Integrating Security Risk Management into Business Process Management for the Cloud

Elio Goettelmann, Nicolas Mayer, Claude Godart

▶ **To cite this version:**

Elio Goettelmann, Nicolas Mayer, Claude Godart. Integrating Security Risk Management into Business Process Management for the Cloud. CBI 2014 (IEEE 16th Conference on Business Informatics), Jul 2014, Genève, Switzerland. pp.86 - 93, 10.1109/CBI.2014.29 . hal-01095868

HAL Id: hal-01095868

https://inria.hal.science/hal-01095868

Submitted on 16 Dec 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Integrating Security Risk Management into Business Process Management for the Cloud

Elio Goettelmann[1,2], Nicolas Mayer[2] and Claude Godart[1]
[1]LORIA - INRIA Grand Est [2]CRP Henri Tudor
Université de Lorraine, Nancy, France L-1855 Luxembourg-Kirchberg
{*elio.goettelmann, nicolas.mayer*}*@tudor.lu*, *claude.godart@loria.fr*

***Abstract*—Security issues are still preventing wider adoption of cloud computing, especially for businesses which are handling sensitive information. Indeed, by outsourcing its information system (IS), a company can lose control over its infrastructure, its software or even its data. Therefore, new methods and tools need to be defined to respond to this challenge. In this paper we propose to integrate Security Risk Management approaches into Business Process Management to effectively treat security issues at the early phases of the Information System construction. We focus on cloud brokers, emerging actors of the cloud delivery model, who enhance and aggregate existing cloud services to match them with their cloud consumers' requirements. Our main goal is to provide them with tools and techniques to increase the global security level of an IS through different risk treatment strategies.**

***Index Terms*—Business Process Management, Security Risk Management, Cloud Computing**

I. Introduction

Cloud Computing helps companies in different ways. Its pay-as-you-go approach transforms the traditional capital expenditure (CAPEX) for an information system into operating expenses (OPEX). Therefore, cloud computing does not only enable cost reduction through outsourcing and resource pooling, but it also entails the enhancement of service quality by focusing on the company's core business activities.

However, the widespread use of such services is slowed down by different kinds of security risks bound to them, and recent revelations (as the PRISM[1] surveillance program) corroborate their relevance. It is of great importance for companies to identify and manage such new kinds of risks in order to preserve the security of their information system (IS). While the identification of the security risks that are emerging from cloud computing is globally cleared through different taxonomies and surveys ([10], [6]), it is rather unclear how to handle them and especially how to integrate their management in the company's specific business operations.

A starting point can be Business Process Management (BPM), an approach which consists in adjusting the business processes of an organization to the needs of its clients. Aligning existing Risk Management (RM) approaches with BPM could greatly help to identify, understand and manage the security risks for a company during the construction of its information system.

[1]The clandestine mass electronic surveillance program of the National Security Agency (NSA)

Moreover, in a cloud context, where different actors can support a same business process, it is particularly important to separate the duties and to know who is responsible for what. As the different phases of BPM can be distributed among different cloud actors, all risks cannot always be handled by one actor and at one phase of the IS construction. Indeed, some risks may be easier to identify and to be handled at a different phase. In this sense we propose to focus on the cloud context to align RM with BPM. We take the perspective of a **cloud broker** and analyze in which way he can help a company to **build a secured and risk-aware information system** while taking advantage of the full power of **cloud computing**. The objective of our paper is not to define yet another risk management method based on non-standard risk assessment practices. Our research work acknowledges that existing standards are efficient to determine the relevant risks and their magnitude [1], even in the context of cloud computing [10]. Our research work is focused on integrating risk management with BPM and thus smoothly integrating the decisions based on risk assessment in the process supported by BPM. The main objective of our research is to supply the cloud broker with methods and tools to support its activities.

The paper is organized as follows. In Section II we present briefly the research methodology we have used to build our approach. In Section III we define the different concepts and actors related to BPM, RM and Cloud computing. Section IV details our risk-based IS construction approach. An example illustrating our proposal is presented in Section V. Then, we discuss the related work in Section VI and finally present some ongoing and future work in Section VII.

II. Research Methodology

The methodology applied in this paper follows the *two dimensional research framework in information technology* presented by March *et al.* [14]. This framework gathers the types of activities and outputs produced when leading natural science ("understanding reality") or design science ("creating products that serve human purpose") research on IT. Design science activities can be of two types, *build*, to demonstrate feasibility, and *evaluate*, to measure how well it works. Whereas natural science activities are either *theorize*, to explain why it works, or *justify*, to gather evidence the theory is true. These activities are conducted on four artifacts: *constructs*, *model*, *method* and *instantiation*.

