
Book Section:
Corrales, M and Djemame, K orcid.org/0000-0001-5811-5263 (2017) A Brokering Framework for Assessing Legal Risks in Big Data and the Cloud. In: Corrales, M, Fenwick, M and Forgo, N, (eds.) New Technology, Big Data and the Law. Perspectives in Law, Business and Innovation . Springer , pp. 187-222. ISBN 9789811050381

https://doi.org/10.1007/978-981-10-5038-1_8

A BROKERING FRAMEWORK FOR ASSESSING LEGAL RISKS IN BIG DATA AND THE CLOUD

MARCELO CORRALES & KARIM DJEMAME

Contents

ABSTRACT "Cloud computing" and "Big Data" are amongst the most hyped-up terms and buzzwords of the moment. After decades in which individuals and companies used to host their data and applications using their own IT infrastructure, the world has seen the stunning transformation of the Internet. Major shifts occurred when these infrastructures began to be outsourced to public Cloud providers to match commercial expectations. Storing, sharing and transferring data and databases over the Internet is convenient, yet legal risks cannot be

eliminated.[1] Legal risk is a fast growing area of research and covers various aspects of law. Current studies and research on Cloud computing legal risk assessment have been, however, limited in scope and focused mainly on security and privacy aspects.[2] There is little systematic research on the risks, threats and impact of the legal issues inherent to database rights[3] and "ownership" rights of data. Database rights seem to be outdated and there is a significant gap in the scientific literature when it comes to the understanding of how to apply its provisions in the Big Data era. This means that we need a whole new framework for understanding, protecting and sharing data in the Cloud. The scheme we propose in this chapter is based on a risk assessment brokering framework that works side by side with service level agreements (SLAs). This proposed framework will provide better control for Cloud users and will go a long way to increase confidence and reinforce trust in Cloud computing transactions.

Keywords Cloud Computing, Big Data, Service Level Agreements (SLA), Cloud Brokers, Legal Risks, Mutual Trust.

1 Introduction

Before embarking on the generally known caveats regarding legal risks, we would like to point out what Claudio Ciborra, an information theorist, has explained in his writings on information systems and risk management.[4] In what he called the "duality of risk",[5] he reminds us "life, risk and technology are getting more intimate than ever…".[6] According to Ciborra, it is not just that our society is becoming increasingly dependent on mobile phones and computers as the primary means of communication; it is not about business transactions processed through electronic networks; it is not even about jobs being fully automated; or human reasoning being replaced by human-like artificial intelligence that emulates the

[1] See, e.g., Disselkamp (2013), Chapter 8 with further references.
[2] See, e.g., Peng, Dutta and Choudhary, (2014), p. 134.
[3] See Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
[4] Gutwirth and Hildebrandt (2010), p. 33.
[5] For details, see Ciborra (2005).
[6] Ciborra (2007), p. 27.

decision-making of human experts[7]. Looking ahead and reflecting on the next generation of information communication technology (ICT) platforms and risk management, the challenge is that "our life (project) becomes simultaneously conditioned, constrained or enabled by Grid technologies. The technology is already there, albeit in an indirect and hidden form…".[8]

Ciborra wrote the above lines more than ten years ago and Grid technologies evolved into different models.[9] As a matter of fact, Cloud computing is a kind of Grid computing, which focuses on the quality of service (QoS) and reliability problems.[10] The Cloud differs from the Grid essentially in the implementation details.[11] According to Ciborra, change and innovation brings the emergence of new risks, however, his vision goes beyond to suggest that risks are often the source of innovation[12] and new order.[13] As such, risk is not, in itself, a bad thing; rather, it is essential for accelerating progress.[14]

The aim of this chapter is to widen the lens through which we view risk and analyze particular kinds of legal risk connected to the design and deployment of Grid and Cloud computing infrastructures in brokerage scenarios.[15] This chapter presents an SLA brokering framework including innovative risk-aware assessment techniques, which facilitates the clarification of database and "ownership" rights of data and evaluates the probability of SLA failure. We use the web service agreement specification (WS-Agreement)[16] as a template and extend prior work on risk metrics from the OPTIMIS project[17] to facilitate SLA creation between service consumers and providers within typical Cloud brokerage scenarios. However, since the WS-Agreement allows for an automated mechanism between only two parties and does not cover the use of an intermediary within the agreement process, we use the specific

[7] For details about artificial intelligence (AI) and expert systems, see e.g., Jackson (1998).
[8] Ciborra (2007), p. 27.
[9] For details about the evolution of Grid infrastructure technologies, see e.g., Jones and Bird (2013), pp. 160 et seq.
[10] Kasemsap and Sunandha (2015), p. 33.
[11] Teng and Magoules (2010), p. 126.
[12] Shantz (2005), p. 511.
[13] Ciborra (2009), p. 78.
[14] Drissi, Houmani and Medromi (2013), p. 143.
[15] See, e.g., Gourlay, Djemame and Padgett (2008), pp. 437-443.
[16] See Andrieux et al. (2007); See also, Gourlay, Djemame and Padgett (2008), p. 438. More specifically, for negotiating and creating SLAs, we use the WSAG4J framework developed at Fraunhofer Institute SCAI. The WSAG4J is basically a tool that helps you to create and manage SLAs in distributed systems and has been fully implemented as part of the Open Grid Forum (OGF) WS-Agreement standard. For details, see https://packcs-e0.scai.fraunhofer.de/wsag4j/ accessed 10 October 2016.
[17] Optimized Infrastructure Services (OPTIMIS) was a EU funded project within the 7th Framework Program under contract ICT-257115. The project developed an open source toolkit designed to help Cloud service providers to build and run applications in the Cloud. New features that include the clarification of database rights and "ownership" rights of data have been implemented. The toolkit has been integrated into the Open Nebula Ecosystem and the Infrastructure as a Service Cloud computing project Open Stack.

work carried out in the AssessGrid project[18] that includes a brokerage mechanism and pays considerable attention to addressing a risk assessment.[19]

SLAs are facilitators for increasing the commercial uptake of Cloud computing services. They provide clear-cut rules concerning the expectations and obligations between service consumers and providers.[20] However, current frameworks fail to provide flexibility[21] and there is no global standard that clarifies database rights and more generally "ownership" rights of data. Therefore, it is always advisable to thoroughly check Cloud SLAs before being legally bound by the terms of contracts. Furthermore, without the ability to evaluate the probability that a SLA might fail, market growth will be limited, since neither party will be willing to agree. By introducing a database and "ownership" rights risk assessment alongside automated SLA creation and negotiation processes, end-users can uncover high-risk areas to attenuate such risks, and eliminate those Cloud providers that will not promote their needs.

This chapter is divided into 10 sections. Section 2 briefly reviews the extant literature with regard to risk assessment in the Cloud. It also explains the motivation and justification for deepening and expanding research into other areas of law such as database rights and "ownership" rights of data. Section 3 is concerned with the methodology used for this study, namely a risk-based approach through the whole service life cycle. Section 4 presents an overview of the legal risks involved and how a risk mitigation strategy will enhance legal interoperability. Section 5 delves into detail concerning database and "ownership" rights of data, focusing on the three key themes that create risk in Cloud computing and Big Data projects. Section 6 begins by offering a glimpse of the main actors involved. Then it goes on to explain the two general use cases considered. Finally, it explains the brokering mechanism and risk assessment techniques using WS-Agreement, which facilitates the creation of risk-aware SLAs between end-users and Cloud providers. Section 7, presents the risk inventory within the system architecture design. It includes an updated and customized risk inventory focused on the legal areas considered to present the higher risks and constrains. Section 8 explains step-by-step the different stages of the risk assessment process in Cloud brokerage scenarios. In Section 9 a hypothetical scenario is considered to showcase how risk assessment can be effectively applied in real cases. Finally, Section 10 concludes.

[18] The Advanced Risk Assessment and Management for Trustable Grids project (AssessGrid), was founded by the EU Commission under the FP6 IST framework (contract no. 031772).
[19] Padgett et al. (2009).
[20] Djemame et al. (2011b), p. 1558.
[21] See, e.g., Kirkham et al. (2012), p. 1063.

2 Risk Assessment: Literature Review, Motivation and Justification

As the realization of Cloud-based services and infrastructures advance[22] from one single private Cloud infrastructure, towards more complex migrations in dynamic federated scenarios consisting of several coexisting public or hybrid Clouds, there are increasing high level concerns. These concerns include issues of risk, trust and legal considerations that establish solid foundations for the non-functional requirements[23] of the ecosystem. Cloud migrations have reached a high level of development, yet the management of Cloud services entails a loss of control over the data being processed. This also impairs the trustworthiness in Cloud computing technology because end-users are not entirely confident in using the Cloud.[24]

There are many legal risks involved that have been magnified by the Big Data movement to the Cloud.[25] The American Heritage dictionary defines risk as "the possibility of suffering harm or loss; danger". "A factor, thing, element, or course involving uncertain danger; a hazard".[26] Similarly, the Black's Law Dictionary defines risk as "the uncertainty of a result. Happening or loss; the chance of injury, damage or loss; esp., the existence and extent of the possibility of harm".[27] Therefore, the term risk can be loosely described as exposing oneself to an activity or event that can lead to the possibility of damage, harm or loss.

Risk assessment is fundamental for widespread commercial adoption, and risk management tools need to be integrated into the emerging Cloud paradigm.[28] While a variety of definitions of the term "risk management" have been suggested, in this work we adopt the definition given by the International Standards Organization (ISO) as follows: "a coordinated set of activities and methods that are used to direct an organization and to control the many risks that can affect its ability to achieve objectives".[29] This definition is close to the Black's Law Dictionary definition that refers to risk management as: "the activity of identifying,

[22] See Mahmood (ed) (2014).
[23] Note: Non-functional requirements present a systematic approach that provides quality to the software system. They define the criteria used in the system operation, which is specified in the system architecture. For a comprehensive explanation of non-functional requirements see, e.g., Chung et al. (2000); Chung and Sampaio Do Prado Leite (2009).
[24] Li and Singh (2014), p. 670.
[25] Note: "Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs." See Vaquero et al. (2009), pp. 50-55; See also Smith (2009). The above definition is very useful because it also introduces a "customized SLA", which is explored in greater detail in this chapter.
[26] For this term see American Heritage Dictionary.
[27] Garner (2014), p. 1524.
[28] See, e.g., Gourlay, Djemame and Padgett (2009), p. 36.
[29] Plain English ISO 31000:2009.

estimating and evaluating the probability of harm associated with an activity and determining an acceptable level of risk".[30] The underlying concepts of risk assessment and risk management aim to improve the confidence level between a provider and end-user to sign a SLA.[31]

Risk assessment must be introduced proactively into the SLA framework to allow the end users and Cloud providers to automatically recognize critical points of failure (PoF), and to propose corrective actions that would reduce the risks in specific points of the contract in order to avoid soaring transaction costs and preventing future controversies. This precautionary approach is meant to fill in the gaps in the current SLA frameworks, and to imbue a risk management culture among Cloud providers.[32]

Despite the fact that many generic risk management assessment standards exist today such as the ISO 31000:2009,[33] one major difficulty that might arise in the implementation of this requirement is the lack of a standard risk assessment method for database rights and "ownership" rights of data. There are several risks and significant effort has been devoted to other areas of law such as privacy, data protection and data security.[34] For example the ISO 22307:2008 [35] privacy impact assessment (PIA), [36] for financial services and banking management, the ISO/IEC WD 29134 PIA methodology,[37] which is expected by 2016, the ISO/IEC 29101:2013 for information technology security techniques and privacy architecture framework[38] and the ISO/IEC NP 19086-4 for Cloud computing SLA framework still under development.[39]

