Information Security Risk Management in a World of Services

Vincent Lalanne, Manuel Munier, Alban Gabillon

Information Security Risk Management in a World of Services

Vincent Lalanne and Manuel Munier
LIUPPA
Université Pau & Pays Adour
Pau, France
Email: {vincent.lalanne,manuel.munier}@univ-pau.fr

Alban Gabillon
GePaSud EA 4238
Université Polynésie Française
France
Email: alban.gabillon@upf.pf

***Abstract*—Service Oriented Architectures (SOA) offer new opportunities for the interconnection of systems. However, for a company, opening its Information System to the "world" is not insignificant in terms of security. Whether to use available services or provide its own services, new technologies have introduced new vulnerabilities and therefore new risks. Our work aims to propose an approach for risk management which is based on the ISO/IEC 27005:2011 standard: we propose a development of this standard (by an extension of Annex D) so that it can fully take into account the type "service" as web services and cloud services. Indeed, a world of services is not limited to link interconnected systems, it is more a relationship between customer and supplier, where notions of trust, accountability, traceability and governance are developed. Following this study we introduce a new security criterion, controllability, to ensure that a company keeps control of its information even if it uses such outsourced services.**

Keywords*—*information security; risk management; SOA; cloud; web services; ISO/IEC 27005; controllability;

I. Introduction

First information systems (IS) used in companies operate autarky, that is to say closed to the outside world and only supplied by the internal data from the enterprise. The need to connect to other systems quickly emerged, thus increasing the amount of information available, outsourcing some processes and offering new services to both employees (working at home, nomadic users,...) and customers (web portals, information flow,...). The increasing use of mobile devices, smartphones or tablets in the professional world (BYOD[1]) also introduces new risks that companies must face: storing information on the terminal, business applications installed (data, but also configuration parameters like usernames, passwords or server addresses),...

These early infrastructures used private connections, but with the Internet growth, IT designers decided to use this network to connect their information systems. This change has reduced connection costs and provided greater flexibility in the deployment of such infrastructures. From the point of view of the network, security managers have to implement various technologies to control the opening of the corporate network over the Internet: routers, firewalls, VPNs,...

With the emergence of new needs, the interconnection of information systems is the next step. This evolution is a fact in particular through the development of service-oriented architectures (SOA) that have gained great popularity because they allow the creation of new services by composition (orchestration, choreography,...) of existing services over the Internet. They may have very different features: computation, data storage, remote database access (data warehouses, schedules,...). Web Services (WS) is one of the most widely used technologies for such SOA.

Infrastructure design using external services (which we do not control) and/or exposing new services outside the company raises new problems for the information system security (ISS). It concerns not only the classical criteria as confidentiality, integrity and availability, but also new concepts like traceability, trustworthiness and controllability.

The paper is organized as follows. After detailing in Section II various technologies used to secure such web services and a quick reminder of the services offered by the cloud, Section III discusses methods and standards widely used in risk management information systems. Section IV presents our work based on a risk management approach for information system vulnerabilities related to those services. For the purpose of this work, we rely on the ISO/IEC 27005:2011 standard [1] that we extend to "services". We conclude the paper with some related works in Section V and pointers to future research directions in Section VI.

II. Web Services and Security

A. A World of Services

Interconnections between information systems via web services can be carried out either on private infrastructures or through the Internet. For obvious reasons of cost, the use of Internet and its standards is becoming more common. There is another concept very close to web services: the cloud. Indeed, this "technology" involves many services in the field of computing, storage, information processing,... The cloud model takes concepts already known in the world of services, but with aggressive marketing discourse.

The number of available services on the cloud is constantly increasing. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) first appeared, often as variations of existing web services. Now come new concepts such as Monitoring as a Service (MaaS), Communication as a Service (CaaS), Data as a Service (DaaS), inFormation as a Service (FaaS),... The XaaS (Anything as a Service) are born

[1]BYOD: Bring Your Own Device

and include all services directly accessible from the Internet and that grow on the business model of cloud computing.

Note that we can distinguish two notions: the private cloud and public cloud. Even in a private cloud (internal to the company) it is possible to control the overall infrastructure, it is not the same in public cloud.

B. Web Services Security

Many exchange protocols exist, including REST [2] and SOAP [3] in particular, but we do not detail the XML-RPC[2] [4] protocol, an ancestor of SOAP, unmaintained since 1999. We can note that REST is the native HTTP protocol while XML-RPC and SOAP uses XML over HTTP as a transport protocol over the Internet.