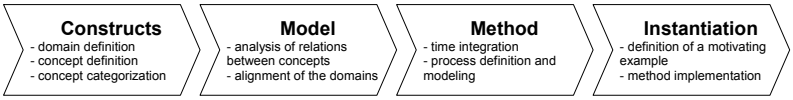

Fig. 1. Research methodology: *build* activity [14]

In this paper we try to define an approach for modeling risk-aware business process before deploying them on the cloud. This typically corresponds to the *build* activity of design science research. In order to produce a relevant and effective approach we conducted in this paper the *build* activity on all four artifacts.

First we build our *constructs* through different descriptions gathered in the existing literature (Section III), this in order to define precisely the terms used in our approach. We have studied 3 main domains: business process management, risk management and cloud computing. We define each of these domains and the important concepts regarding the goal of our paper.

Then we build our *model* by aligning the different constructs of the different domains (Section IV-A). The goal is to find how to integrate the three domains and to establish the relations between the previously built constructs in order to define an integrated framework.

The third stage consists in defining our *methodology* (Section IV-B). By adding the notion of time to our previously built artifacts, we are able to design a global approach to build risk-aware business processes for a cloud context.

Finally, we *instantiate* our approach on a motivating example to demonstrate the feasibility and the effectiveness of our approach (Section V).

III. Background

In a first step we build the *constructs* used in our approach. In this sense, for each studied domain (business process management, risk management, cloud computing), we define the different concepts related to our proposal as the domain itself.

A. Business Process Management

Usually, business process management refers to the traditional Business Process Lifecycle ([9],[21]) depicted in Fig. 2, which is similar to the well-known Plan-Do-Check-Act approach. To support this lifecycle, business processes are represented using models. These models evolve through the lifecycle as each phase has its specific objectives. So there are different *abstraction levels* to represent a business process (sometimes also called *perspectives*).

In the literature, there are often three levels of business process, even if the content is often different depending on the authors [16]. We decided to use the definitions coming from Ahmed *et al.* [4], which are quite similar to those given by Dreiling *et al.* [8].

*Definition 1 (***Enterprise-level Business Processes):** Enterprise-level business processes are high-level processes which relate an organization to its business environment. It defines the business functions in a coarse-grained fashion.

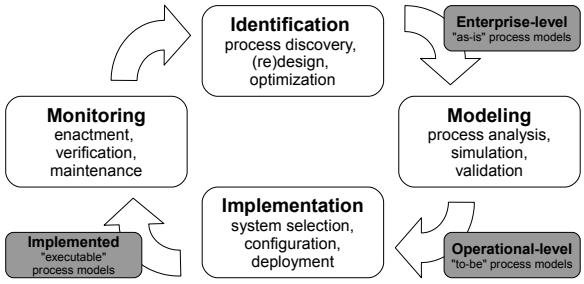

Fig. 2. Business Process Lifecycle drawn from [9], [21]

They typically specify the inputs and outputs of each process and their dependencies on other business processes.
This abstraction level is mainly used to get an overview of the business processes of the company and their intra- and inter-organizational relations. Such type of processes are obtained after the *identification* phase and are used as input of the *modeling* phase.

*Definition 2 (***Operational Business Processes):** Operational business processes specify the activities and their relationships used to realize the business functions. The processes are modeled in a more fine-grained fashion, but disregarding any detail about their implementation.
This level can be seen as "between" the abstract high-level and the detailed technical level. According to Dreiling *et al.* [8], this perspective is intended for business analysts. Such type of processes are realized during the *modeling* phase and are used as input of the *implementation* phase. This processes can be defined for example in BPMN ([3]).

*Definition 3 (***Implemented Business Processes):** Implemented business processes are the technical specifications to realize the activities of a business process. In an IT environment they are basically the software components supporting the execution of the process.
This processes can be defined for example as executable BPMN or BPEL ([3],[2]). To obtain such processes, the operational processes are used as input of the *implementation* phase and transformed in different steps:

- First, the supporting systems are *selected* (infrastructure, platform, etc.).
- Secondly, if not already existent, the needed software components are *developed/implemented*.
- Then, the different systems components are *configured*.
- Finally, the processes are tested and then *deployed* in their production environments.

B. Risk Management

The most common and standard risk management process, depicted in Fig.3, involves the following activities [1]:

- **Establishing the context** of the organization, including the definition of the scope, objectives and context of the

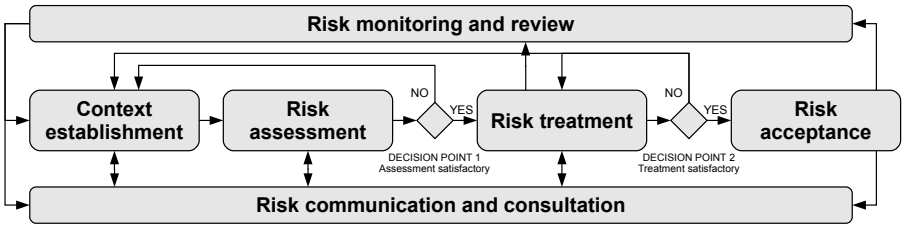

Fig. 3. Risk management process as in [1]

risk management process and making clear what criteria will to be used to evaluate the significance of risk.

