time – and design time ranges by Context Element Range. The purpose of Context Element Range is to represent the actual ranges of values of relevant Context Elements for a specific Context Set. The attribute Calculation expression is used to specify the calculation of the context element value using measurable properties.

Given that our objective is neither to typify nor to define measurement properties of context elements in the semantic enhancement of the BSE metamodel, only the Context Set as a container of Context Element Ranges, as well as the Context Element, the Context Element Range and the Context Element Value appear to be at the appropriate level of abstraction and, hence, will be considered to design the context of the system.

3.3 Concepts From the Reuse and Variability Perspective

The part of the metamodel dedicated to the reusability and variability is composed of the context situation, the pattern, and the process variant. According to Zdravkovic et al. [26], the *Capability formulates the requirements for the ability of accomplishing a Goal, realised by applying a solution described by a capability delivery Pattern*. In that regard, Sandkuhl et al. in [10] explain that capability is supported by exactly one pattern which supports the description of a solution

for realising a capability and explain how this capability must be delivered according to the context [27].

One possible interpretation of the pattern from the CaaS point of view, related by Sandkuhl et al. [10], is that the pattern aggregates process variants which in turn are specialisations of process. This process variant is used to represent variants of the capability process [24]. The context situation at run time represents the context set in which a capability is designed to be deliver in a business situation [28]. Hence, the context situation describes the context data in capability delivery phase [28]. It is illustrated in Zdravkovic et al. by the use a model-based patterns to describe how software applications can adhere to changes in the execution context [26]. A meta-model for capability design and delivery is presented with the consideration to delivering solutions as cloud services.

For the semantic enhancement of the BSE metamodel, the two elements (ContextSituation and Pattern) from the reuse and variability perspective of the CaaS metamodel are significant and have to be considered.

3.4 Financial Application Case

The analysis of the three perspectives of the CaaS metamodel has allowed determining the concepts that are relevant and necessary to model an ecosystem. These concepts are the context situation, the pattern (also named capability delivery pattern), the context set, the context element, the context element range, the context element value and the context situation. These concepts are integrated in the extended BSE metamodel represented in Figure 2 and are named, respectively: Ecosystem ContextSituation, Ecosystem Pattern, Ecosystem ContextSet, Ecosystem ContextElement, Ecosystem ContextElementRange, Ecosystem ContextElementValue, and Ecosystem ContextSituation. This section first presents the application case, and then illustrates the BSE instantiated accordingly.

Leading application case. Since 2014, the LIST is mandated by the Commission de Surveillance du Secteur Financier (CSSF – regulator – http://www.cssf.lu) to structure and model systemic risk management approaches for the Luxembourgish financial sector [29]. The CSSF's mission is to protect the financial stability of the supervised entities and of the financial sector as a whole as well as to ensure compliance with the financial laws and regulations applicable to the supervised entities. To realise this mission, the CSSF regulates the enterprises that compose the ecosystem and offers services that generate systemic capabilities. It is also in charge of promoting transparency, simplicity, and fairness in the financial products and services market, and is responsible for the law enforcement on financial consumer protection, on the fight against money laundering, and terrorist financing [7]. The structure of the financial sector is adapted to the regulatory authorisation scheme, and introduces the concept of Professional of the Financial Sector (PFS) as regulated companies performing non-banking financial services. These services may be offered in the form of a single financial activity, as well as in the form of connected activities. More specifically, the following actors are subject to the PFS regulation in Luxembourg: (1) Investment Firms, offering financial services in relation to the investment of financial instruments; (2) Specialised PFS, offering services of a financial nature to private investors and/or other PFSs; support-PFS, offering services of an organisational and technical nature to PFS. The support-PFS can provide services to any type of undertakings whether they belong to the financial sector or not. The fact that they provide services to financial professional clients qualifies them as professionals of the financial sector and subjects them to the supervision by the CSSF. Lab Group (http://www.labgroup.com) is a CSSF certified document and data management company, with offices in Luxembourg, Dublin, and Gibraltar. As such, it is a support-PFS, which supports the financial sector through the delivery of archiving services. On 18 July 2012, the CSSF published the circular 12/544 [7], which requires the support-PFS's to perform risk self-assessments and provide the CSSF with the risk analysis reports. This rule

primarily intents at optimising the supervision through the introduction of a risk-based approach, motivated by the increasing number of supervised entities.

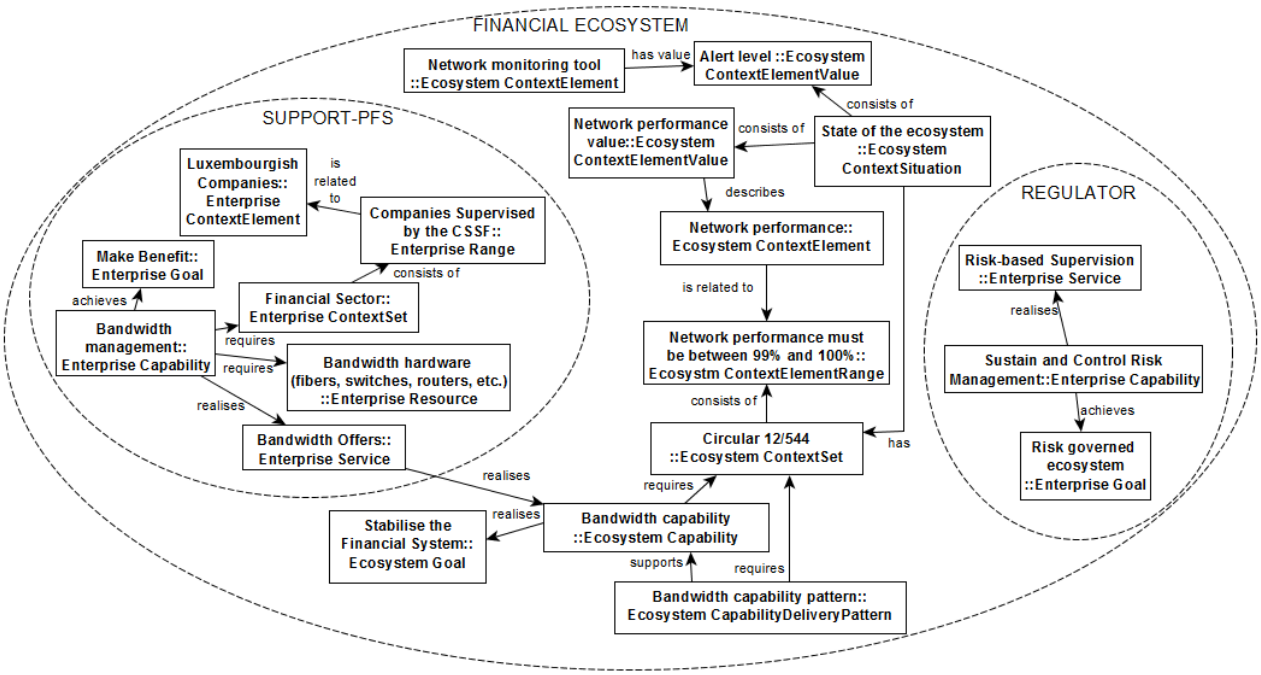


Figure 3. Extended Business Service Ecosystem metamodel instantiated to the financial ecosystem

The BSE instantiated. At run time, in regard to the leading application case in the financial sector (Figure 3), the context in which the ecosystem evolves may be, for instance, a normal situation, or a situation where an attack occurs. This information is represented using the Ecosystem ContextSituation element. This situation consists in a set of context element value which describes related context elements. For instance, the State of the ecosystem which is an Ecosystem ContextSituation consists in a Network performance value which is an Ecosystem ContextElement Value that describes the ContextElement Network Performance. This Context element is related to a context element range, like for instance Network performance must be between 99% and 100%.

The context situation is also defined according to a context set, like the Circular 12/544 in the financial sector. This is written Circular 12/544::ContextSet. This context set consists of context element range and it is required by the capability delivery pattern in order to specify the context when this pattern is applicable. For instance, Circular 12/544::Ecosystem ContextSet allows selecting when Bandwidth capability pattern::Ecosystem CapabilityDeliveryPattern applies. Aside the context set, the monitoring of the capability is also achieved using KPIs. The latter are used to monitor goals fulfilment, to know in this application case, if the financial system is stable or not (e.g. if the bank network cannot support transactions overload anymore). For the sake of clarity, this monitoring by the KPIs has not been represented in the figures.

