CLOUD ACCOUNTABILITY PROJECT

D:C-2.1 Report detailing conceptual framework

Deliverable Number	D32.1
Work Package	WP 32
Version	Final
Deliverable Lead Organisation	HP
Dissemination Level	PU
Contractual Date of Delivery (release)	30/09/2014
Date of Delivery	13/10/2014

Editor

Massimo Felici (HP), Siani Pearson (HP)

Contributors

Brian Dziminski (QMUL), Massimo Felici (HP), Carmen Fernandez Gago (UMA), Frederic Gittler (HP),Theo Koulouris (HP), Ronald Leenes (TiU), Jesus Luna (CSA), Maartje Niezen (TiU), David Nuñez (UMA), Alain Pannetrat (CSA), Siani Pearson (HP), Jean-Claude Royer (EMN), Dimitra Stefanatou (TiU), Vasilis Tountopoulos (ATC)

Reviewers

Simone Fischer-Hübner (KAU), Martin Jaatun (SINTEF), Anderson Santana de Oliviera (SAP), Jenni Reuben Shanthamoorthy (KAU)

Executive Summary

This document is an external project report setting out the Cloud Accountability Project's (A4Cloud) model and framework for accountability, together with the project glossary. It consists of the main aspects of accountability together with the project's contributions underpinning the foundations for an accountability-based approach tailored to data stewardship in the cloud.

The A4Cloud project is targeted at EU Framework 7 Call 8 Objective ICT-2011.1.4 Trustworthy ICT, and particularly on objective (c), i.e. data policy, governance and socio-economic ecosystems. Accordingly, and reflecting our project focus, we concentrate on accountability for ethical governance and stewardship of personal data within cloud environments. Although the focus of the project is on personal data, in addition certain types of confidential information that may not involve personal data, such as business secrets, are being considered. The project focus is particularly on the accountability of organisations using and providing cloud services to data subjects and regulators. Government surveillance, including government acquisition of data from cloud service providers, is outside the scope of this project, except where it relates specifically to a data protection law accountability mechanism: no accountability controls of the types considered in the project (which are based upon assisting compliance with domestic data protection legislation and private contracts) are likely to provide effective protection against such activities.

Accountability is an important but complex notion that encompasses the obligation to act as a responsible steward of the personal information of others; to take responsibility for the protection and appropriate use of that information beyond mere legal requirements; to be transparent (give account) about how this has been done and to provide remediation and redress. This notion is increasingly seen as a key market enabler in global environments and in helping overcome barriers to cloud service adoption. Accountability also has a strong role to play in encouraging appropriate data stewardship by organisations both using the cloud and providing cloud services. However, the relative complexity of the service provision chain, in combination with a lack of transparency and control, makes it very challenging both legally and technically to provide accountability for and in the cloud. We propose a co-designed approach that encompasses legal and regulatory mechanisms and a range of technological enhancements that can provide the necessary basis for initiating and sustaining trustworthy data processing and a trusted relationship between data subjects, regulators and information and communications technology (ICT) providers. This document is the result of a comprehensive study of accountability as being fundamental in supporting data stewardship in the cloud. It reports on different contributions forming together a conceptual framework for accountability.

Accountability Highlights

This document reports in detail the main results contributing towards a conceptual framework for accountability. The following paragraphs highlight the main outcomes on accountability.

The Concept of Accountability. There are numerous references to accountability in regulatory frameworks, and these are surveyed in this document. Within this analysis, the most relevant opinions expressed by the EU's Article 29 Working Party (an independent advisory body on the interpretation of the data protection framework set up under article 29 of Directive 95/46/EC) as well as the European Data Protection Supervisor (EDPS), among others, are described. Definitions and models of accountability used in computer science are also reviewed, from high-level presentations to low-level cryptographic models used for proving properties about systems. This document reports on a comprehensive multidisciplinary (e.g. social, legal, ethical) critical analysis of accountability, as understood from different viewpoints. This analysis helps to identify and clarify the nature of accountability and its foundations. In particular, it clarifies how the concept of accountability relates to the notion of account and what is expected by organisations in order to be accountable. Our **conceptual definition of accountability** captures such an understanding that may be relevant across different application domains (and not only cloud environments):

> *Accountability consists of defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly.*

Cloud-factors Affecting Accountability. Most of the time, the cloud is perceived no differently than other Information and Communication Technology (ICT). However, moving data to the cloud exposes both cloud customers and providers to new emerging challenges (e.g. isolation failure, dynamic data flows, lack of transparency about service delivery chains) concerned with security, privacy and governance. This document reviews the emerging challenges that are relevant to cloud environments and discusses how such challenges affect accountability.

Cloud Ecosystems. Our analysis of accountability in the cloud and emerging relationships between cloud actors has supported the extension of the NIST taxonomy of cloud computing roles in order to highlight more effectively how different stakeholders relate to the cloud. We have identified seven cloud accountability roles:

1) **Cloud Subject:** An entity whose data is processed by a cloud provider, either directly or indirectly. When necessary we may further distinguish:
   a) **Individual Cloud Subject**, when the entity refers to a person
   b) **Organisation Cloud Subject**, when the entity refers to an organisation
2) **Cloud Customer:** An entity *that (1) maintains a business relationship with, and (2) uses services from a Cloud provider*. When necessary we may further distinguish:
   a) **Individual Cloud Customer**, when the entity refers to a person
   b) **Organisation Cloud Customer**, when the entity refers to an organisation
3) **Cloud provider:** An entity responsible for making a [cloud] service available to Cloud Customers
4) **Cloud Carrier:** The intermediary entity that provides connectivity and transport of cloud services between Cloud providers and Cloud Customers
5) **Cloud Broker:** An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud providers and Cloud Customers
6) **Cloud Auditor:** An entity that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation, with regards to a set of requirements, which may include security, data protection, information system management, regulations and ethics
7) **Cloud Supervisory Authority:** An entity that oversees and enforces the application of a set of rules.

Notably, these cloud roles allow a distinction to be made between cloud subject and cloud customer, both for individuals and organisations. This distinction is important for analysing accountability aspects of data protection in the cloud.

Accountability Model. This document defines a multi-layer model of accountability as a general concept for data governance. Accountability can be captured at different layers of abstraction. The accountability model captures our generic conceptual definition of accountability. Moving from an abstract definition of accountability to an operational view of being accountable, the defined accountability model provides a systematic and structured way of analysing accountability. Corresponding to different abstraction levels the accountability model consists of different layers:

- **Accountability Attributes** – conceptual elements of accountability applicable across different domains (i.e. the conceptual basis for our definition, and related taxonomic analysis). These are the central taxonomic aspects of accountability, namely: *transparency*, *responsiveness*, *remediability*, *responsibility*, *verifiability, effectiveness* and *appropriateness*.
- **Accountability Practices** – emergent behaviour characterising accountable organisations (that is, how organisations operationalise accountability or put accountability into practices). Accountability practices define the central behaviour of an organisation adopting an accountability-based approach. These are: *defining governance to responsibly comply with internal and external criteria*, *ensuring implementation of appropriate actions*, *explaining and justifying those actions*, and *remedying any failure to act properly*.
- **Accountability Mechanisms** – diverse processes, non-technical mechanisms and tools that support accountability practices (that is, accountability practices use them). These mechanisms operationalise accountability; organisations will use these to support and implement accountability practices, but in addition will need to use privacy and security controls appropriate to the context to provide data stewardship and data protection. Accountability mechanisms may form a toolbox from which organisations can select as appropriate. They can be (extensions of) existing business processes like auditing, risk assessment and the provision of a trustworthy

account, or non-technical mechanisms like formation of appropriate organisational policies, remediation procedures in complex environments, contracts, certification procedures, and so on. Or they can be technical tools, which would include tracking and transparency tools, detection of violation of policy obligations, notification of policy violation, increased transparency without compromising privacy, and so on. The mechanisms are targeted at different stakeholders, and some are designed for usage as a preventive measure (for example, to assess and reduce privacy harm before personal data is collected), some as a detective measure (for example, to assess the degree to which privacy obligations are actually being met) and others as a corrective measure (for example, to facilitate redress).

Accountability Framework. In order to tailor the concept of accountability to the cloud, we have refined our conceptual definition in the **definition of accountability for data stewardship in the cloud**:

> *Accountability for an organisation consists of accepting responsibility for data with which it is entrusted in a cloud environment, for its use of the data from the time it is collected until when the data is destroyed (including onward transfer to and from third parties). It involves the commitment to norms, explaining and demonstrating compliance to stakeholders and remedying any failure to act properly.*

Moving from the conceptual analysis of accountability towards an operational understanding of accountability in the cloud, the accountability model underpins various functional elements that form our accountability framework. The accountability framework helps to operationalise accountability by identifying those accountability functions that support different stakeholders (from cloud subjects to cloud auditors) in the cloud supply chain at different stages, i.e. preventive, detective and corrective phases. Such accountability functions at each phase are supported by different accountability mechanisms (in particular, tools) that form our reference architecture.

Accountability Governance. Alongside a structured view of accountability captured conceptually in the accountability model and functionally in the accountability framework, we have defined an accountability governance lifecycle that orchestrates the different accountability functions. The accountability governance lifecycle supports organisations in becoming accountable by adopting an accountability-based approach for data stewardship in the cloud. The accountability governance lifecycle in combination with the accountability model and framework helps organisations to identify appropriate and effective accountability measures, and to put them into practice. Among the critical functions enabling the identification of such measures is risk analysis extended in order to take into account accountability perspectives, with a particular focus on privacy and data protection.

Accountability Maturity Model. Our analysis and contribution towards a comprehensive understanding of accountability assumes that accountability is a market differentiator for cloud services. In this respect the role of certification and assurance has been taken into account while defining an Accountability Maturity Model. This provides a means for assessing how organisations are accountable. This also takes into account an operational view of accountability that is concerned with the provision of evidence and the quantification of accountability attributes by metrics. This supports different stakeholders. Cloud providers have systematic instruments for assessing their accountability practices and measures. Cloud subjects and customers have a means to support the adoption of cloud services based on accountability. This suggests further developments towards an accountability certification of organisations in cloud ecosystems.

Report Organisation and Reading Guidelines

This document captures our comprehensive multidisciplinary analysis of accountability. It has evolved from different contributions and discussions within the project as well as with the project Advisory Board and other external experts. Our critical analysis and different contributions are supported by relevant literature. This is a valuable source of information to whosoever is interested in acquiring further knowledge about accountability. The document has been written and organised in order to include self-contained elements and to be accessible to a broad audience with different interests relating to accountability. In order to make our contributions accessible for different reasons and readers, we have structured the document in two different parts: Part I (White Paper) and Part II (Technical Sections).

- **Part I - White Paper:** The white paper is intended for a general audience who would like to acquire an understanding of accountability and its relevance to the cloud. The white paper highlights the main contributions of this work package and explains them in such a way as to be accessible to informed readers (such as cloud customers or policy makers) who might benefit from a greater understanding of accountability. It provides a synthetic description of the main work package outcomes. It is useful to read as an overview of the key approach and findings in relation to the project's conceptual framework.
- **Part II - Technical Sections:** The technical sections provide more detailed analyses of the main contributions supported by relevant literature. The organisation of the white paper and the technical sections are aligned with the intention of supporting readers who are interested in the detailed analysis behind each contribution highlighted in the white paper. The technical sections are organised as follows:
  - **Section 1 Introduction:** This describes the context of the project, including the socio-economic landscape, motivations for an accountability-based approach in the cloud and scoping of the project.
  - **Section 2 The Concept of Accountability:** This provides an overview and analysis of the concept of accountability, together with assessment of the impact of different interpretations and explanation about what organisations need to do to take an accountability-based approach. The provision of an account is a central part of what an accountable organisation does, and this is also discussed. A definition of accountability is provided, and its essential elements and relationship with key related terms are considered. This complements the material produced by WP C-7, which considers the relationship between privacy, transparency and accountability in more detail.
  - **Section 3 Cloud-Specific Factors Affecting Accountability:** This discusses issues specific to cloud computing that need to be considered when developing an accountability approach to data governance, further to those already discussed in Section 1.
  - **Section 4 Accountability in Cloud Service Provision Ecosystems:** This explains what cloud service provision ecosystems are and provides some examples, showing how analysis of accountability in such ecosystems is very much reliant upon the different roles and responsibilities involved, some of which are legally determined. This analysis includes an extension of the roles identified by the National Institute of Standards and Technology (NIST), and assessment of a variety of cloud scenarios with respect to accountability.
  - **Section 5 Accountability Model:** This sets out the notion of accountability by presenting a three-part abstract model of accountability, layering the notion into accountability attributes, accountability practices, and accountability mechanisms. The interrelationships between these layers are discussed and a wider taxonomic analysis of accountability is provided.
  - **Section 6 Accountability Framework:** This presents an accountability framework for the cloud, comprising preventive, detective and corrective controls, usable throughout the service provision chain to enable chains of accountability.
  - **Section 7 Accountability Governance and Processes in the Cloud:** This discusses aspects of accountability governance in the cloud such as the relevant processes to be implemented by an organisation that uses or provides cloud services, how this can be achieved throughout the cloud service ecosystem and how such organisations can be held to account. Accountability governance is set out as comprising a process, a maturity model (described further in Section 8), and a scheme for certification. These ideas are integrated to provide a model of organisational accountability. In addition, the way in which enforcement can be dealt with effectively in the cloud is discussed.
  - **Section 8 Contextual Accountability in the Cloud:** This considers how an accountability-based approach might vary across different contexts in an intelligent way. We build upon an idea of "intelligent accountability" as a means to provide greater accountability without damaging performance, recognising that "good governance is possible only if institutions are allowed some margin for self-governance of a form appropriate to their particular tasks." We investigate how accountability may be introduced in distributed and cloud environments in an intelligent way, trying to avoid the situation where trust does not increase and the overall effect is negative with regard to the increased administrative burden. Part of this relates to an analysis of how the appropriateness of measures might vary according to different contexts, and part relates to how a maturity model could be devised for accountability mechanisms, both for a single organisation and across cloud supply ecosystems.

- **Section 9 Conclusions:** This section highlights the main conclusions drawn from defining our conceptual framework on accountability.
- **References**
- Appendices: The final part of the document consists of the appendices and a glossary. More specifically:
  - **Appendix A A4Cloud Project Objectives** pinpoints the project objectives.
  - **Appendix B Prior Analysis of Accountability** is an in-depth literature review of accountability as understood by various disciplines to help put the analysis given in Section 2 into context and provide more detail.
  - **Appendix C Cloud Computing** provides a brief explanation of cloud computing.
  - **Appendix D Accountability Functions and Mechanisms** highlights how the different accountability mechanisms support the functional elements of accountability.
  - **Appendix E Examples of Accountability Chains and Mechanisms** provides some further consideration beyond that given in Subsection 4.2.
  - **Appendix F Accountability Maturity Model**
  - **Appendix G Accountability Maturity Model Scoring** provide the Accountability Maturity Model and its scoring.
- **Glossary of Terms and Definitions** consists of the project's glossary of terms and definitions. Most definitions are supported by references. Therefore, the glossary itself is a valuable source of information concerned with accountability as well as information security, privacy and data protection. Key aspects of the project glossary that we have developed are fully defined and free online access to the complete glossary is available via the project website http://www.a4cloud.eu/. The white paper might be of interest to any audience. For the rest of the document, particular sections are likely to interest different audiences to a greater level. For example, a socio-economist might be most interested in Sections 1, 2, 4 and 8, corporate governance in Sections 1, 2 and 7, or a computer scientist in Sections 1, 2, 4 and 8. This structure intends to support a wide audience of stakeholders who might benefit from our multidisciplinary comprehensive understanding of accountability.

Table of Contents

Index of Figures

Index of Tables

PART I
WHITE PAPER

Accountability for Cloud Service Provision Ecosystems

This white paper provides context and explanation of key findings in relation to the conceptual framework for accountability in the cloud proposed by the Cloud Accountability Project (A4Cloud), a project targetted at EU Framework 7 Call 8 (Trustworthy ICT). It includes a background introduction, consideration of the concept of accountability and accountability relationships in the cloud, and proposes an approach, model and framework. The document is intended for a general audience who would like to acquire an understanding of accountability and its relevance to the cloud, and/or to read an overview of the key approach and findings in relation to the A4Cloud project's conceptual framework.

The goal of the A4Cloud project is to develop and validate techniques for implementing accountable cloud ecosystems. The focus of analysis is on personal data, but in addition certain types of confidential information that may not involve personal data, such as business secrets, are being considered. The project emphasis is particularly on the accountability of organisations using and providing cloud services to data subjects and regulators.

The National Institute of Standards and Technology (NIST) defines cloud computing as "*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*"[1]. The service models defined by NIST are: *Software as a Service (SaaS),* where consumers use cloud service providers' (cloud providers') applications running on a cloud infrastructure; *Platform as a Service (PaaS),* where consumers deploy (onto a cloud infrastructure run by a cloud provider) applications that have been created using programming languages and tools supported by that provider; *Infrastructure as a Service (IaaS),* where consumers deploy and run software, with a cloud provider controlling the underlying cloud infrastructure. Deployment models encompass private, community, public and hybrid clouds. The combination of such cloud computing features enables different business models, and hence different types of cloud ecosystem.

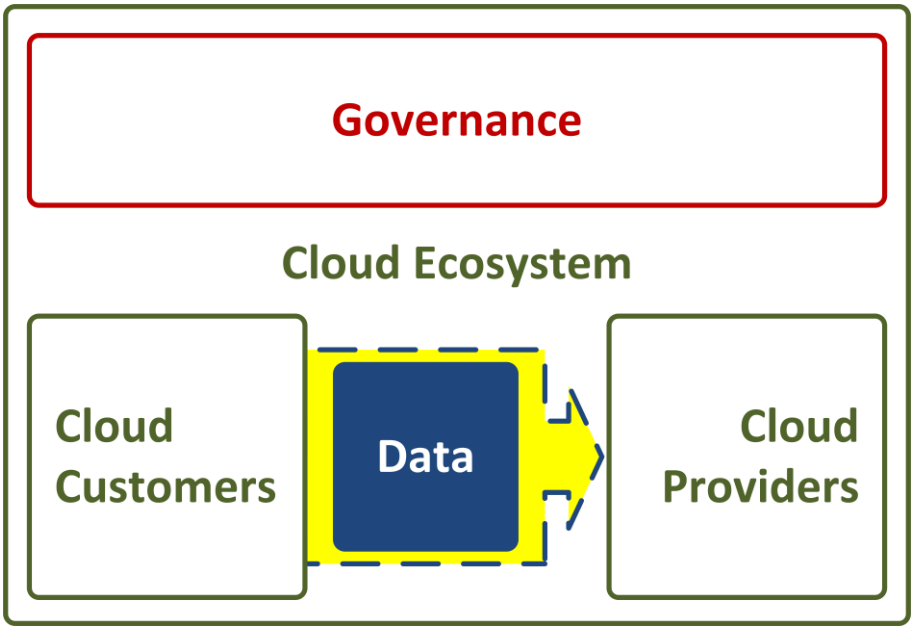
Cloud computing has transformed the way information technology is delivered, promising rapid, efficient, and cost-effective deployment of computational resources across different industries, geographies and application domains. Cloud computing provides a market opportunity with a huge potential both for efficiency and new business opportunities (especially in service composition). Due to the advantages its usage is rapidly increasing, but unfortunately it can result in a higher risk to privacy and security, where issues faced in subcontracting and offshoring can be magnified. Therefore, there are a number of key issues related to such expansion that need to be addressed. In particular, trustworthiness of the service provision should be ensured and regulatory and contractual compliance should be facilitated throughout cloud service provision ecosystems. These issues are considered further in the following section.

Data Protection Issues in the Cloud

We are here concerned with accountability as stewardship of data becomes shared between cloud customers and potentially complex chains of cloud providers. As shown in the following figure (Cloud Ecosystem), the former have to place trust in the cloud ecosystem and its governance. Correspondingly, organisations may be reluctant to let data flow outside their boundaries into the cloud, especially for public cloud, and are especially concerned in cloud environments with data breaches and data loss[2]. Furthermore, lack of consumer trust is commonly recognised as a key inhibitor to moving to the cloud.[3] People have increasing expectations that their data will be handled in a responsible way and will be protected by the companies they choose to share data with.[4] The recent Snowden revelations have encouraged concerns about increased access to data including by foreign governments and exacerbation of privacy risk through sub-processing and de-localisation. However, current terms of service push back risk to consumers and offer limited safeguards, while they limit the liability of cloud

[1] Mell, P., Grance, T. (2011): The NIST Definition of Cloud Computing, NIST Special Publication 800-145.
[2] CSA (2013): The Notorious Nine: Cloud Computing Top Threats in 2013, Cloud Security Alliance, Top Threats Working Group.
[3] IDC (2012): Quantitative Estimates of the Demand of Cloud Computing in Europe, International Data Corporation.
[4] In a 2010 survey by Fujitsu Research Institute on potential cloud customers, it was found that 88% of potential cloud consumers are worried about who has access to their data and demanded more awareness of what goes on in the backend physical server.

service providers, therefore leaving little room for request for remedy. There is a perceived lack of transparency and relatively limited sense of control compared to traditional models, and this is of particular concern for sensitive information[5].



Cloud Ecosystem

The second barrier to migration to cloud business models is the difficulty of compliance with different regulatory regimes. A major reason for this is that data flows tend to be global and dynamic. The collection and processing of personal information is subject to regulation in many countries across the world. Some national laws restrict transborder flow of personal information, including access to this information. This (sometimes inconsistent) matrix of national laws can make it difficult for businesses that wish to provide effective stewardship of the data that they handle to ensure full compliance when operating in multiple jurisdictions. It can be difficult even to determine which laws apply and which courts should preside. There is pressure from organisations for greater harmonisation to reduce unnecessary administrative burdens and risks. These two issues – *trust* and *complexity* – are closely linked. Both legal and ethical obligations arise to ensure privacy and protect data, and these need to be built upon to demonstrate the trustworthy nature of cloud services.

There are a variety of data protection concerns related to cloud computing that include ongoing questions of jurisdiction and exacerbation of privacy risk through sub-processing and de-localisation, as well as legal uncertainty. For example, a study on security and privacy in public cloud computing has pointed out concerns for cloud adoption that include governance over data use and processing, the compliance to laws, regulations, standards and specifications, the management of risks to assess trust and trustworthiness along the cloud service chains and the effective implementation of incidence response mechanisms[6]. The table below (Cloud Features and Issues) highlights key issues by means of illustrating how many of the features that characterise the cloud can enhance data protection risks. For example, cloud vulnerabilities include the multi-tenancy of cloud applications, in which co-tenants may gain inappropriate access to the data of another application instance and the simplification of data access from multiple geographic locations, but with completely different legislative regimes. Also, data duplication and proliferation in the cloud create problems in terms of compliance, since the loss of control and transparency significantly affect the data lifecycle management across various involved providers in a service provisioning chain. A categorisation of risks from an EU perspective has been made according to lack of transparency or control by the Article 29 Working Party in their Opinion on Cloud

[5] See for example the analysis given within: Pearson, S. (2012): Privacy, Security and Trust in Cloud Computing. In: Pearson, S., Yee, G. (Eds.), Privacy and Security for Cloud Computing, Computer Communications and Networks. Springer pp. 3-42; and, European Parliament (2012): Fighting Cyber Crime and Protecting Privacy in the Cloud, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs.
[6] Jansen, W., Grance, T. (2011): Guidelines on Security and Privacy in Public Cloud Computing, NIST SP 800-144.

Computing[7]. Similar risks were highlighted by the French data protection authority[8], with the addition of ineffective or non-secure destruction of data, or excessive data retention periods, and of takeover of the cloud provider by a third party. A more detailed analysis of cloud computing risks has been provided by European Union Agency for Network and Information Security (ENISA)[9].

Cloud Features and Issues

Cloud features	Potential data protection issues
Multi-tenancy	• Data of co-tenants may be revealed in investigations • Isolation failure • Proper deletion of data and virtual storage devices
Elasticity	• Multiplies attack surfaces • De-anonymisation facilitated
Abstraction	• Cannot rely upon physical security controls
Automation	• Ensuring appropriate data protection when data flows are dynamic • Decrease in human involvement in data protection
Data duplication	• Detecting and determining who is at fault if privacy breaches occur • Difficulty in knowing geographic location and which specific servers or storage devices will be used
Easy data access from multiple locations	• Data access from remote geographic locations subject to different legislative regimes, and transborder data flow compliance issues • Potential for risky usage by employees without due consideration
Subprocessing	• Potential complexity of cloud service delivery chains, both horizontally and vertically • Lack of transparency or compliance by subprocessors • Unauthorized data access from employees of CSPs • Risks to confidentiality from subpoenas or access by foreign governments • Overlapping responsibilities in data management • Unauthorized secondary usage and profiling • Vendor demise

With regard to security, it is a common legal requirement that if an organisation outsources the handling of personal data to a third party, it has some responsibility to make sure the outsourcee uses 'reasonable security' to protect those data. This means that any organisation creating, maintaining, using or disseminating personal data must ensure that data has not been tampered with, and take precautions to prevent its misuse. However, in the cloud, issues such as unauthorised secondary usage of data and inappropriate retention of data can be difficult to address. Of course, in addition, organisations need to take into account the privacy-related expectations of their customers, which may be specified within private contracts. This is likely to involve a combination of process-based and access control mechanisms. Other legal obligations vary according to the regulatory context and there are likely to be some significant changes in the near future. Once these are implemented, many service providers will gain a range of data security obligations including adopting risk management practices and reporting major security incidents to competent authorities and affected parties.

In this document accountability can essentially be regarded as stewardship. Accountability is central to a trustworthy cloud – an accountable cloud ecosystem is necessary for innovation and growth ambitions. Higher accountability, if adequately explained, should result in higher acceptance and trust by

[7] Article 29 Data Protection Working Party (2012): Opinion 05/12 on Cloud Computing, 05/12/EN WP 196, European Commission, Directorate General Justice.
[8] CNIL (2012): Recommendations for Companies Planning to Use Cloud Computing Services, Commission nationale de l'informatique et des libertés.
[9] Catteddu, D., Hogben, G. (Eds.) (2009): Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA Report.

prospective cloud customers. Cloud customers want to be confident that service providers are treating data appropriately and that customers can retain control over how it is used, that the legal frameworks are effective, and that they have ways to hold providers liable for what happens to that data. Cloud providers need a way to implement accountable cloud services. Therefore, there are a number of reasons for taking an accountability-based approach:

1. to improve the level of data stewardship
2. to provide trustworthy mechanisms for data protection in the cloud (for cloud customers, data subjects, data controllers and regulators)
3. to decrease regulatory complexity, and
4. to provide more effective mechanisms for complex and dynamic business environments.

In what follows, we highlight our contributions towards an accountability-based approach to data governance in the cloud. Based on analysis of relevant literature, we contribute to a comprehensive understanding of the concept of accountability, characterising accountability from different viewpoints (e.g. data protection, legal, ethical, etc.). After that, we explain how our analysis of the different roles in a cloud ecosystem combined with a systematic understanding of accountability enables identification of mechanisms supporting accountability and deployment of these within cloud ecosystems.

The Concept of Accountability

Accountability, in general, is used prescriptively; accountability of some agent to some other agent for some state of affairs. It reflects an institutional relation arrangement in which an actor can be held to account by a forum (for example, a consumer organisation, business association or even the public at large). Accountability then focuses on the specific social relation or the mechanism that involves an obligation to explain and justify conduct. Subsequently, accountability is "*a relationship between an actor and a forum, in which the actor has an obligation to explain and to justify his or her conduct, the forum can pose questions and pass judgement, and the actor can be sanctioned*"[10].

In an accountability relationship thus two parties and an object can be distinguished: a) the steward or accountor, b) accountee or forum, and c) the codes or norms on the basis of which the relationship is struck. The latter are the shared framework for explanation and justification that are negotiated between the accountor (to answer, explain and justify) and accountee (to question, assess, and criticise). An accountability code then is a system of signals, meanings and customs, which binds the parties in a stewardship relation. In order to do so there are different stages in accountability relations:

a) information in which explanation is given and one's conduct is justified
b) debate, in which the adequacy of the information and / or the legitimacy of conduct is debated (answerability)
c) the forum must pass judgement and sanction whether formally (for example, via fines, disciplinary measures and unwritten rules leading to resignation) or informally (for example, having to render account in front of television cameras or via disintegration of public image and career).

Accountability as a mechanism thus can be used as a tool to induce reflection and learning. It provides external feedback on (un)intended effects of an organisation's actions. However, accountability is also used in a more normative way. Bovens calls this '*accountability as a virtue*'. Accountability as a virtue is largely defined by bad governance: what is irresponsive, opaque, irresponsible, ineffective or even deviant behaviour. Accountability as a virtue, a normative concept, entails the promise of fair and equitable governance. Behaving in an accountable or responsible manner then is perceived as a desirable quality and laid down in norms for the behaviour and conduct of actors. Moreover, accountability then is not something imposed upon someone or an organisation by another actor, but an inherent feeling, the feeling of being morally obliged to be responsive, open, transparent and responsible. Hence, accountability as a virtue is a normative concept whereby a set of standards is provided for the evaluation of behaviour of public actors, and being accountable is seen as a positive quality in organisations or officials,[11] while accountability as a mechanism is used in a narrower, descriptive sense, to describe an institutional relation or arrangement in which an actor can be held to account by a forum.[20]

[10] Bovens, M. (2007): Analysing and Assessing Accountability: A Conceptual Framework, European Law Journal, 13(4):447-468.
[11] Bovens, M. (2010): Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism. Special Issue: Accountability and European Governance, West European Politics, 33(5): 946-967.

Accountability is a notion with many dimensions, different meanings to different people and different usages. In particular, accountability has been used in data protection regulation since the 1980s in the sense that the data controller is responsible for complying with particular data protection legislation and, in most cases, is required to establish systems and processes which aim at ensuring such compliance. The notion of accountability appears in several international privacy frameworks in addition to the Organisation for Economic Co-operation and Development (OECD)'s Privacy Guidelines[12], including Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)[13], Asia-Pacific Economic Cooperation (APEC)'s Privacy Framework[14], Article 29 Working Party papers[15,16] and some elements of the draft EU General Data Protection Regulation (GDPR). Notably, the EU's Article 29 Working Party recommendation on accountability to the EC in July 2010 recommended inclusion of a new principle of accountability in the GDPR. It stated (p2): *"this Opinion puts forward a concrete proposal on accountability which would require data controllers to put in place appropriate and effective measures to ensure that principles and obligations set out in the Directive are complied with, and to demonstrate so to supervisory authorities upon request."*[15]

The Global Accountability Project started by privacy regulators and privacy professionals has also been for the last few years defining and refining the concept of accountability in the context of these latest regulations. Guidance has also been produced by Canadian Privacy Commissioners outlining the form of comprehensive accountability programs that organisations adopt. The notion of accountability utilised by regulators is evolving towards an 'end-to-end' personal data stewardship regime in which the enterprise that collects the data from the data subject is accountable for how the data is shared and used from the time it is collected until when the data is destroyed. This extends to onward transfer to third parties. An example of this evolution is the development of governance models which incorporate accountability and responsible information use. Frameworks such as the EU's Binding Corporate Rules (BCRs) and APEC's Cross Border Privacy Rules (CBPRs) are being developed by legislative authorities to try to provide a cohesive and more practical approach to data protection across disparate regulatory systems, and can be viewed as operationalising accountability, as regulators increasingly require that companies prove they are accountable. Thus, BCRs require organisations to demonstrate that they are, and will be, compliant with EU Data Protection Authorities' (DPAs) requirements for transferring data outside the EU.

Based on an interdisciplinary analysis of the usage of the term accountability, we propose a generic definition to be:

> *Accountability consists of defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly.*

The focus of this definition is on what organisations need to do to be accountable and this is considered further below. A central part of this behaviour is the provisions of accounts, which we look at next.

The Notion of Account

The core of accountability, and indeed, the root word of accountability, is 'account', the scope of which can be summarised as follows[17]:

> *"… the account must … include descriptions and explanations of the actions, for two reasons. First, so that we can better understand the organisation's intentions and its understanding, or theory, of its own situation or how it might act in it. Second, because most of a steward's actions*

[12] OECD (1980): Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organisation for Economic Co-operation and Development – These guidelines were reviewed in 2013.
[13] Government of Canada (2000), Personal Information Protection and Electronic Documents Act (PIPEDA), Minister of Justice, available at http://laws-lois.justice.gc.ca/eng/acts/P-8.6/.
[14] APEC (2005): Privacy Framework, Asia-Pacific Economic Cooperation.
[15] Article 29 Data Protection Working Party (2009): The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 02356/09/EN WP 168.
[16] Article 29 Data Protection Working Party (2010): Opinion 3/2010 on the principle of accountability, 00062/10/EN, WP 173.
[17] Raab, C. (2012): The Meaning of 'Accountability' in the Information Privacy Context. In: D. Guagnin, D. et al. (Eds.), Managing Privacy through Accountability, MacMillan, pp. 15-32.

are invisible to the principal, and therefore have to be re-presented, through stories or accounts, explanations, and justifications."