- **Assessing the risks**, that means identifying sources of risk and areas of impacts, analyzing the risks through the estimation of the consequences of risks and the likelihood that those consequences can occur, and finally evaluating which risks need treatment and their priority level.
- **Treating the risks** via the selection of risk treatment options (e.g. *modifying* the risk with the help of design decisions leading to likelihood or consequences change, *sharing* the risk with another party, *avoiding* the risk by deciding not to start or continue with the activity that gives rise to the risk, *retaining* the risk by informed decision) and definition of risk treatment plans. The risks are then assessed again to determine the residual risks: risk remaining after risk treatment.
- **Accepting the risk** treatment plan and the residual risks by the organization's managers.

In parallel of the preceding activities, it is also necessary to regularly monitor and review the risks and the underlying risk management process. Moreover, communication and consultation with the different stakeholders should take place during all stages of the risk management process.

Information security risk management suggests four risk treatment strategies defined as follows [1]:

*Definition 4 (***Risk modification):** The level of risk should be managed by introducing, removing or altering controls so that the residual risk can be reassessed as being acceptable.
Risk modification involves improvement of the information system, leading to an increase of the information security level.

*Definition 5 (***Risk retention):** The decision on retaining the risk without further action should be taken depending on risk evaluation.
The risk is accepted as it is, but this decision is informed and the accepted risk is subject to monitoring and review.

*Definition 6 (***Risk avoidance):** The activity or condition that gives evidence that the particular risk should be avoided. In this case, modifications occur before implementing the business process of the organization in such a wise that the risk no longer occurs.

*Definition 7 (***Risk sharing):** The risk should be shared with another party that can most effectively manage the particular risk depending on risk evaluation.
It is important to note that in the case of risk sharing, new actors will be involved in the business processes. Risk sharing is particularly relevant in the context of cloud computing where some processes, or parts of them, can be outsourced.

C. Cloud Computing

Generally cloud computing is defined as a form of demand-driven and flexible use of IT performance, made available in real time as a service over the Internet and billed according to use [17]. This leads to the introduction of new actors. We are listing here the three main actors of the domain using the NIST definitions [19], others can also be identified, but are not relevant in our context.

*Definition 8 (***Cloud Consumer):** Is "a person or organization that maintains a business relationship with, and uses service from *Cloud Providers*".
The cloud consumer subscribes to a service proposed by a provider, uses it according to its needs and may have to pay for it if the delivered service is not free.

*Definition 9 (***Cloud Provider):** Is "a person, organization, or entity responsible for making a service available to interested parties". The provider offers and delivers services to the cloud consumer.
He may be the owner of the computing infrastructure, but he can also be using it from another provider to deliver its own upper level service. Thereby a cloud platform provider, can be the cloud consumer of a cloud infrastructure provider. Dropbox for example uses the cloud storage system of Amazon to deliver its services[2].

*Definition 10 (***Cloud Broker):** Is "an entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers". A cloud consumer can subscribe to a service offered by a cloud broker, instead of contacting directly a provider.
This definition proposes to categorize the broker services into three types:

- *Service Intermediation* - In this case, the broker enhances an offering of a provider by adding a specific layer (like reporting, identification, etc.).
- *Service Aggregation* - By combining multiple services into new services which are more interesting or more adapted to the cloud consumer.
- *Service Arbitrage* - By comparing different cloud offerings, the broker can propose to select the most appropriate provider.

As the cloud context introduces new actors, it creates new kinds of security risks. In opposition to a classical setting,

[2]https://www.dropbox.com/help/7/en (2013)

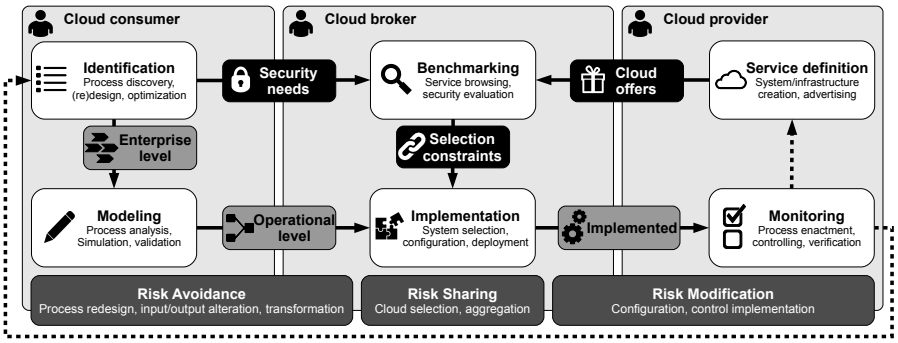

Fig. 4. Concept alignment

where a company controls its entire information system, here the consumer needs to rely on its cloud providers. Therefore, threats like *Shared technology vulnerabilities*, *Malicious insiders*, *Data breaches* or *Denial of service* are new emerging risks the cloud consumer needs to deal with [10]. We argue that the cloud broker's role is to support the cloud consumer to manage these risks. In the following we will present our model to help understand in which way he can do that.

