CLOUD ACCOUNTABILITY PROJECT

D:C-6.1: Risk and trust models for accountability in the cloud

Deliverable Number:	D36.1
Work Package:	WP 36
Version:	Final
Deliverable Lead Organisation:	SAP
Dissemination Level:	PU
Contractual Date of Delivery (release):	31 March 2014
Date of Delivery:	02/01/2014

Editor
Anderson Santana de Oliveira (SAP)

Contributors
Anderson de Oliveira, Alexandr Garaga (SAP); Leonardo A. Martucci (KAU); Massimo Felici, Rehab Alnemr (HP); Dimitra Stefanatou, Maartje Niezen (TiU); Carmen Fernandez, David Nuñez (UMA); Bushra Hasnain, Asma Vranaki (QMUL) and; Erdal Cayirci (UiS)

Reviewer(s)
Alain Pannetrat (CSA), Thomas Ruebsamen (HFU)

Executive Summary

Adequate trust and risk management are fundamental for governance in the cloud. Data controllers, processors, or more generally cloud customers must be aware of specific risks for business confidential, personal and other kinds of sensitive data subject to regulatory restrictions when using cloud services.

In this deliverable we describe the progress in defining a representation of trust and risk for cloud service chains. We build on existing methodologies to create a high level approach to define risk in terms of the actors involved in a cloud service chain, possibly combining Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), their responsibilities, obligations, and other accountability attributes, to finally determine how the trust assigned to each link in the chain will influence risk assessments.

We reviewed extensively risk analysis methodologies, guidelines, models and standards to identify the gaps they have when applied to cloud computing, under the perspective of accountability. We propose a broad approach covering all risk categories mentioned in the literature, very close to the enumeration proposed by ENISA(ENISA, 2009).

Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. The majority of cloud computing agreements are offered in standard form, often drawn on traditional outsourcing or technology licensing models, but those types of agreements may not cover the particular risks associated with cloud computing. We provide an analysis of the impact of risks to the conclusion of cloud contracts, and how risk allocation affects the reliability of contracts as effective trust mechanisms - in particular, the security obligations allocated to data controllers -and data processors- established under the Data Protection Directive aim at mitigating risks, given that both entities are obliged to adopt "appropriate security measures" depending on the nature of processing.

Trust also greatly influences the adoption of cloud services, shifting the cloud market. It is necessary to understand how social behaviour of (potential) cloud consumers will affect their choice to make use of cloud services. Aiming to integrate both the computer and social science perspectives on trust we investigate the social economic impact of changing roles, responsibilities and risks due to the use of cloud services by the different cloud consumers, as trust is shaped by the consumers' perceptions of risk in cloud providers and their services. We depicted different perspectives on trust, in particular on how to make it measurable via the notion of reputation and other important elements for a risk and trust model. The deliverable also elaborates on the understanding of the relationships among accountability, risk, and trust and how this enables accountability governance. We present an analysis of stakeholder feedback (from the B2 – Stakeholder Elicitation workshop dedicated to risks)

We created an abstract meta-model for cloud ecosystems, to which we mapped the A4Cloud conceptual framework of the work package C2. From this we can instantiate specific cloud service chains, following a structured approach in order to determine the trust and risk levels. In this deliverable, we set up the basis for modelling trust relationships and for enumerating risks in cloud ecosystems that will be the starting point for the privacy impact assessments. We also investigated how continuous risk monitoring of cloud services can be performed in an accountable and trustworthy setting, by creating a generic analytical model to understand how concrete events about the service operations, security and privacy will influence the risk and reputation levels for a given service composition. We confirmed the fitness of the model using numerical analysis using Monte Carlo simulations.

Table of Contents

Index of Figures

Index of Tables

1 Introduction

Cloud security requirements reflect intrinsic security problems not seen in regular IT security scenarios. Current risk assessment methods are not tailored to cloud computing: the lack of transparency on how cloud service ecosystems are composed prevents the seamless application of traditional methodologies and standards. While the future internet creates new business opportunities it also creates a variety of new risks as connectivity and the multi-domain created by trust and organizational boundaries increases. Because of its setup, cloud computing creates several types of technical, organizational and regulatory “complexities” and risks.

The typical risk management lifecycle involves risk assessment, setting policies to mitigate these risks, implementing controls and running systems in accordance with these controls, and monitoring and auditing to ensure risks are mitigated.

Nowadays, the state of the art does not tackle new, emerging aspects related to cloud and accountability. Uncertainty about cloud service providers’ behaviour or practices and uncertainty about the cloud services offered can affect cloud consumers’ risk perceptions. As highlighted in (Silva, Westphall, Mattos, & Santos, n.d.) major difficulties regarding risk analysis in cloud computing stem from the lack of clarity about the involved agents and their respective responsibilities in the risk management processes.

For example, moving to cloud will remove control and flexibility from service users, so that better risk planning must be achieved prior to contract negotiation and service initiation. In this report, we provide an initial socio-economic analysis of the notions of risk in cloud ecosystems, looking at the interaction between (perceived) risks and the cloud ecosystem. Exploring these notions will provide an understanding of stakeholders’ behaviour with regard to cloud computing.

As IT functions are spread across the cloud, companies will need not only event monitoring systems that cross cloud boundaries, but also assurance systems that demonstrate that each service provider is enforcing their required policies and that the combination adequately manages risk. These objectives are to be achieved by the A4Cloud project as a whole; however the missing link among them is a common model to allow assessing risk based on some trust assumptions and how to use such representations to derive contracts, policies and controls that will enable accountability. In this report we describe how we can build machine-readable models to allow for an accountability-based approach for risk and trust management for the cloud. In order to understand the objectives of this work, we introduce briefly the terminology, the cloud scenarios where risk analysis is needed, and the relationship of the risk and trust models to other parts of the A4Cloud project.

1.1 Terms and Definitions

Throughout this document the following terms are defined according to the A4Cloud glossary, which describes common terms used along the A4Cloud project, and the EC ICT Work Programme 2011-12. In this section, we list the terms that are relevant to this deliverable and define others that are included in the A4Cloud glossary[1].

- *Risk* Is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.
- *Risk analysis* is the systematic use of information to identify sources and estimate risk.
- *Trust*: Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action.

[1] http://www.a4cloud.eu/lexicon/glossary/letter_a

- *Trustworthiness* is defined as: The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfil assigned responsibilities.

"Risk in the modern world is confronted and dealt with in three fundamental ways. Risk as feelings refers to our fast, instinctive and intuitive reactions to danger. Risk as analysis brings logic, reason and scientific deliberation to bear on hazard management. When our ancient instinct and our modern scientific analyses clash, we become painfully aware of a third reality – risk as politics." (Slovic, Finucane, Peters, & MacGregor, 2004). The literature brings further definitions for risk:

"Risk, in general, means the perceived probability of loss or harm." (Rousseau, Sitkin, Burt, & Camerer, 1998)

"Risk is a measure of probability and severity of adverse effects" (Lowrance, 1976).

An essential element of risk management is risk analysis, for which an analytical definition is the following: risk analysis is an estimation of the occurrence of events, their possible consequences, their causes, and existing and/or planned countermeasures and mitigations. Risks are related to uncertainty, which is expressed as a probability *P* that is associated to a given event. The information used to assess a probability P associated with an event *A* is a base of knowledge *K*. The conditional probability *P(A|K)* expresses the probability of occurrence of event *A* given *K*, and the conditional probability *P(B|A,K)* expresses the probability of occurrence of consequence *B* given *A* and *K*. Note that knowledge base *K* is full of assumptions and uncertainties.

Risk analysis is defined as "an attempt to envision how the future will turn out if a certain course of action or inaction is taken" (Kaplan and Garrick 1981). Three questions are answered during a risk analysis:

- A scenario s_i (i.e., What can go wrong?)
- The probability p_i of s_i (i.e., the probability that the scenario is realized)
- The consequence x_i of s_i

Hence, the risk *R* is a set of triplets that answers three questions (i.e., $R=\{<s_i, p_i, x_i>\}, i=1, 2, \ldots, N$) for N scenarios (i.e., *N* represents the number of all possible scenarios) (Kaplan and Garrick 1981). This definition focuses on a single risk. However, risk analysis should end up with a set of N risks, where hopefully N is the number of all risks.

From (Landoll, 2011), we take some key terms and definitions:

- Asset - Resource, data, or other item of value to the organization
- Threat - A threat is an undesired event that may result in the loss, disclosure, or damage to an organizational asset
- Vulnerability - A vulnerability is a flaw or oversight in an existing control that may possibly allow a threat agent to exploit it to gain unauthorized access to organizational assets

The next sections of the document discuss in depth the concepts of trust and its implications to accountability from a security and privacy perspective.

1.2 Generic Scenarios

Here we present the generic scenarios considered in this WP that illustrate the problem of concern within concrete contexts thus giving a rationale behind the requirements in the next section.

1.2.1 Scenario 1a: Enterprise moving to Cloud

In this scenario an Enterprise would like to move part of its business process to the cloud thus improving the connectivity with their customers (Figure 1). However, such a drastic change apart from opportunities presents a number of risks (e.g. see Section 6.4). If the Enterprise is the data controller

this move will lead to compliance challenges as whatever happens with the personal data in the cloud service provision chain, the data controller is liable according to the EU Data Protection regulation.

Thus, before switching to the new business model the Enterprise has to do a thorough risk assessment of the different cloud deployment models (Private, Public, Community, or Hybrid) and different CSPs. The decision then will be made balancing the business opportunities versus risks.

1.2.2 Scenario 1b: Enterprise reassessing subcontracting risks

Over time the risk landscape provided by the initial risk assessment changes. This may be due to change in the cloud ecosystem (e.g. new subcontractor, new software installation) as well as the environment (e.g. discovery of new hypervisor vulnerabilities, new regulations). In order to have an up-to-date risk landscape the Enterprise has to continuously monitor these risks and revaluate its decisions if necessary (e.g. switch to a more secure CSP or implement additional controls).

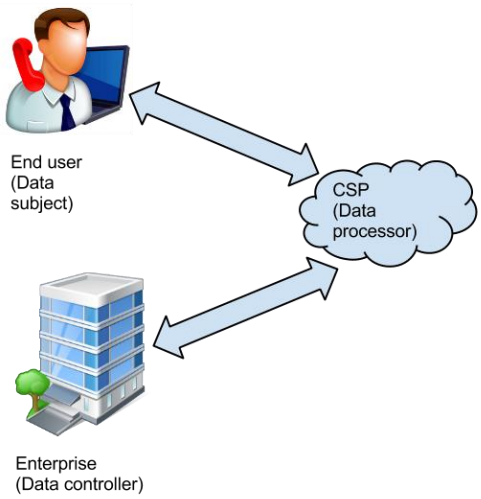

Figure 1 Scenario 1 - Enterprise to CSP

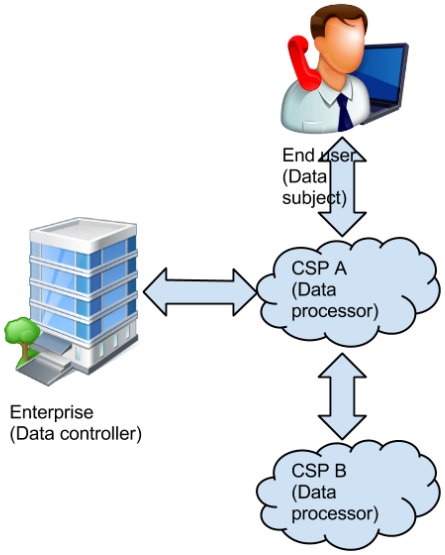

Figure 2 Scenario 2 - CSP to CSP

1.2.3 Scenario 2a: CSP subcontracting another CSP

In this scenario CSP A acting as a data processor decides to subcontract another CSP B and outsource part of the provision, e.g. infrastructure (Figure 2). However, if the binding agreements are in place between the Enterprise and CSP A regarding the security guarantees in case of a security incident CSP A will be liable even if the incident is a subcontractor's fault. In order to contain the risks resulting from this change CSP A has to perform a thorough risk assessment of the different cloud deployment models and different subcontractors. The decision then will be made balancing the business opportunities versus risks.

1.2.4 Scenario 2b: CSP reassessing subcontracting risks

Over time the risk landscape provided by the initial risk assessment changes. In order to have an up-to-date risk landscape CSP A has to continuously monitor these risks and revaluate its decisions if necessary (e.g. switch to a more secure subcontractor or implement additional controls).

1.2.5 Scenario 3a: Cloud broker subcontracting a CSP

In this scenario an Enterprise would like to move part of its business process to the cloud but it decides instead of dealing directly with potential CSPs to use a Cloud broker (Figure 3). They setup binding agreements that transfer the liability on Cloud broker in case of the selection of an unreliable CSP. In order to contain the risks the Cloud broker has to perform a thorough risk assessment of the different cloud deployment models and different CSPs. The decision then will be made balancing the business opportunities versus risks.

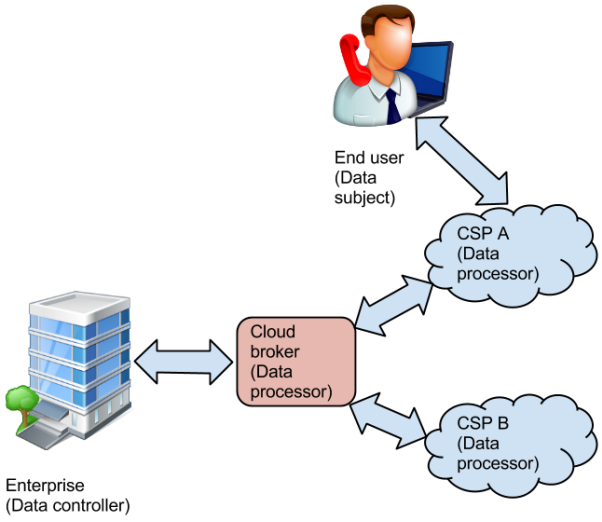

Figure 3 Scenario 3 - Cloud broker to CSP

1.2.6 Scenario 3b: Cloud broker reassessing subcontracting risks

Over time the risk landscape provided by initial risk assessment changes. In order to have an up-to-date risk landscape, the Cloud broker has to continuously monitor these risks and revaluate its decisions if necessary (e.g. switch to a more secure subcontractor or implement additional controls).

1.3 Objectives and Scope of the Risk and Trust Models Work package

Understanding the risks of using cloud services is a fundamental issue, whose importance is reinforced by the need to analyse the risks to accountable data processing in the cloud.

In WP:C-6 we follow a multidisciplinary approach to embed the concept of accountability in the cloud. We integrate legal, socio-economic, regulatory and technical approaches into a framework to provide accountability pre-emptively, to assess risk and avoid privacy harm and reactively to provide transparency, auditing and corrective measures for redress. In addition to the interdisciplinary background of the work package partners themselves, it is important to explain how the WP:C-6 results will be used across the project. The interactions of our results with other work packages from the requirements work stream are highlighted in Figure 4.

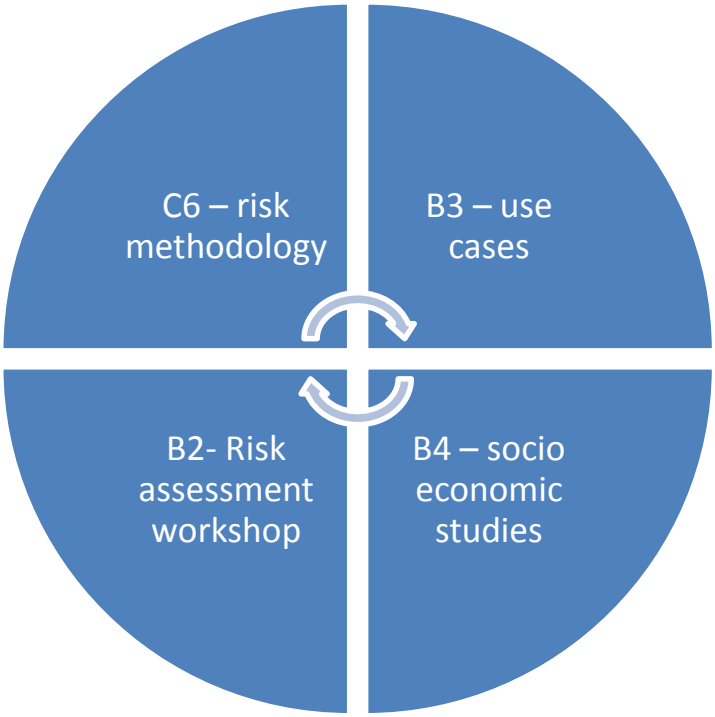

Figure 4 C6 dependencies with respect to Stream B

Our approach is to focus on the concepts emerging from the framework from WP:C-2 to determine the methodology and to identify which input we need to collect from cloud stakeholders in the inter-disciplinary risk workshop organized by WP:B-2. In B4, the development of a game-theoretic model of economic governance to study under which circumstances and how accountability can solve the moral hazard problem – or, in different terms, the one-sided Prisoner's Dilemma problem – involved in cloud computing. The model will use input from risk assessment (WP:C-6), consequence estimations of accountability breaches and data collected from enterprises through case studies and interviews. In the current report, we used some simple scenarios from the B3 use cases to illustrate some features of our models. A complete risk and trust analysis of the use cases will be performed in Task T:C-6.4.

In terms of the work stream C, the cohesion of the work in C6 is also very strong, as shown in Figure 5.

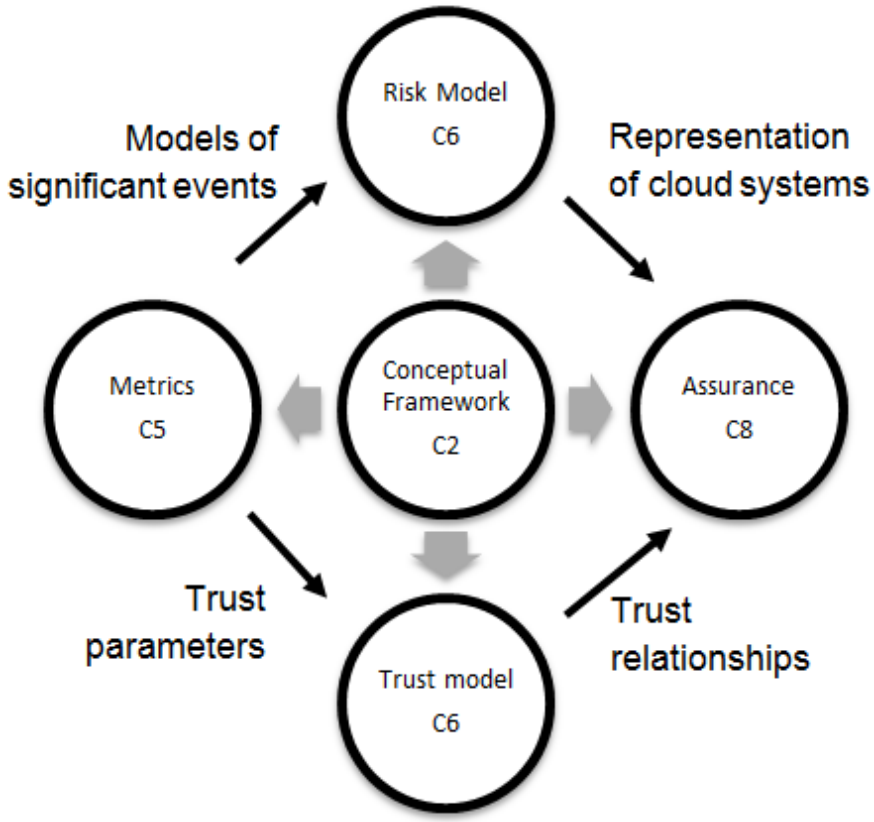

Figure 5 C6 relationships in Stream C

The conceptual framework from C2 determined the attributes of the cloud environment itself to the C6 models, in particular the way we represent accountability relationships. As we follow a very classic object oriented approach, the models can assume a machine-readable representation in a straightforward way, to be later used in combination with the metric techniques emerging from WP:C-5. These machine readable representations will be useful in WP:C-8, in order to automate the A4Cloud framework of evidence.

This report covers the first two tasks of work package C6. First we investigate the relationships among accountability, risk, and trust, and we derive a computer-based representation for it that will allow us to continuously assess the risk and trust levels for a given cloud service. Second, we develop a representation for cloud ecosystems, together with a methodology to analyse risks in cloud service chains, where multiple levels of outsourcing may happen. Our work focuses on personal data protection, but other regulatory compliance concerns could also be modelled.

From the input received from the other work packages, we identified the following requirements for A4Cloud risk and trust model and relate it to the main tasks:

T:C-6.1 Definition of the risk and trust models

- **REQ (Representing stakeholders assets)** Capture each stakeholder's assets, specifically personal and business sensitive data.
- **REQ (Modelling trust relationships)** Provide a representation usable for modelling of trust relationships and delegations in the cloud supply chain.
- **REQ (Separate risk profiles)** to allow for the creation of separate risk profiles for different stakeholders: cloud consumers, cloud providers, cloud brokers, when performing their risk assessments.
- **REQ (Represent vulnerabilities and threats)** Be able to represent explicitly in the risk and trust models specific vulnerabilities and threats

T:C-6.2 Modelling cloud infrastructures and controls

- **REQ (Modelling cloud environments)** Encapsulate cloud and accountability concepts (main parties, deployments model, service supply chains, security (accountability) controls).
- **REQ (Machine-readable representation)** Provide machine-readable representations amenable to automated treatment by tools.
- **REQ (Dynamic risk monitoring)** Associate risk analysis with event monitoring in order to determine impact and the risk thresholds in different cloud landscapes. Constantly update the risk and trust model based on the new events.

T:C-6.3 Data protection impact assessment tool - this task started on month 13 and will use the results reported in the current deliverable.

- **REQ (Impact assessment)** Assess the impact of specific events from cloud environment (using accountability metrics from WP:C-5).
- **REQ (Risk estimation)** Estimate the risk levels (using accountability metrics from WP:C-5).
- **REQ (Facilitate CSP selection)** Facilitate the selection of a Cloud Provider matching customer's business needs and risk profile.
- **REQ (Support contractual negotiations)** Support the negotiations of contract terms and SLAs based on the risk profile.

T:C-6.3 Use cases risk and trust assessment – this task will start on month 19, thus it will benefit from the maturity of the research and development performed in the previous tasks

- **REQ (Applicability to Business Use Cases)** the models must support realistic use cases, composed of multiple cloud service providers, as defined in WP:B-3

1.4 Document Organisation:

The remainder of this document is organised as follows:

- Section 2 discusses related works and the state of the art concerning risk for cloud computing complemented.
- Section 3 presents different perspectives on the notion of trust with an analysis of the socio-economic and aspects in dealing with (perceptions of) risks related to cloud computing technologies by organisations and individuals.
- In Section 4 we will explore how contracts might operate as trust mechanisms between cloud service providers and cloud service users.
- Section 5 discusses the emergent relationships between accountability, risk and trust, and how such relationships underpin accountability governance.
- On Section 6 we elaborate a meta-model where it is possible to represent the different accountability concerns in terms of the relationships among the different cloud actors, building on the knowledge introduced in the first sections and on the A4Cloud conceptual framework.
- Section 7 describes an accountability-based approach to risk, positioning the modelling approach within the risk management life cycle, including the risk monitoring phase, for which we propose an analytical approach for computing risk and reputation, based on the observed events in the cloud ecosystem, supported by experimental results.
-
- Section 8 summarizes the contributions reported here and how it responds to the requirements enumerated above.

2 Perspectives and Related Work on Risk

Risk and trust are complex notions that have attracted researchers for thousands of years in various contexts. Recently in the field of computer science, risk assessment and security –especially for cloud computing– have become one of the focal research fields both for industry and academia. In this section, we provide a survey on the recent literature for risk and trust modelling in the field of computer science as well as related standards. Please note that our survey in this report cannot be exhaustive due to the extensive literature in the field. We include the most recent and relevant work to the accountability based approach for cloud computing in this section. In the following section, the social and legal perspective of risk and trust are discussed.

2.1 Risk Assessment

Risk assessment is a more difficult issue for a cloud customer than for a conventional information system user. Not all cloud service providers (CSP) clearly inform the locations of their server farms and data centers to customers[2]. The architecture and the details of the CSP's infrastructure are not known by its customers. Due to the autonomic features of a cloud, such as self-configuration, self-optimization and self-healing algorithms, even CSPs may not know in which actual physical servers the processes and the data of a consumer are located at a given time. Additionally, CSPs have to prioritize the issues to solve when risks occur. These uncertainties increase the risks for cloud users. Similarly, all these facts also introduce new threats and vulnerabilities with increased value of assets and consequences for CSPs. Therefore, the risks that a CSP is exposed to may also be much higher than a conventional IT service provider, which makes risk assessment a more important and difficult task for CSPs.

Risk assessment is a part of risk management and includes risk analysis (see Section 6 for details). There are many risk assessment methodologies available in the literature, and they can be categorized based on various approaches as listed below:

- Formal versus informal procedures: For risk assessment, a formal process can be used. Alternatively, it can be carried out without following any predefined formal technique.
- Qualitative versus quantitative techniques: The results of risk assessment can be given by using qualitative scales, such as high, moderate and low, or by using numbers, such as 0.95.
- Consequence versus cause analysis: For risk assessment, the consequences, the causes or both can be analyzed.
- Inductive versus deductive techniques: Risk assessment can be made forward looking and planned starting from potential threats and vulnerabilities. It may be made also backward looking from the potential events.

In this subsection we explain a selected set of risk assessment methodologies and identify their categories according to the approaches listed above when applicable.

2.1.1 Microsoft's Cloud Risk Decision Framework

Microsoft has proposed a Cloud Risk Decision Framework(Stone & Noel, 2012) based on the ISO 31000 risk management standard[3]. Its purpose is to help cloud consumers assess potential cloud offerings and select the one that meet certain risk acceptance criteria. For each of the cloud offerings, the adapted ISO 31000 process is executed to construct the respective risk profile, which is subsequently compared to the current solution (maybe a non-cloud solution) as the baseline. During the analysis particular attention is paid to the relevant corporate governance policies and guidelines and to the regulatory environment. The document provides a list of possible risks for the cloud grouped in four categories: compliance risks, strategic risks, operational risks and market & finance risks, aimed at helping the risk identification. For the compensating controls the framework recommends to use CSA Cloud Control Matrix (CCM)(CSA Cloud Security Alliance, 2013b).

[2] http://www.cloud-council.org/publiccloudSLA.pdf
[3] http://www.iso.org/iso/home/standards/iso31000.htm

Microsoft's Cloud Risk Decision Framework seems to be better suited for risk assessment of cloud scenarios than general frameworks. At the same time the process remains quite abstract and does not dictate which specific Risk and Trust models to build that would facilitate subsequent risk identification and estimation. Additionally, it considers only the point of view of a cloud consumer and ignores those of cloud provider and cloud end user.

2.1.2 Quantitative Impact and Risk Assessment Framework for Cloud Security - QUIRC

In (Saripalli & Walters, 2010), a framework for assessing security risks associated to cloud platforms is presented. A set of six primary security objectives is identified relative to cloud security – CIAMAU (Confidentiality, Integrity, Availability, Multiparty trust, multiple Auditability and Usability), but they do not address explicitly the principle of accountability. Each organisation defines the priorities for the security objectives.

The risk assessment is performed by analysing a predefined set of common cloud threats and assessing the probability and impact values of each one on the corresponding objective. Among the list of common cloud threats only few are cloud-specific and the rest are generic internet threats.

The probabilities are estimated by analysing the history of previous attacks, e.g. the one provided by SANS Institute[4]. However, it should be noted that this report gives only the number of attacks and without an actual number of access attempts and the percentage of successful attacks. Therefore, it is problematic to infer real attack probabilities based on it. The impact values are organization specific assigned by managers and domain experts. Lastly, the quantitative risk values can be calculated by multiplying threat events probabilities on the impacts and aggregating for all security objectives.

Similarly to the previous approach, the paper does not attempt to construct a comprehensive risk and trust model for the cloud ecosystem, taking into account the service supply chains, trust and accountability relationships. However, it could be practical when there are statistics of previous incidents and several security experts are involved.

2.1.3 Failure Modes and Effect Criticality Analysis (FMEA)

FMEA(Bowles & Peláez, 1995) (or FMECA) is a simple analysis designed to reveal possible failures and predict effects on a system. It is a systematic inductive method. FMEA divides a system into singular components and investigates the consequences of a failure. FMEA is based on forms that list all components of a system, their relationship to other components, probabilities of failure and their consequences among other fields in a given form. FMEA considers one component failure at a time and thus is not suitable for detecting critical combination of components. FMEA provides a systematic view of important failures and also a good basis for more comprehensive risk analysis. However, FMEA overlooks human failures, as it focuses on component failures and is unsuitable for systems with much redundancy. In addition, FMEA is a resource demanding analysis, as all components of a system are analyzed individually.

This kind of analysis requires a great deal of knowledge of the security processes implemented in the cloud ecosystem and hence can be used mainly by the CSPs.

2.1.4 Fault-Tree Analysis (FTA)

FTA (W. S. Lee, Grosh, Tillman, & Lie, 1985) is one of the most used threat modelling methods. It is based on a deductive logical tree which describes the relations between system failures (events) and failures of the components of a system. It starts by identifying undesirable events and identifying their causes and placing them on top (root) of a logical tree. The bottom of the tree (the leaves) consists of component failures and/or human errors, the so-called basic events. The branches of the tree are

[4] http://isc.sans.edu/reports.html

connected with logical gates, such as logical AND, OR, etc. FTA is able to identify combination of component failures.

Like FMEA, FTA is time consuming and not tailored to the cloud or even the IT domain.

2.1.5 European Network and Information Security Agency (ENISA)

ENISA's Cloud Computing Security Risk Assessment guide (ENISA, 2009) provides an overview of assets, vulnerabilities and risks associated to the cloud (specific to the cloud and to Internet in general). The risks are categorised into policy and organizational risks, technical risks, legal risks and risks not specific to the cloud. The description of each risk includes risk levels (likelihood, impact), the comparison to the baseline (non-cloud solution), affected assets and exploited vulnerabilities. The guide also provides a template questionnaire for a typical CSP that covers various control categories and thus provides transparency into CSP's operations.

It aims to help the cloud consumers at comprehensively assessing risks to moving to the cloud and choosing appropriate CSPs as well as developing effective strategies and policies for mitigating the underlying risks. We extensively used this guide in developing our approach described in Sections 5 and 7.

2.1.6 Shared Assessments Guide

Shared Assessments (Niall Browne, Susanna Space, 2010) is a process specifically designed for the financial institutions for the evaluation of the security controls introduced by their information technology service providers. It discusses how new technologies present unknown risks that must be considered before and during migration to cloud environments, and is based on ISO 27002 (see the standards subsection of this section of our document). It includes agreed upon procedures (AUP) and standardized information gathering questionnaire (SIG). AUP and SIG are used for evaluating security controls.

2.1.7 Joint Risk and Trust Model for MSaaS Mashups

Joint Risk and Trust Model for MSaaS Mashups (JRTM) is a model developed by an A4Cloud partner and published recently (Cayirci, 2013), where a mashup is a service comprising multiple cloud services in various forms (i.e., Iaas, PaaS or SaaS) for providing a composite service. JRTM is a quantitative trust and risk model introduced for modelling and simulation as a service (MSaaS) mash-ups. In this model, the real risk is defined as the risk that cannot be (or is not) eliminated by a CSP. The model describes how to estimate the security and the service outage risk to the cloud service customer, where the risk is perceived as the probability that a security threat is realized or the probability that a service outage occurred. The trust is evaluated as the probability that the CSP can eliminate a security risk when it occurs or the probability that the CSP can recover from a service outage before it hampers the user's operations. The probabilities for risk and trust are determined based on historic data. For trust negative and positive performances are differentiated and the freshness of the data is taken into account. We explored this model as a means to perform continuous monitoring of risk indicators and of the performance of accountability controls in Section 7.6

2.1.8 Cloud Security Alliance (CSA) Guidance

CSA does not provide a full-fledged methodology for risk assessment for the cloud. Its security guidance report (Brunette & Mogull, 2009) brings an editorial note on how to assess the relevance of critical risks, intended as a quick method for estimating risk tolerance of potential cloud adopters. The approach is structured as follows:

- Identify the asset for cloud deployment (data, or applications, functions and processes) – this consists in determining exactly what data or business process will move to the cloud.
- Evaluate the asset – determine the importance of the asset to the organisation. It is a basic assessment of the sensitivity of the asset. In essence, determine confidentiality integrity, and

availability requirements for the asset, and whether the risk changes if all or part of it is handled in the cloud.
- Map the asset to a Cloud deployment model (public, private, community, or hybrid) – choose a model that provides an acceptable risk level.
- Evaluate the potential cloud ecosystem models and providers – evaluate whether IaaS, PaaS, or SaaS is the appropriate choice for the asset, depending on the desired level of control. This will impact on being responsible for implementing risk mitigations. Specific requirements will influence the decision, for instance, if handling data subject to specific regulations.
- Map out the potential data flow – it is necessary to identify the data flows from the cloud consumer organisation, the cloud provider service, and customers (or other nodes). The principle is to understand how data can move in and out of the cloud. Risk exposure points can be delineated, and some unacceptable flows eliminated in this manner.

The security guidance suggests the approach to be performed prior to adopting the security recommendations it makes, as not all security controls are suitable or necessary for a given asset and cloud deployment. A high-value regulated asset might entail audit and data retention requirements. For high-value assets, which are not subject to regulatory restrictions, the cloud consumer may focus on more technical security controls, such as encryption to protect it on the cloud, with fewer constraints on auditability.

The report also emphasizes the importance of an effective program for governance and enterprise risk management for cloud computing, see the CSA GRC Stack project[5], from which we highlight the CCM – Cloud Control Matrix (CSA Cloud Security Alliance, 2013b): The Cloud Control Matrix is a list of control points and their specification, which are mapped to other security standards, control frameworks and regulations, such as NIST, ISO certifications. It will be useful in modeling controls in our work.

2.1.9 Open Security Architecture

Open Security Architecture (OSA)[6] provides a generic architecture implementing a set of controls and addressing a number of threats. The most relevant part of this initiative is the control catalog and graphical security architecture patterns which map controls to specific elements in the architecture. The Cloud Computing pattern, in particular, depicts the involved actors and the recommends the distribution of security controls between the system components and involved actors. This is the main difference with CSA CCM that merely lists the security controls without specifying so explicitly the application points.

2.2 Information Security and Risk Management Standards

As stated above, regulatory compliance is an important factor that influences the trust in a CSP. Moreover, CSPs have to comply with regulations to operate within the EU. We also survey international standards to which CSPs can be required to comply with in this subsection. Apart from international standards, every EU member state has a special law, typically called “Data Protection Act” on the protection of personal data. Most of these laws have been in effect for around 15 years, and mandate the protection of personally identifiable information, for which a high demand for IT security risk management framework emerged. Recent cyber security incidents have increased the interest in this topic and efforts for standardization.