4 Risk Governance and Regulatory Ecosystem

Although the history of business regulation could be seen as successive waves of imposing and releasing constraints on the business, there is a clear evolution over the years from prescriptive rules the business has to follow to cost-benefit approaches. The rationale behind this evolution has its roots in the deregulatory waves of 1980–1990's, specifically in the UK, and its associated New Public Management (NPM) trend: public regulation was pressured to justify its own operational costs, as well as the costs imposed on business, and adopted cost-benefit analysis to bring objectivity and transparency. Risk-based tools were adopted from the business sector as

instruments for making policy and aiding in decision-making: the allocation of resources could now be explained from the level of risks identified [30]. In May 2005, UK Prime Minister Tony Blair delivered multiple speeches referencing the implementation of the reform recommended in Hamptons Review, which pillars are fewer regulatory bodies and risk-based enforcement by local authorities. He also stressed the need to reduce administration burden, but also promote public sector entrepreneurship by reducing the unnecessary inspections and making them proportionate to the risk faced. He advocated a programme of *Better Regulation which contains regulatory requirements for regulators to use a rigorous risk-based approach and powers to reform penalties according to risk-based principles* [31].

A risk-based approach to regulation requires the regulator to follow a policy cycle centred on risk: forecasting (risk assessment), prevention (risk management), oversight (regulatory review), implementation (including enforcement), coping, and evaluation [32]. The risk is assessed by considering the likelihood of non-compliance, as well as the impact of this non-compliance in terms of the occurrence of an adverse event (failure of a particular service, injury/death, ect.). The Information System Security Risk Management (ISSRM) [33] captures the concepts required to manage the risks in an organisation, and more specifically the information security risks: a risk is seen as an (adverse) event and its impact on the assets of the organisation. In information security, the event is traditionally expressed in terms of threat and vulnerability: the threat exploits vulnerabilities of the resources to harm the assets of the organisation. ISO 31000:2009 [3] proposes a risk management model applicable to manage any risk, and not only information security risks.

The assessment of both the likelihood and the impact of non-compliance are based on defined criteria to ensure consistency and rigour in the assessment process. The result of the risk assessment allows the regulator to make informed choices regarding both its rule making and enforcement activities: highest risks of non-compliance should be addressed with the highest priority, requiring more severe enforcement approaches, while lighter enforcement would be justified to address low risks.

The deregulatory wave also introduced the principle of self-regulation, and therefore the rise of market oriented regulation and the decentralisation of the control: the rules governing each market are defined and managed by the market itself. This has resulted in a fragmentation of the regulation, with responsibilities distributed amongst a plethora of regulatory actors, such as public agencies, market organisation, and US-style independent regulatory agencies. Such fragmentation into specialised regulatory entities can be desirable, as only experts in a market might be able to adequately assess the risks associated with that market. It however can also yield problems when issues are interconnected, especially when entities are subject to multiple regulations. Fragmented institutions have difficulty dealing with interconnected risks (multiple simultaneous risks, risks that are transmitted across or cause impacts in multiple domains, and policies that reduce one risk but increase other risks in other domains), causing a risk management issue known as risk-risk tradeoffs: it typically occurs when a regulator intents decreasing a specific risk in a specific area, which leads to another unexpected risk in another area. Risk-risk tradeoffs can be better managed, by following a set of recommendations, amongst which increasing the transparency behind risk management decisions, and adopting an evidence-based policy-making [34], which both can be met through a scientific approach to risk management and a better understanding of both the structure of the market and the context in which it resides.

Risk governance is defined as *the critical study of complex, interacting networks in which choices and decisions are made around risks* [35]. In terms of regulation, many risks are systemic, in the sense they are embedded in the larger context of societal processes. Systemic risks cannot be addressed with the usual probability-effect analysis and require a more holistic approach integrating interdependencies, and ripple and spillover effects: they have indeed a growing potential of harm as their effects can be amplified (or attenuated) throughout their propagation in a complex system of interdependencies [36]. Systemic risks cannot be constrained

to defined boundaries, whether they are geographical (national borders), or economical (market sector). Risk governance actually acknowledges that not all risks are simple and can be expressed as a (linear) function of probability and effect. Risk Governance is therefore a major component in today's challenges of systemic risk management. The actual implementation of risk governance requires the adoption of a framework that goes beyond the classical elements of risk management (risk analysis, risk communication) such as defined by international risk standards [37], [3]. Risk governance indeed includes both the institutional structure and the policy process to regulate, reduce or control risk problems. Risk governance frameworks therefore associate both the regulation bodies and private enterprises: it includes matters of institutional design, technical methodology, administrative consultation, legislative procedure and political accountability on the part of public bodies, and social or corporate responsibility on the part of private enterprises. But it also includes *more general provision for building and using scientific knowledge, for fostering innovation and technical competences, for developing and refining competitive strategies, and for promoting social and organisational learning* [38].

Risk governance is closely related to the concept of regulatory system, defined as *the set of processes that include: setting regulatory requirements and voluntary standards for the production of goods and the provision of services; drafting laws and regulations; and putting controls in place to check that products meet requirements and specifications* [39]. The concept of regulatory system can be applied to any economic sector: it requires integrating the regulatory dimensions (structure and process) with the actual production system, as the product/service providers are part of the regulatory system (at the minimum through reporting capabilities to the regulation body). The regulatory system draws the boundaries of the regulated market in terms of structure (the regulated entities, the regulatory body and their relationships) and the policy processes. The regulatory system perspective also offers guidelines on what risks have to be managed at the level of the regulated system, as it differentiates risks that remain internal to any regulated entity (i.e. affecting its own objectives, such as profitability) from risks that have undesirable external effects. The regulatory system therefore defines the risks that are in the scope of the risk governance: (1) the risks that originate with an entity whose consequences have an impact on the external environment of that entity (business-to-consumer, business-to-business, business-to-environment and business-to-society risks); (2) the risks that originate with a single entity but cannot be mitigated by that single entity and require coordination amongst the entities of the system; (3) risks that originate with the business environment of the integrated system, impacting a regulated entity but which that entity cannot control. The concept of regulatory system can therefore be considered as the foundation building block on which risk governance can be built, as it guides the description of the system to be governed in terms of active structure (the entities in the system), the processes (and more specifically the policy processes) and the context in which risk governance should be performed (the influence of the environment).

Rapid technology changes have introduced a rise of Business Service Ecosystems, increasing the interconnections across domains, and therefore calling for an actual management of risk-risk tradeoffs at the level of the ecosystem. Moreover, due to this increase of technological interconnections, an ecosystem cannot be defined anymore through a single regulation body – it is indeed now composed of enterprises of various natures, from financial institutions providing financial services, to telecommunication service providers. An ecosystem not only becomes the subject to market regulations (financial regulation), but also to emerging domain regulations (data privacy, information security) associated with the usage of information technologies. The risk governance therefore becomes a challenge also at the ecosystem level, leading for a need to perform as a regulatory ecosystem, extending the concept of regulatory system to multiple regulatory bodies: FCC chairman Tom Wheeler calls for this new regulatory ecosystem when he proclaims:*"We cannot address these threats in one-sector or one-agency silos. Particularly among regulatory agencies, we must coordinate our activities and our engagement with our sector stakeholders"* [40].

In summary, in regard to this inescapable evolution of the market regulation, from a traditional approach to risk of non-compliance based approach, new requirements emerge in terms of modeling and designing the risk-governance of Business Service Ecosystems. The multiple regulation the private companies are subject to, and the resulting impact of the risk-risk tradeoffs, set forth new needs of *transparency* and *evidence based policy making*, the whole in a more *holistic approach which considers inter-sectors interdependencies*. Appropriate dedicated frameworks of risk governance are necessary conditions to make this change work. The latter must allow *associating regulation bodie*s and private companies, and must strongly consider supporting *the integration of the regulatory dimensions with the production system* being described in terms of *active structure, process,* and *context* in which risk governance happens.

5 Towards Risk Governance in Business Service Ecosystems

The capability-driven approach for modeling enterprise ecosystems paves the way to an innovative method for managing the risks of the ecosystem, aka systemic risks. To present our approach, we exploit the information system security risk management reference model and apply it at both levels (A and B) of the extended BSE metamodel of Figure 2.

For comprehensibility and readability in the illustration of the mapping between the Risk Model and the BSE metamodel, only the four most important concepts of the BSE will be exploited during the mapping, respectively: the capability, the resource, the service, and the goal.

5.1 ISO 31000:2009 Risk Model

ISO 31000 consists of a family of international standards dedicated to the risk management and published by the International Organisation for Standardisation. ISO 31000:9000 [3] provides a set of principles and guidelines to structure a *universally recognised paradigm* for practitioners and companies to manage risk. In that regard, the standard defines the risk as *an effect of uncertainty on objectives* that can have different aspects (e.g. security, quality, environment, privacy, etc.) and that can apply at different levels, such as the enterprise or the ecosystem. The risk is characterised by reference to potential events and consequences. According to the standard, an event consists of *the occurrence or the change of a particular set of circumstances and the consequence represents the outcome of that event which affects an objectives*.