IV. Building risk-aware business processes for the cloud

In this section we align the previously defined constructs in order to build a *model* and define a *methodology* for creating risk-aware business processes in a cloud context.

A. Concept alignment

By clarifying the role of each actor during the BPM lifecycle, we can identify the responsibilities and possibilities of each actor in the risk management process as depicted in Fig. 4.

1) Cloud providers: They are providing the services which support the business process implementation. Basically, they cannot, neither change the enterprise-level perspective of the business process, nor the operational. But, the provider influences technological choices to run a business process and has therefore a, even if not complete, view of the **implemented** business process.

Obvious actions it can take to reduce security risks are to implement countermeasures or security controls in its system. This corresponds to the **risk modification** treatment of the RM process. But these measures are rather part of an offer than specific to a process. Therefore, the security controls implemented in the providers systems determine the security level characteristic to its offers. In this sense, the implemented controls become more a selection criteria of the provider, than a risk treatment strategy.

Moreover, a cloud provider cannot avoid cloud risks because it is by definition exposed to them. Likewise, by subcontracting or outsourcing parts of its services (which corresponds to *risk sharing*), the cloud provider becomes a cloud consumer of another service; this case is handled in the next paragraph.

It is interesting to note that the main action of the provider concerning security takes place during the **monitoring** phase of the BPM lifecycle, where it has to control its system and trace back to the consumer each potential security breach.

2) Cloud consumers: They are obviously defining the **enterprise-level** processes as they are the ones who define their business strategies and the corresponding business functions. In a cloud environment, the idea is that a consumer can disregard any details about the implementation. In our case, even the system selection can be delegated to a cloud broker. As we are studying the cloud risks threatening the consumers processes, it is of their responsibility to define the **security needs** of their processes.

As cloud consumers do not own the infrastructure, they have no control over the vulnerabilities of the information system and cannot reduce them. However, they can change their processes in such a way that risks are limited (by not using cloud services for some parts of the system for example). This corresponds to **risk avoidance**. They can change the impact of a potential security breach by designing their processes otherwise.

Of course, cloud consumers do not rely on an entire cloud-based information system. The security of this internal information system can and has still to be managed in a classic risk management approach. But this problem is not addressed in this paper, as we consider that classic methodologies solve it. We only focus on business processes candidate for being outsourced.

The phases during the BPM lifecycle where the main actions of the cloud consumer take place are **identification** and **modeling** which are respectively conducted by the company's managers and its business analysts.

3) Cloud brokers: As the cloud broker's role is still emerging, it is rather unclear how far its expertise will go. Depending on the previously definition, its main business activity will be the *system selection* step for the **implementation** phase.

Basically, the role of a cloud broker could be summarized as translating functional requirements (**operational-level processes**) and non-functional requirements (**security needs**) given by the consumer into **selection constraints**. Thus, the implemented processes, based on one or multiple cloud services, will be secure. A cloud broker can aggregate multiple services to fulfill the initial requirements, and so distribute the risk among a set of different cloud providers. And as for the other requirements, the broker needs to ensure that the global security level of the distribution is acceptable. Therefore, the main risk treatment activity of the cloud broker