Internationally recognized information/cyber security standards also applicable to cloud infrastructures include the following:

[5] https://cloudsecurityalliance.org/research/grc-stack/
[6] http://www.opensecurityarchitecture.org/cms/

- International Organization for Standardization (ISO) Standards 2700x series publications: ISO 27001[7] standardizes the certification process for Information Security: it defines an information security management system that includes a structure and controls. ISO/IEC 27002[8] describes good IT security management process. The standard is arranged into 11 control areas, covering confidentiality, integrity and availability properties.
- National Institute of Standards and Technology (NIST) 800-xx series publications[9]: NIST 800-12[10] gives an overview of computer security good practices and elaborates on control areas; NIST 800-14[11] explains security principles commonly used; NIST 800-37[12] introduces a risk management framework to federal information systems; and NIST 800-53[13] is a guide for assessing the security controls in federal information systems.
- Internet Engineering Task Force (IETF) publications: Request for Comments (RFC) 2196[14] is an IETF publication that provides an overview on topics related to the development of security procedures and policies for the information systems in the Internet.
- International Society for Automation (ISA) standards: ISA/IEC 62443[15] describes the electronically secure industrial automation and control systems with a wide perspective that includes all the stakeholders from various domains, such as, manufacturers, security practitioners, system integrators and users.

However, the standards explained in this subsection define a set of generic processes and controls for ensuring information security and as such are also applicable to cloud infrastructures. However, these generic frameworks have the following disadvantages:

- Expensive and time consuming. For example, to perform a full risk assessment process (e.g. from ISO 31000[16]) would need hiring a consulting agency and involve a number of parties and iterations. This is not often feasible for SMEs and so they would need a more efficient approach tailored for cloud computing. Moreover, this process ideally has to be done for each potential CSP, in case the customer is deciding which one to choose for outsourcing part of his business process.
- Opacity of CSP infrastructures and processes. For an effective risk evaluation one would need to get objective picture of the level of security that the CSP has implemented in his infrastructure. CSPs, however, rarely disclose this kind of information: at best they can reference some obtained certificates.
- Limited treatment scope. In case the risks are unacceptable cloud consumers have little room for introducing mitigations. As they do not usually have management access to the underlying cloud infrastructure the choice are restricted to contractual mitigations or adopting another CSP.

There are also international standards on risk management. A generic standard for risk management is ISO 31000, which provides principles and guidelines for risk management. ISO 31010[17] focuses on risk assessment concepts, principles and approaches for selecting risk assessment techniques.

[7] http://www.iso.org/iso/iso27001
[8] http://www.iso.org/iso/catalogue_detail?csnumber=54533
[9] http://csrc.nist.gov/publications/PubsSPs.html
[10] http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/
[11] http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
[12] http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
[13] http://dx.doi.org/10.6028/NIST.SP.800-53r4
[14] http://tools.ietf.org/html/rfc2196
[15] http://isa99.isa.org/ISA99%20Wiki/Home.aspx
[16] http://www.iso.org/iso/iso31000
[17] http://www.iso.org/iso/catalogue_detail?csnumber=51073

Examples of risk management related standards specialized on IT: NIST SP 800-30 and NIST SP 800-37 (NIST, 2010, 2012) and cloud computing: NIST SP 800-144 and NIST SP 800-146 (Badger, Grance, Patt-Corner, & Voas, 2012; Jansen & Grance, 2011). Although these publications cover both risk management and security in cloud computing, there is not yet a publication on the intersection of both areas. It is clear that the intersection of risk management and cloud computing needs careful attention, as cloud computing raises new problems and challenges to organizations that outsource their information systems.

In the cloud-related publications, NIST provides a collection of identified risks and threats, categorized according to the cloud ecosystem model (Software as a Service, Platform as a Service, and Infrastructure as a Service) and type of cloud (public, private, community and hybrid). One of the main points made in these publications is that the outsourcing of services, systems and processes to the cloud makes the evaluation of threats and risks difficult, as the internal procedures and systems of the cloud cannot be controlled, and in some cases, little or no information about them is available to the cloud customer. Organizations should then carefully assess the trade-off between the advantages of moving to the cloud and the disadvantages associated to the loss of control.

Apart from NIST SP 800-30 series, ISO13335[18], ISO/IEC 27005[19], BS7799-3[20] and ISACA Risk IT are also standards that specifically address IT risk management. The ISO/IEC 27005 framework provides guidelines for risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and review. It accepts context establishment as the first step in IT risk management in which basic criteria, purpose, scope and boundaries of risk management are determined. Risk assessment consists of risk analysis (risk identification and estimation) and risk evaluation.

ISO/IEC 27005 recommends the following among the things to be examined for risk assessment: security policy, organization of information security, human resources security, physical and environmental security, access control, information security incident management and regulatory compliance. Risk identification aims to identify what could cause a potential loss and examine the following for this: assets, threats, security measures, vulnerabilities, consequences and related business process; risk estimation involves deriving the risk levels by estimating probabilities and consequences of potential unwanted events; risk evaluation is concerned of providing decision on the risk mitigation strategies (accept, transfer, mitigate).

2.3 The Notion of Risk and Stakeholders' Risk Perception

The emergence of cloud computing has drastically changed the use of information technology; from a private to a public utility. However, together with the rapid transition towards the clouds, the number of concerns with regard to e.g. security, reliability, and privacy has risen. Uncertainty about cloud service providers' behaviour or attributes (i.e. competence, benevolence, and integrity) and uncertainty about the cloud services offered can affect cloud customers' risk perceptions (D. H. McKnight, Choudhury, & Kacmar, 2002). The concept of perceived risk, from a customer perspective, defines risk in terms of the customer's perceptions of the uncertainty and adverse consequences of using a service, in this case cloud computing (Dowling & Staelin, 1994). Perceived cloud risk means the extent to which a user believes it is unsafe to use the cloud or that negative consequences are possible. Perceived risks therefore (might) affect purchasing behavior and subsequently innovation. The different stakeholders in cloud ecosystems potentially identify different cloud computing risks and/or perceive the identified risks differently. With respect to governing the behavior of cloud customers and cloud providers an understanding of the perceived risks is relevant since choices to adopt the cloud are not only based on facts, but often also on more intuitive considerations (Ryan & Falvey, 2012; Sjoberg & Fromm, 2001).

[18] http://www.iso.org/iso/catalogue_detail.htm?csnumber=39066
[19] http://www.iso.org/iso/catalogue_detail?csnumber=56742
[20] http://shop.bsigroup.com/ProductDetail/?pid=000000000030125022

2.3.1 Risk Perceptions: Customers' Cloud Concerns

In this section we will analyse cloud computing risks and trust from a customers' perspective. In the following, we will focus on the perception of a) business cloud customers and b) individual cloud users on risks. It appears that both type of cloud customers see the (potential) benefits of cloud computing, but also have concerns with cloud computing. Whereas the business cloud customers concerns encompass both technical and perceived risks, the individual cloud customers' concerns mainly relate to perceived and/or emotional risks. This reiterates the necessity of a socio-economic perspective on cloud computing as well as the concerns stakeholders might have. Not only uncertainty of the technology itself is commented upon in the perceptions described below, but also economic and societal concerns.

In general, business cloud customers mainly see the benefits of cloud computing (it offers scalability of resources and subsequently cost reduction) and focus less on the risks. Nevertheless, research on cloud adoption demonstrates that the risks of using cloud-services, according to business cloud customers in general are: a) policy and organizational risks, b) technical risks, c) legal risks, and d) non-cloud specific but infrastructural risks(Lin & Chen, 2012). Policy and organizational risks refer to, for example, vendor and data-lock in and loss of governance. Technical concerns relate to, for example, the loss of data due to misuse of cloud services by other users and identity verification and outsiders attacks due to multi-tenancy (Phaphoom, Oza, Wang, & Abrahamsson, 2012). The legal risks specifically focus upon the protection of data, for example, when jurisdictional boundaries are crossed. Infrastructural risks most often refer to the (lack of) availability of cloud services, and likely is one of the main perceived risks by business cloud customers. "Uncertainty of service availability and reliability, especially the concern over unexpected system downtime and disruption, could deter companies from adopting cloud computing because it increases project and business risk" (Lin & Chen, 2012, p. 534).

With regard to cloud security business cloud customers do not only have technical concerns (e.g. related to the underlying infrastructure and the security), but also have more emotional concerns e.g. trust and privacy issues (Savola, Juhola, & Uusitalo, 2010). Though scalability is the main benefit of cloud computing, business cloud customers perceive risks in lack of verifiable knowledge in the utilization of resources available (Phaphoom et al., 2012). Last, the cloud offers a business model that requires changing role and responsibilities within business customers' organizations. The latter includes the risk of resistance to change and is due to feelings of loss of control.

Importantly, Lin & Chen indicate that the categories of risks, the number of risks and the perception of their severity vary between most businesses (Lin & Chen, 2012). These variations in risk perceptions depend on the company's size, technological expertise and corporate culture of the businesses. Whereas SMEs and LEs both have business perspectives on the use of cloud services, their positioning might still differ. Smaller enterprises are likely less capable of negotiating contracts with cloud providers than bigger enterprises. Yet SMEs seem to adopt cloud computing quicker than large organizations. Moreover, there are differences between small and large companies as regards the ease of adoption (adoption simplicity) and the costs induced by the effort of implementing Cloud Computing services (adoption costs). Also, these characteristics imply that a learning effect can occur which affects marginal adoption costs (adoption costs).

Similar to business cloud customers, individual cloud customers (or the population at large) mainly see the benefits of cloud computing and are only to some extend aware of related risks. However, individual cloud customers' and/or end-users' perceptions of risk seem more related to the ability to control one's information in the cloud and transparency rather than related to e.g. technical risks as identified by business cloud customers. (Sjoberg & Fromm, 2001) demonstrate that risks of on-line service use are above all ethical and legal risks and concerns issues such as personal integrity, privacy and freedom of speech.

Moreover, individual cloud customers' risk perceptions are often related to their understandings of the Cloud. Research by Marshal & Tang (2012) on File Synch and sharing in the Cloud for example shows that cloud users' uncertainty and misconceptions limited their ability to fully take advantage of the service's features. Users needed more accurate and robust models to be able to discover and trust cloud computing services" (Marshall & Tang, 2012). It is reasonable to assume that cloud customers' lack of knowledge and understanding of cloud computing influences their risk perception.

2.3.2 Risk Assessments in Cloud Computing

Governing innovation, in a modern technological culture in which the existence of uncertainty of scientific knowledge and related societal problems are key characteristics, requires a thorough understanding of the risks that come with innovation (Beck, 1992). Cloud computing is such an innovation in need of responsible governance. The cloud's complex and opaque nature (e.g. the relation between data-subjects, data-controllers and data-processors is unclear) and its inherent technological, cross-border and dynamic character raise problems for its responsible governance. Subsequently, identifying what uncertainties exist, and what the (potential) risks are, has become core business in the analysis and assessment of innovations. Whereas cost-benefit analysis and other positivist sciences seem to dominate the risk assessment landscape, societal and other values have less room for informing regulators in the responsible governance of science and technologies. Yet, increasingly it is recognized that social, ethical and economic impacts have an important role in the assessment of science and technology. The A4Cloud project recognizes that the concerns with cloud computing not only relate to the uncertainty of the technology itself, but also to its ethical, economic and societal impacts.

Taking this wider socio-economic approach to risks and governing innovation entails that risk assessment should not only produce the best estimate of the harm that a threat may induce but should be complemented with a concern assessment. This concern assessment will identify and analyze issues that individuals or society as a whole link to a certain risk. Whereas for the first purpose classical risk modeling will suffice, the latter requires a more social scientific approach such as survey methods and macro-economic modeling (Renn, Klinke, & Asselt, 2011). Many risks cannot be calculated on the basis of probability and effects alone. The latter approach provides the opportunity to focus more on possible socio-economic and ethical implications of cloud computing.

Socio-economic implications refer to how the social behavior of (potential) cloud customers will affect their choice to make use of cloud services and vice versa how economic activity in the cloud (e.g. responsible stewardship) affects the social processes of cloud customers. In specific, we are interested in the social economic impact of shifting roles, responsibilities and risks due to the use of cloud services by the different cloud customers.

2.3.3 Preliminary Analysis on Stakeholders' Risk Perception

Based upon the findings in section 2.3.1 we can indicate that from a socio-economic cloud customer perspective, relevant factors or concepts that belong in a risk model are:

a) policy and organizational risks
    i. vendor- and data-lock in
    ii. loss of governance
b) technical risks
    i. loss of data
    ii. security
        i. outsiders attack
    iii. non-cloud specific / infrastructural risks
        i. (lack of) cloud services' availability
c) legal/ethical risks
    i. data protection
    ii. privacy concerns
    iii. freedom of speech
d) emotional risks
    i. trust concerns
    ii. lack of knowledge in the utilization of resources available
    iii. users' understanding of the cloud
    iv. feelings of loss of control
    v. privacy concerns

vi. resistance to change
vii. ability to control one's information
viii. personal integrity

3 Perspectives and Related Work on Trust and Reputation Models

There are multiple perspectives on the notion of 'trust'. In this section we will highlight two complementary perspectives; the computer science approach and the social science approach. Whereas the latter aims to understand the social relationships between cloud service providers and cloud service users and how risk and trust shape such relationship, the former approach focuses on reputation, an important element in this social relationship, and how this can be modelled.

From the discussion in Section 2, we can point out some deficiencies in existing risk management methodologies when applied to cloud ecosystems: a) there is no adequate methodology to analyse risks; b) it is difficult to allocate liabilities according to the roles an actor plays in the cloud service supply chain; c) to assess risks according to different service and deployment models; d) low visibility of the overall risk landscape and how controls are implemented across the supply chain. Moreover, it is fundamental to determine how trust influences risk perception and to create mechanisms to evaluate CSP reputation. In addition to the description of the notion of trust, we present in this section a review of the state of the art regarding trust and reputation models.

Finally, the socio-economic perspective on risks and risk perceptions provided in Chapter 2 demonstrates that an understanding of how the increased demand for giving account, e.g. in the form of risk assessments, is shaped by the notion of risk. Below we will discuss how risk (perception) and trust are related. This is important since trust in the Cloud greatly influences the adoption of cloud services, and might cause shifts in the cloud market.

3.1 The Notion of Trust

The concept of trust in Computer Science derives from the concept in sociological, psychological and economical environments. The definition of trust is not unique. It may vary depending on the context and the purpose where it is going to be used. Despite that the notion of trust is of paramount importance when considering systems security, a standard definition of trust has not been provided yet. (Fulmer & Gelfand, 2012) and (Castelfranchi & Falcone, 2010) provide a comprehensive overview of various definitions of trust in the literature. For example, (Gambetta, 1988) defines *trust* as:

> *Trust is the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends.*

(Mayer, Davis, & Schoorman, 1995) define trust as:

> *The willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party.*

(Castelfranchi & Falcone, 2010) define trust as:

> *Trust is a mental attitude, an attitude of an agent X towards another agent Y about the behavior/action α relevant for complex the result g.*

These definitions stress 3 main aspects of trust:

- Belief component: a mental attitude
- Decisional component: a decision to rely upon the other
- Behavioural component: an intentional act of trusting

The origins of computational trust date back to the nineties, when Marsh (Marsh, S. P, 1994) analysed social and psychological factors that have an influence on trust and replicated this concept in a computational setting. A few years later, Blaze (Blaze, Feigenbaum, & Lacy, 1996) identified trust management as a way to leverage and unify authentication and access control in distributed settings. These two early contributions show that trust can be conceived in different ways and for different purposes. From these seminal works onwards, different types of trust models have been proposed, with different purposes and targeting different settings. (Castelfranchi & Falcone, 2010) outline the following components that a trust model should ideally contain:

- beliefs about the trustee's internal attitudes and future conduct
- the subjective propensity of the trustor to accept a given degree of uncertainty and of ignorance, and a given perceived amount of risk
- the trustor's decision to rely upon the action of another entity for the realization of a goal, and the expectations upon which such a decision is based
- the relationships of dependence and power between the trustor and the trustee with respect to the intended goal of the former

Trust models are very heterogeneous, which often leads to confusion as one might easily lose the most relevant concepts that underlie these trust models. This heterogeneity depends on many factors such as the trust definition they use or their application domain. We can establish a classification of them. This task is not straightforward and there are many ways to tackle it. We propose the following classification:

- Decision Models. Trust management has its origins in these models (Blaze et al., 1996). They aim to make more flexible access control decisions, simplifying the two-step authentication and authorization process into a one-step trust decision. Policy models and negotiation models fall into this category. They build on the notions of policies and credentials, restricting the access to resources by means of policies that specify which credentials are required to access them. TrustBuilder (Seamons et al., 2003) is the first representative implementation of them. Trust negotiation models add a protocol, called negotiation strategy, during which two entities perform a step-by-step, negotiation-driven exchange of credentials and policies until they decide whether to trust each other or not. This strategy allows protecting the privacy of the entities as policies and credentials are only revealed when required. A later work (A. J. Lee, Winslett, & Perano, 2009) supports the implementation of different trust negotiation models. Here the authors state that trust negotiation can use evidence types, which represent information about the negotiation process (e.g. certain steps of the negotiation were already accomplished) and have a purpose (e.g. optimization of the negotiation).
- Evaluation Models. These models are often referred to as computational trust, which has its origin in the work of Marsh (Marsh, 1994). Their intent is to evaluate the reliability (or other similar attribute) of an entity by measuring certain factors that have an influence on trust in the case of behaviour models, or by disseminating trust information along trust chains, as it is the case in propagation models. An important sub-type of the former are reputation models, in which entities use other entities' opinions about a given entity to evaluate their trust on the latter.

The definitions above do not fully capture all the dynamics of trust, such as the probabilities that the trustee will perform a particular action and will not engage in opportunistic behavior (Pearson, 2012). There are also hard and soft aspects of trust (Osterwalder, 2001; Singh & Morley, 2009; Yan Wang & Lin, 2008). Hard part of trust depends on the security measures, such as authentication and encryption, and soft trust is based on things like brand loyalty and reputation. In (Ko et al., 2011), the authors introduced not only security but also accountability and auditability as elements which impact user's trust in cloud computing, and can be listed among the hard aspects. In (Kandukuri, V., & Rakshit, 2009), Service Level Agreement (SLA) is identified as the only way that the accountability and auditability of a CSP is clarified, and therefore a CSP can make users trust them.

McKnight is one of the leading academics in exploring the relation trust and information technology (IT) (D. McKnight, Choudhury, & Kacmar, 2002; McKnight, 2005). With IT the object of trust might be another person, another institution or an IT service. "Trust in information technology (IT) is an important concept because people today rely on IT more than ever before" (McKnight, 2005). Trust in IT has to do with relying or depending on infrastructure systems like the Web or relying on specific information systems. This trust in IT, according to McKnight (2005), is very similar to trust in people and reflects: a) trusting beliefs; you can believe both IT and a person to have favourable attributes, b) trusting intentions; you can be willing to depend on both an IT and/or a person and c) trusting behaviours; you can depend on

another person or on IT to do a task for you. Harder to ascribe to IT than to a person or an institution are the notions of benevolence and integrity (McKnight, 2005).

The adoption of cloud computing services by cloud customers is greatly affected by customers' trust in cloud computing. Trust in IT is a general assessment of the technology that probably affects other IT perceptions; the relative advantage or usefulness of a technology (McKnight, 2005). However, trust can be compromised. As long as technologies work, we seldom think of trust. When they don't, the trust question arises (D. McKnight et al., 2002). Trust may influence beliefs and attitudes affecting intentions to use a technology.

Therefore, building trust in IT can be regarded as an important strategic aspect in the relation between IT providers and IT customers. As the previous section demonstrated the perception of risks and uncertainty with respect to interacting with IT hinders the embracement of cloud computing. A lack of trust might make cloud customers hesitate to engage in behaviours necessary for the diffusion of IT such as cloud computing (D. McKnight et al., 2002). Improved trust, either enforced or intrinsically motivated, can positively affect e-commerce (Nemati & Van Dyke, 2009). Therefore, it is necessary to understand both the (perception of) risks and the nature and antecedents of customer trust in IT services like cloud computing.

Using McKnight's model it becomes possible to identify socio-economic factors of trust at different analytical layers (see also PRIME).

1. Socio-cultural defined trust;
    a. General propensity to trust
    b. General propensity to privacy
    c. General attitude to cloud / e-commerce
    d. General attitude towards (e)government
    e. User characteristics
2. Institution based trust; trust in the situation or structures
    a. Structural assurance via:
        i. Legal system
        ii. Institutions
        iii. Type of judicial system
    b. Situational normality; the roles and setting are normal
3. Trusting beliefs, trust in the service area / concrete area
    a. Competence, the belief that the trustee has the ability or power to do for one what needs to be done. E.g. trust in the level of service maturity in the sector.
    b. Benevolence, the belief the trustee cares and will act in the trustor's interest.
    c. Predictability, the belief that the trustee's actions (good or bad) are consistent enough that one can forecast them. E.g. trust based upon the reputation of the industry/sector.
    d. Integrity, the belief that the trustee makes good faith agreements, tells the truth and fulfils promises.
4. Trusting intentions; one is willing to depend, or intends to depend, on the other party with a feeling of relative security in spite of lack of control over that party and even though negative consequences are possible. E.g. trust in the media used in the particular application (e.g. mobile device, the Internet), and the user's attitude with respect to this medium.
    a. Trust in IT & Internet
    b. Trust in specific medium
5. Trust related behaviour, the voluntarily dependence on another person with a feeling of relative security and the acceptance of risk.
    a. Cooperation; e.g. prisoner dilemma situation
    b. Information sharing; e.g. transacting business
    c. Informal agreement; no benefit of legal contract enforcement thus relying on the reputation of specific service provider

d. Reducing the controls, e.g. service risk
e. Accepting Influence; depend on the other's opinion to be correct
f. Granting autonomy; depend on the other to make the right decisions; e.g. with respect to service benefit

We elaborate on these dynamics and the relations of trust with notions like confidence, control and reputation in the following section.

3.2 Trust, Confidence and Control

Cofta (Cofta, 2007) provides a comprehensive general trust and control model that covers many aspects of trust. In terms of the above classification this is more an evaluation model backed by a formal semantics. Figure 6 illustrates the schematic relationships between the concepts of trust, confidence, accountability and control. The central concept in the model is confidence that is built upon assessing trust and control, and confidence is defined as one's subjective probability of expectation that a certain desired event will happen (or that the undesired one will not happen), if the course of action is believed to depend on another agent. Trust and control are perceived complementary. According to the model, trust is in fact a deficiency of control that expresses itself as a desire to progress despite the inability to control. The interesting point, shared with (Castelfranchi & Falcone, 2010) is that control effectively inhibits trust.

Figure 7 illustrates how the level of confidence is derived from trust-related inputs (evidence of trust, confidence in honesty of source) and control-related inputs (evidence of control, confidence in honesty of source, confidence in instrument of control).

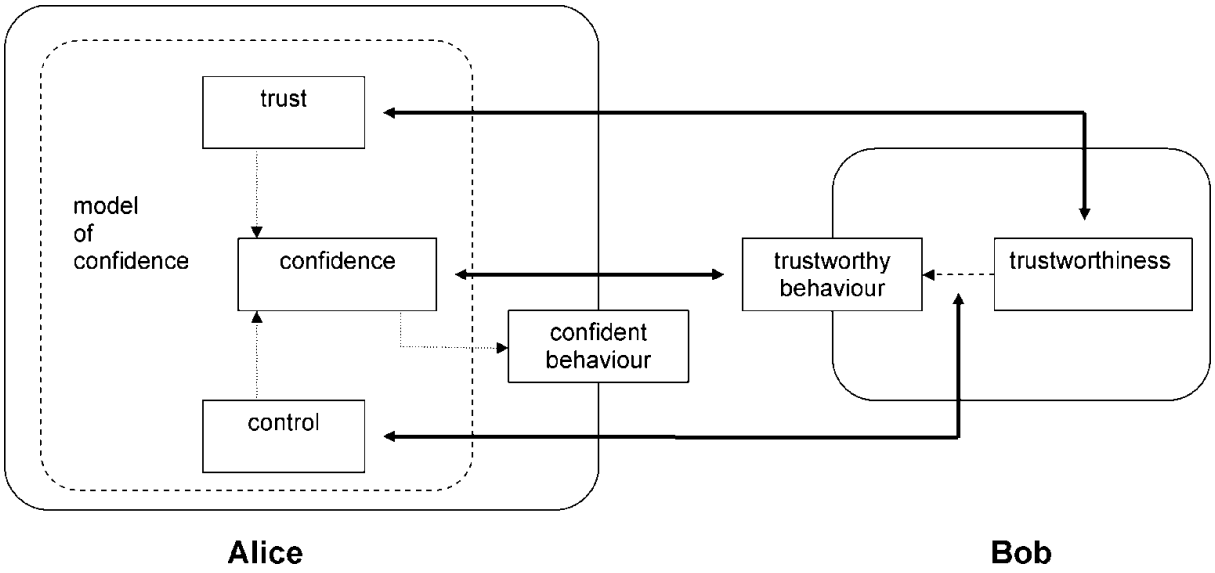

Figure 6 Cofta's trust model - basic concepts

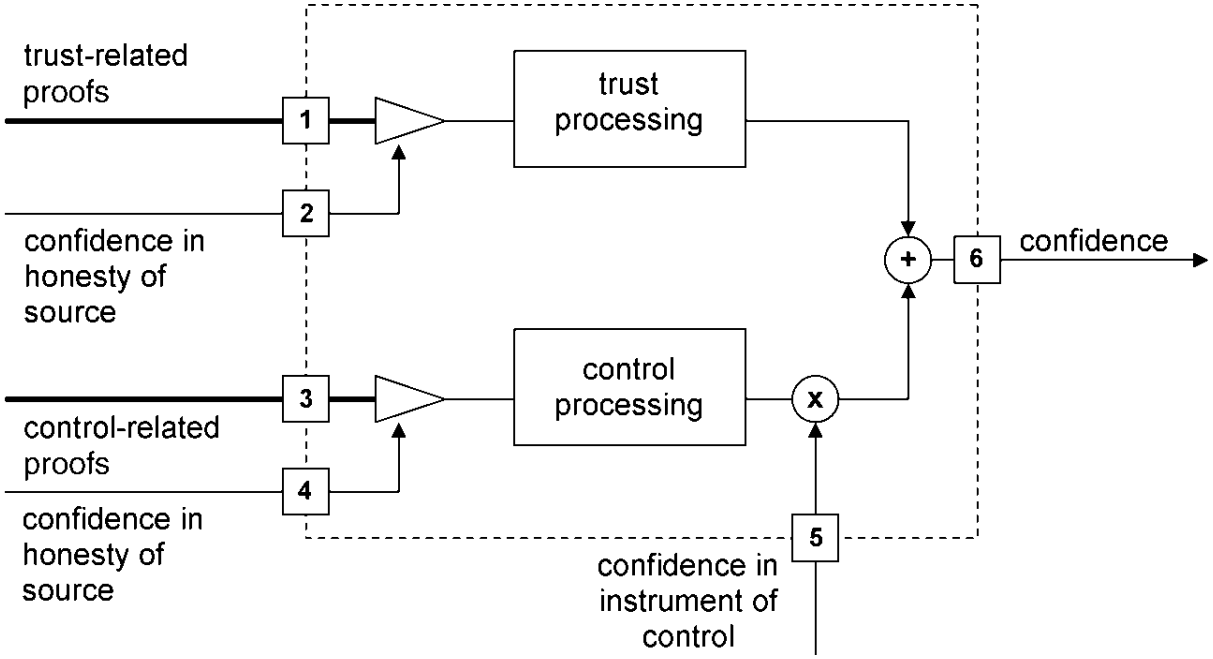

Figure 7 Cofta's trust model - basic building block

The author identifies three classes of evidence to trust: continuity, competence and motivation. Though during an assessment of trust in a CSP all these elements are important, in the course of A4Cloud we focus on competence the area on which the project is providing technical solutions.. An example of competence evidence is a certificate issued by a trusted third party, which attests certain competences of a CSP or its solution (SaaS, PaaS or IaaS).

Likewise the author identifies three classes of evidence to control: influence, knowledge and assurance. In the scope of A4Cloud we focus mostly on knowledge and assurance, because the project's methodologies and tools are targeting increased transparency (knowledge about CSP's implemented security controls and practices), and on the construction of assurance mechanisms.. An example of knowledge is the history of previous interactions: direct or through other parties. Reputation is an aggregation of this knowledge in the community. In this case the evidence is received indirectly through the reputation center. Relevant evidence that fits into the knowledge class is audit trails collected in the cloud infrastructure by auditors. An example of assurance evidence is the use of a legal system (expectation of redress) to enforce a contract.

A4CLOUD aims to build effective controls through technical and legal accountability mechanisms – to ensure confidence in CSPs regarding their provided services. A4CLOUD is also concerned to a lesser extent with building trust relationships, which are impossible to control (enforce) by definition. The governing mechanisms of 'trust' and 'control' can be perceived as compensatory. This means that sometimes trust will emerge from controlling activities, sometimes trust will lead to lesser need for control, and sometimes conversely more control is needed when trust is low. Governing via trust (building) refers to two distinct mechanisms; one a more intuitive regarding the CSP's intentions, and second a more cognitive regarding the CSP competence. Offering transparency with regard to the security and privacy of cloud customers' data in the cloud based on demand by cloud customers' can be regarded as a more intuitive form of trust building (responsiveness). However, in innovative businesses as cloud computing, imposing control is another way of dealing with (relational) risks. Risk analysis and risk assessments of cloud providers' services (stewards) will facilitate cloud customers with such control mechanisms. Especially when these risk assessments can be held against the cloud customers' risk profiles. In other words, the expectations of proper behaviour (trust) are enforced via control and not on the intrinsic motives of ethical conduct by the steward.

3.3 Trust and Reputation

Trust can be derived primarily from the reputation of the parties in the system. For example, a Primary Service Provider (PSP) could consult a database containing reputation values and reviews from other cloud consumers when to assess the trust level for a particular Cloud Service Provider (CSP). As the trust is usually context dependent (one may trust another for something and not for another), reputation systems that value several aspects of CSPs performance are valuable (e.g. eBay detailed seller rating). The reputation values may be both objective and subjective (as compared to the trust values that are intrinsically subjective). Examples of objective values are the number of positive interactions with the CSP vs. the number of negative interactions.

In our society, trust is a subjective belief about someone (or something) based on the expectation of their reliability and integrity. The trustor expresses a level of dependency and expectation of performance irrespective of the future implications (or risks). It is used as a strategy to deal with unpredictable future interactions. Reputation represents a collective belief (or opinion) about a particular characteristic of someone that is usually based on what has happened in the past. It is concerned with the formation and circulation of social evaluations and functions as a method to enforce some kind of social control, to reduce uncertainties, and to avoid dangerous partnerships. Reputation promotes good behaviour by regulating social collaboration and coalition formation; it also enforces social control through fear of sanctioning.

Trust systems attempt to create an environment in which two unrelated parties (i.e. strangers) can establish sufficient trust to interact together. *Trust management mechanisms* are used to establish trust using a collection of evidence and contracts. They address both structured and unstructured communities. One way to establish trust is through the enforcement of institutional policies, contracts, and credential negotiation. When these formal mechanisms are not available, rating and reputation mechanisms are used to establish trust. The goal of reputation mechanisms is to help lower the risks of online interactions, thereby increasing the robustness and efficiency of internet-based applications. Reputation mechanisms are then used in finding experts, selecting compatible partners or service providers, and locating reliable recommendations and opinions.

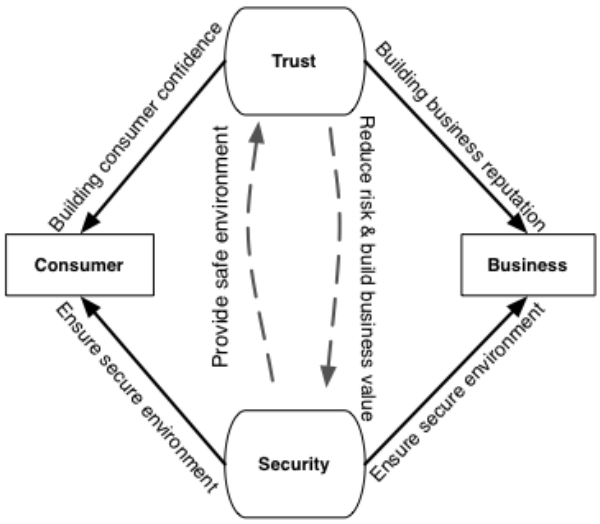

Figure 8 Security and Trust in Computer and Business Context (Chang, 2006)

In (Chang, 2006) the authors differentiate between trust in the computing paradigm and in the business one. They consider "trusted computing" as "trust in security context", which is related to security issues, security mechanisms, security technology, and security services. Trust in the business paradigm (the trust between the customer and the business provider) is a specially tailored trust for ensuring honest

dealings and quality of products or services, and it is usually related to mutual agreements and understandings, see the representation in Figure 8. The distinction corresponds to two categories of trust management: one includes security measures (policy-based) and soft trust relationships (reputation-based). In policy-based frameworks, trust is established gradually by disclosing credentials and requests for credentials, in an iterative process (credential-based approach). The process is known as trust negotiation. In (Squicciarini, Bertino, Ferrari, Paci, & Thuraisingham, 2007) reputation-based approaches depend on the user's local experiences and feedback to create a soft measure for trust decision. They use various clues and past experience to decide on taking the risk of dealing with an entity. Incentives to good behaviour are used in the form of enhancing one's reputation. Sanctions are used to punish trust violations in the form of decreasing one's reputation (which can have other consequences).

However, the relationship between trust and reputation can be seen in a broader way. Trustor and trustee establish a certain relationship, which might be used for the trustor in order to determine the trust placed on the trustee. The way this is done is through a *trust mode*l. Basically, what a trust model does is to transform information into a trust value (this may include a trust matrix or a complex trust object) for the trust relationship. The information that the trust model takes into account may depend on many factors that may include trustor's and trustee's objective and subjective factors.

As for the case of reputation, many (probably anonymous) users rate (i.e. issue claims about) other users based on their personal experience, and probably, personal trust. Technically, reputation does not necessarily create a trust relationship. It basically computes a score, which may help a user to make a trust decision. A reputation engine determines how the score is computed and how it is made accessible to other users.

In the last stage, reputation can be used as one of the sources of information that allows the trustor to determine the level of trust, but reputation itself could have been based on a huge amount of anonymous trust relationships. This explains the bidirectional relationship between trust and reputation at the conceptual level. Yet, it should be taken into account that this relationship is not always executed and trust and reputation models can exist independently. Figure 9 tries to explain this relationship in a graphical way. Reputation can be seen as a building block for trust, whereas claims (building blocks of reputation models) issued by (probably anonymous) users can be based on the relationships established between the trustor and the trustee.