ISO 31000:2009 also stresses the importance of establishing the context in which the system evolves. This context aims at defining the external and internal parameters to be taken into account when managing risk. The internal context includes, amongst other, the capabilities, the knowledge and the resources available in the system to achieve the business goal. The external context, in turn, refers to the environment in which the organisation seeks to achieve its objectives (cultural, social, political, legal, regulatory, financial, etc.)

5.2 Mapping Risk Model-Business Service Ecosystem Metamodel

In an attempt to integrate the domains of risk management and capability management, this section addresses the mapping between the risk model provided by ISO 31000:2009 and the extended BSE metamodel. The resulting integrated model is illustrated in Figure 4, where the concepts from the risk model are in blue, and the concepts from the BSE metamodel are in black.

During the model integration, at design time, four concepts of the extended BSE metamodel (presented on Figure 2) have been mapped with the following concepts of the risk model: the event and the consequence (which constitute the abstract concept of risk), the control and the context:

- The event is defined by ISO 31000:2009 as the occurrence or change of a particular set of circumstances. Hence, it represents a context situation that, following CaaS, capture the actual context during the system run time and that has a purpose to describe a certain context

affecting capability delivery. Consequently, both concepts may be mapped and be represented by the element Event::Enterprise/Ecosystem ContextSituation.

- The consequence is defined by ISO 31000:2009 as the outcome of an event affecting objectives. The consequence of an event is hence a (new) state of the context. Accordingly, it is mapped with the context element of CaaS which describes run time context and represents information that can be used to characterise the situation of an entity [25]. The mapping between both concepts is represented by the element Consequence::Enterprise/Ecosystem Context Element. Furthermore, the consequence is outcome of the event and both concepts are referred to the Enterprise/Ecosystem risk. These associations are represented by blue dash lines in Figure 4.
- The control is defined by ISO 31000:2009 as a measure that is modifying risk. Given that the risk exists in regard to the consequence generated by an event, the control is a "measure" that has a goal to mitigate this consequence. We consider, in accordance with the CaaS philosophy, that this goal is achieved by a dedicated capability delivery pattern which represents a specific solution (for mitigating the role) in a certain context. The mapping between both concepts is represented by the element Control::Enterprise/Ecosystem CapabilityDeliveryPattern.

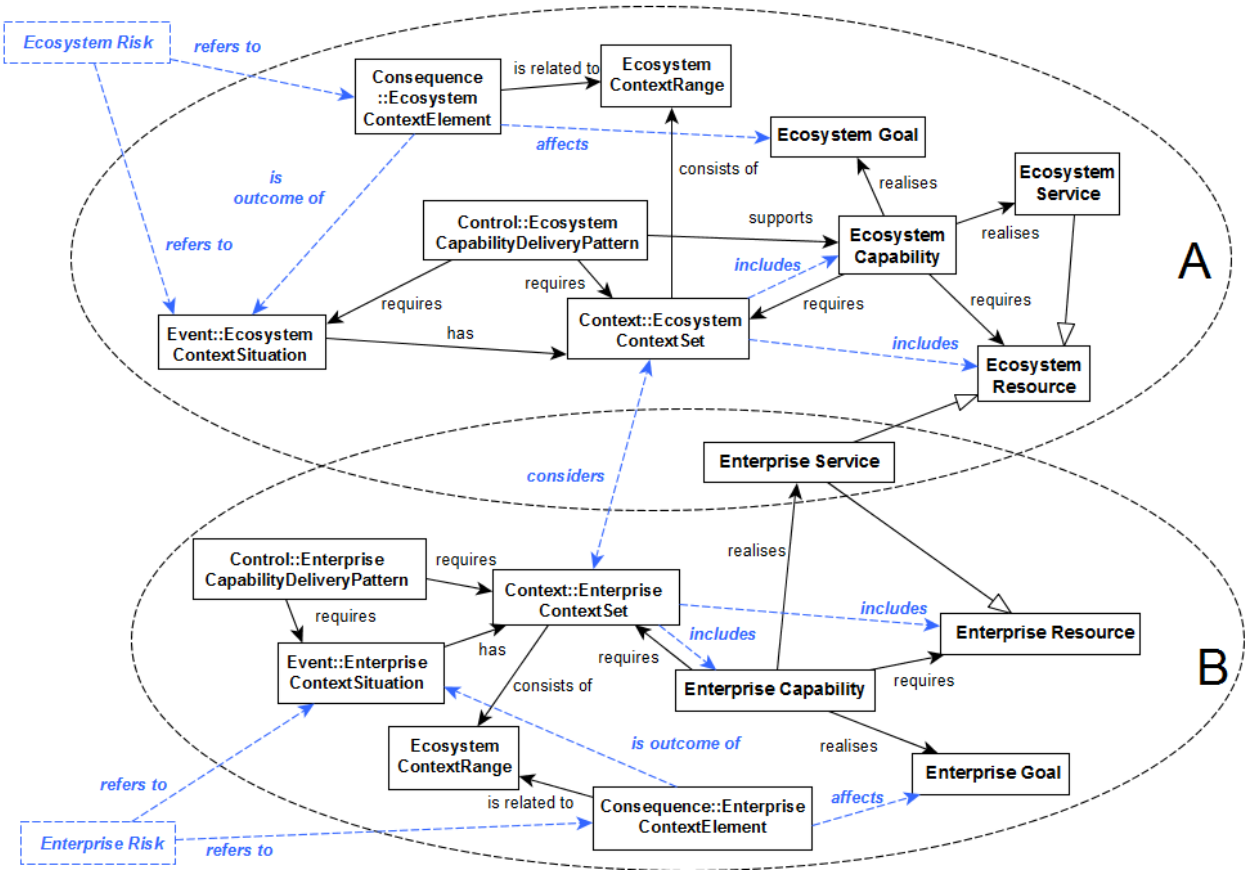


Figure 4. Mapping risk model – Extended BSE metamodel

- Finally, the context in ISO 31000:2009 defines the external and internal parameters to be taken into account when managing risk. It is equivalent to the context element from CaaS which represents any information that can be used to characterise the situation of an entity. The mapping between both is represented by the element Context::Enterprise/Ecosystem ContextSet. This context, within a system (enterprise or ecosystem), corresponds to an internal context and includes, following ISO 31000:2009, the system capability and resources. Beside the system, this context corresponds to the system environment (e.g. cultural, social, political, legal, regulatory, financial, etc.). Provided that CaaS does not

explicitly refer to internal or external parameters, in order to consider this element at the BSE level, both the enterprise context element and the ecosystem context element have been associated with a relation meaning that both consider each other, e.g. an enterprise of an ecosystem must consider the Ecosystem Context Set, like, for instance, the regulation that applies to this context.

5.3 Luxembourg Financial Ecosystem in Normal Situation

At run time, the Luxembourgish financial sector (Figure 5 and Figure 6) is regulated by a multitude of rules, amongst which the *Circular 12/554* [7] that imposes the support-PFS to perform risk self-assessments and that provides the CSSF with the risk analysis reports. The circular requires, amongst others, to have systemic risk managed at the national level. Systemic appropriate risk management contributes to the ecosystem goal that is to *stabilise the financial system*.

Figure 5 represents an extract of the model related to the normal state of the ecosystem, composed of a support-PFS and the regulatory body:

- The regulator is a specific type of enterprise which performs risk governance of the ecosystem. This risk gov*ernance* is a type of *enterprise goal* written Risk governed ecosystem::Enterprise Goal in the model. To achieve this governance, the regulator requires the enterprise capability to *sustain and control the risk management*. The later realises the *enterprise service* of *risk-based supervision* and therefore, according to ISO 31000:2009, the risk is analyzed in a function of the ecosystem events and ecosystem consequences.
- The support-PFS is an enterprise of the ecosystem which offers a bandwidth service to the financial sector enterprises. This enterprise service is named standard bandwidth offer and is realised by the enterprise capability of bandwidth management. This enterprise capability requires enterprise resources of a type bandwidth hardware (fibers, switches, routers, etc.) and achieves the enterprise goal to make benefit. This bandwidth management capability is designed to be used in a specific enterprise context set named financial sector which, according to ISO 31000:2009, is defined considering the external context, to know: the ecosystem context set. This enterprise context set consists of enterprises supervised by the CSSF. The latter represents the enterprise range and is related to Luxembourgish companies, which are enterprise context element.
- The standard bandwidth offers enterprise service realises, at the ecosystem level, the standard bandwidth capability which is an ecosystem capability supported by the normal situation bandwidth capability ecosystem capability delivery pattern.
- At the ecosystem level, the context situation is a normal situation. This normal situation is defined according to an ecosystem context set which, in our case, is the Circular 12/544 and consists in a network monitoring tool that indicates a low alert level. The Circular 12/544 is an instance of an ecosystem context element and the network monitoring tool is an instance of an ecosystem context element. This context situation consists of an ecosystem context element value (in this case: the network performance is 99.9%), which describes the network performance and which affects the stability of the financial system ecosystem goal (positively in this case). The network performance is an instance of the ecosystem context element and is related to a context element range (Network performance must be between 99% and 100%) which specifies the range of the network performance in the context set of the circular 12/544.