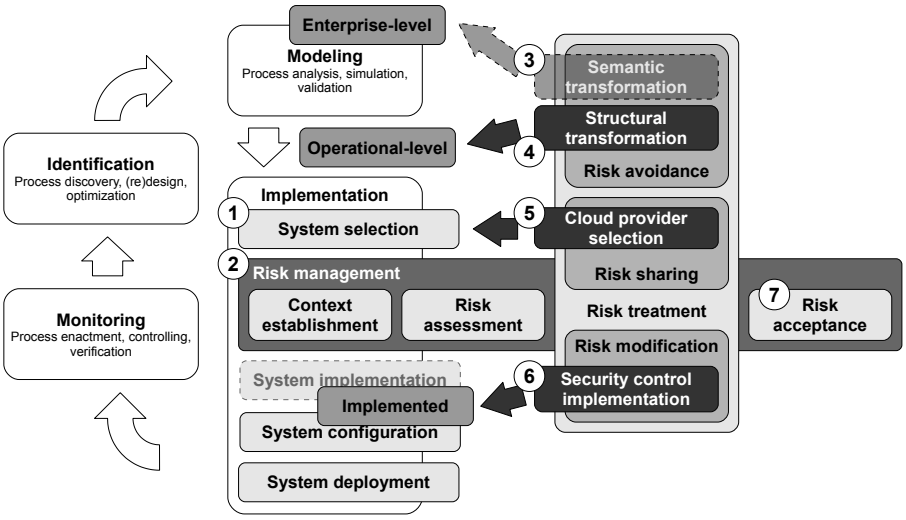

Fig. 5. Overview of our approach

corresponds to **risk sharing**. Cloud brokers have neither the ability to change the business functions, nor to change the infrastructure, as they act as intermediation. But very complete cloud broker could also provide the process *configuration* and *deployment* steps on which risk modification activities can be conducted. We even argue that a broker could advise a cloud consumer in some decisions as they are generally well documented on existing cloud services. In this sense a cloud broker could help the consumer to avoid some risks.

As shown in Fig. 4, we propose to align the BPM lifecycle with the three risk treatment strategies and the three previously defined cloud actors. These actors intervene in a cyclic way following the different phases of the BPM lifecycle. First a cloud consumer identifies and models its business processes at the enterprise-level. At this phase he is able to avoid some cloud security risks by "preparing" its processes for the cloud. Once modeled, the operational-level processes are transferred to the cloud broker who has to implement them. The cloud broker is sharing the risks among the different selected cloud providers executing the business processes. The broker can also somewhat avoid and reduce some of the risks through different actions which are detailed in the next section IV-B. The cloud providers enact and monitor the business processes and have previously reduced some of the cloud risks by implementing countermeasures. The monitoring can help to improve the processes by looping through the different phases once again (dotted arrows in Fig.4).

B. Methodology

Our objective consists in integrating the risk management process into the BPM lifecycle to handle the security risks emanating from the cloud. This allows us to define security risk-aware business processes before deploying them on the cloud. Our goal is to provide the cloud broker with tools to lower the security risks to which the business process is exposed in a cloud context. In the following we are taking the perspective of the cloud broker and see the different risk treatment strategies he can follow to transform the operational-level business processes into risk-aware implemented processes. This section is summed up in Fig.5, where the RM process is integrated into the BPM lifecycle.

1) System selection: (Fig.5.1)
As the first step of the risk management process is to *establish the context*, this can only be done once the execution context of the process has been defined. Therefore, in our approach, first, the candidate cloud services are selected at the *system selection* step of the BPM lifecycle.

2) Risk management: (Fig.5.2)
Then, the risk management process can begin, which allows to loop through the different phases of the BPM lifecycle to redefine the processes and the systems. The RM process follows a classic RM methodology by establishing the context and assessing the risk. For the three types of treatment strategies we defined four different business process transformations.

a) Semantic transformation: (Fig.5.3). One way to **avoid** some risks can be to change the semantic of the process. This means that the global business function is altered in order to avoid one or multiple security risks emanating from the cloud. Of course the alteration cannot change the main strategy conducted by the company. Therefore this is not part of the core activity of a cloud broker, as he cannot alter a business process in such a way. But it can be interesting to advise the cloud consumer in some cases because a small change at the enterprise-level of a business process could dramatically change the global risk level of a business process, and at very little costs. A cloud broker can for example advise the consumer to use a inhouse infrastructure rather than a public cloud. Another example will be given in the next section V.

b) Structural transformation: (Fig.5.4). Another way to **avoid** some risks can be to change the structure of the process. A structural transformation means that the process is changed, but without modifying the semantic of the process (what the process is actually doing). The global business function remains unchanged, but the way this function is achieved is done in a different way. Such transformations are made on the

operational-level of the BP. An example can be the splitting of some operations into multiple activities and the adding of separation of duties constraints. This is a task which typically a broker can do. He can also combine different services or add a specific layer in order to achieve the same goals but in a more secured fashion. Another example is *redundancy*: the broker can duplicate the process on multiple clouds to increase the availability of the process.

c) Cloud provider selection: (Fig.5.5). This is the core business activity of a cloud broker, called *service arbitrage*, cloud offers have to be compared according to parameters as costs, security or quality of service. As some providers can offer services with a better security levels than others, it can be interesting to transfer the process to another location. As the security levels of cloud providers are often linked to the price of their services, it is important to balance the risk against the cost: a too secured provider could be too expensive, and on the contrary, the cheapest cloud would probably be not secured enough. When handling one single process, the easiest way is to deploy the process on one selected provider. But in some cases in can be interesting to partition the process into subprocesses and to deploy them onto separate cloud providers. As each activity of the process may not have the same security or functional requirements, it can be interesting to have a more heterogeneous deployment configuration in order to decrease costs or increase the Quality of Service. A contribution to such problems can be found in our previous work [11].