The European Network and Information Security Agency (ENISA) released at the end of 2012 the updated version of its 2009 Cloud security risk assessment. The risks are classified into three categories: a) Policy and Organizational, b) Technical, and c) Legal. It contains a

[30] Garner (ed) (2014), p. 1525.
[31] Sangrasi, Djemame and Jokhio (2012), pp. 445-452.
[32] See, e.g., Nwankwo (2014).
[33] Note: ISO 31000:2009 risk management standard sets out the principles and guidelines on risk management that can be applied to any type of risk in any field of industry or sector.
[34] Cattedu and Hogben (eds) (2009).
[35] Note: ISO 22307:2008 is a privacy impact assessment for financial services and banking management tools. It recognizes the importance to mitigate risks associated to consumer data utilizing automated and networked systems.
[36] See, e.g., generally, Corrales (2012); Wright and De Hert (eds) (2012).
[37] For details, see http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62289 Accessed 10 April 2016.
[38] ISO/IEC 29101:2013 Information Technology - Security Techniques - Privacy Architecture Framework. For details, see http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45124&commid=45306 Accessed 10 October 2016; See also Nwankwo (2014).
[39] ISO/IEC NP 19086-4 Information Technology - Cloud Computing - Service Level Agreement (SLA) framework and technology - Part 4 Security and Privacy. For details, see http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=68242 Accessed 10 October 2016; See also Nwankwo S (2014).

list of 23 risks. One of these risks refers to intellectual property issues, which is a good indicator that the perceptions of associated risks of Cloud computing has put intellectual property rights (IPRs) under the radar. However, this is described, in our view, too broadly and focuses mainly on the copyrights of original work such as new applications, software, etc., while other aspects of IPRs such as database rights are not mentioned. As with all the IPRs described in the ENISA recommendations, database rights and other issues related to "ownership" rights of data must be clarified by the adequate contractual clauses and within the service manifest of the SLA otherwise this might be at risk. ENISA has played a crucial role in providing stakeholders an overview of the main risks involved in Cloud computing and there is a second review round envisaged by the group of experts set up by ENISA where legal aspects will be revised in more detail as this was excluded from the first round.[40]

Until now, no systematic investigation has adequately explained database rights and "ownership" rights of data with consideration being given to the Cloud and Big Data phenomenon. In this regard, the present study is the first to undertake a specific risk analysis in this domain and aims to contribute to this growing area of research. Understanding the link between Big Data, database rights and "ownership" rights of data, will help to reduce the legal uncertainties and risks involved in Cloud transactions. Thus, the broadening of the scope of the risk assessment methods followed hitherto is accordingly designed and advocated in order to establish priorities and make strategic choices of Cloud providers a global reality.

Incorporating risk assessment techniques in Cloud brokerage scenarios and including database rights and "ownership" rights of data during SLA negotiations and service operation, will aid the decision-making process regarding contractual agreements. There is a current lack of confidence and trust in terms of the uncertainties involved with the SLA level of quality.[41] This is one of the most important barriers to the adoption of Cloud computing. In order to improve confidence and create more trust in Cloud transactions, it is necessary to improve control over the resources available. The design of Cloud architecture related to application deployment seems to be the best route to achieve this. This will also create more optimized and transparent resources.[42]

It is important to bear in mind that it is not possible to reduce all the risks down to zero. Nevertheless, mitigation strategies may at least increase the confidence of end-users and lead to a reliable productivity and cost-effective solution for Cloud service providers. In this research confidence is defined as "the expectation of a successful fulfillment of SLA agreed

[40] Dupré and Haeberlen (eds) (2012).
[41] Djemame et al. (2011a), p. 119.
[42] See, e.g., Kirkham et al. (2013), p. 7.

between a Cloud service consumer and a Cloud service provider",[43] and the notion of cost-effective and reliable productivity as a "providers capability of fulfilling an SLA through the entire lifecycle of the service provision and at the same time realizing its own business level objectives". In other words, capitalizing and making a certain amount of profit, while optimizing the efficacy of infrastructure provider resources.[44]

Based on the framework of the OPTIMIS[45] and AssessGrid software toolkits, as a basic risk factor mechanism, the main contributions of this research are the design and effective implementation of a risk assessment framework tailored to database rights and "ownership" rights of data with an eye towards Big Data and other future similar movements. This can be efficiently implemented into other high-level Cloud management and control software systems for both service providers and infrastructure providers. Although a specific risk assessment is the main focus of this chapter, we also consider the decision-making process of how to implement corresponding mitigation strategies that may involve other high level considerations such as cost-efficiency and trust.[46]

3 Risk Assessment Methodology

Risk analysis can be examined at various stages of Cloud interactions. Each of the actors involved in the Cloud will have their own concerns and points of view towards others in terms of trust, risks and legal issues.[47] They might have specific legal demands that need to be taken into consideration. For example, how to reconcile the "ownership" of data that may accrue from the use of Cloud computing technology? New data can be potentially created out of the data derived from the usage of various tools such data mining, analytics, AI, etc. The concept of "ownership" in this context implies that the owner can control how the data will be regulated.[48] Events like this and their impact need to be assessed in order to compute an overall probability of SLA violation, which requires a detailed analysis. This assessment will also depend on the Cloud deployment scenario - bursting, federated, hybrid, etc.[49] In this research we will consider a Cloud brokerage scenario since the broker can participate as an intermediary in any of these scenarios.

[43] Djemame et al. (2011a), p. 119.
[44] Djemame et al. (2011a), p. 119.
[45] For details, see Ferrer et al. (2011), pp. 67-77.
[46] Djemame et al. (2011a), p. 119.
[47] Khan et al. (2012), p. 122.
[48] Djemame et al. (2012), p. 3..
[49] Khan et al. (2012), p. 122.

These legal concerns can also be refined considering the different stages of the Cloud lifecycle as follows: (a) the service deployment stage for initial placement of services on Cloud providers taking into account the legal issues as a gauge for Cloud provider selection, and; (b) the service operation, where Cloud resources and databases are managed by the Cloud provider for the attainment of all the service-level objectives (SLO), including the legal ones. During these two stages, legal risks need to be continuously and systematically monitored in order to avert any additional transaction costs to be incurred to the end-users and Cloud providers.[50] Figure 1 below describes the risk assessment steps during service deployment and service operation.

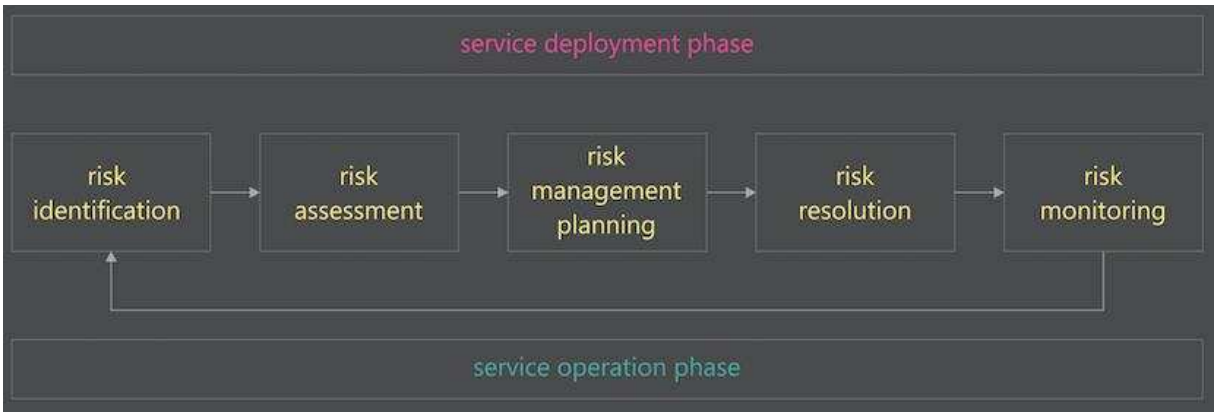

Figure 1: Risk assessment life cycle during service deployment and operation

A number of stages have been identified as a process with the aim of performing a complete risk assessment on Clouds. Each iteration is used to parse in real time, a core risk assessment and helps us to better understand the process. The constituent parts of this approach and their relationships are further explained below.[51]

3.1 High Level Analysis of the System

A primary high-level analysis of the different deployment scenarios aids identifying the actions and assets involved at different stages of the risk assessment process. This helps to effectively identify the vulnerable parts of each asset and how they can change through time. As a general rule, legal concerns need to be assessed before the service deployment phase if the SLA demands specific expectations to be met. In the service operation phase, the legal issues involved are constantly monitored throughout the service execution.[52]

[50] Khan et al. (2012), p. 122.
[51] Kahn et al. (2012), p. 122.
[52] Kahn et al. (2012), p. 122.

3.2 Identifying the Assets Involved

There are various assets that need to be protected from specific threats during service deployment and operation phases. From a legal perspective we refer here to data, databases and the terms specified in the SLA.[53]

3.3 Identifying the Threats in Each Cloud Deployment Scenario

The risk assessment model adopts a systemic approach by which threats and vulnerabilities can be identified. The risk analysis methodology is linked to a threat and vulnerability assessment tool. This systemic approach is particularly helpful because it contains a threat model ensuring synergies with distributed systems and software in general. This model has been adapted to Cloud applications using the CORAS[54] risk modeling language technique, which is an open-source risk-modeling tool.[55]

4 Embracing Legal Risks and Enhancing Legal Interoperability

Richard Susskind, in his book The Future of Law, under the sub-heading: "From legal problem solving to legal risk management", anticipated a paradigm shift in the approach to legal problems. While solving legal problems will not disappear in the future, they will be substantially mitigated with proactive legal risk management tools and services that will pre-empt the conventional reactive legal method.[56] There is an increasing interest in the adoption of risk management methods borrowed from other disciplines that can be effectively adapted to use in the legal domain.[57] Therefore, the proposed software-based risk assessment tools seem a reasonable preventive route for amending the legislative gaps and finding a solution

[53] Kahn et al. (2012), p. 122.
[54] See, e.g., Vraalsen et al. (2005), pp. 45-60.
[55] Kahn et al. (2012), p. 123; Djemame et al. (2012), p. 12.
[56] Note: According to Susskind: "While legal problem solving will not be eliminated in tomorrow's legal paradigm, it will nonetheless diminish markedly in significance. The emphasis will shift towards legal risk management supported by proactive facilities, which will be available in the form of legal information services and procedures. As citizens learn to seek legal guidance more regularly and far earlier than in the past, many potential legal difficulties will be dissolved before needing to be resolved. Where legal problems of today are often symptomatic of delayed legal input, earlier consultation should result in users understanding and identifying their risks and controlling them before any questions of escalation." See Susskind (1998), p. 290.
[57] For details, see e.g., Legal Risk Management http://www.jus.uio.no/ifp/english/about/organization/nrccl/research-areas/ongoing-research/legal-risk-management.html#ref1 Accessed 10 October 2016.

for the many shortcomings of the rigid and unrealistic constraints of traditional black-letter laws.[58]

Preliminary work on legal risk management was undertaken as an approach to providing legal services in various areas of the IT industry and this continues to be an active area of research. However, these generic methods have not reached a high level of sophistication and have not been fully implemented yet.[59] Current software process optimized models do not properly address the legal implications for each phase of the software development lifecycle. The lack of systematic and organized standards in this domain provides only scattered references to legal aspects. This means that legal risks are managed reactively instead of proactively before damage or loss occurs.

