Towards Systemic Risk Management in the Frame of Business Service Ecosystem

Christophe Feltus(✉), François-Xavier Fontaine, and Eric Grandry

Luxembourg Institute of Science and Technology,
5 Avenue des Hauts-Fourneaux, 4362 Esch-sur-Alzette, Luxembourg
{Christophe.Feltus,Francois-Xavier.Fontaine,
Eric.Grandry}@list.lu

Abstract. Ecosystems gather enterprises which collaborate to achieve a common systemic goal like guaranteeing the national healthcare, the telecommunication, or the financial stability. These systems are governed by regulators that supervise the services provided at the ecosystem level using systemic capabilities and resources. In the same way at the enterprise level, risk management at the ecosystem level is a paramount activity for the stability of the targeted sector. This paper proposes a metamodel for modelling the ecosystem capabilities and resources, a risk management approach based on this metamodel, and an ArchiMate extension language to sustain the systemic risk management. The approach is illustrated with a real case study from the Luxembourgish financial market.

Keywords: Capability · Systemic risk · Resource · Business service · Regulation

1 Introduction

Today's enterprises are interconnected and form an ecosystem of interdependent entities delivering value-added products to their customers. As a service economy, Luxembourg is hosting many business service ecosystems, which are interconnected and constitute a constellation of entities delivering services: let's consider the financial ecosystem formed of financial service providers (PFS) and support service providers (Support-PFS), connected to infrastructure and telecommunication ecosystem formed of data centres and telecommunication service providers. Since the Luxembourgish environment is characterised by high-level of costs in terms of HR, buildings and infrastructure, Luxembourg-based service providers can only differentiate their service offering in terms of qualities such as performance, compliance and security rather than their price. The global IT strategy of Luxembourg (Digital Lëtzebuerg) is aligned with this view and aims at positioning Luxembourg as a safe data hub, where compliance and information security are core enabling properties.

In order to increase trust in the business service ecosystems, national regulators are appointed to supervise and control the compliance of the participating actors with the regulation. As such, the regulator is part of the business service ecosystems, as it is responsible for the compliance of the delivered services. The added-value of the

A. Persson and J. Stirna (Eds.): CAiSE 2015 Workshops, LNBIP 215, pp. 27–39, 2015.
DOI: 10.1007/978-3-319-19243-7_3

regulator in the ecosystem is therefore to transform business services into regulated business services, through additional services and controls. As an ecosystem is usually a complex system (many elements and many interactions), risk management is a mean exploited by the regulator to control specific aspects of the ecosystem: the *Institut Luxembourgeois de Régulation* (http://www.ilr.lu), regulating the telecommunication ecosystem, imposes that each telecommunication service provider performs a security risk analysis to guarantee the availability of their networks. To date, regulators require that appropriate risk management activities are performed by each organisation. In the future, the regulator will also focus their attention on the risks at the level of the ecosystem, the systemic risk. In this paper we investigate how the concept of capability can be leveraged to drive risk analysis at the ecosystem level.

After a review of the concept of capability, in the next section, we present our metamodel of a Business Service Ecosystem (BSE) in Sect. 3, and we demonstrate how this metamodel perfectly supports systemic risk analysis in Sect. 4. We propose a systemic risk management language for expressing the BSE metamodel at the enterprise and at the systemic level, based on an ArchiMate extension, in Sect. 5, and we conclude the paper in Sect. 6. Our approach is illustrated with a use case that has been run in a project with the national regulator of the financial System.

2 State of the Art

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 [10].

The CaaS project has defined a Capability metamodel [1, 2, 6, 7]. This metamodel gathers elements from three domains: the context, the enterprise modelling, and the reuse and variability dimension [2]. At the CaaS metamodel level, the Capability is defined as *the ability of an organization to manage its resources to accomplish a task* [4] and *as the ability and capacity that enables an enterprise to achieve a business goal in a certain context* [7]. This context represents the *characterisation of a solution in which the capability should be provided* [1]. 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 [3]) and the dynamic capability (enabling a firm adaption to rapidly and discontinuously changing external environments [5]). [3] 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 organizational capability implies that the organization has the capacity to perform a particular activity in a reliable and at least minimal satisfactory manner. This organizational capability is equivalent to the main capability as expressed by [4]. The goal (that requires capabilities), as defined in CaaS, may be of five types according to [1]: *Strategic, Business, Technical, Design time and Run-time,* and therefore they may be achieved by dynamic or organizational capabilities. [14] considers that a capability is composed of *capacity*: resources (e.g. money, time, staff, tools) for delivering the capability, and *ability*: competence (e.g. talent,

intelligence and disposition), skills, processes. For [14], capabilities are of three types: *strategic, value-added, commodity*. According to [13], the capability is an *ability to perform* that requires *investment of time and effort*. [13] also considers the resources as an element which *can be bought* or *easily acquired*. An explanation of resource is proposed by [10] which consider it as the *assets that organization 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) [11].