d) Security control implementation: (Fig.5.6). This corresponds to the mainly used risk treatment strategy: risk **modification**. The security risks threatening the business process can be sometimes easily reduced by changing or adapting the implementation of the process. If possible, the broker can integrate itself security controls into the system (encrypting the database for example). Other security layers (authentication for example) can be included to the system to increase the global security level. Otherwise it is still possible to reduce the risks by configuring the system correctly. An example could be to use SSL to secure all communication channels if this option is available for the selected cloud offer. This can obviously lead to an increase of the usage costs, which relates closely this option with the third treatment possibility (*provider selection*).

3) Risk acceptance: (Fig.5.7)
The last step is the acceptance of the risk, which can be reached after multiple loops in the RM process. Each time an action is taken, the risk has to be re-assessed to determine if the risk can be accepted or not. This is usually done by defining a risk threshold: if all risk values are below this value, the process can be securely deployed to the cloud.

As implied previously, the last action a broker can take, when no acceptable solution can be found, is to advise the consumer not to deploy its processes to the cloud.

V. Example

In the following we *instantiate* our methodology through an illustrating example.

Process name: *Recommendations Definition*	Responsible Process Manager: *M. Sample*
Process Inputs: *Customer order history*	Supplier Processes: *Archiving Process*
Process Results: *Product and Customer relations*	Customer Processes: *Marketing Process*

TABLE I
Enterprise-level business process

Suppose a company wants to increase the loyalty of its customers and its advertisement efficiency by using the *customer order history* to implement a recommendation system. This basically corresponds to an enterprise-level business process (represented in Table. I). The company knows what has to be done: the inputs and the expected results are defined.

But the company does not know how to extract any valuable information from its data sets. Therefore the company searches an adequate cloud service answering such requirements. Moreover, the company knows that there will be some security issues when using external cloud service, especially as sensitive personal and business critical information are concerned. In this sense, the company contacts a cloud broker, which will help to implement this system in a secured fashion. Together they analyze existing cloud *threats* and retain the followings:

- Data breaches = {Confidentiality}
- Denial of Service = {Availability}
- Malicious Insiders = {Confidentiality, Integrity, Availability}

Each of these threats are related to one or more security objectives. Here we chose the CIA-triad (*Confidentiality*, *Integrity* and *Availability*) but other can be used. These relation indicates in which way the threat will affect the assets of the business process. For this purpose, the data of the process is annotated with *security needs*, which are levels (on a scale from 0 to 2) based on the same security objectives. Here we consider only one data object, the *Customer order history*, for which following *needs* are defined (underlined):

- Confidentiality = {Public=0, Restricted=1, Secret=2}
- Integrity = {Passable=0, Alterable=1, Fixed=2}
- Availability = {Sparse=0, Usual=1, Continuous=2}

The cloud broker knows different cloud providers offering services answering the consumer's requirements. The broker also proposes to adapt the company's data as the existing services require a specific input format. A model depicting this business process is shown in Fig.6.

The cloud broker has an internal method to assess the security level of cloud providers. It defines a score for each provider and each threat. A high score means that the provider is highly exposed to this threat, a low score means that it is well protected. This value depends on the security controls the provider has implemented to modify existing cloud risks. We are not detailing how such scores are obtained, as it is not the purpose of this paper, but indications can be found on [6]. We give three cloud providers and their *exposure* scores for the three selected threats. This score is defined on a scale ranging from 0 to 5:

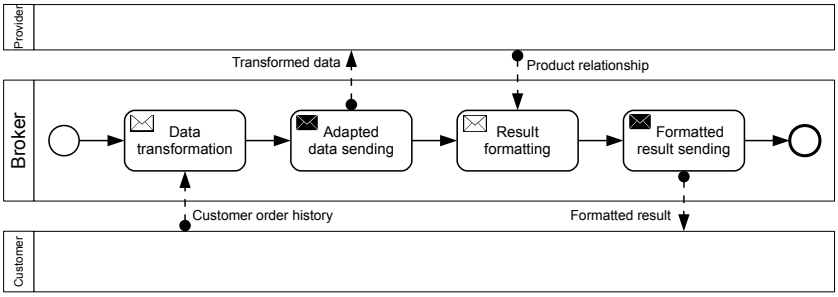

Fig. 6. Operational business process (cloud broker perspective)

- CloudSigma AG[3] = {Data Breaches=1, Denial of Service=0, Malicious Insider=1}
- FireHost[4] = {Data Breaches=4, Denial of Service=2, Malicious Insider=2}
- Terremark[5] = {Data Breaches=2, Denial of Service=0, Malicious Insider=1}

By combining the three values (*threats* × *security needs* × *exposure*), the broker gets a risk value for the selected data element, and this for each threat, on each provider. These values are shown in Table.II.