Regarding the *risk-based supervision* achieved by regulator, the risk is appraised in a function (1) of the context situation which is a normal and (2) of the value of the network performance resulting of this context which is of 99.9%. This is represented at the model level using two associations between concepts of a type *refers to*.

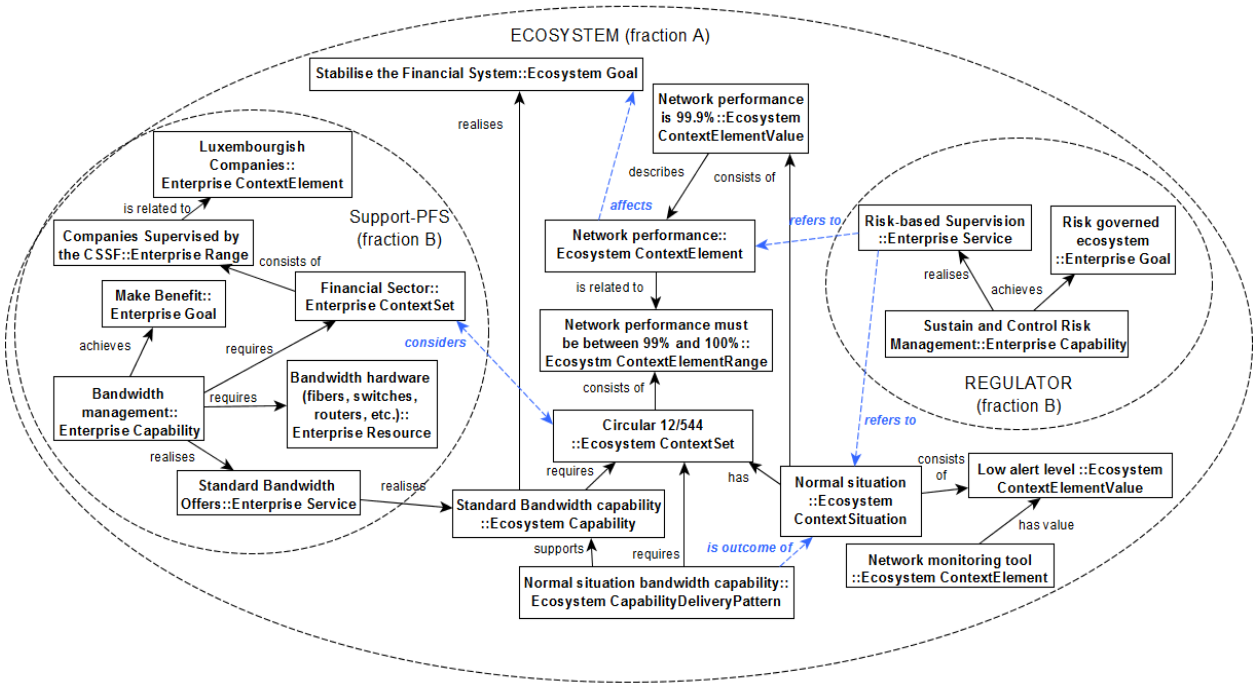


Figure 5. Business Service Ecosystem metamodel instantiated to the financial sector in case of normal situation

5.4 Luxembourg Financial Ecosystem Under a DDOS Attack

Figure 6 represents an extract of a model of the financial ecosystem when a distributed denial of service (DDOS) attack occurs. Alike in the case of a normal situation, this model represents ecosystem elements including a support-PFS and the regulator enterprises.

- In case of DDOS, at the ecosystem level, the *context situation* changes from *normal situation* to *bandwidth reduced by DDOS*. It is represented by a *network monitoring tool* that indicates a *high alert level* and means a reduction of the value of the context element from 99.9% to 50%, which is written *Network performance reduced by 50%*. Given that this network performance is out of the range 99% to 100% of performance specified by the *context set*, the level of this value may affect the stability of the financial system which is an *ecosystem goal*. According to ISO 31000:2009, this risk must be mitigated by a dedicated control which following CaaS is expressed as a new instance of *ecosystem capability delivery pattern*. This pattern, named *bandwidth capability during DDOS*, aims to support an *exceptional bandwidth capability* which is a new instance of an *ecosystem capability*.
- Alike in a normal situation, the support-PFS remains the enterprise which offers a bandwidth service even when an attack occurs. However, in order to realise the new ecosystem capability requirement of exceptional bandwidth, the support-PFS must offer a *complementary bandwidth service*, in addition to the standard one. Both support-PFS enterprise services are realised by the *bandwidth management enterprise capability*.
- Regarding the *risk-based supervision* achieved by a regulator, the risk is appraised in a function (1) of the context situation which is *bandwidth reduced by DDOS* (2) of the value of the network performance resulting of this context which is a *network performance reduced by 50%*.

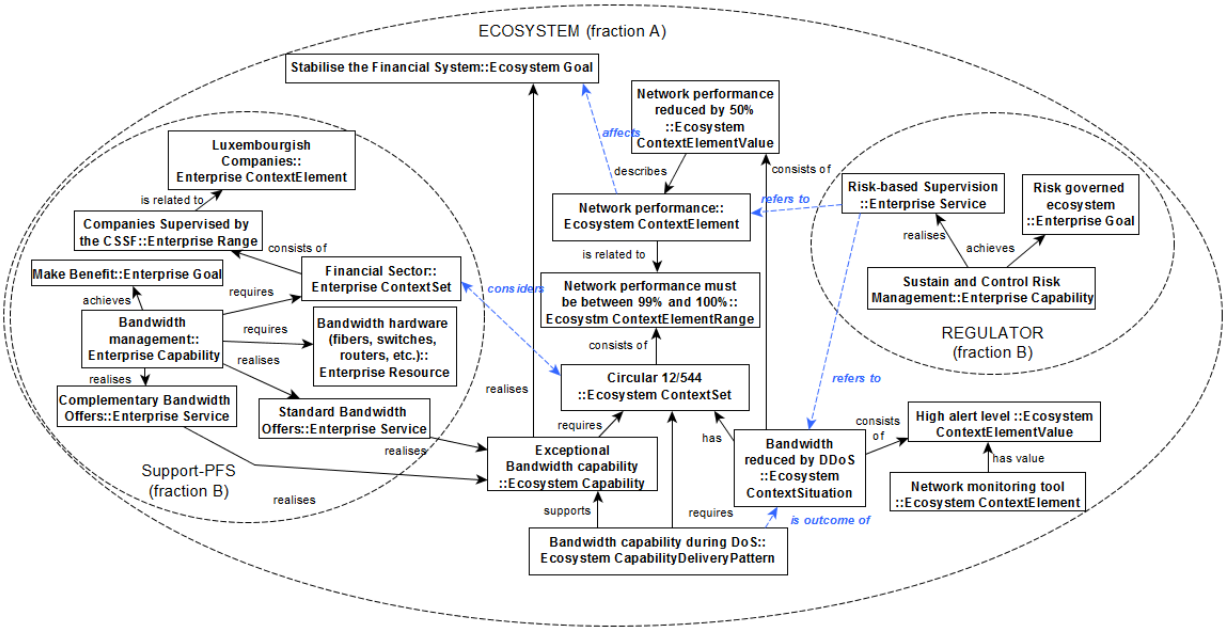


Figure 6. Business Service Ecosystem metamodel instantiated to the financial sector when a DDOS attack occurs

6 Risk Management Language

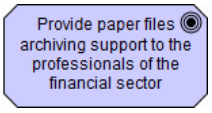
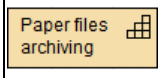
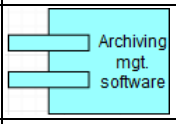
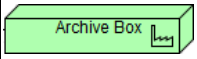
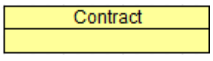
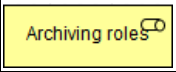
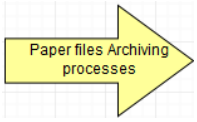
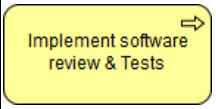
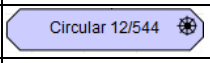
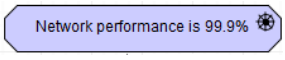
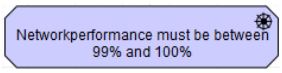
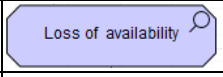
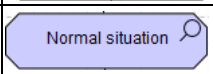
In [41], we have highlighted that, in general, risk analysis approaches lack from formal notation and representation, and that the traceability between the different elements of the risk model is also difficult to manage. To overcome these difficulties, we have proposed to extend the enterprise architecture model in the ArchiMate 2.0 modeling language [42] with the ISSRM [41]. Therefore, we have considered the business motivation model from ArchiMate, which we use through the ArchiMate motivation extension, for expressing the specific risk analysis related motivations for architecture principles and decisions. At the systemic level, in the previous sections of this article, we have explained how, at the metamodel level, it is possible to integrate the enterprise capability and resource with the systemic capability and resource, using the fractal approach from [4]. Than we have explained how to manage the risk at both levels using the risk model provided by ISO 31000:2009. At this level, no language exist yet for managing the risk. Given the mapping between the ISO standard and the BSE, the enterprise architecture language defined in ArchiMate 3.0 [43] may be extended at the systemic level.