Drawing on software projects, Rejas-Muslera et al., presented a significant analysis and discussion on the subject. The authors identified that legal audits are closely related to planning activities. According to Muslera et al., legal activities and measures must be planned in advance and invoked as time goes by across the entire lifecycle of the product or project in order to avoid or reduce negative legal impacts on the achieved objectives. Despite their study covers many aspects of law, including copyright, registration and users rights, data protection, trading standards, etc.,[60] the core interest of the present research lies in the risks associated with managing databases.

The main goal is not to deny these risks and their overall implications but to create a smart strategy than can deal with this trade-off. In the following sections and subsections, we discuss these legal aspects in the context of Big Data and Cloud computing. Legal issues are present at each phase of the whole outsourcing life cycle of a Cloud service. Figure 2 below shows a graphic depiction of the overall model from a high level perspective:

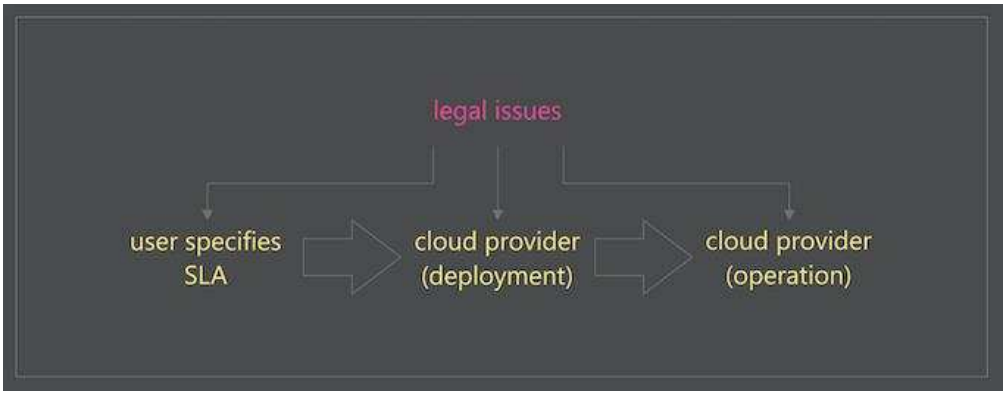

Figure 2: Legal issues and service life-cycle stages

[58] Wahlgren (2007), p. 91; See also Wintgens and Thion (2007), Introduction.
[59] Burnett (2005), pp. 61-67.
[60] Rejas-Muslera, Cuadrado-Gallego and Rodriguez (2007), pp. 118-124.

In the initial contractual agreement stage, the end-user may specify legal clauses with regard to certain service requirements and how such databases must be handled. While large companies and institutions may have more resources to bargain and negotiate specific contractual clauses, the standard nature of the SLAs do not allow much room for single users and SMEs to negotiate the contract.[61] However, an XML automated schema[62] has been specifically crafted to provide more flexibility for smaller companies and individuals so they can clarify database rights and "ownership" rights of data, and all parties involved can be better off. Nevertheless, the point to bear in mind for the moment is that notwithstanding the negotiation capabilities of end-users, these contracts are legally binding. The Cloud provider must fulfill all the requirements and ensure that all clauses will conform to legal rules before deploying the service. Otherwise it will be at risk of facing liability issues should there be any breach of the contract. Therefore, monitoring strategies of legal risks should be present throughout the operation phase.[63]

This framework will improve the legal interoperability among providers on a global scale. According to the GEO Data Sharing Task Force, legal interoperability among multiple datasets from different sources occurs when: "the legal rights, terms, and conditions of databases from two or more sources are compatible and the data may be combined by any user without compromising the legal rights of any of the data sources used.[64] This definition is important for what it includes as the following conditions:[65]

a) The conditions to use data are clear and readily determinable for each dataset,[66]
b) The legal conditions granted to use each dataset permits the creation and use of "combined and derivative products",[67] and;
c) End-users may lawfully get access and use each dataset without seeking permission from data creators.[68]

[61] Bradshaw, Millard and Walden (2010).
[62] Note: XML is a markup language standard that aims to define a format that is both human and machine understandable. Thus humans based on a template model may edit it, and the produced created instance can be processed by according software, following a relevant decision logic. For example, the template model dictates the available fields, the user selects the according values, and then the relevant software may retrieve the XML-based provider descriptions and filter them based on the user's requirements. The XML Description Schema is available at: http://www.optimis-project.eu/content/xml-description-schema-improvement Accessed 10 October 2016. For details about the XML schema see previous chapter.
[63] Batré et al. (2007), p. 193.
[64] For details, see Draft White Paper on Legal Options for the Exchange of Data through the GEOSS Data-CORE. Group on Earth Observations.
[65] White Paper, Mechanisms to Share Data as Part of GEOSS Data-CORE, p. 3.
[66] White Paper, Mechanisms to Share Data as Part of GEOSS Data-CORE, p. 3.
[67] White Paper, Mechanisms to Share Data as Part of GEOSS Data-CORE, p. 3.

Legal interoperability is a bottleneck in Cloud computing transactions, where many resources are available and data is used, re-combined and then derivative data is re-disseminated. This might also prove a great hindrance to public research. The protectionist mentality underlying database rights is, however, very dangerous because it automatically frames access to data as a threat. Within this mindset, there is a risk of databases being locked in. As we shall see soon, the database righst (sui generis right) casts serious problems on the Big Data movement, which does not understands the protection of databases in the same way as the protectionist mentality. The quest for Big Data invites the researcher or entrepeneur to a place where information can lead to innovation and productivity. There should be an equitable trade-off between the protection of databases and access to data that is in the public domain.

The term public domain has come to be used to refer to "information that is: a) not subject to copyright or related rights (including database rights), and; b) not subject to conditions on reuse imposed by other means".[69] This approach could raise and promote social welfare and the goals intended by the Big Data movement by making datasets available to end-users. In a free market economy individuals should be allowed to obtain unrestricted use and re-dissemination of data. This market competition process may help to correct behavioral market problems. The public domain status may be created formally through laws and policies that exempt certain categories of data and information from database protection. However, this could also be achieved through contractual private agreements among parties.[70]

For many scholars, the database right is considered unsuccessful. The detractors of the EU Database Directive have often expressed the criticism that this could be raising hurdles to innovation and free development in various areas of industry.[71] Another objection to database rights is that this may lock up data and information, which can negatively affect the research and academic community that rely on the availability of data and information to carry on their business or research.[72] According to Kingston, the EU Database Directive has been influenced by publisher lobbying, which confers them the potential to attain a continuous monopoly on data.[73] Coining the words of Reichman and Samuelson, the database right is "one of the least

---

[68] White Paper, Mechanisms to Share Data as Part of GEOSS Data-CORE, p. 3.
[69] Summary White Paper, Legal Options for the Exchange of Data through the GEOSS Data-CORE, p. 2.
[70] Summary White Paper, Legal Options for the Exchange of Data through the GEOSS Data-CORE, p. 19.
[71] Sundara Rajan (2011), p. 286.
[72] For the extensive case law on this topic see, e.g., Fixtures Marketing Ltd. v Oy Veikkaus AB, ECJ – Case C-46/02, 9 November 2004 (Finland); Fixtures Marketing Ltd. v Organismos Prognostikon Agonon Podosfairou [the OPAP case], ECJ-Case C-444/02, 9 November 2004 (Greece); Fixtures Marketing Ltd. v Svenska Spel AB, ECJ – Case C- 338/02, 9 November 2004 (Sweden); The British Horseracing Board Ltd and Others v William Hill Organization Ltd., [the BHB case], ECJ, Case C-203/02, 9 November 2004 (United Kingdom).
[73] See Kingston (2010), p. 112. Notably, statistics have shown that about 50% of all legal suits have been raised by a scarce minority of companies that own telephone directories, sport betting fixtures, concert events, and broadcast schedules. See Maurer S (2008), pp. 13-4 – 13-80. Ironically, what these companies have in common

balanced and most potentially anti-competitive intellectual property rights ever created".[74] Finally, opponents of these rights argue that this form of protection is too narrow in scope and fails to address other relevant issues for the database industry.[75] These arguments clearly show the negative perception among some scholars, which prompts worries about its potential negative effects.

It is not the purpose of this research to enter into such controversies. Nevertheless, we would generally agree with the idea that database rights could potentially distort the right to access information and certain issues of abuse of monopoly could emerge, in particular if one look at this problem from a global Cloud computing perspective. We think all these arguments are legitimate and that sui generis rights could eventually lock up data to the detriment of the scientific and academic community as well as other areas of industry. This yields much greater protection to databases, yet with a certain degree of uncertainty that may fall foul of prior intellectual property law principles by placing strong exclusive property rights on investment instead of creativity and innovation. Still, we find it possible to argue for a more balanced approach, which is more flexible and less objectionable than database rights. In order to respond to the critics of sui generis rights, what we propose is a mechanism that follows the core principles and guidelines of best practices through which legal interoperability, and, a right balance between the transferability of conventional databases and the availability of Big Data can be achieved.

5 Conventional Databases vs. Big Data: Striking the Right Balance

As seen above, the sui generis right is a well-established IPR protected under the umbrella of the EU Database Directive. This right stems from the necessity to foster the database industry in the EU in a time where databases needed an extra scope of protection.[76] However, this right caused some concerns and uproar among legal experts, mainly due to its failure to come to terms with new technological advances of the Internet and with the onset of Cloud computing

is that they do not collect data from the outside world. They create it through events organized by them. This sort of data is known as "synthetic data". See Maurer, Hugenholtz and Onsrud (2001), pp. 789-790.

[74] Bently and Sherman (2009), pp. 310-311.

[75] DG Internal Market and Services Working Paper, First Evaluation of Directive 96/9/EC on the Legal Protection of Databases, p. 4.

[76] Note: The concept of protecting databases with only copyright changed radically right after a series of case laws rejecting copyright protection such as the Van Daele v Romme ruling in the Netherlands, where Van Daele could not protect the copying of its dictionary because of lacking the threshold of originality, and; the Feist Publications v Rural Telephone Service Co. [Feist case] judgment in the US, where the courts decided not to grant copyright protection to a phone directory on the same grounds. See Van Dale Lexicografie B.V. v Rudolf Jan Romme, Hoge Raad, Supreme Court of the Netherlands, 4 January 1991, NG 1991, 608, (The Netherlands); Feist Publications v Rural Telephone Service Co. 499 U.S. 340 (1991) (United States).

services along with the Big Data movement, which may undermine and hamper scientific and research activities.

The Database Directive is still clinging to old fashioned ideas of conventional databases that have a fixed structure on which one accumulates and stores data. Another defining factor is the ubiquitous nature of the Cloud that often obscures the physical location of databases. The ability of Cloud providers to transfer databases across multiple countries represents the problem of dealing with different legal jurisdictions. This situation can collide with the legislation of those countries where database rights do not even exist. Therefore, the first problem to be addressed in the contracts is that database rights should only be implemented in jurisdictions where this right exists and limited to a geographic location due to its territorial nature.