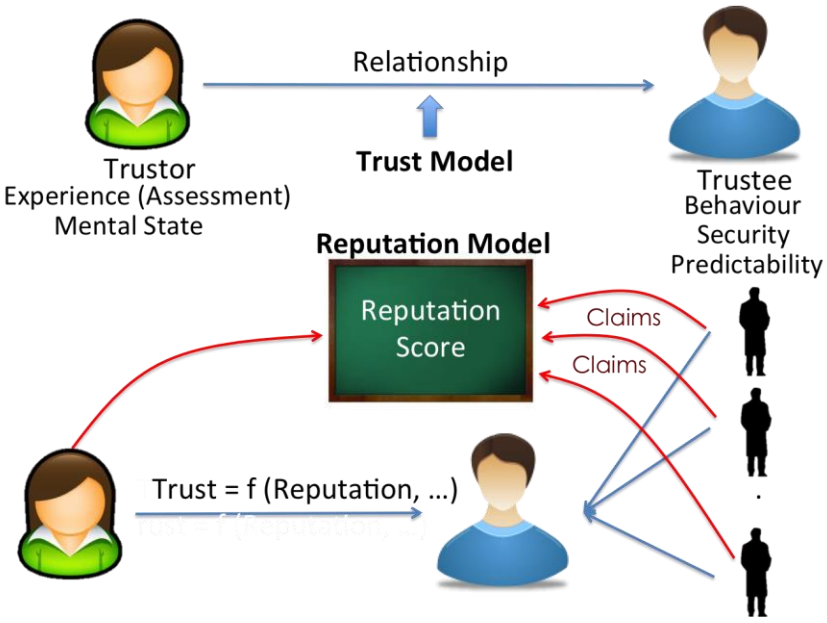

Figure 9 Relationship between Trust and Reputation

In a distributed environment, reputation is divided into *global* and *personalized* categories. A *global reputation* is derived by the underlying network, visible by all agents in it, and based on the opinion of

the general population. A *personalized reputation* is the agent's reputation in the eyes of the others, which is relative to the embedded network. An individual's reputation comes from direct encounters with others or from inference based on propagated information through the network (indirect reputation). Reputation systems and frameworks provide methods to establish trust by encouraging the participants to provide feedback about each other's trustworthiness and estimating the future behaviour based on these feedbacks. They minimize the *risks* involved in trusting a participant by sharing knowledge about the participants' experience as well as by expecting sanctioning and reciprocity. Holding an entity accountable to their actions helps to enforce reputation sanctioning. Having a system that ensures accountability helps increasing trust within the network.

(Resnick, Kuwabara, Zeckhauser, & Friedman, 2000) defines a reputation system as: *"a system that collects, distributes, and aggregates feedback about participants' past behaviour"*. A reputation system should describe:

- Computation functions/mechanisms, i.e. how to calculate reputation?
- Communication model, i.e. how to collect and disseminate reputation?
- Participants, i.e. who uses and/or is affected by reputation?
- Resources, i.e. what is the information used to calculate reputation?
- Representation model, i.e. how to represent, view, or visualize reputation?
- Storage, i.e. where and how is reputation stored?
- Functionalities and applications, i.e. what are the benefits of using reputation in the domain of its creation?

Reputation systems can be generally categorized as *centralized (*a central authority is dedicated to collect, process, and emit reputation values*)* and *decentralized (*Reputation is either kept in distributed stores or kept as an own personal opinion which is provided on request*)* based on the network architecture or protocol, see Figure 10. ENISA defined a set of security requirements for a reputation system such as integrity, availability, accountability, efficiency, usability, and trustworthiness.

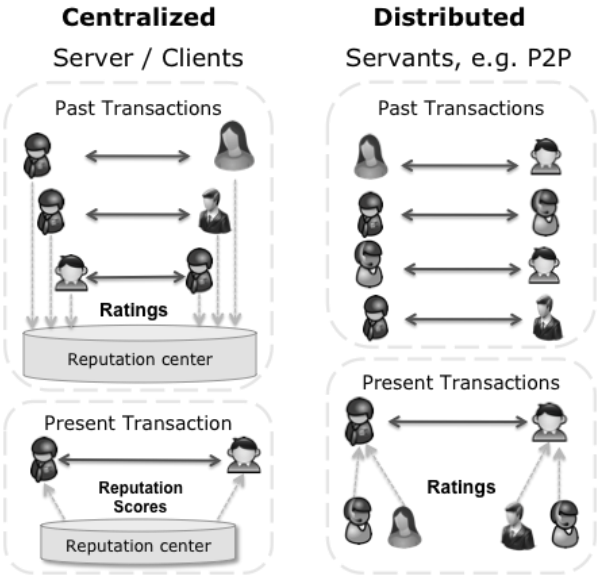

Figure 10 Reputation Network Architectures

Reputation in e-markets is an instrument for trusted partner or service provider selection. In a multi-agent environment a computational trust and reputation model has to deal with three types of information sources (Sabater-Mir & Paolucci, 2007) *direct information*, which is information that comes from direct experience with another agent without intermediaries; *third-party information*, which is information

obtained from a third party or an informant, and *meta information* which is the knowledge resulting from different analysis of the two other types of information sources. In online reputation communities, trust and reputation (or rating) are represented numerically or graphically using bars and stars, karma, or in natural language from a finite set of possibilities (i.e. *good* vs. *bad*), or from an infinite set of possibilities (i.e. textual comments). The computation engine used in each online reputation system is different such as aggregation and Bayesian models. In their book (Farmer & Glass, 2010) Farmer and Glass, elaborated on the types of reputation systems and their patterns that exist in current successful online systems, however it is beyond the scope of this document.

In an open environment such as service-oriented architectures and cloud environment, reputation is used in service selection and the selection of trusted transaction partners. In such environments, services from different service providers can offer the same functionality, and given the scale of SOA and cloud systems, service selection became a challenge. Since the services provide the same functionality, the consumer has to factor some other non-functional properties in his decision-making. He considers the quality of the service itself, its availability and reliability, and how well he can trust the provider. This information is usually kept as QoS metrics that are either associated with the service description or separately in the service registry. Usually, a service consumer may trust that a service offered by a provider with a good reputation will be a good service. In (Y. Liu, Ngu, & Zeng, 2004) the service provider can be bound to the QoS by an agreement formed during the negotiation phase: a service level agreement (SLA). Reputation can also be produced using client side monitoring techniques to generate information regarding functional and non-functional quality of service (Bianculli, Binder, Drago, & Ghezzi, 2008; Yao Wang & Vassileva, 2007).

The works in (Banaei-Kashani, Chen, & Shahabi, 2004; Vu, Hauswirth, & Aberer, 2006) propose several P2P trust models to avoid having one central node to collect and process QoS data and disseminate reputation information in a cloud or SOA environment. The idea is that some service registries or cloud brokers are distributed in the network and are collecting QoS feedback from consumers. QoS metrics used in getting reputation information are defined in (Yao Wang & Vassileva, 2007) and (K. Lee, Jeon, Lee, Jeong, & Park, 2003).

In summary, reputation systems:

- enable customized trusted partner or service provider discovery and selection
- aid in quality assessment processes
- discourage opportunistic behaviour that leads to bad behaviour
- are used as a dynamic factor in risk assessments to reduce uncertainties and mitigate risks in environments such as internet of services
- solve large-scale collaboration problems such as resource allocation in cloud computing environment

3.3.1 Trust and Reputation Metrics

An important aspect of trust is how it is evaluated by the trustor. A trust metric is a measurement of the degree to which one entity trusts another which is based on an expectation on the future behaviour. Trust values are usually derived based on entity's reputation, hence there is a related notion of reputation metrics. Many trust and reputation metrics with various semantics have been proposed in the literature, some of which are described in MS:C-5.1. Some of the authors mix these concepts, however we should distinguish a measure of trust, that is specific for a given individual and a measure of reputation which is usually global for the system. In our work we assume that reputation is just one of the attributes used to infer trust values for a particular entity.

Another attribute contributing to the trust perception is the history of past experiences (positive vs. negative). An evaluation of such history could be represented in the simplest form as a tuple $\langle p|n\rangle$, where p is the number of positive interactions and n is the number of negative interactions. Given these values the overall trust values can be computer simply as $p - n$, as in eBay feedback rating $\frac{p}{p+n}$ or using

statistical approaches as in beta reputation system(Jsang & Ismail, 2002) as $\frac{p-n}{p+n+2}$. In the cloud ecosystem this approaches however seem too simplistic as these values represent an aggregate over many implicit subjective factors. Indeed, a positive interaction does not specify what concrete aspect of an entity is evaluated. A trust metric for the cloud should likely consider different aspects for evaluation, for instance the performance of a CSP regarding providing security to personal data, providing audit logs on demand or other evidence of conformance, allowing customization of service contracts and facilitating the procedure of exit and transition to another CSP. The eBay detailed seller rating provides a simple example of such approach.

If, however, the experience with an entity is not direct, but by a third party the trust in that third party should be considered also for deriving impact on the trust level. For instance EigenTrust algorithm (Kamvar, Schlosser, & Garcia-Molina, 2003) proposes to weight the response from other peers by the trust values that are placed on them by simple multiplication[21] $t_{ik} = \sum_j c_{ij} c_{ik}$. In this approach the authors use a trust graph representation and assume that the transitivity property holds (transitivity is discussed in more detail below). Trust graphs are very common for representing trust relationships (used e.g. in PageRank, PGP) and could potentially be used also in the cloud scenarios, e.g. to describe the trust relationships between CSPs. This is supported by the fact that service supply chains in the cloud are becoming complex involving many entities (contactors, subcontractors, brokers).

3.3.2 Transitivity of Trust

A desired property of a trust model is the transitivity. As applied to the cloud ecosystem, this leads to the question: if a Primary Service Provider (PSP) trusts a CSP A which subcontracts (and hence trusts) another CSP B, can the PSP trust CSP B? This question is very relevant considering that the PSP when playing the role of data controller is responsible for data protection along the whole processing chain. In the A4Cloud approach we postulate that trust should be built on accountability and more precisely on accountability claims and evidence that those claims are satisfied. In this case if CSP A trusts CSP B then CSP B should have provided some evidence of his trustworthiness. So for PSP to trust CSP B and any other subcontractors this evidence should be either forwarded to PSP or CSP A should provide evidence that he is effectively verifying the subcontractors' compliance.

The situation is complicated by the fact that often PSPs do not know all the actors that participate in the service delivery chain. In this case PSP cannot explicitly trust CSP B.

3.3.3 Trust Models for Cloud Computing

The idea of using trust and reputation in order to leverage cloud security can be found in several works. Usually, trust and reputation are used to help cloud stakeholders to make a decision about other stakeholders and services they have to interact with. For instance, (Habib, Ries, & Muhlhauser, 2010) explore how these concepts can support consumers in selecting trustworthy cloud providers. Reputation-based trust models have been considered lately. Liman and Boutaba (Limam & Boutaba, 2010) propose a reputation system in order to improve the process of selecting external services for integration in development projects. A similar goal is pursued by Abawajy (Abawajy, 2009), who suggests using a trust-based reputation system to determine service trustworthiness in intercloud computing environments. The work in (Pawar, Rajarajan, Dimitrakos, & Zisman, 2013) introduces a trust model for cloud based on cloud characteristics as defined by NIST. Trust is defined in the form of reliability and reputation.

(Cerbo et al., 2012) proposes the concept of a trustworthy service marketplace where the security features of the services (SaaS) are certified and represented in a machine-readable format. This would enable marketplace users to quarry for services satisfying specific security requirements. The authors do not propose a trust model per se, but rather a solution for gathering and sharing evidence regarding the trustworthiness of particular services (as opposed to the trustworthiness of the service providers). If

[21] Although the authors present this as an algorithm computing trust values, given our considerations above it is rather a reputation system.

a certificate contains an assert statement backing a particular security aspect of the service, this service could be considered trustworthy in the context of the given security feature. In the risk assessments we consider certificates as an evidence of trust, but also take into account other factors (previous experiences, accountability mechanisms and tools).

In (Rashidi & Movahhedinia, 2012), the user trust to a CSP is related to the following parameters:

- Data location: Users know where their data are actually located.
- Investigation: Users can investigate the status and location of their data.
- Data segregation: Data about each user are separated from the others.
- Availability: Users can access services and their data pervasively at any time.
- Privileged user access: The privileged users, such as system administrators, are trustworthy.
- Backup and recovery: CSP has mechanisms and capacity to recover from catastrophic failures and not susceptible for disasters.
- Regulatory compliance: CSP complies with security regulations, certified for them and open for audits.
- Long-term viability: CSP has been performing above the required standards for a long time.

The authors in (Rashidi & Movahhedinia, 2012) statistically analyze the results of a questionnaire answered by 72 cloud users to investigate the perception of the users on the importance of the above parameters. According to this analysis, backup and recovery produces strongest impact on user's trust in cloud computing followed by availability, privileged user access, regulatory compliance, long-term viability and data location. Their survey showed that data segregation and investigation have weak impact on user's trust on cloud computing.

Chief information officers perceives the barriers for cloud adoption (Pearson, 2012) as vendor lock-in (i.e., to be dependent on a vendor), cloud performance and availability, security and challenges in integrating internal and external services. According to another survey among 264 non information technology executives (non-IT) and 462 information technology executives, the barriers are security, regulatory risks, business case, adapting business processes, interoperability, lack of awareness, adjusting policies and building skill sets (Pearson, 2012). These barriers are important in trust modelling because they are why the potential users trust or do not trust a CSP.

3.3.4 The Relation between Trust and Risk

Chapter 2 has demonstrated that socio-economic risk factors predominantly refer to 'soft trust' and involve aspects such as intrinsic human emotions, perceptions and interactions. Moreover, the chapter provided insight in what the consequences might be for cloud computing ecosystems if cloud customers' risk perceptions are not addressed. In this chapter we have provided insight in what trust entails, how it relates to IT and to reputation, and how trust can be made measurable. Importantly, risk and trust are intrinsically linked. Trust is positively related to the perceived risks present in a situation. "This means that an increase in risk perceptions could result in the augmentation of people's degree of trust" (Beldad, 2011). For example, deficient software at one level may hurt perceptions at several levels. Previous research with regard to privacy and online behaviour demonstrates that many customers do not trust most Web providers enough to exchange personal information in online relationships with them (Leenes & Oomen, 2009). Moreover, the public's perceptions of having little control over information privacy on the Internet have a strong influence on the customer's willingness to engage in relationship exchanges online (Beldad, 2011; Hoffman, Novak, & Peralta, 1999; Olivero & Lunt, 2004). Therefore, it is a reasonable assumption that improved trust in cloud computing in general, and specifically in cloud service providers can positively affect cloud business. "In particular, an increased level of trust improves disclosure, reduces the demand for legislation, and reduces perceived risk" (Kaliski,Jr. & Pauley, 2010, p. 2). Although the mechanisms of 'trust' and 'control' can be perceived as compensatory, trust will emerge from controlling activities and v.v. sometimes trust will lead to lesser need for control, this WP will be mostly interested in providing confidence by (accountability) controls and the trust will be secondary, even though still important for risk assessment.

4 Risk Mitigation and Cloud Contracts - A Legal Perspective on Risks

Under the cloud-computing paradigm, a cloud customer (e.g. a small medium enterprise or an individual) relinquishes direct control over many aspects of data security and data protection to the primary cloud service provider. Key aspects of cloud computing, such as shared off-premise infrastructure between organizations and rapid technological innovations, raise complex privacy and security issues due to the particularities of the technology per se allowing for the international data flows and the remote processing of data. Consequently, in this sense, data protection and security issues raised by cloud computing can be conceptualized as risks in the sense of the harm which results, for example, from unauthorized access, use, disclosure, disruption, modification or destruction of personal data. Typically, cloud computing services are offered by the primary cloud service provider to the cloud customer under the terms of standard form contracts. Such standard form contracts are drafted on the terms of the primary cloud service providers, are not negotiated -in most cases- by the cloud customers, and may not cover all data protection and security issues raised in the context of the cloud computing technology. Given the lack, though, of a uniform approach at European level regarding business sensitive information, the section below will focus on the processing of personal data as provided under the Directive 95/46 "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (hereafter: "Data Protection Directive").This analysis is instructive as it sheds lights on how specific risks, such as security risks, can be allocated or mitigated in cloud computing through contracts.

4.1 Data Controllers and Data Processors

From a legal perspective it is important to determine whether the cloud provider is acting as a 'data controller' or a 'data processor' as this places different data protection and security obligations on the cloud provider. According to Article 2 of the Data Protection Directive, "a data controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of processing of personal data". Moreover, Article 2 defines data processor as the "natural or legal person who processes data on behalf of the data controller." In cloud computing the allocation of responsibilities to the entities taking part in the processing is linked, of course, to the particularities of the technology itself.

> *With respect to cloud computing, characterization of an entity as a controller or a processor may depend on the type of cloud computing system that is used or on the technical setup of the system. This characterization will determine the liability of the respective parties for compliance with data protection obligations. Further, and perhaps more significantly, a controller remains responsible for discharging data protection obligations even where the data has been outsourced or transferred to a third party—including a cloud vendor—for processing. It is therefore important for a company to undertake a rigorous assessment of its responsibility for the personal data processed by the cloud provider and, if applicable, enter into a data processing agreement requiring the cloud provider to act only according to the company's instructions, to ensure adequate technical and organizational security and otherwise to comply with legal requirements* (Sotto, Treacy, & McLellan, 2010).

Within cloud ecosystems, cloud customers might fulfill both roles, being data controllers or data processors, depending on the actual circumstances. It should be noted that the term "cloud customer" might refer either to individuals or companies[22]. However, taking into account that cloud customers are mostly companies, this section focuses mainly upon cloud computing and SMEs.

[22] See, also, Cnil "Recommendations for companies planning to use Cloud computing services" http://www.cnil.fr/fileadmin/documents/en/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf

4.2 Contracts and SLA's

Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Since cloud customers usually lack control of cloud resources, they are not in a good position to utilize technical mechanisms in order to protect their data against unauthorized access or secondary usage or other forms of misuse. Instead, they must rely on contracts as a trust mechanism aiming to ensure appropriate usage, in combination with mechanisms that provide compensation in the event of a breach, such as insurance, court action, or penalties for breach of service level agreements (SLA's).

Usually, the contract between the cloud customer and cloud provider is a standard form contract, such as a Click Wrap Contracts[23] which often draw on traditional outsourcing or technology licensing models and may not always cover the specific data protection and security issues raised by cloud computing. Cloud customers often rely on brand perception or the perception that such and such cloud providers can be trusted when choosing a cloud service or technology. Such brand perception is invariably linked to the data protection and security standards and policies which are adopted by the cloud provider. However, such perceptions of trust are very fragile in cloud computing due to the key features of cloud computing, such as the often invisible cloud provider supply chain. However, the move to an age of third-party audit in cloud computing, currently proposed in the reform of the European data protection law, may offer a middle ground position[24]. By this we mean that third-party audits, such as data security audits, could be conducted to evaluate the compliance of cloud providers with their data protection and security obligations.

4.3 Regulatory Risks

The section below discusses how data protection and security issues are addressed under the Data Protection Directive. This analysis is relevant to the current discussion as the provisions of the Data Protection Directive on data protection and security can often impact on risk allocation and mitigation in standard form cloud computing contracts between primary cloud service providers and cloud customers.

4.3.1 Data Security and Confidentiality

Under Article 17 of the Data Protection Directive, the 'data controller' is under an obligation to choose a processor who can "implement appropriate technical and organizational measures… sufficient guarantees in respect of the technical security measures and organizational measures governing the processing". Cloud computing raises complex data protection and security issues which are not always present in the traditional computing model. In a traditional computing model, one where applications reside on client machines or somewhere else on the infrastructure owned and controlled by the enterprise, it is possible to levy a host of counter measures to mitigate security risks.[25]However, if the application is moved to a cloud infrastructure provided by an outside provider, whose business model is typically driven by the provision of a common service to a wide variety of users, then the security of that data will be largely a function of the skill, willingness, diligence, and fiscal ability of the provider to protect the data and provide a reliable service.

Here, contractual agreements between the cloud provider and the cloud customer are vital in imposing

[23]Click Wrap Agreements are a type of standard form contract associated with software licensing. In practice, Click wrap agreements involve the end users indicating consent or rejection to the provider's terms and conditions on their screen. Usually the terms will be on a separate page, which is linked to the actual acceptance screen.

[24] Article 22 of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[25]Counter measures can include firewalls, data encryption, antivirus solutions, tight access permissions, separation of networks either virtually or physically etc. in addition to the use of the use of trusted administrators, trusted application developers, and internal processes.

data protection and security obligations on the cloud provider. By so doing, the contract mechanism establishes trust between the cloud provider and the cloud customer by allocating and mitigating the data protection and security risks.

In the cloud environment, this type of trust is both being put into question by the relative and perceived lack of maturity of the offered technology solutions, and strengthened by institutional structures such as well-devised formal contracts (i.e. Service Level Agreements). Potential users with limited or no experience of a particular service provider depend almost completely on the terms of the contract between the cloud provider and the cloud customer to protect their personal data.

In this context, transparency appears to serve a key role in achieving compliance with the security obligation aiming at ensuring that data is processed in a fair and legitimate manner. Transparency in the way the cloud provider operates, including the provisioning of composite services, is a vital ingredient for effective oversight over system security and privacy by an organization. To ensure that policy and procedures are being enforced throughout the system`s lifecycle, service arrangements should include some means for the organization to gain visibility into the security controls and processes employed by the cloud provider and their performance over time.

Related to data security are the notions of data integrity and availability. Many cloud providers include terms relating to redundant connectivity, fault tolerance, and automatic back up of data. However this does not necessarily mean that the cloud customer is safe from data loss and his/her data will remain intact. Cloud providers may take backups of user data, although they may not commit contractually to doing so and will not usually warrant data integrity, or accept liability for data loss. Moreover, according to the Data Protection Directive, data cannot be kept in an identifiable form for longer than necessary.[26] This creates a risk for cloud customers since personal data may be kept redundantly on different servers at different locations; it must be ensured that each instance of data is erased irremediably (i.e., previous versions, temporary files and even file fragments are to be deleted as well). The cloud customer should make sure that the cloud provider ensures secure erasure in the above-mentioned sense and that it contains clear provision for the erasure of personal data. The same holds true for contracts between cloud providers and subcontractors.

One example of ensuring transparency with respect to security of data processing is for the service agreement to include the right to audit controls via a third party, as a way to validate control aspects that are not otherwise accessible or assessable by the user. Pre-contractual audits, allow users to assess and ensure that providers have taken adequate security measures and that they have implemented security policies; post contractual audits are met with the same approach in standard form contracts.

However, from the cloud provider`s view, particularly with shared infrastructure and multi-tenancy, it can be detrimental to security and against their own security policies to provide full details of their security policies and practices to all prospective users, or allow data center visits (Hon, Millard, & Walden, 2012). This is especially evident in multi-tenant cloud agreements, where the cloud user will want to ensure that data is segregated to prevent personal data from being processed for illegitimate purposes.[27]

Another trend emerging in standard form contracts is the adoption of industry-accepted standards and linking cloud provider security policies to such standards. These can be seen as a compromise in agreements and an attempt to strengthen transparency and trust where audit rights are left out. Industry standards and certifications specific to cloud security have not been fully developed, although organizations like the Cloud Security Alliance, Open Data Centre Alliance and Cloud Industry forum are progressing matters. With so much contractual content being determined and set by the service provider’s, cloud customers would make sense to look towards a tool allowing them to compare their chosen cloud providers against an industry and or sector benchmark. Organizations which are developing standardization across cloud computing include the Green Grid, the Cloud Security Alliance (CSA), the Institute of Electrical and Electronics Engineers (IEEE) Standards Association, and the National Institute of Standards and Technology (NIST).

However there are still issues from a legal point of view influencing the level of trust towards cloud offered services. The first is that at present there is no industry wide set of standards or codes that the

[26] Data Protection Directive Article 6.e
[27] Article 6(b) of the Data Protection Directive.

user can rely upon. This again is down to the market being immature; cloud models themselves are developing so fast that many standards simply cannot keep up, and therefore, become obsolete too quickly. The result is a dilution of the overall impact of standardization itself as a tool to reduce and mitigate risks. Secondly, there is no consensus as to the content of any industry wide code – how can one define a secure cloud environment.

Confidentiality, on the other hand, in a general sense refers to the duty not to share information with persons who are not qualified to receive that information[28]. In a more specific sense, it refers to the confidentiality of communications provided for in Article 5 of the E-privacy Directive (2009/136/EC). Confidentiality of processing refers, also, to the obligation of any person acting under the authority of the controller or the processor who has access to personal data, not to process them except on instructions from the controller, unless he is required to do so by law (Article 16 of the Data Protection Directive). It is important to note, though, that terms relating to confidentiality obligations can result in liability for data breach, but since data loss or corruption may not involve confidentiality breaches these may not incur liability. In this context, specific warranties (with liability) in relation to data loss or corruption can be an important addition to the agreement. Contractual clauses should also impose, of course, confidentiality obligations on employees of cloud customers, primary service providers and sub-providers.

Note that Article 17 of the Data Protection Directive provides for the implementation of technical measures (e.g encryption, authorization mechanisms and strong encryption) aiming at ensuring the confidentiality –and integrity- of personal data being processed. In case data processors are involved in the processing, then they should implement the "appropriate security measures" depending on the risk presented and the nature of the personal data processed as if the processing was performed only by data controllers. However, even if a security breach has occurred, for instance, due to the adoption of "non-appropriate" security measures, data controllers are held liable towards data subjects. Subsequently, data processors will be liable towards data controllers on the basis of the contractual agreement, establishing their relationship.

1. Third Party Relationships

In the cloud context it is often the case that the cloud provider with whom an entity is contracting (the "Primary Provider") is not the cloud provider that will actually be processing, storing and transmitting the user's data (the "Third-Party Provider"). The classic example is the Software as a Service provider that hosts its software in an Infrastructure as a-Service cloud. In such scenarios, the breached third party provider may not have any contractual relationship with the cloud customer and the cloud customer may not have any rights when a data breach happens. Since the third party provider is once (or more) removed from the cloud customer, it may be difficult to even investigate the incident response capabilities of the downstream providers.

Moreover, even if the standard form contract between the Primary Provider and the cloud customer provides that the Primary Provider will undertake specific actions when a data breach occurs, the Primary Provider may not always be able to fulfill its contractual obligations if it has not obtained the necessary corresponding rights in its own contract with the Third-Party Provider. Additionally, conflict of interest problems and investigation access issues may exacerbate this problem further. As much as it may often be difficult for the Primary Provider to gain access to a third party provider when there is a contractual relationship between the parties, it is virtually impossible for the cloud customer to gain access to the necessary resources of the Third-Party Provider as the cloud customer has no contractual relation with the Third-Party Provider. If the third party provider is the cause of a data breach -or its failure to provide a service to the main service provider usually-, there will be a contractual relationship between the cloud service provider and the cloud customer on the one side and another contractual relationship in the form of a subcontract between the cloud service provider and the third party provider. In the relationship between the cloud provider and the cloud customer a failure of the third party provider would be regarded as a failure of the cloud provider with the consequence that the cloud provider would be liable to the cloud customer for any damages incurred.

The contract should examine the manner in which the Primary Provider may use Third Party Providers,

[28] https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/73#confidentiality

to outsource certain functions; the agreement should ensure they are bound to the same obligations as the cloud service provider. Cloud services that use third-party cloud providers to outsource or subcontract some of their services should raise concerns, including the scope of control over the third party, the responsibilities involved (e.g., policy and licensing arrangements), and the remedies and recourse available should problems occur. Trust is often not transitive, requiring that third-party arrangements are disclosed in advance of reaching an agreement with the cloud provider, and that the terms of these arrangements are maintained throughout the agreement or until sufficient notification can be given of any anticipated changes.

The contract can be used to limit a cloud provider's use of third parties to handle personal data. Terms can be added that prevent the cloud provider from providing data to a third party service provider without the cloud customer's prior permission. If third-party providers are to be used, the contract can impose an obligation on the service provider to engage in a due diligence investigation to ensure the third-party can satisfy the obligations agreed to by the direct provider. The cloud user can also demand contract terms requiring the cloud provider to impose contractual obligations on third-parties that are similar to those the direct provider agreed to, and which allow the direct provider to satisfy its own obligations. With the addition of these terms, the cloud user could have more control and a greater ability to respond to a data breach suffered by a third-party provider.

2. Data Location and Data Transfers

Closely related to the risk of sub-contractors in the cloud agreement service chain is the restriction imposed by the Directive on transferring personal data outside the European Economic Area.[29] Standard form contracts on the whole do not address this issue adequately. Nevertheless, users need to be informed about not only where the primary service provider's data centers are located, but also where the data centers of the sub-providers are located, provided that the user is informed, of course, in the first place that processing operations have been allocated to sub-processors.

Data transfers to the US are done under the Safe Harbor Transfers to US organizations adhering to the principles, which can take place lawfully under EU law since the recipient organizations are deemed to provide an adequate level of protection to the transferred data. In terms of data security, cloud computing raises several cloud-specific security risks, such as loss of governance, insecure or incomplete data deletion, insufficient audit trails or isolation failures, which are not sufficiently addressed by the existing Safe Harbor principles on data security. Additional safeguards for data security may thus be deployed by incorporating, for instance, the expertise and resources of third parties that are capable of assessing the adequacy of cloud providers through different auditing, standardization and certification schemes. It is, however, questionable whether Binding Corporate Rules reduce risk of personal data being transferred outside the European Economic Area or they, actually, increase risk simply because they allow for such transfers.

However, although standard form contracts usually include reference to Safe Harbor Agreement, many contracts do not directly make reference to transfers of data outside the European Economic Area. Even in negotiated contracts where the use of standard clauses and Binding Corporate Rules can be relied, this may not be enough. Exporting data should not merely rely on the statement of the data importer claiming that he has a Safe Harbor certification. On the contrary, the entity exporting data should obtain evidence that the Safe Harbor self-certifications exist and request evidence demonstrating that their principles are complied with.

4.4 Liability

Establishing data protection and security obligations between the parties is not enough on its own to increase trust towards cloud offered services. The agreement must contain clear terms relating to liability to ensure that the contract can effectively mitigate any risk involved in moving personal and confidential data to the cloud. As explained below, this is where current standard form contracts fail. Consequently, their value and effectiveness as a trust mechanism can be questioned as well.

The most important terms within contracts are those that establish which party is to bear the consequences of the loss if a service provider suffers a security breach. Where possible, cloud customers, particularly small and medium enterprises, should negotiate for contract terms that transfer the risk of loss to the cloud provider which suffers the security breach. This can come in the form of an indemnity clause that requires the cloud provider to indemnify the cloud customer for all claims and losses arising out of data security breach. Cloud customers will also want to look at and potentially try to modify limitation of liability clauses and consequential damages disclaimers. These clauses limit service provider liability for contract breach and cloud user may want to negotiate for unlimited liability for data breaches (or at least higher limits of liability for such breaches). The data breach-related duties, though, need to be carefully articulated in order to recover for a contract breach and the failure to have meaningful liability terms in a contract can limit the effectiveness of imposing such duties in the first instance.

Limitation of liability clauses simply set the cloud provider's monetary cap for loss or damages owed to the cloud customer under the contract. Most limits of liability purport to limit liability for any liability arising out of the services provided under the agreement, whether such liability arises out under relevant laws or under the contract. Significantly, even if a cloud customer is able to get favorable data protection and security terms from a cloud provider, they may only be able to recover up to the limitation clause should the provider breach those terms. Also important, cloud contracts may have exceptions to the limitation clause that allow the cloud customer to recover for certain types of losses, including for example, confidentiality breaches and indemnification-related losses.

Cloud service agreements generally only warrant that the service will conform to the service levels, or that the service will perform in accordance with certain specifications. Depending on the type of cloud transaction involved, cloud users should carefully review the warranties offered by the cloud provider such as warranties relating to performance and compliance with law etc. Cloud providers may provide certain warranties, but then typically desire to disclaim all other warranties and guarantees concerning their services. The reason is obvious; they do not want to be held to a higher standard of care that a warranty may encompass. Cloud providers want to also avoid liability for implied warranties because of uncertainty and legal risk associated with such clauses. Users will want to get, as many warranties as possible, and to have loss arising out of breaches of those warranties not be subject to contractual limitations of liability.

It is apparent that risk is not effectively allocated between the cloud customers and the cloud provider/s, especially in standard form contracts, which reduces their value as reliable trust mechanisms greatly. Although cloud providers are seen to be the more appropriate actor to have the risk associated to, data privacy and security contractual agreements do not always effectively identify, allocate or remediate these risks.

4.5 Summary

From a legal point of view, cloud computing does entail risks for the processing of personal data. These risks relate mainly to the particular circumstances of processing allowing, for instance, international data transfers or shifting of roles between the entities taking part in the processing operations. Although a legal approach does not aim at measuring such risks, there are certain elements stated in the analysis above which aim at mitigating them, while increasing trust to cloud.

In particular, the security obligations allocated to data controllers -and data processors- established under the Data Protection Directive aim at mitigating risks, given that both entities are obliged to adopt "appropriate security measures" depending on the nature of processing. Cloud computing agreements not only address, but also specify further the security obligations framed under the overarching regulatory framework. Nevertheless, the widespread use of standard cloud contracts -and the lack of equal negotiation powers between the cloud customers users and the service providers- often does not allow the concluding of cloud agreements tailor made to the interests of the cloud customers, especially, when they are end-users or SMEs. Moreover, security audits discussed earlier contribute to building trust to cloud and increasing transparency in relation to certain types of processing, which - by default- appears to be vague and opaque to cloud users.

Despite the continuous flow of data in the cloud, the existence of certain safeguards purports to mitigate

the related risks. In this context, the existence of Binding Corporate Rules submitted for approval by the competent Data Protection Authority or the concluding of agreements such as Safe Harbour could enhance trust to the cloud with respect to processing of personal data. It should be noted, though, that the lack of communication of the entire chain of processors or sub-processors to cloud users as well as the fact that the exact locations of data remain often unknown to cloud users undermine the trust and transparency of cloud offered services.

Furthermore, the issue of liability is of fundamental importance in case of cloud computing, given that it raises -reasonably- the question on how the cloud user could actually trust the cloud given that cloud contracts limit the liability of cloud service providers. In cases of data losses, for instance, cloud contracts often exempt cloud service providers of any obligation to indemnify cloud users for the damages caused. Under a broader perspective, the fact that cloud contracts provide, of course, for the applicable law and the competent courts could be seen as an element creating a positive impact on the levels of trust being built towards the cloud. Given, though, the judicial expenses and the fact that the applicable law -as provided in such arrangements- is the law of the country where a service provider is located, cloud customers –especially, Small and Medium Enterprises- are not facilitated in making use of such provisions.