Next sections illustrate how the ArchiMate risk extension language is usable for managing the risk at the enterprise and at ecosystem levels. In both cases, our approach is carried out in two stages. First, we design the domain model. Second, we model the risk-based on the domain model. The models represented with the ArchiMate language are illustrated in Figure 7 and Figure 8.

With the ArchiMate 2.0 version, it was not possible to directly express all the concepts from the risk model with concepts from the ArchiMate metamodel. For instance, the concept of business capability was not supported and therefore, we opted for the Business Function to represent it. With version 3.0 of the ArchiMate specifications, most of the concepts of BSE extended metamodel and of ISO 31000:2009 may be expressed (Table 1), including the capability and the resources that are defined respectively by *an ability that an active structure element, such as an organisation, person, or system, possesses* and *an asset owned or controlled by an individual or organisation*. Still in this alignment between the ArchiMate metamodel and the risk/BSE extended models some concepts are style not supported, such as the context. As a consequence, the five concepts introduced in the extended BSE for representing the context (i.e. *ContextSet, ContextElement, ContextElement Range, ContextElementValue and*

ContextSituation) will be represented by specialisations of two concepts from the ArchiMate motivation extension (i.e. the *driver* and the *assessment*).

Table 1. BSE metamodel-ArchiMate 3.0 metamodel alignment

	BSE metamodel element	Risk model (Cf. 16)	ArchiMate 3.0 metamodel element	Example	ArchiMate 3.0 metamodel element symbol
Goal	Goal		Goal	Provide paper files archiving support to the professionals of the financial sector	
Service	Service		Service	Store archives	
Capability	Capability		Capability	Paper files archiving	
Resource	Resource		Software	Archiving software	
			Location	Archive box	
			Business object	Contract	
			Role	Archiving roles	
			Process	Paper file archiving processes	
			Employee	Archive employee	
Control	Resource		Process	Implement physical protection of building	
Risk	Context set		Driver	Circular 12/544	
	Context Element		Driver	Network performance is 99.9%	
	Context Element Range		Driver	Network performance must be between 99% and 100%	
	Context Element value	Impact	Assessment	Loss of availability	
	Context Situation	Threat	Assessment	Normal situation	

The driver in ArchiMate *represents an external or internal condition that motivates an organisation to define its goals and implement the changes necessary to achieve them*. At the ISO 31000:2009 level, the context is defined, amongst other, as *the key drivers and trends having impact on the objectives of the organisation*. Therefore, we may consider that three concepts (namely: the context set, the context element, and the context element range) constitute elements necessary to define and implement the goal of a system and that they may be represented by specialisations of the driver concept from ArchiMate. Additionally, it's also worth to note that the drivers are logically appropriate to represent concepts existing at the design time of the system.

The assessment is defined in ArchiMate as *a representation of the result of an analysis of the state of affairs of the enterprise with respect to some driver*. At the CaaS level, the context element value and context situation are defined respectively as a value [of the context] at *a given run time situation and as a capture of the actual context during the system run time*. Therefore, we may consider that context element value and context situation constitute the result of an analysis of the context and that they may be represented by a specialisation of the assessment concept from ArchiMate. Equally to the driver, we also note that the assessments are logically representing concepts existing at the run time of the system.

6.1 Enterprise Risk Language

In Figure 7, the business model starts with a goal *provide paper file archiving support to the professionals of the financial sector* which is realised by *paper files archiving capabilities: identification & scheduling of resources, transportation, handling, and securing.*

Each capability groups a bunch of *enterprise resources* – abilities (processes, roles) and capacities (applications, infrastructures, equipment, business objects). *Paper files archiving processes* are high-level operational processes that orchestrate the delivery of the *paper files archiving services*. The value-added capabilities of the support-PFS are exposed to the world through the following services: *store archives:* ingest new document collections from the client; *access archives*: deliver and return a collection of archives to the client; and *dispose archive*: definitely return archives to the client.

Based on this business model, two risks are identified by *Lab Group* in regard to the context element range *Archives must be protected and available at 99.9%* included in the context set of circular 12/544. Risk1 is an information security risk related to the theft of archives and Risk2 is an operation risk related to software issues. Since a risk, according to ISO 31000:2009, is referred to an event and a consequence, we have for Risk1: *theft of media or documents* is an event that causes a *loss of integrity* (consequence) on the *securing* and *handling* capabilities. The chosen treatment is to reduce the risk through *the implementation of physical protection of building*. And Risk2: *software malfunction* is an event that causes a *loss of availability* (consequence) of the *paper files archiving capabilities*, thus, the *paper files archiving* services and consequently impacts all the clients of the support-PFS. The chosen treatment is to *reduce the risk through the implementation of software review and tests*. Both risk treatment requirements are realised through the capability *develop & manage business capabilities*.

6.2 Systemic Risk Language

In Figure 8, we define two business goals at the ecosystem level: stabilise the financial system, which is realised by the management of the systemic risk capability; and professionalise the financial system, which is realised by the client communication support capability. Put together, both capabilities realise high-level regulated support-PFS services. The management of the systemic risk capability requires a risk self-assessment service provided by the support-PFS and a risk-based supervision service provided by the regulator. The latter uses the risk assessment reference model produced by the LIST and used by all the support-PFS during their risk self-

assessment service. The client communication support capability requires, among others, paper file archiving services provided by the support-PFS.

In the frame of this sectorial ecosystem, one risk managed by the *CSSF* is identified in regard to the context element range *service must be available on a 24/7/365 basis* included in the context set of *circular 12/544*. In the risk model we identify a risk of insolvency of the support-PFS that comes with the event *loss of an important client* causes a *service unavailability* (consequence) of the regulated service for all the support-PFS clients. The chosen risk treatment is to reduce the risk through an *improved regulatory framework*, applicable to the ecosystem regulation capability.