We think that this represents a good starting point. However, if we follow this approach only, this debate continues to be stuck in the old paradigm. In view of the immense influence of the Big Data phenomenon, the real issue lies elsewhere. If our aim is the empowerment of end-users so they can take the initiative and make decisions in the face of the Big Data movement, then database rights seem entirely counterproductive. The explosive growth[77] and breadth of reach of Big Data has expanded so much that it has surpassed the traditional logistics of storing, processing, or analyzing data.[78] It touches upon almost every corner of the digitized world and its benefits have enthralled all aspects of human life.[79]

Nevertheless, this great exposure comes along with various risks and opens the door for litigation.[80] Big data in the Cloud refers not only to the storage and accumulation of large amounts of data but also how to organize and label such data in a variety of different and useful ways[81] (structured, unstructured,[82] semi-structured,[83] etc.).[84] Big data generally slices and dices information. This breakdown process implies a systematic reduction of information into smaller pieces that can be arranged in a way that will yield new information. This includes machine-generated data from automated sensors, nuclear plants, X-ray and scanning machines, airplane engines, consumer interaction from businesses,[85] mobiles and social media.[86] If this information is exploited properly it will revolutionize the decision-making

[77] Majkic (2014), Preface.
[78] Dean (2014), p. 10.
[79] Ridley (2015), p. 79.
[80] Ridley (2015), p. 79.
[81] See, e.g. generally, Sakr and Gaber (eds) (2014).
[82] Note: Unstructured data is the subset of information. For example: text mining in the medical field. For details, see e.g., Holzinger et al. (2013), p. 13.
[83] Semi-structured data such as XML. See, e.g. generally, Ishikawa (2015).
[84] See, e.g. generally, Kitchin (2014).
[85] Krishnan (2013), p. 5.
[86] Vashist (2015), p. 1.

process - entrusting more on data analysis instead of intuition and experience. This being said, individuals and institutions need to consider not only the best means to generate and exploit data but also how to protect and manage their data. This raises challenging questions about policies and practices that have direct implications on our lives.[87]

The vexed question is how to strike the right balance between the transferability of conventional databases and the availability of Big Data. This research attempts to answer some of these lingering questions and fill a long held gap in the scientific literature. In line with the principle of free and open access to data,[88] the framework we propose endows end-users and Cloud providers with a flexible mechanism through the Cloud broker to ensure freedom of contract. This interpretation gleaned from the aforementioned principles and ideas can best be treated under three headings: 1) Territorial scope of protection, 2) "Ownership" rights of new data generated by the Big Data movement in the Cloud, and; 3) Lack of international legal and contractual standards, as follows:

5.1 Territorial Scope of Protection

This problem relates to the ubiquitous nature of the Cloud and the territorial scope of protection of database rights that creates legal hurdles. One of the most contentious provisions of the EU Database Directive, which is relevant to our discussion in particular in the context of Cloud computing and Big Data, is Article 11 which establishes territorial constraints with regard to who may be subject to obtain database rights. In principle, the right extends only to makers or rights holders who are nationals or habitual residents of a EU Member State. This is further explained in Article 11 (2) that includes companies or firms, which have their principal place of business or central administration within the EU.[89] This is a controversial and anachronistic provision in the context of Cloud computing and Big Data due to its essentially pervasive nature. In view of the fact that servers can be located in different countries outside of the EU, and that databases can be easily reproduced in virtual machines (VM), there is a risk of potential future controversies between the parties involved in Cloud computing transactions.

If a database qualifies for protection, and it is stored on a server, which is within the jurisdiction of EU/EEA Member States, then there is no doubt that it will be protected. However, the crucial question to determine here is whether the jurisdiction applies to the

[87] Lohr (2015).
[88] See, e.g. generally, OECD Principles and Guidelines for Access to Research Data from Public Funding (2007).
[89] Davison (2003), p. 97.

place where the database has been created or where the database has been recorded. This distinction will fundamentally affect database protection in Cloud transactions, as there are no database rights in other countries outside of the EU.[90]

Currently, there is not such an automated procedure for checking whether database rights are clearly defined and specified so that a broker can "on the fly" confirm the legal compliance. These checks may include the location of the federated infrastructure provider using a location constraint mechanism. If the target infrastructure provider is inside the jurisdiction of the EU/EEA Member States then the outsourcing of data and databases may be fulfilled with minimal intervention taking into account that database rights exist within the jurisdiction of European countries. If the infrastructure provider is located outside the boundaries of any of the EU/EEA Member States, and, therefore, outside of the scope of the Database Directive, then the federation cannot be performed if these checks are not in place in advance.[91]

However, Cloud customers can decide to waive their database rights in order to federate the databases outside the boundaries of the EU/EEA Member States. As seen earlier, databases represent the risk of being potentially "exported" overseas to a jurisdiction without database rights. Therefore, they should only be implemented in jurisdictions where this right exists and limited to a "geographic location" due to its territorial nature. For this reason, we propose a legal "glocalizational"[92] solution that includes an unconditional waiver as an alternative for scientific databases and/or for databases transferred across different jurisdictions outside the EU/EEA countries.

5.2 *"Ownership" Rights of New Data Generated by Big Data*

As hinted above, the exponential growth of data, both structured and unstructured, and the booming of Big Data trends, have the ability to create new information from the data submitted to the Cloud. This newly created data has value for both end-users and Cloud providers. This means that some of the provisions enshrined in the EU Database Directive are becoming obsolete. Furthermore, there seems to be a lack of international legal standard that defines "ownership" rights of data accruing from scientific research and Big Data analyses.

[90] With the exception of Mexico, South Korea and Russia.

[91] See, e.g., Kousiouris, Vafiadis and Corrales (2013), pp. 61-72. In this work the authors refer mainly to data protection issues, however the same principles and ideas underlying the geographic location and data transfers could apply to database rights.

[92] According to Annupan Chander, legal glocalization "would require the creation or distribution of products or services intended for a global market but customized to conform to local laws - within the bounds of international law". See Chander (2013), pp. 11, 16, 137, 143, 144, 145 and 169.

There is some sort of prevailing "global norm", where the person or company who collects the data, "owns" it. This problem seems to bring conflicting arguments between the involved parties. Therefore, there is a need for an efficient and automated procedure during the negotiation of SLAs in Cloud computing transactions, which aims to establish a clear and effective procedure to layout early in the contract who "owns" this data and define the conditions as to whether data will be shared or not among, for example, Cloud providers and end-users, researchers/doctors and patients, etc.

5.3 Lack of International Legal and Contractual Standards

The third problem is the lack of a common international contractual framework to mitigate these legal risks. This leads to a lack of interoperability at the global scale that obstructs the Cloud computing and Big Data markets from thriving. Cloud customers are facing difficulties in choosing the right Cloud provider that best fits their needs. The lack of a structure or frame supporting the clarification of such rights creates tension between the stakeholders involved in Cloud computing transactions. Customers using Cloud computing services are not longer satisfied to deal with these uncertainties post facto. They need clear guidelines at the time they enter into a Cloud computing transaction.

As a corollary, due to the lack of an efficient and automatic procedure for the clarification of database rights and "ownership" rights of data in the Cloud, end-users have to cope with the uncertainties and intricacies of the decision-making. The current state of the art in the Cloud market allows only for a limited category of static and non-negotiable click-through SLA (usually ranked as gold, silver, or bronze). The manual selection of Cloud providers in order to meet their functional requirements (e.g. storage capabilities, number and size of servers, etc.) and non-functional capabilities (e.g. legal) has been perceived as imposing transaction costs. End-users must go through the cumbersome procedure of visiting manually the websites of Cloud providers to compare their quality of services and legal policies.[93]

In short, what we want to achieve is a flexible and automated SLA that includes: a) the possibility to keep databases (and as a consequence database rights) within the EU jurisdiction.[94] This would be the case an end-user does not want to share data and still keeps database rights and enjoy the benefits of the EU Directive. If so, databases should stay within the EU jurisdiction, b) the possibility to clarify who "owns" the processed and derivate data.

[93] See Wu et al. (2013), pp. 235-244.
[94] Or, for example, in Mexico, South Korea and Russia as these countries have also database rights similar to the EU Database Directive.

This would be the case of Big Data projects/applications, e.g. using data mining tool techniques, statistics, analytics, etc., where there is potentially valuable information for both the end-users and Cloud providers. The contract should be able to clarify who "owns" this new data. This situation is between end-users and providers, or potentially among end-users working in the same project e.g. a research project using genetic, geo-data, spatial data, etc. It goes without saying that all these legal issues could be clarified via a consortium agreement (CA). In a realistic Cloud computing scenario, however, what we need to avoid are manual negotiations. Therefore, this capability should be carried out automatically, and c) a waiving mechanism, by which end-users may relinquish their database rights and "ownership" rights of data. This would be the case of a Big Data collaborative project where many countries are involved.[95] This way databases would remain open and everyone could get access and tap into it. On the one hand, most research is conducted by joint efforts of public as well as private institutions in interdisciplinary and international contexts. On the other, competition in a behaviorally imperfect market is inevitable, and the possibility of waiving database rights does not mean that competition has to be curtailed. Providing more information and warning signals can offer end-users more choices and grant them more control over their data.

6 Risk Assessment Techniques and Typical Actors Involved in Brokering WS-Agreements

This section focuses on explaining in more detail the brokering mechanism, which facilitates the creation of risk-aware SLAs between the typical actors involved in Cloud computing transactions. Three actors exist in the architecture of a typical Cloud brokerage scenario: end-user, broker and provider. An end-user is an individual or a company who wants to use the Cloud in order to perform certain task consisting of one or more services. The user must explicitly specify the tasks and associated requirements within an SLA template. In the preamble of this process, the end-user needs to make informed and risk-aware decisions on the SLA quotes. In order to make this risk assessment more practical, we consider two broad typical brokerage scenarios that provide ideal use cases. In both situations resources are dynamically allocated and redistributed. These scenarios are the following:

a) Broker as Mediator: In this case the broker performs a risk assessment on behalf of the end-user in order to find the most suitable Cloud provider and bring the parties

[95] See, e.g., GEOSS-data Core project, p. 11.

together. It follows a four-step process: First, the end-user sends an SLA request to the broker. Then, the broker forwards the SLA quotes to a pool of suitable Cloud providers. Once all the SLA quotes are received from the providers, the broker performs an independent risk assessment of each provider. Then, the broker creates a ranked list according to their PoF. Finally, the end-user is then free to choose and commit to an SLA quote by engaging directly with the selected provider.[96]

b) Broker as Contractor: In this case the broker takes a more active role and offers its own SLA to end-users. The risk assessment works in the same way of the previous scenario. However, the main difference here is that the broker takes full responsibility of the SLA and performs the role of a "virtual" provider. Therefore, an end-user contracts directly with a broker instead of with the Cloud provider. The broker agrees to the terms and conditions of the SLA between itself and each Cloud provider.[97]

This brokerage mechanism will be used as a technical framework to include database and "ownership" rights of data risk assessment techniques. It is in the best interest of both sides: a) end-users: as it increases the selection of Cloud providers by comparing SLA quotes that match their expectations, and; b) Cloud providers: as it generates a larger user pool base and attempts to reduce deliberation costs in deciding upon which SLA requests to accept. From a provider's perspective, accepting an SLA implies the potential risk of paying a penalty if such commitment cannot be met.[98]

It is important to bear in mind the limitations of this framework. The introduction of a broker alone will not dissipate all the uncertainties before signing the SLA. Nonetheless, the implementation of a risk-aware brokering mechanism provides the means to formally evaluate the probability and expected impact of potential adverse events. Without such knowledge end-users and Cloud providers cannot take the right decisions with regard to costs and benefits. In a nutshell: this is a win-win situation that will reduce transaction costs.[99]

Nevertheless, the crucial question that remains still is whether the Cloud brokers are poised to offer a viable and transparent alternative route for end-users and Cloud providers.[100] To some extent the Cloud broker-enabling technology should improve the available choices by providing the means for control and transparency to make effective and proactive data-