Reference [4] proposed an approach to support business transformations based on capability. It assumes that an enterprise consists in any organization that generates operation activities funded by stakeholders that do not work for the enterprise. This organization has the capability to produce value for external entities (like customers in case of private organizations or citizens in the case of public ones) in exchange of money. In this context, [4] suggests structuring the organizations 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 are called sub-capabilities. To uncover the structure of an organization regarding these capability-resource patterns, [4] has 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 patterns constitutes a fractal organization which supports the achievement of organizational and dynamic goals from the business layer of the organization down to the supporting layers. According to [6], this pattern also aggregates process variants, which are themselves specialisations of processes. The variability in capability modelling allows facing the rapidly changing environment in companies. Therefore [6] 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 Business Service Ecosystem Metamodel

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

In [4], the authors explain that *any organization 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 specialization of an enterprise too, provided that this ecosystem has a specific and well dedicated goal (for instance, the goals of a financial ecosystem is to guarantee the delivery of highly secured financial products). To achieve its goals, the ecosystem gets money from external stakeholders (e.g. the customers paying for the financial products, the state injecting money to stabilize the financial). In exchange, the ecosystem produces high value for its beneficiaries (guarantee the performance of the financial activities at the national level). To deliver this value, the ecosystem uses capabilities at the ecosystem

level. These capabilities are amongst others, the capability to regulate the system, the capability to support core activities (archiving, control, etc.)

Given the similarity between the enterprise structure and the ecosystem structure, we propose to extend the fractal organization approach proposed by [4] and raising the capability-resource pattern from the enterprise level (pattern B of Fig. 1) up to the ecosystem level (pattern A). This allows elaborating what we have named the Business Service Ecosystem (BSE) metamodel where the (main) capability of the entire system is the ecosystem capability and where the resources of the ecosystem are derived from the ecosystem enterprises capability.

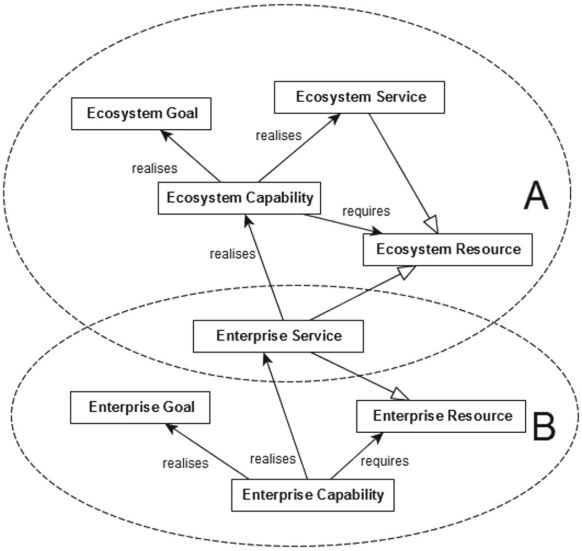

Fig. 1. Business Service Ecosystem metamodel

The Systemic Capability metamodel relies on three concepts: resource, capability and goal. These elements have already been defined in the CaaS metamodel and we have decided to keep their definitions unchanged, namely: the Capability is *the ability and capacity that enable an enterprise to achieve a business goal in a certain context* [7]. Given patterns 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 organization has or can call upon* [10]. At the ecosystem level, a resource may consist of a set of employees that manage the ecosystem (like the regulators) and at the enterprise level, it could consist, e.g. in a financial asset management software. The goal *is a desired state of affairs that needs to be obtained* [1]. 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. A specialization of the resource has been represented in Fig. 1 and consists in the enterprise service.