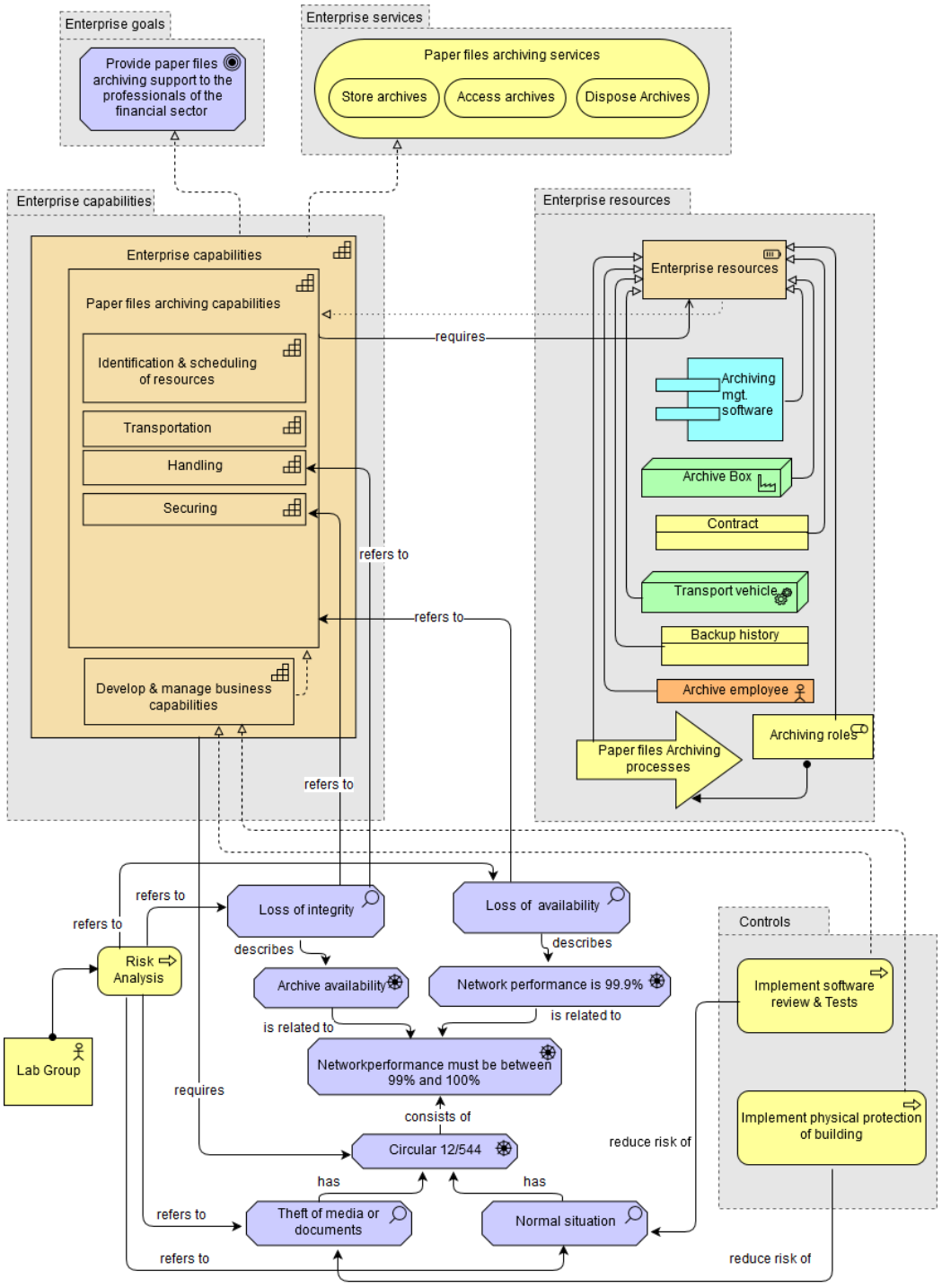


Figure 7. Use case: Paper files archiving services

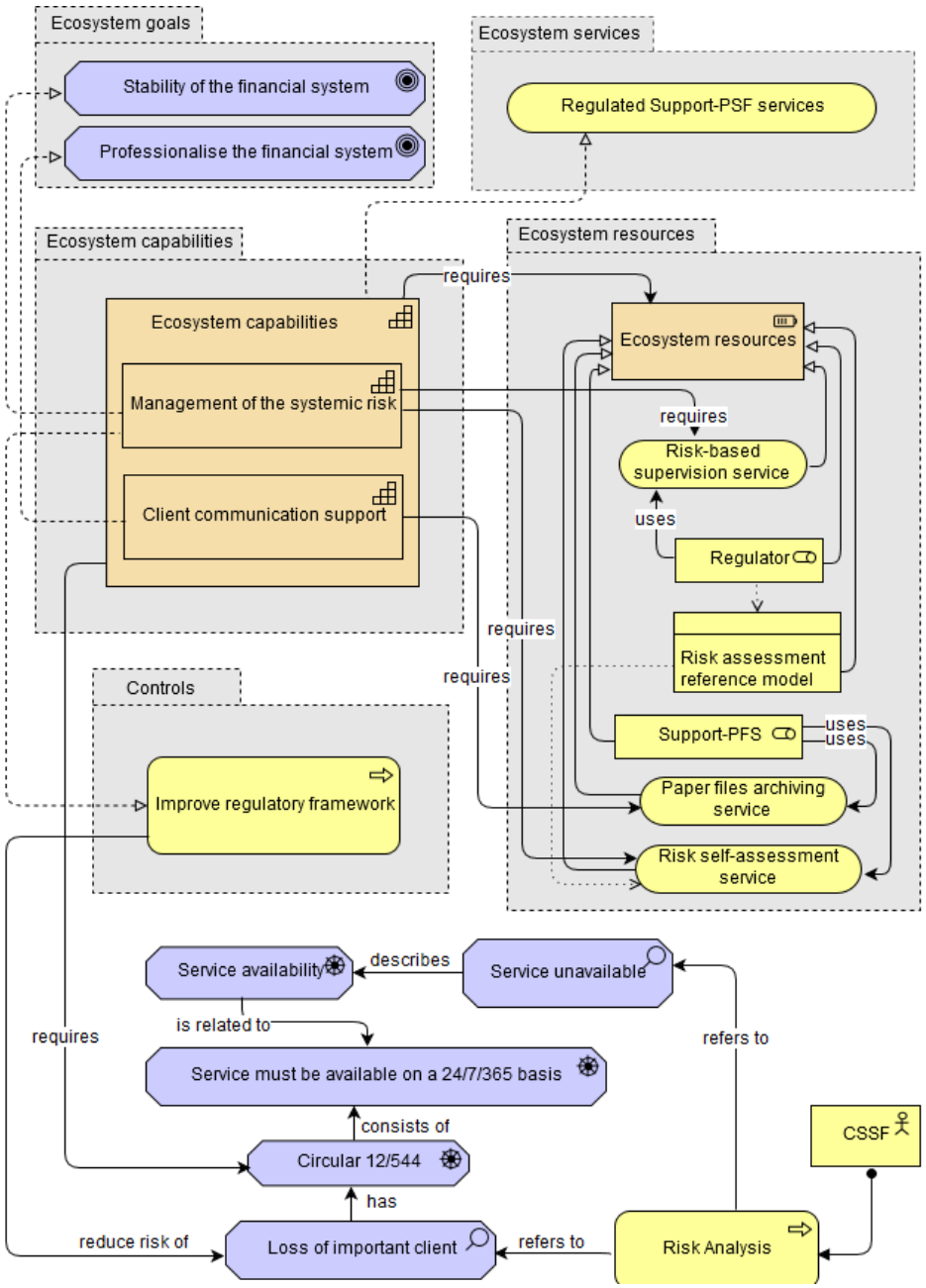


Figure 8. Use case: Regulated Support-PFS services

7 Conclusions and Future Works

In this article, we have conceptually extended a basic business service ecosystem model to address risk governance of regulatory ecosystems. In the first step, the concepts of the BSE presented in ASCDENCA 2015 [5] have been reviewed, along the three dimensions of the Capability as a Service (CaaS) metamodel: the Context, the Reuse and Variability, and the Enterprise Modeling.

According to a fractal approach, the capability-resource pair from Henkel et al. [14] has been reproduced at the ecosystem level and associated to the enterprise capability using the concept of business service. In the second step, the extended BSE has been used to address the risk governance of the regulatory ecosystem. An application case ran in the Luxembourgish financial sector has validated the approach, and has illustrated how the resulting model can be used to actually support risk governance. Finally, a security risk management extension of the

ArchiMate language has been defined to represent and support the design of risk governance in regulatory ecosystems.

This preliminary research opens the door to many interesting and new perspectives, which might be categorised as modeling concerns (related to the capability of the extended BSE metamodel to capture the elements of the ecosystem), and methodological concerns (related to the capability of the extended BSE to support specific usage).

7.1 Modeling Concerns

Many lessons have been learned from the implementation of risk-based frameworks in various economic sectors [44], amongst which the need to keep the framework simple and enable it for continual adjustments. We argue that our extended BSE provides the required elements to define a simple risk-based regulation framework: it abstracts the entities to the required capabilities and provided services, and captures the risks in term of contextual elements of the relevant capabilities. The BSE metamodel offers the possibility to gather in the same model: (1) the actors composing the ecosystem (e.g. enterprise, regulator) as well as the capabilities and services associated with their role; and (2) systemic information (e.g. systemic goal, capability, and services) relevant to support the informed governance of the ecosystem. It therefore represents a sound base for representing the structure of an ecosystem (economic sector, market) at a manageable level of abstraction.

At this stage, the extended BSE has been leveraged to represent a system subject to one regulator, i.e. a regulatory system. It could also be exploited to represent a system with many of regulatory bodies, therefore supporting the design of regulatory ecosystems. Through the instantiated concepts and relationship, the designed model can act as a vector for information sharing between the regulators at run time, as a foundation for understanding the intricacies associated with the complexity of regulatory ecosystems, as an instrument to improve the design of the regulatory objectives and responsibilities, and ultimately lead to what is known as better and smart regulation.

In this iteration, the extended BSE integrates the concepts required to manage risks. It could however be used to support other purposes, such as a better alignment between the services offered by the enterprises and the resources required by the system. The contextual part of the Capability can indeed be specialised to capture any element of context which is of concern for the ecosystem.

The BSE metamodel has been limited to the ecosystem level. It could also be extended outside the boundaries of the ecosystem to model how the ecosystem services are required by other (higher) system resources.

7.2 Methodological Concerns

The introduction of the context structure associated with capabilities brings a new knowledge area in risk management: the context modeling. This leads to expected improvements in the identification and assessment of regulatory risks. Context modeling is oriented towards the identification of the cause of the variability in a system, and the elicitation of the context elements is performed through an actual analysis of the variations [45]. Identifying risks closely relates to identifying potential variations sources (risk factors) and consequences (risk impact). Adopting techniques from context modeling knowledge base can be valuable to improve the elicitation of the risks to be considered at the ecosystem level.