A4Cloud tools serve as a means to enhance accountability and trust in the cloud in relation to processing of personal and business sensitive information. Therefore, the present Deliverable will give input to other Working Packages, such as D-4, which addresses Cloud Contracts and SLAs aiming developing tools for remediation and redress.

The next chapter discusses aspects of our accountability-based approach to risk and trust governance. It explains the nature of emerging relationships between accountability, risk and trust. It presents the underlying assumptions about how accountability relates to risk and trust, as discussed with stakeholders during the work package B2 workshop on cloud risks.

5 Accountability, Risk and Trust in Cloud Ecosystems

Accountability concerns data protection in the cloud. It provides a means to address some of the data governance's concerns with the shift required by adopting cloud computing. Accountability supports data stewardship. It is a mitigating factor for emerging threats and enhances trust in cloud services. Accountability is therefore related to both risk and trust. This section is concerned with understanding emerging relationships between accountability, risk and trust in order to support governance. It discusses accountability, risk, and trust in cloud ecosystems, and argues that understanding their relationships enables accountability governance, that is underpins governance processes that enhance accountability in the cloud. This section builds on the concepts of risk and trust introduced earlier in this deliverable, the accountability definitions and model defined by the C2 Conceptual framework, and on stakeholder elicitation workshop (Risk Modelling for Cloud Services Workshop) organised in collaboration with B2 Elicitation. It points out an understanding of emerging relationships between accountability, risk and trust. The engagement with stakeholders and the analysis of their feedback consolidate our understanding of emerging relationships between accountability, risk and trust in order to support accountability governance. This section first describes the relationships between accountability, risk and trust. These relationships underpinning accountability governance, an accountability-based approach to risk and trust governance, are the focus of our enquiries with stakeholders. The assumption is the better our understanding of such relationships the better our support to accountability governance. It also relates the main concepts of accountability, risk and trust each other in the context of accountability governance. It also reports some stakeholder feedback on accountability (DB-3.2), risk and trust, and discuss their relationships.

5.1 Accountability, Risk and Trust Relationships

Accountability addresses concerns with Data Protection (Article 29, 2010) or in general confidential data. It is among the identified "technical and organizational measures of data protection and data security" (Article 29, 2012). Accountability therefore provides a means to unlock the cloud potential by addressing relevant problems of data protection emerging in cloud ecosystems (Pearson, 2011). Our work (drawn from C2 and its collaboration with other project work packages) is concerned with Accountability in the Cloud, see (Felici et al., 2013) and (Felici, Koulouris, Pearson, 2013). The work in (Felici et al., 2013) highlights how accountability is necessary in order to align cloud ecosystems with relevant regulatory regimes like the ones envisaged by the EU Data Protection Directive (Directive 95/46/EC). It discusses how accountability addresses emerging issues and legal perspectives in cloud ecosystems. It highlights both legal and technical aspects of accountability. The work in C2 introduces a conceptual model, consisting of attributes, practices and mechanisms for accountability in the cloud. The proposed model characterizes cloud-mediated interactions between actors in terms of accountability attributes. This forms the basis for analysing accountability relationships and requirements between cloud actors, hence chains of accountability in cloud ecosystems.

From a security perspective various threats affect the cloud (CSA, 2013). Accountability provides a means to address some of the data governance's concerns with the shift required by adopting cloud computing (ENISA, 2009). On the one hand, accountability supports data stewardship Accountability therefore is somehow related to both risk and trust. However, their relationships are yet vaguely understood. Intuitively, accountability mitigates risk and increases trustworthiness of the cloud. It acts as a balancing factor between risk and trust. It enables the identification based on accountability of acceptable trade-offs between risk and trustworthiness. This underlies our accountability-based approach to risk and trust governance.

This section provides an in introduction to the concepts of Accountability, Risk and Trust. In particular, it highlights aspects of these concepts that are relevant for cloud governance. The relationship between risk and trust has been considered (in particular, from social and policy perspectives) underpinning the governance of privacy (Bennett, 2006). Although accountability is difficult to define and operationalize (that is, to put it into practice) uniformly – *"defining what exactly accountability means in practice is complex"* (*Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor,"* n.d.)– it is critical for supporting governance of privacy, data protection and security in the cloud (Guagnin, 2012). The assumptions that characterise emerging relationships between accountability, risk and trust are:

- Risk affects accountability
- Risk requires trust (to take decision)
- Accountability mitigates risk
- Accountability mediates risk and trust
- Trust facilitates interactions
- Trust relies on operational evidence of trustworthiness.

The remainder of this section introduces the concepts of risk, accountability and trust and position them with respect to accountability governance.

5.1.1 Emerging Threats in Cloud Ecosystems

Cloud customers and providers are exposed to various problems. For instance, from a resource viewpoint, it is necessary to improve data management processes and to a certain extent to automate them. The increasing amount of data and resources requires new mechanisms enabling cost-effective management while guaranteeing critical features like security and privacy. Some of the issues that cloud customers and regulators are mostly concerned about are things like lack of transparency and control in cloud service provision. Compliance with evolving international regulatory regimes may also exacerbate complexities from a legal perspective. Such challenges are perceived as barriers to the adoption of cloud computing. Figure 11 highlights some of the main threats (e.g. loss of governance, lock in hazard, isolation failure) in cloud ecosystems. The threats are drawn from existing risk analyses of cloud computing, in particular, CSA Top Threats (CSA Cloud Security Alliance, 2013a), CSA Security and Privacy Challenges (CSA Cloud Security Alliance, 2012)(CSA 2012), CSA Security Guidance for Critical Areas of Focus in Cloud Computing (CSA Cloud Security Alliance, n.d.) and ENISA Benefits, risks and recommendations for information security (ENISA, 2009). The emerging threats are continuously monitored and assessed in order to highlights areas for mitigations, and minimize potential risks (ENISA, 2013).

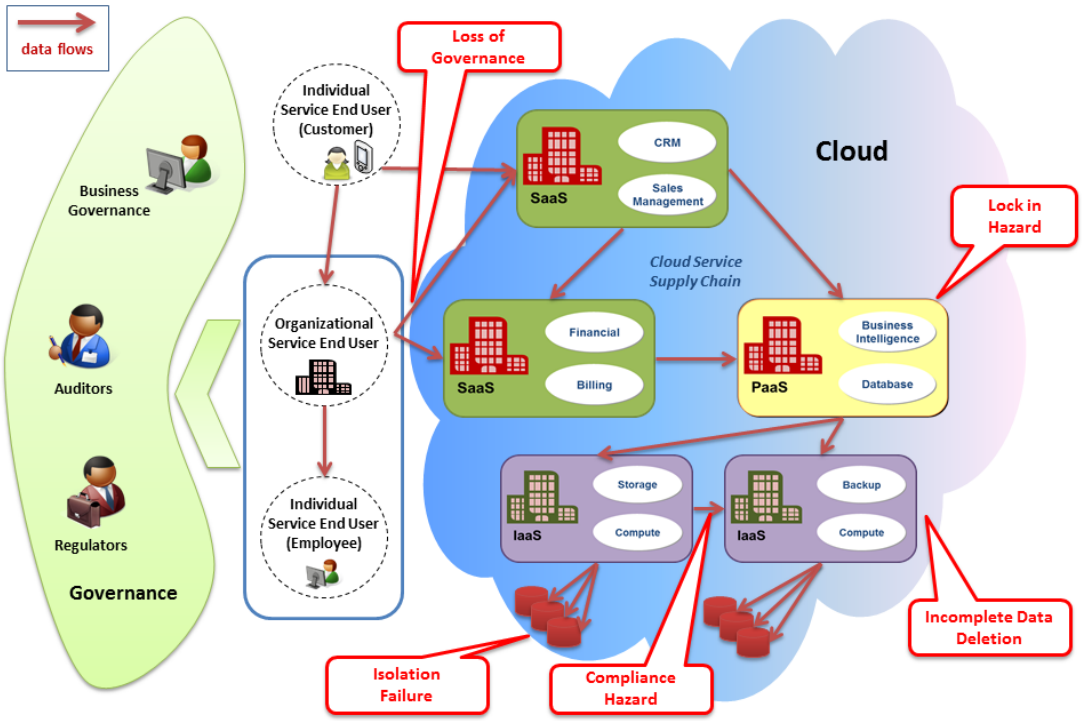

Figure 11 Emerging Threats in Cloud Ecosystems

The remainder of this section introduces basic concepts underlying risk assessment. It defines *Risk* for specific *Threat Scenarios* concerning cloud ecosystems, that is, *Threats* exploiting *Vulnerabilities* and affecting *Assets*. These are the main aspects of risk that are taken into account while performing risk assessment. They provide a systematic way of capturing and discussing Threat Scenarios (Figure 12).

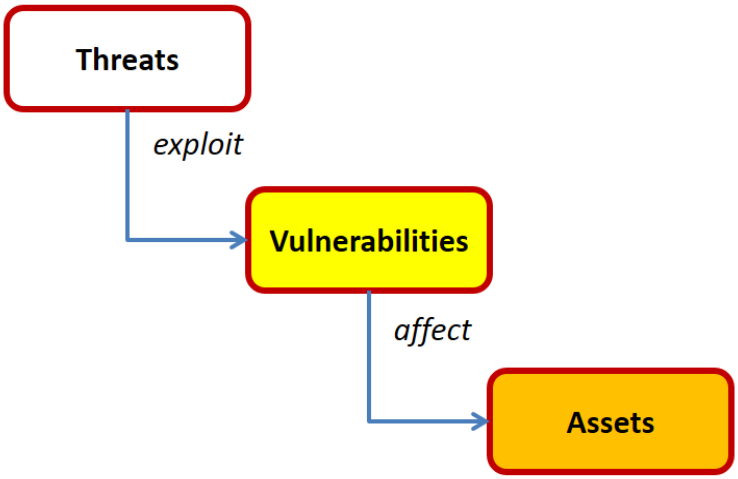

Figure 12 Threat scenario

Threats: The ENISA risk analysis in (ENISA, 2009) identifies 35 different threats grouped as Policy and Organizational Risks, Technical Risks, Legal Risks (and Risks not specific to the cloud). The standard ISO/IEC 27000 defines threat (ISO IEC, 2012): "potential cause of an unwanted incident, which may result in harm to a system or organization."

Vulnerabilities: The ENISA risk analysis in (ENISA, 2009) lists 53 different vulnerabilities (e.g. V1 AAA vulnerabilities, V2 User Provisioning Vulnerabilities, and V53 Inadequate or misconfigured filtering resources). The standard ISO/IEC 27000 defines vulnerability (ISO/IEC 27000:2009): "weakness of an asset or control that can be exploited by a threat." This definition clearly states that vulnerabilities are associated with assets (that is, elements in cloud ecosystems that are critical and need to be protected or preserved) as well as controls (that is, mechanisms that are meant to mitigate risk). Therefore, in cloud ecosystems, for instance, assets are personal and confidential data as well as services (and related technologies like hardware and software on which they build on). Controls are also concerned with accountability practices and mechanisms that intend to mitigate risks.

Assets: ENISA in (ENISA, 2009) takes into account 23 different assets (e.g. A1 Company reputation, A2 Customer Trust, and A23 Backup or archive data). Specific actors own or are concerned with specific assets. Interestingly, assets are allocated (or belong to) specific actors. This is to take into account to whom it might have particular interest in protecting and/or preserving specific assets. For the sake of simplicity, assets are grouped into three main categories (Figure 13): Data, Cloud Services and Controls. Accountability practices, mechanisms and tools fall into the controls category.

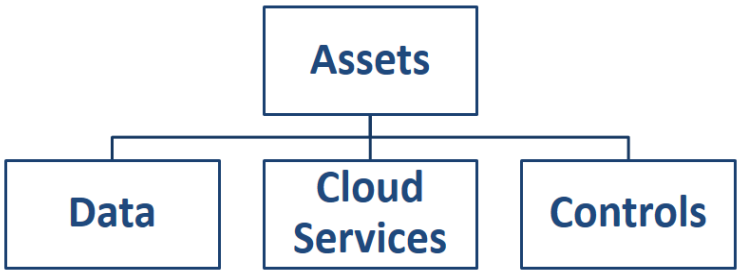

Figure 13 Assets: Data, Cloud Services and Controls

Risk: The evaluation of risk involves an assessment process intended to gather relevant information in a systematic manner. Risk assessment is concerned with the "overall process of risk analysis and risk evaluation" (ISO/IEC 27000:2009). The risk analysis, "systematic use of information to identify sources and to estimate risk" (ISO/IEC 27000:2009), is conducted for the identified threat scenarios. The risk estimation is concerned with assigning values to the probability and consequences of a threat scenario. The resulting risk level (Figure 14) is the combination of Likelihood (5-value scale: very low to very high) of a particular threat (scenario) and Impact (5-value scale: very low to very high) of the specific threat scenario.

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Figure 14 Risk Levels (ENISA, 2009)

Figure 15 groups the elements underpinning risk assessment.

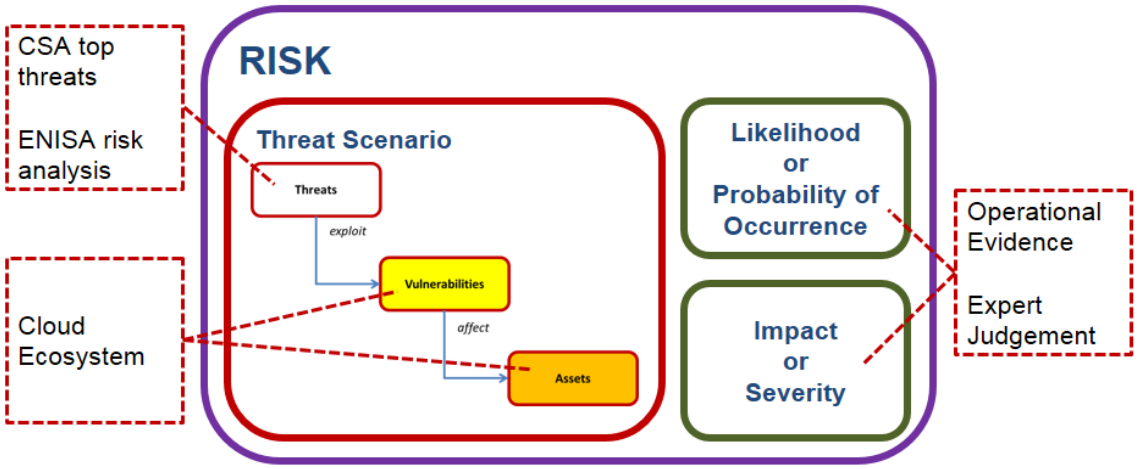

Figure 15 Elements informing risk assessment

5.1.2 Accountability Definition and Model

The C2 Conceptual Framework discusses accountability and introduces an accountability model tailored to the cloud (Felici, Pearson, & Koulouris, 2013). The definition contextualizes accountability and makes it relevant to the data governance problem in cloud ecosystems.

Definition of Accountability for Data Stewardship in the Cloud: *Accountability for an organization consists of accepting responsibility for the stewardship of personal and/or confidential data with which it is entrusted in a cloud environment, for processing, storing, sharing, deleting and otherwise using the data according to contractual and legal requirements from the time it is collected until when the data are destroyed (including onward transfer to and from third parties). It involves committing to legal and ethical obligations, policies, procedures and mechanisms, explaining and demonstrating ethical implementation to internal and external stakeholders and remedying any failure to act properly.*

Building on the definition of accountability, we have also introduced a model for data stewardship in the cloud (Felici et al., 2013) – Appendix E reports for convenience the *accountability model* defined by the C2 Conceptual Framework. Structuring accountability (in terms of attributes) allows us to interpret relationships between actors in the cloud. Figure 16 illustrates the scope and inter-relationships among the defined accountability attributes in the context of a cloud-mediated interaction between two generic actors (Actor A and Actor B). The actors are intentionally kept generic to allow for generalizations where one of the actors is actually an oversight or enforcement entity (e.g. regulator and auditor).

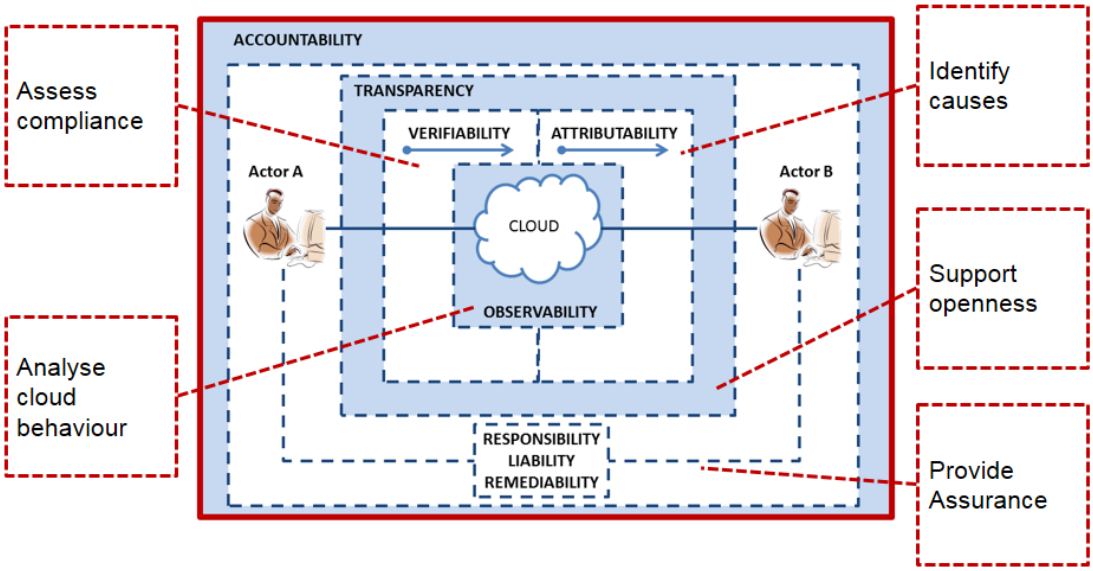

Figure 16 Accountability Attributes and Evidence

Figure 16 highlights how the attributes fit together to enable accountability (evidence). Transparency relies on verifiability and attributability, which in turn rely on observability. Responsibility, liability and remediability rely on transparency. Other aspects of accountability are also relevant. For instance, sanctions are (legal) consequences of failing to fulfill responsibilities. Assurance (resulting from responsibility and liability) is a positive declaration intending to give confidence. Assurance can take the form of evidence, which can be used to convince a third party about, for example, the reason for a failure that has happened. Remediation is the act or process of correcting, for example, a failure or deficiency. Some of these concepts (e.g. obligations, sanctions and holding to account) are further discussed within accountability governance.

5.1.3 Trust in Decision Making

Accountability supports trustworthy cloud ecosystems and trust decisions within them. This intuitive interpretation of the relationship between accountability and trust relies on some assumptions about the nature of trust and trustworthiness. Although they are related to each other, they are two different concepts. The following intuitive propositions characterise and distinguish trust and trustworthiness:

- trust is not trustworthiness
- trust is about making decision (e.g. A trusts B in context/situation X)
- trustworthiness is about behaviour (e.g. B exhibits trustworthiness).

Figure 17 highlights further aspects of trust and trustworthiness that enable decision making. The work in (Felici, 2012) provides also a detailed review of the two concepts. This deliverable is mainly concerned with their relationships with accountability and risk. Intuitively, individuals decide to trust and take actions, with a particular confidence level based on the evidence of trustworthiness exhibited by individuals or systems[30]. The model for trust decision making helps also to explain the relationship between risk and trust. Decisions are taken based on diverse information and factors. Risk assessment (as presented in the previous sections) takes into account an analytical interpretation of risk. Unfortunately, risk assessment relies often on partial information. Therefore, it involves to a certain extent uncertainty. Trust decisions are then often taken based on other considerations, e.g. psychological, socio-cultural and institutional factors as reported in the previous sections. Trust (decisions) and risk are then related and characterized by uncertainty[31], that is, any trust decision based on trustworthiness (evidence) involves risk.

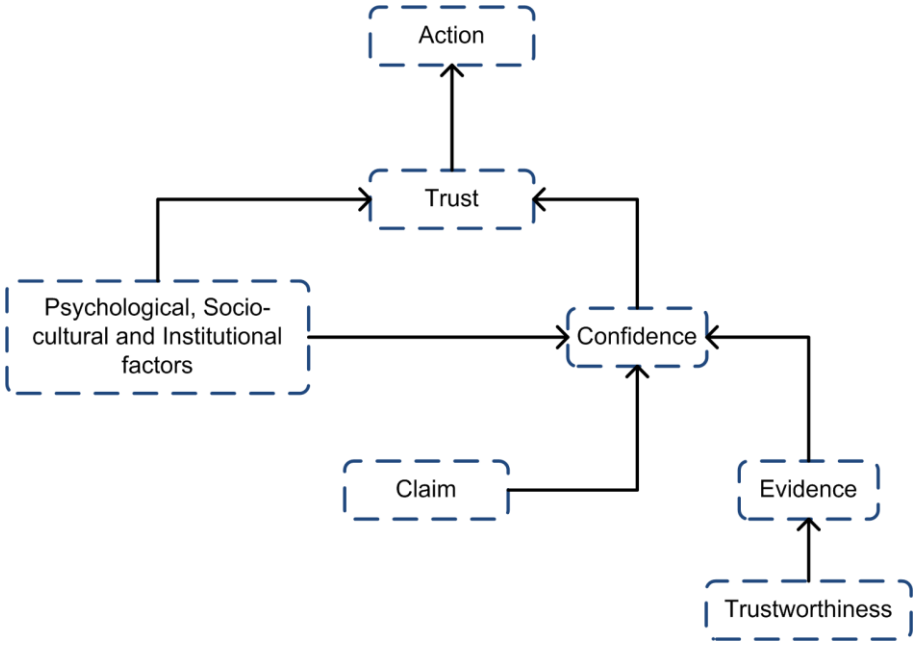

Figure 17 A model for trust decision making (Felici, 2012)

Trust decisions characterize also emerging relationships between cloud actors. Let's consider two actors that interact each other in the cloud Figure 16), for instance, Actor A is a cloud customers and Actor B is a cloud provider. Actor B is expected to address specific risks by accountability (as highlighted by the mapping between accountability attributes and risks). Therefore, relevant trust questions are: Does Actor A trusts Actor B to address specific risks? Does Actor A trust the cloud to not so vulnerable to risks? Does Actor A trust Actor B in specific situations (A trusts B in context X)? Does Actor A trust cloud services to work in a particular manner (Does Actor A trust the cloud to work as intended in Y)? The model for trust decision making underpins also trust decisions between cloud actors A and B. B trustworthiness could be estimated by how successfully accountability claims have been supported by evidence. Note that this characterization captures most (commonly accepted in literature) aspects of trust and trustworthiness (e.g. subjectivity, trust is different than trustworthiness, relational, rational). Of course, there could be situations in which the decision to trust is misplaced due to insufficient evidence or untrustworthy behavior of B. These trust decisions emerge also in the relationships between cloud actors (e.g. Actor A assesses trustworthiness based on evidence of Actor B based on the accountability relationships and emergent behaviour w.r.t. specific service agreements). Trust decisions based on accountability would characterize accountability-based risk assessment and mitigation in cloud ecosystems, hence accountability governance.

[30] For example, the work in (Amato et al., 2011) reports an empirical study of trust decisions and observations.

[31] The work in (Anderson & Felici, 2012) provides an account of socio–technical aspects of risk.

5.2 Accountability Governance

Accountable organizations need to define and implement appropriate governance mechanisms relating to treatment of personal and/or confidential data in cloud environments. The actions in question pertain to the collection, storage, processing and dissemination of personal and/or confidential data. Figure 18 shows the interaction between two organizations (as a continuous process) driven by accountability governance (constrained by external criteria and regulatory regimes but orchestrated independently by organizations). Organization A could be part of a service provision chain that involves cloud service providers and Organization B is actually an oversight and enforcement actor (e.g. regulators) in the chain. Organization A defines and implements appropriate governance mechanisms, which enable to demonstrate governance. Organization B, holding to account Organization A, can ask for further clarification, engage in discussions and also apply sanctions. As a result, Organization A may modify organizational governance.

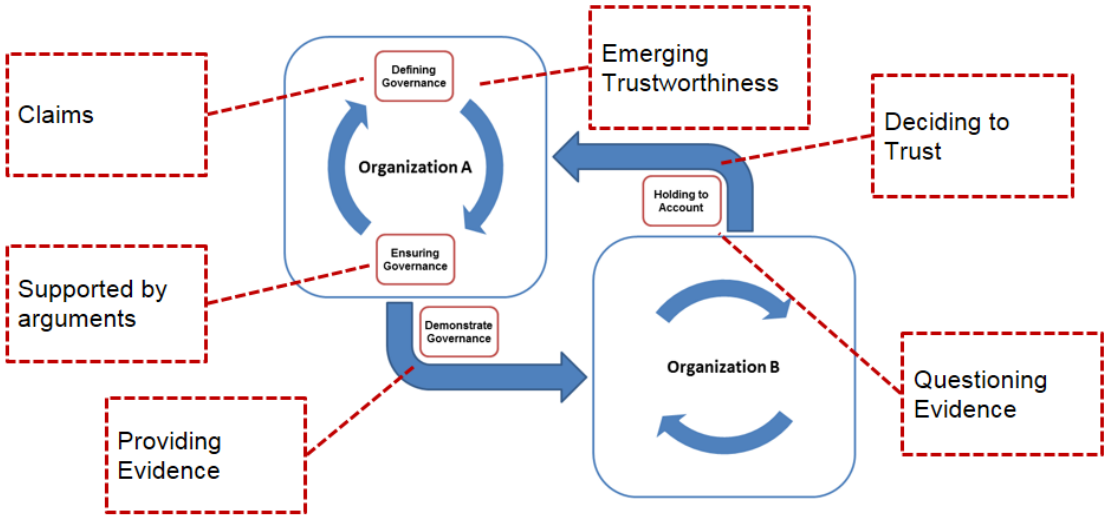

Figure 18 Accountability governance

Organizations need to provide transparency of those actions taken in order to show that stakeholders' expectations have been met and that organizational policies have been followed. They also need to remedy any failure to act properly (e.g. by notifications, remedies, sanctions) even in cloud-supply chains involving multiple service providers. Accountability governance redefines interactions between providers and regulators as well as between providers themselves. The ethical nature of an accountability-based approach and the organizational obligations that result from taking this approach represent a shift from reactive to proactive governance of personal and/or confidential data. Organizations commit to the stewardship of personal and/or confidential data by addressing legal, contractual and ethical obligations. In order to do so, organizations deploy and use different mechanisms (e.g. policies, standards), take into account social norms, provide evidence to internal and external stakeholders, and remedy any failure to act properly.

5.3 Stakeholder Elicitation

The previous sections introduced accountability, risk and trust. This section describes the rationale for gathering stakeholder perception (and understanding) about emergent relationship between accountability, risk and trust. The accountability-based approach described allows us to structure the elicitation activity and to gather specific feedback. The problem of analysing emergent relationships between accountability, risk and trust can be exemplified by four different alternative decisional situations (Figure 19). For each identified risk and any supported accountability it is possible to have trust or not trust in such particular situation. In general, accountability needs to mitigate risk, hence suggesting trust or mistrust depending on the supported accountability in practice.

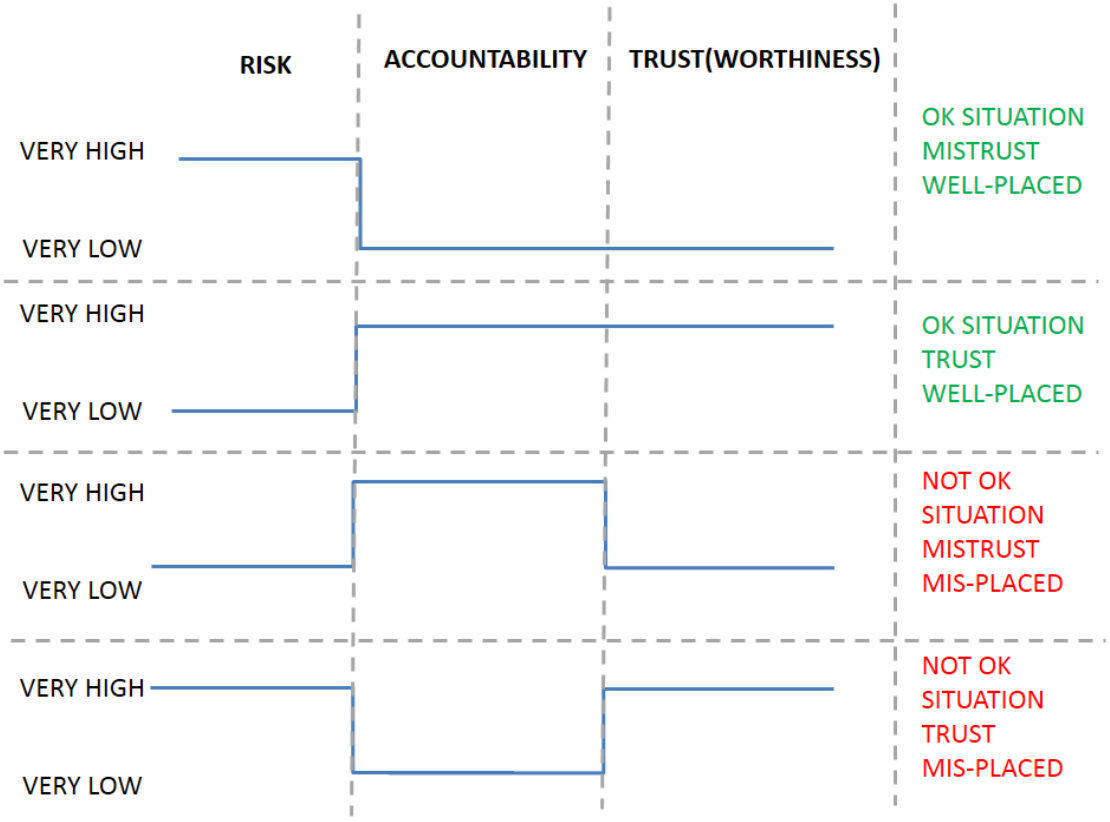

Figure 19 Accountability, Risk and Trust Situations

The problem then is to understand how accountability mitigates specific threats (risks). Accountability mechanisms would address some of these threats by supporting accountability (attributes) – *How does accountability address emerging threats?* In order to answer such question, it is necessary to explicit the relationships between accountability attributes, practices, and mechanisms. Moreover, we need to understand how accountability addresses risk. In particular, we need to explicit the relationships between the different aspects of the accountability model mitigating the risks of threat scenarios. For instance, the CSA Cloud Control Matrix already identifies specific controls (e.g. Governance and Risk Management, Legal & Standards Compliance, Supply Chain Management, Transparency and Accountability) that relate directly to some of the accountability attributes (we have already done an exercise of reviewing the CSA CCM from an accountability perspective). Mapping accountability to specific mechanisms (and explaining how such mechanisms mitigate risks, e.g. eliminating vulnerabilities, decreasing impact) highlights how accountability (if successfully supported) contributes to mitigate specific risks. An accountability assessment with respect to risk then consists in assessing whether or not relationships between mechanisms and accountability are successfully supported. Another relevant question is then: *how does accountability if successfully supported mitigate risk?* That is, if accountability is successfully supported the result would be to mitigate risks (in practice, to lower either the likelihood of occurrence or the impact). It would also support trust decisions. This would enhance trustworthiness, hence, trustworthy cloud ecosystems. Next section reports the feedback we collected in a dedicated workshop with stakeholders in order to gather their perception and understanding about emergent relationships between accountability, risk and trust.

5.4 Feedback Analysis and Discussion

This section reports discussions with stakeholders, who provided feedback to the structured representation of accountability (Accountability Model) and its characterization of interactions between cloud actors. During a dedicated workshop (co-located with the CSA EMEA Conference, Edinburgh, UK, September 2013) we collected stakeholders feedback, critically analysed such feedback and drew some concluding remarks about

emerging relationships between accountability, risk and trust and their underpinning of accountability governance, that is, an accountability-based approach to risk and trust governance. At the workshop, we briefed stakeholders with all concepts introduced in this deliverable, in particular, accountability. The main discussion question asked to the workshop participants was: *How does Accountability relate to Risk and Trust?* We discussed such questions with stakeholders and collected their feedback by minutes of the discussions and by a questionnaire. The stakeholder workshop focused on risk in the cloud. In particular, this paper reports on the discussions about accountability, risk and trust as well as on our accountability-based approach to risk and trust in cloud ecosystems. The discussions with stakeholders provide us with insights about accountability, risk and trust.

The discussions highlighted that stakeholders agree that trust facilitates interactions. They additionally point out that trust is related to the context of the interaction (cloud ecosystem), whereas risk needs to be taken into account regardless trustworthiness. High risk levels would affect trustworthiness. The relationship between accountability and risk stimulated interesting discussions too. Stakeholders affirmed that accountability will enhance trustworthiness and change risk perception –*"responding to perceived risk can lead to less secure solutions, instead of optimal controls"*, hence *"reduced perceived risk will increase cloud adoption, increased transparency will mean increased usage"*. On the relationship between accountability and trust, stakeholders agreed that accountability supports trust decisions and enhances cloud trustworthiness. They also highlighted that *"accountability is a good starting point to trust but not the answer"*, that is, being accountable of specific actions would not necessary imply being trusted. However, they confirmed that *"accountability is very important".* Accountability will influence trust in cloud services. Enhancing trustworthiness will have also an effect on risk due to trust decisions. Feedback was also collected by a questionnaire. The questionnaire consisted of 10 statements describing the relationships between accountability, risk and trust (Appendix F). Stakeholders were asked to express their agreements with such statements. The questionnaire provided a means to collect stakeholders' feedback in a systematic manner at the end of the focus group discussions. The questionnaire's outcomes somehow reinforce our understanding of the discussions with stakeholders. Figure 4520 shows the box plots of the feedback collected by the questionnaire. Based on the median values, the box plots show a stronger agreement about the relationship between accountability and trust (statements S7-S10). Whereas, there are mixed views about the relationship between accountability and risk (statements S1-S6), in particular in which way risk affects accountability and accountability addresses risk. Deliverable D-B-2.2 (Risk Modelling for Cloud Services –Workshop Results) reports further analyses and discussions about stakeholders' feedback.