On a simple level, an account can simply be defined as 'a report or description of an event.' On a deeper level, the notion of the account can be examined through a number of different lenses to be understood, including: social/ethical/moral obligations (those social standards governing businesses and individuals to do the right thing and account for their actions); business considerations, and/or good practices (to be accountable and for the business to succeed); and metrics and evidence (analysing the account from what the quantity and quality of evidence available to support it).

Traditionally, the notion of the 'account' was closely aligned with accounting, which generally involved numbers and currency, usually in the form of currency, and tracing of funds. However, the notion of the account has evolved in a manner that is applicable to cloud ecosystems, in that the account is used in much broader contexts involving all types of information, including not just numbers and currency, but documents, tables, figures, logs and any other sort of information helpful in fully examining any given situation. The notion of the account has also partially evolved in its timing, as in the past an account most often served a retrospective function, i.e. demonstrating what has happened, but now commonly is used in a prospective function, especially where something has gone wrong with the accountor providing information as to how such situations might be remedied or addressed in the future.

There is little dispute, however, that the primary driving force behind the notion of the account is the regulatory and contractual obligations required of cloud actors. Yet, quite oddly, those same dominating forces provide little guidance about what 'the account' might include, or when and where it should be provided. A good example of this is the EU Data Protection Directive 95/46/EC (DPD)[18] and other supporting legislation, and the resulting Member States' implementations, where the account is limited to requiring information to be provided by a data controller to a data subject and notification to the DPA. Recognising this deficiency, the proposed General Data Protection Regulation (GPDR), currently under scrutiny, attempts to advance matters by introducing -under certain circumstances- the performance of Data Protection Impact Assessments, the maintenance of documentation by Data Controllers (and Processors), as well as, the notification of Data Breaches. Whether the GDPR will succeed in remedying the shortcomings of the DPD remains, however, the subject of great debate.[19]

Similarly, contracts between data controllers and end users, and, to a lesser extent, contracts between data controllers and data processors, also do not shed much light on the notion of the account. Indeed, the contractual provisions most commonly found in cloud contracts have taken regulatory obligations, which may be at a high level, and attempt to translate them into specific binding obligations between the parties.[20] Nevertheless, it is those same contracts that will generally dictate the necessity of an account and the legal obligations of the cloud actors.

In general, it is suggested that an account, when required and/or provided, should mean the accountable actor providing a report or description of an event or process. Forms of the account may include Data Protection Impact Assessments, notifications to supervisory authorities, notifications to data subjects, contractual compliance verifications, audit reports, investigation reports and even certifications and seals obtained by data controllers and/or data processors from third party certification agencies such as the Cloud Security Alliance. Ultimately, the account, while contextually and factually dependent, should generally include the answers to what are traditionally referred to as the 'reporters' questions', i.e. who, what, where, when, why and how, backed up with as much evidence as possible to validate the account. Often an account will also include the measures being taken to remedy a breach or failure and to prevent such breaches or failures in the future. Thus, despite the failures of the DPD, proposed GDPR, contractual definitions, and other controlling standards within the cloud ecosystem, an accountable organisation can surpass such requirements

[18] European Commission (EC) (1995) 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[19] See DB-5.1 Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation for a detailed analysis of the DPD and the proposed GDPR.

[20] It is also important to note that contractual obligations are not only based on regulatory obligations. Non-legislative obligations such as industry standards and certifications or even accepted industry norms can also be included into agreements, transforming those standards into legal contractual obligations.

and achieve accountability by simply doing the right thing in fully describing, documenting and supporting its description of any given event and its response to that event. Ultimately, that will prove to be the real notion of the account.

Accountable Organisations

Accountable organisations are those organisations that commit not only to legal but, also, to moral obligations dictating responsible behaviour. As far as the project's scope is concerned, responsible behaviour implies responsible stewardship of personal and confidential data processed in a cloud ecosystem from the time of collection until the time of deletion, including the onward transfers to and from third parties. Accountable organisations, firstly, are driven from moral incentives and, secondly, take concrete steps to implement accountability in practice. The implementation of accountability through concrete measures is facilitated, of course, provided that organisations have adequate resources; large organisations due to their financial capacity have, therefore, greater flexibility compared to Small and Medium Enterprises (SMEs) in terms of the technical and organisational measures they employ.

Accountable Organisations and their Moral Obligations

Accountable organisations do not only aim for compliance with law but take decisions based on ethics and values too. This was reflected when we considered above the aspect of 'accountability as a virtue'. Behaving accountably in accordance with legal rules because one is forced to do so differs from accountable behaviour driven by inner convictions; the latter will generally be more extensive than the former. Accountability as defined in A4Cloud refers − among other things− to the obligation to act as a responsible steward with respect to personal information of others. This obligation is not only legally prescribed, but also implied by the values of good governance (behaving responsibly) and the definition of a community (the other).

Moral obligations, in general, are considered as requirements or promises derived from social norms. They are linked to the content of the account since giving an account is one means by which individuals and organisations are constituted as moral agents. The account or the 'subject of accountability' refers to what individuals and organisations are accountable for, namely, their actions and the results produced, as well as their intentions. Moreover, moral obligations require a public: the moral community. Organisations must become more responsive to others, by seeking an understanding of accountability that formally recognises the obligation to others – even if it does not and cannot reflect the original relationship from which this obligation derives.[21] In other words, the scope of the moral community to which an organisation is accountable is extended as organisations are held accountable to a wider scope of good than their own.

For organisations to behave as moral agents entails a reflection upon the question of what good governance means to them. Organisations therefore should not only focus on accountability as mechanisms of control, but also on accountability as doing the right thing, with the right outcomes, for the right reasons. Despite the lack of general standards for accountable behaviour, organisations' accountability might still imply the presence of one or more (in)formal norms against which the actual and active behaviour of the organisation in question will be assessed. The ethical aspect of accountability for an organisation entails an iterative learning cycle of implementing, executing and reflecting upon good governance, for–itself and for-the-other.

Implementing Accountability in Practice

An accountable organisation – amongst other things – must define what should be done, monitor how it is done, remedy any discrepancies between definition and fact, and explain and justify relevant actions. Senior management must support accountability with concrete actions at an organisational level, while a reporting structure based on the allocation of responsibilities to employees should be established. Building on that approach, A4Cloud identifies three additional

[21] Shearer, T. (2002): Ethics and Accountability: From the For-itself to the For-the-other. Accounting, Organisations and Society 27 (6) (August) pp. 541–573.

aspects that need to be explored further, focusing largely on the relationship between accountable organisations and external stakeholders[22]. Note that the A4Cloud tools put emphasis on those additional aspects identified by the project. In particular, those three additional aspects relate to:

1. The way accountability extends across their service supply chains, ensuring that the services and the actors taking part in the accountability chain are accountable too. This could be implemented in practice through the proper allocation of responsibilities and the provision of evidence linking to the compliance with obligations across the service provision chain.
2. The way in which accountable organisations interact with other entities needs to be clarified. The cloud customer, for example, or the data subjects might, also, play a role by putting forward their own requirements, which could then be "negotiated" with the accountable organisation.
3. The way that the enforcement and verification mechanisms for accountability will operate, the scope of risk assessment and the ways in which others take holders are able to hold an organisation to account.

In practice, organisations often develop Codes of Ethics or Codes of Conduct[23] to explicate and enforce moral (ethical) norms and guide behaviour[24]. This approach generates improved business performance and risk reduction. However, it might also have limitations if these values are not developed in a participative way (i.e. they are imposed top down) or without consulting external stakeholders (need for explicit linkages to societal expectations). Breaches of the Codes of Ethics or Conduct are sanctioned, either formally (e.g. removal from industry associations) or informally (e.g. via reputation).

In this context, A4Cloud will encourage organisations to adopt an ethical approach by providing the technical, legal and procedural mechanisms to promote moral behaviour (data stewardship), by elucidating and disseminating the business case for doing so, by facilitating the measurement of corporate accountability, by ensuring that our solutions are socially acceptable and meet the needs of stakeholders and by creating optimal incentive structures for accountability.

The SME Perspective

SMEs are considered to benefit significantly from cloud computing technology. Cloud computing allows them to "acquire at a marginal cost, top-class technologies, which would otherwise be out of their budget range"[25,26]. Due to the absence, though, of adequate financial capacity, SMEs often cannot maintain their own specialised departments to lead the accountability practices as a whole; certain responsibilities must be allocated, essentially, to third parties. Third parties might, therefore, get involved in:

- Consulting and/or outsourcing services on the specification of the privacy management programme. On the grounds of the business objectives of an SME, which presuppose a given set of the SME customers' personal data that have to be collected and processed, external consultants can help SMEs in the identification of their legal obligations.
- Consulting and/or outsourcing services on the delivery of a creditable risk assessment plan, which will help the SME identify the potential business risks from the collection and processing of their customers' personal data.
- Consulting services to drive SMEs to properly implement accountability mechanisms.
- Consulting services on the liability measures arising from the exposure of a failure in the correct implementation of the organisational data protection practices.
- Outsourcing services for periodic internal audits to verify the compliance of the implemented mechanisms with the organisational data practices.

[22] Note that due to the scope of the project and our understanding of the notion of the account, external stakeholders refer to whosoever might be concerned with the EU Data Protection Directive 95/46/EC (DPD) and the proposed General Data Protection Regulation (GPDR).
[23] See for example the work performed by the C-SIG groups of the European Cloud Strategy (in particular the C-SIG CoC).
[24] De Colle, S., Gonella, C. (2002): The Social and Ethical Alchemy: An Integrative Approach to Social and Ethical Accountability. *Business Ethics: A European Review* 11 (1): 86–96. doi:10.1111/1467-8608.00261.
[25] Article 29 Working Party (2012): Opinion on Cloud Computing, WP 196, July, p. 4.
[26] See also: 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

The involvement of third parties in the implementation of an accountability based approach does not necessarily increase financial costs. The support that SMEs can obtain – both externally and internally – might compensate for the limited financial and technical resources available. Industry associations, for example, are in the position to play a role in promoting suitable privacy programmes specifically addressed to SMEs. Also, notably, the role of each employee becomes naturally more prominent within the context of SMEs with limited number of employees. Taking into account that the individual actions – or omissions – may create a direct on impact on the organisation's profile, employees have additional incentives to behave in an accountable manner following an in depth understanding of their moral obligations. Subsequently, the accountable behaviour of personnel could decrease to some extent dependencies to external consultants; accountable employees, aware of their roles, can ensure and accelerate the implementation of organisational policies and the monitoring of compliance to data practices.

Accountability in Cloud Ecosystems

The *cloud ecosystem* is a business ecosystem of interacting organisations and individuals − the actors of the cloud ecosystem – who provide and consume cloud services. In other words, the main stakeholders in the cloud ecosystem are cloud providers and cloud users. In this ecosystem the stakeholders interact in a constant process of change. Moreover the stakeholders within the ecosystem are controlled not only by the internal factors of the system, such as codes of conduct and existing relations, but also by external factors such as regulations, the wider environment or even required skills. Within cloud ecosystems accountability is becoming an important (new) notion, defining the relations between various stakeholders and their behaviours towards data in the cloud.

A4Cloud's cloud accountability combines the notions introduced earlier of accountability as a mechanism and accountability as a virtue within the private sector of cloud computing and its cloud ecosystem. Our approach is to build on these notions to incorporate accountability in the cloud ecosystem by allowing for a mechanism that ensures the possibility of giving account *ex post facto* (via accountability tools) and steering accountability behaviour *ex ante* (via accountability as a virtue). Accountability as a virtue is extended to apply to cloud actors including cloud service providers, and accountability as a mechanism entails the social relation between the accountor and accountee that involves an obligation to explain and justify conduct.

We provided a definition of accountability at the beginning of the last section (P19), but defining accountability is not sufficient to monitor and change behaviour in the cloud. This requires further operationalisation of the way accountability should be embedded in the cloud ecosystem's norms, practices and supporting mechanisms and tools. As a starting point, accountability in the cloud ecosystem should be: a) defined, b) monitored, and c) corrected in order to stimulate responsible behaviour with data in the cloud.

In addition, accountability not only requires this loop of defining, monitoring and correcting, but also the explanation and justification of the actions taken to define, monitor and correct accountability. An accountable organisation therefore must:

1. Demonstrate willingness and capacity to be responsible and answerable for its data practices
2. Define policies regarding their data practices[27]
3. Monitor their data practices
4. Correct policy violations
5. Demonstrate compliance to the cloud ecosystem's norms.

For the project scope, the accountors are cloud actors that are organisations (or individuals with certain responsibilities within those) acting as a data steward (for other people's personal and/or confidential data). The accountees are other cloud actors, that may include private accountability agents, consumer organisations, the public at large and entities involved in governance.

Based upon the definition of cloud accountability, we can identify the objects that a cloud actor is accountable for within a cloud ecosystem to be:

[27] The policies should incorporate relevant external norms, such as requirements derived from data protection regulation.

- **Norms[28]:** the obligations and permissions that define data practices; these can be expressed in policies and they derive from law, contracts and ethics.[29,30]
- **Behaviour:** the actual data processing behaviour of an organisation.
- **Compliance**: entails the comparison of an organisation's actual behaviour with the norms.

Contracts express legal obligations and business considerations. Also, policies may express business considerations that do not end up in contracts, for example that authentication of requesting parties should be carried out using OpenID. Enterprise policies are one way in which norms are expressed, and are influenced by the regulatory environment, stakeholder expectations and the business appetite for risk. Hence, accountability is framed in terms of displaying norms, behaviour and compliance and hence is broader than (but also includes) norm compliance. By the accountor exposing the norms it subscribes to and the things it actually does, an external agent can check compliance.

As we shall consider later, evidence of this accountability may be diverse: for instance, provided in the form of accounts, notifications, privacy impact assessments, certifications and any other relevant supporting information. Next we consider further who the cloud actors are, and the accountability relationships between them.

An Accountability-Based User Taxonomy in Cloud Ecosystems

There is a need to describe scenarios in terms of actors endorsing roles in a cloud provisioning ecosystem from an accountability-based perspective, using a neutral terminology that is applicable both to data protection and business confidentiality domains. In the A4Cloud project, we chose to extend the well-known NIST cloud supply chain taxonomy[31] to create the following cloud accountability taxonomy composed of seven main roles:

1. **Cloud Subject:** An entity whose data are processed[32] by a cloud provider, either directly or indirectly. When necessary we may further distinguish:
    a. Individual Cloud Subject, when the entity refers to a person.
    b. Organisation Cloud Subject, when the entity refers to an organisation.
2. **Cloud Customer:** An entity that (a) maintains a business relationship with, and (b) uses services from a Cloud provider. When necessary we may further distinguish:
    a. Individual Cloud Customer, when the entity refers to a person.
    b. Organisation Cloud Customer, when the entity refers to an organisation.
3. **Cloud provider:** An entity responsible for making a [cloud] service available to Cloud Customers
4. **Cloud Carrier:** The intermediary entity that provides connectivity and transport of cloud services between Cloud providers and Cloud Customers.
5. **Cloud Broker:** An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud providers and Cloud Customers.
6. **Cloud Auditor:** An entity that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation, with regards to a set of requirements, which may include security, data protection, information system management, regulations and ethics.
7. **Cloud Supervisory Authority:** An entity that oversees and enforces the application of a set of rules.

We briefly examine some of the key reasons that motivated us to adopt the above taxonomy. Today, the cloud taxonomy defined by NIST has been almost universally adopted by industry and academia to described cloud supply chains in terms of Consumers, Providers, Brokers, Auditors and Carriers. Yet, it has some shortcomings when it comes into describing cloud accountability roles, most notably because the end-user who ultimately owns the data is often invisible in this taxonomy and because the relevant

[28] Ruiter, D. (1993): Institutional legal facts. Legal powers and their effects, Kluwer, Dordrecht.

[29] Larenz, K. (1975): Methodenlehre Der Rechtswissenschaft, Berlin.

[30] Raz, J. (1975): Practical reason and norms, Oxford University, Oxford.

[31] Liu, F. et al. (2011): NIST Cloud Computing Reference Architecture, NIST Special Publication 500-292, September.

[32] Where processed means "*any operation or set of operations which is performed upon data*", "*such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*". (Inspired from article 2 of Directive 95/46).

supervisory authority is missing in the picture as well. Rather than creating a novel taxonomy, we decided to extend the existing NIST model to capitalise on its wide adoption, while adding roles that are necessary for providing accountability in the cloud.

The NIST cloud taxonomy defines a cloud customer as an entity that both (1) has a business relationship with, and (2) uses the services of, a cloud provider. We observe that in the data protection domain, the data subject does not always fit that definition: the data subject may not have a business relationship with a cloud provider directly (or through a broker), but rather with a cloud customer. In the business confidentiality domain a similar situation may also materialise: a business will provide data to another business, which itself uses the service of a cloud provider. This has conducted us to add the cloud subject as a distinct actor to our extended taxonomy. All actors in the supply chain are ultimately accountable to the cloud subject.

Once we add a cloud subject in our model, we need to also consider the role of the relevant supervisory authority. This is particularly clear in the data protection domain: while Data Protection Authorities (DPAs) or telecom regulators (NRAs) may be seen as cloud auditors in the NIST model, they also have the distinct characteristic of holding enforcement powers (in a similar way to the EC defining the competent authority that should be designated in all Member States, as per the February 2013 Proposal for a directive of the European parliament and of the council concerning measures to ensure a high common level of network and information security across the Union). This has similarly conducted us to include the cloud supervisory authority in our extended taxonomy.

In some cases, in order to facilitate the discussion, we found it useful to further distinguish both cloud subjects and cloud customers as individuals or organisations. Furthermore, some actors may endorse more than one role. For example, in the original NIST model, cloud customers may also act as cloud providers. This is also true in our taxonomy where additionally cloud subjects may act as cloud customers, and the supervisory entity may act also as an auditor in some situations. As a final note, we slightly altered the original definition of cloud auditor proposed by NIST to better encompass the scope of the A4Cloud project, which does not only encompass security but also more generally compliance.

Accountability Relationships

Our discussion enhances cloud deployments by adding accountability relationships. The NIST cloud recommendations allow us to structure the discussion, but do not deal with emerging data protection problems that can be to a certain extent addressed by accountability and related accountability mechanisms. Structured representations of the chains of accountability allow comparison of different cloud ecosystems and identification of accountability relationships supported by different mechanisms. The analysis of any particular cloud ecosystem should identify specific accountability relationships among actors and how they relate to the elements of accountability in high level scenarios relating to the treatment of personal and of business sensitive information within service provision chains. The discussion of such roles in terms of accountability allows us to identify specific responsibilities. Moreover, the identified cloud computing roles extend the ones identified from technical considerations of cloud computing. The discussion of specific scenarios further points out roles and responsibilities in cloud ecosystems.

In a given scenario, and from a data protection perspective, as shown in the table below (Cloud Actors' Roles), entities may take on data protection roles as appropriate. To understand the table, at this point it is useful to explain some terminology commonly used in data protection[33]. According to the current European data protection directive, a *data controller* (DC) essentially determines the purposes for which and the manner in which personal data is processed. A *data processor* (DP) processes personal data upon the instructions of the data controller. The *data subject* is the living person that can be identified by personal data, and the *data protection authority* (DPA) is the supervisory body. In other regulatory contexts, different roles may apply to entities, such as data owner, in a similar manner. The following table summarises the roles identified from both perspectives (i.e. cloud computing and data protection) and their possible mapping.

[33] Van Alsenoy, B. (2012): Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC. Elsevier, Computer Law & Security Review, 28(1):25-43.

Cloud Actors' Roles

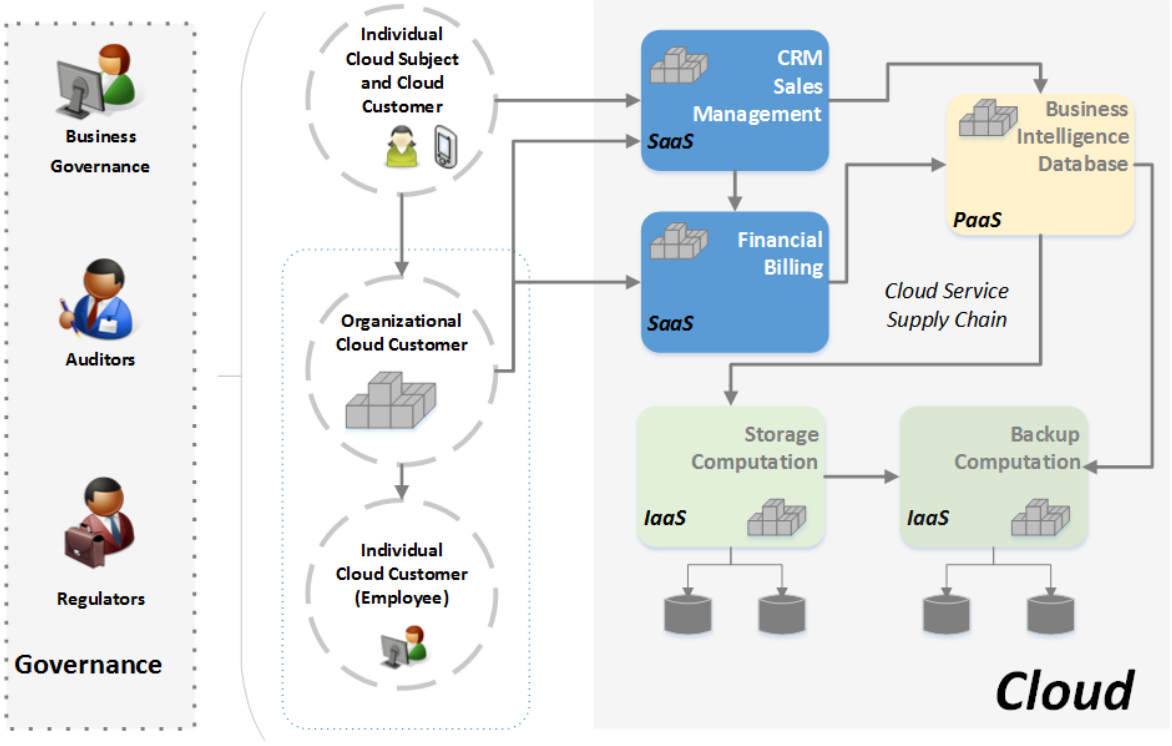
Extended NIST model role	Data protection possible roles
Cloud subject	Data subject
Cloud customer	Data controller or Data processor
Cloud provider	Data processor or Data controller
Cloud carrier	Data processor or Data controller (unlikely) or Not applicable.
Cloud broker	Data processor or Data controller
Cloud auditor	(Not Applicable)
Cloud supervisory authority	Supervisory authority (DPA or NRA)
(Not Applicable)	Third party
(Not Applicable)	Recipient

In the cloud context, cloud subjects may be data subjects, cloud customers and cloud providers would be Data Controllers (DCs) or Data Processors (DPs), and cloud carriers and cloud brokers may be DPs, or possibly DCs or else fall outside the controller/processor distinction, depending upon their function. The organisational cloud customer (which is a business or a legal person) is in general considered to be the DC and is regulated by the DPA. Even though in most cases cloud customers are not in a position to negotiate with cloud providers, they may still choose amongst offerings and hence are still considered a DC[34]. An individual cloud customer (who is a natural person) is likely to be considered to be a data subject, although there are situations where they would be considered as a DC, for example where they use a cloud service for professional purposes involving processing data of other data subjects. Cloud providers are nearly always a DP but could be a DC. They may need to assume co-controllership responsibilities, but may not know who the users are or what their services are being used for. If they process personal data which is not provided by a cloud customer, acting autonomously to define the means and the purpose of the processing, the cloud provider is a DC. On the other hand, the cloud provider is a DP if it processes personal data to provide a service requested by a cloud customer and does not further process the data for its own purposes. There are also cases where the cloud provider can be a joint DC, namely when it processes data to provide a service requested by a cloud customer but in addition further processes the data for its own purposes (e.g. advertising). In the proposed EU General Data Protection Regulation (GDPR), DPs who process data beyond the DC's instructions would be considered as a joint DC, and this case might include changing security measures or data handling practices.

Let us now consider the accountability relationships between the various actors in an example cloud ecosystem such as those illustrated by the figure below showing an example cloud ecosystem. Every party of the cloud service is called to be accountable to other parties. There are different obligations according to the roles that apply in a given scenario. The DC is accountable for applicable data protection measures. The cloud providers as DPs must provide security measures, and their responsibilities will vary according to the combination of cloud service and deployment models. For example, Platform as a Service (PaaS) providers are responsible for the security of the platform software stack and Software as a Service (SaaS) providers are responsible for security applications delivered to end users. The lower down the stack the cloud provider stops, the more security the consumer is tactically responsible for implementing and managing. The liabilities involved are expressed within contracts as there can be ramifications of failure within cloud ecosystems, affecting other parties. The DPs are accountable for co-operation with the DC to meet data subjects' rights, assist the DC in providing security measures, and should act only on the DC's behalf. Thus, there are chains of accountability through the cloud service supply chains to the cloud customer. In addition, cloud providers and customers are accountable to the actors involved in governance and enforcement, as shown on the

[34] Article 29 Data Protection Working Party (2012): Opinion 05/12 on Cloud Computing, 05/12/EN WP 196, European Commission, Directorate General Justice.

left hand side of the figure. These include regulators, stakeholders and society, as well as auditors and business governance. These are especially interested in monitoring and measuring non-functional aspects, leaving it to the service providers to determine how they actually want to achieve those. The cloud customer is in general accountable to these governance entities for applicable data protection measures. All actors in the supply chain are ultimately accountable to the cloud subject. Extending the accountability relationship between cloud providers and cloud consumers to the provider's responsibility to society at large provides a broader perspective on the need for accountability in the cloud.



Example Cloud Ecosystem

Hence, most of the data protection risks associated with cloud considered earlier should be reduced by contractual provisions that can include penalties for the service provider, and by technical and organisational measures for the customer and the service provider. If the DC is ultimately made accountable for meeting obligations right along the service provision chain, they should try to obtain contractual assurances that lessen the risk of potential weak links in dynamically formed cloud provider chains. That is, contractual agreements between the series of actors taking part in the cloud chain should provide for the accountability obligations of DCs ultimately owed to data subjects.

Accountability can be achieved via a combination of *public accountability* that is derived from transparent interaction (between subjects of personal data, supervisory authorities, regulatory bodies and DCs), legislation, soft regulation, on-going Privacy Impact Assessments (PIAs), certification, audit, public policy, etc. and *private accountability*, that is derived from interactions between DCs and data processors (premised on contract law, technological processes and practical internal compliance requirements) [35]. Furthermore, we advocate the combination of a strong and soft approach to support accountability provision. The soft approach relates to addressing how accountability can be achieved in a socially beneficial way, including ethical governance and the democratic aspect. The strong approach involves supporting accountability of practice, provision and analysis of trusted evidence to show whether or not data protection obligations have been fulfilled, verification by independent, trusted entities and certification based on such verification, and we consider this further next.

[35] Charlesworth, A., Pearson, S. (2013): Developing Accountability-based Solutions for Data Privacy in the Cloud. Innovation, Special Issue: Privacy and Technology, European Journal of Social Science Research, Taylor & Francis, UK, 26 (1), pp. 7-35.

Proposed 'Strong Accountability' Approach

In this section we argue that an accountability-based approach should have a number of characteristics that include a notion of *strong accountability.* This term has recently been proposed by Butin and co-authors[36] to describe an approach that applies not only to policies and procedures, but also to practices, so that the effectiveness of the processing of personal data can be overseen (this stresses a distinction between 'reporting' and 'demonstrating'). This is supported by precise binding commitments enshrined in law and involves regular audits by independent entities. The proposers assert that this should not be contradictory with the need for flexibility that is required by the industry. The A4Cloud project approach is similar and is described further in this section.

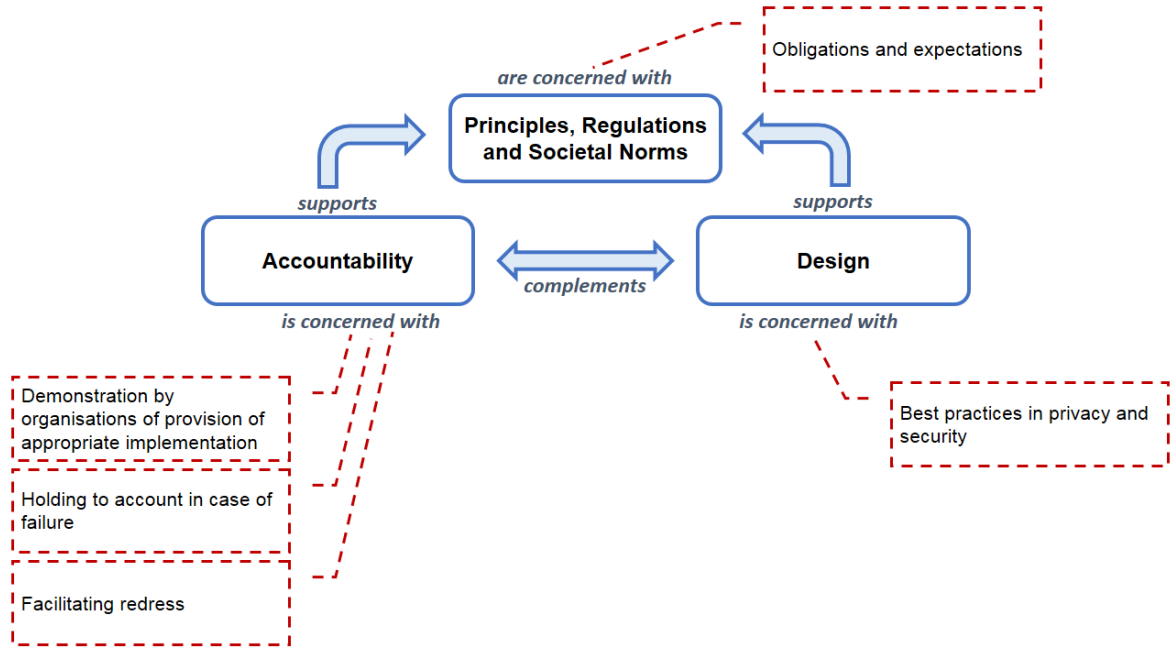
In order to avoid charges of 'privacy whitewashing', whereby apparent accountability encourages a false basis for trust in DCs by data subjects, we argue that an accountability-based approach should have the following characteristics:

- **Supporting externally agreed data protection approach:** Accountability should be viewed as a means to an end (i.e. that organisations should be accountable for the personal and confidential information that they collect, store, process and disseminate), not as an alternative to reframing basic privacy principles or legal requirements. Thus, the accountability elements in the GDPR provide a certain assurance of compliance with the data protection principles, but do not replace them.
- **Trust in the verification process:** There needs to be a strong enough verification process to show the extent to which commitments have been fulfilled. Missing evidence can pose a problem, and guarantees are needed about the integrity and authenticity of evidence supporting verification. In addition, the actor carrying out the verification checks needs to be trusted by the data subject and to have the appropriate authority and resources to carry out spot checking and other ways of asking organisations to demonstrate compliance with regulatory and contractual obligation by providing accounts that may take various forms (e.g. certificates, seals and audit reports). This is why the data protection authorities will need to play a key role in the trust verification, for example in data protection certification. In terms of external governance mechanisms, strong enforcement strategies, not only in terms of verification, but also in terms of increasing the likelihood of detection of unlawful practices and strong penalties if caught, seem to be a necessary part of accountability. Data protection impact assessments, codes of conduct and certifications are proposed to increase trust in cloud providers who adhere to them. It is thus of the utmost importance that regulatory and supervisory bodies have a primary role in the verification of the level of compliance of these tools. Furthermore, to give data subjects give back some control it would be another level of interaction if the data subjects' comments and needs receive a response and ideally even show some fundamental development in the application or organisational data processing. This form of feedback to the data subjects (in response to their feedback) is another form of verification. There are further related aspects supporting this approach in terms of responsibility and transparency, as listed below.
- **Clarity and acceptance of responsibility:** The relationship between controllers and processors in cloud service provision chains can sometimes be complex. The commitments of the data controller need to be well defined – this is (part of) the aspect of responsibility, that is an element of accountability. The respective responsibility of cloud customers and cloud providers will need to be defined in contracts and the definition of standard clauses by the industry, as validated by regulators, will help cloud customers with lower negotiation capabilities. The commitments of the data controller should include all applicable legal obligations, together with any industry standards (forming part of the external criteria against which the organisation's policies are defined) and any other commitment made by the data controller. Once again, the responsibilities of the entities along the cloud provider chain need to be clearly defined, including relative security responsibilities. On the other hand, certain tasks will need to be jointly carried out to be effective, such as risk assessment and security management. In this case there is a clear need for cooperation and coordination. Note that to what extent cloud providers should be considered as controllers or processors remains questionable.[37]

[36] Butin, D., Chicote, M., Le Métayer, D. (2014): Strong Accountability: Beyond Vague Promises. In Gutwirth, S., Leenes, R., De Hert, P. (Eds.), Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges, Springer.
[37] Van Alsenoy, B. (2012): "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC." *Computer Law & Security Review*, 28, pp. 25-43.