1) REST (REpresentational State Tranfert): REST [2] is a design pattern for implementing connected systems. It is neither a technology nor a standard. It is a type of architecture to publish resources on the web. RESTful architecture meets several principles: Applications are client-server, requests are stateless, clients and servers use a uniform interface; all resources are accessed through well defined methods like HTTP GET, POST, PUT, DELETE, HEAD and OPTIONS. Clients access to named resources; the system understands named resources using URLs such as HTTP URLs (but not only limited to HTTP URLs);

2) SOAP (Simple Object Access Protocol): SOAP [3] establishes a general framework for exchanging complex data in XML. SOAP does not depend on the programming languages (C, Java, PHP, NET, PERL,...) or the operating system on which it is implemented. A SOAP message is a unidirectional transmission between SOAP nodes, from a SOAP sender to a SOAP receiver. SOAP messages are supposed to be combined by applications to implement more complex sequences of interactions: from the basic question and answer model to multiple bidirectional exchanges for "conversational" scenarios.

A SOAP message is an XML document constituted by an envelope containing a Header (optional) and a Body (the message). The envelope is the root of the XML document containing the SOAP message. Header tag allows to pass additional information about this message. This element is optional, but if present it must be the first element in the SOAP envelope of the message. The header can have multiple uses. It may, for example, contain authentication information from the issuer, or the context of a transaction in which the message is only a step. For transport layers (such as FTP) that do not provide return address, one can use the header to identify the sender of the SOAP message. The message body consists of a single Body element containing one or more sub-elements. The message body can carry remote procedure calls, results or error messages. But the practice has become enlarged and the message body is often used to exchange structured data between applications.

Over the SOAP protocol, we can list a number of existing security measures. Additional specifications have been defined over the XML/SOAP stack[5], [6] to strengthen security of infrastructures using web services (Figure 1).

[2]XML-RPC: XML Remote Procedure Call

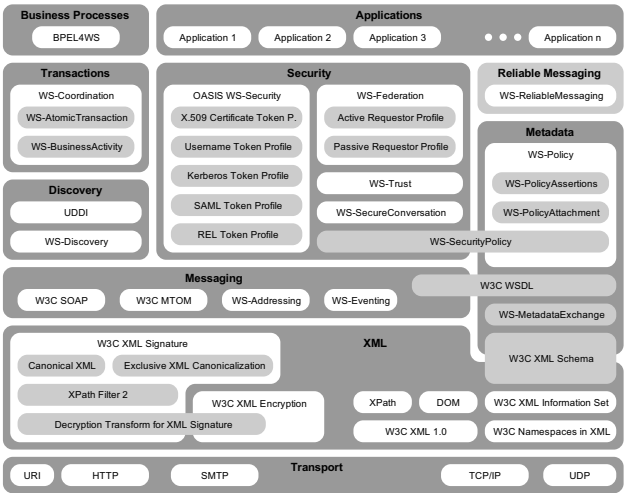

Fig. 1. The Web Services specifications stack (WS-*) [7]

Core technologies around XML are all defined by the World Wide Web Consortium (W3C). This is the case for example for XML Encryption [8] and XML Signature [9] which respectively address the issue of confidentiality (encryption) and data integrity (message authentication and/or signer). Based on these standards, standardization organizations such as OASIS have developed specifications such as Web Service Security [10]. This is a set of SOAP extensions that ensures the message integrity and confidentiality. This specification is flexible and can be adapted to security models as varied as PKI, Kerberos, and SSL. A number of specifications are associated with WS-Security:

- WS-Trust: specification for the generation, renewal and validation of security tokens
- WS-SecureConversation: creation and sharing security contexts (using security context token)
- WS-Federation: mechanisms for allowing disparate security realms to broker information on identities, identity attributes and authentication
- WS-Authorization: expression of authorizations
- WS-Policy: flexible and extensible grammar for expressing the capabilities, requirements and general characteristics of entities (customers or suppliers)
- WS-Privacy: model to indicate how confidentiality requirements and practices related to private data is transmitted between organizations

Other specifications concern more specifically the phases of authentication and authorization. Authentication is the process to validate identity, while authorization is the process of deciding if authenticated user can access such resources or perform such actions. SAML[3] specification [11] defines a framework for exchanging authentication information and authorization between business partners. SAML supports single sign-on (SSO) for affiliated sites. Another specification, XACML[4] [12], [13], defines a language for access control, rule propagation and administration of security policy for information systems.

[3]SAML: Security Assertion Markup Language
[4]XACML: XML Access Control Markup Language

III. Methods and Standards for Information System Risk Management

In this section we will briefly list the main methods used in risk management in information security, then we will, after a short history that led to its creation, detailing the main steps of the ISO/IEC 27005:2011 [1] international standard. We conclude this section with a statement that shows the limits of this standard in consideration of services as we now approach.

A. Why a Standard for Information Security ?

Existing methods for ensuring information security can not be a trust mark for the overall security of the company, because it is often developed internally and difficult to change (long term support ?). To meet the need for overall confidence in the digital economy, work has been initiated to establish international standards for information security.