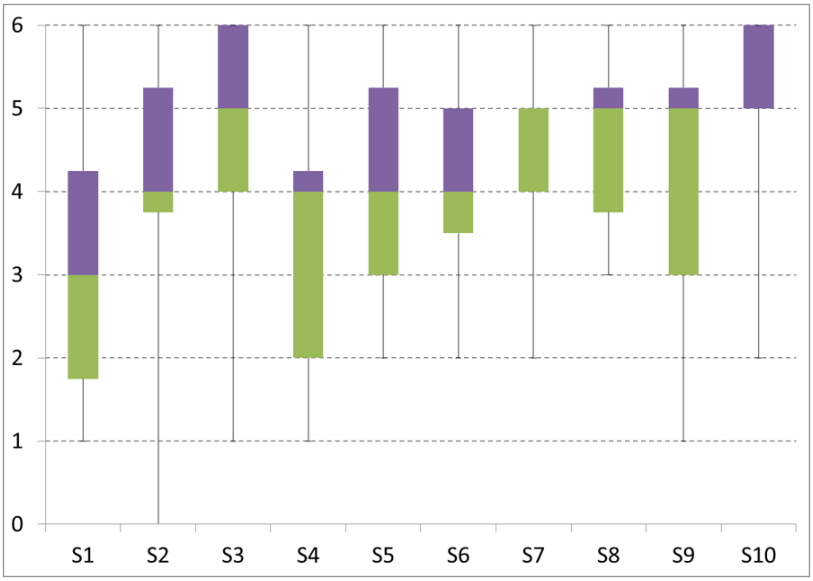

Figure 20 Box plots of questionnaires

- **Accountability** – The term accountability is understood differently by stakeholders. There is not yet a shared understanding of the accountability concept itself. Stakeholders recognise different attributes (or elements) such as responsibility and liability contributing to accountability. However, they understand the contributions of such attributes toward accountability in different ways. This depends on their background and expertise. There were no major objections about the presented accountability model. A structured representation of accountability would support discussions on accountability and building a shared understanding of the concept itself. Other comments concerned with the relationship between accountability, risk and trust. There was somehow a converging understanding that the relationships between accountability and risk and accountability and trust are different (or of a different nature).
- **Accountability and Risk** – Although accountability addresses risk, it is yet unclear how. The relationship between accountability and risk is a generalised one. That is, it is believed that accountability addresses emergent risks in cloud ecosystems. However, stakeholders had difficulties to figure out in which way. This is probably due to the fact that the concepts were presented in general terms and in the context of an accountability-based approach to risk and trust. Future work would need to identify clear examples of the effect of accountability on risk. Stakeholders questioned whether accountability addresses risk (by modifying risk profiles in terms of likelihood of occurrence or severity of impact) or changes risk perception of emerging threats in cloud ecosystems. This is another interesting aspect of the relationship between accountability and risk that requires further investigations.
- **Accountability and Trust** – The relationship between Accountability and Trust seem to be more context-dependent than the one with Risk. Accountability helps to make trust decisions, however accountability itself seems to be necessary but not sufficient for (or implying unconditionally) trust. Accountability will help to make trust decisions. A critical aspect of trust decisions seem to be related to the evidence provided to stakeholders. Therefore, accountability (in particular transparency) plays an important role in trust decisions and supports trustworthiness (in particular based on accountability evidence).

5.5 Summary

This section discusses aspects of our accountability-based approach to risk and trust governance. It explains the nature of emerging relationships between accountability, risk and trust. The underlying assumptions about how accountability relates to risk and trust have been discussed with stakeholders. A final remark on the emerging relationships between accountability, risk and trust is concerned with the proposed accountability-based approach to risk and trust. It has emerged that understanding the interplays between accountability, risk and trust would support the identification of alternative strategies (e.g. providing further evidence in order to gain trust) of accountability governance. Hence, the relationships between accountability, risk and trust are fundamental in defining an accountability-based approach to risk and trust, hence accountability governance. The better we understand such relationships the better we will operationalize accountability. The sections that follow model cloud ecosystems and introduce our accountability-based approach to risk management.

In the next chapter we develop a first version of a meta-model taking in consideration the issues and concerns to support accountability and the insights with respect to risk mitigation described above. The models will be used for supporting trust for cloud customers, to identify necessary risk-mitigations, to effectively perform privacy impact assessments, and to monitor compliance.

6 Risk and Trust Models for Cloud Ecosystems

Figure 21 taken from MS:C-2.2 (Catteddu et al., 2013) illustrates how the accountability layer developed in A4Cloud serves as a connection between regulatory regimes and cloud ecosystems. In this WP we contribute to the project goals by adapting risk modelling to the cloud considering the accountability dimension.

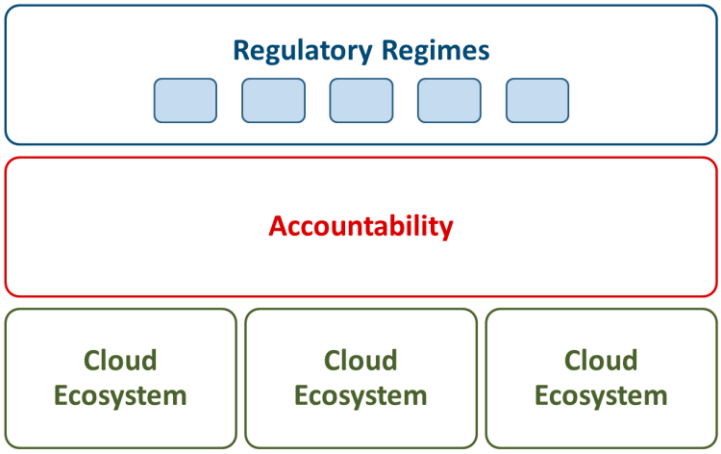

Figure 21 Accountability as enabler for cloud ecosystems

In this chapter we introduce the models for representing cloud ecosystems and cloud-related risks; and in the next one we describe the accountability-based risk assessment process for constructing those models. Section 6.1 presents the models of cloud ecosystems and introduces some structures drawn from relevant regulatory regimes; Section 6.2 introduces the accountability model; Section 6.3 describes the risk and threat model; and Section 6.3 proposes the trust model. Figure 22 schematically illustrates the models and their interdependencies. The cloud ecosystem model is complemented with accountability model to enable constructing both trust and risk models.

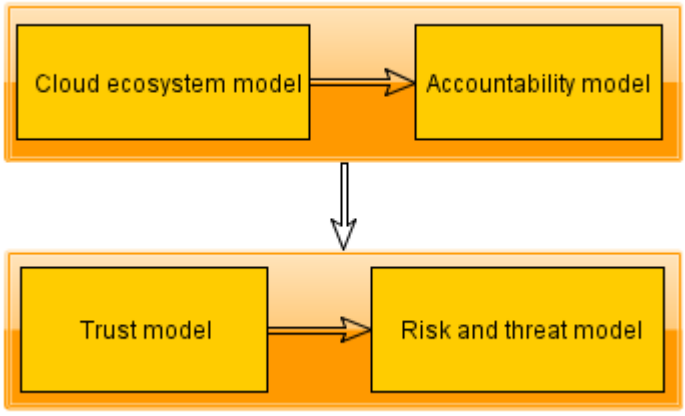

Figure 22 Models overview

6.1 Cloud Ecosystems Model

Knowledge about the data movements in the cloud ecosystem and the involved parties is an essential prerequisite for risk assessment of a cloud solution. This section introduces the cloud ecosystem model supporting the representation of data flows. The model consists of the following main parts:

- High level representation of a cloud ecosystem based on NIST Cloud Computing Reference Architecture (F. Liu et al., 2011) and MS:C-2.2 (Catteddu et al., 2013).

- Elements relevant to regulations on data governance and compliance, such as additional roles from a data protection viewpoint.
- Relationships among cloud actors (roles), such as data provision/transfer, service provision and auditing.

The above 3 points give us a structured representation of the cloud ecosystem by representing the cloud supply chain and mapping it to a specific regulatory regime (i.e. Data Protection Directive).

Figure 23 illustrates all relevant entities in the cloud ecosystem and the relationships between them:

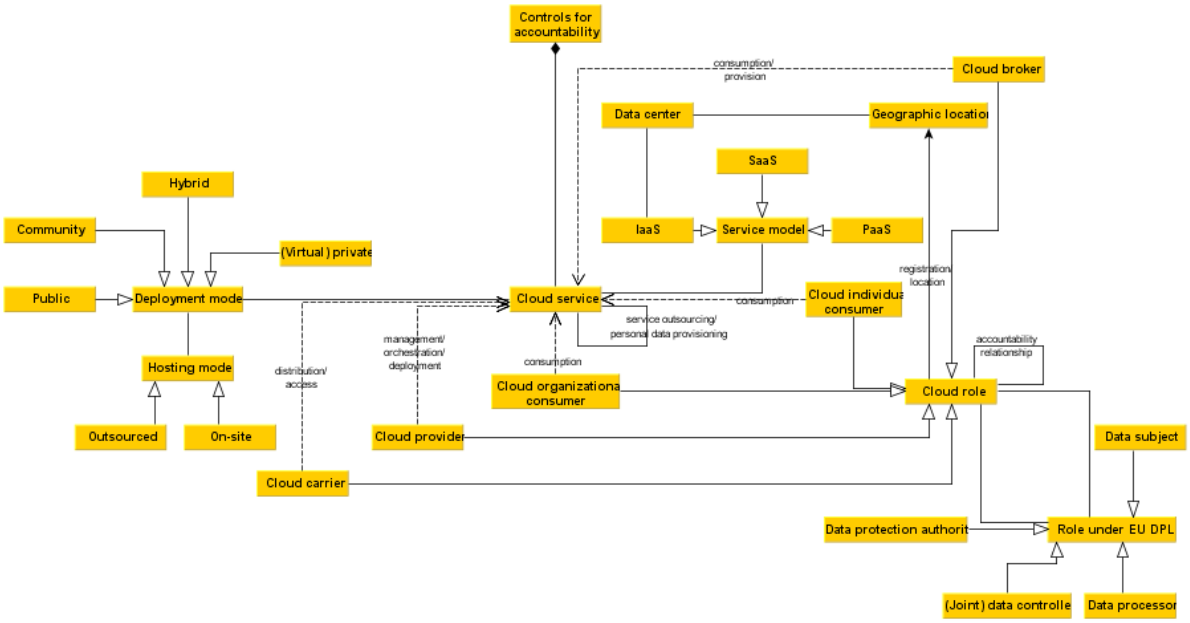

Figure 23 Cloud ecosystem conceptual model

The next subsections detail the cloud ecosystem concepts and relationships on an example of a SaaS solution, based on D:B-3.1 business use case 2 (Bernsmed et al., 2013), depicted in Figure 24. In a nutshell, this is a mobile SaaS solution provided by a supermarket chain MarcheAzur to its customers. However, the implementation of the solution is delegated to Check-it-out (independent software vendor) and is hosted by PaaSPort and InfraRed, providing respectively the platform and infrastructure.

In Section 6.4 we describe the impact this representation on the risk and trust model. The reader should be aware that a thorough analysis of all A4Cloud use cases will be performed in the context of the work package C6 by the task T:C-6.4.

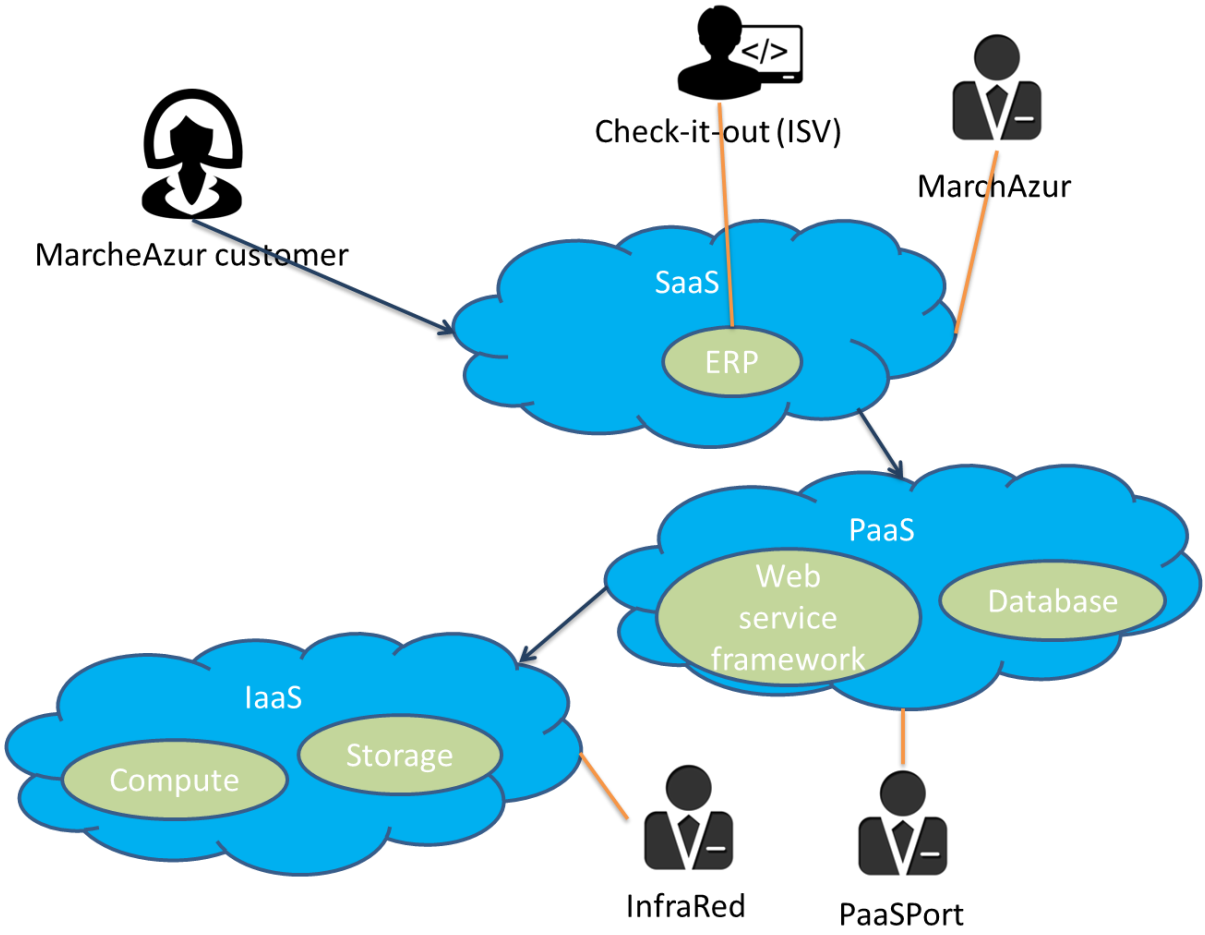

Figure 24 ERP cloud solution for MarcheAzur

6.1.1 Actors

In addition to the service itself, it is necessary to describe the actors interacting with it. In Figure 24, we highlight two entities: the Cloud Customer (data controller), who uses the CRM SaaS application, and the Cloud End-user (data subject), from whom data is being collected and processed in the cloud.

Table 1 lists the attributes from the actors we need for the risk and trust model. The attributes in the model were drawn from the needs to identify responsibilities of the actors regarding the data stewardship (and later the risks associated to those), one of the main principles for accountability in the cloud.

Table 1 Actor attributes

Attribute	Value	Comment
Name	MarcheAzur customer	Free-text reference to the entity
Cloud role	Cloud End-User	The role of the actor in the cloud ecosystem according to MS:C-2.2. Other possible values are Primary Service Provider (business cloud customer), Individual cloud customer, Cloud Service Provider, and

		Cloud Auditor (internal, external).
Role under EU Data protection legislation (EU DPL)[32]	Data subject	Other possible values are (Joint) Data controller, Data Processor, Data Protection Authority, Corporate governance actors (e.g. Data Protection Officer). The roles are fundamental for the identification of regulatory compliance risks.
Geographical location	Europe	Indicate the region or country where natural or legal persons are located. This has implications to regulatory and compliance risks.

6.1.2 Service

Table 2 lists the service technical attributes relevant to the risk and trust modelling.

Table 2 Service attributes

Attribute	**Value**	**Comment**
Service name	ERP	For referencing purposes
Delivery model	SaaS	Alternatives: PaaS, or IaaS. Apart from traditional SPI (SaaS, PaaS and IaaS) we may consider in our modelling approach emerging delivery models, such as business processes as a service, or cloud brokering services. These models however were not the subject of many studies in the literature and deserve more research on the specific risks they may involve. We will discuss them in next versions of this modelling approach.
Deployment model	Public	Alternatives: (Virtual) Private, Hybrid, or Community. Private and Community deployments can be on-site or outsourced (to a CSP's data center).
Geographical locations	France	The list of physical locations of the data centers running the service (e.g. countries).

[32] EUC Directive 95/46/EC and its extensions including proposed General Data Protection Regulation

Service provider name	MarcheAzur (SaaS)	Company Name. For reference purpose only, this is the SaaS provider name
Operations	Recording, Storage, Alteration, Retrieval, Use, Erasure	A set of operations allowed to be performed on user data
Controls for accountability	<List of accountability controls>	See section 6.2.2 for an overview of possible controls.
Service policies	Use for buying products and receiving personalized offers; Do not distribute to 3rd parties[33].	List of processed data and associated data handling policies that derive from service requirements and corporate policies. The policies may specify which actions are allowed by the Data Subject on its personal data and for which purposes. For other properties see D34.1 (Cherrueau et al., 2013).

The composition of cloud services and other relationships are described in section 6.1.2.

6.1.3 Relationships

The following categories of relationships are distinguished inside the cloud service provision ecosystem: delegation relationships and service relationships.

6.1.3.1 Delegation Relationships

The delegation relationships provided below are adapted from Secure Tropos methodology (Giorgini, Massacci, & Zannone, 2005). There are two types of delegations: sensitive data provision and service outsourcing, described below.

Sensitive Data Provision

This relationship represents the movement of sensitive data between parties (i.e. personal or confidential) in the cloud service provision ecosystem. The movement of data can happen between an actor and a cloud service and between cloud services for service provisioning, redundancy, backup, etc. Table 3 presents the attributes of the sensitive data provision relationship.

Table 3 Data provision relationship attributes

Attribute	Value	Comment
Delegator	MarcheAzur customer	Can be a Cloud end-user, PSP or CSP.
Delegatee	MarcheAzur	Usually a PSP or CSP.

[33] The actual format and types of machine readable policies is provided in D34.1 (Cherrueau et al., 2013).

Data: data category {data types}	Personal data {Name, Address}	Indicates the kind of data handled in the specific cloud scenario being modelled. This can be various kinds of personal data or confidential data with different associated sensitivity levels. Personal data with higher sensitivity level is subject to stricter regulations. Examples of personal data: name, address, medical or banking details; examples of sensitive personal data: Payment Card Industry (PCI)-regulated data, racial or ethnic origin, political opinions, religion[34].
Client privacy preferences	Use for buying products and receiving personalized offers; Do not distribute to 3rd parties[35].	Policies for data handling based on end-user preferences. The policies may specify which actions are allowed by the Data Subject on its personal data and for which purposes (usage control). These client preferences should be matched with service policies before engaging into any usage relationship. For more information on policies and matching see D34.1 (Cherrueau et al., 2013).

In order to identify the risks involved in moving data to the cloud, it is important to determine its nature. Regulatory considerations depend specifically on the kind of data being handled in the cloud. For instance, data protection laws govern how personal data is to be processed, but more specific regulations can also apply to health care data, or to financial reports. With regards to the risk and trust model work package, we will not make extensive lists of specific regulatory frameworks for every domain, since the scope of the A4Cloud project focuses on personal data mainly. In addition, one of the use cases is related to healthcare therefore, we may also look at specific risks concerning patient data. Secondly, accountability obligations will vary according to the role played in the data processing. A data controller has many more responsibilities than a data processor. This distinction is fundamental for identifying regulatory compliance risks.

We created a catalogue containing different types of data that may be transferred to the cloud and are subject to specific regulatory compliance risks (this list is not exhaustive and serves for illustration purposes only):

- Personal data, including pseudonymized personal data (we may consider how data was anonymized to indicate its vulnerability to attacks)
- Payment Card Data (a specific type of personal data governed by additional regulations: PCIDSS)
- Encrypted data: we may have considerations about where the decryption key is stored and who can access it
- Trade secrets
- Financial/credit reports (this category is subject to Sarbanes–Oxley Act or Fair Credit Reporting Act)

[34] http://www.bbc.co.uk/schools/gcsebitesize/ict/legal/0dataprotectionactrev4.shtml

[35] The actual format and types of machine readable policies is provided in D34.1 (Cherrueau et al., 2013)..

Service Outsourcing

This relationship determines to which parties and what part of the service provisioning is outsourced. There can be two types of outsourcing: vertical and horizontal. Examples are respectively outsourcing the infrastructure to an IaaS provider and outsourcing part of the business process to another SaaS provider. Multiple outsourcing relationships can be represented for the same service. The corresponding model attributes are listed in Table 4.

Table 4 Outsourcing relationships

Attribute	Value	Comment
Delegator	MarcheAzur	Usually a PSP or CSP.
Delegatee	PaaSPort	Usually a CSP. Sometimes the actual delegate is unknown to the party performing the modelling since a CSP can change subcontractors frequently (ENISA, 2009). However, it is very desirable to know at least what service is outsourced. In this case Delegatee is Unknown.
Service(s)	Database, Web service framework	The outsourced service(s).
Outsourcing policies	Non-redelegation, ISO 27001 certification	Policies controlling the service outsourcing. They are mostly derived from contracts between parties and corporate policies. Examples of policies are non-redelegation of service implementation to 3rd parties, access control policies, certifications, etc.

6.2 Accountability Model

According to C2 – conceptual model, the accountability model is composed of the following elements: attributes, practices, and mechanisms and tools. Below we describe in more detail accountability concepts, their relationships and their role in risk management: in particular, how accountability relationships extend the cloud ecosystem model and how accountability mechanisms can mitigate risks.

Figure 25 illustrates the accountability conceptual model and Figure 26 details the relationship with accountability attributes. The reader must be aware that the models have a high abstraction level and do not determine which controls can be implemented by automated means and the ones that need human intervention or evaluation, such as manual audits. These questions will be clarified by the project as a whole, as A4Cloud solutions will address concerns about complexity and enforceability of legal, regulatory and contractual provisions, socio-economic and corporate constraints, issues of trust for service-users such as risk-mitigation, privacy, confidentiality and transparency, and operational challenges such as interoperability and enforcing and monitoring compliance. The model is abstract such that it can be reflect the accountability framework we are building for these objectives.

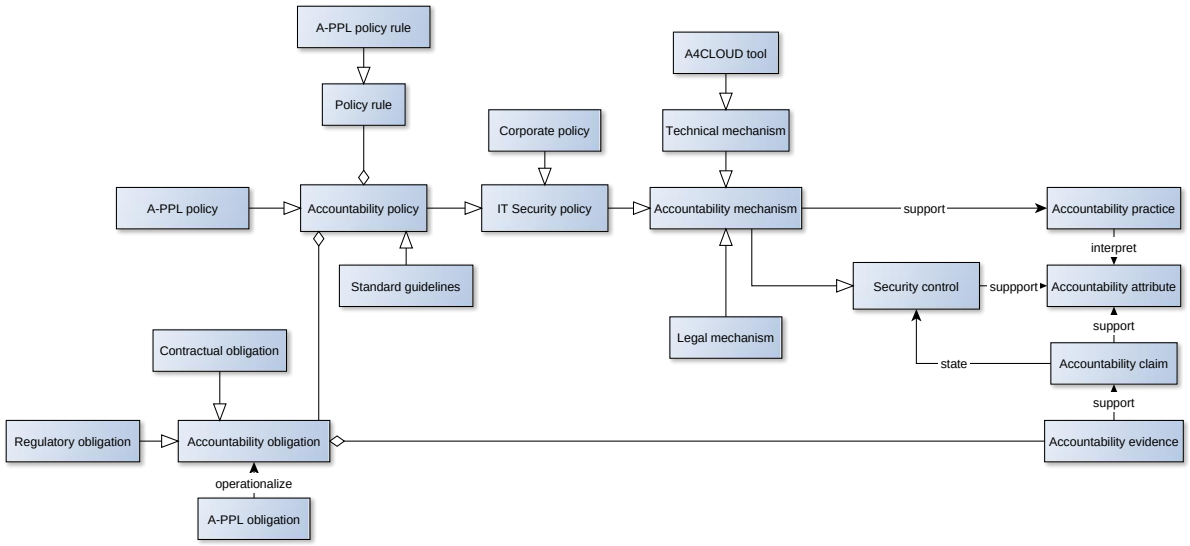

Figure 25 Accountability conceptual model

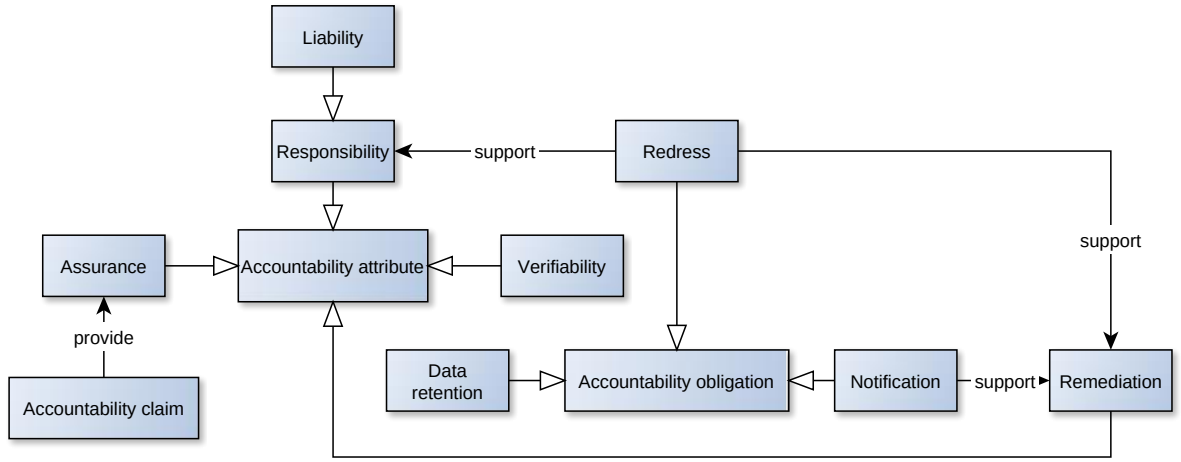

Figure 26 Accountability conceptual: accountability attributes

Table 6 summarizes the accountability concepts introduced and/or adopted in the scope of A4Cloud:

Table 6 Cloud accountability concepts

Concept	Description
Accountability attribute	Defined in the conceptual model (Catteddu et al., 2013). E.g.: transparency, observability, liability, verifiability. Accountability attributes can also be seen as objectives for cloud consumers and together with assets (described in Section 6.4.2) drive the risk assessment.
Accountability practice	Defined in the WP:C-2 (conceptual model). E.g.: data governance program, consent management, remediation policies.

Accountability mechanisms	Defined in the conceptual model (Catteddu et al., 2013). Any control, security and other, that enforces some accountability attributes by mitigating the relevant risks. May include technical mechanisms, standards, IT policies and legal mechanisms.
Accountability policies	Defined in WP:C4 (policy mapping and representation) as a machine-readable Accountability Privacy Policy Language (A-PPL).
Accountability obligations	Defined in WP:C4 (policy mapping and representation) and WP:B5 (contractual and regulatory considerations). Accountability obligations are usually part of accountability policies (see MS:C-4.2) and in contrast to the non-binding nature of the accountability claims, force the related party to be fulfilled. Examples of accountability obligations may be the anonymization of personal data after a certain time, the notification of users in case of data breaches, and logging of all personal data usage. Non-fulfilment of such obligations may result in liability, loss of certificates with a very negative impact on business. As Figure 26 shows, accountability obligations may support various accountability attributes. Accountability obligations create trust relationships among the parties in the cloud ecosystem by supporting accountability attributes, such as liability, sanctions and remediation. However, not all obligations entail liability and this depends on the context. For instance, a CSP that processes credit card data is obliged to pass a Payment Card Industry Data Security Standard (PCI DSS) certification. In case of failure, he is not allowed to perform credit card transactions (sanction), but he is not liable.
Accountability claim	Accountability claims are any assertions regarding the security of the personal data made by a party (usually a PSP or CSP). For instance, a CSP may claim that he has appropriate privacy impact assessment and risk management in place. Accountability claims are generally in a form of non-binding declarations, e.g. self-certifications (CSA STAR[36]) or trusted third-party certifications (PCI DSS, Service Organization Controls, ISO2700, Common Criteria). However, to support the claims parties may provide additional evidence, e.g. in the form of an audit report. Issuing and accepting accountability claims create trust relationships among the parties in the cloud ecosystem by supporting transparency and assurance accountability attributes.
Accountability evidence	Defined in WP:C8 (evidence for verification and assurance). In order to support accountability claims and ensure that accountability obligations are fulfilled evidence shall be provided by the accountable party (usually CSP). This evidence is either provided directly by the CSP or is gathered during the internal or external audits. The evidence can have many forms: e.g. audit

[36] https://cloudsecurityalliance.org/star/

	logs, proofs of retrievability, security or operational logs, self- or third-party certifications. Evidence creates trust relationships among the parties in the cloud ecosystem by supporting accountability attributes, such as transparency and verifiability.

A4CLOUD tool on the diagram of Figure 25 signifies any technical mechanism developed in the scope of A4Cloud (see the Deliverable D-2.1 (Tzoannos et al., 2013) for the full list of A4Cloud tools; a schema displaying the tools is given in Figure 47).

6.2.1 Accountability Relationships

MS:C-2.2 (Catteddu et al., 2013) describes how accountability attributes create emerging relationships in cloud ecosystems. However, we note that saying that a party is accountable to the other for something is somewhat ambiguous in the light of multiple interpretations of this term. For instance, in the following sentences the term *accountable* actually means responsible and liable.

CSPs are accountable for data stewardship of the personal information to the PSP and to regulators.

The PSP is accountable for ensuring that obligations to protect the personal information passed into the cloud are respected all the way along the service provision chain.

This kind of relationships could be considered as accountability obligations in the cloud ecosystem. However, the notion of accountability is not restricted to responsibility and liability and has many other attributes, e.g. transparency, observability, verifiability, assurance. In these examples it is unclear if the notion of being accountable implies these attributes. In fact, these attributes are more concerned with some claims and evidence to these claims, and not directly to obligations.

In order to avoid confusion we will explicitly mention the type of accountability relationship (e.g. obligation, claim, supported by evidence) and the related accountability attributes.

These relationships form accountability chains in the sense proposed MS:C-2.2.

6.2.2 Controls for Accountability

Analyzing how security controls are implemented and their effectiveness across the cloud service provision chain is an essential part of the risk management.

MS:C-2.2 (Catteddu et al., 2013) defines *controls* as:

Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature.

CSA Cloud Control Matrix (CCM) (CSA Cloud Security Alliance, 2013b), briefly described in Section 2.1.8, provides a list of high level security management policies (which they name controls) recommended for implementation in the cloud. This work will mainly refer to the controls from CSA CCM for two reasons: it is cross-linked with major standards and it is mapped to the cloud service and delivery models.

The policy categories (control domains, in CSA terminology) are provided briefly below.

- Application & Interface Security
- Audit Assurance & Compliance
- Business Continuity Management & Operational Resilience
- Change Control & Configuration Management
- Data Security & Information Lifecycle Management
- Data centre Security
- Encryption & Key Management
- Governance & Risk Management

- Human Resources
- Identity & Access Management
- Infrastructure & Virtualization Security
- Interoperability & Portability
- Mobile Security
- Security Incident Management, E-Discovery & Cloud Forensics
- Supply Chain Management, Transparency and Accountability
- Threat and Vulnerability Management

One particular category of controls – *Supply Chain Management, Transparency and Accountability* – is the most relevant with respect to the scope of A4Cloud. For a comprehensive risk assessment it is vital to analyse all these controls in the cloud infrastructure, but we will pay special attention to this category. Table 7 summarizes the characteristics used to describe implemented security controls.

Table 7 Characteristics of security controls implementation

Characteristic	**Comment**
Name/Reference	Identifier for facilitating reference
Control domain	Control category according to CSA CCM (CSA, 2013).
Owner	The actor in charge of implementing the control. Maybe cloud consumer, CSP or other 3rd parties.
Deployment point	The place in the cloud ecosystem where the control is deployed. This may be a service, channel, etc.
Mitigated risks	The risks addressed by the control and the level of mitigation (likelihood, impact).

A4Cloud provides a set of tools supporting accountability (see the Appendix B and (Tzoannos et al., 2013) for a full list of tools and their descriptions). Each of the tools changes in some way the cloud risk landscape and this impact should be considered when selecting appropriate tools for mitigation (see Section 6.4.4).

6.3 Trust Model

Modelling the trust relationships in the cloud ecosystems is no less important than performing risk assessment. In fact, the notions of risk and trust are tightly connected and thus should be modelled together. Not only modelling the trust attitude from the perspective of the person who performs risk assessment is relevant (e.g. the trust of the PSP to the CSP when PSP is conducting the analysis) but also modelling the trust attitude from the perspective of other parties (e.g. the trust of the PSP's users in PSP). The latter can have a direct impact on the business of the organization for which the risk assessment is performed.

For the description of trust relationships we use the definition of (Castelfranchi & Falcone, 2010)

Trust is a mental attitude, a complex attitude of an agent X towards another agent Y about the behavior/action α relevant for the result g.

6.3.1 Trust Attributes

Table 8 lists possible attributes of a trust relationship.

Table 8 Trust attributes

Attribute	Value	Comment
Trustor	MarcheAzur customer	Can be a Cloud end-user, PSP or CSP.
Trustee	MarcheAzur	Can be a PSP or CSP. However, it can be also a non-human actor, e.g. a service.
Object of trust	Secure personal data	An action, object or state of affairs on which trustor depends. Examples could be execution of some task, fulfilment of a goal (e.g. providing some service).
Context	Buy products, Get offers	The context within which the trust relationship exists. Examples could be execution of some task, fulfilment of a goal. We emphasise that the trustor can trust a trustee for something and not for something else. For instance, a Cloud end user would entrust his personal data to a PSP for buying goods and not for advertisements. This context is often represented as a purpose and it is specified in the service contracts.
Source(s) of trust	Positive history of using MarcheAzur services; Claims from the MarcheAzur; Positive media coverage (reputation).	The bases for the development of this trust relationship. Examples could be accountability controls (e.g. certificates), reputation, previous history of direct interaction, etc.
Level of trust	Trust	The level of confidence in the trustee by the trustor. This value is very much influenced by the information in the source of trust. Possible values could be Trust, No Trust, Distrust (Giorgini et al., 2005) or an real value in the interval [-1..1], where -1 corresponds to distrust, 0 to no-trust and 1 to trust. Many other trust metrics are described in the literature, some of which are summarized in MS:C-5.1 .

We represent the trust model as a directed graph with the arcs going from trustors to trustees. The edges are labelled with the object of trust and level of trust attributes. Figure 27 illustrates the trust relationships for the BUC2.