- **Transparency:** A main goal of accountability is to go beyond regulation through fostering transparency about actual practices and thus enabling promotion of good data handling practices, in a proactive sense. The commitments of the data controller(s) need to be expressed in an understandable language by the data subjects affected and other parties as appropriate – this is a key transparency aspect. In addition, the mechanisms used and relevant properties of the service providers in the provision chain need to be clarified as appropriate to cloud customers and regulators. It would also be beneficial to integrate social interaction between data subjects and the cloud infrastructure and service providers, for example via feedback mechanisms that enable comments on privacy policies and data usage reports.[38] Furthermore, data protection impact assessments and privacy impact assessments are forms of verification for accountability (that should be used in conjunction with others) that can be used to help provide transparency about the nature of the risks, including the criteria used in the risk assessment, how decisions are made to mitigate risk, and whether the mechanisms to be used and implemented are appropriate for the context. Comprehensive obligations for controllers to inform supervisory authorities and data subjects of personal data breaches would further increase transparency.
- **Avoidance of increased risk:** Technical security measures (such as open strong cryptography) can help prevent falsification of logs, and privacy-enhancing techniques and adequate access control should be used to protect personal information in logs. Note however that data that is collected for accountability might be itself data that can be abused and hence needs to be protected as much as the processed data. The potential conflict of accountability with privacy is somewhat reduced as the focus in data protection is not on the accountability of data subjects but rather of data controllers, which need to be accountable towards data subjects and trusted "intermediaries".
- **Avoidance of increased burden:** Accountability must deliver effective solutions whilst avoiding where possible overly prescriptive or burdensome requirements.
- **Avoidance of social harm:** Accountability should have democratic and ethical characteristics. Transparency should be as high as possible, in balance with other interests (as considered above while describing transparency). Mechanisms should also be developed to help regulators do their job, notably with respect to enhancement of the verification process as discussed above.

The following figure (Accountability Framing) shows how accountability should complement the usage of appropriate privacy and security controls in order to support democratically determined principles that reflect societal norms, regulations and stakeholder expectations.

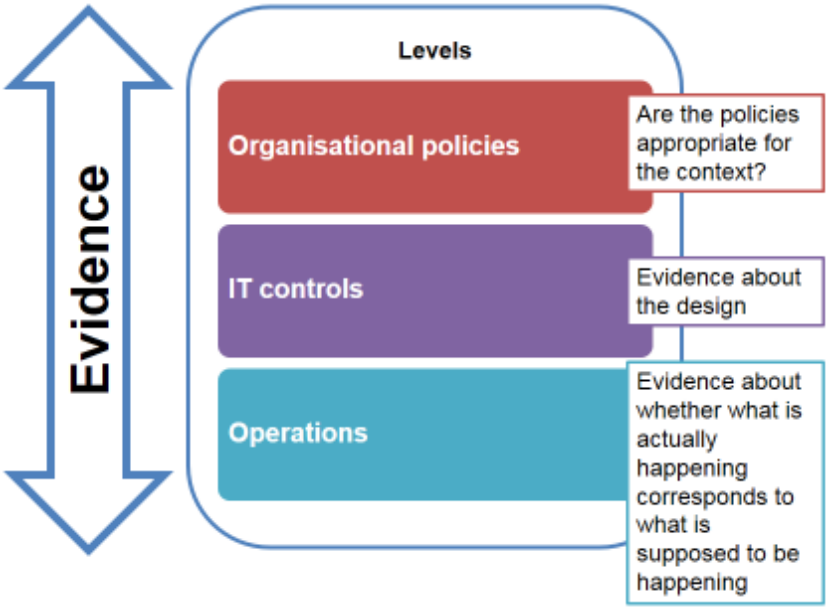


Accountability Framing

[38] Guagnin, D., Hempel, L., Ilten, C. (2012): "Bridging the gap: We need to get together". Guagnin, D. *et al.* (eds.), *Managing Privacy through Accountability*. Palgrave, pp. 102-124.

Governance and oversight of this process is achieved via a combination of Data Protection Authorities, auditors and Data Protection Officers within organisations, the latter potentially supplemented by private accountability agents acting on their behalf. As shown in the above figure (Accountability Framing), accountability and good systems design (in particular, to meet privacy and security requirements) are complementary, in that the latter provides mechanisms and controls that allow implementation of principles and standards, whereas accountability makes organisations responsible for providing an appropriate implementation for their business context, and addresses what happens in case of failure (i.e. if the account is not provided, is not adequate, if the organisation's obligations are not met e.g. there is a data breach, etc.).

Although organisations can select from accountability mechanisms and tools in order to meet their context, the choice of such tools needs to be justified to external parties. A strong accountability approach would include moving beyond accountability of policies and procedures, to accountability of practice. As illustrated in the following figure (Accountability Evidence), evidence needs to be provided at a number of layers. At the policies level, this would involve provision of evidence that the policies are appropriate for the context, which is typically what is done when privacy seals are issued. But this alone is rather weak; in addition, evidence can be provided about the measures, mechanisms and controls that are deployed and their configuration, to show that these are appropriate for the context. For example, evidence could be provided that privacy enhancing technologies (PETs) have been used, to support anonymisation requirements expressed at the policy level. For higher risk situations continuous monitoring may be needed to provide evidence that what is claimed in the policies is actually being met in practice; even if this is not sophisticated, some form of checking the operational running and feeding this back into the accountability management program in order to improve it is part of accountability practice, as described above, and hence evidence will need to be generated at this level too. In particular, technical measures should be deployed to enhance the integrity and authenticity of logs, and there should be enhanced reasoning about how these logs show whether or not data protection obligations have been fulfilled. The evidence from the above would be reflected in the account, and would serve as a basis for verification and certification by independent, trusted entities.



Accountability Evidence

Accountability is particularly hard to achieve in the cloud context, but that is actually a context where it is strongly needed. The main factors contributing to this difficulty are:

1. The complexity of technology offers
2. The necessity to split responsibilities depending on the service delivery model
3. Potential weak links in dynamically formed cloud provider chains, and
4. The current shallowness of transparency and verifiability in the cloud context.

If the data controller is ultimately made accountable for meeting obligations right along the service provision chain, they should try to obtain contractual assurances that lessen the risk of potential weak links in dynamically formed cloud provider chains. That is, contractual agreements between the series of actors taking part in the cloud chain should provide for the accountability obligations of data controllers owed to data subjects. Regarding the potential shallowness of transparency and verifiability, technical and organisational measures embedding transparency and verifiability by design are key for effective accountability. A model is proposed that includes such tools. Without this, accountability-based approaches in the cloud can only be relatively weak. Extending the accountability relationship between cloud providers and cloud customers to the provider's responsibility to society at large provides a broader perspective on the need for accountability in the cloud.

Our approach is to integrate legal, regulatory, socio-economic 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. This enables us to implement chains of accountability, including interdisciplinary mechanisms to ensure that obligations to protect data are observed by all who process the data, irrespective of where that processing occurs. To achieve this for the cloud a chain of accountability needs to be built through the cloud service supply network starting from the cloud service users, which can be overseen by regulators, auditors and business governance. A4Cloud provides a framework and technologies enabling accountability for how personal and confidential data is used in the cloud. Accountability is then the result of complying with a combination of public (external to ecosystems) and private (internal to ecosystems) criteria. Actors within cloud ecosystems use mechanisms to support accountability practices, and thereby help them to comply with relevant regulatory regimes within specific application domains.

The legal and contractual context defines the norms applicable to actors in a given cloud ecosystem, and their associated obligations, responsibilities and liabilities. Businesses need to meet these obligations, as well as obligations and requirements imposed by other stakeholders that include customers and data subjects. Before explaining more about this approach, we will present the conceptual model that underlies it.

Accountability Model

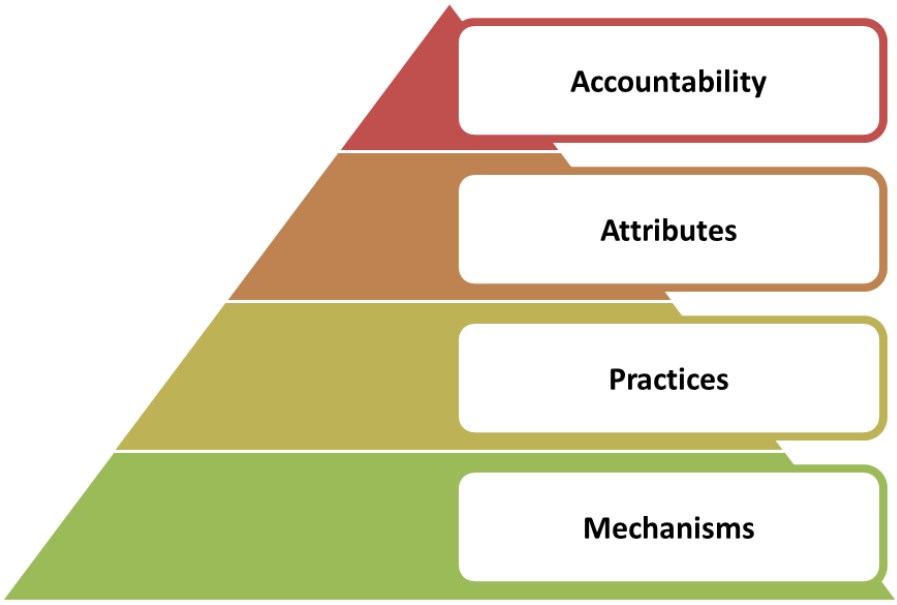
Building on a conceptual definition of accountability, we will define a model of accountability that brings together different attributes, practices, and mechanisms. This A4Cloud accountability model consists of:

- **Accountability attributes:** conceptual elements of accountability applicable across different domains (i.e. the conceptual basis for our definition, and related taxonomic analysis)
- **Accountability practices:** emergent behaviour characterising accountable organisations (that is, how organisations operationalise accountability or put accountability into practice)
- **Accountability mechanisms:** diverse processes, non-technical mechanisms and tools that support accountability practices.

An attribute is a characteristic of an object, and can be a conceptual component as well as a concept on its own. Accountability attributes encompass elements and properties of accountability at the conceptual level. Accountability practices characterise organisational behaviour, and hence define what it means to be an accountable organisation. Diverse mechanisms are used in order to support such practices. The following figure (Accountability Attributes, Practices and Mechanisms) illustrates how attributes, practices and mechanisms form a model of accountability for cloud ecosystems.

Accountability is described in terms of accountability attributes. These accountability attributes are operationalised (that is, put into practices) by organisational accountability practices. Accountability practices need to comply with and mediate between external criteria (drawn from relevant regulatory regimes and ethical attitudes) and internal criteria (characterising organisational culture). In order to implement such practices, organisations use different accountability mechanisms tailored to their domains. On the one hand, organisations adopt mechanisms in order to address their needs. On the other hand, they shape (that is, adapt or modify) them in order to embed organisational knowledge derived from experience. These mechanisms therefore constrain and support accountability practices, and the operational implementation of the accountability attributes. The emerging relationships between accountability attributes, practices and mechanisms give rise to an operational interpretation of

accountability. This characterisation explains how organisations may attain accountability in different ways, that is, instantiate this accountability model differently according to their particular contexts.



Accountability Attributes, Practices and Mechanisms

The top layer of the model corresponds to the definition of accountability within cloud ecosystems produced through consideration of relevant interdisciplinary literature, namely:

> *Accountability for an organisation consists of accepting responsibility for data with which it is entrusted in a cloud environment, for its use of the data from the time it is collected until when the data is destroyed (including onward transfer to and from third parties). It involves the commitment to norms, explaining and demonstrating compliance to stakeholders and remedying any failure to act properly.*

This definition differs slightly from the more generic one given at the start of this document, for the following reasons. Security and privacy management is evolving into an information stewardship problem; in the cloud, it will be harder to establish the risks and obligations, implement appropriate operational responses and deal with regulatory requirements. Notions of transparency and assurance receive more emphasis and it is necessary to ensure 'chains of accountability'. Accountability places a responsibility upon an organisation that uses personal information to ensure that the contracted partners to whom it supplies the personal information are compliant, wherever in the world they may be. So, the communities responsible for data stewardship place responsibilities/constraints on other individuals or on the way systems operate, and these constraints are met along the chain of provision. Furthermore, the scope of the project focuses attention on personal and/or confidential data. We now consider the other layers of the model in turn.

Accountability Attributes

Accountability attributes capture concepts that are strongly related to and support the principle of accountability. We propose a number of attributes, coming from our analysis at the topmost layer, i.e. from our definition and related literature. The core (key) attributes are: transparency, responsiveness, responsibility and remediability. In addition, as we shall see, verifiability is a key property of an object of accountability, and accountability indicators about the measures used by an organisation include the key attributes of appropriateness and effectiveness. We now consider these notions in more detail. We shall distinguish between attributes that we consider to be key to the concept of accountability, in the sense that they are most associated with our definition of accountability and related notions in the literature, and those that we consider to be of secondary relevance, in the sense that they are not necessary elements of accountability or have a strongly overlapping meaning to a key attribute.

With reference to the objects defined earlier that one should be accountable for in the cloud ecosystem (i.e. norms, behaviour and compliance), we define key attributes of accountability. From the definition of accountability given above, the core attributes are suggested in a direct way: 'commitment to norms' and 'demonstrating compliance' suggest that transparency is an important element; 'explaining to stakeholders' suggests responsiveness; 'accepting responsibility' suggests responsibility; 'remedying failure to act properly' suggests remediability. More specifically, these key attributes refer to:

- **Transparency**: the property of a system, organisation or individual of providing visibility of its governing norms, behaviour and compliance of behaviour to the norms.
- **Responsiveness**: the property of a system, organisation or individual to take into account input from external stakeholders and respond to queries of these stakeholders.
- **Responsibility:** the property of an organisation or individual in relation to an object, process or system of being assigned to take action to be in compliance with the norms.
- **Remediability:** the property of a system, organisation or individual to take corrective action and/or provide a remedy for any party harmed in case of failure to comply with its governing norms.

By 'system' here we mean (parts of) the accountable cloud ecosystem, which could for example be a chain of cloud providers or an IT process, which should be accountable to humans. However, since in a legal sense the entities further down the chain are not accountable to cloud customers, but rather to the entity one step up the chain, often in our domain of interest the accountability property will relate to a single cloud provider.

Being transparent is required not only with respect to the identified objects of the cloud ecosystem (i.e. norms, behaviour and compliance) but also with respect to remediation. Hence transparency can be argued to be the most important attribute of accountability. A stronger definition would require demonstration of the governing norms, behaviour and compliance of behaviour as part of the definition of transparency; however, we hold that it is more natural for this aspect of demonstration to be captured mainly within the verification attribute given below. A weaker definition of transparency would only require visibility of the governing norms, but we consider this interpretation of the notion of transparency in the context of accountability to be too weak.

Responsiveness is a key element of the notion of accountability in the relation between government and electorate[39] because ultimately, it is the electorate that mandates what happens (for example, via a social contract). In the context of cloud computing the providers are private entities that determine their own actions, between the boundaries set by regulation, and if users do not like this, they can refuse to use the service. However, even in the relation between cloud providers and their users, responsiveness is required. It refers to the two-way communication relation between cloud providers and external stakeholders (such as individual cloud customers and regulators) needed within the cloud ecosystem to define part of the governing norms. Generally speaking, the audience for an organisation's account should somehow be involved with the process by which the account is produced, and not only with the product[40,41].

Responsibility is revealed through being an attribute of the accountability objects, so is slightly different from the other attributes listed here, in that for each object, process or system within an accountable ecosystem a responsible entity (i.e. cloud actor that here would be the accountor) should be provided.

The remediability attribute provides assurance that being responsible, etc. is not sufficient and further action is required in order to be accountable; although legal responsibility, namely liability, leads to remedies, accountability equally puts emphasis not only on whom to blame but how to heal. An attribute that is a property of the *objects* of accountability (i.e. norm, behaviour, compliance) is:

[39] Mulgan, R. (2003): Holding power to account: accountability in modern democracies. Basingstoke: Palgrave MacMillan, p. 11.
[40] Raab, C. (2012): The Meaning of 'Accountability' in the Information Privacy Context. In: Guagnin, D., et al. (Eds.), *Managing Privacy through Accountability*, MacMillan, pp. 15-32.
[41] However, it can be difficult to define who the audience should be. For example, an investigation report drafted following an investigation by a data protection officer to the premises of a cloud service provider is essentially the outcome of a dialectic process/interrogation with the providers' employees. Given that these investigation reports (a form of account) most probably will be kept confidential, it is questionable which entity exactly can be considered as the audience and if it is in the position always to interact.

- **Verifiability:** the extent to which it is possible to assess norm compliance.

This is a property of the behaviour of a system, service or process that it can be checked against norms. We consider this to be a core attribute because of our explanation of accountability in terms of defining and displaying relevant norms, behaviour and compliance to the norms. Other attributes that are properties of accountability objects but are of secondary relevance are:

- **Attributability**: the possibility to trace a given action back to a specific entity.

This is a property of behaviour or of a norm violation. Attributability is considered of secondary relevance as it is not explicit in our definition of accountability, but is implied in the notions of responsibility and transparency. For responsibility to materialise in a meaningful way, actions have to be attributable to those responsible for them. Furthermore demonstration of this responsibility through transparency allows for accountability.

- **Observability:** the extent to which the behaviour of the system is externally viewable.

This is a property of behaviour of a system, service or process which describes how well the internal behaviour of a system, service or process can be described by observing the external outputs of the system, service or process. Observability is considered of secondary relevance as it is not necessary for accountability (as observability implies transparency and verifiability but the opposite is not true), even though if organisations know that they are likely to be observed then they may be more likely to behave in a responsible manner. While transparency requires an actor taking actions to be transparent, observability is more passive and the actor may not even be aware of it. It is possible to be transparent (and accountable) and non-observable, by the intervention of a third party that can observe a party instead and transfer the element of transparency.
Accountability is not a binary state, but often has many factors indicating the extent of accountability of an organisation. If accountability is seen as a process in which an organisation can mature, accountability indicators can assess the maturity of the organisation, with a focus on the mechanisms used and resultant behaviour. Accountability attributes may be defined to capture the important aspect of deployment of 'appropriate and effective measures' that meet technical, legal and ethical compliance requirements, and act as this type of indicator:

- **Appropriateness:** the extent to which the technical and organisational measures used have the capability of contributing to accountability.
- **Effectiveness:** the extent to which the technical and organisational measures used actually contribute to accountability.

By 'contribute to accountability', we mean (in the light of the analysis above) contribute to defining and displaying relevant norms, behaviour and compliance to the norms. We believe that it is acceptable to refer to accountability within these definitions since they are accountability indicators (properties of the measures used to support organisational accountability).

The cloud ecosystem not only has internal factors steering accountability, there are also some external factors that have the ability or are needed to keep the process of accountability in motion. These external factors often relate to governance mechanisms that, for example, sanction when compliance is not met. Hence there are accountability attributes that relate to the process by which the accountee holds the accountor to account. One of these is punishability, which is achieved through sanctions. Another attribute relevant to this process is verifiability, which, as already considered above, allows for the provision of evidence that compliance to the norms is (or is not) met. A further relevant attribute is liability. When an actor becomes liable for his actions, one could perceive this as a form of sanctioning. Liability is the legal obligation (either financially or with some other penalty) in connection with failure to apply the norms. It is closely related to legal responsibility (although being held liable does not necessarily mean that the same entity is actually responsible[42]), and is not referred to directly in our definition, and so could be considered to be a secondary attribute.

[42] For example, according to the DPD, data controllers are always held liable towards data subjects, even in connection with a damage actually caused by data processors.

- **Liability**: the state (of an organisation or individual) of being legally obligated or responsible in connection with failure to apply the norms.

There exist emerging relationships (e.g. implication and inclusion) among the concepts described above dependent on different viewpoints of analysis (which are related to societal, legal and ethical aspects of accountability). For example: from a legal perspective, responsibilities imply obligations, which consequently may involve sanctions; liability is based upon the establishment of norms, allowing the request for remedies and the imposition of sanctions should these norms not be met. If the norms are not met it is not necessarily the case that all related failures can be entirely remedied (e.g. in case of a data breach the "harm" resulting from the disclosure of information is done and that cannot be entirely corrected).

Accountability Practices

From the definition of accountability we can see that, in our model, an accountable organisation:

- 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; this is ensured/checked via the commitment to norms, explaining and demonstrating compliance and remedying any failure
- Explains and justifies those actions, namely, demonstrates regulatory compliance that stakeholders' expectations have been met and that organisational policies have been followed
- Remedies any failure to act properly, for example, notifies the affected data subjects or organisations, and/or provides redress to affected data subjects or organisations, even in global situations where multiple cloud providers are involved.

However, how accountable organisations implement accountability is just one aspect; the other, as we have discussed above, relates to the incentives that drive them to an accountability-based approach. Further detail is now provided about what this involves.

Implementing Accountability in Practice. An accountable organisation must define what should be done, monitor how it is done, remedy any discrepancies between definition and fact, and explain and justify relevant actions. Senior management must support accountability with concrete actions at an organisational level, while a reporting structure based on the allocation of responsibilities to employees should be established. In this context, as considered briefly above, the Accountability Project[43] and related opinions[44] point out four key actions that need to be taken by an organisation to be considered accountable: a) define and deploy policies regarding data practices, b) monitor data practices, c) correct policy violations and d) demonstrate compliance with norms.

Building on that approach, A4Cloud identifies two additional aspects that need to be explored further, focusing largely on the relationship between accountable organisations and external stakeholders:

1. These interactions need to be clearly defined. Accountable organisations must ensure that accountability extends across their service supply chains, ensuring that the services and the actors taking part in the accountability chain are accountable too. This could be implemented in practice through the proper allocation of responsibilities and the provision of evidence linking to the compliance with obligations across the service provision chain. Furthermore, the way in which accountable organisations interact with other entities needs to be clarified.
2. There are implications in terms of the way that the enforcement and verification mechanisms for accountability will operate, the scope of risk assessment and the ways in which other stakeholders are able to hold an organisation to account.

[43] CIPL: Accountability Project (Galway Project), Center for Information Policy Leadership. http://www.informationpolicycentre.com/accountability-based_privacy_governance/.
[44] Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner for British Colombia (2012): Getting Accountability Right with a Privacy Management Program, http://www.oipc.bc.ca/guidance-documents/1435.

Implementing accountability in practice is not simply a matter of good will. On the contrary, it depends on the available resources, which may vary highly between large scale organisations and Small and Medium Enterprises (SMEs).

Corporate Governance for Privacy. Implementing accountability in practice requires accountable organisations to act as responsible stewards of the data they are entrusted with in the cloud, ensuring responsible behaviour via accountability mechanisms and balancing innovation with individuals' expectations. Nevertheless, accountability should not be seen as an equivalent to privacy[45]. In addition to the accountability mechanisms, privacy controls[46] and security techniques including encryption need to be used.

Not all organisations have the same resources, so the development of privacy management programmes will inevitably differ. Large organisations may have a Chief Privacy Officer and privacy staff in order to ensure compliance in their organisations. Smaller organisations will often not have the resources for hiring qualified privacy experts. As a result, responsibility for compliance with applicable privacy legislation may well rest with the owner or the operator. In such circumstances, key elements of privacy management, such as defining a corporate privacy policy can be difficult to achieve. Many small companies operate within a single state and are affected solely by domestic legislation, although small companies in niche technology areas may quickly find themselves becoming multinational. For multinational companies, requirements are more diverse and privacy management is more difficult. Nevertheless, data is an asset, so proper privacy management will be valuable for forward-thinking companies, quite apart from being mandatory from a legal point of view.

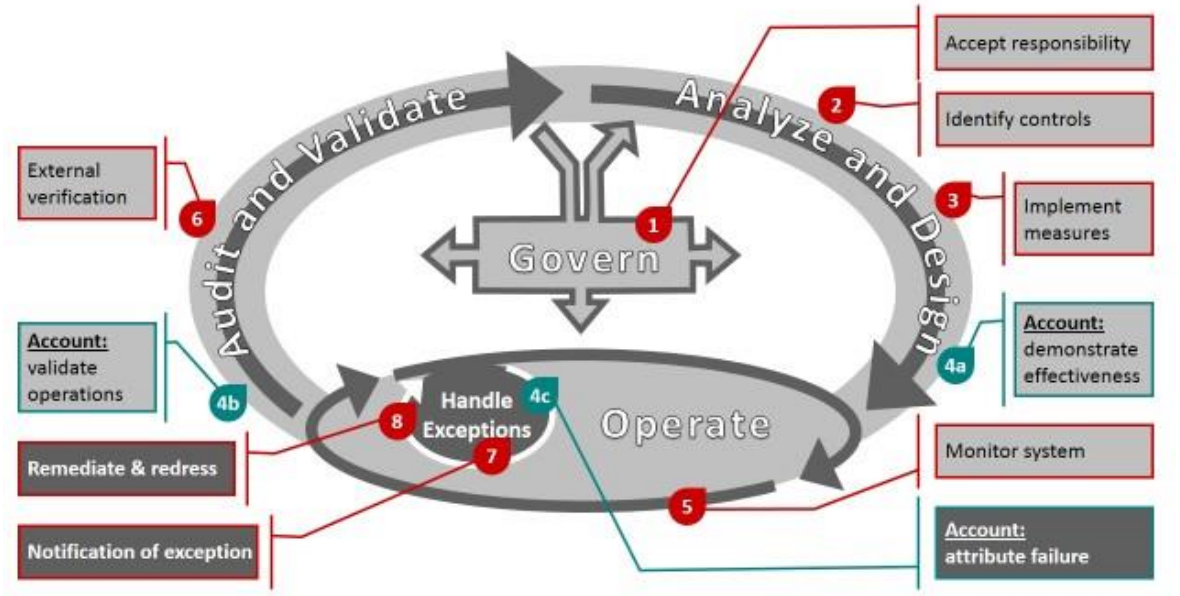
Accountability practices form part of the emerging organisational culture resulting from following an accountability approach. The *functional elements* of accountability within such a process are as follows:

1. *Accept responsibility*: as part of the governance for the organisation, the management accepts responsibility for data protection objectives, and establishes and sponsors the operational structure and process to meet these objectives
2. *Identify controls*: this is the first step of the risk mitigation lifecycle. It starts with a risk analysis, which identifies all business processes related to the data protection objectives and documents each application and people process. Business management performs the risk analysis to ensure that the perspective is from a business view. These risks are then analysed and the proper treatment is determined. This treatment could correspond to adaptations in the business processes, or a treatment through organisational or technical measures, the latter being rolled-out in terms of controls. This process should include appropriate identification of privacy and security by design techniques and consideration of measures and certification that would be required along the whole of the cloud service provision chain.
3. *Implement measures*: these have been selected in the previous step.
4. *Provide an account*: the account plays a central role in accountability. Several steps in the overall lifecycle explicitly address the account:
    a. Demonstrate effectiveness: this is a static validation, based on the risk analysis and decisions taken for the risk treatment, with the objective of doing a first validation of the complete system and of validating what will be reported in the account. Further (periodic) provision of an account is considered within 6. Below.
    b. Validate operation: this step of the audit and validate part of the risk mitigation lifecycle involves reporting the operational aspects of the system to the party to which the account is owed.
    c. Attribute failure: in this step of the incident response and mitigation lifecycle, the provider reports to its customer the attribution of the failure corresponding to the incident

[45] Bennett, C.J. (2012): The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats. In: D. Guagnin, D., et al. (Eds.), Managing Privacy through Accountability, MacMillan, pp. 33-48.
[46] For instance, privacy controls such as those developed within PrimeLife: Camenisch, J., Fischer-Hübner, S., Rannenberg, K. (Eds.) (2011), Privacy and Identity Management for Life, Springer.

5. *Monitor the system*: this groups all processes associated with the monitoring of the systems, collection of metrics, of logs and of other elements which constitute the foundation by which the organisation of the provider can demonstrate to its customers, auditors, and regulatory authorities that it meets itsobligations. This is a continuous process which is part of the daily operations. It includes monitoring of the satisfaction of data protection obligations by partners and subcontractors.
6. *Provide external verification*: this is part of the 'audit and validate' phases. Executed at regular intervals, it includes most of the processes involving external parties. This includes assessment of the account of step 4b, in the context of the enforcement process in relation to the satisfaction of obligations
7. *Notify:* for example, an incident or data breach.
8. *Provide remediation and redress*.

Such points identify an iterative accountability process consisting of cycles of operationalisation and interpretation of accountability attributes by practices, and cycles of adoption and assessment of accountability mechanisms and tools supporting accountability practices. The figure below (Functional Elements of Accountability in an Organisational Lifecycle) shows how the functions listed above are triggered at different phases of an organisation's operational security lifecycle, and how some of these (namely attribution of failure, notification and remediation) are triggered within exception loops corresponding in this case to non-satisfaction of obligations, for example by a data breach. It can be seen how there is involvement both of proactive elements (clarification and acceptance of responsibility, determination and implementation of appropriate measures and preparation of a demonstration that these meet the obligations involved for when it might be needed), as well as reactive elements (corresponding to detection and handling of data breaches or other non-satisfaction of obligations).



Functional Elements of Accountability in an Organisational Lifecycle

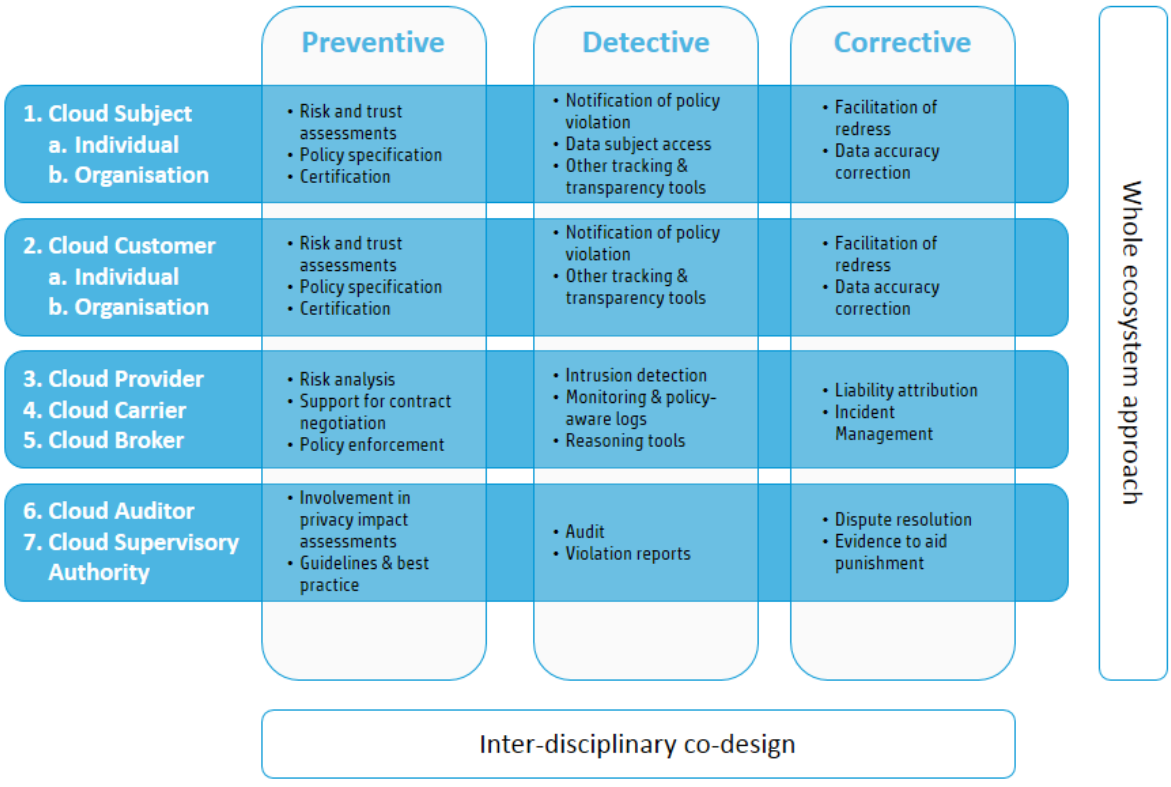
Accountability Mechanisms

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 organisations need to achieve). Organisations can adopt different available accountability mechanisms (e.g. security controls, policies, tools, standards, legal mechanisms, penalties) as appropriate for their contexts. They will use what suits their particular processes best, demonstrating that the appropriate mechanisms have been selected. Accountability mechanisms focus on the core aspects of accountability (e.g. remediation, notification and risk assessment) and as discussed above are expected to be used in conjunction with separate privacy and security mechanisms.

A combination of legal requirements, governance mechanisms and technical measures can be used to enable chains of accountability to be built along cloud service provision chains. The aim in particular is to strengthen the accountability of organisations that use cloud services and organisations that provide cloud services to data subjects and regulators. Accountability promotes implementation of practical mechanisms whereby legal requirements and guidance are translated into effective protection for data. Legislation and policies tend to apply at the data level, but the mechanisms can exist at various levels, including the system level and data level. It could be argued that the current regulatory approaches do not provide incentives that could encourage organisations to do the right thing, thereby, going beyond the minimum required by law. Our approach is the provision of a hybrid accountability mechanism via a combination of policies, regulatory and technical means. It is a co-regulation strategy based on a corporate responsibility model underpinned primarily by contract. This approach places the onus upon the DC to take a more proactive approach to ensuring compliance, and encourages cloud service vendors and subcontractors to compete in providing services on the basis of evolving better privacy and security enhancing mechanisms and processes.