[96] Djemame et al. (2011b), p. 1561.
[97] Djemame et al. (2011b), p. 1561.
[98] Djemame et al. (2011b), p. 1561.
[99] Djemame et al. (2011b), pp. 1559-1560.
[100] Fellows (2013); See also, Gourlay, Djemame and Padgett (2008), p. 438.

driven decision-making.[101] From the perspective of end-users, the broker should be seen as a trusted advisor that aids them to make better decisions.[102]

For this reason, a relevant aspect of this framework is the implementation of a software component - a confidence service; designed to perform an independent and objective assessment of the reliability of Cloud providers in relation to the SLA PoF. Cloud providers usually run their own risk assessment, however this can be too optimistic and overlook some of the important facts that are relevant for end-users. Therefore, the confidence service component provides more transparency and additional risk information to enhance the SLA decision-making process of end-users.[103]

7 Risk Inventory Design

Designing a risk inventory depends on the purpose and area in which they are applied. It has to be contextualized taking into account all the parties involved. As explained above, in our use case scenarios, these actors are end-users, Cloud providers and the broker who can acquire different roles (mediator or contractor).[104] The risk inventory may also have different categories. In the case of the OPTIMIS risk assessor component, there are four broad categories i.e. general, technical, policy and legal.[105] A risk inventory must be tailored and refined to fit a specific purpose. For the implementation of this framework, a set of processes has been identified as follows:[106]

1. **Use cases:** determine precisely which use case scenario to focus on: in this case, a Cloud brokerage scenario.[107]
2. **Levels of interaction:** establish the areas of interaction in the Cloud. Interactions may involve various levels in the Cloud. In this case we consider two levels: a) end-user to service provider, and b) service provider to infrastructure provider. Insomuch as during each of these levels particular aspects of the SLA needs to be agreed upon and its fulfillment monitored.[108]

[101] Fellows (2013).
[102] Fellows, Ring and Rogers (2014), p. 2.
[103] Djemame et al. (2011b), pp. 1559-1560.
[104] Djemame et al. (2011b), p. 1561.
[105] Djemame et al. (2011a), p. 122.
[106] Djemame et al. (2012), pp. 9-10.
[107] Djemame et al. (2012), pp. 9-10.
[108] Djemame et al. (2012), pp. 9-10.

3. **Assets:** it is necessary to identify what is the asset being protected. In this case, database and "ownership" rights (and their characteristics) and SLAs. Risks events will be assessed and protected taking into account external or internal dangers (risks).[109]
4. **Incidents/Risk Scenarios:** it is necessary to describe any event, condition or a blend of both that has the potential to diminish the capacity or availability of an asset. These consist of the vulnerabilities and threats these assets may have during service operation. This includes the "adaptive capacity", which is the specific description of the mitigation strategy to be carried out for each risk scenario and its asset.[110]
5. **Triggering Factor:** it is necessary to identify the factors that lead to activate risk. Risks may also be dynamic. This means they can change and continually fluctuate over time as they are directly exposed to changes in the Cloud ecosystem such as regulatory requirements, changes in policies and contractual clauses, transactions, etc. The implementation of monitoring strategies may help to mitigate them during Cloud service deployment and operation phases.[111]

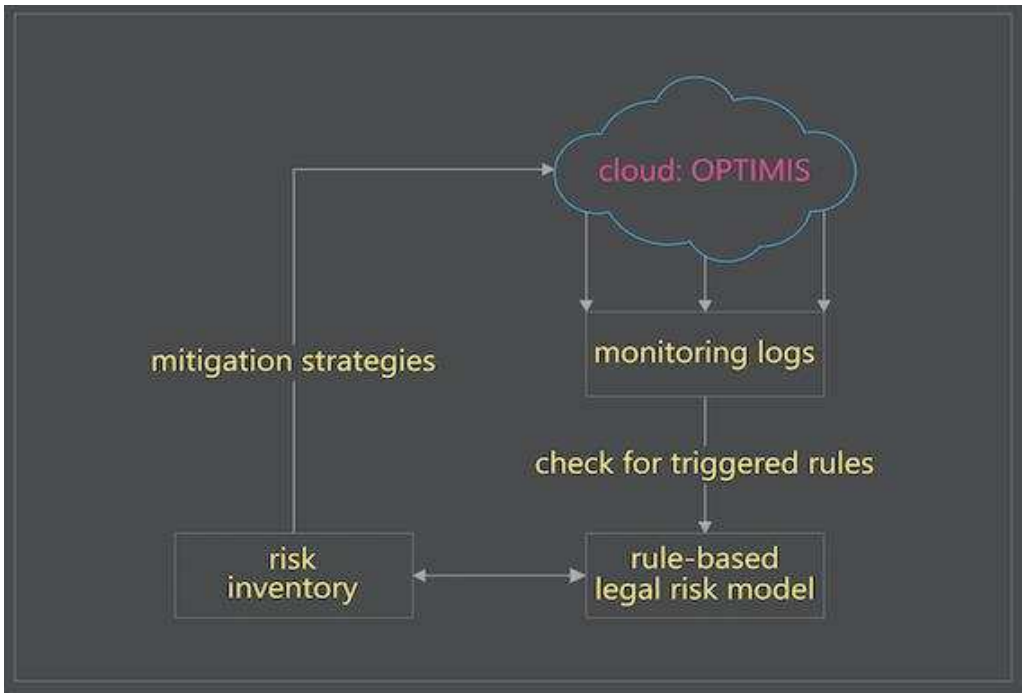

Figure 3: Risk Inventory for the Identification of Legal Risks in the Cloud Architecture

[109] Djemame et al. (2012), pp. 9-10.
[110] Djemame et al. (2012), pp. 9-10.
[111] Djemame et al. (2012), pp. 9-10.

The risk inventory designed within the scope of the OPTIMIS project has been integrated as a rule-based legal risk[112] modeling component and an integral part of the risk assessment software tool (see Figure 3 above). The risk assessment tool is a "self-contained independent functional model", which means that it is a completely independent component that enables customization and is able to work as a "plug-in".[113] This allows the addition of specific features to the existing software application. In the context of the OPTIMIS toolkit, the risk assessment tool has been implemented as two coexisting but independent components as follows: a) the service provider risk assessment tool (SPRAT), and; b) the infrastructure provider risk assessment tool (IPRAT).[114]

8 Different Stages of Risk Assessment in Cloud Brokerage Scenarios (CBS)

As explained earlier, in a typical CBS there are three main parties involved. These are, the end-users, the broker and the Cloud provider. The Cloud provider could be a service provider or an infrastructure provider (i.e. virtual machine (VM) provider). From a service and infrastructure provider perspective, data management services are supplied by the broker to co-ordinate and provide services or infrastructure in terms of data processing and quality of service. Figure 4 below shows the document flow for creating an SLA and the different stages where the risk assessment can take place. This procedure takes part during the whole service life-span (establishment, deployment and execution phase).[115] With a view to making it easier for the lay person, this process can be split into five consecutive steps as follows:

1. At stage number 1, the SLA request is sent to various infrastructure providers (e.g. IP A, IP B, and IP C). At this stage the broker wants to know which provider can run a service upon end-user's request. Prior to making this contact the broker should be able to assess the end-user's requirements and "filter" from its list of infrastructure providers those that may be able to make an SLA offer. Note that upon receiving an SLA request the infrastructure provider can selectively choose to accept it (and consequently the SLA needs to be fulfilled at service operation) or reject it.

[112] In computer science and software development, rule-based systems (also known as "expert-systems") are used to store and analyze information in useful ways that tell you what to do in different situations. They are often used as the basis for AI programing and systems to find answers to various problems. See, e.g. generally, Grosan and Abraham (2011), pp. 149-185; Toosizadeh and Reza Farshchi (2011). Rule-base systems work as a set of "If-then" rules and facts to represent different actions to take. For details, see Cawsey. Rule-Based Systems http://www.zemris.fer.hr/predmeti/krep/Rules.pdf Accessed 10 October 2016.
[113] Plug-in, add-in or add-on extensions are all synonyms for software components.
[114] Djemame et al. (2011a), pp. 121-122.
[115] Kirkham et al. (2012), p. 1067.

2. At stage number 2, the broker receives a reply from the infrastructure provider in the form of an SLA offer. It may happen that the broker will receive several replies from different infrastructure providers. In the figure below, the broker receives an SLA offer from IP A and IP C.
3. At stage number 3, the broker filters all the offers received from the infrastructure providers who can run the service. At this stage the broker can see which offer is more favorable to the end-user, i.e. proceeds with a ranking.
4. At stage number 4, the broker selects the most suitable infrastructure provider among all the SLA offers and contracts with one of them. At this stage the SLA is bound between the infrastructure provider and the broker.
5. At stage number 5, the service is in operation. At this stage, the broker has chosen and told the infrastructure provider to run the service.

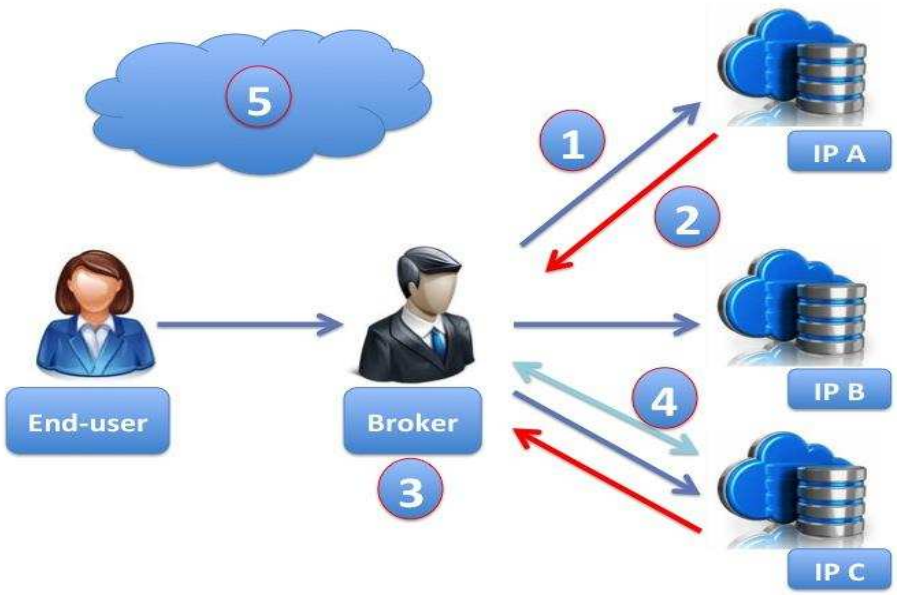

Figure 4: Different Stages of Risk Assessment in CBS

Risk can occur at any time. That is, at stage 1, risk can take place before sending an SLA request to the infrastructure provider. In this case, the risk assessment is going to assess the risk of dealing with various infrastructure providers. This will work as a kind of "pre-assessment" when the broker is about to choose the provider. After this first screening procedure, the broker can then discard the providers that do not comply with the end-user's requirements. At stage 3, the broker filters the provider's offer. In this case, the risk assessor component can "look" inside the shortlisted SLA offers and can assess the risk of accepting the SLA. At stage 5, the infrastructure provider is running the service. Therefore, the risk

assessor component assesses the risk of the SLA failing during service operation. These are all different kinds of risk assessments. In addition, the risk assessment is from both sides as it can be run by the broker on behalf of the end-user and by the infrastructure provider. In the latter case, the infrastructure provider might have the same questions i.e. what is the risk of dealing with this broker? What is the risk of accepting this SLA request? And, finally, what is the risk of the SLA failing during service operation?[116]