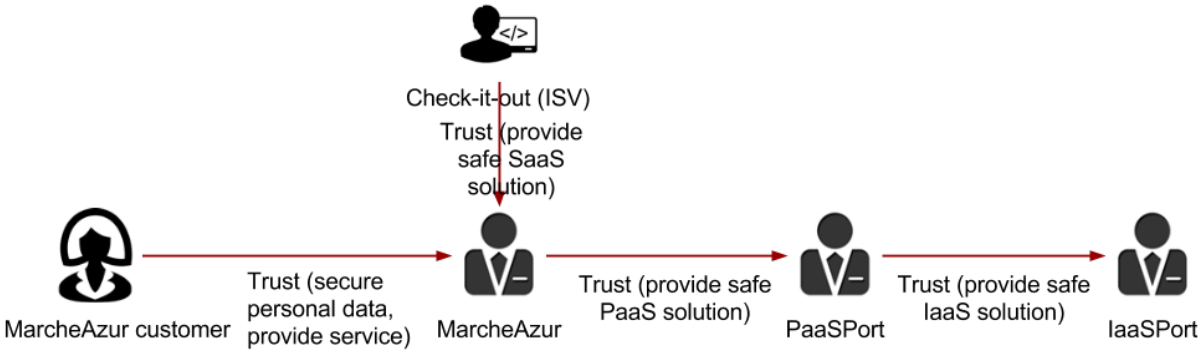

Figure 27 BUC2 trust relationships

We note here that there is no trust relationship from MarcheAzur to InfraRed, because MarcheAzur is supposedly not aware of this subcontractor or PaaSPort is not sharing the evidence of InfraRed's compliance. In this case there is not explicit trust transitivity. However, MarcheAzur is aware of the InfraRed and InfraRed does provide him with enough evidence of compliance then MarcheAzur could trust him as well.

In this case, given that the trust relationships are within the same context – provide cloud service – there is a trust chain from the MarcheAzur customer through all the actors processing his personal data.

6.4 Risk Model

In this section we describe the risk and threat conceptual model, the taxonomy of risks and influence factors.

Figure 28 illustrates the main security concepts and relationships used in this work.

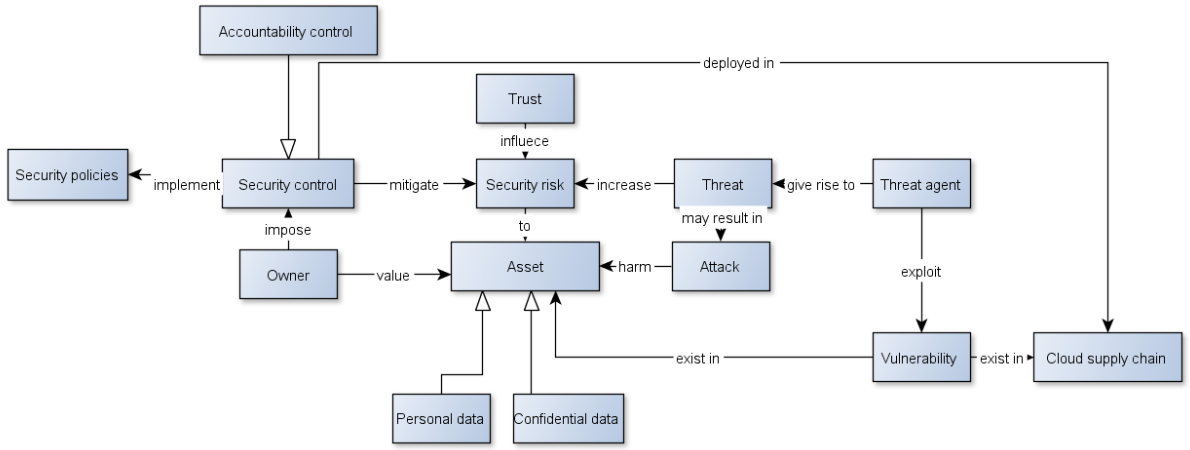

Figure 28 - Risk conceptual model

6.4.1 Assets

The first step in virtually all risk assessment methodologies consists of identifying stakeholders (organizations) and their assets. The stakeholders have a particular interest in protecting the assets they own and the risk assessment is aimed at analysing the risks associated with those assets.

A4Cloud and this WP in particular are mainly focused on the protecting personal and confidential data. Anonymity and confidentiality of the traffic metadata are also related to privacy and hence taken into consideration. Other assets, such as those listed before, are considered in the second place.

Assets represent a certain value for their stakeholders that can be expressed as absolute or relative to other assets. For example (ENISA, 2009) provides relative qualitative values: it speculates that (A1) Company reputation and (A2) Customer trust are more valuable than (A6) Personal data, although there is an obvious interconnection. Specifying an absolute quantitative value for assets, such as personal data is hard and depends on the regulations in place (e.g. the redress the company is obliged to pay in case of personal data theft). For the confidential assets this may be e.g. an estimation of the lost benefit if the competitive advantage is lost due to the theft of business strategic plans or product designs.

Table 9 lists the possible asset attributes instantiated to the MarcheAzur use case.

Table 9 Asset attributes

Attribute	Value	Comment
Asset name	Personal data	For referencing purposes
Owning actor	MarcheAzur	The actor to whom the asset represents a value
Asset value	HIGH	The value of the assets to the owning actor. Depending on the asset type this could be qualitative or quantitative.
Other	Data Sensitivity	Other attributes applicable for particular assets. For example, for Personal data this could be Data sensitivity, for Certification it could be the certificate type and level.

6.4.2 Risk Characteristics

Risk assessment models like the ones identified in Section 2 intend to support the causal analysis of the emergence of specific threats (i.e. how threats exploit vulnerabilities and then affect assets or controls). The resulting risk models combined with empirical evidence (or experts' judgment) support the assessment of risk (in terms of likelihood and impact).

Below we describe how the risks can be represented and categorized.

Table 10 Risk attributes

Characteristic	Comment
Name/Reference	For reference.
Category	Risk categories according to the ENISA report (ENISA, 2009). E.g. Policy and Organizational, Technical, Legal.
Threat	The (malicious) actor and/or event causing the risk. The sources of cloud threats besides the traditional ones may include adversaries, government discovery, cloud administrators, auditors and regulators. Next versions of this model may include attacker profiles and capabilities.

Related vulnerabilities	For instance, authentication vulnerabilities are related to data leakage and privilege escalation risks
Affected asset	The asset, which value maybe decreased as a result of this risk.
Risk likelihood	The probability of the realization of the threat.
Risk impact	Impact level on the asset once threat is realized.
Risk level	A function of risk likelihood and impact on the asset (see Section 7.3).

We adopt in this work the categorization of risks proposed by ENISA (see Section A). The report (ENISA, 2009) provides a list of most frequent risks in the cloud and compares their level to traditional solutions. However, this list should not be viewed as all-inclusive and organization should add other appropriate risks depending on the situation.

6.4.3 Risk Factors and Mapping

Below we describe which factors influence the risks and map between cloud ecosystem model and accountability representation to the related risks. This is used in Section 7.3 to identify and evaluate the risks in a given cloud ecosystem.

The following factors may influence risk levels and can be considered as input parameters for risk assessment:

- Asset value (e.g. sensitivity of personal or confidential data)
- Location of data processing (CSP's data centers)
- Location of CSPs and data subjects
- Applicable data protection regulations (depends on location)
- Implemented controls (e.g. technical, legal). See Section 6.2.2
- Available certifications (e.g. PCI DSS)
- Regulatory and contractual obligations

ENISA (ENISA, 2009) provides a mapping between the common cloud risks and specific cloud service and cloud deployment models. For instance, for "R.2 Loss of governance" the impact is very high for IaaS and low for SaaS, (the report does not bring much explanation justifying this rating). It also schematically illustrates the change of levels of accountability attributes (liability and assurance) for different cloud deployment models: the levels increase from Public to Private (see Figure 46 in Appendix A). The deployment model more likely influence on the risk perception and possibly governance, technical and security risks associated to outsourcing and multi-tenancy. Risk assessment in the case of Hybrid models can be a challenge, depending on how data will flow across on premise (in house servers connected to cloud services) versus combinations of public and private clouds. It may be hard to identify examples and risks applicable to community clouds.

NIST SP 800-146 (Badger et al., 2012) also maps the risks for different cloud deployment models and cloud locations (on-site or outsourced). In general, the cloud related risks are lower in Private deployments, moderate in Community and higher in Public. A summarized version of this is provided in Appendix C. This report also mentions the allocation of responsibilities for providing security for different

cloud service models: the responsibility shifts from CSP to Cloud Consumer down the cloud stack (from SaaS to IaaS).

In addition, we have investigated how the A4Cloud tools are going to change the risk landscape and compiled a survey responded by tool owners (the results are in *Survey on accountability mechanisms* folder). For this we assessed the potential increase or decrease in probability and impact for the set of risks from (ENISA, 2009). The introduction of these mechanisms may change some risks as controls may introduce new vulnerabilities that must be taken into account. Among the risks that were most positively affected by the introduction of controls are: R.2 loss of governance, R.3 compliance challenges, R.7 supply chain failure, R.20 conflicts between customer hardening procedures and cloud environment, R.22 risks from changes of jurisdiction, R.23 data protection risks. The results of the survey, though subjective, may facilitate the selection of controls for risk mitigation.

Next steps include the definition of a machine-readable form, possibly XML-based to represent this knowledge in suitable for automatic analysis by the tool for data protection impact assessment, and other A4Cloud tools. In the next chapter we discuss the methodology to build instances of the meta-model we introduced here.

6.5 Summary

In this chapter we provided a) a possible representation for modeling essential elements of a cloud ecosystem and various accountability relationships and b) a risk and trust model built on that representation. For modeling a cloud ecosystem we consider various cloud actors and relationships between them, such as service outsourcing and sensitive data flows in a cloud service supply chain. Furthermore, we address accountability dimension by listing controls supporting accountability and the emerging accountability relationships between cloud actors. Finally, we identified the key characteristics of risks in the cloud ecosystem, described the influencing factors and mapped between cloud ecosystem model and accountability representation to the related risks. Chapter 7 will present how to construct these models and use them in a typical risk management cycle.

7 Accountability-Based Approach for Risk Management for Cloud Ecosystems

This chapter introduces the accountability-based risk management methodology and describes the process steps based on the models from Section 5.

7.1 Modelling Methodology

Figure 29 illustrates ISO 31000 risk management process. It is taken as a reference in this work since it is the one of the most commonly used and others described in Section 2.1 contain similar steps.

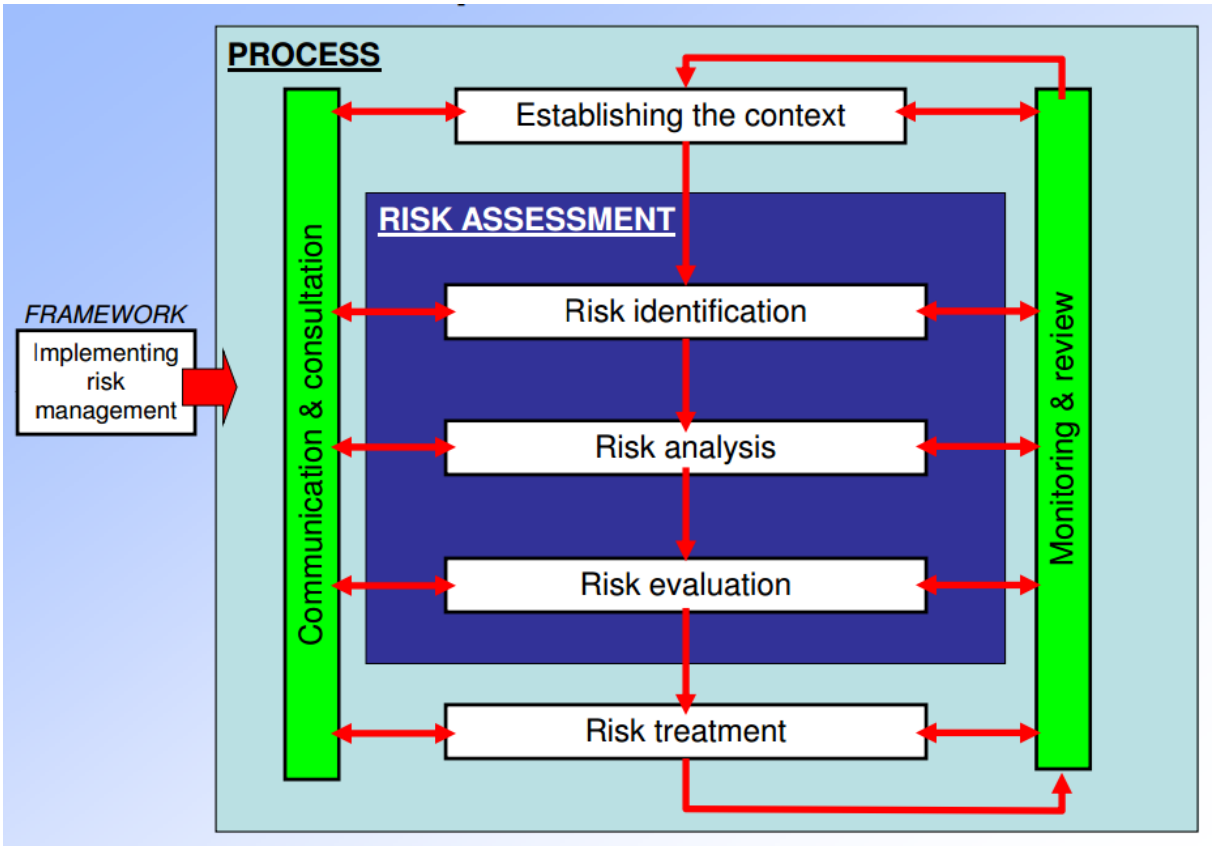

Figure 29 ISO 31000 risk management process

We also base our approach on the guide to risk assessment in the cloud described in Section 2.1.8 from CSA Security Guidance for Critical Areas of Focus in Cloud Computing (Paul Simmonds, Chris Rezek, & Archiee Reed, 2011). The approach builds on knowledge and established methodologies already reviewed in Section 2, but with the purpose of supporting cloud stakeholders in their decision making process. We develop a method to associate risks to the elements in cloud ecosystem model, to help stakeholders understand the risks, and then define appropriate mitigation actions – distributing responsibility across the chain. This will then provide a basis for defining the accountability of each player in the represented ecosystem.

The methodology we expose here enables to understand technical, governance, and security risks, to identify responsibilities and mitigation processes, and to determine follow-up actions. For instance, it is possible for CSPs to reflect responsibilities and obligations in SLAs and contracts thus addressing the economic and legal concerns discussed in Chapter 4. We do not say that all CSPs will negotiate contracts, but an accountable CSP will make clear their own duties and the manner these are carried out, and how failure to comply with policies will be remediated.

The risk assessments will also allow selecting protection mechanisms to be adopted by the CSP, but also by the cloud consumer – remark that depending on the service delivery model, some security

controls depend on the cloud consumer. Thus, the models produced in this way can be of valuable help to all stakeholders in the decision making process.

Below we present how to adapt this process for an accountability-based approach to risk management. Figure 30 links the ISO 31000 process steps to the models described in Section 5. In the scope of this report we describe the first two steps: establishing context, risk assessment and risk treatment – we will address risk monitoring and review in future deliverables due at Month 18 and Month 24. Subsequently, we will also analyze risk monitoring, in particular how the events in the cloud ecosystem change the risk and trust profiles.

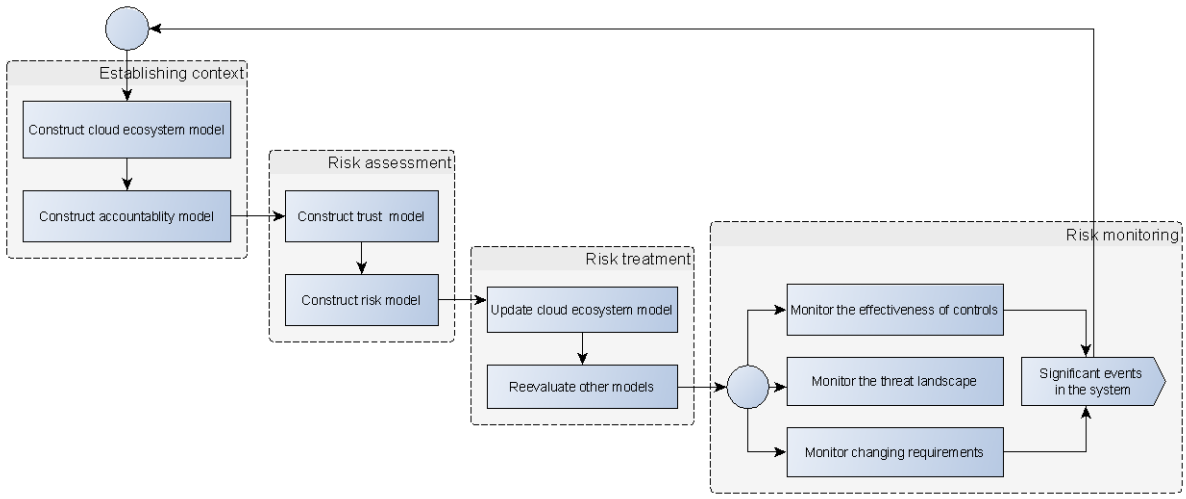

Figure 30 Accountability-based risk management process

The sections below detail each step in the process.

7.2 Establishing Context

Context can be obtained from the internal factors in the cloud customer organization or in the CSP internal factors, but also from external elements influencing the risk management parameters. We provide the detailed steps to establish context phase of ISO 31000.

7.2.1 Preliminary Steps

The preliminary steps to constructing the cloud ecosystem model are illustrated below:

1. Identify the scope and constraints
2. Identify risk and trust metrics
3. Define risk and trust criteria

The process starts with identifying the scope of the analysis (e.g. business processes to be outsourced to the cloud) and the constraints on the future cloud solution. Further, the risk and trust metrics are described, e.g. the scale of likelihood and impact of unwanted events, CSP reputation. Finally, the risk appetite of the organization is defined (i.e. what risks levels are acceptable and which must be addressed). We may provide further guidance in next deliverables for this WP on determining what the acceptable risk level for an accountable organisation is.

7.2.2 Constructing Cloud Ecosystem Model

Below we present the successive steps to build a cloud ecosystem representation in our modelling approach. The major steps are:

1. Define the actors and assets
   Firstly, we define the actors participating in the cloud service delivery chain; their geographic location and the role they play under EU data protection regulation (see Section 6.1.1).
   Secondly, we identify the assets for the concerned actors[37] (see Section 6.4.2). After identifying the type of data its value for the owning actor is determined.

2. Define possible service delivery models
   In this step we define possible service delivery models considering the solution constraints, the inherent risks associated with each of the service delivery model and the organization risk tolerance (see 6.1.2 and Section 6.4.4).

3. Define possible deployment models
   In this step we define possible service deployment models considering the solution constraints, the inherent risks associated with each of the service delivery model and the organization risk tolerance (see 6.1.2 and Section 6.4.4).

4. Define the service provisioning chain and data flows
   In this step the cloud ecosystem model representation is augmented with the data flows in the service delivery chain. Although lack of transparency may prevent us from having a representation of chains of processing, we expect the situation to evolve, as cloud providers will adhere to new standards and have fair and clear contractual clauses, making it explicit whether and which intermediary subcontractors are involved in the service provisioning.

Figure 31 below illustrates a possible graphical representation of a cloud ecosystem.

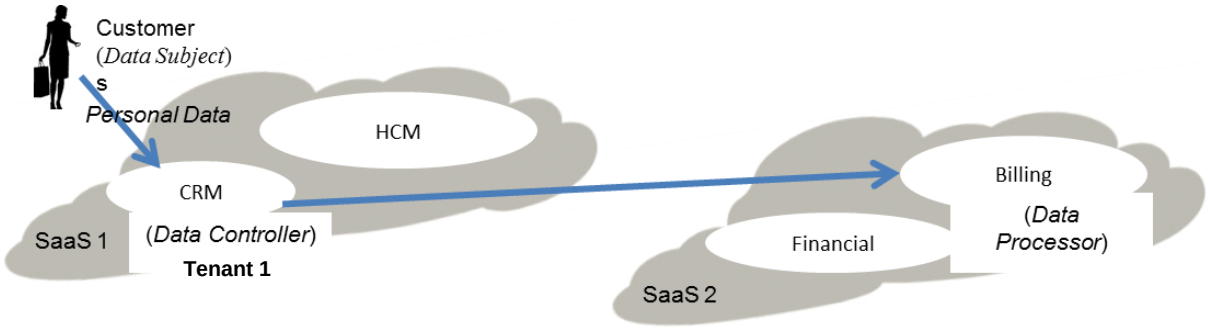

Figure 31 Example graphical representation of a cloud ecosystem

In this example, the responsible for the personal data collection is the organisation using the SaaS 1 CRM; let it be called Tenant 1. The service names, such as “CRM” or “Billing” have no specific impact on the risk analysis. We are abstracting the actual processing, and considering risks to data governance, without taking into account the exact nature of the processing in the first version of this risk modelling approach. This does not mean that we completely disregard purpose declaration and consent management for personal processing.

The cloud providers SaaS 1 and SaaS 2 are data processors, whereas Tenant 1 is the single data controller. In this step, the data flows must also be indicated. The arrows show how data is transferred across the services. Notice that SaaS 1 and SaaS 2 service provisioning may include outsourcing for platform and or infrastructure. In this case, the model can be expanded to include further actors, their roles, and the data flows.

[37] Assets are part of the risk model but are still identified as part of establishing the context.

7.2.3 Constructing Accountability Model

This activity consists of analysing the cloud ecosystem and identifying various accountability relationships between cloud actors and the implemented controls (see Section 6.2). Accountability obligations can be extracted from relevant (data protection) regulations, industry standards, SLA's, best practice recommendations, to cite a few.

In order to provide a comprehensive view on which of these security controls are implemented by a given CSP the cloud consumers can use the questionnaire from CSA Consensus Assessment Initiative[38] (CSA CAI). A precompiled repository of answers to these questions is available as CSA Security, Trust & Assurance Registry[39] (CSA STAR). There are also other catalogs of controls and questionnaires (e.g. Open Security Architecture described in Section 2.1.9) allowing to document implemented security controls, however the CSA approach seems to be most relevant for the Cloud. The major disadvantage, though, is that the used format is designed for humans, thus automatic analysis of the STAR database is not possible by a tool. Moreover, the "attributes" in CAIQ (the CAI Questionnaire) are qualitative in nature, and are not numbers.

A typical source of obtaining this information is an interview or questionnaire with the CSP, reports on the CSP's website, or 3rd party certifications, such as Service Organization Control (SOC 1-3).

Obtaining more details regarding the implemented controls (e.g. installed defense software components) is usually a challenge for a cloud consumer, but still possible for auditors (internal or external). If such detailed information is available it should be documented and properly assessed during the risk management.

7.3 Risk Assessment

After the cloud ecosystem and accountability models are created, the trust and risk models are built as part of the risk assessment. In Figure 32, the process starts with a definition of the cloud ecosystem and accountability models, as explained in Sections 6.1 and 6.2 respectively. These are provided as input to the trustworthiness assessment step, which will produce the actual trust model that will be used to the risk mapping – associating controls and mitigations with the risks, producing as outcome the risk model, and the profile with the accepted residual risks.

[38] https://cloudsecurityalliance.org/research/cai/
[39] https://cloudsecurityalliance.org/star/

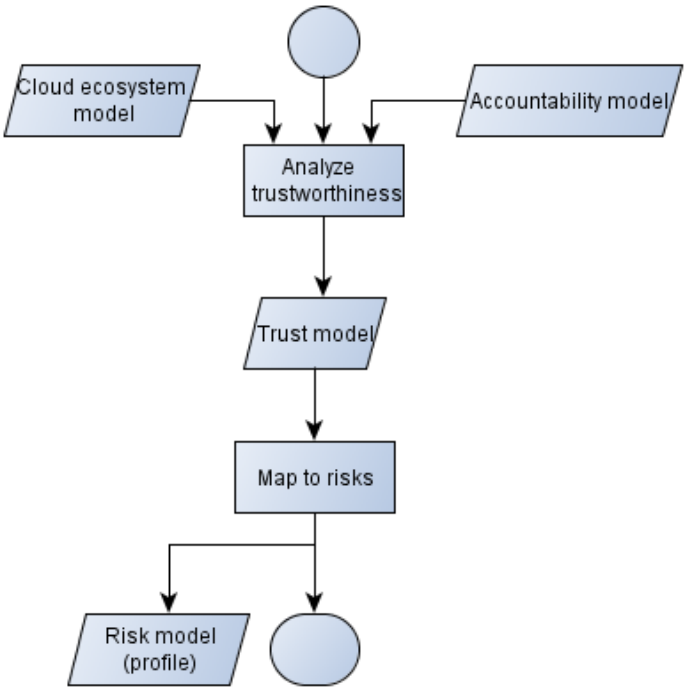

Figure 32 Risk identification and evaluation

We start by enumerating a set of common threats, based on common cloud threats identified by ENISA (ENISA, 2009). These threats are evaluated considering the cloud ecosystem model (see Section 6.4.4) and the risk is assessed by combining the likelihood (or probability) of occurrence of the threat with the impact (if such threat successfully exploits vulnerabilities and affects assets or controls). This account (risk as combination of likelihood and impact) identifies different risk levels.

Note that this classical account of risk is often debated from different multi-disciplinary perspectives (e.g. social accounts of risk). Other comments or criticisms are often concerned with the 'linearity' of the causal analysis underlying most of the risk assessment models. Our model is evolving towards a better conceptualization of accountability, risk and trust to address this point[40].

Next, we classify the relevance of each risk with respect to delivery and deployment models. We assign a qualitative indication of the probability and impact according for each risk, based on our expertise – therefore subject to our interpretation. These factors will be adjusted after the risk workshop, where we will collect input from the cloud stakeholder community on risk perception, which will bring much more reliability and relevance to this work.

For instance we define the following classification for the R1 – Lock in. For each delivery and deployment models, we define the probability of lock in, and its impact, thirdly we use this information for assigning an overall risk level.

R1. Lock in Probability				
	Public	Private	Hybrid	Community

[40] For A4Cloud internal use, refer to the work in progress in https://www.assembla.com/code/a4cloud/subversion-2/nodes/4693/StreamC/C-6%20risk%20and%20trust%20modelling/MSC6.1/Risk%20Accountability%20Trust/Accountability%20Risk%20Trust%20-%20M%20Felici.docx

SaaS	High	Low	High	High
PaaS	High	Low	High	Medium
IaaS	Low	Low	Low	Low

R1. Lock in Impact				
	Public	Private	Hybrid	Community
SaaS	High	Low	High	High
PaaS	High	Low	High	High
IaaS	High	Low	High	High

R1. Lock in Risk				
	Public	Private	Hybrid	Community
SaaS	High	Low	High	High
PaaS	High	Low	High	Medium
IaaS	Low	Low	Low	Low

The approach for risk assessment presented here is still a very basic one. We are currently defining probabilistic-based approach to assess risk and trust[41]. A second point we will need to address is how to address individual risks or how to aggregate the risks at different levels of granularity, for different stakeholders. For instance, there are about 120 or more controls in CSA CCM associated with many different risks: it is possible that one may have the same numbers of probabilities/risks, making it really difficult to take decisions.

7.4 Risk Treatment

After the risks are identified they are evaluated against the established risk criteria. Subsequently, the subset of risks that require treatment is derived and possible treatments are proposed in form of controls (see Figure 33). The risk assessment should be repeated since the introduced controls will change the risk landscape (some risks can be mitigated, but others aggravated). If the treatment is economically infeasible other alternative solutions should be investigated. The accountability model instance will then be updated, reflecting the controls and accountability attributes.

[41] For internal A4Cloud consortium use only, the interested reader can have a preview of the approach here: https://www.assembla.com/code/a4cloud/subversion-2/nodes/StreamC/C-6%20risk%20and%20trust%20modelling/Telco%20Presentations/UiSTrustRiskModel.pdf?_format=raw&rev=4693

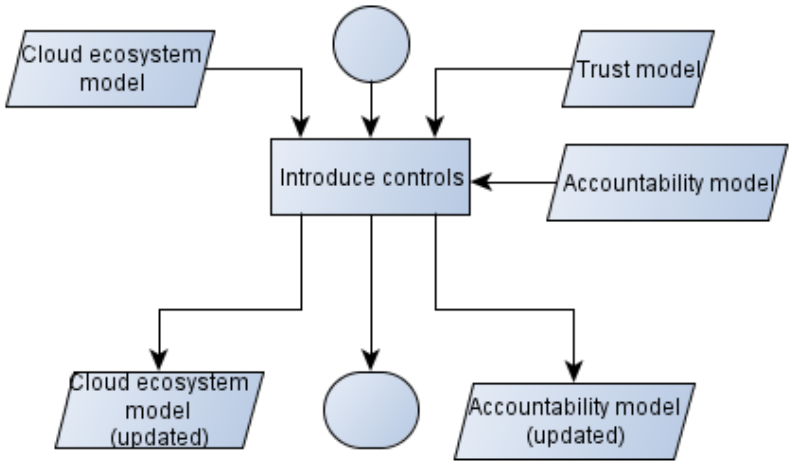

Figure 33 Risk treatment

7.5 Risk Monitoring

In order to check the effectiveness of the controls ensuring accountability and other security and compliance objectives, it is necessary to perform continuous monitoring of events that may indicated that the cloud ecosystem performs as expected, i.e. in accordance with service level agreements, privacy policies and other agreements.

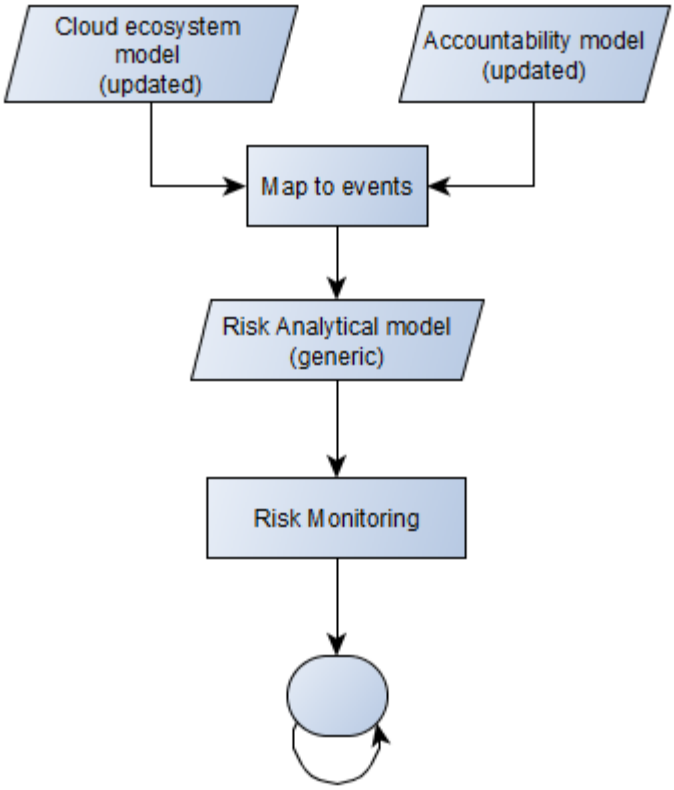

Figure 34 Risk monitoring

Obviously, disclosing such events is considered sensitive to most CSPs. We rely on a trusted third party to collect evidence and to process them in order to render information concerning potential incidents in the cloud, as well as the capacity of the CSP to prevent incidents; in an approach we call Trust as a Service (TaaS).

The actual events to be observed and monitored depend on each application and cloud ecosystem, and the process to identify them will highly benefit from the outcomes of the C5 work package on metrics see Figure 5. Here we introduce a generic model that can be applied to multiple cases. The Figure 34 illustrates the overall approach to risk monitoring. Once the representation of the cloud ecosystem and of the accountability and mitigating controls are defined, the events indicating the performance of these controls need to be identified in the cloud concrete landscape. Events indicating potentially service, security and privacy incidents need to be mapped. Actual risks levels can be computed using the service analytical model explained in Section 7.6

7.6 Joint Risk and trust model (JRTM) Trust Model[42]

Current risk assessment methods are not tailored to cloud computing: the lack of transparency on the cloud service compositions prevents the seamless application of traditional methodologies and standards. We introduce in this section a joint trust and risk model (JRTM) for federated cloud services, which abstracts the impact of risks to assets, but allows to define weights to its parameters, such that the users of the model can address specific concerns for a given use case. The model is based on historic data related not only security and privacy incidents but also performance records. The negative and positive tendencies in performances are differentiated and the freshness of the historic data is taken into account in the model. It addresses uncertainty through probability distributions and static stochastic

[42] This work has been submitted to the IEEE Transactions on Computers Journal

simulation. We obtained analytical insight into the model through the numerical analysis by Monte-Carlo simulation.

JRTM is based on the evidence about each CSP collected by a TaaS provider. Evidence is collected (i.e., counted) for periods as shown in Figure 35. The length of the periods depends on the CSP dynamics, such as the number of subscribers and services, and may vary from the order of hours to the order of weeks.

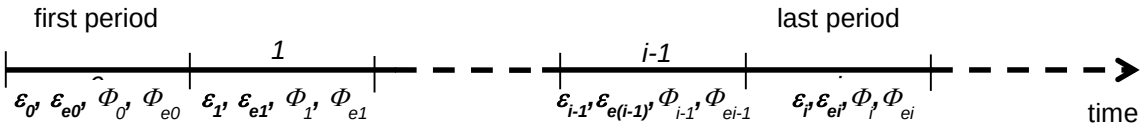

Figure 35 collecting the evidence for risks

For collecting evidence, monitoring controls and access may need to be given to TaaS providers. These controls may include areas, such as, the security of software and data stored and processed, regulatory compliance and billing. This approach (i.e., giving controls to TaaS providers) may be more practical comparing to the approach that recommends giving controls to every Cloud Customer (CC) (Khan & Malluhi, 2013), because:

- It is more secure for CSP comparing to the controls given to every CC. The probability that a TaaS provider misuses its access to compromise the security or the performance of a cloud is lower.
- TaaS provider does not need to share all the technical data with every CC. Therefore, CSP can protect both commercially and security wise sensitive data.
- CCs do not need to monitor or to control CSP for every cloud service. Instead, they take a recommendation from a third party who is an expert on this topic.
- When TaaS providers are organizations accepted by the cloud industry, they may act also as a quality assurance mechanism. Therefore, accredited certification 3rd parties can naturally become also a TaaS provider.