Since a decade, companies having many data exchanges with other companies (national or international) or with many partners and customers, have experienced the need to agree on standards to secure information and exchange processes. It is precisely this goal that led to the creation of the ISO/IEC 27005 standard. It aims to establish a trust mark for the overall information security within enterprises.

B. Standard or Method ?

A standard is defined as a document based on a consensus covering a broad industrial or economic interest and established by a voluntary process. In contrast, a method is an effective way to achieve a desired and accurate result. But a method does not include the notion of document, neither the concept of consensus. We should not oppose standards and methods, but rather combine them: a method will be the "tool" used to meet a standard.

To effectively implement the ISO/IEC 27005 standard, we can thus rely on a risk management method as CRAMM[5] (United Kingdom), Octave [14] (United States), EBIOS[6] (France).

C. Introduction to the ISO/IEC 27005:2011 Standard

This is the latest standard for information security and it is expected to be widely used in the field of ISMS[7]. Since 1995, several standards for ISMS have been published:

BSI[8] publishes (1995) BS 7799 standard [15], it focuses on ten major chapters that list the actions (one hundred) that can be taken in relation to information security. In 2000, ISO officially adopts it under the reference ISO 17799 (now known as ISO 27002). The creation of ISO 27001 this is BS 7799 plus the requirements that an organization must meet to implement an ISMS, all in one approach closer to ISO 9001. At east ISO 27005 is published in 2008; its purpose is to provide guidelines for information security risk management; it supports the general concepts specified in ISO 27001; it is a consensus between the various methods used in different countries as CRAMM, OCTAVE, EBIOS it will progressively replace. A new version of ISO 27005 standard appeared in 2011.

ISO/IEC 27005:2011 gives recommendations and therefore it quite often uses the conditional. It is not required to follow all the steps of the method: the implementer applies what is most appropriate for his case study. This is a standard that, when applied, allows us to follow a process compliant with ISO/IEC 27001:2005.

The first six chapters of the standard are very short and deal only with generalities. The text begins by clarifying the scope of the standard (Clause 1), recalls some normative references (Clause 2), gives some terms and definitions (Clause 3), shows the general structure of the standard (Clause 4) and points out the advantages of following a risk management approach (Clause 5). Clause 6 gives an overview of the information security risk management process (steps appear in Figure 2). The information security risk management process consists of context establishment (Clause 7), risk assessment (Clause 8), risk treatment (Clause 9), risk acceptance (Clause 10), risk communication and consultation (Clause 11), and risk monitoring and review (Clause 12). Here are the steps that we need to perform to conduct the process.

In the remainder of this section we will briefly present the standard necessary to explain the following main points of our presentation, these items are highlighted in bold.

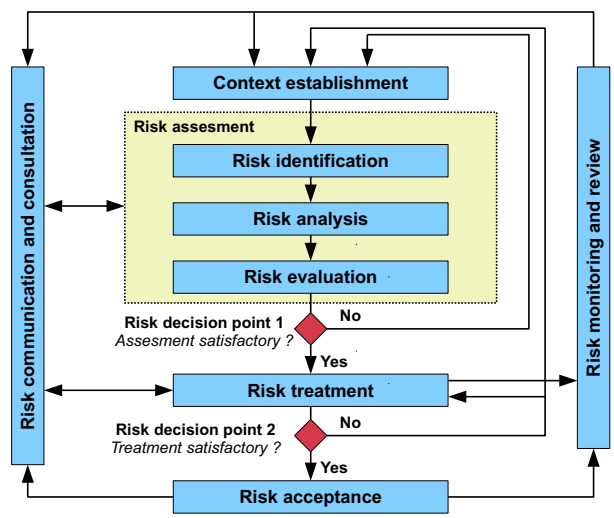

Fig. 2. Information security risk management process

We must first define the scope and **boundaries** of the information security risk management (Clause 7): this step is context establishment. This notion of context is essential, because later in our presentation, it will allow us to set the point of view of risk assessment through the consideration of risks associated with the use of Web Services. The context also sets a number of criteria which are then used as the basis for risk assessment: risk evaluation criteria, impact criteria and risk acceptance criteria.

Clause 8 contains the main steps of the process. It points

[5]CRAMM: **C**CTA (Central Computer and Telecommunications Agency) **R**isk **A**nalysis and **M**anagement **M**ethod

[6]EBIOS: **E**xpression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité (expression of needs and identification of security objectives)

[7]ISMS: Information Security Management System

[8]BSI: British Standards Institution

in particular that the risk assessment is composed of three sub-tasks: "risk identification", "risk analysis" and "risk evaluation". Firstly we need to identify the **assets** that fall within the scope defined above and give them a **value**. The level of granularity of the assets can be refined. This point is very important and will be developed further in the following section about Web Services used by our information system. We then need to identify **threats** that may be of accidental origin or come from inside as well as outside. In the standard, Annex C provides a referential (not exhaustive) of the various possible threats. When an IT architect builds an information system, he implements security mecanisms which he considers essential. ISO/IEC 27005 takes into account this legacy and specifies that an inventory of security measures already deployed (or whose deployment is scheduled) must be done.