The next figure (Accountability Framework) illustrates different functional aspects of accountability, with examples of corresponding mechanisms that can be used by different types of user (shown in the rows):

- **Preventive –** investigating and mitigating risk in order to form policies and determine appropriate mechanisms to put in place; putting in place appropriate policies, procedures and technical mechanisms
- **Detective –** monitoring and identifying policy violation; putting in place detection and traceability measures, and
- **Corrective –** managing incidents and providing notifications and redress.



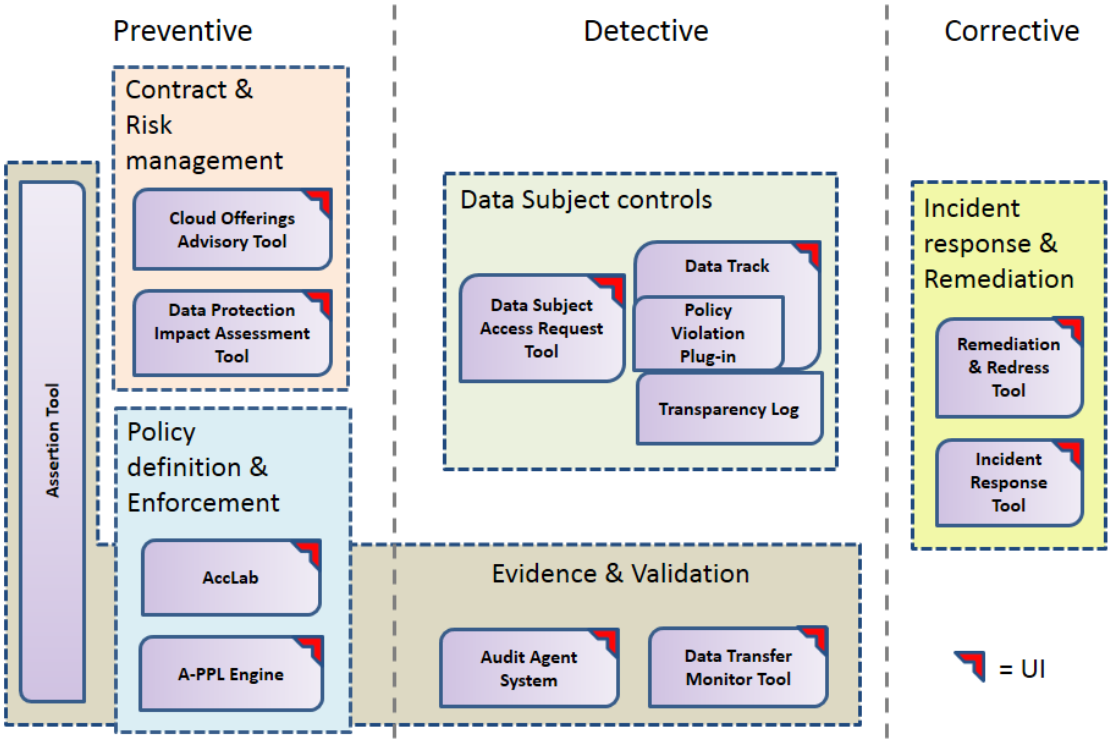
Accountability Framework

The following table illustrates how the accountability practices described in the previous section are supported by the A4Cloud tools that we are developing within the project.

How A4Cloud Tools Support Accountability Practices

Practice	Function	Mechanisms
Define governance	Policy definition	• Clear definition of responsibilities within policies • Enhancement of policies to include ethical aspects reflecting social values • Machine readable policies
Ensure implementation	Policy implementation	• Automated policy enforcement
	Risk assessment	• Data protection impact assessment
Explain & justify actions	Transparency	• Tool to support contractual transparency • Tool to support data subject access and correction
	Evidence for verifiability (e.g. within provision of accounts or for certification)	• Automated monitoring and collection of evidence tools • Assurance about accountability tools deployed
	Detection of policy violation	• Assessment of satisfaction or violation of obligations
Remedy failure	Remediation	• Remediation tool • Attribution of failure
	Exception notification	• Incident response tool

The following figure (Functional Model of the A4Cloud Tools) shows a functional model of the A4Cloud mechanisms and tools forming together the reference architecture supporting and implementing the accountability framework. The Accountability Framework enables different mechanisms, which combined together, form an architecture supporting chains of accountability in cloud ecosystems. Usage of such tools should be made in conjunction with privacy and security controls encompassing best practice as explained above, and does not replace them. Further explanation about the individual tools and the architecture is given in the A4Cloud architectural deliverables, available via the project website.



Functional Model of the A4Cloud Tools

In conclusion, current regulatory structure places too much emphasis on recovering and not enough on trying to get organisations to proactively reduce privacy and security risks. New data governance models for accountability can provide a basis for enhancing data protection when cloud computing is used. Accountability is becoming more integrated into our self-regulatory programs as well as future privacy and data protection frameworks globally. If cloud providers do not think beyond mere compliance and demonstrate capacity for accountability then there is a good chance that regulation may develop that will be difficult to follow and that may stifle innovation, or potential cloud customers would be deterred[47]. It is an upcoming challenge to strengthen this approach and make it more workable by developing intelligent ways in which accountability and information stewardship can be provided. This goes beyond traditional approaches to protect data, in that it includes complying with and upholding values, obligations, and enhancing trust. The A4Cloud Accountability Framework addresses this need in a comprehensive way. The framework based on the accountability definitions and concepts enables different mechanisms and tools. These mechanisms and tools form together a reference architecture enabling cloud service provision and deploying accountability. The A4Cloud Accountability Framework together with the mechanisms supports formation of chains of accountability in cloud service provision.

Contextual Accountability in the Cloud: towards an Accountability Maturity Model

Given the challenges and complexities associated with the notion of accountability in the cloud, how can organisations assess their accountability practices in order to improve them? Despite cloud security assurance (notably, involving assurance about confidentiality) having received some attention in the past, the evaluation of accountability is still an open problem in terms of state of the art. In this section we introduce the idea of adaptive or intelligent accountability, which relates to the notion of what is appropriate to expect in terms of accountability may vary across different scenarios (i.e., contextual accountability). Furthermore, in order to aid organisations (in particular, SMEs) to assess their accountability practices in order to enable adaptive accountability, this section proposes an Accountability Maturity Model (AMM) that can be used to quantitatively assess the maturity of the mechanisms deployed to support accountability. The proposed AMM is based on well-known security and privacy control frameworks (e.g., ISO/IEC 27002 and NIST 800-53) both of which are concepts tightly related to accountability. The definition of an AMM aims to capture both the maturity of individual organisations in terms of accountability practices, as well as a measurement of the appropriateness of the measures used across whole cloud supply chains. As relates to the cloud, intelligent accountability would involve:

- moving away from “box checking” and static privacy mechanisms
- assessing potential harms to data subjects before exposing data to risks; this would be part of ongoing risk assessment and mitigation, for which privacy impact assessments (PIAs) are one important tool
- allowing organisations more flexibility in how they provide data protection so that they can use internal mechanisms and controls that make the most sense for their business situation
- employing various degrees of accountability; it might be that more stringent standards and tests for accountability could facilitate proof of cloud providers’ readiness to engage in certain activities (such as those that involve processing highly sensitive data) or even relieve them of certain administrative burdens (such as re-notification of minor changes in processing), and
- developing clever, automated analysis, automated internal policy enforcement, and other technologies to enhance enforcement and avoid increasing the human burden.

Intelligent accountability is actually a notion closely related to the principle of “accountability-by-design” (as proposed by Butin et al.[48]). As an integral part of intelligent accountability, organisations will need to spend time and resources analysing what this means to them and gaining the management support to implement necessary changes. It is well known that contextual factors affect the degree of protection that is appropriate for an organisation. For instance, from a data protection perspective, such factors include sensitivity of data, location of data (both the locations of stored data and the potential locations of transferred data), sector, whether an anonymous data set could be usable, contractual restrictions, cultural expectations, user trust (in organisations), trustworthiness of partners, security deployed in the

[47] IDC (2012): Quantitative Estimates of the Demand of Cloud Computing in Europe, International Data Corporation.
[48] Butin, D., Chicote, M., Le Métayer, D.: Accountability by Design for Privacy, prescient-project.eu/prescient/inhalte/download/3-**Butin**.pdf

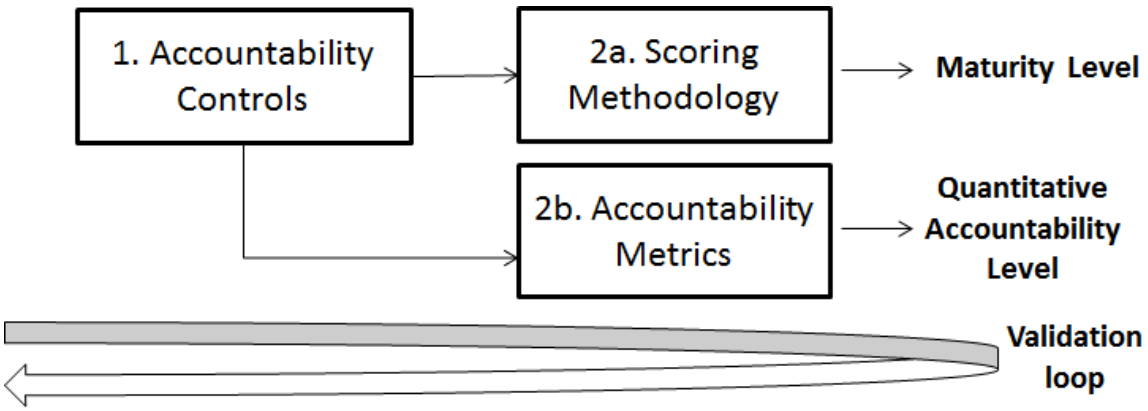
infrastructures well as potentially other factors that influence the solutions to be selected, such as expected number of users of the system and conformance to existing agreements between parties or compatibility with legacy systems. The relationship between these factors and privacy control measures that should be deployed can be complex, as suggestion of design patterns based upon contextual factors can be quite difficult.

In the rest of this section, we present the proposed Accountability Maturity Model as an approach to empower organisations (in particular SMEs) in implementing realistic levels of intelligent accountability. This approach relies on the well-known notion of capability maturity models (CMM) as introduced by the Software Engineering Institute (SEI). The CMM is generally context-aware, because it helps to understand the maturity of organisations through various characteristics. Such maturity models can help facilitate process development and enterprise evolution by identifying maturity milestones and benchmarks for comparison. In the state of the art, most maturity models consist of two basic elements:

- **Control Framework:** the actual set of individual parameters that are being considered for the assessment.
- **Scoring Methodology:** the technique used to assign a quantitative or qualitative value to the assessed control framework. In current practice, the assigned value is known as a “maturity level" and assesses how well activities in the control framework are managed.

The methodological approach to develop the proposed AMM consists of the building blocks shown in the next figure (Development of the Accountability Maturity Model) and summarised below:

- **Stage 1 – Defining the accountability controls:** During this initial stage the (accountability) controls framework of the AMM is developed. There are two possible approaches for eliciting the controls that are relevant to cloud accountability either by (i) starting from scratch developing customised controls (possibly departing from the notion of accountability attributes), or (ii) applying a gap analysis to relevant security/privacy controls frameworks in order to select those individual controls relevant for cloud accountability.
- **Stage 2a – Scoring methodology:** Despite its inherent subjectivity, human stakeholders (e.g., cloud auditors, decision makers) are nowadays quite familiar with the use of high-level quantifiers known as maturity levels while assessing a control framework. The contributed AMM proposes that the scoring methodology should be consistent with the accountability lifecycle (described above), so each stage can be assessed through the degree of maturity being achieved (e.g., any of proactive, improvement, or optimising).
- **Stage 2b – Accountability metrics:** Despite the quantification features enabled by the use of the scoring methodology (Stage 2a), the obtained maturity level is usually too high-level (and often subjective) so it cannot be directly used to automate the organisation's accountability management (e.g., adaptation of data protection mechanisms in case of cyber-incidents). In this case, the usage of fine-grained metrics derived from the controls framework is a clear benefit for automation (although possibly more suitable for non-SMEs). A similar approach was recently used by the European Cloud Strategy in the field of cloud Service Level Agreements (SLAs).



Development of the Accountability Maturity Model

The AMM focuses on the type of data and the risks involved as being the central factors influencing the suitability of context-specific accountability measures (as emphasised by the Opinion of the Article 29 WP which focuses on the adoption of "appropriate measures"[49]). This principle is already part of the notion of accountability, because although some specific measures would have to be implemented for most processing operations (i.e., baseline mechanisms), for reasons of flexibility (or as often referred to instead when making a similar point – scalability), the suitability of additional measures needs to be determined on a case-by-case basis, with particular reference to the type of data and to the risks involved as argued above. It is acknowledged that accountability could reduce and even replace some existing requirements. In terms of organisational obligations that should apply across all institutions and technologies, we can include the following key aspects: transparency about policies and practices, collection of personal information only for defined and relevant purposes, use and disclosure of personal information only in ways consistent with those purposes, provision of access and correction rights to individuals, data retention and security protection for the personal information. Corresponding to the organisational mechanisms needed to meet these obligations, some may be core (fundamental, mandatory activities that should be carried out by all organisations) and some may be elective (i.e. desired activities that are nevertheless optional). Core activities will vary from one organisation to the next and will be influenced by the industry/sector as well as jurisdiction. Such activities may even vary within an organisation. In analogy, the AMM aims to be also context-aware/organisation-specific by identifying the different stages by which an organisation would become accountable.

It is not necessarily feasible and realistic for an organisation (in particular a SME) to commit to an accountability-based approach immediately: it would require organisations to gradually change their work practices and to change their culture (i.e. adaptability). The size and type of an organisation needs to be taken into account – what is appropriate for an SME is not the same for example as for a larger enterprise (i.e. context awareness), and other factors including the sensitivity of information being handled must also be taken into account. Because we acknowledge that not all organisations (in particular SMEs) will have the resources to implement the proposed intelligent accountability strategy, the contributed AMM seeks to avoid complex approaches for assessing (and improving) accountability practices e.g., when considering migrating to the cloud. This vision is achieved through (i) the use of accountability controls based on widely-used security/privacy frameworks, and (ii) adopting a scoring mechanism that is easy to apply and interpret by humans (e.g., decision makers). Both features of the proposed AMM are compatible with self-assessment approaches suitable for SME, just like the business continuity management (BCM) documented by the European Network and Information Security Agency (ENISA).Through the AMM, it is possible for organisations (including SMEs) to plan, prioritise and invest in order to progress along the maturity model until the most effective and beneficial state is achieved for the enterprise. Finally, given the gaps in existing security and privacy controls frameworks, by considering an accountability maturity model for cloud exploitation we hope to identify the key developmental stages for a number of organisational characteristics, which in turn will have implications for information security and data protection strategies. Hence it may be possible to anticipate future needs and begin delivering techniques for designing data-protection aware clouds based on the notion of intelligent accountability.

Summary

There is a rapid growth in the usage of cloud computing and correspondingly a strong need to ensure that data is adequately protected in such scenarios. New data governance models for accountability, such as those underpinning Binding Corporate Rules in Europe and Cross Border Privacy Rules in Asia-Pacific Economic Cooperation (APEC) countries, could provide a basis for providing protection of personal data and confidential information when cloud computing is used. Accountable organisations would ensure that obligations to protect such data are observed by all who process the data, irrespective of where that processing occurs. However, the cloud is an incredibly complex and challenging domain. Not only are there fundamental trust issues as highlighted by the recent PRISM revelations, but in the cloud context, the cloud client/controller may not be solely able to determine the purposes and the means of processing because the cloud provider designs the infrastructure and also to some extent the services, in a way that depends upon the cloud service model, as well as typically elaborating standard service level agreements (SLAs) with little or no customisation possibility.

[49] Article 29 Data Protection Working Party (2010): Opinion 3/2010 on the principle of accountability, 00062/10/EN, WP 173.

In addition, lack of transparency and verifiability is a major problem that needs to be addressed, and without which accountability-based approaches in the cloud just may not work. The complexity of the environment is a major challenge for solutions and indeed it still needs to be demonstrated that an accountability-based approach can really add value in a practical sense in this domain without adding to the complexity. It is the goal of the project's approach to help cut through the complexity and help provide more workable, effective solutions for data protection in cloud environments. The A4Cloud project is supporting this vision by developing:

- A framework for accountability: a comprehensive specification for accountable service provision in the cloud and other future internet service provision models, spanning regulatory, legal, technical, business and user issues.
- Trustworthy tools to support accountability (for a variety of different stakeholders). These will be largely based upon contractual assurances from cloud providers to the accountable organisation and enhanced by a number of approaches including enforcement of the corresponding machine-readable policies, greater transparency, assurance and audit, with a potential role also for decision support.

In this document we have described our overall approach and the associated novelty in terms of:

- a conceptual analysis of the concept of accountability
- a set of proposed characteristics of our approach (including strong accountability)
- a model for accountability that bridges across different layers of abstraction
- an analysis of how accountability is reflected into organisational security lifecycles.

Finally, we have proposed an accountability framework for the cloud which involves deployment of a range of accountability mechanisms within cloud ecosystems, which provide different types of evidence to support accountability of practice and not just policy and which has necessitated refinements to the NIST cloud actor taxonomy in order to properly reflect accountability relationships. This framework serves as a common conceptual basis of reference for the research within the A4Cloud project.

PART II
TECHNICAL SECTIONS

1 Introduction

It is the role of the conceptual framework work package (namely, WP 32, also referred to as WP C-2) to develop a generic conceptual framework, independent of the use cases developed in B-3, as well as context-specific models of accountability for use within the EU Cloud Accountability (A4Cloud) project. Among the purposes of the conceptual framework is to establish a common set of definitions and models of basic concepts across the project. In order to help to ensure consistent understanding of those concepts across the project, a glossary of terms is included. First we define the project scope and then set out various motivations for an accountability-based approach, before moving in the next section to analyse the concept of accountability itself.

1.1 Project Scope

The overall goal of the A4Cloud project is to develop and validate techniques for implementing accountable cloud ecosystems (Appendix A points out the project objectives as described in the Description of Work and Appendix C provides a background about the concept of cloud and cloud computing). The overall goal includes development of techniques that can enable improved trustworthiness of cloud service provision networks, and to prevent breaches of trust by using audited policy enforcement techniques, assessing the potential impact of policy violations, detecting violations, managing incidents and obtaining redress. The outputs of the project include an accountability framework (including recommendations, guidance, models of data governance, accountability metrics and a reference architecture) as well as a range of accountability tools and mechanisms. These are being developed for individuals and organisations using cloud services as well as for cloud service providers and regulators.

The focus of the project is on personal data, but in addition certain types of confidential information that may not involve personal data, such as business secrets, are being considered. The focus is particularly on the accountability of organisations using and providing cloud services to data subjects and regulators. Government surveillance, including government acquisition of data from cloud service providers, is outside the scope of this project, except where it relates specifically to a data protection law accountability mechanism: no accountability controls of the types considered in the project (which are based upon assisting compliance with domestic data protection legislation and private contracts) are likely to provide effective protection against such activities.

1.2 Motivations for an Accountability-Based Approach

Cloud computing has transformed the way information technology is delivered, promising rapid, efficient, and cost-effective deployment of computational resources across different industries, geographies and application domains. Appendix C reports a commonly-accepted definition for cloud computing provided by the United States (US) National Institute of Standards and Technologies (Mell & Grance, 2011): *"Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."* Cloud provides a market opportunity with a huge potential both for efficiency and new business opportunities (especially in service composition), and is almost certain to deeply transform our IT. Not only are there cost savings due to economies of scale on the service provider side and pay-as-you-go models, but business risk is decreased because there is less need to borrow money for upfront investment in infrastructure. However, to help realise these benefits, we need to address two potential barriers: lack of consumer trust and the complexity of compliance.

Lack of consumer trust is commonly recognised as a key inhibitor to moving to Software as a Service (SaaS) cloud models. People have increasing expectations that their data will be handled in a responsible way and will be protected by the companies they choose to share data with. Furthermore, compared to traditional server architectures, cloud customers are more concerned about the integrity, security and privacy of their data, as there is a shift from a server-health perspective to a data perspective. However, current terms of service push back risk to consumers and offer very little remediation or assurance. Furthermore, there is a perceived lack of transparency and relatively less control compared to traditional models, and this is of particular concern for sensitive information. There

have also been some cases where Cloud Service Providers (cloud providers) have been forced by subpoenas to hand over data stored in the cloud, and there is a fear that governments might also be able to get access to information stored in servers within their countries. Moreover, it is not clear what would happen if things go wrong. Would a cloud user be notified if a privacy breach had occurred, and who would be at fault in such cases? It can be much more complex to work out how redress could be obtained, and also hard to ascertain if data has been properly destroyed in case of change or bankruptcy of cloud provider. So people are concerned about weak trust relationships along the chain of service provision, especially 'on demand' models where cloud providers may have to be found quickly, and as a result it is not true that trust will be transitive right along the chain. Further analysis about trust in cloud computing is provided for example in (Pearson, 2012b).

The second barrier to migration to cloud models is the difficulty of compliance for cloud providers. A major reason for this is that data flows tend to be global and dynamic. As location matters from a legal point of view, this leads to regulatory complexity. It can be difficult to comply with legislation, especially transborder data flow requirements, and even to determine which laws apply and which courts should preside. Issues such as unauthorised secondary usage of data and inappropriate retention of data also can be difficult to address. These two issues – trust and complexity - are closely linked: cloud providers have both legal and ethical obligations to ensure privacy and protect data, and thereby demonstrate the trustworthy nature of their services.

The advantages of cloud computing can result in a higher risk to privacy and security, as we have seen above when discussing the danger of non-compliance, where issues faced in subcontracting and offshoring can be magnified. It is not just consumers who are worried about privacy and security concerns in the cloud (Forrester Research, 2011). The European Network and Information Security Agency (ENISA)'s cloud computing risk assessment report (Catteddu & Hogben, 2009) states 'loss of governance' as one of the top risks of cloud computing, especially for Infrastructure as a Service (IaaS). 'Data loss or leakages' is also one of the top seven threats listed by Cloud Security Alliance in their 'Top Threats to Cloud Computing Report' (CSA, 2010). The autonomic and virtualised aspects of cloud can bring new threats, such as cross-virtual machine (VM) side channel attacks, or vulnerabilities due to data proliferation, dynamic provisioning, the difficulty in identifying the location of physical servers or the lack of standardisation. Although service composition is easier in cloud computing, the source of services may be malicious. However, privacy and security risks may actually be decreased compared to traditional models if cloud providers with expertise in privacy and security are used.

This section argues that accountability is key to addressing these issues. It is especially helpful for protecting sensitive or confidential information, enhancing consumer trust, clarifying the legal situation in cloud computing and facilitating cross border transfers of data. Our focus here is on data protection issues in the cloud. The meaning of 'data protection' has rather more of a privacy focus in Europe, but a broader data security context in US. We focus on privacy, but some of these issues do transcend personal data handling and generalise to other types of data, beyond privacy concerns. It is likely that over time, legislation will put more emphasis on accountability: the move to cloud (and related changes) has been straining traditional legal frameworks. We discuss in the next section how right over the world, our current laws are likely to be revised, with accountability a central feature of these new laws. Further explanation is now provided about these points, from the point of view of an enterprise that wishes to provide good stewardship of the data that they handle.

1.2.1 Regulatory Complexity

The collection and processing of personal information is subject to regulation in many countries across the world. Figure 1 illustrates how many different countries have national data protection legislation in place. The United States (US) does not have a comprehensive regime of data protection but instead has a variety of laws targeted at the protection of particularly sensitive types of information that tend to be sector-based or enacted at the state level. This (sometimes inconsistent) matrix of national laws can make it really hard for businesses to ensure full compliance if they are operating in multiple jurisdictions. Hence there is pressure from organisations for greater global interoperability to be achieved via development of a clear and consistent framework of data protection rules that can be applied, in order to reduce unnecessary administrative burdens and risks.

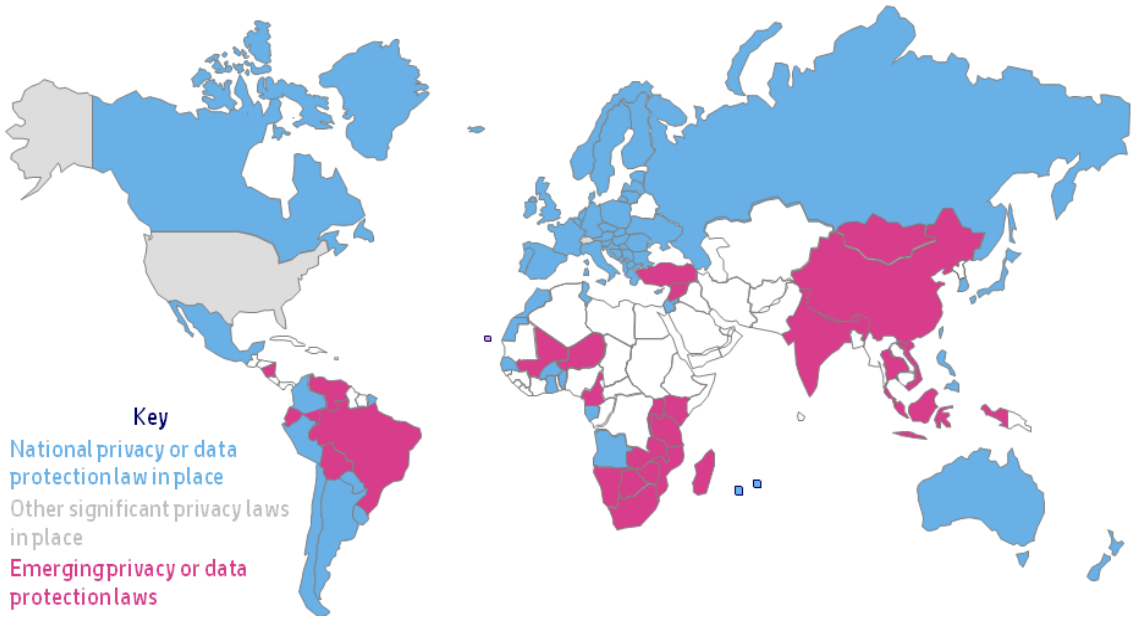


Figure 1 Global Data Protection Laws

Transborder flow of personal information, including access to this information, is restricted by some of these laws. For example, the European Data Protection Directive 95/46/EC (that we shall henceforth refer to as the DPD) (EC, 1995) (and its supporting country legislation) is an important piece of privacy legislation that restricts the movement of data from EU to non-EU countries that do not meet the EU 'adequacy' standard for privacy protection. Legislation similar to the European Data Protection Directive (DPD) has been, and continues to be, enacted in many other countries, including Australia, New Zealand, Hong Kong, Japan and Asia-Pacific Economic Cooperation (APEC). In practice contractual mechanisms like Binding Corporate Rules or Model Contracts might need to be put in place in order to allow data access. However, these arrangements typically take several months to set up, and hence are not well suited to dynamic environments. Hence the OECD revised guidelines (OECD, 2013) now recommend the practical implementation of privacy protection through an approach grounded in risk management and stress the need for improved global interoperability. With regard to security, it is a common requirement under data protection law that if a company outsources the handling of personal data to another company, it has some responsibility to make sure the outsourcer uses "reasonable security" to protect those data. This means that any organisation creating, maintaining, using or disseminating records of personal data must ensure that the records have not been tampered with, and must take precautions to prevent misuse of the information.

Of course, in addition, organisations need to take into account the privacy-related expectations of their customers, which may be specified within private contracts, and this is likely to involve a combination of process-based and access control mechanisms. The legal obligations vary according to the regulatory context and indeed there are likely to be some quite significant changes in the near future. Problems with the 1995 EU DPD (EC, 1995) as a harmonisation measure and in relation to new technologies including cloud computing have led the European Commission (EC) in January 2012 to publish a draft of replacement General Data Protection Regulation (that we shall henceforth refer to as GDPR) (EC, 2012) that is currently being discussed and revised, in which accountability features and privacy by design take greater precedence. Amongst other things, this imposes new obligations and liabilities for data processors, new requirements on data breach notification and stricter rules on international data transfers. It also empowers National Regulatory authorities to impose significantly higher fines. In addition, a European Cloud Computing Strategy (EC, 2012d) has been launched aiming at more clarity and knowledge about the applicable legal framework and making it easier to verify compliance with the legal framework (e.g. through standards and certification). Furthermore, in February 2013 the European Commission published a cybersecurity strategy (EC, 2013a) alongside a draft directive on network and information security (EC, 2013b). Once the GDPR combined with the cybersecurity strategy will be implemented, many service providers will be covered by a range of data security obligations including adopting risk management practices and reporting major security incidents.

1.2.2 The General Importance of Accountability in Cloud Ecosystems

Building upon the discussion given above, in this section the emerging issues relating to the cloud computing environment that relate to accountability are discussed at a high level. Further discussion is provided in Section 3, which looks in more detail at cloud-specific factors affecting accountability. The growth of "Big Data" - the raw material on which many new and innovative cloud services are founded and the sophisticated analytic techniques that are used by them – has resulted in increasingly large amounts of data being held by cloud service providers. However, alongside its numerous business benefits for consumers and providers of information services alike and the potential for innovation that it offers, cloud computing presents new challenges in terms of security, privacy and trust. The transfer of personal or confidential data into the cloud (Figure 2) may provide the opportunity for innovators to create new services and may provide operational advantages such as improved accessibility and reduce the probability of catastrophic loss. At the same time this may make data more vulnerable to unauthorised access or handling. The broader issue is essentially one of loss of transparency and control in what happens to data once moved to the cloud. As stewardship of data becomes shared between users and potentially complex chains of cloud providers, the former have to place trust in the cloud ecosystem and its governance. This has proven to be a significant barrier limiting the adoption of cloud computing – one that can be lifted by ensuring that there is accountability throughout the cloud service ecosystem.

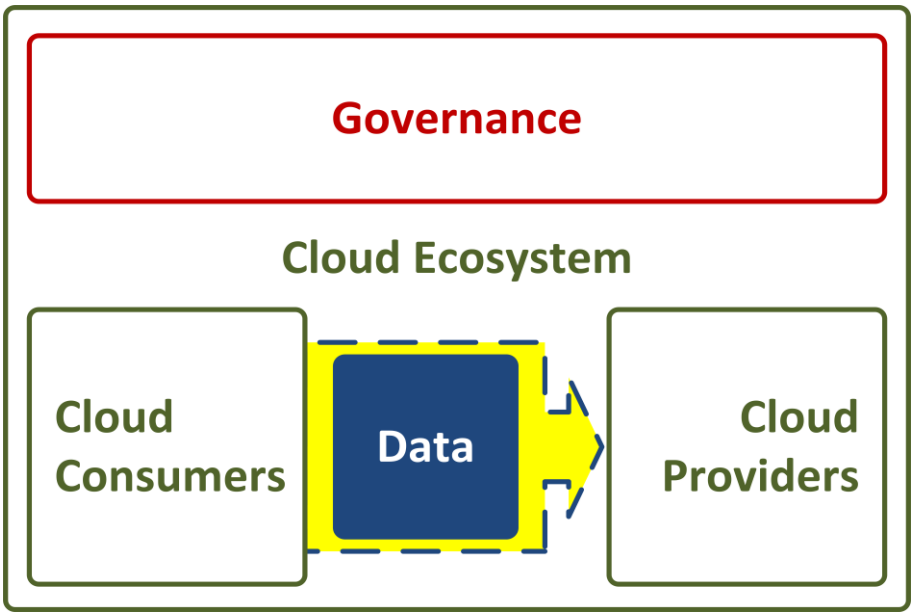


Figure 2 Cloud Ecosystem

Accountable organisations ensure that obligations to protect data are observed by all who store and process the data, irrespective of where that processing occurs. This highlights a rationale for an accountability-based approach for cloud services supporting three different aspects of data governance; those that are preventive (for example mitigating risk, and to certain extent, policy enforcement), detective approaches (such as monitoring and identifying risk and policy violation) and corrective techniques (managing incidents and providing redress).

Accountability is emerging not only as an essential aspect of data protection (for several decades it has been regarded as a privacy principle), but in particular within the deployment of cloud computing. For example, as argued within Opinion 05/2012 on Cloud Computing by the Article 29 Data Protection Working Party (European DG of Justice, 2012): *"In IT accountability can be defined as the ability to establish what an entity did at a certain point in time in the past and how. In the field of data protection it often takes a broader meaning and describes the ability of parties to demonstrate that they took appropriate steps to ensure that data protection principles have been implemented."*

Accountability, if implemented by cloud service providers, can unlock further potential cloud services by addressing relevant problems of data stewardship and data protection in emerging in cloud ecosystems. Governance is the process by which accountability is implemented in the cloud. All the actors involved in the cloud - service providers, consumers of cloud services (whether individual end-users, businesses, public organisations and even other cloud service providers), and those directly involved in IT governance have a role to play in making cloud services accountable for how data is used and managed in the cloud.