The enterprise services have been defined as *acts performed for others, including the provision of resources that others will use* [18]. As a result, it is a type of behaviour that allows an enterprise's goal to be realized and that requires enterprise 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 [13], 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, to be friendly offered outside the perimeter of the enterprise, the resources are organised in services. As a result, the latter constitutes a hyphen between the enterprise capability and the ecosystem resource and hence, a common element to both patterns 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 another capability of the same institution. 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.

4 Systemic Risk Management

The capability-driven approach for modelling 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 (ISSRM) and apply it at both levels (A and B) of the BSE metamodel of Fig. 1. This alignment between the metamodels is illustrated with the following case:

Since mid-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. The ecosystem related to this collaboration is partially represented in Fig. 3 which models two specific actors of the sector (CSSF and Lab Group) following the BSE metamodel. The CSSF is a specific type of enterprise with a regulator goal to regulate the ecosystem. Hence, it is a public institution which supervises the professionals and products for the financial sector. To reach this goal, the CSSF regulates the enterprises that compose this 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 [15]. As part of its mission, the CSSF has several objectives: promoting a considered and prudent business policy in compliance with the regulatory requirements; protecting the financial stability and of the financial sector; supervising the quality of the organisation and internal control systems; and strengthening the quality of risk management.

Lab Group (http://www.labgroup.com) is a financial sector professional that supports the financial sector. One characteristic of the Support-PFS (like Lab group) is that they do not exercise a financial activity themselves, but act as subcontractors of operational functions on behalf of other financial professionals. Lab Group is a CSSF certified document and data management company, with offices in Luxembourg, Dublin and Gibraltar. On 18 July 2012, the CSSF published the circular 12/544 [15], which imposes the Support-PFS's to perform risk self-assessments and provide the CSSF with the risk analysis reports. Because of the low quality in risk reports, the CSSF has decided to produce a risk reference model to be used in the self-assessment exercise. The LIST has been charged with designing this reference model.

4.1 ISSRM

In the ISSRM [12], a risk is composed of event and impact and it occurs when the first leads to the second. The event is in itself composed of threat and vulnerability and equally exists when the first leads to the second. The impact harms an asset of the enterprise which may be of a resource type or business asset. The resource is the target of the threat and is characterized by vulnerability. We have voluntarily simplified the ISSRM in order to focus on the most significant concepts and relationships among concepts. The cardinalities have also been removed, for the same reasons. Fig. 2 shows the mapping between the ISSRM and BSE metamodel at the systemic level and at the enterprise level.

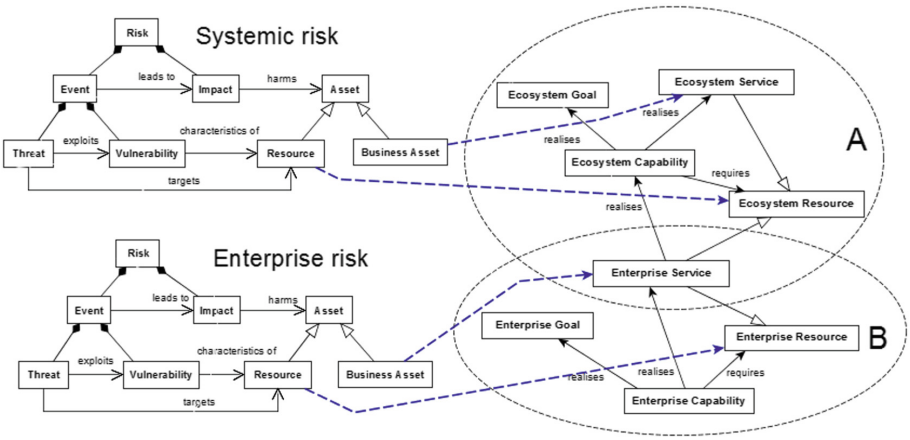

Fig. 2. Mapping ISSRM – BSE metamodel

4.2 Mapping ISSRM-Business Service Ecosystem Metamodel

This section explains the mapping between the ISSRM and the BSE metamodel illustrated by the financial system (Fig. 3). The ecosystem goals are to *professionalise the financial system* and to *stabilise the financial system*.