The context structure can also be used as a vector to standardise the reporting of the regulated entities to the regulator body. In an attempt to understand how regulatory requirements and technology could come together through Regulatory Technologies (RegTech), the Financial Conduct Authority (FCA) has conducted a call for input to financial services firms, technology suppliers and FinTech start-ups. This has led to a report issued in July 2016 structuring the RegTech domain into four themes [37]: (1) Efficiency and Collaboration, i.e. technology that

allows more efficient methods of sharing information; (2) Integration, Standards and Understanding, i.e. technology that drives efficiency by closing the gap between intention and interpretation; (3) Predict, Learn, and Simplify, i.e. technology that simplifies data, allows better decision making and the creation of adaptive automation; (4) New Directions, i.e. technology that allows regulation and compliance processes to be looked at differently. In each theme, technologies and concepts are identified as source of potential benefits. The standardisation of regulatory requirements and rules is a pillar of the second theme, contributing to an increased coherence in the reporting mechanism. In BSE, the context structure is the recipient for capturing the variation of the Capabilities and can be used to express the regulatory information to be reported to the regulatory body, such as the level of risk associated with the enterprise capabilities. Associated with a reference model of the capabilities delivered by each business in the ecosystem, it becomes an instrument of standardisation of regulatory reporting.

In the same line, the BSE metamodel can support the selection of services/capabilities to meet specific quality (and security) needs. In previous research, a technique for assessing security risks associated with business services before deploying them in a multi-Cloud environment has been proposed and developed [46]: it supports the selection of the cloud offer that best fits the needs. This technique relies on a cloud security broker, which helps companies to deploy securely their service on a multi-Cloud environment. It leverages a specific model of capabilities and services, associated with concepts associated with security risk assessment (threat and vulnerability coverage, mitigation and consequence). The context structure associated with the Capability can be used to support this model, supporting the broker to match demand and offering in terms of contextual elements of a business service. The main advantage is that the broker only requires implementing one model to cover various contextual elements: it can support security objectives and risks, but also any other quality attribute defined as the context of the delivered Capability.

Rolling out the BSE metamodel to implement these risk-related methods requires technology to be adopted, so that both the model and the method are constrained to be used for what they have been designed. CaaS provides a technological environment supporting the Capability-Driven Design (CDD) methodology. The outcome of the integration of BSE with CaaS is that the CaaS-related technology could be leveraged to implement risk governance in regulatory ecosystems. The Capability Design Tool (CDT) provides capabilities for designing enterprise models, including concept models, and could be used at design time to specify the actual context associated with the capability. The CaaS technological architecture however also provides run time environment dedicated to the capture of context information from various sources, such as social network and application data, in order to support the design and monitoring of relevant context elements.

As a future work and respecting the existing capability for enterprise models design and the context information collecting environment described above, we view the integrated metamodel not only to serve as the basis for a potential new language extension to ArchiMate, but complementary, we understand that the BSE-Risk management mapping also drives, *de facto*, the management of the various parts of the model, in the way it is prescribed by megamodeling theory. Indeed, the latter expresses that a megamodel is a special kind of model, composed of models, which provides the holistic view on all the models of the system [47]. Megamodels could contribute to handle the context information from various sources, such as social network and application data as explained earlier. These megamodels have additionally been demonstrated as powerful instrument for system management and we plan to leverage it as an instrument to manage complex ecosystem environment determined by multiple regulators at the source of multiple risk-risk tradeoffs. In that regard, we are actually developing such as model management platform, enabling the run time execution of the models by facilitating the collection of the different parts of the integrated metamodel expressed in various languages, e.g. ArchiMate for the Enterprise Architecture model, Excel for catalogues of risks, threats and

vulnerabilities [48] and instantiated during concrete and real execution of risk assessments, e.g. security of internet payments analysis, internal audit or CERT[†] reports.

References

[1] R.F. Lusch and S. Nambisan, "Service Innovation: A Service-Dominant Logic Perspective," Mis Quarterly, vol. 39, no. 1, pp. 155–175, 2015.

[2] Y. Naudet, G. Wided and D. Chen, "Systems Science for Enterprise Interoperability," in Proc. Interoperability for Enterprise Software and Applications, China, IESA'09, International Conference on. IEEE, pp. 107–113, 2009. Available: https://doi.org/10.1109/i-esa.2009.57

[3] ISO 31000:2009, "Risk Management—Principles and Guidelines," Geneva, International Standards Organisation, 1st Edition, pp. 24, 2009. Available: https://www.iso.org/standard/43170.html

[4] H. Cholez and C. Feltus, "Towards an Innovative Systemic Approach of Risk Management," in Proc. the 7th ACM International Conference on Security of Information and Networks (ACM SIN 2014), Glasgow, United Kingdom, ACM New York, NY, USA pp. 61, 2014. Available: https://doi.org/10.1145/2659651.2659734

[5] C. Feltus, F.-X. Fontaine and E. Grandry, "Towards Systemic Risk Management in the Frame of Business Service Ecosystem," in Proc. 2nd International Workshop on Advances in Services DEsign based on the Notion of Capability (ASDENCA 2015), an International Workshop of the 27th Conference on Advanced Information Systems Engineering (CAISE2015), Sweden, Springer International Publishing, pp. 27–39, 2015. Available: https://doi.org/10.1007/978-3-319-19243-7_3

[6] 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 Proc. 20th European Conference on Software Process Improvement, Ireland, Springer Berlin Heidelberg, pp. 13–24, 2013. Available: https://doi.org/10.1007/978-3-642-39179-8_2

[7] CSSF, "Circulaire CSSF 12/544, Optimisation of the Supervision Exercised on the "Support PFS" by a Risk-Based Approach," Circular CSSF, pp. 38, 2012. Available: http://www.cssf.lu/fileadmin/files/Lois_reglements/Circulaires/Hors_blanchiment_terrorisme/cssf12_544eng.pdf

[8] L. Rafati and G. Poels, "Capability Sourcing Modeling – A High-Level Conceptualisation Based on Service-Dominant Logic," in Proc. 1st International Workshop on Advances in Services DEsign based on the Notion of Capability (ASDENCA 2014), an International Workshop of the 26th Conference on Advanced Information Systems Engineering (CAISE2014), Springer International Publishing, pp. 77–87, 2014. Available: https://doi.org/10.1007/978-3-319-07869-4_7

[9] S. España, T. González, J. Grabis, L. Jokste, R. Juanes and F. Valverde, "Capability-Driven Development of a SOA Platform: A Case Study," in Proc. 1st International Workshop on Advances in Services DEsign based on the Notion of Capability (ASDENCA 2014), an International Workshop of the 26th Conference on Advanced Information Systems Engineering (CAISE2014), Greece, Springer International Publishing, pp. 100–111, 2014. Available: https://doi.org/10.1007/978-3-319-07869-4_9

[10] K. Sandkuhl and H. Koç, "On the Applicability of Concepts from Variability Modelling in Capability Modelling: Experiences from a Case in Business Process Outsourcing," in Proc. 1st International Workshop on Advances in Services DEsign based on the Notion of Capability (ASDENCA 2014), an International Workshop of the 26th Conference on Advanced Information Systems Engineering (CAISE2014), Springer International Publishing, pp. 65–76, 2014. Available: https://doi.org/10.1007/978-3-319-07869-4_6

[11] J. Stirna, "Capability as a Service in Digital Enterprises," position presentation at "Digital Business Innovation Paths" Event – How to take Digital Business Innovation to the next level?, Brussels, Belgium, July 8, 2014. Available: http://www.futureenterprise.eu/groups/iii-capability-service-digital-enterprises

[12] J. Stirna and K. Sandkuhl, "An Outlook on Patterns as an Aid for Business and IT Alignment with Capabilities," in Proc. 1st International Workshop on Advances in Services DEsign based on the Notion of Capability (ASDENCA 2014), an International Workshop of the 26th Conference on Advanced Information Systems Engineering (CAISE2014), Springer International Publishing, pp. 148–158, 2014. Available: https://doi.org/10.1007/978-3-319-07869-4_13

[†] Computer emergency response team – http://www.cert.org/.