Accountability is central to a trustworthy cloud – an accountable cloud ecosystem is necessary for innovation and growth ambitions. Without accountability, cloud customers will lack confidence to put personal data (and any other confidential data) in the cloud. Cloud customers want to be confident that service providers are treating data appropriately and that they can retain control over how it is used, that the legal frameworks are effective, and that they have ways to hold providers accountable for what happens to that data. Cloud providers need a way to implement accountable cloud services.

Cloud services are defined (Mell & Grance, 2011) in terms of different essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity and measured services), service models (Software as a Service, Platform as a Service and Infrastructure as a Service) and deployment models (private, community, public and hybrid clouds). Combining such features enables different business models and cloud ecosystems involving various stakeholders (e.g. cloud customers and providers). Switching to the cloud model involves a change in control, a change in trust and security boundaries, and may be also a change in legal regulatory requirements. In order to enhance trust in cloud computing it is necessary to have a thorough understanding of the potential benefits of adopting a cloud computing model (e.g. in terms of the business opportunities that it may enable and the cost-effectiveness of business operations) and of the consequent issues and risks (Catteddu & Hogben, 2009) which may include issues of governance, compliance and legislation challenges to security and privacy risks (CSA, 2011).

Moving data to the cloud involves a shift in responsibilities across organisational boundaries – *Who can access personal data? How can personal data be used? Who is responsible for data governance? Whom to trust in the cloud?* This redistribution of responsibilities across the cloud ecosystem changes risk fundamentals (e.g. likelihood of occurrence and severity of impact) as well as risk perceptions of such threats. It becomes necessary to understand limitations of technologies (e.g. security mechanisms) as well as to identify new mechanisms and tools enhancing trustworthiness in the cloud. Implemented as tools and services and combined with legal and regulatory approaches, an accountability-based approach will enhance the confidence of service providers, business, regulators, and end users to deploy, use, and monitor cloud services. Used individually or collectively, they will make the cloud services more transparent and trustworthy for: cloud customers (who gain control and transparency over how their data is used, and support in obtaining redress), service providers (who acquire techniques to make services more trustworthy, meet business policies and allow differentiation) and for regulators (who have assurance about compliance with stakeholders' expectations and regulations).

Accountability has emerged as a relevant concept underpinning data protection. In response to data protection directives, recent research has identified some essential elements of accountability. According to the Galway Project (CIPL, 2011), these are:

1. *Organisation commitment to accountability and adoption of internal policies consistent with external criteria*
2. *Mechanisms to put privacy policies into effect, including tools, training and education*
3. *Systems for internal on-going oversight and assurance reviews and external verification*
4. *Transparency and mechanisms for individual participation*
5. *Means for remediation and external enforcement.*

These elements highlight basic features of any accountability-based approach and point out the complexity of accountability. There are a vast number of application domains such as retail, logistics, customer relationship management, financial services and healthcare to which cloud computing and cloud services may be applied. On the one hand, regulatory regimes (like the EU Data Protection Directive) constrain cloud services. On the other hand, different mechanisms and tools enable the deployment of cloud services in the many different application domains.

Accountability governance is central to maintain a compliance alignment between regulatory regimes and cloud services. Accountability provides a means to achieve compliance with respect to regulatory regimes as well as enabling transparency, security and privacy mechanisms tailored to protect data and data subjects. Figure 3 illustrates how accountability enabled cloud ecosystems position themselves with respect to regulatory regimes. The way we use governance in A4Cloud is as an organising framework providing understanding in the changing processes of governing accountability (in the cloud's case, from legal data protection to actual integration and operationalisation in practices via both technical and non-technical measures. *"The governance concept points to the creation of a structure or an order which cannot be externally imposed but is the result of the interaction of a multiplicity of governing and each other influencing actors"* (Kooiman and Van Vliet, 1993, p. 64). Governance and accountability are explored further in Section 7.

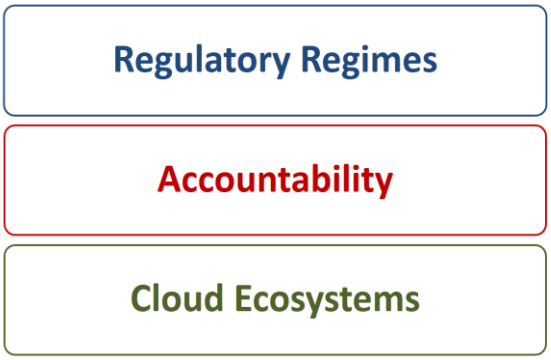


Figure 3 Context of Accountability Governance

The A4Cloud's accountability framework has a particular enabling role for cloud ecosystems. It enables cloud ecosystems to position themselves with respect to and to comply with regulatory regimes, as discussed further in Section 6. Figure 4 shows a representation of a typical cloud ecosystem involving different actors who contribute to data governance in the cloud.

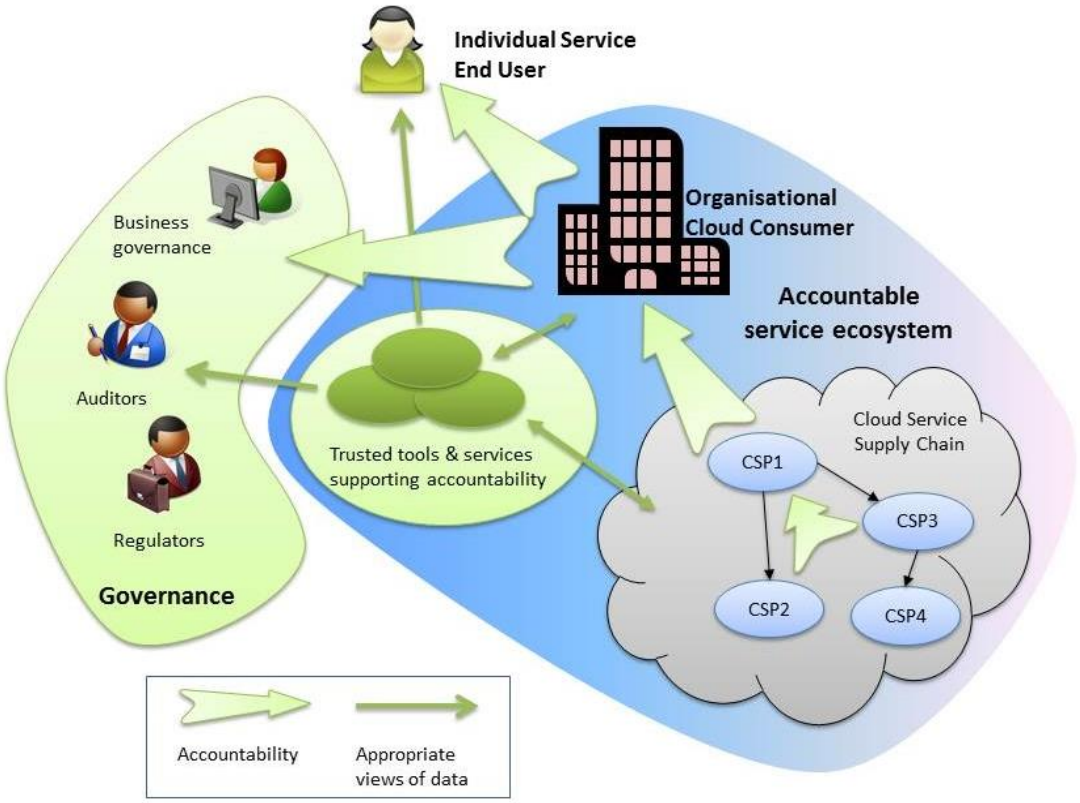


Figure 4 Sample Actors in a Cloud Ecosystem

Organisations that use or provide cloud services operate in a complex dynamic environment, they use cloud services in a service supply chain, and they need to feel confident that providers further down that chain are accountable for how they manage personal and confidential data. Governance includes regulatory agencies, those involved in providing business governance, and those who support those functions such as auditors. A chain of accountability should exist that extends all the way back to the cloud users, whether they are individual end users, or organisations who are using cloud services and also those involved in governance.

Accountability governance will help industry properly protect personal data and confidential information in new business environments and overcome the major barriers to the adoption of cloud computing. Real benefits and tools can be delivered to a number of stakeholders in order to increase consumer, business and government trust in cloud computing services. In particular, the following three main stakeholder groups would benefit from accountability:

- **Cloud Subjects and Cloud Customers:**
  - Control and transparency over how their data is used
  - Help in assessing trustworthiness of cloud providers and assurance of compliance to regulations
  - Support in obtaining redress even in complex and borderless processing
  - Reducing information asymmetry about cloud services
- **Cloud Providers:**
  - Technologies and processes to make services more trustworthy
  - Ways to satisfy business policies and demonstrate compliance
  - Reducing complexity of cross-border compliance obligations
  - Clear attribution of responsibility and liability (e.g. for incident management)
  - Analysis and remediation in case of breach or incident
  - Allowing differentiation and competitiveness based on accountability
- **Cloud Auditors and Supervisory Authorities:**
  - Assurance and evidence about compliance with policies and regulations
  - Forensics and transparency for (policy) enforceability
  - Cross-border enforceability
  - Scalability of operations through increased efficiency
  - More time and resource to focus on effective compliance objectives (such as addressing new technology challenges).

The A4Cloud project provides assistance in this direction, according to the project objectives as defined in Appendix A and discussed further in later sections of this document, especially Section 4. Section 3 will expand our analysis by discussing further emerging issues in cloud ecosystems. It will draw on current understandings of risks in cloud ecosystems with a particular emphasis on those risks (e.g. data protection issues) that might be mitigated or addressed by accountability. A number of issues will be considered, including the emerging importance of accountability in respect to cloud supply chains, the inherent complexity involved, issues and potential solutions to liability in such chains, the changing legal context and its effect, the degree to which having mechanisms in place to protect information should be taken into account, the degree to which individual privacy rights might be threatened in an accountability-based approach and constraints on business solutions.

1.3 Socio-Economic Landscape for the Cloud and Accountability

The socio-economic landscape for cloud computing and accountability is constituted from the following social and economic factors explaining cloud stakeholders' motivations for (non-)responsible behaviour:

- The ideal of cloud computing
- The drivers of cloud computing
- Current governance of cloud computing
- Incidents that make problems with cloud computing visible
- Society's interest in cloud computing
- Security in cloud computing.

These are now considered in turn.

1.3.1 The Ideal of Cloud Computing

Cloud computing is attributed to have a number of promising characteristics. This ideal of cloud computing is extensively described in white papers, most of these used for business-to-business marketing aiming to guide its readers to understand the benefits of cloud computing (and adopt the services offered by the companies represented by the authors). Stakeholders impacted by cloud computing (specifically cloud customers) relate the promises of cloud computing to administration, cost, partnerships and collaborations, and data ownership. These advantages are also reflected in communications to business customers. The dynamic flexibility and agility of cloud computing is promoted. Other promising characteristics are: lower costs, less complexity, increased collaboration, a greener approach to everyday business, and the boundary-less information flow throughout the world. Similarly, organisations like National Institute of Standards and Technology (NIST) promote or describe the promises of cloud computing (NIST, 2009). Although cloud computing has reached its peak in the Gartner hype-cycle for emerging technologies and is expected to reach stabilisation in 2 to 5 years (Gartner, 2013), it is this ideal of cloud computing that greatly has influenced and still influences stakeholders' behaviour and positive attitude to cloud computing. This positive attitude can be corrupted by a lack of trust in cloud ecosystems if cloud providers are unable to demonstrate the responsible handling of data in the cloud.

1.3.2 Driver(s) of the Cloud Computing (R)evolution?

Whether perceived as a revolution or an evolution, it is generally agreed that cloud computing will change society's organisation and business. Main drivers of the cloud are:

a) The underlying economics of the cloud provide an understanding of the long-term cloud computing landscape. The business delivery model that cloud computing offers (i.e. utility computing over conventional hosting) entails a big financial incentive.
b) Whereas in the past data was regarded of no value, current markets and society perceive data as valuable, turning data in a commercial and tradable asset. The cloud allows for storage and computing of more data than conventional computing devices.
c) Cloud computing embodies the digitalisation of society and enforces organisational changes (e.g. new ways of living our lives, performing work, doing business and administering public tasks and services) and societal changes (towards a 'better' society) (De Pous, 2012).

1.3.3 Current Governance of Cloud Computing

The (lack of) governance in the socio-economic landscape of cloud computing can be defined as the mechanisms that shape and steer the actions of relevant actors within cloud ecosystems. These mechanisms can be law and regulation, but might also be standardisation, certification or risk assessments of cloud services. With respect to cloud computing the new GDPR, greatly shapes stakeholders' behaviour in the cloud ecosystem. For example, any uncertainty with respect to who are the data controllers or data processors will affect trust. At a lower, or micro-level, the governance of the relation between cloud customers and cloud providers comes into play. Market mechanisms like competition and reputation come into play, as well as notions like good governance or responsible stewardship. Governance, in this sense, also entails, for example, standardisation for security and availability of cloud services.

1.3.4 Incidents

Incidents often are breakdowns of previous invisible infrastructures or ecosystems. Gaining insight in the practice of cloud computing and its potential problems with regard to accountability requires an approach that explores the entire cloud ecosystem. One of the most important features of ecosystems is that they only become visible upon breakdown. Exploring (previous) incidents with respect to privacy and data protection might provide insight valuable to the cloud ecosystem. For example, public reactions in the form of protests to governments bills such as the Protect IP Act (PIPA), the Stop Online Piracy Act (SOPA), and the Anti-Counterfeiting Trade Agreement (ACTA) in the USA provides insight into how the public perceives e.g. privacy, security and freedom of knowledge. Insights into these types of incidents are necessary to gain understanding of the (societal) need for accountability and the way accountability should be operationalised.

1.3.5 Society's Interest 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. Cloud computing is such an innovation in need of responsible governance. From a democratic accountability point of view it is the articulation of the public issue that should steer future development of technologies and related regulations (Beck, 1992; Beck, 2002; Jasanoff, 2009). Global innovations like cloud computing "…should respond to people's self-determined needs and aspirations, provided that certain background conditions of information and deliberation are met" (Jasanoff, 2009). Previous research with regard to privacy and online behaviour demonstrates that many consumers do not trust most Web providers enough to exchange personal information in online relationships with them (Leenes & Oomen, 2009), although the recent explosion in usage of social networks may render such conclusions no longer valid. Moreover, the public's perceptions of having little control over information privacy on the Internet have a strong influence on the consumer's willingness to engage in relationship exchanges online (Beldad, 2011; Hoffman, Novak and Peralta, 1998; Olivero and Lunt, 2004). Within this line of reasoning one can conclude that understanding the public's perceptions and concerns with regard to cloud computing provides a fair prediction of their willingness to adopt (accountable) cloud services and subsequently the need for tools and mechanisms that stimulate accountable behaviour.

1.3.6 Security

One recent important development is the PRISM-related revelations (EP, 2013), highlighting government mass surveillance programmes, especially in the US and UK, and including transfer of personal information via certain cloud providers. The Snowden revelations have changed the landscape "*by single handedly unveiling a major problem with the way we store and share files*". More specifically, Snowden "*has exposed one of the largest issues involved with trusting all of our valuable information to the cloud — security*"[50]. However, apart from the issue of enhanced government access to data via the cloud (which may be possible in any case even if the cloud were not used), the cloud does not necessarily offer less security than individuals can achieve on their own. In fact, the opposite can be argued since security is promoted as one of the cloud's advantages (see Subsection 1.3.1). Yet, cloud computing does create an easier and much more manageable target from a threat-economics perspective to attack for well-equipped adversaries like nation states: data from millions collected in a handful of data centres. Importantly, the perception of security in cloud computing from a business perspective (e.g. the lack of proper data and Virtual Machine segregation) has a different focus than laymen's perception of security (focusing on control of your information). These perceptions on risks with respect to security affect the need for accountability in the cloud ecosystem.

The elements outlined above thus argue that drivers for accountable behaviour also should be sought in the domains of economics and reorganising society. Motivations for accountability can be found within the economics of the cloud (financial gain) e.g. the costs and benefits of compliance to law or improvements in business opportunities and processes as a result of better quality data and controls, Also the public demand or wish for sustainable development or making our society a better place to live will drive and maintain the public perception of fair and responsible use of personal or sensitive business data (Leenes & Oomen, 2009). In line with this motivation one can argue that an overarching trend is visible towards good governance and accountability as a response to contemporary risk society (Beck 1979).

1.4 Summary

There are a number of reasons for taking an accountability-based approach, which may be summarised as follows:

1. *To improve the level of data stewardship.* Accountability can provide a motivation for organisations to improve their data stewardship; for example, by adopting privacy by design and security by design approaches. This is discussed further in Section 2.

[50] http://pandodaily.com/2013/09/11/the-snowden-effect-changing-the-course-of-cloud-security/ (accessed 2013-09-13)

2. *To provide trustworthy mechanisms for data protection in the cloud (for cloud customers, data subjects, data controllers and regulators).* Lack of consumer trust is already a key inhibitor to adoption of cloud services: people are suspicious about what happens to their data once it goes into the cloud; they are worried about who can access it, how it will be copied, shared and used, and they feel that they are losing control. In addition, companies who change from carrying out their computing in-house to using the public cloud are not so much concerned any more about the health of servers, but instead the confidentiality and security of their data. Surveys indicate that CIOs see security concerns as the top reason for not embracing the cloud, with lack of transparency cited as a key concern. Regulators are worried about the effects of cloud on jurisdictional controls and compliance; their lack of trust is resulting in stricter and more cumbersome regulations and increased penalties for non-compliance. All parties are also concerned about potential access by foreign governments if sensitive data is stored or accessed within and from those countries, or even in their own countries if controlled by a multinational company which may have to comply with foreign court orders or accede to foreign authorities' requests for data even if not legally required to do so. Increased trust can come from improved transparency and sound stewardship of information by service providers for which we need to hold them accountable. By providing trustworthy services to support accountability in the cloud, we aim to reduce the risk of disproportionate harm (in context) to subjects of personal data and to owners of confidential information, and thereby to also reduce negative consequences for data controllers and satisfy regulators.
3. *To decrease regulatory complexity.* Companies operating in multiple jurisdictions today face very different, even contradictory, regulatory approaches and this creates legal uncertainty and then unnecessary administrative burdens and risks. The current system provides an inconsistent and often divergent matrix of regulations, which adds unnecessary layers of complexity and technical and administrative burden for cloud providers and other stakeholders. The agility of the cloud is seriously undermined by the necessity in many cases to obtain regulatory approval for model contracts or undergo other complex procedures before any processing takes place. Further problems and delays emerge as cloud services can involve several contracts including contracts between the provider and user, the provider and sub-provider and between the user and sub-provider. The application of foreign regulation is often a risk even when the legal requirement for the level of data protection is low, or non-existent, in the country of the cloud provider. We aim to reduce these unnecessary layers of complexity and risks in our approach by fostering development of clear and consistent frameworks of data protection rules - rather than a complex matrix of national laws, which makes it really hard for businesses to ensure full compliance[51]. However, it may still be that the complexity in some cases could increase by the A4Cloud accountability measures, as such measures will be addressed in contracts, indemnification provisions, liability clauses, choice of law, etc. – we would like to avoid this but the effect is still to be determined. Accountability can also bring related benefits for regulators, in terms of them being able to lower their own administrative burden and rely on trustable service providers (so far as the applicable law permits) to implement adequate measures to ensure effective data protection and compliance.
4. *To provide more effective mechanisms for complex and dynamic business environments.* In a complex and dynamic context we need fluid and flexible tools instead of rigid prescriptive requirements.

The objective of this document is to provide a conceptual framework for the rest of the project. In order to achieve this aim, in this document we define accountability and the scope of its usage within the A4Cloud project. We also identify and define an accountability framework and approach for creating and sustaining chains of accountability throughout cloud service provision networks, in order to help specify and build trustworthy services to support accountability within the cloud. Existing definitions of accountability from the literature are surveyed, and a detailed analysis of related concepts is carried out. A model of accountability is presented, dividing the concept of accountability into constituent attributes, practices, mechanisms, and showing how these are related. This document also identifies problems and issues that cloud service provision poses for accountability, and a framework for governing data in the cloud is presented. A model of an accountable organisation is given, along with a process and maturity model and investigation of the relationship of these to certification for accountability.

[51] However, note that Bennett argues that accountability should not be an alternative to adequacy assessments in the cross-border context (Bennett, 2012).

2 The Concept of Accountability

Before we consider more specifically the cloud context, this section provides general context about accountability, especially with respect to the scope defined in the previous section. Furthermore, the relationship of accountability to privacy, security, design, risk assessment, self-verification and other relevant concepts, is assessed.

The structure of the section is as follows: first, an introduction to the concept is given, with an emphasis upon its usage within the domains falling most within the scope of the project. A definition is given of accountability, and analysis is provided about different interpretations of the concept and the implications that these have.

2.1 General Introduction to Accountability

It is likely that over time, legislation will put more emphasis on accountability: the move to cloud (and related changes) has been straining traditional legal frameworks. We discuss in this section how in many places across the world, our current laws are likely to be revised, with accountability a central feature of these new laws, and relate the usage of this term to a broader usage in other contexts.

Accountability is a notion of which there is no universally agreed definition, although it is generally agreed that responsibility, transparency and holding to account are key elements. It is a complex notion that is used in a slightly different sense in different domains. For example, in IT governance, accountability is used in the sense that the information security management system of an organisation is meant to generate assurance, transparency and responsibility in support of control and trust. There are also other types of usage coming from corporate governance, social science and computer science. For example, the privacy-oriented definition of accountability given in ISO standard 29100 (ISO/IEC 29100) expresses accountability in terms of the practices associated with it in organisations: *"Accountability: document policies, procedures and practices, assign the duty to implement privacy policies to specified individuals in the organisation, provide suitable training, inform about privacy breaches, give access to effective sanctions and procedures for compensations in case of privacy breaches."*

This subsection provides a high level overview of the notion of accountability, with a focus on the data protection domain, reflecting the A4Cloud project scope. However, the scope of accountability can cover a range of diverse aspects, including politically sensitive areas such as intrusive Government surveillance and the responsibilities of organisations to contribute fairly to their local societies via appropriate payment of taxes. Some of these, like Sarbanes-Oxley requirements, do not have a strong connection to privacy. In our analysis we focus most specifically on the areas related to the project scope. Related to this point, the issue of accountability in relation to intrusive governmental surveillance for national security purposes is more general than cloud computing, although two secret mass surveillance programmes recently revealed (i.e. PRISM and Tempora) have a connection to cloud computing in that information collected by certain US-based cloud companies about EU citizens was made available to the US and UK security services (Guardian, 2013).

Accountability controls that centre on enforcement of private contracts and domestic data protection legislation would not provide effective protection against such activities; instead, the relevant sphere of governance is such cases seems to be in application of the principle of legality, proportionality and judicial and parliamentary accountability, potentially combined with technical measures to help make scrutiny of social media accountable (Omand et al., 2012). Appendix B contains further analysis of the notion of accountability in different domains.

2.1.1 Accountability in the Data Protection Domain

In data protection regulation since the 1980s, accountability has been used in the sense that the data controller is responsible for complying with particular data protection legislation and, in most cases, is required to establish systems and processes which aim at ensuring such compliance. The Organisation for Economic Cooperation and Development (OECD) privacy guidelines stated that *"[a] data controller should be accountable for complying with measures which give effect to the [other privacy] principles"*

(OECD, 1980). Indeed, the notion of accountability appears in several international privacy frameworks in addition to the OECD Privacy Guidelines (OECD, 1980), including Canada's PIPEDA (Personal Information Protection and Electronic Documents Act) (PIPEDA, 2000), Asia Pacific Economic Cooperation (APEC)'s Privacy Framework (2005), Article 29 Working Party papers (European DG of Justice, 2010) and some elements of the draft European Data Protection Regulation (although in that case not directly associated with the word 'accountability' largely for reasons of translatability) (EC, 2012). For example, the APEC privacy principles hold controllers accountable for compliance with all the principles and obligate them to use reasonable steps to ensure that the recipients of personal data also comply: thus, there is an insight that accountability should follow the data (Crompton, 2006). Notably, the EU's Article 29 Working Party subsequently submitted a detailed recommendation on accountability to the EC in July 2010 (European DG of Justice, 2010), which recommended inclusion of a new principle of accountability in the revised EU Data Protection Directive (GDPR). It stated (p2):

> *"this Opinion puts forward a concrete proposal on accountability which would require data controllers to put in place appropriate and effective measures to ensure that principles and obligations set out in the Directive are complied with, and to demonstrate so to supervisory authorities upon request"*

and provided suggested wording to include in the forthcoming revision of the Directive (GDPR), namely:

> *"1. The controller shall implement appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with.*
> *2 The controller shall demonstrate compliance with paragraph 1 to the supervisory authority on its request."*

In addition, the European Data Protection Supervisor (EDPS), as well as the data protection and privacy regulators at the 31st International Conference of Data Protection and Privacy Commissioners (ICDPP, 2009) have all within the last five years paid special attention to the principle of accountability.

The EDPS glossary (EDPS, 2012) defines accountability as a: "*Principle intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities*."

The Global Accountability Project started by privacy regulators and privacy professionals has also been for the last few years defining and refining the concept of accountability in the context of these latest regulations (CIPL). Guidance has also been produced from Canada about the expected form of comprehensive accountability programs that organisations should put in place (Office of the Information and Privacy Commissioner of Alberta et al., 2012).

The usage of the notion of accountability by regulators is evolving towards an 'end-to-end' personal data stewardship regime in which the enterprise that collects the data from the data subject is accountable for how the data is shared and used from the time it is collected until when the data is destroyed. This extends to onward transfer to and from third parties.

Region block governance models are now evolving to incorporate accountability and responsible information use, with regulators increasingly requiring that companies prove they are accountable. Frameworks such as the EU's Binding Corporate Rules (BCRs) (ICO, 2012) and APEC's Cross Border Privacy Rules (CBPRs) (APEC Data Privacy Subgroup, 2011) are being developed by legislative authorities to try to provide a cohesive and more practical approach to data protection across disparate regulatory systems, and can be viewed as operationalising accountability. For example, BCRs require organisations to demonstrate that they are, and will be, compliant with EU Data Protection Authorities' (DPAs) requirements for transferring data outside the EU.

Although it is a complex notion, it could be argued that its core, accountability is a very simple idea. It says that not only should an organisation do everything necessary to exercise good stewardship of the data under its control, it should also be able to demonstrate that it is doing so. Good stewardship is

achieved by designing systems appropriately, so that they reflect privacy principles and security expectations from partners, regulators and data subjects, as well as by the organisation living up to its promises and ensuring responsible behaviour. The demonstration – via provision of an account – is an essential aspect, but can be challenging to provide. Furthermore, if events do not work out as planned, organisations need to provide a means of remediation as well as needing to try to prevent such an occurrence happening again. These aspects are considered further below.

2.1.2 Accountability Measures

Organisations must both be responsible (in terms of policies, mechanisms and internal oversight) and answerable (in the sense of standing ready to demonstrate). These elements are captured within the Global Accountability Project's Essential Elements of Accountability (CIPL, 2009), namely:

1. Policies that link to the external criteria and are supported by senior management
2. Mechanisms, including risk assessment tools, to put policies in place
3. Internal review to assure mechanisms are working and are improved over time
4. Means to make uses transparent to individuals and assure their rights are respected
5. Openness to enforcement agency oversight and remedies if the goals of data protection are abused.

The Article 29 WP (in its principle on Accountability: Opinion 3/2010) provides an illustrative list of possible 'common accountability measures', namely (European DG of Justice, 2010):

- Establishment of internal procedures prior to creation of new personal data processing operations
- Setting up written and binding data protection policies, which should be made available to data subjects
- Proper identification of data processing operations & maintenance of an inventory of these
- Appointment of a DP officer and other individuals with responsibility for data protection
- Data protection, training and education
- Procedures to manage access, correction and deletion requests, which should be transparent to data subjects
- Internal complaints handling mechanism
- Internal procedures for effective management and reporting of security breaches
- PIAs in specific circumstances
- Implementation and supervision of verification procedures to ensure that all the measures not only exist on paper but that they are implemented and work in practice (internal or external audits, etc.).

The proposed General Data Protection Regulation (GDPR) lists a Data Controller's accountability instruments (in art. 22) as being (EC, 2012):

- Policies
- Documenting processing operations
- Implementing security requirements
- Data Protection Impact Assessment
- Prior authorisation/consultation by DPA
- Data Protection Officer
- If proportional, independent internal or external audits

The measures have to be appropriate and effective in a verifiable way. The following subsection provides further analysis of accountability from societal, legal, ethical and economic perspectives.

2.1.3 Accountability in a Broader Perspective

Like transparency and trust, accountability is an umbrella term covering many different social relations subject to their own procedures and rules: accountability is "a very elusive concept [...] that can mean many different things to different people" (Bovens, 2007). In this section accountability is placed in a broader perspective (societal, legal, ethical and economic) in terms of reasons for holding organisations and actors accountable for their actions, in order to supplement and broaden the discussion given above. Further discussion about different notions of accountability is given in Appendix B.

2.1.3.1 Legal Perspective

Accountability clearly has a strong legal connotation, especially because the A4Cloud project primarily focuses on personal data and hence is framed by the data protection legal framework. The law imposes rights and obligations on individuals and corporations. Rights can (ultimately) be effectuated through legal means such as court orders and obligations can be backed or enforced by means of legal instruments such as sanctions. In a sense, the law thus forces accountability upon cloud providers and users even if they feel no moral, social or economic obligation to be accountable. All attributes in the accountability model have a legal aspect or component.

2.1.3.2 Economic Perspective

A different perspective on accountability derives from an economic viewpoint. Agents can be considered economic agents (for individuals this is known as *homo economicus*). They will individually consider costs and benefits in planning their actions. Transparency and observability contribute to individuals' capabilities to assess risks and benefits and choose the right options. Accountability leads to information regarding cloud practices and this information will have a governing effect on the market. Accountability may lead to trust creation that can be an incentive to create and maintain a competitive advantage valued equally by data subjects, business clients and regulators. Furthermore, ethical and privacy-respecting business practices can enhance the value of a company (e.g. in the stock market).

Connecting the economic perspective to the societal perspective, accountability can be seen as a tool to encourage "co-operation" in the form of good data stewardship and discourage "defection" in the form of poor security practices and abuse of personal data or confidential information. From this perspective, key aspects of accountability can be seen as incentives to co-operation and disincentives to defection. For example:

- **Liability** is a disincentive to service providers to abuse data.
- **Transparency** is an incentive to good data stewardship because it makes bad behaviour more observable.
- **Remediation** is a disincentive to data abuse. From an economic perspective, it acts as a commitment mechanism because in promising remediation in the case of bad behaviour, the service provider is discouraged from abusing data.
- **Verifiability** and **Assurance** are a disincentive to data abuse - because the service provider cannot deny bad behaviour and its detection may be facilitated.

2.1.3.3 Moral Perspective

People and organisations should not only behave according to certain rules because they have a legal obligation to do so, they also have a moral obligation: *"[i]deal-typically, the fully moral action will involve an agent doing the right thing (as a matter of act morality), for the right reasons (as a matter of agent morality)*" (Brownsword, 2008). In other words, people and organisations should act according to the rules because they morally subscribe to the rules (e.g. corporate social responsibilities relate to sustainable and green IT). Cloud providers therefore have a moral responsibility towards those impacted by cloud computing since they have a good deal of latitude (power, influence, discretion) in what they create. In order to be responsible, cloud providers should recognise the values that affect their work and the ways their work influences values. Accountability could encourage organisations to act as moral agents in regard to respecting and protecting the personal data and confidential information of customers, employees and partners, and encourage corporate responsibility.

More specifically, we believe that A4Cloud will help organisations move away from a checkbox mentality for compliance and adopt techniques that not only meet data protection compliance needs but also satisfy the expectations of stakeholders and society and wider ethical principles (such as privacy and transparency) – for example this could be by highlighting whether a decision will be consistent with customers' or employees' expectations. The A4cloud project thus makes use of ethics not to demonstrate how much responsibility cloud providers have, but what type of responsibilities are appropriate for their work practices.

2.1.3.4 Societal Perspective

Accountability comes in many forms and shapes, yet a shared understanding is that the notion of accountability entails a power relationship. The process of being held to account 'determines, reflects, reifies, strengthens and soldifies power relationships between the accountee and the accountor'. One actor explains, justifies and defends his behavioural conduct against a significant other. These accountability relationships often have a structural and not an incidental character; they are somehow institutionalised or organised and not based on single incidents or complaints. As these power relationships are structural, the nature of the relationship between the accountee and accountor likely shapes what type of accountability arrangement is used. These arrangements can be: a) a vertical accounting arrangement: a hierarchical relationship or principal-agent relationship in which the accountor has a formal power over the accountee, b) a diagonal accounting arrangement: the accountor has no direct formal power over the accountee, yet informal power as the accountor reports to the actor with formal power as supervisory agencies do, and c) a horizontal accounting arrangement; although there's no formal hierarchical relationship between acountee and acountor, the accountee does provide information to some forum based upon a formalised obligation, rather like a supervisory board of an organisation (Schillemans & Bovens, 2009).