The question arises, what does this all have to do with databases and the "ownership" rights of data? The reason is that all of the above could be tailored to database rights and "ownership" rights of data. It could be an integral part of the equation, i.e., part of the SLA negotiations. A key point of this research is to extend the scope of parameters and the range of conditions that can be understood, measured and evaluated. This needs to be included in the risk assessor model as an extension to the legal category. Database rights and "ownership" rights of data can be part of the "policy", "legal", "technical" and "general" criteria to be considered and evaluated. For instance, what is the risk of dealing with an infrastructure provider considering database rights? To answer this question, one may look at different criteria that can be assessed quantitatively or qualitatively. These criteria can refer to different areas that have been filtered from the ISO standards[117] and ENISA guidelines such as: back SLA performance, business stability, general security practices, privacy practices, certification standards, geographic location of the infrastructure providers, general infrastructure practices (e.g. information about back-up, history, machine), etc.[118]

A quantitative risk assessment provides a numerical expression of probabilities.[119] It is based on track records of the broker dealing with the infrastructure provider. It is a reputation-based mechanism that classifies information based on past SLA performance. A risk level numerical estimation can be used to represent the probability of a risk that a specific harm will result from the occurrence of a particular event. For example, a 10-point rating scale: from 10 times, the infrastructure provider fails 1 time. The score is 9 out of 10.[120] Travel websites such as Trip Advisor are clear examples of this kind of ranking system. They often provide a forum where previous travellers can share their opinions and experiences.[121]

The data is analyzed within the inherent reputation engine of the risk assessor model using algorithms and statistical analysis. This score is then translated into the risk. The highest score represents a high risk and lowest score a very low risk. This forms part of the "confidence

[116] Djemame et al. (2011a), p. 125.
[117] See, e.g., ISO 31000:2009; ISO 27000 standards; ISO Guide 73:2009.
[118] For details of the ENISA Guidelines see Cattedu and Hogben (2009).
[119] Summer, Ross and Ababouch (2004), p. 6.
[120] Djemame et al. (2011b), p. 1570.
[121] Lebber and Hermann (2013), p. 406.

service" that has been developed as part of the risk assessment model.[122] The only downside to a quantitative reputation-based risk assessment is when there are no track records, i.e., when there is no past-SLA information. In this case, the information has to be garnered from scratch. Stages number 1 and 3 in the figure above are relatively easy as they refer to existing data, i.e., data that has already been collected.

Stage number 5 is, however, more difficult to calculate, as this data has to be interpreted semantically and needs to be collected when the service is running during service operation. At this stage, the approach of any risk assessment must be qualitative. This method is conditioned to prior expert knowledge based on non-numeric values.[123] This means that the information or data that needs to be collected are expressed in verbal form instead of numbers or quantities as in the case of the quantitative method.[124] Therefore, the risk inventory must be extended to support database rights and "ownership" rights of data either as a new category or as part of the legal risk criteria. The qualitative risk assessment model needs data to be monitored based on the vulnerabilities and threats attached to it. This becomes one more component at the moment of assessing the overall risk of the SLA failing at the service operation phase (e.g. the risk of a computer system or VM failing in cases of natural disasters such as earthquakes, floods, etc.).[125]

9 Use Case Scenario: Examples

In this section a hypothetical scenario is considered to showcase how the risk assessment can be effectively applied in real cases with an emphasis on the different threats and vulnerabilities identified as in the risk assessment process.

To address these legal issues, we need to envisage a hypothetical scenario where database rights and "ownership" rights of data are breached or likely to be breached. For example, if the right to access a database has been granted, what are the inherent risks of that happening? Or, if database rights have not been granted, what are the results of this happening? In other words, we need to identify the specific threats and vulnerabilities related to database rights and "ownership" rights of data. Note that a threat is "a potential cause of an unwanted incident",[126] which may cause harm to a system or organization,[127] whereas a vulnerability is

[122] Djemame (2013), p. 3.
[123] Taubenberger et al. (2011), p. 260.
[124] Sharif and Basri (2011), p. 222.
[125] See, e.g., Cayirci (2015), p. 163.
[126] Lund, Solhaug and Stolen (2011), p. 131.

"a weakness, flaw or deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset"[128], e.g. the database and the right to access it. It is only then when the obvious gaps are realized and the risk assessment model acquires its full value, as we will have a better understanding of the concrete data that we need to assess, measure and monitor in those situations and convert it into a specific risk analysis, risk being "the likelihood of an unwanted incident (an event) and its consequence (impact) for a specific asset". [129] Several consequence descriptors may apply to a single risk. The most serious/significant of these should be used to determine the risk exposure rating. The likelihood and impact levels are then cross tabulated to give a risk exposure rating. This determines whether a risk is categorised as low, medium, high or very high (Table 1).[130] Prioritising of risks that are assigned the same risk exposure rating is achieved by examining the strength of the control measures in place for these risks. For example, a "high" rated risk could have effective control measures in place that cannot be improved upon, whereas a "medium" rated risk may not have any control measures in place, and this is the risk that should be prioritised for action.

Likelihood	**Impact**				
	Negligible	**Minor**	**Moderate**	**Major**	**Extreme**
Rare	Low	Low	Low	Medium	Medium
Unlikely	Low	Medium	Medium	Medium	High
Possible	Low	Medium	Medium	High	High
Likely	Medium	Medium	High	High	Very high
Almost certain	Medium	High	High	Very high	Very high

Table 1: Risk Exposure Rating

We focused on a hypothetical scenario targeting a broad sector within the scope of a globalized world. This use case scenario refers to a research form that is typically found in transnational research such as genetic research projects within clinical trials. In this context, the risk assessment model is combined with an adaptive and flexible SLA with a data centric

[127] Luiijf (2016), p. 69.
[128] Großmann and Seehusen (2016), p. 23; Lund, Solhaug and Stolen (2011), p. 137.
[129] Beckers (2015), p. 457.
[130] Use of colour coding could also facilitate the rapid communication and understanding of risks such as: red, amber, yellow or green.

monitoring infrastructure. The main focus is to expand the range of SLAs to cover cross-border activities similar to the use case depicted below. The outcome is a contribution to equip the involved parties with a tool that can offer more choices to satisfy the legal requirements in Cloud computing transformations.

9.1 Use Case Scenario: Genetic Research Projects within Clinical Trials

Genetic research projects within clinical trial scenarios frequently collect biological and genetic data from patients/participants. This data is then stored in a hospital's databases for future research purposes. Genetic data is regarded to be unique and very sensitive as it has the potential of revealing in the future personal, scientific and medical information of each patient including the family members of the data subject.[131] For this reason, genetic research projects typically handle anonymized data using advanced encryption tools in order to safeguard patients' privacy rights and be in compliance with data protection laws. Once the data has become entirely anonymous, it is ready to be used by the research community. It is not the purpose of this chapter to discuss data protection matters; rather this section focuses on answering the question: who has the "ownership" rights of such data and databases? Or, who is allowed to use and get access to such data for scientific research purposes? In other words, it is more about the controllability of data and databases. And, to point to some general features of the SLA that, in tandem with the risk assessment tool, may help to clarify and mitigate some of the uncertainties around these questions.

For this reason, the role of the broker in this type of use case scenario is very important as it can take a fiduciary nature as a trusted third party and audit such compliance. The broker can intervene and be in charge of engaging with end-users (in this case the hospitals or research institutions) and the Cloud providers. At the same time, some of the brokers may correct the complaints or requests of the end-users and serve as a gate away to information necessary to clarify and rectify the contractual terms of the SLA. This provides the opportunity to expand its assistance as a mere agent considerably beyond the model for what has already been established and cover various use case scenarios within an international framework. Figures 5 and 6 below illustrate some of the risk assessment features that fall within the "policy" and "legal" categories as follows:

[131] Art. 29 Data Protection Working Party (2004), pp. 1-14.

- Risk Category: **Policy/Legal**
- Asset Identified: Data ("ownership" rights of new data generated by Big Data applications)
- Vulnerability of Asset: Lack of clarification within the SLA of who is allowed to use and access the new data generated in the Cloud
- Threat to Asset: SLA
- Risk Likelihood: Possible
- Risk Impact: Extreme
- Resulting Risk Level: Product of risk likelihood and risk impact = High
- Risk Event: Negligence: This risk takes place at steps number 1 and 3 (see Figure 4 above). That is, when the broker sends the SLA request to various Cloud providers and then filters the offers received. In this case the broker must choose the provider according to end-user's criteria.
- Resulting Risk Mitigation: Include a string field capability within the SLA, which allows the inclusion of contractual clauses that can clarify who is allowed to use and access this data e.g. for scientific research.

Figure 5: Example of Policy/Legal Category

- Risk Category: **Legal**
- Asset Identified: Databases
- Vulnerability of Asset: Database rights may create some constraints for scientific research
- Threat to Asset: Database rights
- Risk Likelihood: Possible
- Risk Impact: Major
- Resulting Risk Level: High
- Risk Event: Negligence: This risk takes place at steps number 1 and 3 (see Figure 4 above). That is, when the broker sends the SLA request to various Cloud providers and then filters the offers received. In this case the broker must choose the provider according to end-user's criteria.
- Resulting Risk Mitigation: Clearly define database rights within the SLA through the XML Description Schema and add a Boolean "waiving" system whereby the Cloud provider can choose to keep or waive database rights based on end-users input.

Figure 6: Example of Legal Category

Finally, when the researchers and doctors use a Cloud computing service to store and process the data of patients, they are particularly concerned about the confidentiality and integrity of such data. These two aspects are integral parts of the security infrastructure, but also, in particular, the availability of such data during a time of crisis. While confidentiality

refers to the property of data or information not being made available or disclosed to unauthorized persons,[132] integrity means that the information must be accurate, not allowing data to be modified.[133] Availability, on the other hand, is concerned with ensuring that data and services are accessible where and when it is needed with the proviso that is consistent with the SLA legal framework.[134]

In the event of any disaster (e.g. earthquake, floods, etc.), the risk assessment framework through the CBS may help to fix the situation immediately and fill the gap in emergency situations. According to the ISO 27001, availability is: "a characteristic that applies to assets. An asset is available if it is accessible and usable when needed by an authorized entity. In the context of this standard, assets include things like information, systems, facilities, networks, and computers."[135] From a legal perspective, "availability" is strongly related to "ownership" rights of data as this also refers to the legal wherewithal to control and make good use of data.

The threat analysis suggests that the risk ratings belonging to availability are classified as medium in comparison to confidentiality (high) and integrity (low). This is because the end-users (or patients in this case) are more concerned with their privacy. Therefore, confidentiality has a stronger effect on trust and the provider's reputation. Integrity can be caused by accidental software and user errors, equipment failure and deliberate alteration of data by third parties. It is relatively low because the impact is much lower in comparison to the availability of data. Loss of availability is classified as medium since end-users and enterprises are better off using Cloud computing provider resources rather than deploying their own infrastructure taking into account the cost benefits.[136]

- Risk Category: **Technical/General**
- Asset Identified: Availability of Data and Databases
- Vulnerability of Asset: Lack of maintenance
- Threat to Asset: Database server failure
- Risk Likelihood: Rare
- Risk Impact: Moderate
- Resulting Risk Level: Product of risk likelihood and risk impact = Low
- Risk Event: Unavailability of data due to server failure: This risk takes place at step number 5 (see Figure 4 above) during service operation. That is, when the Cloud provider

[132] Gough and Nettleton (2010), p. 149.
[133] Kattan, Nunu and Saleh (2011), p. 199.
[134] Williams (2013), p. 187; Bonewell (2006), p. 1178.
[135] For this term see, e.g., http://www.praxiom.com/iso-27001-definitions.htm Accessed 10 October 2016.
[136] Kahn et al. (2012), p. 124.

is running the service and unexpectedly there is a server failure e.g. one or more VMs stop running.
- Resulting Risk Mitigation: Fault-tolerance solutions provision

Figure 7: Example of Technical/General Category

- Risk Category: **Technical/General**
- Asset Identified: Availability of data and databases
- Vulnerability of Asset: Data center infrastructure (servers)
- Threat to Asset: Force majeure (such as floods, earthquakes, etc.)
- Risk Likelihood: Rare
- Risk Impact: Major
- Resulting Risk Level: Product of risk likelihood and risk impact = Medium
- Risk Event: Unavailability of data due to server failure: This risk takes place at step number 5 (see Figure 4 above) during service operation. That is, when the Cloud provider is running the service and unexpectedly there is an event of force majeure.
- Resulting Risk Mitigation: Redundancy and use of back-up servers located in different places (cities): Data should be constantly replicated with databases and back-up solutions during the whole Cloud computing service life cycle.