The next step is to identify **vulnerabilities** related to the assets that were set previously. For this, Annex D provides a referential (non-exhaustive) of various vulnerabilities that exist for each type of asset with possible threats. We must then identify and assess the **consequences** of incident scenarios that describe a threat from the exploitation of a vulnerability inherent in the asset. These **scenarios** are assessed through the evaluation of their consequences and their estimated **likelihood**. Finally, we must assess and evaluate the **risk** by linking the likelihood and consequences of the scenarios listed above. A list of valued and ranked risks can thus be established.

Clause 9 is devoted to the risk treatment. There are four options to do this: modification, retention, avoidance or risk sharing. Proposals for risk treatment lead to the identification and estimation of **residual risks**, that is to say, the risk remaining after treatment. The next step is to accept or not the risk treatment plan (Clause 10: risk acceptance).

As for any quality process related to risk management (regardless of the domain), such an audit will hardly be effective without the cooperation of the persons concerned and without regular monitoring of the system. Risk communication process (Clause 11) aims to make all stakeholders aware of the concept of risk. Clause 12 of the standard concludes by reminding the concepts of monitoring, review and improvement inherent in an iterative approach. When applying this standard, it is not enough to proceed the steps above once, but instead it is quite clear that we must constantly analyze, monitor and improve the risk assessment. A continuous watch is indeed necessary to take into account new assets, new features, the discovery of new vulnerabilities, the effectiveness of measures taken, the evolution of the security policy of the company,...

D. Observations

The difficulties encountered in risk management in distributed information systems are intrinsically linked to the SOA model. Such a "logical" architecture relates at the same time hardware aspects (servers of the service provider), software (operating systems, implementation of the SOAP protocol, services themselves) and network (Internet, LAN, routers). Although ISO/IEC 27005 can already take these aspects into account in the study boundaries, it treats them individually: datacenters, network connections, computers, applications,... Moreover, existing technical solutions to improve IS security also address these points individually: backup servers, clusters, redundant links, encryption tools, system administration, application monitoring,...

But now a world of services is not limited to link interconnected systems, it is more a relationship between customer and supplier, where notions of trust, accountability, traceability and governance are developped.

ISO/IEC 27010 provides guidance on information security interworking and communications between industries in the same sectors, in different industry sectors and with governments, either in times of crisis and to protect critical infrastructure or for mutual recognition under normal business circumstances to meet legal, regulatory and contractual obligations. Similarly ISO/IEC 27017 will cover information security aspects of cloud computing, this standard is expected to be a guideline or code of practice recommending relevant information security controls for cloud computing. ISO/IEC 27018 will cover privacy aspects of cloud computing. These standard (not yet published) will intend to normalize communications with a package of good practices but do not reflect the specific risks of using external services.

IV. ISO/IEC 27005 Applied to Risk Management in SOA Based Information Systems

We note that this standard applies to information security has neglected the development of special services in information systems. Indeed the material, human, organizational aspects are planned, but the ability to store, process and use resources via web or generally what is called cloud services. Also, in this section we will proceed in the first part the standard ISO/IEC 27005:2011 considering asset "service" from a technical point of view but also in terms of impact on the processed information.In the second part we will explain why this standard should evolve and how such a service-oriented approach can improve a risk management process.

A. Conduct of ISO/IEC 27005 Standard

1) Context establishment: Unlike existing work in the literature, we do not deal with the study of securing the web services themselves. We rather propose to study the impact of using a SOA on the information system security from the point of view of the risks related to information security. Indeed, if technologies such as web services bring new features and even generate new needs, they introduce however new vulnerabilities within the IS and, therefore, new risks for IS Security.

Our work concerns the interconnection of information systems (broadly defined) through the use of web services. We do not focus on the "internal" security of these web services (eg injection of erroneous parameters), but rather on the impact of a "failure" of a web service on the IS.

2) Identification of assets: In this context, we are led to consider two types of assets:

- web services themselves: input and output data flows, business processes they implement,...
- underlying communications infrastructure: systems (computers and OS), network, software platforms (eg SOAP implementation, servlet container),...

3) Identification of threats: According to the glossary of keywords for information security established by NIST [16], a threat is defined as *"any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service"*.

Within the meaning of ISO standards, a threat is *"a potential cause of an incident, that may result in harm of systems and organization"*. Threats may be of natural or human origin, and could be accidental or deliberate. A risk is *"the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization; it is measured in terms of a combination of the probability of occurrence of an event and its consequence"*.