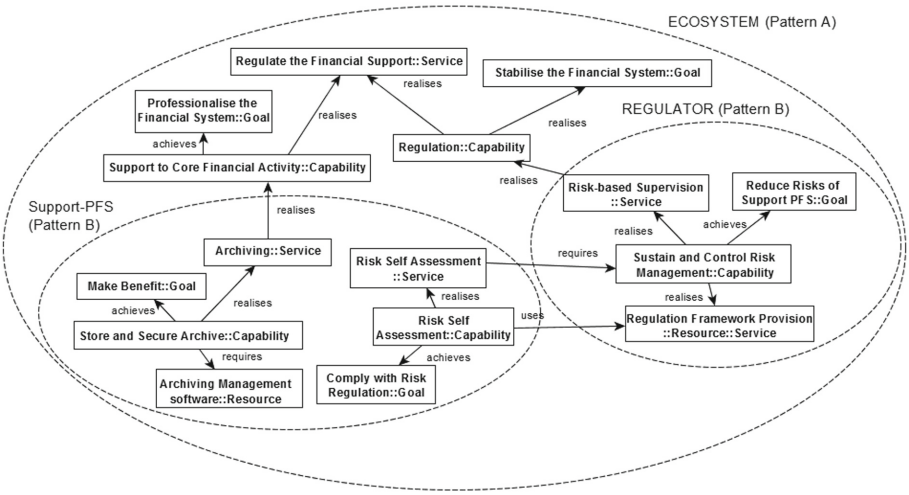

Fig. 3. Business Service Ecosystem metamodel instantiated to the financial system

At the enterprise level, the risk analysis is achieved by depicting the resource's vulnerability, the threat that exploits this vulnerability and the assets that are impacted by the risk occurrence. For instance, the *archiving management software* (resource) of the Support-PFS does not use the security module (vulnerability) and the heap buffer overflow attack (threat) risks to be led. This even makes a hacker able to corrupt (impact) the archiving service (business asset).

This structured and "classical" way of managing the IS risk may be investigated following the capability-resource pattern approach. The concept of resource is defined in ISSRM as a component of the IS which supports business assets. It is also named an IS asset and corresponds, for instance, to the a*rchiving management software*. The concept of capability from the BSE model (pattern B of Fig. 1) is composed of resources and corresponds to the concept of resource from the ISSRM model presented in Fig. 2. According to the above financial case, we argue that the enterprise capability to *store and secure archives* is composed of the *archiving management software* (resource) and that this enterprise capability is required for the *archiving service* which is an enterprise service (business asset). This correspondence between the ISSRM and the capability-resource pattern model highlights how using the capability-resource pattern at the sectorial level helps identifying the resources and capabilities that achieve business services. These resources and capabilities are thus the ones to be considered during the risk management activity.

At the ecosystem level, in [8, 9], we have observed that a structured way does not yet exist for managing the risks and that, on the spot, sectorial risk analysts often make the amalgam between the enterprise resources and capabilities, and the sectorial resources and capabilities. In the following, we argue and explain how using the capability-resource pattern approach contributes in structuring the analyst's approach. Therefore, we consider the correspondence between the ISSRM and the capability-resource pattern model but, this time, at the ecosystem level. The concept of business

asset, at the ecosystem level, represents a service provided by the ecosystem. To realise this ecosystem service, the ecosystem requires ecosystem capabilities. According to the pattern based fractal structure of the ecosystem proposed in Fig. 1, the latter aggregates ecosystem resources and enterprise's services, i.e. the enterprise service from pattern B corresponds to a type of ecosystem resource at pattern A. For instance, in a financial sector, at the ecosystem level, the ecosystem must *regulate the financial support*. To justify this ecosystem service to the government, the ecosystem must have the r*egulation capability* and the s*upport to core financial activity capability*. These capabilities are realized respectively by the r*isk-based regulation service* and by the *archiving service*. Both of these services are also types of ecosystem resource.

To analyze the risk of not being able to *Professionalize the financial system* and to *Stabilize the financial system* (ecosystem goal) as well as, not being able to deliver (impact) the *regulation of the financial support* ecosystem service (business asset), the risk analysis assesses the threats that might exploit vulnerabilities of the ecosystem capabilities (types of resource at the ISSRM level). This means, in the financial system case, that the Support-PFS does no longer provide the archiving or that the CSSF does no longer provide the regulation.