Figure 8: Example of Technical/General Category

.

10 Conclusion

As with any intellectual property matter, the European Database Directive was designed to counterbalance two opposite forces. Along the same lines, it is true that database protection is an instrument that may foster innovation and investment within the database industry. On the opposing end, stringent laws such as database rights may also create potential conflicts with regulations that are not compatible,[137] specially if we consider the global and ubiquitous nature of the Cloud. In addition, the Big Data movement raises the question of "ownership" rights in the new data generated. This issue is far from being clear as this concept glosses over many aspects that ought to be clearly specified during SLA negotiation.

Increasing interest in the use of SLAs to govern interactions in Cloud computing transactions has gained momentum. While such agreements are a vital component to ensure a successful relationship between end-users and Cloud providers, they are limited in scope and

[137] Maurer, Hugenholtz and Onsrud (2001), p. 789; Maurer (2008), pp. 13-4 – 13-80.

coverage. Such limitations may give rise to considerable exposure of risks not only for end-users, but also for service providers. Therefore, a risk assessment component has been fully implemented in the OPTIMIS software toolkit, which aligns with the SLA framework in the context of grid and Cloud resource brokers. This model provides a solution as to how to express these requirements on a technical level in the SLAs and the data management system. It has also been equipped with a monitoring tool as well as the requirements of an inherent legal risk inventory, which provides an additional layer of legal protection. This enables very fine-grained and continuous control over the data and databases thus allowing the identification of the sort of actions that are needed to reduce and mitigate such risks. Crucially, this new framework attempts, not only to raise collective awareness of the risks entailed in a neglected area of research, but also at increasing confidence levels, prompting the involved parties to trust each other to a greater extent than is currently the case.

Acknowledgement: This work has been partially supported by the EU within the 7th Framework Program under contract ICT-257115 - Optimized Infrastructure Services (OPTIMIS), and, by the Japanese Ministry of Eduction, Culture, Sports, Science, and Technology (MEXT) through a research scholarship (Mombukagakusho) conducted at Kyushu University in Japan. The authors would like to thanks Prof. Toshiyuki Kono and Prof. Shinto Teramoto for their valuable guidance.

References

Advanced Risk Assessment and Management for Trustable Grids (AssessGrid). EU funded project within the FP6 IST Framework Program under contract no. 031772 http://cordis.europa.eu/project/rcn/79340_en.html

Andrieux A et al. (2007) Web Services Agreement Specification (WS-Agreement). Global Forum

American Heritage Dictionary. https://www.ahdictionary.com/word/search.html?q=risk&submit.x=-872&submit.y=-210 Accessed 15 April 2016.

Art. 29 Data Protection Working Party (2004) Working Document on Genetic Data adopted on 17 March 2004 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf Accessed 10 October 2016.

Barnatt C (2010), A Brief Guide to Cloud Computing: An Essential Guide to the Next Computing Revolution. [Kindle DX version] Retrieved from Amazon.com

Batré et al. (2007) Gaining Users' Trust by Publishing Failure Probabilities. Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Proceedings of the Third International Conference on Security and Privacy in Communication Networks. Nice, France

Beckers K (2015) Pattern and Security Requirements: Engineering-Based Establishment of Security Standards. Springer, Cham
Bently L, Sherman B (2009) Intellectual Property Law, 3rd edn. Oxford University Press, Oxford
Bonewell D (2006) Security and Privacy for Data Warehouses: Opportunity or Threat? In: Tipton H, Krause M (eds) Information Security Management Handbook, 5th edn. Auerbach Publications, Boca Ratón
Bradshaw S, Millard C, Walden I (2010) Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. Queen Mary School of Law Legal Studies Research Paper No. 63/2010 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374 Accessed 10 October 2016.
Burnett R (2005) Legal Risk Management for the IT Industry. Computer Law & Security Report 21(1):61-67
Cawsey A, Rule-Based Systems http://www.zemris.fer.hr/predmeti/krep/Rules.pdf Accessed 10 October 2016.
Cattedu D, Hogben G (2009), Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA (European Network and Information Security Agency) http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport Accessed 10 October 2016.
Cayirci E (2015) Models for Cloud Risk Assessment: A Tutorial. In: Felici M, Fernández-Gago C (eds) Accountability and Security in the Cloud: First Summer School, Cloud Accountability Project, A4Cloud Malaga, Spain, June 2-6 2014, Revised Selected Papers and Lectures. Springer, Cham
Chander A (2013) The Electronic Silk Road: How the Web Binds the World Together in Commerce, New Haven: Yale University Press
Chung L et al. (2000) Non-functional Requirements in Software Engineering. Springer, New York
Chung L, Sampaio Do Prado Leite J (2009) On Non-functional Requirements in Software Engineering. In: Borgida A et al. (eds.) Conceptual Modeling: Foundations and Applications, Essays in Honor of John Mylopoulos, Lecture Notes in Computer Science / Information Systems and Applications, incl. Internet/Web, and HCI (Book 5600). Springer, Berlin
Ciborra C (2005) Digital Technologies and the Duality of Risk. Centre for Analysis of Risk and Regulation. London School of Economics and Political Science, London.
Ciborra C (2007) Digital Technologies and Risk: A Critical Review. In: Hanseth O, Ciborra C (eds) Risk, Complexity and ICT. Edgar Elgar Publishing, Cheltenham
Ciborra C (2009) Imbrication of Representations: Risks and Digital Technologies. In: Avgerou C, Lanzara F, Willcocks L (eds) Bricolage, Care and Information Systems: Claudio Ciborra's Legacy in Information Systems Research. Palgrave MacMillan, New York
Corrales M (2012) Privacy Risk Impact Assessment: A New Requirement for Safer Clouds. Beck-Online, ZD-Aktuell, 03036
Davison M (2003) The Legal Protection of Databases. Cambridge University Press, Cambridge
Disselkamp L (2013) Workforce Asset Management Book of Knowledge: Official Guide for Workforce Asset Management Certification. John Wiley & Sons, Inc., Hoboken
Dean J (2014) Big Data, Data Mining and Machine Learning: Value creation for business leaders and practitioners. John Wiley & Sons, Inc., Hoboken
DG Internal Market and Services Working Paper, First Evaluation of Directive 96/9/EC on the Legal Protection of Databases http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf Accessed 10 October 2016.

Djemame K et al. (2011a) A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems, The Second International Conference on Cloud Computing, GRIDs, and Virtualization http://www.optimis-project.eu/content/risk-assessment-framework-and-software-toolkit-cloud-service-ecosystems Accessed 10 October 2016.

Djemame K et al. (2011b) Brokering of Risk-Aware Service Level Agreements in Grids. Concurrency Computat.: Pract. Exper. 23:1558–1582.

Djemame K et al. (2012) Legal Issues in the Cloud: Towards a Risk Inventory. Phil. Trans. R. Soc. A, Vol. 371 no. 1983 20120075.

Djemame K et al. (2016) A Risk Assessment Framework for Cloud Computing. IEEE Transactions on Cloud Computing 4(3):265-278

Draft White Paper on Legal Options for the Exchange of Data through the GEOSS Data-CORE. Group on Earth Observations https://www.earthobservations.org/documents/dsp/draft_white_paper_geoss_legal_interoperability_30_october_2011.pdf Accessed 10 October 2016.

Drissi S, Houmani H, Medromi H, (2013) Survey: risk Assessment for Cloud Computing. International Journal of Advanced Computer Science and Applications (IJACSA) 4(12):143-148.

Dupré L, Haeberlen T (eds) (2012) Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA European Network and Information Security Agency https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security Accessed 10 October 2016.

Fellows W (2013) Cloud Brokers: Now Seeking Ready-to-Pay Customers, 451 Research https://451research.com/report-long?icid=2666 Accessed 10 October 2016.

Ferrer et al. (2011) OPTIMIS: A Holistic Approach to Cloud Service Provisioning. Future Generation Computer Systems 28:66-77.

GEOSS-data Core project https://www.earthobservations.org/documents/dswg/Annex%20VI%20-%20%20Mechanisms%20to%20share%20data%20as%20part%20of%20GEOSS%20Data_CORE.pdf Accessed 10 October 2016.

Garner B (ed) (2014) Black's Law Dictionary, 10th edn. Thomson Reuters. St. Paul MN

Gough J, Nettleton D (2010) Managing the Documentation Maze: Answers to Questions You Didn't Even Know. John Wiley & Sons Inc., Hoboken

Gourlay I, Djemame K, Padgett J (2008) Reliability and Risk in Grid Resource Brokering. 2008 Second IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2008)

Gourlay I, Djemame K, Padgett J (2009) Evaluating Provider Reliability in Grid Resource Brokering. 11th IEEE International Conference on High Performance Computing and Communications.