	Cloud sigma AG	FireHost	Terremark
Data Breaches	3	6	4
Denial of Service	0	2	0
Malicious Insider	4	5	4

TABLE II
RISK VALUES FOR 3 PROVIDERS OF *Customer order history*

Together with the cloud consumer, the broker defines a threshold, which will determine which solutions can be accepted. In our example we define the threshold at 3, which means that right now, no solution is acceptable.

But the broker has different treatment strategies to reduce these risk values:

- the broker knows different type of such services, and decides to use more than one and splits the data, in this sense none of the provider holds the complete set of the data. This typically corresponds to **risk sharing** as the risk does not disappear: if the providers cross the different data sets, they get the full information. Or it is still possible for an attacker to break into each of the services to get the full information. But the likelihood of this threat is significantly lower.

[3]http://www.cloudsigma.com
[4]http://www.firehost.com
[5]http://www.terremark.com

- the broker decides to add noise-data to the input data, which does not influence the result, but the provider will not know which of the data is really valuable. This corresponds to **risk mitigation**, it is not sure that the noise-data is enough for hiding the valuable information, but it increases the complexity of recovering the information, and thus lowers the risk.
- the broker decides to anonymize the data (delete any information concerning the user, or the products) before uploading it on the provider's platform. This corresponds to **risk avoidance**, as the sensible information are no longer available for the cloud provider, but other risks can now appear (as *de-anonymization* [18]).

The transformed business process model proposed by the cloud broker is shown in Fig.7. The newly added tasks are coloured in gray. These measures reduce the risk values of *Data Breaches* and *Malicious Insider* by 1. The new risk values, related to this new configuration is shown in Tab.III. We notice that two cloud services are now available for answering the requirements: *CloudSigma AG* and *Terremark*. On the contrary, *FireHost* presents a risk value for the *Data breaches* threat which is too high, and can still not be used.

	Cloud sigma AG	FireHost	Terremark
Data Breaches	2	5	3
Denial of Service	0	2	0
Malicious Insider	3	4	3

TABLE III
RISKS OF TRANSFORMED PROCESS

The cloud broker can now propose these two solutions to the cloud consumer, and would probably advise to select the solution with the lowest costs. An interesting setting could be if the costs of the third provider (*FireHost*) would be extremely lower than the others. It could for example be free, as many cloud services are. In this case, the broker could propose even another solution to the cloud consumer: by using only a sample

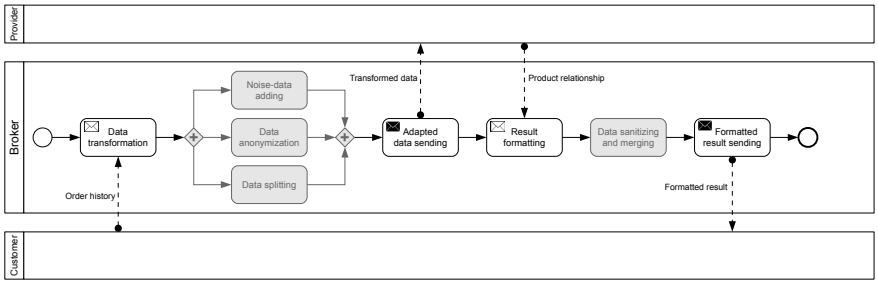

Fig. 7. Transformed business process (cloud broker perspective)

of the input data, the results could still be very interesting for the company, while lowering the security risks to a value which would make this free service eligible. But, as this option changes the semantic of the initial process (the results have to be interpreted differently), this decision can only be made by the company itself. The resulting enterprise-level business process is presented in Tab.IV.

Process name: *Recommendations Definition*	Responsible Process Manager: *M. Sample*
Process Inputs: **Customer order history sample**	Supplier Processes: *Archiving Process*
Process Results: *Product and Customer relations*	Customer Processes: *Marketing Process*

TABLE IV
TRANSFORMED ENTERPRISE-LEVEL BUSINESS PROCESS

In this case, as the data object has changed, the **security needs** have to be redefined and the risks must be re-assessed. As the needs would be lower, the free configuration would probably be possible. But only the company (the cloud consumer) can take the decision wether it accepts higher costs for better results or not.

VI. Related Work

Different authors are addressing the same problem, which consists in aligning business process management and risk management. For example, Matulevicius *et al.* [4] are working at the modeling level to coordinate the BPMN standard with the ISSRM domain model [15]. These authors are proposing patterns to reduce security risks in business processes [5]. But these contributions are limited to the modeling layer of business processes and do not consider the context of cloud computing.