Moreover, JRTM is a very practical scheme that requires collection of only the following information (i.e., evidence) in every period:

- ε_i: the number of CCs who were subject to at least one security event in period *i*
- ε_{ei}: the number of CCs whose all security events were treated before they become incidents that affect the CCs in period *i*: a particular sequence of events may indicate an attack pattern in many cases, thus cloud provider must keep up to date to avoid vulnerabilities and to eliminate threats
- Φ_i: the number of CCs who were subject to at least one privacy event in period *i*
- Φ_{ei}: the number of CCs whose all privacy events were treated, eliminating the risk of such event to give rise to a privacy incident that affect the CCs in period *i*
- ρ_i: the number of CCs who were subject to at least one service event in period *i*
- ρ_{ei}: the number of CCs whose all service events are corrected before they become a service incident and hamper the operations of the CCs in period *i*
- u_i.: the total number of CCs in period i
- *D*: the set of privacy event durations (i.e., the number of time periods between the time period that a privacy event starts and the time period that the privacy event is detected)

As implied by the evidence collected and definitions, JRTM distinguishes three types of risks: security, privacy and service. Privacy has a difference from the other two. It is very likely that a privacy

event is not detected when it is initiated. It is even probable that some privacy events may never be detected because their effect is not directly observable. On the other hand, the potential damage of a privacy event is higher when its duration is longer. Therefore, we collect evidence about privacy event durations and address this issue within our model. However, we cannot take undetected privacy events into account not only because they are not measurable but also because the recommendations by a TaaS provider cannot be based on speculations but evidence.

7.7 Computing Risk and Trust

In JRTM, risk and trust are modeled jointly by using the events mentioned in the previous section. The real risk is the risk that cannot be (or is not) eliminated by the CSP. If the part of the security risk δ_ε, privacy risk δ_Φ and the service risk δ_ρ not eliminated by the CSP is lower than what the CC can take (i.e., τ_ε, τ_Φ *and* τ_ρ), then the cloud service is viable for the CC. We further elaborate on this relation at the end of this section. As shown in Equations 1, 2 and 3, we perceive the risk as the probabilities r_ε, r_Φ, and r_ρ that a security, privacy or service event occurs, and trust as the probabilities t_ε, t_Φ and t_ρ that the CSP can eliminate the risks before they become security, privacy or service incidents.

$$\delta_\varepsilon = r_\varepsilon - (r_\varepsilon \times t_\varepsilon), \quad (1)$$

$$\delta_\phi = r_\phi - (r_\phi \times t_\phi), \quad (2)$$

$$\delta_\rho = r_\rho - (r_\rho \times t_\rho). \quad (3)$$

This approach to model risk fits well for the dynamics in cloud computing because of two reasons: Firstly, it does not require that the TaaS provider assesses the consequence for the occurrence of a risk, which is very much dependent on the CCs' functions. Instead, the consequences are represented by the thresholds τ_ε, τ_Φ *and* τ_ρ given by the CCs. We discuss the selection of thresholds in Section 3.3. Secondly, it does not need to assess all threats and vulnerabilities. For a TaaS provider or CC, it is not practical to list all threats and vulnerabilities because it is not likely that CSP will share all the details about their physical architecture, platforms and security systems with public, their CCs or even with TaaS providers.

The periodical data related to risks r_ε, r_Φ,and r_ρ can be weighted based on their freshness as given by Equations 4, 5 and 6. *R* in Equations 4, 5 and 6 is a random variable based on the probability distribution functions derived from the statistical analysis of the observations on security, privacy and service events. The period *i* is the latest period, and $r_{\varepsilon(i)}$, $r_{\Phi(i)}$ and $r_{\rho(i)}$ are the current risk assessments for security, privacy and service respectively. The security, privacy and service event ratios (i.e., $s=\varepsilon/u$, $p=\Phi/u$ and $g=\rho/u$) are fit to a distribution and statistics (i.e., shape, scale and location parameters), and this analysis for distribution and the statistics is repeated at the end of every period. The random processes *R(s)*, *R(p)* and *R(g)* use these distributions and statistics.

$$r_{\varepsilon(i)} = (1-\omega)R(s) + \omega\frac{\varepsilon_i}{u_i}, \quad (4)$$

$$r_{\phi(i)} = (1-\omega)R(p) + \omega\frac{\phi_i}{u_i}, \quad (5)$$

$$r_{g(i)} = (1-\omega)R(g) + \omega\frac{\rho_i}{u_i}. \quad (6)$$

The parameter ω in Equations 4, 5 and 6 is the weight parameter, and can be given any value between 0 and 1 including 0 and 1 (i.e., $\{\omega \in \Re \mid 0 \le \omega \le 1\}$) . The higher ω implies the lower level of uncertainty and the higher level of influence by the statistics in the last period. When it is 1, risk is determined based on the frequency of the incidents in the last period and there is not any uncertainty for the end result. When it is 0, risk is completely random according to the distribution and the statistics

of the observations. Please note that the distribution and statistics in *R(s), R(p)* and *R(g)* include also the data from the last period.

Trust parameters t_{ε}, t_{Φ} and t_{ρ} consists of two parts, i.e., hard $t_{\varepsilon h}$, $t_{\Phi h}$, $t_{\rho h}$ and soft $t_{\varepsilon S}$, $t_{\Phi S}$, $t_{\rho S}$, as shown in Equations (7), (8) and (9). Hard part of trust is based on the architecture (i.e., the security systems and capacity) of the CSP and the content of SLA. Therefore, it is mostly related to evidence, and we calculate it purely based on the performance of CSP. On the other hand, soft trust is sensitive to the latest incidents and more sensitive to negative incidents comparing to positive incidents. Typically trust and reputation are built slowly but can be lost very quickly. We capture this relation through Equations 7 to 15.

$$t_{\varepsilon} = \begin{cases} 0, & if\ t_{\varepsilon h} + t_{\varepsilon s} < 0; \\ 1, & if\ t_{\varepsilon h} + t_{\varepsilon s} > 1; \\ t_{\varepsilon h} + t_{\varepsilon s}, & otherwise. \end{cases} \quad (7)$$

$$t_{\phi} = \begin{cases} 0, & if\ t_{\phi h} + t_{\phi s} < 0; \\ 1, & if\ t_{\phi h} + t_{\phi s} > 1; \\ t_{\phi h} + t_{\phi s}, & otherwise. \end{cases} \quad (8)$$

$$t_{\rho} = \begin{cases} 0, & if\ t_{\rho h} + t_{\rho s} < 0; \\ 1, & if\ t_{\rho h} + t_{\rho s} > 1; \\ t_{\rho h} + t_{\rho s}, & otherwise. \end{cases} \quad (9)$$

Hard trust is measured similar to risk. In Equations (10), (11) and (12), ε_{ei}, Φ_{ei} and ρ_{ei} is the number of subscribers whose all security, privacy and service events are treated [43]before they become incidents respectively at period *i*. Random variable *R* generates random numbers according to the distributions and statistics of the ratios between the number of eliminated security events and total number of security events (i.e., $s_e=\varepsilon_e/\varepsilon$), the number of eliminated privacy events and total number of privacy events (i.e., $p_e=\Phi_e/\Phi$) and between the number of eliminated service events and the total number of service events (i.e., $g_e=\rho_e/\rho$). In Equation (11), we have another random variable *R(D)*, which is assigning random values distributed according to the distributions and statistics of the values in privacy event duration set *D*.

$$t_{\varepsilon h(i)} = (1-\omega)R(s_e) + \omega\frac{\varepsilon_{ei}}{\varepsilon_i}. \quad (10)$$

$$t_{\phi h(i)} = \left((1-\omega)R(p_e) + \omega\frac{\phi_{ei}}{\phi_i}\right)^{R(D)}. \quad (11)$$

$$t_{\rho h(i)} = (1-\omega)R(g_e) + \omega\frac{\rho_{ei}}{\rho_i}. \quad (12)$$

Soft parts of trust $t_{\varepsilon S(i)}$, $t_{\Phi S(i)}$ and $t_{\rho S(i)}$ are calculated based on the change in the performance of CSP. In Equations (13), (14) and (15), the slope value γ is a positive real number larger than or equal to one (i.e., $\{\gamma \in \Re \mid \gamma \geq 1\}$) and represents the relation of trust with the negative/positive change (i.e., trend) in performance. If the performance of the CSP gets worse, the CSP loses its credibility quickly. The

[43] Sometimes we will say an event was "eliminated" meaning that an event that is a premise to an incident was diligently managed by the CSP, eliminating the possibility to concretize an incident.

sharpness of the drop in trust is related to the slope value γ. On the other hand, it takes more effort and time to gain trust as captured by Equations (13), (14) and (15).

$$d_{\varepsilon(i)} = \frac{\varepsilon_{ei}}{\varepsilon_i} - \frac{\varepsilon_{e(i-1)}}{\varepsilon_{i-1}};$$

$$d_{\phi(i)} = \frac{\phi_{ei}}{\phi_i} - \frac{\phi_{e(i-1)}}{\phi_{i-1}};$$

$$d_{\rho(i)} = \frac{\rho_{ei}}{\rho_i} - \frac{\rho_{e(i-1)}}{\rho_{i-1}};$$

$$t_{\varepsilon s(i)} = \begin{cases} d_{\varepsilon(i)}^{\gamma}, & if\ d_{\varepsilon(i)} \geq 0; \\ -\sqrt[\gamma]{|d_{\varepsilon(i)}|}, & if\ d_{\varepsilon(i)} < 0; \end{cases} \quad (13)$$

$$t_{\phi s(i)} = \begin{cases} d_{\phi(i)}^{\gamma}, & if\ d_{\phi(i)} \geq 0; \\ -\sqrt[\gamma]{|d_{\phi(i)}|}, & if\ d_{\phi(i)} < 0; \end{cases} \quad (13)$$

$$t_{\rho s(i)} = \begin{cases} d_{\rho(i)}^{\gamma}, & if\ d_{\rho(i)} \geq 0; \\ -\sqrt[\gamma]{|d_{\rho(i)}|}, & if\ d_{\rho(i)} < 0. \end{cases} \quad (15)$$

Equations (1), (2) and (3) are for a single service risk. Since cloud service ecosystem, also called here service mashups consist of multiple services, we need to extend them for multiple services. In Equations (16), (17) and (18), *S, P* and *G* are the expected overall security, privacy and service risk (i.e., the risk that cannot be eliminated by the CSP) for cloud service mashups respectively. The number of services in a mashup is *n*, and a_k is the number of alternative services available for service *k* in the inter-cloud (all the clouds that can be accessed for this service). It is trivial to see at Equation (16) and (17) that the higher the number of services composes a mashup, the higher the security and privacy risks become. The same relation can also be observed at Equation (18) with a difference: the higher number of alternatives decreases the service risk. We examine these relations more detailed in Section 4.

$$S = 1 - \prod_{k=1}^{n} (1 - \delta_{\varepsilon k}); \quad (16)$$

$$P = 1 - \prod_{k=1}^{n} (1 - \delta_{\phi k}); \quad (17)$$

$$G = 1 - \prod_{k=1}^{n} (1 - \prod_{m=1}^{a_k} \delta_{\rho km}) \ . \quad (18)$$

Since *S, P* and *G* are stochastic processes, their results are not deterministic (i.e., includes uncertainty through random variables). Therefore, a TaaS using our model first needs to build confidence intervals for *S, P* and *G* (i.e., *u(S)<S<v(S)*, *u(P)<P<v(P)* and *u(G)<G<v(G)*) according to the confidence level λ given by the CC. For this, static Monte-Carlo simulation can be used. We follow this approach in our statistical analysis experiments, detailed in Appendix D. Our experimentation validates that our model is aligned with the perception of risks and trust as explained in first chapters of this deliverable.

It differentiates the negative performance from the positive performance in risk assessment based on the cloud customer risk profile. It also takes into account the freshness of the data about the performance of the CSP again according to the parameters specified by the CCs. The model is simple enough to be

practical for a TaaS used for cloud service ecosystems. A detailed discussion on the experimental results is given in Appendix D.

7.8 Summary

In this section we discussed how organizations can integrate the A4Cloud approach to risk analysis, assessment, and monitoring to their risk management frameworks towards a strengthened accountability in particular in the processing of personal data in the cloud. The approach will be useful to guide the data collection phase for data protection impact assessments of cloud ecosystem, and also in defining the strategy for the continuous monitoring of risk levels in the cloud.

8 Conclusions

We reported here the results of tasks T:C-6.1 – definition of the risk and trust models and T:C-6.2 modelling cloud infrastructures and controls, creating, respectively – machine-readable representations for risk and trust, and Models for cloud infrastructures and controls. Our review of the state of the art identified the lack of unified abstract models for risk analysis and for trust among the different cloud stakeholders, for whom we also discussed socio-economic and legal concerns. A model to allow the comprehension of accountability, risk, and trust is essential to gather information for risk-based business decisions – in supplier selection and negotiation of appropriate contracts for the context (still not possible today in most of the cases), for instance.

Moreover, representing cloud controls and accountability relationships will enable much more precise data protection impact assessments, which is the main purpose of the tool we will prototype in the next task, T:C-6.3. The prototyping activity will also trigger refinements and updates to the meta-models introduced here.

Below we provide an evaluation of the achievements so far with respect to the requirements from Chapter 1:

T:C-6.1 Definition of the risk and trust models	
REQ (Representing stakeholders assets) Capture each stakeholder's assets, specifically personal and business sensitive data.	Our Model support representation of the full chain with the data flows, thus the assets handled in the cloud.
REQ (Modelling trust relationships) Provide a representation usable for modelling of trust relationships and delegations in the cloud supply chain.	The trust model is able to capture the trust relationships, as shown in Chapter 5.
REQ (Separate risk profiles) to allow for the creation of separate risk profiles for different stakeholders: cloud consumers, cloud providers, cloud brokers, when performing their risk assessments.	All profiles are captured according to their role in the service chain and to the EU Data Protection regulatory framework. Risks are then analysed according to the responsibilities for that stakeholder and roles.
REQ (Represent vulnerabilities and threats) Be able to represent explicitly in the risk and trust models specific vulnerabilities and threats	Technical and other threats are properly representable.
T:C-6.2 Modelling cloud infrastructures and controls	
REQ (Modelling cloud environments) Encapsulate cloud and accountability concepts (main parties, deployments model, service supply chains, security (accountability) controls).	This is the foundation of the model, as we can represent service and delivery models
REQ (Machine-readable representation) Provide machine-readable representations amenable to automated treatment by tools.	Our graph-like representation will have an XML schema for storing and updating descriptions. To be integrated in the tool in the next tasks.
REQ (Dynamic risk monitoring) Associate risk analysis with event monitoring in order to determine impact and the risk thresholds in different cloud landscapes. Constantly update the risk and trust model based on the new events.	We introduced a joint risk and trust model, which permits to continuously analyse events from the cloud ecosystem, in a privacy preserving manner, in order to evaluate cloud service reputation. The experimental results demonstrate the models fitness to our objectives. The next steps consist in interaction with the WPs

	C5 – metrics and C-8 evidence, to identify how events can be fed into our model.
T:C-6.3 Data protection impact assessment tool	
REQ (Impact assessment) Assess the impact of specific events from cloud environment (using accountability metrics from WP:C-5).	Our analytical model allows cloud customers and providers to continuously measure risk and trust levels. From C5, we need to understand which specific events need to be monitored for each specific service ecosystem.
REQ (Risk estimation) Estimate the risk levels	The Data Protection Impact Assessment Tool (DPIAT) tool will be able to give qualitative risk evaluations. Our analytical model can give more precise measures.
REQ (Facilitate CP selection) Facilitate the selection of a Cloud Provider matching customer's business needs and risk profile.	The DPIAT tool will cover this requirement, as privacy impact assessments are likely become mandatory in the near future.
REQ (Support contractual negotiations) Support the negotiations of contract terms and SLAs based on the risk profile.	We will work closely with D4 (Contracts, SLA's, remediation), on the integration of data protection impact assessments with the tools for contracts.
T:C-6.3 Use cases risk and trust assessment	
REQ (Applicability to Business Use Cases) the models must support realistic use cases, composed of multiple cloud service providers, as defined in WP:B-3	This task starts on Month 19.

References

Abawajy, J. (2009). Determining Service Trustworthiness in Intercloud Computing Environments. In *2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN)* (pp. 784 –788). doi:10.1109/I-SPAN.2009.155

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor." (n.d.).

Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2012). *Cloud Computing Synopsis and Recommendations* (No. 800-146). NIST.

Banaei-Kashani, F., Chen, C.-C., & Shahabi, C. (2004). Wspds: Web services peer-to-peer discovery service. In *Proceedings of the International Conference on Internet Computing* (pp. 733–743).

Beck, U. (1992). From Industrial Society to the Risk Society: Questions of Survival, Social Structure and Ecological Enlightenment. *Theory, Culture & Society*, *9*(1), 97–123. doi:10.1177/026327692009001006

Beldad, A. D. (2011). *Trust and information privacy concerns in electronic government*. University of Twente.

Bennett, C. J. (2006). *The governance of privacy: policy instruments in global perspective* (2nd and updated ed.). Cambridge, Mass: MIT Press.

Bernsmed, K., Felici, M., Santana De Oliveira, A., Sendor, J., Brede Moe, N., Rübsamen, T., … Hasnain, B. (2013). *Use Case Descriptions* (Deliverable No. D:B-3.1) (p. 68). A4Cloud.

Bianculli, D., Binder, W., Drago, L., & Ghezzi, C. (2008). Transparent Reputation Management for Composite Web Services (pp. 621–628). IEEE. doi:10.1109/ICWS.2008.39

Blaze, M., Feigenbaum, J., & Lacy, J. (1996). Decentralized trust management (pp. 164–173). IEEE Comput. Soc. Press. doi:10.1109/SECPRI.1996.502679

Bowles, J. B., & Peláez, C. E. (1995). Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis. *Reliability Engineering & System Safety*, *50*(2), 203–213. doi:10.1016/0951-8320(95)00068-D

Brunette, G., & Mogull, R. (2009). Security Guidance for critical areas of focus in Cloud Computing V2. 1. *CSA (Cloud Security Alliance), USA. Online: Http://www. Cloudsecurityalliance. Org/guidance/csaguide. v2*, *1*.

Castelfranchi, C., & Falcone, R. (2010). *Trust theory: a socio-cognitive and computational model*. Chichester, West Sussex, U.K: J. Wiley.

Catteddu, D., Massimo Felici, Giles Hogben, Christopher Millard, Nick Papanikolaou, Siani Pearson, … Chris Reed. (2013). *MSC-2.2 Initial Conceptual Framework* (A4Cloud Milestone Report). A4Cloud.

Cayirci, E. (2013). A Joint Trust and Risk Model for MSaaS Mashups. In *Proceedings of the 2013 Winter Simulation Conference*. Piscataway, New Jersey: R. Pasupathy, S.-H. Kim, A. Tolk, R. Hill, and M. E. Kuhl.

Cerbo, F., Bezzi, M., Kaluvuri, S. P., Sabetta, A., Trabelsi, S., & Lotz, V. (2012). Towards a Trustworthy Service Marketplace for the Future Internet. In F. Álvarez, F. Cleary, P. Daras, J. Domingue, A. Galis, A. Garcia, … T. Zahariadis (Eds.), *The Future Internet*

(Vol. 7281, pp. 105–116). Berlin, Heidelberg: Springer Berlin Heidelberg. Retrieved from http://www.springerlink.com/index/10.1007/978-3-642-30241-1_10

Chang, E. (2006). *Trust and reputation for service-oriented environments: technologies for building business intelligence and consumer confidence*. Chichester, England ; Hoboken, NJ: John Wiley & Sons Inc.

Cherrueau, R.-A., Douence, R., Grall, H., Royer, J.-C., Sellami, M., Sudholt, M., … Bernsmed, K. (2013). *Policy Representation Framework* (Deliverable No. D34.1) (p. 92). A4Cloud.

Cofta, P. (2007). *Trust, complexity and control confidence in a convergent world*. Chichester, England; Hoboken: John Wiley & Sons. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=208376

CSA Cloud Security Alliance. (2012). *Top Ten Big Data Security and Privacy Challenges*. CSA.

CSA Cloud Security Alliance. (2013a). *The Notorious Nine: Cloud Computing Top Threats in 2013*. Top Threats Working Group.

CSA Cloud Security Alliance. (n.d.). *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0*. 2011: CSA.

CSA Cloud Security Alliance, C. S. (2013b). *Cloud Controls Matrix V3.0 Draft*. Cloud Security Alliance.

Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research*, 119–134.

ENISA. (2009). *Cloud Computing: Benefits, risks and recommendation for information security*.

ENISA. (2013). *Threat Landscape 2013 - Overview of current and emerging cyber-threats*. European Network and Information Security Agency.

Farmer, F. R., & Glass, B. (2010). *Building Web reputation systems* (1st ed.). Sebastopol, CA: O'Reilly.

Felici, M. (2012). How to Trust: A Model for Trust Decision Making. *International Journal of Adaptive, Resilient and Autonomic Systems*, *3*(3), 20–34. doi:10.4018/jaras.2012070102

Felici, M., Pearson, S., & Koulouris, T. (2013). Accountability for Data Governance in Cloud Ecosystems. In *CloudCom*.

Fulmer, C. A., & Gelfand, M. J. (2012). At What Level (and in Whom) We Trust: Trust Across Multiple Organizational Levels. *Journal of Management*, *38*(4), 1167–1230. doi:10.1177/0149206312439327

Giorgini, P., Massacci, F., & Zannone, N. (2005). Security and Trust Requirements Engineering. In A. Aldini, R. Gorrieri, & F. Martinelli (Eds.), *Foundations of Security Analysis and Design III* (Vol. 3655, pp. 237–272). Berlin, Heidelberg: Springer Berlin Heidelberg. Retrieved from http://www.springerlink.com/index/10.1007/11554578_8

Guagnin, D. (2012). *Managing privacy through accountability*. Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan.

Habib, S. M., Ries, S., & Muhlhauser, M. (2010). Cloud Computing Landscape and Research Challenges Regarding Trust and Reputation. In *2010 7th International Conference on*

Ubiquitous Intelligence Computing and 7th International Conference on Autonomic Trusted Computing (UIC/ATC) (pp. 410 –415). doi:10.1109/UIC-ATC.2010.48

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM*, *42*(4), 80–85. doi:10.1145/299157.299175

Hon, W. K., Millard, C., & Walden, I. (2012). Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now. *SSRN eLibrary*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2055199

ISO IEC. (2012). *Information technology — Security techniques — Information security management systems — Overview and vocabulary* (International Standard No. ISO/IEC 27000) (p. 32).

Jansen, W., & Grance, T. (2011). *Guidelines on Security and Privacy in Public Cloud Computing* (No. 800-144). (U. S. D. of Commerce, Trans.). National Institute of Standards and Technology.

Jsang, A., & Ismail, R. (2002). The beta reputation system. In *Proceedings of the 15th bled electronic commerce conference* (pp. 41–55).

Kaliski,Jr., B. S., & Pauley, W. (2010). Toward Risk Assessment As a Service in Cloud Environments. In *Proceedings of the 2Nd USENIX Conference on Hot Topics in Cloud Computing* (pp. 13–13). Berkeley, CA, USA: USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=1863103.1863116

Kamvar, S. D., Schlosser, M. T., & Garcia-Molina, H. (2003). The Eigentrust algorithm for reputation management in P2P networks (p. 640). ACM Press. doi:10.1145/775152.775242

Kandukuri, B. R., V., R. P., & Rakshit, A. (2009). Cloud Security Issues (pp. 517–520). IEEE. doi:10.1109/SCC.2009.84

Khan, K. M., & Malluhi, Q. (2013). Trust in Cloud Services: Providing More Controls to Clients. *Computer*, *46*(7), 94–96. doi:10.1109/MC.2013.254

Ko, R. K. L., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., & Lee, B. S. (2011). TrustCloud: A Framework for Accountability and Trust in Cloud Computing. Presented at the 2nd IEEE Cloud Forum for Practitioners (ICFP), IEEE Computer Society.

Landoll, D. J. (2011). *The security risk assessment handbook a complete guide for performing security risk assessments, second edition*. Boca Raton, Fla.: CRC Press. Retrieved from http://proxy.uqtr.ca/login.cgi?action=login&u=uqtr&db=books24x7&ezproxy=1&ezurl=http://library.books24x7.com/library.asp?%5EB&bookid=37005

Lee, A. J., Winslett, M., & Perano, K. J. (2009). TrustBuilder2: A Reconfigurable Framework for Trust Negotiation. In E. Ferrari, N. Li, E. Bertino, & Y. Karabulut (Eds.), *Trust Management III* (Vol. 300, pp. 176–195). Berlin, Heidelberg: Springer Berlin Heidelberg. Retrieved from http://www.springerlink.com/index/10.1007/978-3-642-02056-8_12

Lee, K., Jeon, J., Lee, W., Jeong, S.-H., & Park, S. (2003). *Qos for web services: Requirements and possible approaches* (No. 25) (pp. 1–9). W3C. Retrieved from http://www.w3c.or.kr/kr-office/TR/2003/ws-qos/

Lee, W. S., Grosh, D. L., Tillman, F. A., & Lie, C. H. (1985). Fault Tree Analysis, Methods, and Applications ߝ A Review. *IEEE Transactions on Reliability*, *R-34*(3), 194–203. doi:10.1109/TR.1985.5222114

Leenes, R., & Oomen, I. (2009). The Role of Citizens: What Can Dutch, Flemish and English Students Teach Us About Privacy? In S. Gutwirth, Y. Poullet, P. Hert, C. Terwangne, & S. Nouwt (Eds.), *Reinventing Data Protection?* (pp. 139–153). Dordrecht: Springer Netherlands. Retrieved from http://www.springerlink.com/index/10.1007/978-1-4020-9498-9_8

Limam, N., & Boutaba, R. (2010). Assessing Software Service Quality and Trustworthiness at Selection Time. *IEEE Transactions on Software Engineering*, *36*(4), 559–574. doi:10.1109/TSE.2010.2

Lin, A., & Chen, N.-C. (2012). Cloud computing as an innovation: Percepetion, attitude, and adoption. *International Journal of Information Management*, *32*(6), 533–540. doi:10.1016/j.ijinfomgt.2012.04.001

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., & Badger, L. (2011). NIST Cloud Computing Reference Architecture-Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*.

Liu, Y., Ngu, A. H., & Zeng, L. Z. (2004). QoS computation and policing in dynamic web service selection (p. 66). ACM Press. doi:10.1145/1013367.1013379

Lowrance, W. W. (1976). Of Acceptable Risk: Science and the Determination of Safety.

Marsh, S. P. (1994). *Formalising Trust as a Computational Concept*. University of Stirling.

Marshall, C., & Tang, J. C. (2012). That syncing feeling: early user experiences with the cloud (p. 544). ACM Press. doi:10.1145/2317956.2318038

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review*, *20*(3), 709–734. doi:10.5465/AMR.1995.9508080335

McKnight. (2005). Trust in Information Technology. In *The Blackwell encyclopedia of management* (Vol. 7, pp. 329–331). Malden, MA: Blackwell Pub.

McKnight, D., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *The Journal of Strategic Information Systems*, *11*(3-4), 297–323. doi:10.1016/S0963-8687(02)00020-3

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research*, *13*(3), 334–359. doi:10.1287/isre.13.3.334.81

Nemati, H. R., & Van Dyke, T. (2009). Do Privacy Statements Really Work? The Effect of Privacy Statements and Fair Information Practices on Trust and Perceived Risk in E-Commerce: *International Journal of Information Security and Privacy*, *3*(1), 45–64. doi:10.4018/jisp.2009010104

Niall Browne, Susanna Space. (2010). *Evaluating Cloud Risk for the Enterprise: A Shared Assessments Guide*. Shared Assessments. Retrieved from http://www.sharedassessments.org/media/pdf-EnterpriseCloud-SA.pdf%E2%80%8E

NIST. (2010). *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (No. SP 800-37). NIST.

NIST. (2012). *Guide for Conducting Risk Assessments* (No. SP 800-30 rv 1). NIST.

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, *25*(2), 243–262. doi:10.1016/S0167-4870(02)00172-1

Osterwalder, D. (2001). Trust Through Evaluation and Certification? *Social Science Computer Review*, *19*(1), 32–46. doi:10.1177/089443930101900104

Paul Simmonds, Chris Rezek, & Archiee Reed. (2011). *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0* (No. 3.0) (p. 177). Cloud Security Alliance. Retrieved from http://www.cloudsecurityalliance.org/guidance/

Pawar, P. S., Rajarajan, M., Dimitrakos, T., & Zisman, A. (2013). Trust Model for Cloud Based on Cloud Characteristics. In C. Fernández-Gago, F. Martinelli, S. Pearson, & I. Agudo (Eds.), *Trust Management VII* (Vol. 401, pp. 239–246). Berlin, Heidelberg: Springer Berlin Heidelberg. Retrieved from http://link.springer.com/10.1007/978-3-642-38323-6_18

Pearson, S. (2012). Privacy, Security and Trust in Cloud Computing. In S. and Y. Pearson (Ed.), *Privacy and Security for Cloud Computing*. Springer.

Phaphoom, N., Oza, N., Wang, X., & Abrahamsson, P. (2012). Does cloud computing deliver the promised benefits for IT industry? (p. 45). ACM Press. doi:10.1145/2361999.2362007

Rashidi, A., & Movahhedinia, N. (2012). A Model for User Trust in Cloud Computing. *International Journal on Cloud Computing: Services and Architecture*, *2*(2), 1–8.

Renn, O., Klinke, A., & Asselt, M. (2011). Coping with Complexity, Uncertainty and Ambiguity in Risk Governance: A Synthesis. *AMBIO*, *40*(2), 231–246. doi:10.1007/s13280-010-0134-0

Resnick, P., Kuwabara, K., Zeckhauser, R., & Friedman, E. (2000). Reputation systems. *Communications of the ACM*, *43*(12), 45–48. doi:10.1145/355112.355122

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). NOT SO DIFFERENT AFTER ALL: A CROSS-DISCIPLINE VIEW OF TRUST. *Academy of Management Review*, *23*(3), 393–404. doi:10.5465/AMR.1998.926617

Ryan, P., & Falvey, S. (2012). Trust in the clouds. *Computer Law & Security Review*, *28*(5), 513–521. doi:10.1016/j.clsr.2012.07.002

Sabater-Mir, J., & Paolucci, M. (2007). On representation and aggregation of social evaluations in computational trust and reputation models. *International Journal of Approximate Reasoning*, *46*(3), 458–483. doi:10.1016/j.ijar.2006.12.013

Saripalli, P., & Walters, B. (2010). QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security (pp. 280–288). IEEE. doi:10.1109/CLOUD.2010.22

Savola, R. M., Juhola, A., & Uusitalo, I. (2010). Towards wider cloud service applicability by security, privacy and trust measurements (pp. 1–6). IEEE. doi:10.1109/ICAICT.2010.5612067

Seamons, K. E., Chan, T., Child, E., Halcrow, M., Hess, A., Holt, J., … Lina Yu. (2003). TrustBuilder: negotiating trust in dynamic coalitions (Vol. 2, pp. 49–51). IEEE Comput. Soc. doi:10.1109/DISCEX.2003.1194912

Silva, P. F., Westphall, C. B., Mattos, M. M., & Santos, D. R. dos. (n.d.). An Architecture for Risk Analysis in Cloud. In *n proceeding of: Tenth International Conference on Networking and Services*. IARIA.

Singh, S., & Morley, C. (2009). Young Australians' privacy, security and trust in internet banking (p. 121). ACM Press. doi:10.1145/1738826.1738846

Sjoberg, L., & Fromm, J. (2001). Information Technology Risks as Seen by the Public. *Risk Analysis*, *21*(3), 427–442. doi:10.1111/0272-4332.213123

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality. *Risk Analysis*, *24*(2), 311–322. doi:10.1111/j.0272-4332.2004.00433.x

Sotto, L. J., Treacy, B. C., & McLellan, M. L. (2010). Privacy and Data Security Risks in Cloud Computing. *World Communications Regulation Report*, *5*(2), 38.

Squicciarini, A., Bertino, E., Ferrari, E., Paci, F., & Thuraisingham, B. (2007). PP-trust-X: A system for privacy preserving trust negotiations. *ACM Transactions on Information and System Security*, *10*(3), 12–es. doi:10.1145/1266977.1266981

Stone, greg, & Noel, P. (2012). *Cloud Risk Decision Framework: Principles & risk-based decisionmaking for cloud-based computing derived from ISO 31000*. Microsoft. Retrieved from http://download.microsoft.com/documents/australia/enterprise/SMIC1545_PDF_v7_pdf.pdf

Tzoannos, S., Dalianis, T., Brown, R., Luna, J., Mantzoukas, K., Sellami, M., … Koulouris, T. (2013). *D:D-2.1 Architecture guidelines and principles* (Deliverable No. D-42.1) (p. 47). A4Cloud.

Vu, L.-H., Hauswirth, M., & Aberer, K. (2006). Towards P2P-Based Semantic Web Service Discovery with QoS Support. In C. J. Bussler & A. Haller (Eds.), *Business Process Management Workshops* (Vol. 3812, pp. 18–31). Berlin, Heidelberg: Springer Berlin Heidelberg. Retrieved from http://www.springerlink.com/index/10.1007/11678564_3

Wang, Yan, & Lin, K.-J. (2008). Reputation-Oriented Trustworthy Computing in E-Commerce Environments. *IEEE Internet Computing*, *12*(4), 55–59. doi:10.1109/MIC.2008.84

Wang, Yao, & Vassileva, J. (2007). Toward trust and reputation based web service selection: A survey. *International Transactions on Systems Science and Applications*, *3*(2), 118–132.