With regard to the field of our study, here is a non exhaustive list threats that could affect the operation of web services:

- an incident on the network causes malfunctions (excessive delays, loss of connection)
- a malicious person intercepts messages and forge new posts to harm the IS and/or access certain information
- a software error (accidental or deliberate) on a WS causes the sending of erroneous results

4) Identification of vulnerabilities: Vulnerability can be defined as *"a weakness in the information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source"*. This definition considers not only the vulnerabilities of software components, but also organizational aspects.

When talking about vulnerabilities of service-oriented architectures (SOA), some are now known (OWASP[9], MITRE and the CVE[10] project), but we must also take into account all the components that are part of this technology and are the target of attacks (WS-attacks.org[11]) like web service client, web service server, BPEL engine, intermediaries in the web service architecture (threat as "Man in the Middle"), XML parser, schema validation (XML), signature verification, encryption and decryption processes.

From these, it is possible to point out some examples of vulnerabilities and associated threats as interception and tampering of a WS request ($\rightsquigarrow$ identity spoofing), tampering WS metadata (WSDL file, WS-security-policy) ($\rightsquigarrow$ abuse of rights), WS-Addressing hacking to change the destination address of the message ($\rightsquigarrow$ data theft), BPEL engine flooding with a huge number of SOAP requests ($\rightsquigarrow$ service no longer available).

Under the ISO/IEC 27005 standard, these vulnerabilities are already referenced in Appendix D within the types "hardware", "software" or "network". Moreover, a number of existing standards and related technologies already allows to strengthen these aspects of WS security (cf. Section II-B2).

[9]OWASP: the Open Web Application Security Community

[10]CVE: Common Vulnerabilities and Exposures

[11]http://clawslab.nds.rub.de/wiki/index.php

Our research activities are at a higher level of granularity: we focus on the security of the information itself (content structure, chain of production and consumption, economic and legal issues related to the information) and not as a "simple" input/output parameter flowing within the IS. If you look at the cycle of information processing (storage, processing, transport) as such, it is certain that many vulnerabilities and threats are emerging with the use of "cloud" services. Thus, we can classify these vulnerabilities according to several categories [17].

a) ***Quality of Service****:* despite the Service Level Agreements (SLA) it is not uncommon to be faced with frequent breakdowns and unavailable services (eg, Amazon EC2, April 2012) which can reach thousands of users around the world. The only possible compensation is financial whereas your image reputation and goodwill may have been heavily impacted. Similarly what about the customer ? Can he migrate to another service provider ? Are there interoperability, portability, transferability when the client wants to take back his information ?

b) ***The location of data and processing****:* these outsourced services can be located anywhere in the world, sometimes without any possibility to choose the country. However, as laws differ from one country to another, some information may be acceptable in one country but prohibited in another.

c) ***Loss of control of information****:* when using outsourced services, companies entrust their data to the provider. That raises various issues about control over critical data of companies (eg research & development, business strategy):

- ***incident*** at the service provider: is it always possible to recover data ? Who is responsible for making backups: clients or the provider ?
- ***reversibility***: it is supposed to allow the client to repossess his data at any time without justification. But the lack of standards for interoperability and migration induces a strong dependency towards the provider.
- ***termination of the contract***: physical erasure of data is rarely complete. Frequently, the provider can not offer any warranty: redundant architectures, backups, archives, indexes, analytics (how many copies ? location ? are there still data somewhere?)

d) ***Information ownership****:* when processing information in the cloud, we entrust the capital of the company to a third party. What happens in case of litigation (eg non-payment, injunction), if the provider goes out of business (eg bankruptcy, acquisition by another company),... ? Can the provider keep your data ? Has he contractually the right to continue to exploit them ?

e) ***The type of information****:* in addition to the traditional data that can be processed in a company, there are those who are particularly sensible: critical data (research and development) and personal data. Regarding personal data, they can be opened by laws in a country whereas they are closed in others (eg USA PATRIOT Act, FISAAA[12]), which may have an impact on privacy.

[12]FISAAA: US Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008

5) Identification of consequences: From this list of vulnerabilities (not exhaustive) we can now present some basic scenarios illustrating the occurrence of a threat that exploits a vulnerability in a service with its impact on the information system. We distinguish "classical" vulnerabilities (•) that can be addressed using existing technologies and security controls (cf. Section II-B2) and "organizational" vulnerabilities (○) affecting the security of the information itself.