Conforti *et al.* [7] propose a system supporting risk-informed decisions during business process execution. In opposition to our approach, they are handling risks at runtime, while we are working at design-time. The two approaches are complementary, but also handle different types of risks.

In a cloud context, Jensen *et al.* [13] propose different strategies to limit the impact of security issues. But this approach is rather high level and does not consider, neither business processes, nor risk management methodologies and thus is hard to automate. Process splitting and cloud provider selection problems are addressed in [20]. Similar to our approach, providers are selected based on security levels and compared to annotated data elements of the process. But only process splitting is considered, and security is not addressed from a risk perspective.

In previous works [11], we already considered security aspects before deploying processes on multiple cloud environments, but without methodological considerations. A first study in this sense was presented in [12].

VII. Conclusion

In this paper we presented an approach integrating Business Process Management and Security Risk Management in a Cloud context. We defined the different actors, the process models they manipulate and the possible risk treatment strategies to secure a business process preceding a cloud deployment. The detailed methodology takes the perspective of a cloud broker, and categorizes the techniques he can use to lower cloud security risks threatening the business process. We illustrated our approach on a motivating example.

Our paper presents some limitations which will be addressed in future works. The main one is the lack of empirical evaluation, as we only instantiated our approach on a motivating example. The next step will consist in the second activity of our research methodology: *evaluating* the artifacts defined in this paper. This will mainly consist in experimenting our approach on real use cases. Another point is the lack of automation of our methodology, which is currently addressed by extending the prototype developed in [11]: in addition to fragmenting processes and deploying them on clouds, it will conduct automated risk assessments and transform the structure to enhance security.

References

[1] ISO/IEC 27005, Information tech., Security techniques, Information security risk management.
[2] Web services business process execution language (wsbpel) 2.0, standard,, 07.
[3] Business process model and notation (bpmn) 2.0, standard,, 11.
[4] N. Ahmed and R. Matulevicius. A taxonomy for assessing security in business process modelling. In *RCIS*, pages 1–10, 2013.
[5] O. Altuhhova, R. Matulevicius, and N. Ahmed. Towards definition of secure business processes. In *CAiSE Workshops*, pages 1–15, 2012.
[6] Cloud Security Alliance. Cloud Control Matrix / Security, Trust & Assurance Registry / Consensus Assessments Initiative Questionnaire. Technical report.
[7] R. Conforti, M. de Leoni, M. L. Rosa, and W. M. van der Aalst. Supporting risk-informed decisions during business process execution. In *CAiSE'13*, pages 116–132, Valencia, Spain, 2013.
[8] A. Dreiling, M. Rosemann, and W. M. van der Aalst. From conceptual process models to running workflows : a holistic approach for the configuration of enterprise systems. In *PACIS'05*, pages 363–376, 2005.
[9] M. Dumas, M. L. Rosa, J. Mendling, and H. A. Reijers. *Fundamentals of Business Process Management*. Springer, 2013.
[10] European Network and Information Security Agency. Benefits, risks and recommendations for information security. Technical report, 2009.
[11] E. Goettelmann, W. Fdhila, and C. Godart. Partitioning and cloud deployment of composite web services under security constraints. In *IC2E'13*, 2013.
[12] E. Goettelmann, N. Mayer, and C. Godart. A general approach for a trusted deployment of a business process in clouds. In *MEDES'13*, 2013.
[13] M. Jensen, J. Schwenk, J. Bohli, N. Gruschka, and L. Iacono. Security prospects through cloud computing by adopting multiple clouds. In *CLOUD'11*, pages 565 –572, 2011.
[14] S. T. March and G. F. Smith. Design and natural science research on information technology. *Decis. Support Syst.*, 15(4):251–266, Dec. 1995.
[15] N. Mayer. *Model-based Management of Information System Security Risk*. PhD thesis, University of Namur, Apr. 2009.
[16] C. Monsalve, A. April, and A. Abran. Requirements elicitation using bpm notations: Focusing on the strategic level representation. ACACOS'11, pages 235–241, 2011.
[17] G. Münzl, B. Przywra, M. Reti, J. Schäfer, K. Sondermann, M. Weber, and A. Wilker. Cloud computing - evolution in der technik, revolution im business. Technical report, 2009.
[18] A. Narayanan and V. Shmatikov. Myths and fallacies of "personally identifiable information". *Commun. ACM*, 53(6):24–26, June 2010.
[19] National Institute of Standards and Technology. Cloud Computing Reference Architecture, 2011.
[20] P. Watson. A multi-level security model for partitioning workflows over federated clouds. In *CloudCom*, pages 180–188, 2011.
[21] M. Weske. *Business Process Management - Concepts, Languages, Architectures, 2nd Edition*. Springer, 2012.