Accountability in the following sections is presented as a concept governing the relation between cloud provider and cloud user. The user has an interest in the cloud provider accepting responsibility for the stewardship of personal and confidential data because it concerns their data. Also society as a whole has an interest in accountability for cloud providers. Cloud computing is a technology that potentially has a significant impact on society socially. Socially, because the way in which we structure work and leisure may change as a result of cloud services and cloud arrangements. Society thus has an interest in the responsible development of the technology. This is also acknowledged by the OECD:

> *"Transparency and accountability towards the range of stakeholders in business – including employees, customers, suppliers, shareholders, local communities, society at large and the environment – are both a standard that is expected, and a mechanism for securing compliance with codes of conduct designed to meet society's expectations." (p2: Lake, 1999)*

Accountability and the associated mechanisms and tools allow inspection of what happens in the cloud, not only for individuals, but indirectly also for society at large. Society, for example through policy makers and legislature, will respond to signals derived from the accountability mechanisms and tools. Assurance, transparency, observability, responsiveness, attributability and verification are particularly relevant in this respect. Whether these attributes have the same meaning and operationalisation in view of the relation between provider and user and the relation between individual providers, sectors of industry or even the cloud in general is a topic for further study. Next we consider one particular aspect, namely democratic accountability.

2.1.4 Democratic Accountability

In the cloud computing industry, the relationship between cloud provider and cloud customer is mainly determined by the market mechanism of consumer choice, the capacity of the consumer to exit to an alternative provider and not by 'voice'. However, accountability usually is understood as a voice strategy. In the accountability relationship between cloud providers and cloud users the arrangement should have a vertical or diagonal accounting arrangement in place that would allow for such a voice strategy. Nowadays increased calls for such an accountability relationship can be understood as a reaction to the insufficient functioning of the market relationship between cloud provider and cloud user. Though formally an exit strategy in the cloud computing ecosystems exists, in practice it appears to be more difficult as consumers either lack knowledge to understand the differences between cloud providers or due to vendor lock-in are not able to move as freely as they should or because current cloud industry lacks incentives for negotiating contracts.

The relationship between cloud providers and society at large is rarely mentioned, yet might be of great importance for the sustainable development of the cloud computing industry. The perceived lack of trust in the cloud urges more direct, external and explicit accountability relationships, not only taking into account one's customers as accountors but also the general public. Incidents in the past with private

global industries like Shell demonstrate how private organisations increasingly face public scrutiny when things go wrong. Moreover, the global character and central role of cloud computing in modern economies demand increased accountability to the general public.

Democratic accountability defines a power relationship that brings back power to the demos. In a strict sense, when used in public governance, democratic accountability is political accountability of a democratic sort (Goodin, 2003). Democratic accountability then refers to "*the accountability of elected officials to their electorates for their performance in office*" (p. 361: Goodin, 2003). However, democratic accountability also entails giving account to a virtual entity; the general public, or society at large. Society at large not only has a right to information about the extent to which a private organisation had complied with the (minimum) standards of law and other regulation of a quasi-legal nature. Society at large also can demand information about public domain matters of a more social and ethical nature. These public domain matters of substance can be elicitated via public opinion. Organisations then owe accountability to the public at large for these specified public domain matters of substance. Therefore, in the case of cloud computing, society at large might want to be informed about the social and ethical impact of the cloud on society, due to its global nature and stimulus for reorganising society.

In order to bring back the power to the demos via democratic accountability, the accounting arrangements are characterised by two essential elements: transparency and responsiveness. The right to receive information is an essential element of participatory democracy. With the right to information, development of democratic accountability also increases the need for transparency of organisations. Specifically with respect to information about actions which influence society, other societies, and/or future societies. The general public then is the level at which information is reported, and the level at which transparency must be sought. Responsiveness refers to the aim of making private organisations accord with the preferences of their customers and the general public, and can be equated with the principles of deliberative democracy. Private organisations providing services to members of the public are called on to be responsive to not only consumer demands but also public needs. In other words organisational accountability is extended to public dialogue, a dialectical activity involving open discussion about matters of public interest

In conclusion, extending the accountability relationship between cloud providers and cloud customers to the provider's responsibility to society at large provides a broader perspective on the need for accountability in the cloud. A restriction to financial account, or legal accounts in the cloud provider-cloud user relationship would critically limit the attempts at holism in the cloud ecosystems. A democratic account would potentially lead to a more effective response to citizens' needs, interests and aspirations and subsequently a sustainable development. Nevertheless, extending democratic accountability to the private sector also involves certain dangers or worries. First, democratic accountability can also be used by private organisations as a legitimisation purpose. Involving a citizen panel to understand their needs without actually addressing these needs does not entail true responsiveness and hence accountability. Second, private organisations face a methodological problem: *How to facilitate equal representation of all affected interests?* Third, demanding democratic accountability raises another question: *Over what information about private organisations does the general public have rights?*

2.1.5 Accountable Organisations

The concept of accountability is reflected clearly upon the accountable behaviour of organisations. Accountable behaviour captures accountability from the various perspectives, while it ties the concept to its implementation through the adoption of concrete accountability measures. Accountability at an organisational level brings about the value of democratic accountability as it is based upon the distribution of responsibilities, the diffusion of power and the relationships with external stakeholders.

Accountable organisations are those organisations who commit not only to legal but, also, to moral obligations dictating responsible behaviour. As far as the project's scope is concerned, responsible behaviour implies responsible stewardship of personal and confidential data processed in a cloud ecosystem from the time of collection until the time of deletion, including the onward transfers to and from third parties. Accountable organisations, firstly, are driven from moral incentives and, secondly, take concrete steps to implement accountability in practice.

For organisations to behave as moral agents entails to reflect upon the question what good behaviour means to them as an organisation. Organisations therefore should not only focus on accountability as mechanisms of control, but also on accountability as doing the right thing, with the right outcomes, for the right reasons. Accountability is both a moral phenomenon that can and should be subject to moral reflection and a mechanism to control or govern responsible behaviour. Though no general standards for accountable behaviour exist, organisations' accountability might still imply the presence of one or more (in)formal norms against which the actual and active behaviour of the organisation in question will be assessed. In practice, organisations often develop Codes of Ethics or Codes of Conduct[52] to promote and guide ethical behaviour (De Colle and Gonella, 2002). Similarly, accountable stewardship of personal –and business sensitive information– in a cloud environment calls organisations to take initiatives to define cloud practices promoting the principles of reducing the vulnerability of individuals and society, and of promoting a social sustainable development (Paraphrasing Berleur et al. Ethics of Computing: Codes, Spaces for Discussion and Law, p.11). The key benefit for organisations to behave in such a way are the improvement of business performance and reduction of risk. It might also have limitations, though, if these values are not developed in a participative way (i.e. they are imposed top down) or without consulting external stakeholders (and hence there is a need for explicit linkages to societal expectations). Notably, breaches of the Codes of Ethics or Conduct can be sanctioned, either formally (e.g. by removal from association) or informally (via reputation).

The implementation of accountability through concrete measures is facilitated, of course, provided that organisations have adequate resources. Financial capacity allows for greater flexibility in terms of technical and organisational measures to be employed. Although at first glance large organisations are privileged in this respect, this does not necessarily mean that they should be considered be "more" accountable, simply, due to their more extensive resources. On the contrary, as will further discussed in later sections, Small and Medium Enterprises (SMEs) are in the position to be "equally" or "more" accountable because there are fewer employees that have to subscribe to ethical behaviour and hence getting everyone on the same page is potentially easier.

2.2 The Nature of Accountability

In this subsection the nature of accountability is explored further, by means of providing a conceptual definition of accountability, and considering how accountability relates to privacy, security, trust, transparency, control and satisfaction of norms.

Accountability, in general, is used prescriptively; accountability of some agent to some other agent for some state of affairs. It reflects an institutional relation arrangement in which an actor can be held to account by a forum (for example, a consumer organisation, business association or even the public at large). Accountability then focuses on the specific social relation or the mechanism that involves an obligation to explain and justify conduct. Subsequently, accountability is "*a relationship between an actor and a forum, in which the actor has an obligation to explain and to justify his or her conduct, the forum can pose questions and pass judgement, and the actor can be sanctioned*" (Bovens, 2007).

In an accountability relationship thus two parties and an object can be distinguished: a) the steward or ***accountor***, b) ***accountee*** or forum, and c) the codes or ***norms*** on the basis of which the relationship is struck. The latter are the shared framework for explanation and justification that are negotiated between the accountor (to answer, explain and justify) and accountee (to question, assess, and criticise). An accountability code then is a system of signals, meanings and customs, which binds the parties in a stewardship relation. In order to do so, there are different stages in accountability relations:

a) information in which explanation is given and one's conduct is justified

b) debate, in which the adequacy of the information and / or the legitimacy of conduct is debated (answerability)

c) the forum must pass judgement and sanction whether formally (for example, via fines, disciplinary measures and unwritten rules leading to resignation) or informally (for example,

[52] See for example the work performed by the C-SIG groups of the European Cloud Strategy (in particular the C-SIG CoC).

having to render account in front of television cameras or via disintegration of public image and career).

Accountability as a mechanism thus can be used as a tool to induce reflection and learning. It provides external feedback on (un)intended effects of an organisation's actions. However, accountability is also used in a more normative way. Bovens calls this '*accountability as a virtue*'. Accountability as a virtue is largely defined by bad governance: what is irresponsive, opaque, irresponsible, ineffective or even deviant behaviour. Accountability as a virtue, a normative concept, entails the promise of fair and equitable governance. Behaving in an accountable or responsible manner then is perceived as a desirable quality and laid down in norms for the behaviour and conduct of actors. Moreover, accountability then is not something imposed upon someone or an organisation by another actor, but an inherent feeling, the feeling of being morally obliged to be responsive, open, transparent and responsible.

Hence, accountability as a virtue is a normative concept whereby a set of standards is provided for the evaluation of behaviour of public actors, and being accountable is seen as a positive quality in organisations or officials (Bovens, 2010), while accountability as a mechanism is used in a narrower, descriptive sense, to describe an institutional relation or arrangement in which an actor can be held to account by a forum.

A4Cloud's cloud accountability combines the notions introduced earlier of accountability as a mechanism and accountability as a virtue within the private sector of cloud computing and its cloud ecosystem. Our approach is to build on these notions to incorporate accountability in the cloud ecosystem by allowing for a mechanism that ensures the possibility of giving account *ex post facto* (via accountability tools) and steering accountability behaviour *ex ante* (via accountability as a virtue). Accountability as a virtue is extended to apply to cloud actors including cloud service providers, and accountability as a mechanism entails the social relation between the accountor and accountee that involves an obligation to explain and justify conduct.

2.2.1 Project Definition of Accountability

Building on such analysis (including that shown in Appendix B), a definition of accountability that is applicable across different domains and that captures a shared multidisciplinary understanding is:

Definition of Accountability: *Accountability consists of defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly.*

Internal criteria are not necessarily visible to stakeholders external to that organisation, as they might for example reflect the risk appetite of that organisation or known security vulnerabilities; external criteria could include best practice on security, data protection and breach notification, as well as privacy regulatory and contractual requirements and societal expectations. However, given the scope of the project, we need to refine this definition to reflect our project focus.

Our project looks at accountability in the context of a *cloud ecosystem,* which is a business ecosystem of interacting organisations and individuals − the actors of the cloud ecosystem – who provide and consume cloud services. In other words, the main stakeholders in the cloud ecosystem are cloud providers and cloud users. In this ecosystem the stakeholders interact in a constant process of change. Moreover the stakeholders within the ecosystem are controlled not only by the internal factors of the system, such as codes of conduct and existing relations, but also by external factors such as regulations, the wider environment or even required skills.

Within cloud ecosystems accountability is becoming an important (new) notion, defining the relations between various stakeholders and their behaviours towards data in the cloud, and we consider this in more detail in Section 4. For the project scope, the accountors are cloud actors that are organisations (or individuals with certain responsibilities within those) acting as a data steward (for other people's personal and/or confidential data). The accountees are other cloud actors, that may include private accountability agents, consumer organisations, the public at large and entities involved in governance.

A definition of accountability within cloud ecosystems that we have produced, again through consideration of relevant interdisciplinary literature, is the following:

> **Definition of Accountability (for cloud ecosystems):** *Accountability for an organisation consists of accepting responsibility for data with which it is entrusted in a cloud environment, for its use of the data from the time it is collected until when the data is destroyed (including onward transfer to and from third parties). It involves the commitment to norms, explaining and demonstrating compliance to stakeholders and remedying any failure to act properly.*

This definition differs slightly from the more generic one given above, for the following reasons. Security and privacy management is evolving into an information stewardship problem; in the cloud, it will be harder to establish the risks and obligations, implement appropriate operational responses and deal with regulatory requirements. Notions of transparency and assurance receive more emphasis and it is necessary to ensure 'chains of accountability'. Accountability places a responsibility upon an organisation that uses personal information to ensure that the contracted partners to whom it supplies the personal information are compliant, wherever in the world they may be. So, the communities responsible for data stewardship place responsibilities/constraints on other individuals or on the way systems operate, and these constraints are met along the chain of provision. Furthermore, the scope of the project focuses attention on personal and/or confidential data. We now consider the scope of accountability further, in the sense of who should be accountable for what to whom.

2.2.2 Scope of Accountability

Given the scope of the project as given in Section 1, we focus on the data protection domain and on accountability of organisations rather than individuals. More specifically, we focus on accountability under data protection laws for personal data processed in cloud service provision ecosystems. In general, we will consider accountability obligations owed by cloud service providers, and organisations that use cloud services, to regulators, stakeholders and society. Regulators can be oversight authorities or legislators. In the data protection field, we consider accountability obligations owed by cloud service providers and organisations that use cloud services to data subjects and Data Protection Authorities (DPAs). The DPAs are the primary targets as it could be regarded that society is served through the DPAs, and legislature is targeted in a broader, societal perspective. Accountability of individuals in a private context is excluded, although accountability of service providers for the actions (or inactions) of their employees is in scope. We will also consider how our proposed accountability mechanisms might apply to certain types of confidential information that do not involve personal data.

Who is accountable in the cloud?

Related to the discussion about how accountability entails a power relationship in SubSection 2.1.2, the European Parliament's Cloud Study (EP, 2012) claims that "*An accountability approach would imply the vesting of obligations and liabilities upon every actor with considerable power, i.e. knowledge and control of the personal data*." This would seem to imply that all actors other than cloud-end users are accountable, as they possess power. The cloud customer as the data controller bears relevant accountability if they are in control, but there is little or no scope for controlling the processing environment, only to make choices about which one to use. Giving instructions to providers about processing and security is not feasible in most cases. The cloud provider is nearly always the processor but often needs to assume co-controllership responsibilities. However, the cloud providers, especially IaaS providers, may not know who the users are or the purposes for which their services are being used.

To whom are they accountable?

As considered above according to the project scope, organisational cloud customers and cloud providers are accountable towards: data subjects (who need to be in control of their data) as well as the relevant DPA, who supervises them and is the guardian of legal compliance. Furthermore, society at large should be taken into account if possible (for example, as part of the moral obligation). Related to this point, in Figure 6 below a referral is made to societal norms, and we argue that accountability should underpin the principles and standards set by society rather than undermining them, and that such principles should be subject to change via a democratic process. We propose that the data subject

should be the rationale and the real beneficiary of the accountability chain (for personal data), and similarly, the data owner should be the rationale and the real beneficiary of the accountability chain (for confidential business data).

What are they accountable for?

According to the forthcoming GDPR (EC, 2012: article 22), the data controller will be accountable for data protection by design and by default and data breach notifications. The data processor on the other hand is accountable (EC, 2012: article 26) for co-operation with the data controller to meet data subjects' rights, assist the controller in providing security measures and should act only on the controller's behalf. According to article 24, the joint controllers need to agree their respective responsibilities and make this transparent to data subjects, such that "... the arrangement shall duly reflect the joint controllers' respective roles and relationships vis-à-vis data subjects..." (EP version of GDPR adopted 12th March 2014). More generally, we can think of the accountability here being for obligations in relation to the treatment of personal data (which can take the form of legal compliance, promises, conformance with notice, contractual agreements, adherence to codes of conduct, etc.).

The principle of accountability within the OECD guidelines (OECD, 1980), states that '*A data controller should be accountable for complying with measures which give effect to the principles stated above*.' It also says that '*It is essential under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau*.' (OECD, 1980).

Mechanisms can be provided both for *internal accountability* (within an organisation this often involves monitoring, for example ensuring control over the chain of responsibilities, continuous monitoring of key indicators/processes and reporting) and *external accountability* (providing assurance and commitment to data subjects, regulators and auditors about the organisation's compliance with its own policies, common expectations, accepted business practices and appropriate regulations). Correspondingly, new laws and regulations (The White House, 2012; EC, 2012) include explicit requirements that an organisation not only comply, but that they have programs that put the principles into effect.

Based upon the definition of cloud accountability given above, we identify the objects that a cloud actor is accountable for within a cloud ecosystem to be:

- **Norms:** the obligations and permissions that define data practices; these can be expressed in policies and they derive from law, contracts and ethics.
- **Behaviour:** the actual data processing behaviour of an organisation.
- **Compliance**: entails the comparison of an organisation's actual behaviour with the norms.

By the accountor exposing the norms it subscribes to and the things it actually does, an external agent can check compliance. We revisit and extend this analysis in Section 5, when we provide a model of accountability.

Responsibility of Individuals versus Liability of Organisations

Even though organisations should appoint a Privacy Officer to be responsible for the organisation's privacy management programme, at least in Canada the organisation remains liable for compliance with applicable data protection legislation and its liability is not passed on to that individual (Office of the Information and Privacy Commissioner of Alberta et al., 2012). It seems that individuals can be responsible for certain actions and areas of responsibility, but it is organisations (and especially data controllers) that are liable or held to account. Key roles and responsibilities of executive officers in cloud scenarios are given in the appendix of (Horwath, 2012).

Within organisations, there are chains of responsibility, contextual to the role and actions of individuals with regard to appropriate treatment and protection of sensitive, personal and confidential data. In these chains, the responsibility is shared rather than being passed down entirely. For example, a primary service provider may be responsible for ensuring appropriate data protection compliance mechanisms are in place to appropriate regulators and company auditors, and this responsibility ultimately falls to

the CEO, who looks to the Chief Privacy Officer of the company to take responsibility for this area. Further down the chain, managers and employees are responsible for their own decisions affecting treatment of other people's personal data to corporate governance. Note the important distinction between sharing responsibility for actions and delegating responsibility for particular actions.

There should be avoidance of responsibilities and liabilities being completely transferred forward through the chain, as senior management buy-in is an important aspect of accountability (CIPL, 2009). Other aspects to consider include what an acceptable risk is and what due diligence would be for an accountable organisation. However, industry standards will generally dictate the standard of care that an organisation must take to avoid liability and in addition, if an officer, director, or employee is acting on behalf of an organisation, then the organisation remains responsible and liable.

2.2.3 The Relationship between Accountability, Privacy, Security and Trust

A major driver for an accountability-based approach is to provide an incentive for organisations to 'do the right thing', in terms of decreasing regulatory complexity, easing transborder data flow restrictions while avoiding increased privacy harm, encouraging best practice and using strong punishment as a deterrent. For example, in response to the seemingly insufficient reflection of EU data protection principles and obligations in concrete measures and practices used by organisations, the Article 29 Working Party advocated in its Opinion on the principle of accountability (European DG of Justice, 2010) that such a general principle could help move data protection 'from theory to practice', as well as provide a means for assisting data protection authorities in their supervision and assessment tasks: "*EU data protection principles and obligations are often insufficiently reflected in concrete internal measures and practices. Unless data protection becomes part of the shared values and practices of an organisation, and responsibilities for it are expressly assigned, effective compliance will be at considerable risk, and data mishaps are likely to continue.*"

There is an associated requirement for DCs to be able to demonstrate compliance to supervisory authorities upon request. Hence, organisations are allowed increased control over aspects of compliance (i.e. which tools and mechanisms to use in order to achieve compliance), but at the expense of having to demonstrate on an ongoing basis that these mechanisms are appropriate for their business context, and operationally work as expected (Figure 5).

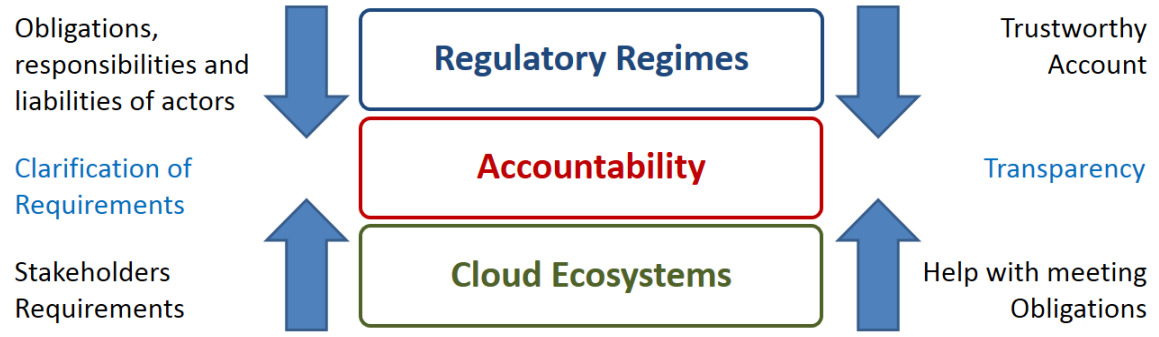


Figure 5 Accountability Context

As shown in Figure 5, the legal and contractual context defines obligations, responsibilities and liabilities of actors in a given cloud ecosystem. Accountability aims to entrust organisations with the practical aspects of complying with data protection obligations. Part of this involves clarification of requirements of the different actors within cloud ecosystems, as well as transparency and provisions of trustworthy accounts by organisations that collect or handle personal information. As discussed further in Section 6, the actors may select mechanisms and tools to support accountability practices, and thereby help them to comply with relevant regulatory regimes within specific application domains.

Figure 6 shows how accountability should complement the usage of appropriate privacy and security controls in order to support democratically determined principles that reflect societal norms, regulations and stakeholder expectations. Governance and oversight of this process is achieved via a combination

of Data Protection Authorities, auditors and Data Protection Officers within organisations, potentially supplemented by private accountability agents acting on their behalf. It is important to state that accountability should not be seen as an alternative to privacy. Instead, as shown in Figure 6, accountability and privacy by design are complementary, in that the latter provides mechanisms and controls that allow implementation of principles and standards, whereas accountability makes organisations responsible for providing an appropriate implementation for their business context, and addresses what happens in case of failure (i.e. if the account is not provided, is not adequate, if the organisation's obligations are not met e.g. there is a data breach, etc.). Privacy by Design may to some extent incorporate corporate accountability mechanisms (Cavoukian, Taylor and Abrams, 2010; Pearson, 2013), in that a privacy management program can be seen as bridging between accountability and privacy by design. At the top of Figure 6, standards are external criteria against which the organisation needs to measure themselves and demonstrate compliance, where relevant to the business context. Some of these are technical best practice standards, as considered further within the following section. Others are social principles that are reflected in legislation, such as the OECD privacy principles discussed also in Section 3. Accountability should underpin the principles and standards set by society rather than undermining them; such principles should be subject to change via a democratic process. Additional constraints may come from other legal and stakeholder requirements. Together, these set societal, regulatory and contractual obligations that organisations need to meet, and for which they are accountable to certain other parties, such as business partners and regulators.

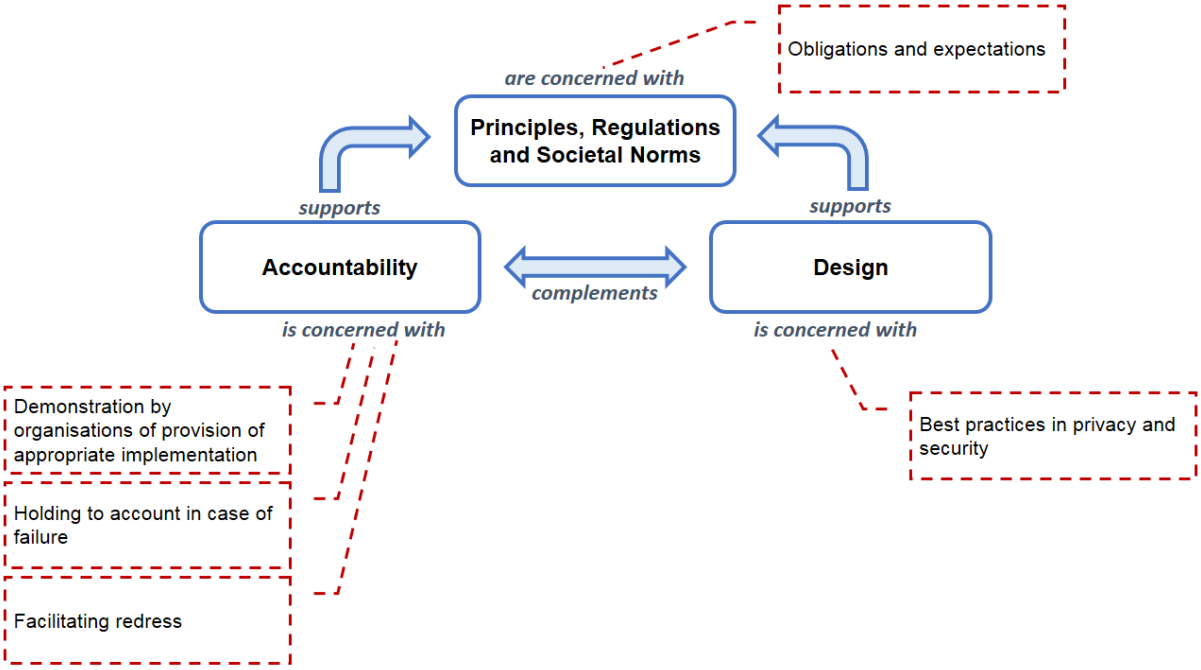


Figure 6 Accountability Framing

These principles may be reflected in privacy by design, via privacy aware technologies (PATs) and privacy enhancing technologies (PETs) (Pearson, 2013). PATs are standard non-privacy related solutions that include features that enable users to protect their privacy. PETs are solutions whose specific purpose is to help consumers and companies protect their privacy. There are a range of different privacy and security controls that could be used, including encryption, that suit different contexts - see for example (Camenisch et al., 2011; Mowbray & Pearson, 2012). Implementation and configuration choices also need to be decided upon. Butin et al. have proposed the notion of 'Accountability by Design' (Butin et al., 2013), but this specific term seems rather superfluous in view of the discussion above, in the sense that design should be a necessary part of accountability in any case. Hence we do not propose to use that term further, although it should still be recognised that design should indeed be an important part of accountability. The A4Cloud Project could be viewed in this sense as being Accountability by Design through the development of policies and tools to achieve accountability, all by design.

Given the explanation above, accountability is concerned with governance mechanisms related to punishment, remediation, transparency, providing a trustworthy account, holding to account, data breach detection and notification, etc. Correspondingly, accountability mechanisms and tools do not focus on providing privacy and security tools *per se*, but rather on formation of appropriate organisational policies, detection of violation of policies, notification, remediation in complex environments, increased transparency without compromising privacy, provision of a trustworthy account, improved verification and assurance, etc. Accountability should involve checking and proving that data stewardship is in place along the service provision chain, which involves showing that appropriate privacy and security 'design' controls are being used. Hence, accountability should not be a replacement for certain other procedures, including privacy controls, but should be used to complement these (Cavoukian et al, 2010; Pearson, 2013) and an accountability-based approach should not be used to justify the abandonment of privacy rights and principles.

Trust is an important factor that has a close relationship with accountability, as for example a good accountability deployment into an organisation might increase its trustworthiness for potential clients. Trust has traditionally also been related to security, although trustworthiness is a much broader notion than security as it includes subjective criteria and experience, among other factors. For an organisation or a person to be trusted, they should demonstrate accountable behaviour; defining governance, ensuring the implementation of trusted services, taking responsibility, remedying any failure, and being able to show justification of any action taken. Correspondingly, there exist both hard trust solutions (i.e. security-oriented trust focused on the degree to which a target object is considered secure e.g. credential-based authentication) and soft trust solutions (i.e. non-security oriented trust defined in terms of belief and behaviour and related to interaction records and reputation systems e.g. web of trust) (Wang & Lin, 2008).

Verification (as considered further in Subsection 2.4.2) is needed to encourage trust within an environment of market compliance. Trust issues will arise if levels of verification are perceived to be low, as has happened already with the Safe Harbour programme and the lack of trust by some parties in the self-certification involved.

2.2.4 Accountability and Control

The interpretations of the concept of control vary depending on the context. It might be used, for example, to indicate security checks in computational systems or monitoring of individuals' behaviour. Control[53] has two meanings referring *"a) to the power to direct, manage, oversee and/or restrict the affairs, business or assets of a person or entity and b) to the exercise of power to control*". Control, therefore, implies an underlying authority, which can be further exercised in practice; in other words, the power to control stems from an authority given by law, contracts or even *de facto*, under certain circumstances. The European Parliament (in a study conducted on Cloud Computing) points out the link between the notions of accountability and control. It states in this respect that an "accountability approach" would imply the vesting of obligations and liabilities upon every actor with considerable power, i.e. knowledge and control of the personal data (European Parliament, 2012), considering, therefore, that within an accountable environment obligations and liabilities are the essential balance against power. How to define, of course, "considerable power" in the cloud is open for discussion. The European Parliament further argues that an accountability based approach would lead to the distribution of obligations and liabilities on every actor with power – and therefore, control would also be distributed. This is particularly relevant for cloud computing, where multiple actors are involved in a delivery of a service. Under a different approach, though, it is considered that accountability falls under the scope of the controlling agenda rather the other way round: *"Accountability is but one aspect of legal and regulatory control, which is concerned with reporting, investigating, justifying and rectifying after the event. It is an essential part of a functioning system of institutional control but it is not the whole of that system."* (Mulgan, 2003).

Control and responsibility are co-dependent concepts. Responsibility sets limits to the entities, who exercise control – in the sense of power – while the allocation of responsibilities cannot lead to concrete actions in the absence of power. In cloud computing, control (and consequently, the allocation of

[53] According to a definition given in http://legal-dictionary.thefreedictionary.com/control

responsibilities) vary depending on the type of service. With different service types, a cloud user *"may have varying degrees of control, and therefore, different degrees of responsibility (...) generally, users have more control and flexibility with IaaS than with PaaS or SaaS (…) PaaS users have control over their application's code. Users decide what applications they wish to install and host on IaaS/PaaS, and such applications maybe user-developed, and therefore, user controlled. In contrast, SaaS users utilise standardised applications, provided by SaaS providers, and in environments that users cannot control, relying on providers to secure applications as well as environments. Thus, SaaS systems generally involve more provider control but still differ regarding provider access to intelligible user data."* (Kuan Hon, Millard, 2013).
In the stricter area of European data protection law, the entities who have the power to exercise control as earlier described bear –at the same time- the burden of accountability obligations. In particular, the Data Protection Directive allocates formally, for example, control on Data Protection Authorities (DPAs) assigning them with investigative powers (such as access to data, collection of information, etc.), effective powers of intervention (power to order the erasure of data, to impose a ban on a processing, etc.), and the power to start legal proceedings when data protection law has been violated (Article 28 of the Directive). In addition, the Directive considers data controllers as the entities who determine the purposes and the means of processing introducing rather an *ad hoc* decision making criterion linking to the notion of control rather than extensive powers (Article 2(d) of the Directive.) Note that both DPAs are assigned with accountability obligations deriving from regulation and from social norms, while data controllers are assigned with obligations stemming primarily from regulation and contracts.

The Article 29 Working Party, however, takes the discussion of controller a step further, pointing out that "*Being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes. Indeed, a merely formal criterion would not be sufficient (...) it may happen that the formal appointment would not reflect the reality, by formally entrusting the role of controller to a body which actually is not in the position to "determine"*" (Article 29 Data Protection WP on the concepts of "controller" and "processor", 2010). In the same spirit, it is stated that: "*the concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis. Therefore, determining control may sometimes require an in-depth and lengthy investigation. However, the need to ensure effectiveness requires that a pragmatic approach is taken with a view to ensure predictability with regard to control. In this perspective, rules of thumb and practical presumptions are needed to guide and simplify the application of data protection law."*[54] So, in the context of data protection, in the case of the data controller it is not only the allocation of power on a formal basis which justifies authority but also the reality of processing itself, which leads to *de facto* concentration of power and explains the allocation of liabilities.

Control and accountability are closely related, yet different, concepts. They both imply the existence of power and the allocation of responsibilities and liabilities. Also, they both aim at preventing harm, detecting vulnerabilities or even remedying any failures occurred. They do not put equal emphasis, though, on the same elements and means employed. Control puts forward the role of monitoring and oversight, heavily relying upon the deterring effect of liability and sanctions. Accountability, on the other hand, brings about the role of transparency, bringing about the key role that the account can play. It is considered in that respect that "*Given the emotive value of the term 'accountability', there is a natural tendency to use it to describe all means of control whether or not these means include actually calling anyone to account*." (Mulgan, 2003). It seems, therefore, that the line between accountability and control is drawn by the account.