[13] H. Koç and K. Sandkuhl, "A Business Process Based Method for Capability Modelling," in Proc. International Conference on Business Informatics, Springer International Publishing, pp. 257–264, 2015. Available: https://doi.org/10.1007/978-3-319-21915-8_17

[14] M. Henkel, I. Bider and E. Perjons, "Capability-Based Business Model Transformation," in Proc. 1st International Workshop on Advances in Services DEsign based on the Notion of Capability (ASDENCA 2014), an International Workshop of the 26th Conference on Advanced Information Systems Engineering (CAISE2014), Greece, Springer International Publishing, pp. 88–99, 2014. Available: https://doi.org/10.1007/978-3-319-07869-4_8

[15] C.E. Helfat and S.G. Winter, "Untangling Dynamic and Operational Capabilities: Strategy for the (N)ever-Changing World," Strategic management journal, vol. 32, no. 11, pp. 1243–1250, 2011. Available: https://doi.org/10.1108/sd.2012.05628caa.005

[16] D.J. Teece, G. Pisano and A. Shuen, "Dynamic Capabilities and Strategic Management," Strategic Management Journal, vol. 18, no. 7, pp. 509–533, Aug. 1997. Available: https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z

[17] M. Rosen, "Are Capabilities Architecture?," BPTrends, pp. 4, 2013. Available: http://www.bptrends.com/bpt/wp-content/publicationfiles/02-05-2013-COL-BA-Are%20Capabilities%20Arch.pdf

[18] TSF, "Taking Service Forward". Available: http://takingserviceforward.org

[19] J.B. Barney, "Gaining and Sustaining Competitive Advantage," Reading, MA, Addison-Wesley, pp. 570, 1997.

[20] J.F. Moore, "Predators and Prey: A New Ecology of Competition," Harvard Business Review, pp. 12, May/June 1993. Available: https://hbr.org/1993/05/predators-and-prey-a-new-ecology-of-competition

[21] S.L. Vargo, R.F. Lusch, "Evolving to a New Dominant Logic for Marketing," Journal of Marketing, vol. 68, no. 1, pp. 1–17, 2004. Available: http://dx.doi.org/10.1509/jmkg.68.1.1.24036

[22] S. Alter, "Metamodel for Service Design and Service Innovation: Integrating Service Activities, Service Systems, and Value Constellations," in International Conference on Information Systems (ICIS), Shanghai 2011, Service Science, pp. 1–20, 2011.

[23] P.P. Maglio, S.L. Vargo, N. Caswell and J. Spohrer "The Service System is the Basic Abstraction of Service Science," Information Systems and e-Business Management, vol. 7, no. 4, pp. 395–406, 2009. Available: https://doi.org/10.1007/s10257-008-0105-1

[24] S. Berzisa, G. Bravos, T. Gonzalez, U. Czubayko, S. España, J. Grabis, M. Henkel, L. Jokste, J. Kampars, H. Koç, J.-C. Kuhr, C. Llorca, P. Loucopoulos, R. Juanes, O. Pastor, K. Sandkuhl, H. Simic, J. Stirna, F. Valverde and J. Zdravkovic, "Capability Driven Development: An Approach to Designing Digital Enterprises," Business & Information Systems Engineering, vol. 57, no. 1, pp. 15–25, 2015. Available: https://doi.org/10.1007/s12599-014-0362-0

[25] CaaS – Capability as a Service for Digital Enterprises. Available: http://caas-project.eu/definitions/

[26] J. Zdravkovic, J. Stirna, M. Henkel and J. Grabis, "Modeling Business Capabilities and Context Dependent Delivery by Cloud Services," in Proc. Advanced Information Systems Engineering 2013, Springer Berlin Heidelberg, pp. 369–383, 2013. Available: https://doi.org/10.1007/978-3-642-38709-8_24

[27] J. Stirna, J. Zdravkovic, M. Henkel and J. Kampars, "Capability Patterns as the Enablers for Model-Based Development of Business Context-Aware Applications," in Proc. CBI-CP-2015 (TEE 2015, CoBI 2015, XOC-BPM 2015) Complementary Proceedings of the Workshops TEE, CoBI, and XOC-BPM at IEEE-COBI 2015, vol. 1408, 2015.

[28] G. Bravos, P. Loucopoulos, C. Stratigaki and D. Valvis, "An Empirical Evaluation of Capability Modelling Using Design Rational," in Proc. 1st International Workshop on Capability-oriented Business Informatics (CoBI 2014), Geneva, Switzerland, 2014.

[29] A. Rifaut, C. Feltus, "Improving Operational Risk Management Systems by Formalizing the Basel II Regulation with Goal Models and the ISO/IEC 15504 Approach," in Proc. Regulations Modelling and their Validation & Verification (REMO2V'2006), an International Workshop of the 18th Conference on Advanced Information Systems Engineering (CAISE2006), Grand-Duchy of Luxembourg, pp. 831–837, 2006.

[30] B.M. Hutter, "The Attraction of Risk-Based Regulation: Accounting for the Emergence of Risk Ideas in Regulation," Centre for Analysis of Risk and Regulation, London School of Economics and Political Science. vol. 33, 2005.

[31] T. Blair, Speech on Compensation Culture, delivered at Public Policy Research Thinktank, May 2005. Available: https://www.theguardian.com/politics/2005/may/26/speeches.media

[32] J.B. Wiener, "Risk Regulation and Governance Institutions," OECD Reviews of Regulatory Reforms, Risk and Regulation Policy: Improving the Governance of Risk, pp. 133–157, 2011. Available: https://doi.org/10.1787/9789264082939-9-en

[33] N. Mayer, P. Heymans and R. Matulevicius, "Design of a Modelling Language for Information System Security Risk Management," in Proc. International Conference on Research Challenges in Information Science, pp. 1–11, IEEE, 2007.

[34] R. Lofstedt and A. Schlag, "Risk-Risk Tradeoffs: What Should We Do in Europe?," Journal of Risk Research, pp. 1–21, 2016. Available: https://doi.org/10.1080/13669877.2016.1153505

[35] M.B.A. van Asselt and O. Renn, "Risk Governance," Journal of Risk Research, vol. 14, no. 4, pp. 43–449, 2011. Available: http://dx.doi.org/10.1080/13669877.2011.553730

[36] O. Renn, A. Klinke and M. van Asselt, "Coping with Complexity, Uncertainty and Ambiguity in Risk Governance: A Synthesis," Ambio, vol. 40, no. 2, pp. 231–246, 2011. Available: https://doi.org/10.1007/s13280-010-0134-0

[37] Financial Conduct Authority, "Feedback Statement – Call for Input on Supporting the Development and Adopters of RegTech," July 2016. Available: https://www.fca.org.uk/publications/feedback-statements/fs16-4-feedback-statement-call-input-supporting-development-and

[38] A. Klinke and O. Renn, "Risk Governance: Contemporary and Future Challenges," Regulating Chemical Risks: European and Global Challenges, Springer, pp. 9–27, 2010. Available: https://doi.org/10.1007/978-90-481-9428-5_2

[39] United Nations Economic Commission for Europe (UNECE), "Risk Management in Regulatory Frameworks: Towards a Better Management of Risks," United Nations, New York and Geneva, pp. 122, 2012. Available: http://www.unece.org/fileadmin/DAM/trade/Publications/WP6_ECE_TRADE_390.pdf

[40] B. Chew, D. Derosby, E. Kelly and B. Miracky, "Regulating Ecosystems," Part of the Business Trends series, Deloitte University Press, 2015.

[41] E. Grandry, C. Feltus and E. Dubois, "Conceptual Integration of Enterprise Architecture Management and Security Risk Management," in Proc. 5th Workshop on Service oriented Enterprise Architecture for Enterprise Engineering (SoEA4EE'2013), an International Workshop of the 17th IEEE, pp. 114-123, 2013. Available: https://doi.org/10.1109/EDOCW.2013.19

[42] The Open Group, "ArchiMate 2.0 Specification". Available: http://pubs.opengroup.org/architecture/archimate2-doc/

[43] The Open Group, "ArchiMate 3.0 Specification". Available: http://pubs.opengroup.org/architecture/archimate3-doc/

[44] J. Black, "Risk-Based Regulation: Choices, Practices and Lessons Being Learnt," OECD Reviews of Regulatory Reforms, Risk and Regulation Policy: Improving the Governance of Risk, pp. 185–224, 2010. Available: https://doi.org/10.1787/9789264082939-11-en

[45] H. Koç, "A Context Modelling Method to Enhance Business Service Flexibility in Organisations," in Proc. Short and Doctoral Consortium Papers, 8th IFIP WG 8.1 Working Conference on the Practice of Enterprise Modelling (PoEM 2015), pp. 91–98, 2015.

[46] E. Goettelmann, K. Dahman, B. Gâteau, E. Dubois and C. Godart, "A Security Risk Assessment Model for Business Process Deployment in the Cloud," IEEE International Conference on Service Computing, IEEE SCC 2014. Available: https://doi.org/10.1109/scc.2014.48

[47] M. Barbero, F. Jouault and J. Bézivin, "Model Driven Management of Complex Systems: Implementing the Macroscope's Vision," Engineering of Computer Based Systems (ECBS 2008), 15th Annual IEEE International Conference and Workshop on, IEEE, 2008. Available: https://doi.org/10.1109/ECBS.2008.42

[48] J.S. Sottet and N. Biri, "JSMF: a Javascript Flexible Modelling Framework," FlexMDE@MoDELS 2016, pp. 42–51, 2016.