- **Identity spoofing:** in a web service context, authentication attacks bypass identification controls by using a number of different techniques, such as session hijacking, session replay, session fixation, identity spoofing, valid credentials theft, authentication module subversion, and brute-forcing. As a result of a successful attack, an illegitimate user will be identified as a legitimate one to access new resources [18].
- **Tampering WS metadata**: Maliciously changing the content of the WSDL file [19]. This usually aims at lowering the security requirements of an web service. The information that certain message data is required to be encrypted just gets removed, resulting in an unencrypted communication between web services, enabling the attacker to read the message content.
- ○ **Trust in service**: a failure of one service may affect the operation of another service cascade hosted in this container. This repetition of failure can lead to a domino effect where each service sends its error successively [20].
- ○ **Quality of Service**: The service provider does not fulfill the service by itself; it is a broker with service subcontractors. In case of litigation or digital forensics the issues regarding the quality of the services and/or responsabilities are very difficult to determine.
- ○ **Data stored in a foreign country**: However, some businesses do not like the ability of a country to get access to their data via the court system, for example, a European customer might be concerned about using Cloud Computing system in the United States given the USA PATRIOT Act [21], FISAAA, RIOT[13] and PRISM (since 2007 and revealed in june 2013 by Edward Snowden). In this case the loss of privacy is obvious, whether data is personal or not [22].
- ○ **Prohibited or copyrighted informations**: when sharing a service that is not looking at the origin of the data it stores, the service can be closed overnight eg. Megaupload 2012, resulting in a direct loss of data for the friendly customers of the law.
- ○ **The provider has financial difficulties**: the supplier fails and stops the services it provides. It can also claim money to restore your data (eg 2e2.com 2013).
- ○ **Data recovery**: closing procedures of a service, such as at the end of a contract, should provide the ability to retrieve data (reversibility) but also ensure their final removal on provider's servers (physical erasure of data).

After identifying the incident scenarios, it is necessary to assess the likelihood of each scenario and impact occurring, using qualitative or quantitative analysis techniques. This should take account of how often the threats occur and how easily the vulnerabilities may be exploited.

[13]RIOT: Rapid Information Overlay Technology by Raytheon

B. Evolution of ISO/IEC 27005 Standard Towards Services

As explained in this paper, our work concerns information security as a whole: from contents to economic and legal issues. This approach does not question the concepts established in the ISO/IEC 27005:2011 standard. Instead, it is complementary because our proposal is to add in Annex D of the ISO/IEC 27005:2011 standard a new type named "service" with vulnerabilities and threats related to WS technology and services provided: it is a kind of super-type over existing types "hardware", "software" and "network".

After setting the type "service" in this nomenclature, vulnerabilities, and therefore the associated threats, are viewed in a new light. The main advantage is that the scenarios are closer to reality: we talk about "denial of service" by example rather than "loss of network connection"; "service provider returning erroneous data" instead of "software failure". These vulnerabilities bring simple questions that are at the heart of every service user and allow it to guarantee some "controllability" about his data:

- Can I act freely on my data ?
- How do I know where is my data ?
- How do I know who can access my data ?
- Do I own my data ?
- Can I easily change provider ?
- In what country is my data stored ?
- My data are they legal in the country where they are stored ?
- Does my provider impose respect for the intellectual property to all its customers (to avoid being forced to close) ?

In the Table I, we used the same formalism as in Annex D of the ISO/IEC 27005:2011 standard to present a (non-exhaustive) list of vulnerabilities and threats associated with specific "service" type and taking into account the proposals developed in the previous sections. The new ISO/IEC 27010, 27017 and 27018 standards will not replace our approach. Instead, they merely reaffirm, by their existence, the necessity to take into account the notion of "service" in a process of risk management.

Thus, the concept of "controllability" appears fundamental in the design of information systems using third party services. The IT architect must be absolutely sure that he can organize, manage and thus "control" his services, to avoid that his information system becomes unusable.

From this premise, it is quite possible to define a fourth security criterion specific to services, in addition to the three basic criteria CIA:

1) **Confidentiality**: it prevents the unauthorized disclosure of information (eg illegal read access)
2) **Integrity**: it guarantees the accuracy, completeness, validity and stability of information
3) **Availability**: it ensures continuity of service and system performance
4) **Controllability**: it ensures complete control over services used

Type	Examples of vulnerabilities	Examples of threats
Hardware	...	...
Software	...	...
Network	...	...
Service	Lack of long term support from service provider	Service no longer available
	Unknown life cycle and update policies from service provider	Unexpected change of the service interface
	Unknown country to host services	Spying, data theft
	Failure to comply with the laws in force	Service no longer available
	Provider goes bankrupt	Service no longer available
	Laws on privacy differ in the country of use	Loss of confidentiality
	Laws on information security are less restrictive	Spying, data theft
	Laws on information security are more restrictive	Service no longer available
	Inadequate Service Level Agreement	Breach of maintainability of the IS
	Lack of data recovery procedure	Breach of maintainability of the IS
	Lack of reversibility (migration, interoperability)	Breach of maintainability of the IS
	Lack of data erasure at the end of the contract	Data theft, unauthorized use
	Lack of WS metadata security	Tampering with the web service
	Possible multiple requests to the WS	Identity spoofing
	Lack of traceability of the service provided	Breach of trustworthiness of information
Personnel	...	...
Site	...	...
Organization	...	...