2.2.5 Transparency: An Important Element of Accountability

A very broad definition of transparency is that it involves operating in such a way as to maximise the amount of and ease-of-access to information which may be obtained about the structure and behaviour of a system or process. For example, a cloud provider offers transparency of its security processes if it provides a web page with current and historical availability. It provides further transparency if it offers explanations for outages. However, this definition is too broad in the sense that it is used as a component of accountability, as there might be a conflict between such maximal openness and the obligation to

[54] See Opinion above, page 9.

have appropriate technical and organisational security measures in place to protect personal data. Furthermore, generating more information does not necessarily lead to transparency (Tsoukas, 1997). More specifically, the focus of transparency as an attribute of accountability is on *'ex ante transparency'* that should enable the anticipation of consequences before data are actually disclosed (usually with the help of privacy policy statements), and on '*ex post transparency'* that informs about consequences if data already has been revealed (i.e. what data are processed by whom and whether the data processing is in conformance with negotiated or stated policies) (Hildebrant, 2009).

Transparency encompasses 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: "*Information Accountability means that Information usage should be transparent so it is possible to determine whether a use is appropriate under a given set of rules"* (Weitzner et al., 2008). More broadly, an accountable organisation is transparent in the sense that it makes known to relevant stakeholders the policies defined about treatment of personal and/or confidential data, can demonstrate how these are implemented and provides appropriate notifications in case of policy violation, as well as responding adequately to data subject access requests. Note that transparency does not involve revealing the personal and/or confidential data itself, as that should be kept confidential, with the exception that data subjects have the right to access their own data (cf. data subject access). This is analogous to the privacy principle of transparency, which is about the need for transparency of privacy policies and not of the personal data, e.g. as elucidated in the OECD privacy guidelines (OECD, 1980).

2.2.6 Obligations

Obligations prove to be very important in terms of discussion of accountability within service provision networks. According to the scope of the project defined in Section 1, our focus is on organisational obligations relating to the treatment of personal data and business sensitive information. We define obligations as follows:

> **Obligation:** *An obligation is a requirement, agreement or promise for which an actor is morally or legally bound and that has certain consequences if it is breached. Obligations can be based on: contract, statute or morality.*

Legal obligations, those derived from contract or statute, often overlap with moral obligations, but not all moral obligations have a counterpart in law or contract, nor do all legal obligations have a moral connotation (e.g., the maximum speed on a road is in a sense arbitrary). Green argues that "*legal obligations are legal requirements with which law's subjects (legal entities, natural persons) are bound to conform. An obligatory act or omission is something the law renders non-optional*" ('Legal Obligation and Authority', 2003, Stanford Encyclopaedia of Philosophy). On the contrary, moral obligations are standards with which legal and/or natural entities are expected to conform because they are moral agents. "Failure to comply" with a moral obligation does not necessarily entail remedies. "Failure to comply" with a legal obligation, however, does lead in –in principle- to sanctions or other forms of remedies.

Organisations have obligations that derive from these three different sources (namely, contract, statute or morality), and need not only to meet the obligations but to consider how to make sure that the behaviour of business partners or subcontractors does not invalidate these. As reflected in the definition of accountability given above, the policies, contracts and promises defined by an organisation should reflect the obligations that act upon them. The accountability practices defined in Section 5.1.2 provide a means for the organisation to put a framework and mechanisms in place to meet these obligations in practice. This is further discussed and evaluated in Section 7. Therefore, an accountable organisation needs to ensure that obligations to protect data are respected by all the parties along the service provision chain, no matter where in the world they may be.

The division of obligations into these three elements is reflected within our model and approach to accountability, in which we argue that ethical aspects and social norms should be taken into account by organisations as part of their accountability programmes, in addition to consideration about how to comply with other stakeholder requirements and legal aspects. Other types of obligations relating, for instance, to user preferences, could fit under these different categories in different contexts; for example,

in some contexts user preferences might be linked to a legal obligation but in others they do not. Another example is the performance of data protection impact assessments, which (although currently provided only within the context of codes of conduct) is introduced within the GDPR (EC, 2012: Article 33) as a clear obligation allocated under circumstances either to data controllers or processors acting on their behalf. An accountability-based approach can be considered not only to help and encourage organisations to clarify and meet their obligations, but also to bring stronger obligations onto organisations, in a sense. First, it brings additional obligations centred on demonstration and taking responsibility: the Galway/Paris project describe accountability as: "the *obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations. Accountability goes beyond responsibility by obligating an organisation to be answerable for its actions"* (CIPL, 2009). Furthermore, as mentioned above, it may vest stronger obligations upon certain parties, such as data processors (EP, 2012). Further discussion about the obligation to render an account is given in the following section.

2.3 The Notion of the Account

A central aspect of accountability is that organisations need to demonstrate acknowledgement and assumption of responsibility, both in terms of having in place appropriate policies and procedures, and in terms of promoting good practices that include correction and remediation for failure and misconduct. Responsible decision making should be used, and in particular organisations should report, explain and be answerable for the consequences of decisions about the protection of data. The account is the principal means for demonstrating accountability, as considered further within this section.

Perhaps the core of accountability, and indeed, the root word of accountability, is 'account'. For all intents and purposes, account can be defined as "a report of an event or process." In that respect, an event is "*any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring*." Process, on the other hand, is "*a series of actions that one takes in order to achieve an ultimate result*." The importance of the account is further highlighted by the fact that it oftentimes proves to be the only interaction between the various actors in demonstrating accountability. It also serves as the element which helps drawing clearly the line between accountability and other related concepts as, for example, responsibility or transparency, which do not otherwise rely necessarily upon the production of a concrete account. Taking into account the conceptual definition of accountability as consisting of "*defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure*", the account goes beyond merely giving a reply to another cloud actor - it serves ultimately to report an event, provide an explanation and justify specific actions in response to the event.

In that context, the discussion herein builds on two distinct aspects and/or forms of accounts: a) the legal account, meaning the type and amount of information required by regulation and contracts; and b) the operational account meaning the entire set of information that a system can actually provide as output. This section addresses the perspective of legal and regulatory requirements, while the latter aspect is addressed in Section 8 from a metrics and business perspective.

2.3.1 Overview of the Account from Legal and Regulatory Perspectives

We begin with the analysis of the notion of the account from a legal and regulatory perspective, specifically data protection laws and other legal requirements which are generally dictated by contracts. There has been little specificity provided by the regulators at the European level until recently as to what accounts must contain exactly, and likewise, most contracts in cloud computing also provide little details as to what an account must contain.

Traditionally, 'account' was closely aligned with an accounting, which generally involves numbers, usually in the form of currency, and tracing of funds. However, the notion of the account has evolved to the present day where it is used in much broader contexts involving all types of information, including not just numbers and currency, but documents, tables, figures, logs and any other sort of information helpful in fully examining any given situation. Moreover, nowadays the account may take various forms, given that an account can be provided digitally, in paper form or even orally depending on the particular

circumstances surrounding the specific obligation from which the particular obligation of account giving arises. Most often, an account will serve a retrospective function, i.e. demonstrating what has happened, though this has evolved into also including a prospective function, especially where something has gone wrong with the accountor providing information as to how such situations might be remedied or addressed in the future. It is oftentimes the underlying accountability obligation, i.e. preventative, detective, responsive, etc., which will, also, dictate the timing of the account. As to the purposes and stages of providing an account, the oft-cited Charles Raab noted:

> *"To 'give an account' – rendre des comptes – is to tell a story, and there are three levels that can be distinguished. First, on a weak definition, it means the obligation of an organisation to report back, to 'give an account of its actions'. Second, on a stronger definition, it means that, plus the implication that the audience can interrogate the account and produce other accounts 'on their own account'. Third, on the strongest definition, it means the previous two plus the implication that sanctions can be brought to bear where there is a general agreement that the organisation has 'given a bad account of itself', either (a) through its inactions, or (b) through its own unsatisfactory production of an account. The audience, which may be the public, can thus 'hold the organisation to account', and that might have real consequences."* (Raab, 2012).

And, as Raab further noted:

> *"But the account must also, and essentially, include descriptions and explanations of the actions, for two reasons. First, so that we can better understand the organisation's intentions and its understanding, or theory, of its own situation or how it might act in it. Second, because most of a steward's actions are invisible to the principal, and therefore have to be re-presented, through stories or accounts, explanations, and justifications."* (Raab, 2012)

Importantly, especially for an organisation to be accountable, an account is not provided only when something has gone wrong, but rather can be presented at any time upon request. As one law firm advised:

> *"Accountability does not wait for a system failure; rather, it requires that organisations be prepared to demonstrate upon request by the proper authorities that it is securing* and protecting data in accordance with the essential elements." (Hunton & Williams LLP, 2009).

However, as it will be further discussed below, the European data protection framework implies, rather than provides, for the availability of accounts.

2.3.1.1 Data Protection Directive and Proposed Data Protection Regulation

Although the Data Protection Directive (DPD) and the proposed General Data Protection Regulation (GDPR) do not refer explicitly refer to the notion of the account as such, they do provide for some forms of accounts. Generally, the DPD requires information to be provided to data subjects and a notification of processing to be submitted to the Data Protection Authorities, while the proposed GDPR takes this one step further adding accounts as, for instance, the mandatory Data Protection Impact Assessment[55] or the documentation to be maintained by Data Controllers and Data Processors. The European Data Protection Supervisor (EDPS) argues that the proposed GDPR strengthens accountability[56] on the basis on of the accounts provided such as the earlier stated Data Protection Impact Assessments (DPIAs). However, due to the fact that there are national laws implementing the DPD at each Member State and that the proposed GDPR provides for implementing and delegating acts specifying further its content, there is not much detailed guidance at the specifics surrounding such requirements, especially, with regard to the process of producing an account. Note that the present document will not discuss in depth the amendments the European Parliament suggested to the Commission's proposal[57].

[55] A Data Protection Impact Assessment is a purely prospective account which requires the data controller to prospectively assess the impact of collecting and processing data upon the data subject's data protection rights.
[56] Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 16th November 2012, para.60.
[57] For a more detailed discussion of the proposed Data Protection regulation, see Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation, W.Kuan. Hon, Eleni Kosta, Christopher Millard, Dimitra Stefanatou.

According to article 10 of the DPD, *"(...) the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it: (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing for which the data are intended; (c) any further information such as - the recipients or categories of recipients of the data, - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, - the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject*." The information requested to be provided to data subjects is actually a form of account reporting on specific aspects of the processing.

Moreover, article 19 of the DPD provides that the data controllers must give almost the same account to Data Protection Authorities in the form of a notification. In particular, article 19 of the DPD states that the notification "*shall include at least: (a) the name and address of the controller and of his representative, if any; (b) the purpose or purposes of the processing; (c) a description of the category or categories of data subject and of the data or categories of data relating to them; (d) the recipients or categories of recipient to whom the data might be disclosed; (e) proposed transfers of data to third countries; (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.*" In that sense, the submission of the notification announcing processing reports on the processing process, before the processing actually starts.

It is notable that these two forms of accounts provided under the DPD to some extent overlap. The identity of the controller or his representative, the purpose of the personal data processing and the recipients of the personal data are requested explicitly in both cases. However, taking into account that the information to be given to the data subject includes *"any information further necessary to guarantee fair processing"* (article 10(c) of the DPD), then the transfers of personal data to third countries or a general description of the security measures required for the notification could possibly be contained in the account given to data subjects, provided that they ask for this.

As far as the DPIAs are concerned, article 33(3) mandates that "*The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.*" The assessments requested to be conducted by controllers and processors under circumstances is proposed to be submitted to the Data Protection Authorities upon request.

Another form of account provided by the proposed GDPR is meant to be in paper. According to article 28(2) of the proposed GDPR: "*The documentation shall contain at least the following information:(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (b) the name and contact details of the data protection officer, if any; (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (d) a description of categories of data subjects and of the categories of personal data relating to them; (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them; (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards; (g) a general indication of the time limits for erasure of the different categories of data; (h) the description of the mechanisms referred to in Article 22(3).*" Note that the documentation proposed to be maintained in all cases of processing would be available to the Data Protection Authorities only following a request.

The earlier stated provisions provided within the DPD and the proposed GDPR constitute forms of accounts in the sense that they all report on the process of processing of personal information, which is

either launched or to be launched. Interestingly, in all four cases earlier stated, both the current and the proposed framework set the minimum information required to be contained in such accounts by stating either what should be included "at least" in the notification to the Data Protection Authorities (article 19 of the DPD), in the documentation maintained (article 29 of the GDPR), in the Data Protection Impact Assessment (article 33 of the GDPR) or by indicating that "any necessary" information could be provided to individuals who are entitled to be informed (article 10 of the DPD). Both the current and the proposed framework allow, therefore, for "minimum accounts" without preventing companies acting in their capacity as data controllers – or processors - to provide more information than the minimum requested by law. The additional information can be included in the operational accounts (as further discussed in Section 8.3).

As to the time the aforementioned accounts are meant to be delivered, this may significantly vary, due to the exact meaning that "events" and "processes" may take in the context of data processing. Under the DPD, the account-information can be delivered on request to the data subject at any stage of processing, including any necessary information relating to the entire process, while the notification-account to the Data Protection Authorities is requested before the launch of processing reporting on the process to be started. Similarly, in the context of the GDPR, it is suggested that the account-documentation be maintained throughout the process of processing and the account-DPIA must report on the process of processing to be started, and it is explicitly required to be periodically repeated.

Note of significant importance in relation to the notion of the account is the reversal of burden of proof in favour of individuals, which – though not explicitly mentioned - derives from several provisions in the text (i.e. articles 7, 12 and 19 of the proposed GDPR). Because personal data processing is customarily conducted behind closed doors and individuals only become aware of their data being processed whenever its results (adversely) affect them, they are frequently unable to adequately prove their case in courts. Therefore, a reversal of the burden of proof obliges data controllers to demonstrate that they comply with the law and that the various legal prescriptions were applied faultlessly. The data subject does not have to demonstrate exactly where the processing, which they never witness, went wrong (de Hert et al., 2013). Accounts at hand could therefore be a proactive way for data controllers to prove that an alleged breach of law did not take place.

2.3.1.2 Accounts in Cloud Contracts

Contracts between cloud customers and cloud subjects, and, to a lesser degree, contracts between cloud customers and cloud providers also do not shed much light on the notion of the account. Contractual obligations essentially take regulatory obligations, which may be at a high level, and translate them into specific binding obligations between the parties.[58] And even then, cloud providers largely try to further limit their obligations, particularly their liability, in their contracts and/or terms of service, see (Bradshaw, Millard, Walden, 2013). Note that that it is not always clear whether cloud customers should be considered to be acting as data controllers or data processors[59,60]. As between data controllers and data processors, Article 17 of the DPD requires data controllers to impose on data processors the same obligations regarding the implementation of security measures as those imposed on data controllers. However, the relationship between data controllers and data processors as such must be established upon the prior conclusion of a contractual agreement (or other legal act).[61]

Finally, the one area where one would most expect an account to be provided would be where there has been a security breach. In this context, the accounts requested within the contractual agreements will most probably report in writing the security breach within a specific number of days following the breach the remedial actions taken and planned to be taken to remediate the breach. Yet, even in negotiated contracts, as opposed to the standard, non-negotiated contracts which currently dominate

[58] It is also important to note that contractual obligations are not only based on regulatory obligations. Non-legislative obligations such as industry standards and certifications or even accepted industry norms can be included into agreements, which turn such obligations into legal contractual obligations.

[59] "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 16th of November 2012.

[60] CNIL's recommendations for companies using these new services, http://www.cnil.fr/fileadmin/documents/en/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf

[61] DPD Article 17.3 *The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that: the processor shall act only on instructions from the controller.*

the cloud computing landscape, "*many providers' standard terms did not require reporting of security incidents and so on to users*" (Hon, Millard, Walden, 2013). Thus, while accounts are imposed by law through legislation and contracts, cloud contracts – though, in principle, aiming at specifying further the high level requirements set by law – do not bring about sufficiently the role accounts might play in enhancing transparency of cloud offered services.

2.3.1.3 The Practicalities of the Account

Despite the foregoing, a failure to provide an account or the provision of an unsatisfactory account could expose a cloud customer, a cloud provider or a cloud subject, depending on the specific circumstances, to a claim of breach of contract. In addition, as examined in greater detail below from a business perspective, it makes good business sense for cloud customers to provide an account from time to time to their users, and likewise, data processors to data controllers, especially where there can be claimed to be a breach of the particular contract. So, even if in most cases an account is due on the basis of a legal/contractual obligation or following a request, it may be also provided out of "goodwill", i.e. serving a business's aim to build/maintain their reputation. Perhaps more importantly from the cloud customer's perspective is that where there is an alleged breach of applicable data protection regulations, the cloud customer will be required to provide a report, i.e. an account, to the applicable data protection authority aiming to demonstrate compliance with law and hoping to avoid sanctions and/or minimise such sanctions.

In light of the foregoing, an account, when required and/or provided, usually consists of the accountable actor providing a report of an event or process. The account should generally include the answers to what are traditionally referred to as the 'reporters' questions', i.e. who, what, where, when, why and how. Often, an account will also include the measures being taken to remedy a breach or failure. In the latter case, the essential corrective measures to be taken might be dictated by decisions delivered by DPAs or held by courts. Still, the form and content of the account are contextually dependent and may be specifically dictated under the specific circumstances. Forms of the account may include Data Protection Impact Assessments, notifications to supervisory authorities, notifications to data subjects, contractual compliance verifications, audit reports, and even certifications and seals obtained by data controllers and/or data processors from third party certification agencies such as the Cloud Security Alliance.

2.3.2 The Obligation to Render an Account

The role of the *obligation to render/or give an account* in relation to accountability has triggered intensive discourse. Note, however, that the obligation – not only the act – to render/or give an account is often formulated in the literature as "being held to account". Scholars such as Mulgan (2003), Bovens (2007) and Schedler (1999) argue that the relationship between two entities forms an accountability relationship only if one party is obliged to render account to the other. Therefore, the "right to demand" explanation and justification and the "right to sanction" resulting for the obligation to deliver an account are essential elements of an accountability relationship.

Philp (2009), on the other hand, considers the obligation to render an account as an accountability requirement, lowering, however, the standards by setting the requirement of an "*ability*" to render an account rather than an obligation to deliver one. Similarly, Hunt (2006) detangles the notion of "the obligation to render an account" from accountability. He argues that accountability should be seen simply as "*a preparedness to explain and justify one's intentions, actions and omissions to stakeholders, and the means by which this preparedness is manifested*."

The obligation to render/give an account is closely related both to the notion of obligations and the notion of the account. Given that the conceptual framework elaborates on the existence of different sources of obligations and that the account – as will be explained later in the document - might be declarative or evaluative, A4Cloud does not consider that the earlier views are necessarily mutually exclusive. Depending on the context, the obligation to render an account might refer either to an obligation to deliver a concrete form of account, for example, a preliminary assessment of the security measures to be notified to the Data Protection Authority or as a general obligation for responsiveness resulting from policies or moral standards.

2.3.3 A Practical Example of an Account

Applying these principles in practice perhaps best demonstrates the notion of the account and what would be encompassed in an actual account.[62] Using Business Use Case 1 (BUC 1) from the Use Case Descriptions Deliverable in WP B-3, it is easy to envisage multiple situations where an account might be necessary. BUC 1 concerns the flow of health care information from medical sensors to the cloud. The actors in BUC 1 include the business end users of healthcare organisations, individual end users of elderly persons using the sensors, cloud providers providing data storage and sharing, and the data regulator of the Norwegian Data Protection Authority.

This provides an example of one common situation where an account is required and provided, namely a data breach scenario. This scenario hypothesises a breach of one of the cloud providers where data has been accessed and downloaded without authorisation. Critically, neither the DPD, nor its implementation in Norway under the Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act) requires a notice of the security breach to be provided to any of the other actors, namely the Norwegian DPA or the data subjects. Such notification may be required under other Norwegian regulations. Regardless, as an accountable cloud provider, the provider here desires to provide an account to the user and the Norwegian Data Protection Authority. The notification holds the role of the account, which gives a report on the event of a data breach. Note that in case of an account including sensitive personal information, the delivery of such an account to the end user does not constitute a breach of data protection law, provided that the end user is the data subject to whom this data relate. To the end users, i.e. the data subjects, the account would likely be sent by email, but depending on the severity of the breach, notice could and quite possibly should also be sent by mail to ensure proper notice and receipt. As noted above, the account here should encompass answers to the fullest extent possible of the reporters' questions, i.e. who, what, when, where, how and why, as well as measures being taken to prevent such breaches in the future. More specifically, the cloud provider will want to (1) explain who committed the breach, if known, or that further investigation is being undertaken to ascertain who committed the breach; (2) what the breach consisted of and the extent of the information that might have been accessed, i.e. health information, financial information, etc.; (3) when the breach occurred and was discovered; (4) where the breach occurred; (5) how and why the breach occurred, if known, what security measures in place, whether those security measures were properly working at the time of the breach, and how the breach generally circumvented such measures; (6) what measures were taken to ascertain the extent of the breach; (7) what measures are being taken to prevent such breaches in the future; (8) contact information for a department or person to respond to any further enquiries regarding the breach; and (9) perhaps a link to a web page where further information, if any, will be disseminated regarding the breach and any further investigation. Thus, hypothetically and at its basic form, the account to the cloud provider may appear as follows:

[62] This is just one example, and the account will vary depending on the factual circumstances of any given event, as well as the specific regulatory and contractual obligations that may specifically apply in any given situation. Further, the practical implications of the account will also be examined further in the A4Cloud Deliverable entitled "Report on legal and regulatory dependencies for effective accountability and governance", 2014.

Dear End User:

We write to you regarding a recent unfortunate incident involving an unauthorised access to our servers in which your personal data may have been accessed.

On [Date], we believe that an outside intruder circumvented our security measures and was able to access the personal information of some of our users. We realised the access almost immediately and were able to minimise the access. The full extent of the breach is not known, or whether your information was accessed and/or otherwise obtained by the intruder. What we do know at this time is that our security measures were operating properly, but the intruder was able to circumvent such measures through illegal means. We have since closed the means through the access occurred and are re-examining all of our security measures to ensure the fullest protection available moving forward. We are also continuing to investigate the situation and further exploring the extent of the information which may have been accessed, of which we will specifically provide updates to you once the extent of the intrusion and the information which was accessible is known.

We will release further pertinent information regarding our investigation on our website at www.cloudprovider.com/[Date]breach, so we invite you to regularly check that page for any updates regarding this situation. Should you desire to contact us for further information, please do so at [email] or [telephone number], where we will be standing by to respond to any enquiries as quickly as possible.

We thank you for your continued patronage and your confidence in us preventing these unfortunate incidents in the future.

Sincerely,

Cloud Provider

Thus, to the end user, the account will be more general and written with more understandable language, without much of the technical information that would otherwise be available and/or provided by the cloud provider to a business customer.[63] The cloud provider may decide to include more technical information on its website or upon request by the end user, but the overriding objective to the end user should be a clear explanation of the event. Further, as noted within the account, more information can and should be provided by the accountor as it is obtained and discovered by the cloud provider. Thus, the accountor can provide more detail, i.e. be more transparent, as to the details and the extent of the breach, especially where the breach is later discovered to have specifically impacted individual data subjects.

2.4 Demonstration

As we have explained above, demonstration is a key aspect of accountability, and the account is a central means for demonstration. This concept will be explored in more detail within this section; first we consider its role, and then consider the closely related notion of verification of the account.

2.4.1 The Role of Demonstration

Demonstration is a central element of accountability, as for example brought out by the following: "*The added value of a general principle of accountability lies in the fact that it could function as a general obligation to demonstrate results, while leaving freedom to data controllers as to the means they employ.*" (Hijmans, 2011). The demonstration might need to be upon request: "*Accountability does not*

[63] The same may not be said for the account of the same breach to the Norwegian Data Protection Authority. There, the account likely should contain more technical information, the extent of the breach, a more technical overview of the breach, and the number of persons impacted by the breach. The account should also include relevant evidence regarding the breach, i.e. any applicable logs, audit trails, system maintenance records, and any other technical evidence regarding the proper operation of the cloud provider's security measures and the extent of the breach.

wait for a system failure: rather, it requires that organisations be prepared to demonstrate upon request by the proper authorities that it is securing and protecting data in accordance with the essential elements" (CIPL, 2009). Figure 7 shows how the demonstration process under accountability (shown on the right hand side, in the cloud context), differs from a more traditional approach.

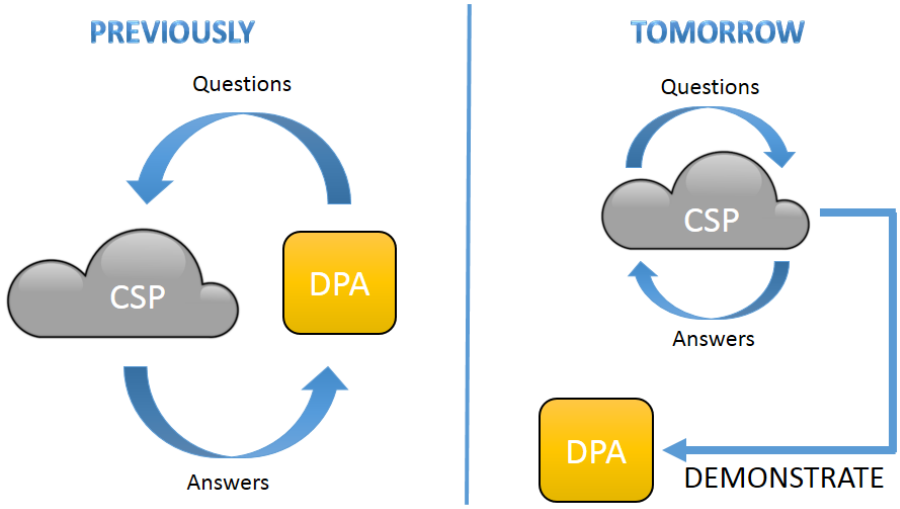


Figure 7 Demonstrating Accountability

Organisations (including cloud service providers) can select from accountability mechanisms and tools in order to meet their obligations, but the choice of such tools needs to be justified to external parties, which is done through the provision of accounts. In so doing, they need to engage in proactive, and not only reactive behaviour. In the data protection context, it is data controllers (and processors) that are protecting personal data rather than the data protection authorities (DPAs), but the accounts are given to the DPAs.

Although organisations can select from accountability mechanisms tools in order to meet their context, the choice of such tools needs to be justified to external parties. It would be a mistake to have this reliant upon self-certification or weak certification processes. As Bennett points out (Bennett, 2012: p45), due to resource issues regulators may need to rely upon surrogates, including private sector agents, to be agents of accountability, and it is important within this process that they are able to have a strong influence over the acceptability of different third party accountability mechanisms. This can be achieved via independent testing of practices, provision of evidence that is taken into account, including auditing against the ISO 27001 series and associated cloud security standards (further related discussion is given in Section 8).

It is still rather an open issue about when exactly organisations must be ready to provide a demonstration. For example, it could be: before any processing (perhaps as part of a third party assurance review), when processing is particularly risky, to provide flexibility, for example via mechanisms such as BCRs and CBPRs, when a data protection breach has occurred or triggered by a spot check by a regulator.

2.4.2 Verification

Verification methods may differ across the different forms of account in the cloud, which include:

- Data Protection Impact Assessment (by data controllers & data processors)
- Notification to the supervisory authorities
- Notification to data subjects
- Contractual compliance verification
- Documentation obtained, created, and maintained by data controllers and data processors
- Certifications and seals
- Audit Reports.

Nymity has provided an example structure for evidence and associated scoring mechanism for accountability based on existing documentation that can form some of these types of accounts – but some organisations may want to take a different approach and so this should not be regarded as a standard. The Nymity accountability evidence framework is intended for collecting evidence in a single organisation and for demonstrating accountability that is structured around 13 privacy management processes (Nymity, 2014). A more generic approach is considered further in Section 8. Broadly speaking, there are different levels of verification for accountability, as proposed by Bennett (Bennett, 1995), which correspond to policies (the level at which most seals programmes operate), practices and operations, as shown in Figure 8.

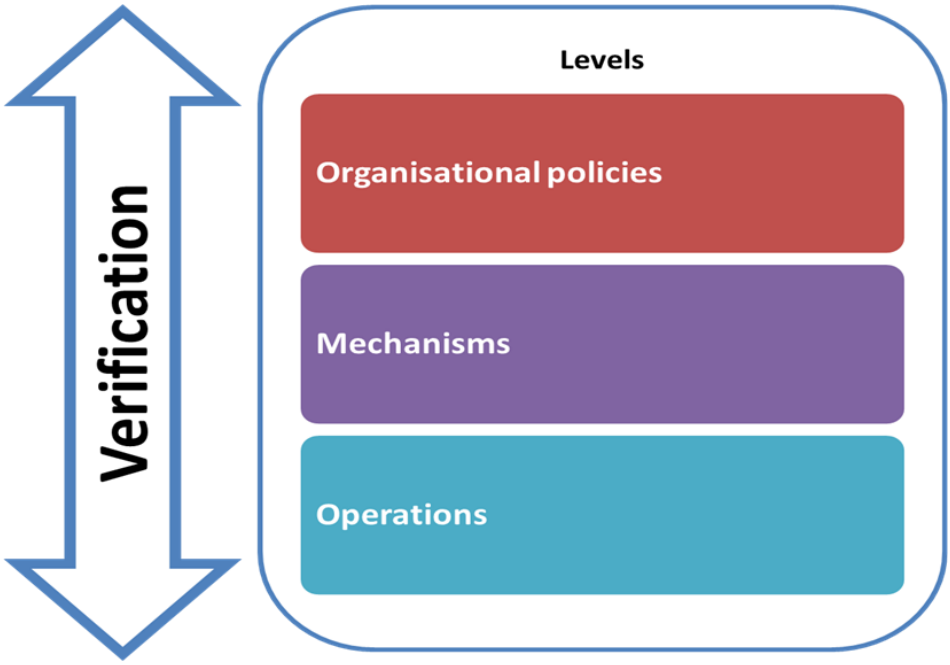


Figure 8 Different Levels at which Verification Should Take Place

It is very weak to carry out verification just at the topmost levels – instead, mechanisms should be provided that allow verification across all levels. As discussed further below, this is indeed the approach of the project. Bennett's distinction (Bennett, 1995) was between accountability of policies, procedures and practice. Most privacy seal programmes just analyse the wording in privacy policies without looking at the other levels, and thus provide verification only at this first level (of policies). The second level relates to internal mechanisms and procedures, and verification can be carried out about this to determine whether the key elements of a privacy management framework are in place within an organisation. Few organisations however subject themselves to a verification of practices, and thereby being able to prove whether or not the organisational policies really work and whether privacy is protected in the operational environment. To do this, it seems necessary to involve regular privacy auditing, which may need to be external and independent in some cases. We talk further in Section 8.3 about how this may be achieved.

In terms of the verification process, there are various different options about how this may be achieved. First of all, there should be spot checking by enforcement agencies (properly resourced and with the appropriate authority) that comprehensive programmes are in place in an organisation to meet the objectives of data protection. Secondly, there could in some cases be certification based on verification, to allow organisations to have greater flexibility in meeting their goals. However, it is still unclear who provides the certification, and what checks are needed. It is also unclear what types of verification are needed for new types of processing, such as big data analysis. It seems still an open question about whether all users of data need to be verified, and if so whether this is practical. Core verification issues related to accountability that still do not appear to be resolved may be summarised as follows:

1. ***How can the verification process be trusted – both in terms of the people doing it and that it is done to a proper standard?***
2. ***What implications do variations in the characteristics of the verification process have, and which might work best for which circumstances as a result?*** There could for example be a push model in terms of the account being produced by organisations or else a pull model from the regulatory side; the production of accounts could be continuous, periodic or triggered by events such as breaches. There may also in some cases be certificate-based options, like BCRs.
3. ***How can the different aspects of verification be obtained, and what is the role for third parties?*** For example, the verification could be in relation to the measures used or else about the appropriateness of what has been deployed for the context or else could be an operational proof of compliance or non-compliance with regard to what is actually happening within the system at runtime.

2.5 Implementing Accountability in Practice

Organisations are proven to be accountable through the implementation of concrete accountability measures. The notion of accountable organisations, though, is not consumed entirely in technicalities, given that accountable organisations are expected to behave in general in an accountable manner. And although accountable behaviour is not a matter of resources, implementing accountability in practice is largely based upon the financial capacities of organisations, which allow –or do not allow- for the development of technical tools and supporting organisational measures. Large organisations have more freedom and flexibility regarding the means –including the staff- they employ. For instance, many large organisations have a Chief Privacy Officer and privacy staff in order to implement compliance in their organisations. SMEs often do not have the resources for hiring qualified privacy experts and instead the person who is responsible for overseeing the organisation's compliance with applicable data protection legislation could well be the owner or operator.

The Galway project has defined the central elements that an accountable organisation needs to address as being (CIPL, 2009):

1. Organisation commitment to accountability and adoption of internal policies consistent with external criteria
2. Mechanisms to put privacy policies into effect, including tools, training and education
3. Systems for internal, ongoing oversight and assurance reviews and external verification
4. Transparency and mechanisms for individual participation
5. Means for remediation and external enforcement.