This correspondence between the ecosystem capability-resource pattern model and the ISSRM shows that, at the ecosystem level, the right abstraction for risk management is the enterprise service (regulator or support-PFS services). This implies that the main focus of the risk analysis, at the sectorial regulation level, is the ecosystem services and ecosystem capabilities, including the ecosystem resources and enterprises services. Thereby, the risk management at the enterprise level in not an activity to be handled and performed by the ecosystem, but an activity that is enforced by the latter. In practice, this risk management activity is sub-contracted from the ecosystem (represented, e.g. by the state) to the ecosystem regulator (often a publicly financed body). In that sense, the regulator may impose rules to be followed by the enterprise such as the legal obligation to make risk analysis and to report annually, and may control rules which are applied and sanction accordingly.

A second consequence of this abstraction of the risk analysis, at the ecosystem level, is related to the counter-measures to be put in place to mitigate the risk. Given that the risk mitigation is at the enterprise service level, the vulnerability and the threat must also be considered at this ecosystem level. For instance, a service vulnerability could be that the enterprise is not able to deliver the service anymore in case of workload increase and a threat could be a sudden workload increase. Practically, an insurance cannot reimburse all the insured (vulnerability) in case of a major disaster due to exceptional conditions (threat). This involves, at the ecosystem level, that the ecosystem service to assure all inhabitants of a country (business asset) is no longer possible.

5 Risk Management Language

In [16], we have highlighted that, in general, risk analysis approach lacks 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 modelling language [17] with the ISSRM. 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 paper, 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 ISSRM. At this level, no language exist yet for managing the risk. Given the mapping between the ISSRM and the BSE, the risk management language defined in [16] 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 (Sect. 4.1, Fig. 3). Second, we model the risk based on the domain model. The models represented with the ArchiMate Language are illustrated in Figs. 4 and 5. Practically, since the concept of business capability is not supported by ArchiMate we opted for the Business Function to represent the Capabilities. A business function is indeed defined by