TABLE I. A NEW TYPE "SERVICE" IN ANNEX D OF THE ISO/IEC 27005:2011 STANDARD

V. RELATED WORK

As we previously described, information exchange between systems and particularly in the cloud introduce new risks with regard to information system security. As pointed out in [23] there are two methods to remedy: trust the service provider or implement technical mechanisms to compensate for a trust worthy supplier.

First to compensate the lack of trust in a service it's necessary to put in place mechanisms that enable secure information exchange between systems. In [24] authors discuss security issues for cloud computing and present a layered framework for secured cloud storage. They focus on essential aspects: how to store data in foreign machines, queyring encrypted data and secure this queries.

On the other hand it is also necessary to estimate the security coverage for different type of services. In [25] authors describe a framework which can prescribe the right combination of security tools for different cloud services and according to the level of security assurance required.

Accountability as seen from a holistic point of view, covering legal, socio-economic, regulatory and technical aspects is presented in [26]. That European project named A4Cloud aims at four objects which tackles accountability developing tools that:

1) enable cloud service providers to give their users appropriate control and transparency over how their data is used,
2) enable cloud end users to make choices about how cloud service provider may be use,
3) monitor and check compliance with user's expectation, business policies and regulations,
4) develop recommendations and guidelines for how to achieve accountability for the use of data by cloud services.

The project seems to be a promising approach that tackles preventive, detective and corrective control which allow to achieve accountability.

In [27] authors introduce the notion of autonomous self-controlling objects (SCO), that adapt to the location and other contextual dimensions. The sensitive resources assure their protection by means of adaptive security policies of various granularity, and synchronization protocols.

In the European Network and Information Security Agency (ENISA) a Preparatory Action entitled "Trust and privacy in the Future Internet" covers in one work package identity, accountability and trust in the Future Internet [28]. The objective is to study security models of electronic services and their performance in highly distributed environments, such as today's Internet. Furthermore, ENISA investigates various ways of assuring privacy and accountability on the Internet, reviewing the most prominent methods used, studying their mapping to the underlying architectures and assessing their level of effectiveness and performance. ENISA also works towards the development of recommendations on the use of specific service models in given environments and architectures.

VI. CONCLUSION AND FUTURE WORK

Service Oriented Architecture (SOA) models incuding cloud services are increasingly used because of the benefits they provide. However, from the point of view of information security risk management, these technologies introduce new vulnerabilities with regard to network connections, the use of external services that we can not control, responsibilities related to the provision of service,... Of course, there are

solutions to secure these exchanges and design "reliable" web services. Our work is complementary to these solutions because we operate at the level of information security within the meaning of the ISO/IEC 27005:2011 standard. Our goal is to refine the process of risk management to the specificities of services in an SOA by taking into account the information in its entirety, including socio-economic and legal aspects. We therefore suggest to extend the ISO/IEC 27005:2011 standard to include consideration of services (web services, cloud) in the risk assessment of information security.

Having identified a number of scenarios that can not be avoided through the existing security mechanisms, the second phase of our work is to propose a security model for communications between IS. To achieve this goal, we consider a usage control oriented approach, as we have already experienced in our previous work on intelligent documents [29], [30], [31] (cf. *Enterprise Digital Right Management*). The use of metadata for traceability of communications (via these services) will also allow us to compute indicators that can, for example, be used to monitor the IS. Thus, these mechanisms allow us to strengthen the security of information we may entrust to a service provider.

Enhancing the importance of providing more transparency and control to processes mediated by the cloud and taking into account that data is dynamic due to the complex responsibility chains, we also propose as a perspective an approach based on preventive, detective and corrective accountability methods [32].

The implementation of this model is obviously one of our prospects. This is what led us to consider Web Services technology since many dedicated security specifications have been developed about the SOAP protocol. Moreover, these specifications (presented in Section II-B2) are "open", that is to say that we are free to implement our own models and security policies.

REFERENCES

[1] ISO/IEC, "ISO/IEC 27005:2011: Information security risk management," International Organization for Standardization (ISO), Geneva, Switzerland, Published, 2011.

[2] R. T. Fielding and R. N. Taylor, "Principled design of the modern web architecture," in *Proceedings of the 22nd international conference on Software engineering*. ACM, 2000, pp. 407–416.

[3] W3C, "SOAP version 1.2," W3C Open Source Software, Tech. Rep., june 2003.

[4] UserLand, "XML-RPC," UserLand Software, Inc., Tech. Rep., 1999.

[5] E. Bertino, L. Martino, F. Paci, and A. Squicciarini, *Security for Web Services and Service-Oriented Architectures*. Springer Publishing Company, Incorporated, 2009.