Appendices

A. ENISA Cloud Computing Risks

Table 11 ENISA risk categories

Policy and Organizational	Includes governance and compliance risks, and others related to choice of provider, lock in, and to organizational processes
Technical	This category contains risks such as isolation failure, resource exhaustion, and data leakages
Legal	Relates to licensing, subpoena and jurisdictional issues
Other technical risks not specific to the cloud	Contains all IT risks that affect, but which are not particular to cloud computing

Table 12 ENISA risks

Risk	**Category**
R.1 lock-in	Policy and Organizational
R.2 loss of governance	Policy and Organizational
R.3 compliance challenges	Policy and Organizational
R.4 loss of business reputation due to co-tenant activities	Policy and Organizational
R.5 cloud service termination or failure	Policy and Organizational
R.6 cloud provider acquisition	Policy and Organizational
R.7 supply chain failure	Policy and Organizational
R.8 resource exhaustion (under or over provisioning)	Technical
R.9 isolation failure	Technical
R.10 cloud provider malicious insider - abuse of high privilege roles	Technical

R.11 management interface compromise (manipulation, availability of infrastructure)	Technical
R.12 intercepting data in transit	Technical
R.13 data leakage on up/download, intra-cloud	Technical
R.14 insecure or ineffective deletion of data	Technical
R.15 distributed denial of service (ddos)	Technical
R.16 economic denial of service (edos)	Technical
R.17 loss of encryption keys	Technical
R.18 undertaking malicious probes or scans	Technical
R.19 compromise service engine	Technical
R.20 conflicts between customer hardening procedures and cloud environment	Technical
R.21 subpoena and e-discovery	Legal
R.22 risk from changes of jurisdiction	Legal
R.23 data protection risks	Legal
R.24 licensing risks	Legal
R.25 network breaks	Other
R.26 network management (ie, network congestion / mis-connection / non-optimal use)	Other
R.27 modifying network traffic	Other
R.28 privilege escalation	Other
R.29 social engineering attacks (ie, impersonation)	Other
R.30 loss or compromise of operational logs	Other
R.31 loss or compromise of security logs (manipulation of forensic investigation) 50	Other
R.32 backups lost, stolen	Other
R.33 unauthorized access to premises (including physical access to machines and other facilities)	Other
R.34 theft of computer equipment	Other
R.35 natural disasters	Other

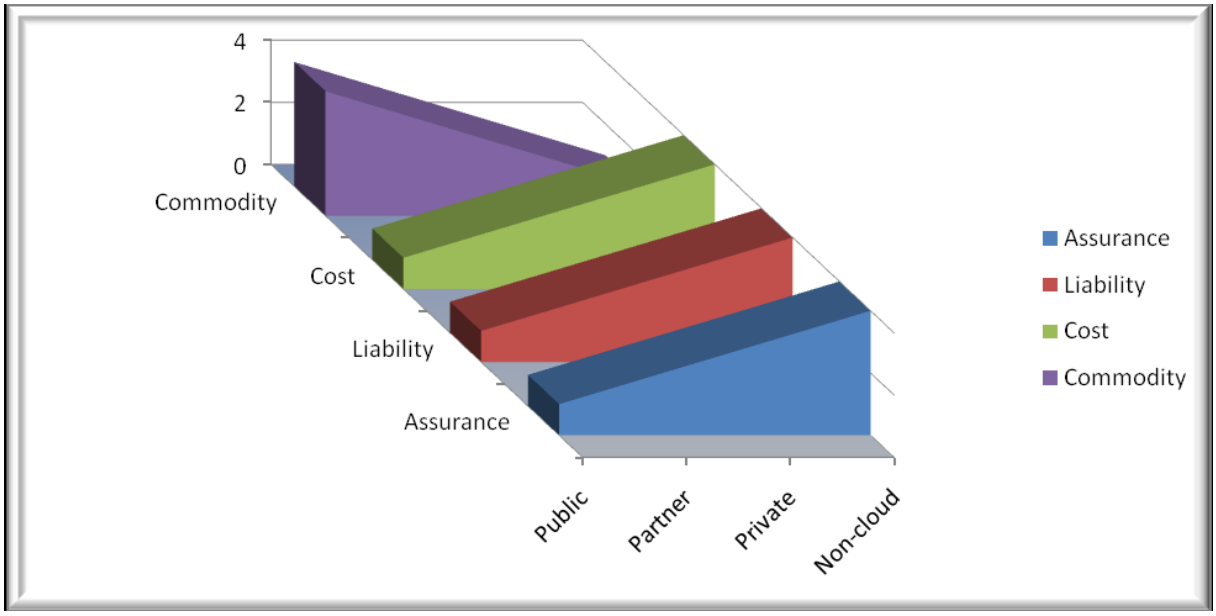

Figure 46 ENISA: Attributes of different cloud deployment models

B. A4Cloud Tools

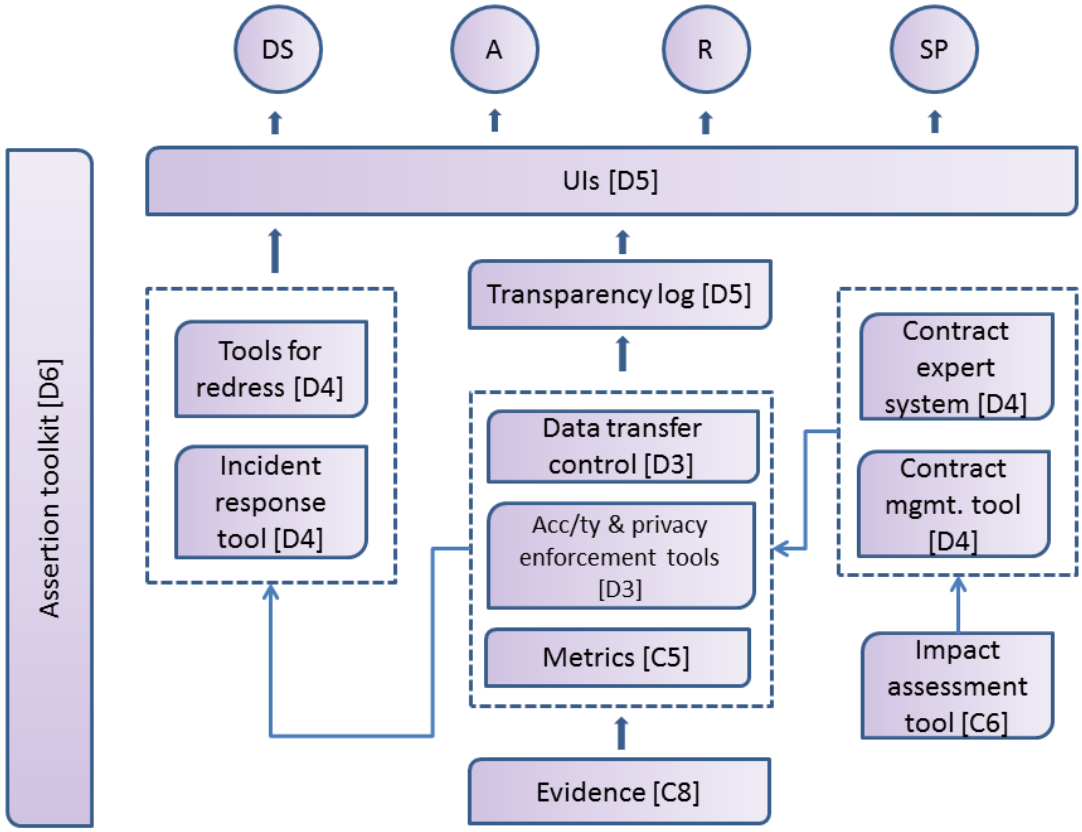

Figure 47 A4Cloud tools

C. NIST Risk Mapping44

Service Model	Extensibility	Security
SaaS	• Least consumer extensibility	• Relatively high level of integrated security - provider responsible • Negotiated into contracts for service (service levels, privacy, compliance)
PaaS	• More extensible than SaaS	• Less complete built-in capabilities • Securing the platform -- provider responsible • More flexibility to layer on additional security • Applications developed on platform and developing them securely -- consumer responsibility
IaaS	• Enormous extensibility	• Protecting underlying infrastructure and abstraction layers -- provider responsible • Less integrated security capabilities and functionality beyond that • Reminder of stack -- OSs, applications, content -- managed/ secured by consumer

Deployment Model	Location	Multi-tenancy Risks and Mitigation
General		Implications: Workloads of different consumers may reside: • Concurrently on same computer system and local network, • Separated only by access policies implemented by provider's software. Consumers security could be compromised by flaw in: • Implementation or • Provider's management and operational policies and procedures. Multi-tenancy risks: • Reliability – failure may occur • Security – attack may be perpetrated by consumer

[44] http://www.computer.org/portal/web/Irena-Bojanova/content?g=5970564&type=blogpost&urlTitle=addressing-cloud-security

Private	On-site	Implications: • General risks apply, as there could be authorized but malicious insiders • Different organizational functions, such as payroll, storage of sensitive personally identifiable information, or generation of intellectual property can become accessible to not authorized users and specific classes of data disclosed. Risks mitigation: • Logical segregation techniques at network layer, such as VPN Routing and Forwarding (VRF) • Clients are restricted to members of organization or authorized guests or partners.
	Outsourced	Implications: • On-site private cloud risks apply. Risks mitigation: • FISMA and OMB policy require external cloud providers to handle federal information or operating information systems on behalf of the federal government meet same security requirements as federal agencies.
Community	On-site	Implications: • On-site private cloud risks apply, but more organizations are encompassed. Risks mitigation: • Restricted number of possible attackers, but more than with private on-side cloud.
	Outsourced	Implications: • On-site community cloud risks apply. Risks mitigation: • Restricted number of possible attackers, but more than with private cloud.
Public		Implications: • Workloads of any combination of consumers may be sharing a single machine • Workload may be co-resident with workloads of competitors or adversaries. Risks:

		• Large collection of potential attackers, as public clouds aim scaling in consumers and resources to achieve low costs and elasticity. Risks mitigation: • Limited kinds of data for computations in the cloud • Data encryption (but then data needs to be unencrypted to be processed) • Physical separation – rent entire computer systems rather than VMs (mono-tenancy), VPNs, segmented networks, or advanced access controls.

D. Joint Risk ant Trust Model Statistical Analysis

We run experiments by using Monte-Carlo simulation methodology for three purposes: having better insight into our models, examining the relations between independent engineering variables (i.e., freshness (ω), slope (γ) and period length) and dependent variables (i.e., confidence intervals for security S, privacy P and service S risks), and more importantly verifying and validating our models. A subset of results from our experiments are depicted and analyzed in this section. For the experiments, we generated random values for $R(s)$, $R(p)$, $R(g)$, $R(s_e)$, $R(p_e)$, $R(g_e)$ and $R(D)$. We factored our experiments for the Poisson and Normal distributions and expected values to analyze the sensitivity of the model against the statistical characteristics of our random variables. Because of the stochastic nature of our model, we repeated each experiment 50 times and construct confidence intervals. For the other independent variables, we changed their value according to our design of experiment, which is based on partial factoring. The details about the value ranges for our factoring parameters are clarified below where we analyze and explain some of our results.

In Figure 48, the sensitivity of security S, privacy P and service G risks against the changes in independent engineering variables freshness (ω) and slope (γ) are depicted. $R(s)$, $R(p)$ and $R(g)$ are distributed according to Poisson distribution with 0.02, which means 2% percent of users were subject to a security, privacy or a service event in every period. In the last period CSP managed to eliminate 95% of all these events before they become an incident. In the period before the last period, this value is 93%. This indicates 2% increase in the CSP performance (i.e., its success in eliminating events before they become incidents), which affects the soft trust according to the slope (γ) value. As expected, the effect of the changes in slope value is not much, because it changes only soft trust, which should not contribute the risk perception in a major way when the change in CSP performance is only 2% and positive. Most probably this would be unrecognizable. On the other hand, the effect of freshness (ω) parameter is significant. The reason for that is the change in the number of events. In our experiments, the number of events in the last period goes down from 0.02 to 0.002. With the effect of CSP performance in eliminating events and therefore soft trust, when risk perception is based on only the events that happened in the last period, the model calculates risks as almost 0 except for privacy risk. In the privacy risk calculation, the duration of an incident before they get detected is also an important parameter. In the experiments for the results shown in Figure 48, the duration is Poisson distributed with 3 period lengths in the average. Therefore privacy risk P is always above 0.0001 and around 60% higher comparing to security and service risks.

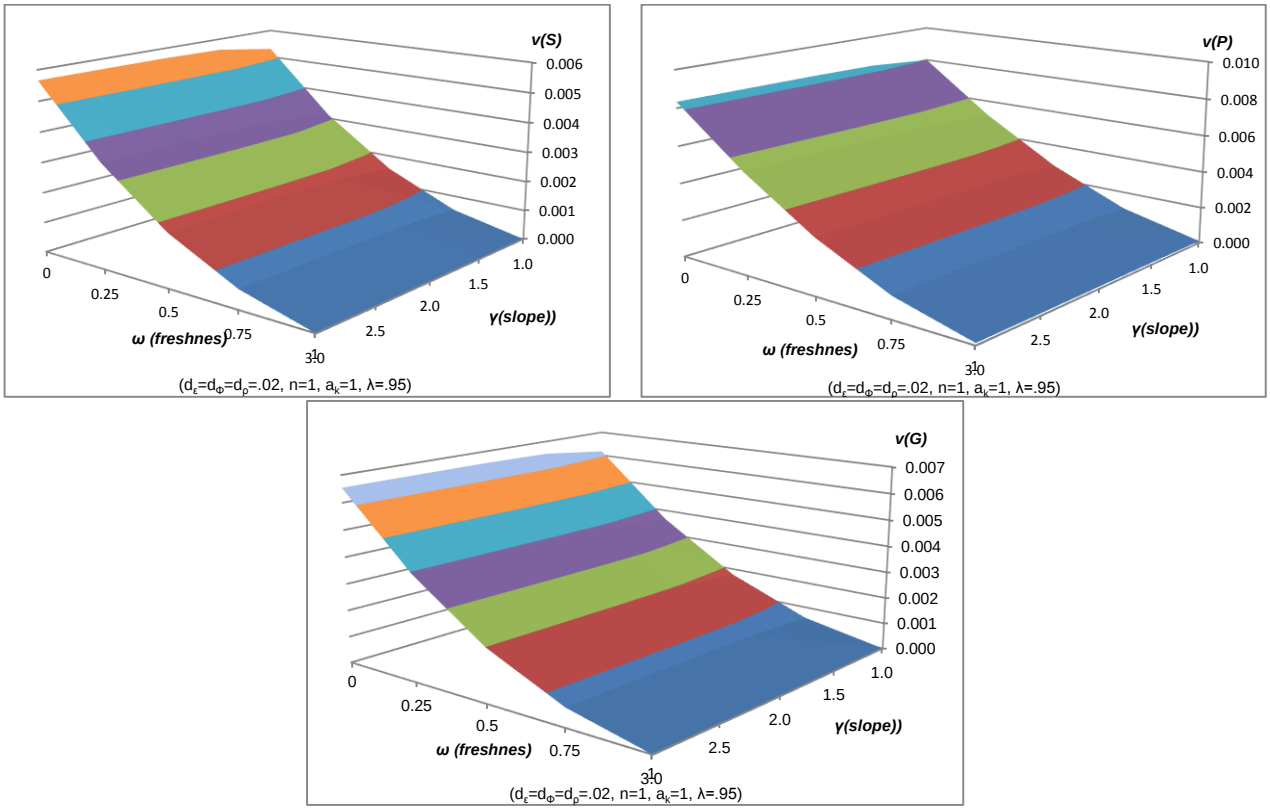

Figure 48 Upper bounds of security v(S), privacy v(P) and service v(G) risks for various slope (γ) and freshness (ω) values, .95 confidence interval, and dε=dΦ=dρ= 0.02.

The difference of the experiments in Figure 49 from Figure 48 is the change in the CSP performance. In Figure 48, it is 0.2 and positive. In Figure 49, it is again 0.2, but this time it is negative, which means the CSP got worse in eliminating the events before they become incidents (i.e., it goes down from 95% to 93%). The impact of this is trivial and the model captures it very well. First, the soft trust gets worse because this is a negative performance change, and therefore the slope *γ* becomes more effective at the risk perception. This is more significant when freshness *ω* is higher. Nevertheless, the relation between freshness and slope are not direct but indirect. Since the number of events were higher in the past in these experiments, when freshness value is higher, their influence in the final risk perception is less. When risk perception is higher, the effect of soft trust and therefore slope also become higher. Except for these differences, the other relations between parameters and results in Figure 49 are almost the same as in Figure 48. We examine the effect of the change in CSP performance more detailed in Figure 50.

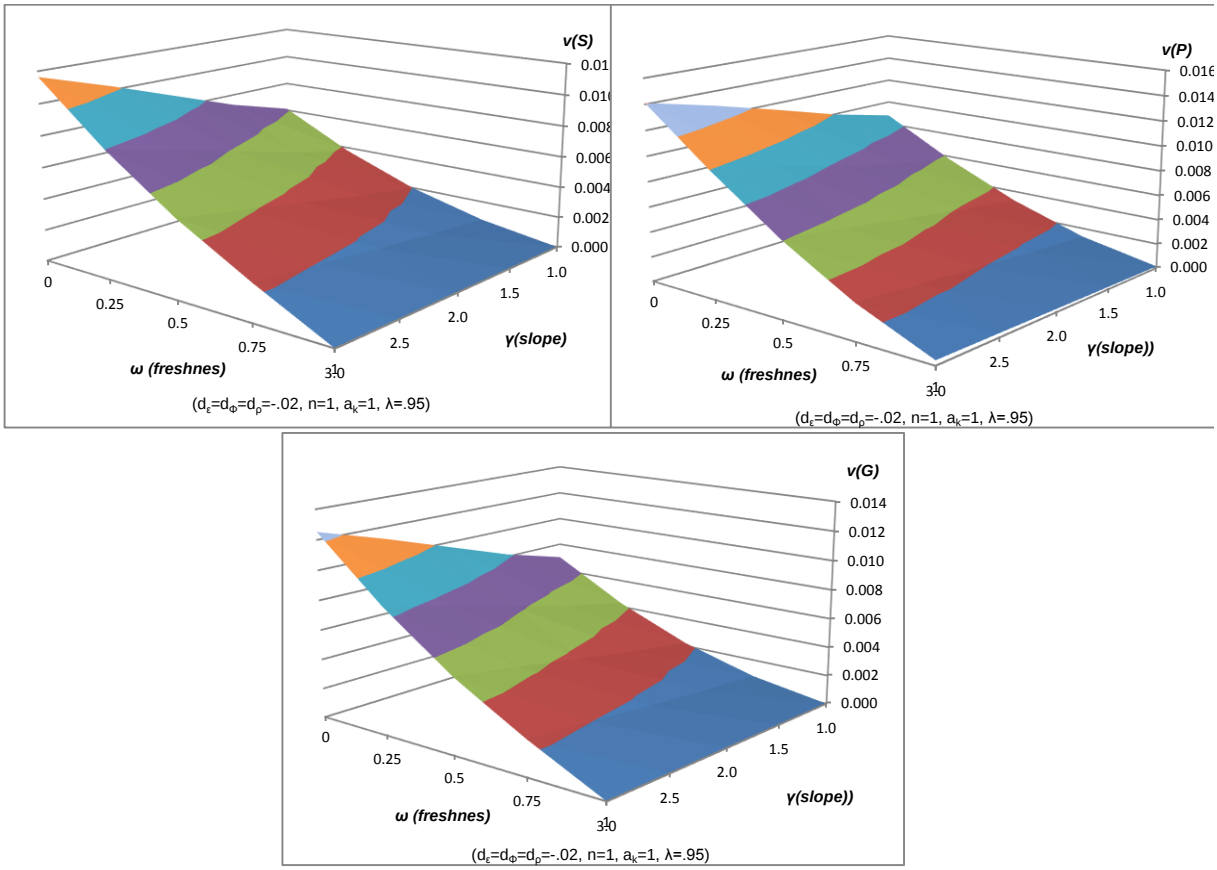

Figure 49 Upper bounds of security v(S), privacy v(P) and service v(G) risks for various slope (γ) and freshness (ω) values, .95 confidence interval, and dε=dΦ=dρ= -0.02

We would like to clarify a critical point for our model. When the performance of a CSP gets better, if the slope value is higher, that is reflected to the risk perception slowly. On the other hand, when the performance of a CSP gets worse, if the slope value is higher, that is reflected to the risk perception aggressively. Therefore, there is always a positive relation with risk and slope *γ*, which means that the higher the slope value becomes, the higher the risk is perceived independent from the tendency in the CSP performance. This behaviour is exactly what we expected from our model, and observable in Figure 48, Figure 49 and Figure 50.

In Figure 50, we examine the relation between slope and the tendency in CSP performance more closely for the changes between positive and negative 0.1. For this, we assign 0.85 for the event elimination performance in the period before the last period. Then we change the event elimination rates between 0.95 and 0.75 for the last period, and examine its effect in relation with the slope value. The results appear to have a baseball cap shape. When there is no change in the CSP performance, changing the slope value does not affect the risk perception. That completely makes sense, because slope is for amplifying the effect of the performance change in soft trust. When the tendency is positive, which means the performance of the CSP gets better in eliminating events, the effect of slope at the risk perception is less comparing to negative tendency. This is also how we wanted the model to behave. Trust can be gained slowly and can be lost more quickly. Therefore, we can tell that our model addresses the soft trust effect as expected and explained in Section 7.6.

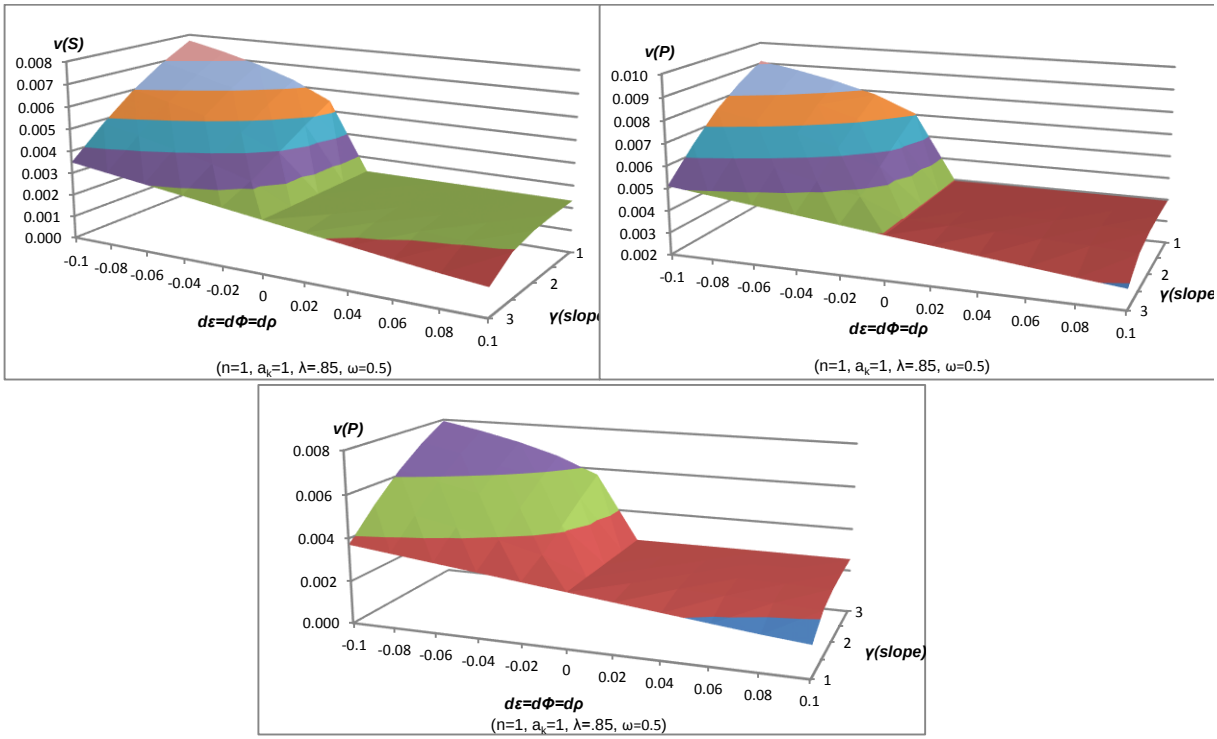

Figure 50 Upper bounds of security v(S), privacy v(P) and service v(G) risks for various slope (γ) and CSP performance tendency (dε=dΦ=d) values, .95 confidence interval, and freshness ω=0.5

In Figure 51, the relation between the number of services and risk is depicted for the same values as the ones used for the experiments in Figure 48 and Figure 49. As illustrated in Figure 51, there is a linear relation, and the privacy risk is the most sensitive against the number of services.

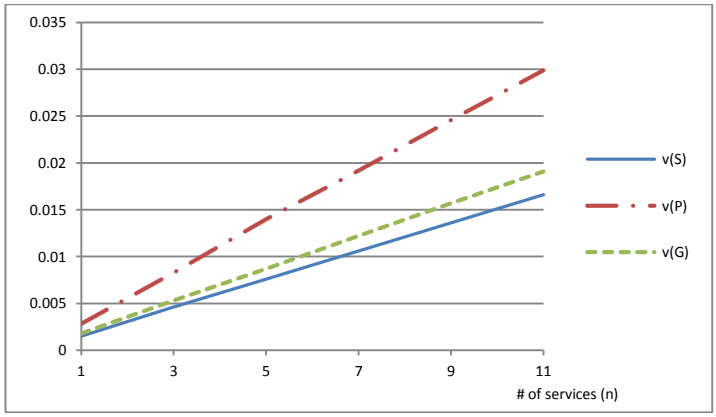

Figure 51 Upper bounds of security v(S), privacy v(P) and service v(G) risks for various number of services n in cloud service mashup

We also examined the sensitivity of risk against the number of alternative services (i.e., available services for the same service type within the intercloud) We observed that the number of alternative services does not change the security or privacy risks. However, it impacts on the service risk. When there is one alternative service in the average for each type of service in a composition made up of 11

service types, the service risk is calculated as 0.0191. When the average number of alternatives becomes two, the service risk goes down to 0.0001. When it is three in the average, the risk becomes almost zero. All these are what we desired in our model and our experiments validates the behaviour of model.

In Figure 52, the sensitivity of the privacy risk against the average duration of events before they are detected is shown. Please note that the security and service risks are not sensitive against the event duration. We tested duration not only for average but also for Poisson distribution and Normal distribution with various standard deviations. We observed an interesting result for Normal distribution. When standard deviation is as large as the average, the risk perception gets higher. This fits with the intuition much because higher variation means higher uncertainty. Nevertheless, when the average gets higher, higher standard deviation may reduce the risk because it also means lower privacy event durations from time to time.

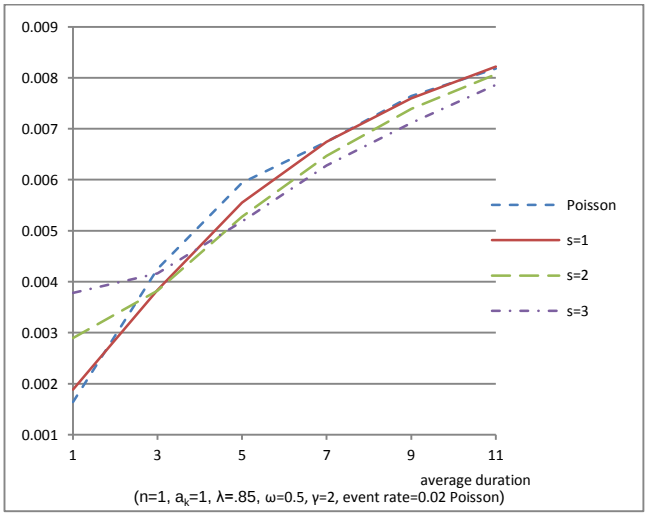

Figure 52 Upper bounds of privacy risk v(P) for various average durations of privacy

Figure 53 depicts the security v(S), privacy v(P) and service v(G) risks for various period lengths. Since the main effect of increasing period length is higher number of events observed within the period, Figure 53 also show the sensitivity of the model against the changes in event rates.

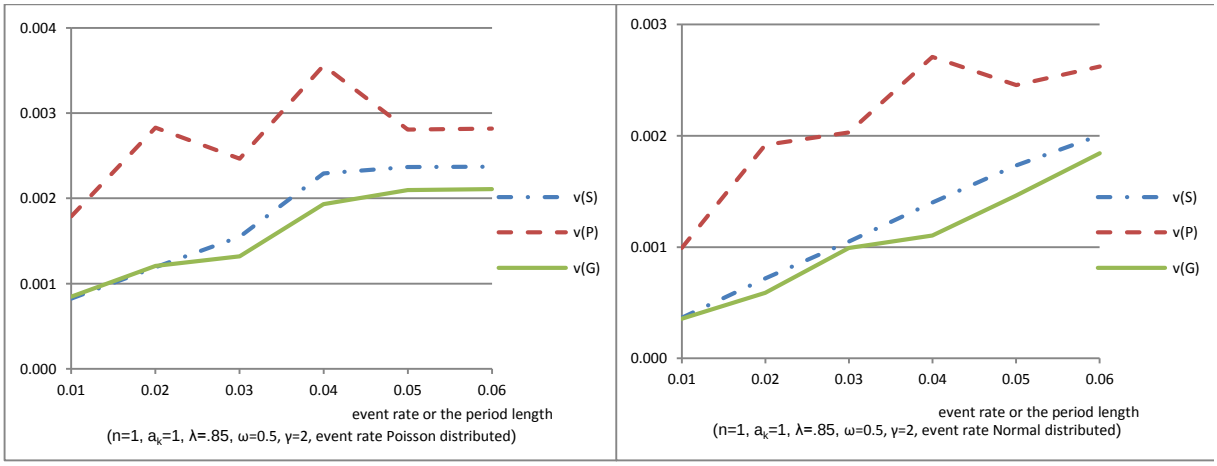

Figure 53 Upper bounds of security v(S), privacy v(P) and service v(G) risk for various event rates, which also means various period length

In Figure 53, we also analyse the effect of changing the distribution for the event occurrence. When we apply the same average rates, the risks calculated for Normal distribution is higher. Please note that we assign a standard deviation equal to 10% of the average for Normal distribution. We observe also an anomaly at the plots for privacy risk v(P) in Figure 53. The risks reduce at some points when the event rate gets higher. That is because in reality we do not increase the event rate but the period length which causes the event durations in the number of periods get reduced when period lengths are increased. When privacy event duration is reduced, that decreases privacy risk. Therefore, we observe a decrease in privacy risk although event rate increases at some points. This is normal and as expected.

E. Accountability Model

The Accountability Model (Figure 55) consists of accountability attributes, practices and mechanisms:

- **Accountability attributes** – conceptual elements of accountability as used across different domains (i.e. the conceptual basis for our definition, and related taxonomic analysis)
- **Accountability practices** – emergent behavior characterizing accountable organizations (that is, how organizations operationalize accountability or put accountability into practices)
- **Accountability mechanisms** – diverse processes, non-technical mechanisms and tools that support accountability practices (that is, accountability practices use them).

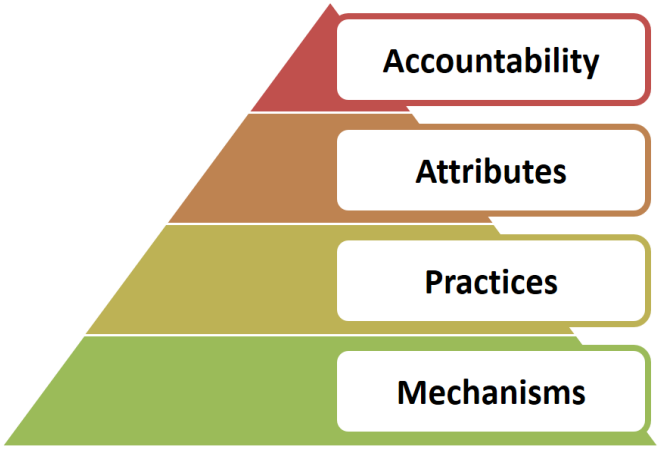

Figure 44 Accountability Model

Accountability Attributes: Accountability attributes capture concepts that are strongly related to and support the principle of accountability. These include: key properties of accountability (e.g. transparency); conceptual elements (e.g. remediation); consequences (e.g. sanctions); related objects (e.g., obligations). There exist emerging relationships (e.g. implication and inclusion) among attributes dependent on different viewpoints of analysis (which are related to societal, legal and ethical aspects of accountability). For instance, from a legal perspective, responsibilities imply obligations, which consequently may involve sanctions. From a social perspective, transparency implies both observability and verifiability (and vice versa, transparency is obtained by combining observability and verifiability). The defined accountability attributes are: *observability*, *verifiability*, *attributability*, *transparency*, *responsibility*, *liability* and *remediability*.

- **Observability** is a property of an object, process or system which describes how well the internal actions of the system can be described by observing the external outputs of the system.
- **Verifiability** is a property of an object, process or system that its behavior can be verified against a requirement or set of requirements.
- **Attributability** is a property of an observation that discloses or can be assigned to actions of a particular actor (or system element).
- **Transparency** is the property of an accountable system that it is capable of 'giving account' of, or providing visibility of, how it conforms to its governing rules and commitments.
- **Responsibility** is defined as the state of being assigned to take action to ensure conformity to a particular set of policies or rules.
- **Liability** is the state of being liable (legally responsible).
- **Remediability** is the state of being able to be remedied.

Accountability Practices: Accountability practices, derived directly from the definition of accountability, characterize emerging behaviour (highlighting operational and organizational objectives to be met) manifested in accountable organizations. Specifically, an accountable organization:

- Defines governance to responsibly comply with internal and external criteria, particularly relating to treatment of personal data and/or confidential data
- Ensures implementation of appropriate actions
- Explains and justifies those actions, namely, demonstrates regulatory compliance that stakeholders' expectations have been met and that organizational policies have been followed
- Remedies any failure to act properly, for example, notifies the affected data subjects or organizations, and/or provides redress to affected data subjects or organizations, even in global situations where multiple cloud service providers are involved.

Accountable organizations need to define and implement appropriate governance mechanisms relating to treatment of personal and/or confidential data in cloud environments. The actions in question pertain to the collection, storage, processing and dissemination of personal and/or confidential data.

Accountability Mechanisms: The accountability model highlights 'what' needs to be implemented. Within the model, accountability mechanisms (cf. the 'how') are instances of tools and techniques supporting accountability practices (that is, high level objectives that accountable organizations need to achieve). Organizations can adopt different available accountability mechanisms as appropriate for their contexts. They will use what is best for their particular processes (but of course, they also need to demonstrate that they have used appropriate mechanisms). Accountability mechanisms focus on the core aspects of accountability (e.g. remediation, notification and risk assessment). In addition, privacy mechanisms need to be used to reduce privacy risk as necessary. Accountability mechanisms (developed by the Cloud Accountability Project) complement others that are available from third parties. They may be used individually or in combination. Organizations may select from different alternatives. For example, they may choose to use the Privacy Level Agreement format specified by the Cloud Security Alliance (CSA) to express privacy-related obligations, or the Cloud Trust protocol to ask for and receive information from cloud service providers about the elements of transparency, or they may take another approach to do so.

F. Questionnaire

Please tick your agreement for each statement based on the presentation on Accountability, Risk and Trust for Cloud Services, the discussions that followed and your expertise.

ID	Statement	0 Strongly Disagre	1	2	3	4	5	6 Strongly Agree
S1	Risk affects accountability							
S2	Risk requires trust (dealing with uncertainty)							
S3	Some threats are specific to cloud services							
S4	Accountability mitigates risk							
S5	Accountability mediates risk and trust (enhancing knowledge)							
S6	Accountability supports interactions in the cloud							
S7	Accountability supports trust decisions							
S8	Accountability enhances cloud trustworthiness							
S9	Trust facilitates interactions							
S10	Trust relies on operational evidence of trustworthiness							

Notes

Figure 55 Questionnaire: Accountability, Risk and Trust in Cloud Services