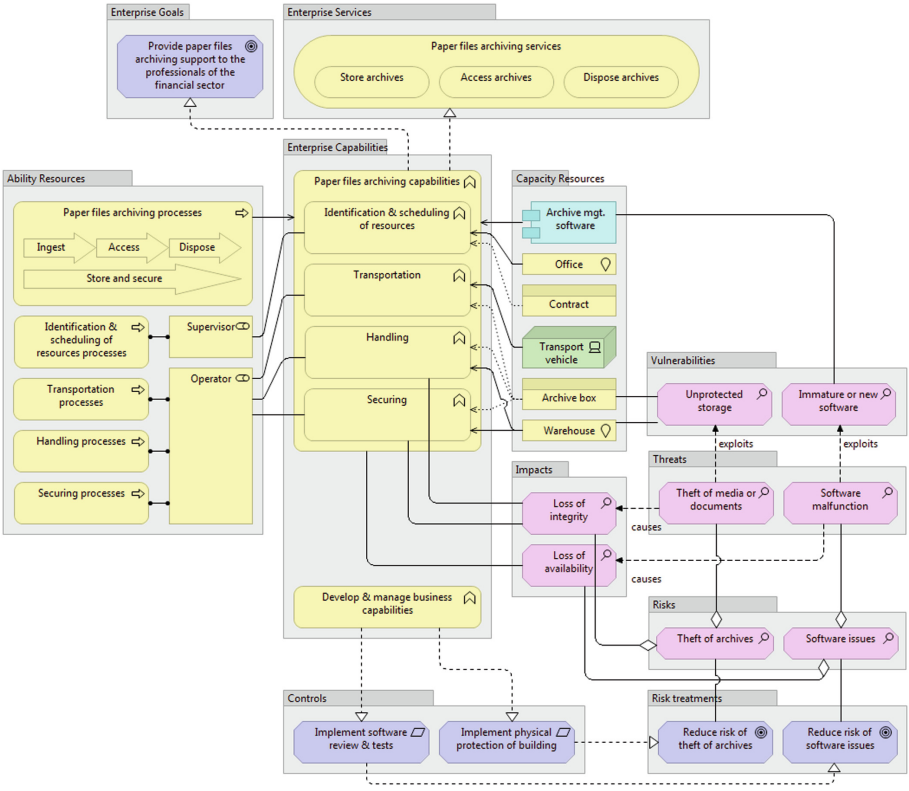

Fig. 4. Use case: Paper files archiving services

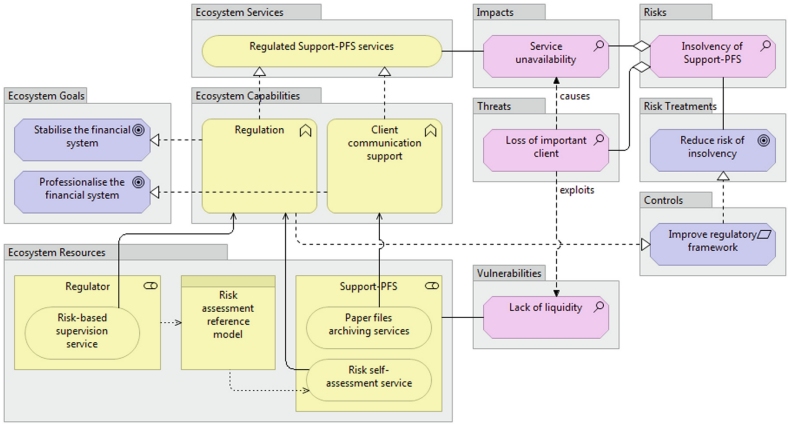

Fig. 5. Use case: Regulation Regulated Support PFS services

ArchiMate as *a behavior element that groups behavior based on a chosen set of criteria (typically required business resources and/or competences)*. The language will probably integrate the concept of Capability in the future, according to current works at The Open Group.

5.1 Enterprise Risk Language

In Fig. 4, 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*, *securing*. Each capability groups a bunch of abilities (processes, roles) and capacities (applications, infrastructures, equipment, business objects). *Paper files archiving processes* are high-level operational processes that orchestrate the delivery of services. The roles of *Supervisor* and *Operator* are defined by the ability for performing specific behaviour (processes, activities) and they may be assigned to actors (capacity resources). The value-added capabilities of the Support-PFS are exposed to the world through *paper files archiving 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 we have identified two risks. Risk1: *Theft of archives* (information security) and Risk2: *Software issues* (operational). Since a risk is composed of threats, vulnerabilities and impacts we have for Risk1: *theft of media or documents* (threat) exploits vulnerability of *unprotected storage* (warehouse and archive box) and causes a *loss of integrity* (impact) on the *securing* and *handling* capabilities. The chosen treatment is to reduce the risk through *the implementation of physical protection of building*. And for Risk2: *software malfunction* (threat) exploits vulnerabilities of *immature or new software* (archive management software component) and causes a *loss of availability* (impact) 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*.

5.2 Systemic Risk Language

In Fig. 5 we define two business goals at the ecosystem level: *Stabilise the financial system*, which is realised by the *regulation* 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 regulation capability requires a *risk self-assessment service* provided by the *Support-PFS* and a *risk-based supervision service* provided by the r*egulator*. 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* requires, among others, *paper file archiving services* provided by the *Support-PFS.*

In the risk model we identify a risk of *insolvency of the Support-PFS* that comes with the threat *loss of an important client*. That threat exploits the vulnerability of *lack of liquidity*. The impact is *service unavailability* 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.

6 Conclusions and Future Works

In this paper, we have investigated how the capability may contribute in sustaining the risk management at the system level. To that end, our first contribution is a BES metamodel built from the capability-resource pattern from [4] that we have reproduced at the systemic level and associated to the enterprise capability through the service. Secondly, the ISSRM has been mapped with the BSE metamodel. This mapping has been illustrated on the basis of a case study for the Luxembourgish financial sector. Finally, we have exploited the security risk management extension of the ArchiMate language to represent and sustain the risk management at the ecosystem level.

This preliminary research paves the way to many interesting and new perspectives. Firstly the BSE metamodel may gather in the same model (1) all the actors of a system (e.g. enterprise, regulator) and (2) systemic information (e.g. systemic goal, capability and services). Secondly, this approach has been exploited in the frame of risk management but it could be extended to other purposes, e.g. better alignment between the services offered by the enterprises and the resources needed by the system. Thirdly, it has been illustrated in a system with one regulator but it could be extended to system with many regulators and hence, acts as a facilitator for information sharing between these regulators. Fourthly, 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 is required by other (higher) system resources.