[6] K. Beznosov, D. J. Flinn, S. Kawamoto, and B. Hartman, "Introduction to web services and their security," *Information Security Technical Report*, vol. 10, no. 1, pp. 2 – 14, 2005.

[7] C. Geuer-Pollmann and J. Claessens, "Web services and web service security standards," *Information Security Technical Report*, vol. 10, no. 1, pp. 15 – 24, 2005.

[8] D. Eastlake and J. Reagle, "XML Encryption Syntax and Processing," W3C, Tech. Rep., 2002.

[9] M. Bartel, J. Boyer, B. Fox, B. LaMacchia, and E. Simon, "XML Signature Syntax and Processing," W3C Open Source Software, Tech. Rep., 2008.

[10] A. Nadalin, C. Kaler, P. Hallam-Baker, R. Monzillo, and E. Al., "Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)," *OASIS Standard*, vol. 200401, no. February, 2006.

[11] Cantor, Kemp, Philpott, and Maler, "Security Assertion Markup Language (SAML)," OASIS, Tech. Rep., 2005.

[12] T. Moses and S. Godik, "eXtensible Access Control Markup Language (XACML) Version 1.0," OASIS, Tech. Rep., 2003.

[13] M. Lorch, S. Proctor, R. Lepro, D. Kafura, and S. Shah, "First experiences using xacml for access control in distributed systems," in *Proceedings of the 2003 ACM workshop on XML security*. ACM, 2003, pp. 25–37.

[14] C. Alberts and A. Dorofee, "An introduction to the OCTAVE method," *Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University*, 2001.

[15] "BS 7799:Part 1:1995 information security management code of practice for information security management systems," BSI British Standards, Tech. Rep., 1995.

[16] "NIST IR 7298 Rev. 1: Glossary of key information security terms," National Institute of Standards and Technology, Computer Security Ressource Center, Tech. Rep., Fév-2011.

[17] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," *Security Privacy, IEEE*, vol. 9, no. 2, pp. 50–57, March 2011.

[18] G. Álvarez and S. Petrović, "A new taxonomy of web attacks suitable for efficient encoding," *Computers & Security*, vol. 22, no. 5, pp. 435–449, 2003.

[19] M. Jensen, N. Gruschka, and R. Herkenhöner, "A survey of attacks on web services," *Computer Science-Research and Development*, vol. 24, no. 4, pp. 185–197, 2009.

[20] V. Dialani, S. Miles, L. Moreau, D. De Roure, and M. Luck, "Transparent fault tolerance for web services based architectures," in *Euro-Par 2002 Parallel Processing*. Springer, 2002, pp. 889–898.

[21] L. T. Lee, "USA PATRIOT Act and telecommunications: Privacy under attack," *Rutgers Computer & Tech. LJ*, vol. 29, p. 371, 2003.

[22] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: a survey," in *Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on*. IEEE, 2010, pp. 105–112.

[23] W. Pieters, "Security and privacy in the clouds: a bird's eye view," in *Computers, privacy and data protection: An element of choice*. Springer, 2011, pp. 445–457.

[24] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, "Security issues for cloud computing," *International Journal of Information Security and Privacy (IJISP)*, vol. 4, no. 2, pp. 36–48, 2010.

[25] D. Dasgupta and M. M. Rahman, "Estimating security coverage for cloud services," in *Privacy, security, risk and trust (PASSAT), 2011 IEEE third international conference on and 2011 IEEE third international conference on social computing (SocialCom)*. IEEE, 2011, pp. 1064–1071.

[26] S. Pearson, V. Tountopoulos, D. Catteddu, M. Sudholt, R. Molva, C. Reich, S. Fischer-Hubner, C. Millard, V. Lotz, M. G. Jaatun *et al.*, "Accountability for cloud and other future internet services," in *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*. IEEE, 2012, pp. 629–632.

[27] A. C. Squicciarini, G. Petracca, and E. Bertino, "Adaptive data protection in distributed systems," in *Proceedings of the third ACM conference on Data and application security and privacy*. ACM, 2013, pp. 365–376.

[28] "Privacy, accountability and trust – challenges and opportunities," European Network and Information Security Agency (ENISA), Heraklion, Crete, Greece, A report by the ENISA Ad Hoc Working Group on Privacy and Technology., 2010.

[29] M. Munier, V. Lalanne, and M. Ricarde, "Self-protecting documents for cloud storage security," in *TrustCom*. IEEE, 2012, pp. 1231–1238.

[30] M. Munier, "A secure autonomous document architecture for enterprise digital right management," in *SITIS*. IEEE, 2011, pp. 16–23.

[31] M. Munier, "A multi-view approach for embedded information system security," in *CRiSIS*. IEEE, 2010, pp. 65–72.

[32] E. Jaramillo, M. Munier, and P. Aniorté, "Information security in business intelligence based on cloud: A survey of key issues and the premises of a proposal," in *WOSIS*, 2013.