Griffith R (2012) A Short Introduction to Cloud Computing: Everything You Need to Know in Around 1000 Words, [Kindle DX version] Retrieved from Amazon.com

Grosan C, Abraham A (2011) Ruled-Based Expert Systems. In: Grosan C, Abraham A (eds) Intelligent Systems: A Modern Approach, Intelligent Systems Reference Library, Vol. 17. Springer, Berlin

Großmann J, Seehusen F (2016) Combining Security Risk Assessment and Security Testing Based on Standards. In: Seehusen et al. (eds) Risk Assessment and Risk-Driven Testing: Third International Workshop, RISK 2015, Berlin Germany. Springer, Cham

Gutwirth S, Hildebrandt M (2010) Some Caveats on Profiling. In: Gutwirth S, Poullet Y, de Hert P (eds) Data Protection in a Profiled World. Springer, Dordrecht

Holzinger A et al. (2013) Combining HCI, Natural Language Processing, and Knowledge Discovery - Potential of IBM Content Analytics as an Assistive Technology in the Biomedical Field. In: Holzinger A, Pasi G (eds) Human Computer Interaction and

Knowledge Discovery in Complex, Unstructured, Big Data, Third International Workshop, HCI-KDD 2013, Maribor, Slovenia, July 2013, Proceedings. Springer, Heidelberg
Ishikawa H (2015) Social Big Data Mining. CRC Press, Boca Raton
ISO/IEC 29101:2013 Information Technology - Security Techniques - Privacy Architecture Framework http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45124&commid=45306 Accessed 10 October 2016.
ISO/IEC NP 19086-4 Information Technology - Cloud Computing - Service Level Agreement (SLA) framework and technology - Part 4: Security and Privacy http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=68242 Accessed 10 October 2016
ISO 22307:2008 Financial Services - Privacy Impact Assessment http://www.iso.org/iso/catalogue_detail.htm?csnumber=40897 Accessed 10 October 2016.
ISO 31000:2009 Risk Management https://www.iso.org/obp/ui/#iso:std:43170:en Accessed 10 October 2016
ISO/IEC DIS 29134 Information Technology - Security Techniques – Privacy Impact Assessment – Guidelines http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62289 Accessed 10 October 2016.
Jackson P (1998) Introduction to Expert Systems, 3rd edn. Addison-Wesley, Harlow
Jrad F (2014) A Service Broker for Intercloud Computing, Doctoral Thesis, Karlsruhe Institute of Technology, KIT http://d-nb.info/1054989486/34 Accessed 1 October 2014.
Jones B, Bird I (2013) Data-Intensive Production Grids. In: Critchlow T, Kleese van Dam K (eds) Data-Intensive Science. Chapman & Hall (CRC Press), Boca Raton
Kasemsap, K, Sunandha S (2015) The Role of Cloud Computing Adoption in Global Business. In: Chang V, Walter R, Wills G (eds) Delivery and Adoption of Cloud Computing Services in Contemporary Organizations. Information Science Reference (IGI Global), Hershey PA
Kattan I, Nunu A, Saleh K (2011) A Stochastic Model for Improving Information Security in Supply Chain Systems. In: Wang J (ed) Supply Chain Optimization, Management and Integration: Emerging Applications. Business Science Reference, Hershey PA
Khan A et al. (2012) Security Risks and their Management in Cloud Computing, IEEE Computer Society, 2012 IEEE 4th International Conference on Cloud Computing Technology and Science.
Kingston W (2010) Beyond Intellectual Property: Matching Information Protection to Innovation. Edward Elgar Publishing, Cheltenham
Kirkham T et al. (2012) Assuring Data Privacy in Cloud Transformations. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications
Kirkham T et al. (2013) Richer Requirements for Better Clouds. 2013 IEEE International Conference on Cloud Computing Technology and Science. IEEE Computer Society
Kitchin R (2014) The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences. Sage Publications Ltd., Los Angeles
Krishnan K (2013) Data Warehousing in the Age of Big Data. Elsevier, Amsterdam
Kousiouris G, Vafiadis G, Corrales M (2013), A Cloud Provider Description Schema for Meeting Legal Requirements in Cloud Federation Scenarios. In: Douligeris et al. (eds) Collaborative, Trusted and Privacy-Aware e/m-Services, 12th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2013, Athens, Greece, April 25-26, 2013. Proceedings, Springer, Heidelberg
Lebber D, Hermann J, (2013) Decision Analysis Methods for Selecting Consumer Services with Attribute Value Uncertainty. In: Lee ML et at. (eds) Risk Assessment and Evaluation of Predictions. Springer, New York

Legal Risk Management http://www.jus.uio.no/ifp/english/about/organization/nrccl/research-areas/ongoing-research/legal-risk-management.html#ref1 Accessed 10 October 2016.
Li T, Singh M (2014) Hybrid Trust Framework for Loss of Control in Cloud Management. In: Jeong H et al. (eds) (2014) Advances in Computer Science and its Applications: CSA 2013. Springer, Heidelberg
Lohr S (2015) Data-ism: The Revolution Transforming Decision Making, Consumer Behavior, and Almost Everything Else. HarperCollins Publishers, New York
Luiijf E (2016) Threats in Industrial Control Systems. In: Colbert E, Kott A (eds) Cyber-security of SCADA and Other Industrial Control Systems. Springer, Cham
Lund M, Solhaug B, Stolen K (2011) Model-Driven Risk Analysis: The CORAS Approach. Springer, Heidelberg
McKelvey N et al. (2015) Cloud Computing and Security in the Future. In: Zhu S, Hill R, Trovati M (eds) Guide to Security Assurance for Cloud Computing. Springer, Cham
Mahmood Z (ed) (2014) Continued Rise of the Cloud: Advances and Trends in Cloud Computing. Springer, London
Majkic Z (2014) Big Data Integration Theory: Theory and Methods of Database Mappings, Programming Languages, and Semantics. Springer, Cham
Maurer S, Hugenholtz B, Onsrud H (2001) Europe's Database Experiment. Science 294: 789-790
Maurer S (2008) Across Two Worlds: Database Protection in the United States and Europe. In: Putnam J (ed) Intellectual Property and Innovation in the Knowledge-Based Economy, Conference Proceedings, 23 to 24 May 2001, Toronto, Canada. University of Calgary Press, Calgary, AB.
Nwankwo S (2014) Developing a Risk Assessment Methodology for Data Protection, IRI Blog. https://blog.iri.uni-hannover.de/index.php/2014/12/17/developing-a-risk-assessment-methodology-for-data-protection/ Accessed 10 October 2016.
OECD Principles and Guidelines for Access to Research Data from Public Funding, OECD 2007 http://www.oecd.org/sti/sci-tech/38500813.pdf Accessed 10 October 2016
Optimized Infrastructure Services (OPTIMIS). EU funded project within the 7th Framework Program under contract ICT-257115 http://www.optimis-project.eu Accessed 10 October 2016.
Padgett J et al. (2009) Risk-Aware SLA Brokering using WS-Agreement. In: Awan I et al. (eds) Conference Proceedings: 23rd International Conference on Advanced Information Networking and Applications, AINA 2009, IEEE Computer Society, Proceedings. The Institute of Electrical and Electronics Engineers, Inc., Danvers, MA
Pearson S, Yee G (eds) (2013) Privacy and Security for Cloud Computing, Computer Communications and Networks Series. Springer, London
Peng G, Dutta A, Choudhary A, (2014) Exploring Critical Risks Associated with Enterprise Cloud Computing. In: Leung V, Chen M (eds) Cloud Computing: 4th International Conference, CloudComp 2013, Wuhan, China, Springer, Cham
Plain English ISO 31000:2009. Risk Management dictionary, http://www.praxiom.com/iso-31000-terms.htm Accessed 10 October 2016.
Radizeski P (2012) Sellecom 2: Selling Cloud Services. Rad-Info, Inc. Lulu.com.
Rejas-Muslera R, Cuadrado-Gallego J, Rodriguez D (2007) Defining a Legal Risk Management Strategy: Process, Legal Risk and Lifecycle. In: Abrahamsson P et al. (eds) Software Process Improvement, Lecture Notes in Computer Science, Programming and Software Engineering, Proceeding of the 14th European Software Process Improvement Conference, EuroSPI 2007, held in Potsdam, Germany, September 2007. Springer, Berlin
Ridley, E (2015) Big Data and Risk Assessment. In: Kalyvas J, Overly M (eds) Big Data: A Business and Legal Guide. CRC Press, Boca Raton
Rosenberg J, Mateos A (2011) The Cloud at Your Service: The when, how, and why of enterprise Cloud computing. Manning Publications Co., Greenwich, CT

Sakr S, Gaber M (eds) (2014) Large Scale and Big Data: Processing and Management. CRC Press, Boca Raton
Sangrasi A, Djemame K, Johkio I (2012) Aggregating Node Level Risk Assessment in Grids Using an R-out-of-N Model. In: Bhawani S. Chowdhry et al. (eds) (2012) Emerging Trends and Applications in Information Communication Technologies: Second International Multi Topic Conference, IMTIC 2012, Jamshoro, Pakistan, March 2012, Proceedings, Communications in Computer and Information Science, Vol. 281. Springer, Heidelberg
Shantz J (2005) Beyond Risk and Boredom: Reflexions on Claudio Ciborra and Sociology. European Journal of Information Systems 14:510-512
Sharif A, Basri S (2011) Software Risk Assessment: A Review on Small and Medium Software Projects. In: Zain J et al. (eds) Software Engineering and Computer Systems, Second International Conference ICSECS 2011, Kuantan, Pahang, Malaysia, June 2011, Proceedings Part 2. Springer, Heidelberg
Summary White Paper, Legal Options for the Exchange of Data through the GEOSS Data CORE, Data Sharing Task Force, Group on Earth Observations.
Summer J, Ross T, Ababouch L (2004) Application of Risk Assessment in the Fish Industry, FAO Fiesheries Technical Paper No. 442, Part 1.
Sundara Rajan M (2011) Moral Rights: Principles, Practice and New Technology. Oxford University Press, Oxford
Susskind R (1998) The Future of Law. Oxford University Press, Oxford
Taubenberger S et al. (2011) Problem Analysis of Traditional IT-Security Risk Assessment Methods – An Experience Report from the Insurance and Auditing Domain. In: Camensich J et al. (eds) Future Challenges in Security and Privacy for Academia and Industry: 26th IFIP TC 11 International Information Security Conference, SEC 2011, Lucerne Switzerland, June 2011, Proceedings. Springer, Heidelberg
Teng F, Magoules F, (2010) Future of Grids Resources Management. In: Magoules F (ed) Fundamentals of Grid Computing: Theory, Algorithms and Technologies. Chapman and Hall/CRC Press, Boca Ratón
Toosizadeh S, Reza Farshchi S (2011) Ruled-based Programming for Building Expert Systems: How do you create an expert system? LAP Lambert Academic Publishing.
Vraalsen F et al. (2005) Specifying Legal Risk Scenarios Using the CORAS Threat Modeling Language: Experiences and the Way Forward. In: Herrmann P, Issarny V, Shiu S (eds) Trust Management, Third International Conference, iTrust 2005, Paris, France, May 23-26, 2005. Proceedings, Series Vol. 3477. Springer, Berlin
Vashist R (2015) Cloud Computing Infrastructure for Massive Data: A Gigantic Task Ahead. In: Hassanien A et al. (eds) Big Data in Complex Systems: Challenges and Opportunities, Studies in Big Data, Vol. 9. Springer, Cham
Wahlgren P (2007) Legislative Techniques. In: Wintgens L (ed) Legislation in Context: Essays in Legisprudence, Applied Legal Philosophy. Ashgate Pub Co, Hampshire
White Paper, Mechanisms to Share Data as Part of GEOSS Data-CORE https://www.earthobservations.org/documents/dswg/Annex%20VI%20-%20%20Mechanisms%20to%20share%20data%20as%20part%20of%20GEOSS%20Data_CORE.pdf Accessed 10 October 2016.
Williams P (2013) Information Security Governance: A Risk Assessment Approach to Health Information Systems Protection. In: Hovenga E, Grain H (eds) Health Information Governanc in a Digital Environment. IOS Press, Amsterdam
Wintgens L, Thion P (2007) Introduction. In: Wintgens L (ed) Legislation in Context: Essays in Legisprudence, Applied Legal Philosophy. Ashgate Pub Co, Hampshire
Wright D, De Hert P (eds) (2012) Privacy Impact Assessment, Law, Governance and Technology Series, Vol. 6. Springer, Dordrecht.

Wu L et al. (2013) Automated SLA Negotiation Framework for Cloud Computing, International Symposium on Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM, May 13016, Delft, The Netherlands https://pdfs.semanticscholar.org/6660/3838e3d4e2bdec718bed6b94d8cd730aea26.pdf?_ga=1.212388371.624674434.1462343094 Accessed 10 October 2016.

XML Description Schema http://www.optimis-project.eu/content/xml-description-schema-improvement Accessed 10 October 2016.

Fellows W, Ring, K, Rogers O (2014) Cloud Brokers: Making ITAAS a Practical Reality? https://451research.com/images/Marketing/DIS/451_CloudBrokers_2014_FINAL.pdf Accessed 10 October 2016.