The first future work consists in more accurately aligning the BSE and the ISSRM. This will be performed using appropriate methods like those proposed by [18] or [19]. The second future work aims at deepening the role of the service as a hyphen between both levels. We consider that some systemic resources are the services provided by the entities of the ecosystem, while others might be actual shared resources. The question is to know if in a service ecosystem, all ecosystem resources are services provided by some entities: a shared network considered as a common resource for the ecosystem, is operated by some entity, whether public or private, and therefore can be seen from the service provision perspective as well. An alignment with service system theories will be considered in order to address this question.

References

1. España, S., González, T., Grabis, J., Jokste, L., Juanes, R., Valverde, F.: Capability-Driven Development of a SOA Platform: A Case Study. In: Iliadis, L., Papazoglou, M., Pohl, K. (eds.) CAiSE Workshops 2014. LNBIP, vol. 178, pp. 100–111. Springer, Heidelberg (2014)
2. Stirna, J.: 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? Belgium, 8 July 2014
3. Helfat, C.E., Winter, S.G.: Untangling dynamic and operational capabilities: strategy for the (n)ever-changing world. Strat. Mgmt. J. **32**(11), 1243–1250 (2011)
4. Henkel, M., Bider, I., Perjons, E.: Capability-Based Business Model Transformation. In: Iliadis, L., Papazoglou, M., Pohl, K. (eds.) CAiSE Workshops 2014. LNBIP, vol. 178, pp. 88–99. Springer, Heidelberg (2014)
5. Teece, D.J., Pisano, G., Shuen, A.: Dynamic capabilities and strategic management. Strateg. Manage. J. **18**(7), 509–533 (1997)
6. Sandkuhl, K., Koc, H.: On the Applicability of Concepts from Variability Modelling in Capability Modelling: Experiences from a Case in Business Process Outsourcing. In: Iliadis, L., Papazoglou, M., Pohl, K. (eds.) CAiSE Workshops 2014. LNBIP, vol. 178, pp. 65–76. Springer, Heidelberg (2014)
7. Stirna, J., Sandkuhl, K.: An Outlook on Patterns as an Aid for Business and IT Alignment with Capabilities. In: Iliadis, L., Papazoglou, M., Pohl, K. (eds.) CAiSE Workshops 2014. LNBIP, vol. 178, pp. 148–158. Springer, Heidelberg (2014)
8. Mayer, N., Aubert, J., Cholez, H., Grandry, E.: Sector-based improvement of the information security risk management process in the context of telecommunications regulation. In: McCaffery, F., O'Connor, R.V., Messnarz, R. (eds.) EuroSPI 2013. CCIS, vol. 364, pp. 13–24. Springer, Heidelberg (2013)
9. Cholez, H., Feltus, C.: Towards an innovative systemic approach of risk management. In: SIN 2014, 61 p. ACM, New York
10. Rafati, L., Poels, G.: Capability Sourcing Modeling. In: Iliadis, L., Papazoglou, M., Pohl, K. (eds.) CAiSE Workshops 2014. LNBIP, vol. 178, pp. 77–87. Springer, Heidelberg (2014)
11. Barney, J.B.: Gaining and Sustaining Competitive Advantage. Prentice-Hall, Upper Saddle River (2002)
12. Mayer, N., Heymans, P., Matulevicius, R.: Design of a Modelling Language for Information System Security Risk Management. In: RCIS. (2007)
13. Taking Service Forward. http://takingserviceforward.org

14. Rosen, M.: Are Capabilities Architecture? BPTrends (2013). http://www.bptrends.com/publicationfiles/02-05-2013-COL-BA-Are%20Capabilities%20Arch.pdf
15. CSSF, Circulaire CSSF 12/544, Optimisation of the supervision exercised on the "support PFS" by a risk-based approach (2012)
16. Grandry, E., Feltus, C., Dubois, E.: Conceptual integration of enterprise architecture management and security risk management. In: SOEA4EE, EDOC WS (2013)
17. The Open Group: ArchiMate 2.1 Specification. Van Haren Publishing (2012)
18. Parent, C., Spaccapietra, S.: Database integration: the key to data interoperability. In: Papazoglou, M., Spaccapietra, S., Tari, Z. (eds.) Advances in Object-Oriented Data Modeling, pp. 221–253. Springer, Heidelberg (2000)
19. Zivkovic, S., Kühn, H., Karagiannis, D.: Facilitate modelling using method integration: an approach using mappings and integration rules. In: ECIS (2007)