Influenced by this approach, the Canadian privacy commissioners have specified the measures that an accountability management program (for the data protection domain) would ideally include (OIPCA et al, 2012):

1. establishing reporting mechanisms and reflecting these within the organisation's privacy management program controls
2. putting in place privacy management *program controls*, namely:
    a. a *Personal Information Inventory* to allow the organisation to identify the personal information in its custody, its sensitivity and the organisation's authority for its collection, usage and disclosure
    b. *policies* relating to: collection, handling and disclosure of personal information (including requirements for consent and notification); access to and correction of personal information; retention and disposal of personal information; privacy *requirements for third parties* that handle personal information; security controls and role-based access; handling complaints by individuals about the organisation's personal information handling practices
    c. risk assessment mechanisms
    d. training and education
    e. breach and incident management
    f. procedures for *informing individuals* about their privacy rights and the organisation's program controls
3. developing an *oversight and review plan* that describes how the organisation's program controls will be monitored and assessed
4. carrying out *ongoing assessment and revision* of the program controls above.

Furthermore, the GDPR includes many accountability elements including, in Article 22, a list of a Data Controller's accountability instruments:

- Policies
- Documenting processing operations
- Implementing security requirements
- Data Protection Impact Assessment
- Prior authorisation/consultation by Data Protection Authorities (DPAs)
- Data Protection Officer
- If proportional, independent internal or external audits.

Of key importance for accountability at an organisational level is the production of accounts, which might take, for example, the form of annual reports. The publication of such forms of accounts creates a great impact on the company's reputation. The more complex –and, therefore, opaque- the organisational structure is, the greater the need for transparency becomes. Giving an account, for example, is one means by which individuals and organisations are constituted as moral agents. As it is argued, "*Giving an account is one activity in which we come to be as selves and particular kinds of communities through forms of discourse that shape, guide and judge life regarding concern for the common good, human solidarity and basic respect*" (Schweiker 1993, 235). In other words, organisations become members of a community of stakeholders through the activity of giving an account, and therefore demonstrating their capacity as shown in the figure below. The act of account giving, therefore, mirrors clearly accountable behaviour within organisations of all size to external stakeholders.

2.5.1 Privacy Safeguards

As far as the project's scope is concerned, organisations are in the position to provide guarantees for the protection of personal information through the implementation of privacy programmes and the promotion of the culture of privacy by design. Though privacy programmes can be put in place by organisations of all kind, privacy by design can be facilitated -or not- depending on the nature, and the scale, of the organisation's activities.

Privacy programmes

Privacy programmes are a core operational mechanism through which organisations implement privacy protection. In addition, a related element that needs to be in place within an organisation is data security breach notification, which may require both notice to an authority and notice to an individual affected by a security breach affecting their personal data. Key elements of a successful privacy programme include (Pearson, 2012):

1. garnering senior management support and establishing a comprehensive organisational privacy policy
2. establishing clear processes and assign responsibilities to individuals
3. using proven, existing standard and frameworks for security and IT management
4. establishing proper monitoring and audit practices, in order to verify and assess what is happening in the organisation against the privacy policies, and take action where required to achieve alignment

Figure 9 illustrates how accountability can be provided within an organisation, by means of the organisation identifying risks, having appropriate policies that mitigate risks, mechanisms for enforcement internally and for monitoring that these are effective within the enterprise, and for internal and external validation of this. In addition, provision of transparency and redress to customers and end users is also very important. Technology can be used here to strengthen the enforcement and monitoring of policies, to support privacy by design and to help provide assurance and transparency. Nevertheless, there are three important aspects that need to be highlighted relating to the relationship of accountable organisations with external stakeholders, including data subjects, auditors and regulators. Firstly, accountable organisations must ensure that accountability extends across their service supply chains, in other words ensuring that the services and partners they use are accountable too, which involves amongst other things proper allocation of responsibilities and provision of evidence about satisfaction of obligations along the service provision chain. Secondly, the way in which accountable organisations interact with other entities needs to be clarified: for example, the cloud customer or data subjects might also play a role by defining their own requirements which can then be

"negotiated" with the accountable organisation. Thirdly, there are implications in terms of the way that the enforcement and verification mechanisms for accountability will operate, the scope of risk assessment and the ways in which other stakeholders (e.g. Data Protection Authorities and auditors) are able to hold an organisation to account.

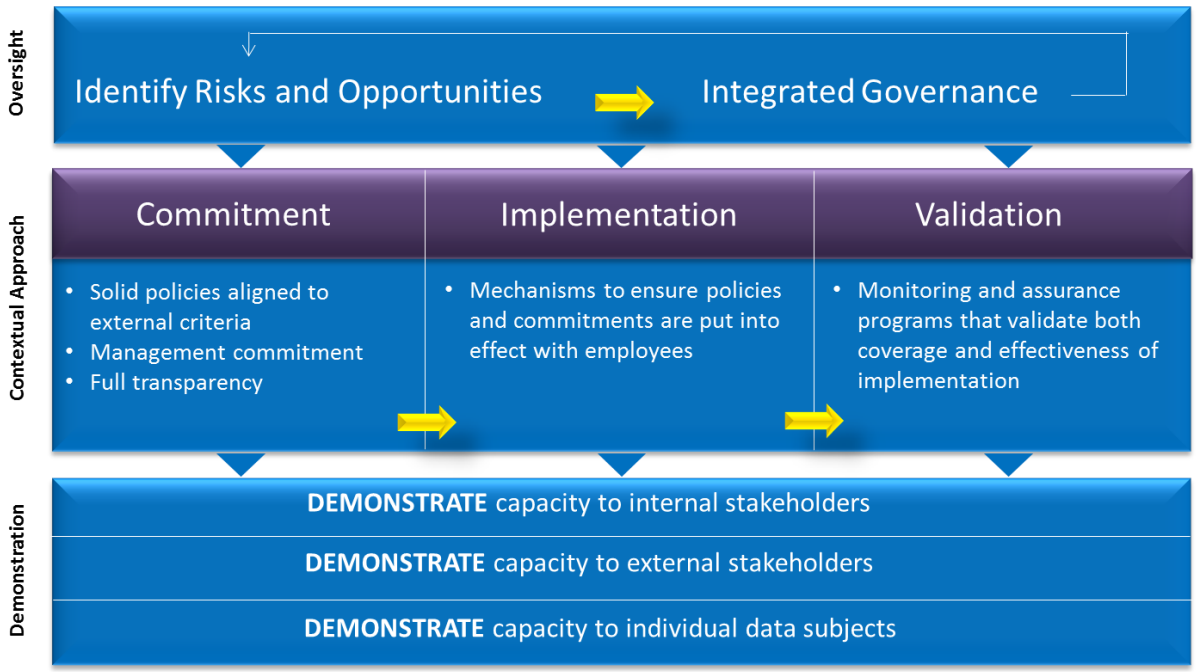


Figure 9 An Accountable Organisation

Notably for multinational companies, requirements are more diverse and privacy management is more difficult. Nevertheless, data is an asset, so proper privacy management will be valuable for forward-thinking companies, quite apart from being mandatory from a legal point of view.

Privacy by Design

Privacy by Design refers to the philosophy and approach of embedding privacy into design specifications, as first espoused by Ann Cavoukian and others (Cavoukian, 2012; ICO, 2008), although others might describe it in a slightly different way. It applies to products, services and business processes. The main elements are:

1. recognising that privacy concerns must be addressed
2. applying basic principles expressing universal spheres of privacy protection
3. mitigating privacy concerns when developing information technologies and systems, across the entire information life cycle
4. integrating qualified privacy input
5. adopting and integrating privacy-enhancing technologies (PETs) (Shen & Pearson, 2011).

In essence, companies should build in privacy protections at every stage in developing products, and these should include reasonable security for customer data, limited collection and retention of that data, as well as reasonable procedures to promote data accuracy. Various companies have produced detailed privacy design guidelines (see for example (Microsoft, 2007)). In addition to the Canadian regulators, there has been strong emphasis and encouragement from Federal Trade Commission (FTC) and EC amongst others on usage of a privacy by design approach (EC, 2012; FTC, 2012).

Privacy by Design may take different forms. In particular, "privacy by policy" is the standard current means of protecting privacy rights through laws and organisational privacy policies, which must be enforced. Privacy by policy mechanisms focus on provision of notice, choice, security safeguards, access and accountability (via audits and privacy policy management technology). Often, mechanisms

are required to obtain and record consent. The "privacy by policy" approach is central to the current legislative approach, although there is another approach to privacy protection, which is "privacy by architecture" (Spiekermann & Cranor, 2008), which relies on technology to provide anonymity. Unfortunately, the latter is often viewed as too expensive or restrictive. Although in privacy by policy the elements can more easily be broken down, it is possible (and preferable) to enhance that approach to cover a hybrid approach with privacy by architecture.

2.5.2 Accountability for SMEs

Small and Medium Enterprises (SMEs)[64] are considered to benefit significantly from cloud computing technology, given that they *"may acquire at a marginal cost, top-class technologies, which would otherwise be out of their budget range"* [65].The majority of SMEs companies exhibit a focused market activity, in order to deliver business solutions that are targeted to customised end users' needs. In the absence, of adequate financial capacity, however, such companies cannot maintain their own specialised departments to lead the accountability practices as a whole, but rather the need for a distribution of responsibilities to third parties is the most suitable approach for them. In order for SMEs to implement, therefore, an accountability-based approach, third parties might be requested, for instance, to get involved in:

- Consulting and/or outsourcing services on the specification of the privacy management program. On the grounds of the business objectives of an SME, which presuppose a given set of the SME customers' personal data that have to be collected and processed, external consultants can help SMEs in the identification of their legal obligations.
- Consulting and/or outsourcing services on the delivery of a creditable risk assessment plan, which will help the SME identify the potential business risks from the collection and processing of their customers' personal data and analyse the impact of their decision making in establishing dynamic collaborations with a list of trusted service providers.
- Consulting services to drive SMEs on the proper implementation of the accountability mechanisms. Such implementation may include assisting in the identification of metrics that should be constantly being monitored and analysed as the baseline information for making decisions on whether accountability is being met.
- Consulting services on the liability measures arising from the exposure of a failure in the correct implementation of the organisational data protection practices.
- Outsourcing services for the periodic internal audits to verify the compliance of the implemented mechanisms with the organisational data practices.

Given the likely extensive involvement of thirds parties, the allocation of resources is rather challenging for SMEs, in the sense that it is questionable whether they have the required resources for what seems to be a non-core activity. In any event, the SMEs will need to allocate the existing resources appropriately, keeping in mind the specific processing operations and the nature of data involved[66].

Whether outsourcing or external consulting is necessary to implement accountability, the SME has to appoint dedicated personnel to be responsible for running the accountability practices on behalf of the SME. Such responsibilities include periodic verification that accountability-based data practices are adopted in everyday business tasks of the SME. The appointed personnel should "sign off" the results

[64] According to Article 2 of the European Commission's Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (notified under document number C(2003) 1422), (2003/361/EC): "The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding 50 million euro, and/or an annual balance sheet total not exceeding 43 million euro".

[65] Opinion on Cloud Computing by the Article 29 Working Party, WP 196, adopted on the 1st of July 2012. See, also, 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

[66]For example, the European Commission estimates that the impact assessments provided in the proposed Data Protection regulation can range in cost from a14,000 (approximately$18,400) for a small-scale one, to a34,500 (approximately$45,344) for a medium-scale one. See, also, Impact assessment (including annexes) accompanying the Proposed Regulation and the Proposed Directive, SEC(2012) 72 final [hereinafter Impact assessment]; and Executive summary of the impact assessment, SEC(2012)]. All the documents are available at http://ec.europa.eu/justice/newsroom/dataprotection/news/120125_en.htm.

of internal audits on the compliance to the organisational policies and the respective actions to deploy and monitor them are successful, so that they do not constantly disturb the business continuity.

Depending on whether the SME acts as a cloud customer or provider, the level of the necessary outsourcing can vary a great deal. For example, in case of an SME acting as a cloud customer, the relevant accountability practices can be partially or fully implemented by the appointed SME personnel and only external consultancy might be requested. However, if an SME takes part in a cloud service chain as a cloud provider, the obligations arising from both the legal framework and their business objectives will lead the SMEs to outsource part of their accountability practices to third parties.

Interestingly, the limitations of SMEs in terms of resources highlight the role of accountability from a moral perspective. Taking into account the limited number of employees within SMEs, the role of each employee inevitably becomes more prominent. The personnel can probably have a better sense of the importance of the responsibilities assigned, the consequences resulting from their actions or omissions, which often create a direct impact on the organisations performance and profile. Subsequently, employees of SMEs can be well aware of their moral obligations and the role as moral agents. Furthermore, such an accountable behaviour by the SME's personnel could possibly minimise dependencies on external consultants. In other words, by making people being accountable for their roles, both the implementation of the organisational policies and the monitoring of the compliance to data practices is accelerated. Note that the moral dimension is rising to be critical in SMEs with international presence, as different culture and societal behaviour may affect the accountability maturity of an SME.

2.6 Summary

This section has introduced the concept of accountability, including a new definition, in order to provide a shared understanding of these terms within, and ultimately outside, the project. The A4Cloud conceptual definition provides a general and comprehensive understanding of accountability. A structured representation of accountability based on such definitions and concepts underpins a novel accountability model, as discussed further in Section 5. This section has also discussed different accountability perspectives. This is useful in order to clarify a comprehensive understanding of accountability, particularly in the context of the project scope. Further background about prior external analysis of the concept of accountability is given in Appendix B.

This section has also discussed the notion of the account from the legal and regulatory perspective. As noted, the account will also be discussed later in Section 8 from the operational, i.e. quantitative (that is, metrics) and evidence perspectives. Of course, these three viewpoints of analysis characterising the notion of account all relate and rely upon each other. However, underpinning the notion of the account is the provision of full transparency, supported by evidence, to third parties in order to be accountable for any specific action or event in a cloud ecosystem. This enhances cloud trustworthiness. The ability to provide an account is constrained (and sometimes dictated) by legal and regularity regimes (and related mechanisms such as obligations) as well as by other technical mechanisms, e.g. security controls or privacy enhancing technologies, deployed in the cloud. As seen above, the legal and regulatory framework places emphasis on the content of the account, i.e. what needs to be included, as opposed to how the account is produced, i.e. the process of the account. Further constraints also arise from share responsibilities and resources across cloud supply chains and compiling the information to promptly obtain the necessary information and, therefore, to provide a detailed account when necessary. Finally, the account also serves to achieve the goal of full transparency, which thereby facilitates the impacted party's access to redress mechanisms via the applicable regulations and/or contractual rights. All of these considerations drive the importance and necessity of providing an account in order to support accountability throughout the cloud ecosystem.

In summary, perfection is not reachable in a complex and moving global context, but both public and private organisations are expected to think upfront about the impact and the risk they create, and privacy by design has a strong role to play in helping organisations balance innovation with the expectations of individuals. In addition, both regulators and individuals expect organisations to act as a responsible steward of the data which is provided to them, and the way in which companies need to do more to live

up to their promises and ensure responsible behaviour is considered in the following section. In particular, corporate governance plays a central role in providing accountability within an organisation, by means of the organisation identifying risks, having appropriate policies that mitigate risks, mechanisms for enforcement internally and for monitoring that these are effective within the enterprise, and for internal and external validation of this. In addition, provision of transparency can help enforce privacy obligations along the service provision chain. Although organisations can select from accountability mechanisms tools in order to meet their context, the choice of such tools needs to be justified to external parties. It would be a mistake to have this reliant upon weak certification processes. As Bennett points out (p45: Bennett, 2012), due to resource issues DPAs will need to rely upon surrogates, including private sector agents, to be agents of accountability, and it is important within this process that they are able to have a strong influence over the acceptability of different third party accountability mechanisms. This can be achieved via independent testing of practices, provision of evidence that is taken into account, including auditing against, e.g., the ISO 27001 series and associated cloud security standards. Hence we incorporate this approach into our framework (in particular in Section 8), in that we aim to integrate the evidence provided by our tools into trusted third party auditing processes against such standards. It is also important to stress that accountability should not be a replacement for certain other procedures, including privacy controls, but that it should be used to complement these (Bennett, 2012). There is the danger in particular that an accountability-based approach could be used to justify the abandonment of privacy rights and principles, which is certainly not the approach of the A4Cloud project.

In this section we have defined accountability, but as we have considered within Subsection 2.1.5, defining accountability is not sufficient to monitor and change behaviour in the cloud. This requires further operationalisation of the way accountability should be embedded in the cloud ecosystem's norms, practices and supporting mechanisms and tools. Accountability in the cloud ecosystem should be: a) defined, b) monitored, and c) corrected in order to stimulate responsible behaviour with data in the cloud. In addition, accountability not only requires this loop of defining, monitoring and correcting, but also the explanation and justification of the actions taken to define, monitor and correct accountability. An accountable organisation therefore must:

1. Demonstrate willingness and capacity to be responsible and answerable for its data practices
2. Define policies regarding their data practices
3. Monitor their data practices
4. Correct policy violations
5. Demonstrate compliance to the cloud ecosystem's norms.

This will be considered further in Section 5.

3 Cloud-Specific Factors Affecting Accountability

While the regulatory frameworks involving accountability considered in Section 2 provide a foundation for data protection, none is specifically designed with cloud computing in mind. However, the extended use of cloud services in modern IT applications raises worries for cloud customers in relation to the proper exploitation of the available data protection means to overcome the associated cloud vulnerabilities. The way that currently data are processed in the cloud remains a huge question mark for cloud customers, who are faced with or perceive a loss of governance or lack of transparency about the way their data are processed in the cloud.

Data processing in the cloud plays an important role in the data protection field, but serious concerns are raised with respect to the security and privacy of cloud computing, which make the task of effective data processing in the cloud a really challenging one from an accountability perspective. The primary concern of the cloud customers relates to the loss of governance over their data in the cloud (European Commission, 2012d). They worry about the possible uncontrolled replication or potential disclosure of their personal and/or business confidential data to third parties. This uncertainty about who is able to access their data stored in the cloud, and for what purposes, is aggravated by the complexity of cloud supply chains. This makes cloud customers feel uncomfortable about how their personal or business confidential data are being managed. The concern is exacerbated as the legal framework is complex.

Accountability across cloud supply chains is an important aspect to consider, but there are many challenges due to the complexity of these chains. This complexity is reflected in a number of different aspects, including the ramifications of failure within the chain, the business risks involved, and the complexity of liability. The nature of cloud computing itself affects the degree of support for accountability, due to a variety of issues, including the scale of cloud services, the pervasive role they will play in future business and personal life, the complexity of the supply chain as already mentioned and the ability of advanced data mining techniques to draw inferences about data subjects from the large datasets under their control. Thus, in this section, we extend the discussion already provided in Section 1 by elaborating on the emerging issues in the cloud, which relate to and serve as a motivation for accountability-based approaches towards efficient data governance in the cloud.

3.1 Risks from the Use of Cloud

Although the adoption of cloud computing accelerates the operation of business and minimises the costs, especially for SMEs, the use of the cloud environment is subject to risks. Such risks affect the quality of the security and privacy mechanisms and have a direct impact on the appropriate implementation of accountability. In principle, the use of Internet services offers grounds for increasing security breaches and emerging threats, which are expanding rapidly (Help Net Security, 2012a). A number of business domains still seek the best compromise to offer their services online, increase their market opportunities and efficiently face the needs for massive access to computational and storage resources in the cloud. But, *what about privacy and data protection in personally identifiable and confidential information?* As reported in (Help Net Security, 2012b), *IT professionals need to address the threats of data leakage and identity theft and the growing consumer and providers concerns about data privacy as well.* However, the challenge in data protection and privacy preservation goes beyond the boundaries of the IT world and lies in a cross-discipline approach, which needs to address the problem in technical, legal and socio-economic dimensions.

As a key action in the top priorities for 2013-2014, the Digital Agenda for Europe identifies the need for *a common level of preparedness at all EU member states to face cross-border cyber incidents, risk management and incident reporting requirements* (European Commission, 2012b). In the conclusions of pillar III for the Digital Agenda, it is said that the EU directives need to focus more on "*the online privacy protection, security breach notification and protection of minors*" (European Commission, 2012c). However, a great many issues need to be clarified and responsibility for cloud security is one of them (Ponemon Institute, 2013). That survey claimed that cloud end users are considered to be responsible for cloud security (although conflicting views are raised) and this is an issue that needs to be resolved with respect to the potential wider adoption of cloud technologies.

3.1.1 Concerns about the Use of Cloud and the Role of Accountability

NIST, in their SP 800-144 study (Jansen and Grance, 2011) on guidelines for security and privacy in public cloud computing that was published back in 2011, raised fundamental concerns with respect to the use of cloud in operation business. These concerns are summarised here:

- *Governance over data use and processing*: personal and business confidential data are handled, based on the purpose of use. Cloud deployment should be checked against compliance to organisational processes and other limitations, such as legal constraints.
- *Compliance to laws, regulations, standards and specifications*: cloud providers still face the problem of providing services and applications in the cloud, taking as an action the privacy preservation and data protection with respect to data location. Cloud storage capacity can span across multiple countries or even continents, which adopt non interoperable regulatory frameworks for cross-boundary communications. The complete distribution of cloud resources (including data collection, processing and management) poses a batch of concerns on how public clouds can actually assure that fundamental privacy and security issues are addressed.
- *Trust and risk assessment*: risk management is a principal process for mitigating the risks threatening the security of IT systems. With regard to the cloud, the risk landscape is multiplied, but the most important aspect is having appropriate tools for monitoring and controlling the process execution with respect to policies and service level agreements.
- *Incidence response*: security leakages can be effectively identified if the most relevant monitoring data is available for inspection and analysis. Monitoring of potential security gaps means that the appropriate detection mechanisms are in place. Within a cloud infrastructure, it is even difficult to establish monitoring, detection and incidence response mechanisms; thus appropriate transparency and exchangeability among cloud users and providers is necessary to ensure that cloud user requirements and policies are met.

Following these NIST concerns on security and privacy in public clouds, a list of recommendations have been proposed, which, amongst others, emphasise the need to *maintain accountability over the privacy and security of data and applications implemented and deployed in public cloud computing environments* (Radack, 2012). The lack of responsibility, as one element of accountability, in the cloud drives a serious lack of data protection in practice, as stated in the opinion expressed by the EDPS (2012d). As per the same opinion:

- Accountability is a cornerstone of data protection.
- Standard commercial terms and conditions have to be developed in governing the interactions of cloud customers and cloud service providers.
- There is a need for implementing best practices to explain the responsibilities of key cloud roles, such as data controller and data processor, and the data subjects' rights.
- There is also a requirement to strengthen the cloud data access criteria and notion of transfer in the regulatory framework.

Another emerging accountability issue relates to incident management, including data breach management. The European Commission and some EU DPAs are currently exploring the possibility of extending incident notification and breach reporting legislation from telecommunications providers under *Article* 13a of the Telecommunications Directive to "Information Society service providers", including cloud providers. Furthermore, an important addition to data protection law introduced by the proposed new European Data Protection Regulation (GDPR) is the introduction of significantly increased maximum sanctions for data breaches – 2% of global revenues, or even more.

These changes represent an important recognition of the need to respond accountably to information security incidents at all layers, involving all stakeholders in the process. Accountability, including a clear attribution of responsibility, is required both in order to co-ordinate detection and response of incidents and data breaches, as well as in the case of any legal or contractual liability for the consequences. At the same time, it also implies a major increase in liability for cloud providers. This increase in liability, as well as the focus on responsible incident management, raises important questions about the attribution of responsibility of incidents occurring in complex cloud computing supply chains. Many parties bear responsibility for the occurrence of incidents, as well as for response. Consider, for example, the following scenario.

A vulnerability in a major browser is exploited to capture and misuse personal information from customers of an application running in a PaaS service, which is running on top of an IaaS service (as in A4Cloud Use Case 3). The vulnerability breaks out of the browser sandbox and exploits an Operating System (OS) vulnerability to install a key-logger. In order to achieve this, it could have exploited flaws in the browser, the PaaS application and the OS. In such a scenario, it would be extremely challenging to decide who is liable for the incident, who is responsible for remediation and communication to affected customers, and so on.

The ability to provide evidence of having applied best practice, to provide timely information, which can be used to resolve the incident, and to identify and rectify root causes is crucial. This is especially true in a situation where services are delivered across interdependent supply chains, where significant liability applies to those determined to be responsible and where failure to resolve an incident can result in serious damages both to customers and to provider reputation. The elements of accountability, such as clear attribution of responsibility, liability, verifiability and other relevant features are all keys to effective incident management in such scenarios.

3.1.2 Risks in Data Governance in the Cloud

Following the growing use of cloud computing, complex service development and delivery supply chains are being built to facilitate the evolving development of different business models, which arise from the broad adoption of cloud services. However, at the same time, the mass use of cloud services has allowed cybercriminals to use reputable services to bypass many of the digital defences erected by companies (GTISC/GTRI, 2013). Thus, cloud data governance and management become highly challenging in order to overcome the problems, which set barriers to the wider adoption of cloud ecosystems. Such problems may relate to various cloud specific features, such as cloud vulnerabilities, and, in principle, they have a direct impact on building proper data governance policies for accountable approaches in the provision of cloud services. Cloud vulnerabilities are varied and are categorised in material including (Catteddu & Hogben, 2009). Table 1 highlights some cloud features and associated potential issues, many of which are at the governance level.

Table 1 Cloud Features and Key Related Issues

Cloud features	Key related issues
Multi-tenancy	Data of co-tenants may be revealed in investigations, isolation failure, proper deletion of data and virtual storage devices
Complex, dynamically changing environment; data flows tend to be global and dynamic	Ensuring appropriate data protection, overlapping responsibilities in data management, unauthorised secondary usage, vendor demise, lack of transparency
Data duplication and proliferation; Difficult to know geographic location and which specific servers or storage devices will be used	Exacerbation of trans-border data flow compliance issues, detecting and determining who is at fault if privacy breaches occur
Easy and enhanced data access from multiple locations	Data access from remote geographic locations subject to different legislative regimes, subpoenas, access by foreign governments, 'idiot with a credit card'

Data duplication and proliferation (and its autonomic aspect) creates problems in terms of compliance: Amazon, for example, creates up to three copies in different data centres when storing data. In addition, public cloud providers make it very easy to open an account and begin using cloud services, and that ease of use creates the risk that individuals in an enterprise will use cloud services on their own initiative, without due consideration of the risks and governance process. There are also fears about increased access to data by foreign governments and other parties. Other issues include data lifecycle management across chains of suppliers, including data discovery and destruction, and legal risks that include security obligations, international transfers and the processing of sensitive data. For example, difficulties exist if users want to end a service, get their data deleted or export their data to another

provider. Often, it is unclear who the data controller is and which parties have what responsibilities. More detailed analysis is given for example in (CSA, 2012; Pearson, 2012). In particular, loss of control and transparency (in the sense of insufficient information, thus making the task more difficult of selecting a suitable service from the vast choice of cloud offerings) are highlighted as key issues by the Article 29 Working Party (European DG of Justice, 2012). As a result, the involved cloud players, ranging from cloud service providers to cloud end users (i.e. people placing personal data in the public and/or private clouds) are often sceptical about the cloud environment due to a justifiable set of worries. Indeed, without knowing what security level can be actually guaranteed, it becomes difficult to plan for the potential risks involved and as such an evolving defensive behaviour is observed against the cloud adoption, which has a long-term, strong negative impact with respect to how the economy is growing and the way in which legacy applications can migrate to more stable and scalable IT environments.

In a nutshell, cloud adoption is currently restricted by its own intrinsic versatility. In (IDC, 2012), uncertainty over the legal jurisdiction and location of one's data in the cloud is considered as one of the main barriers for cloud adoption, while concerns are strongly expressed about how the trustworthiness of cloud suppliers in building chains of cloud service providers can be assessed without taking for granted any security guarantees. Of primary importance is the fact that critical privacy concerns are raised and they have to do not only with the actual storage of both personal and confidential data in the cloud, but also with the doubts on the processing part of this data in order to provide added-value cloud services (Rodriques, 2012). When such processes are delegated to third parties in complex cloud service ecosystems, the derived outcome should be analysed from a profit and loss perspective, meaning that the technological, legal and socio-economic dimensions of the problem should offer the weighting factor over the potential risks and the associated mitigation strategies.

3.2 Difficulty in Building Chains of Accountability across Complex Cloud Service Ecosystems

Cloud deployments face two main barriers that have a direct impact on the adoption of cloud services for data-intensive business contexts: the uncertainty of the regulatory regimes regarding the processing of personal and/or confidential data, and the perception of emerging security threats (CSA, 2013; ENISA, 2009) in cloud service provisioning chains, which result in lowering the cloud customer's trust on cloud computing. As explained in Section 3.1.1, the main concerns for prospective adopters of cloud services are loss of data control, compliance with laws and regulations, gaps in standards and specifications, the lack of simple mechanisms to assess the trustworthiness of potential partners and the effective implementation of incident response mechanisms (Felici, Koulouris, Pearson, 2013).

Lack of customer trust and regulatory complexity in global business environments are difficult issues to tackle, because of the underlying complexity across multiple dimensions and the interdisciplinary nature of the problem. For example, location matters from a legal point of view but processing flows are dynamic, global and fragmented: there are restrictions about how information can be sent and accessed across boundaries, but in cloud computing data can flow along chains of service providers both horizontally between SaaS providers and vertically, down to infrastructure providers, where the information can be fragmented and duplicated across databases, files and servers in different jurisdictions. All enterprises operate a security lifecycle something like the following: assess risk associated with IT; shape investment, controls and policy choices; applications and technical procurement; work hard to configure and patch the infrastructure environment; monitor events to catch incidents and support forensics; carry out audits to see if the controls are mitigating risks. Organisations struggle to operate this cycle effectively because: technology is always changing; threats and attacks evolve faster; the cycle consists of many silos of stakeholders that have very different perspectives and expertise and do not speak the same language. For example, legal or human resources employees involved in people policies are very different from a network security expert configuring firewalls. With cloud this situation is going to get even worse, not just because there are new architectures but because the supply chain of services breaks up the activities of the security lifecycle even further (as shown in Figure 10, in which an additional fourth ring labelled software could if desired be added). The complexity of the service provision chain results in a lack of visibility and transparency within the service supply chain and a subsequent lack of trust in data protection practices in the cloud. As the number of involved stakeholders grows, the probability of the providers involved in the service chain failing to implement and guarantee appropriate data protection controls increases and critical privacy concerns are raised

regarding the storage and processing (i.e. operations on data) of confidential or personal data in the cloud, any of which may be allocated to third parties.

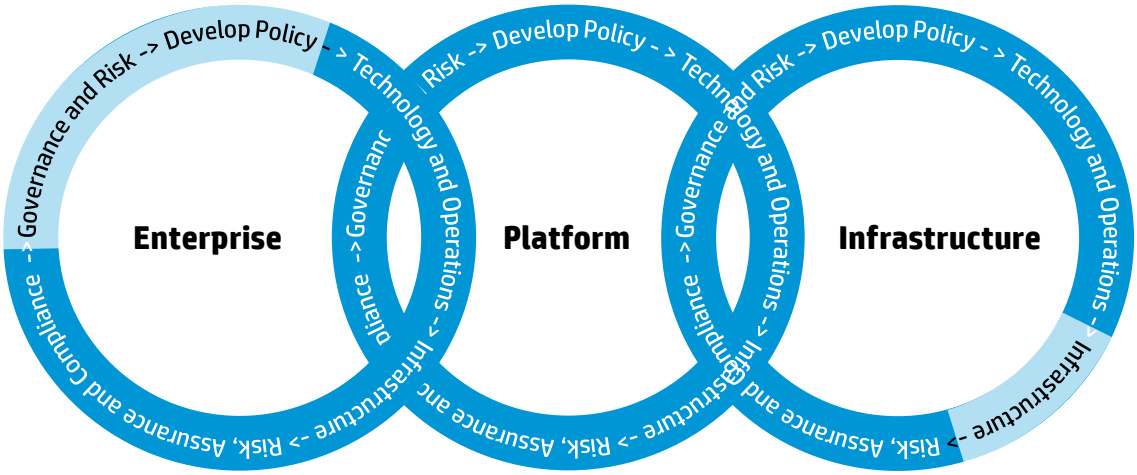


Figure 10 Need for Accountability and Transparency in the Cloud Service Provision Chain

For instance, if the enterprise buys CRM from a SaaS provider that in turn uses an AWS for IaaS, then the people judging risks and forming policy now have to rely on and influence the investment and monitoring choices of the SaaS provider, and are also dependent on the configuration and infrastructure purchases of the IaaS. Hence there is a need for data stewardship and accountability along the service provision chain. The 'data-centric' nature of cloud computing creates a tension between service suppliers who perceive that the data that they hold could be a strategic business resource and their customers who are increasingly aware of risks posed by the perceived lack of control over data in the cloud. The actual level of control can be very variable – for example, IaaS relationships tend to confer a high level of control, SaaS relationships potentially less so.

3.2.1 Ramifications of Failure along the Cloud Provider Chain

Within a cloud ecosystem, issues from one cloud provider may have ramifications further up the chain, for example in terms of loss of governance. This is illustrated in Figure 11.

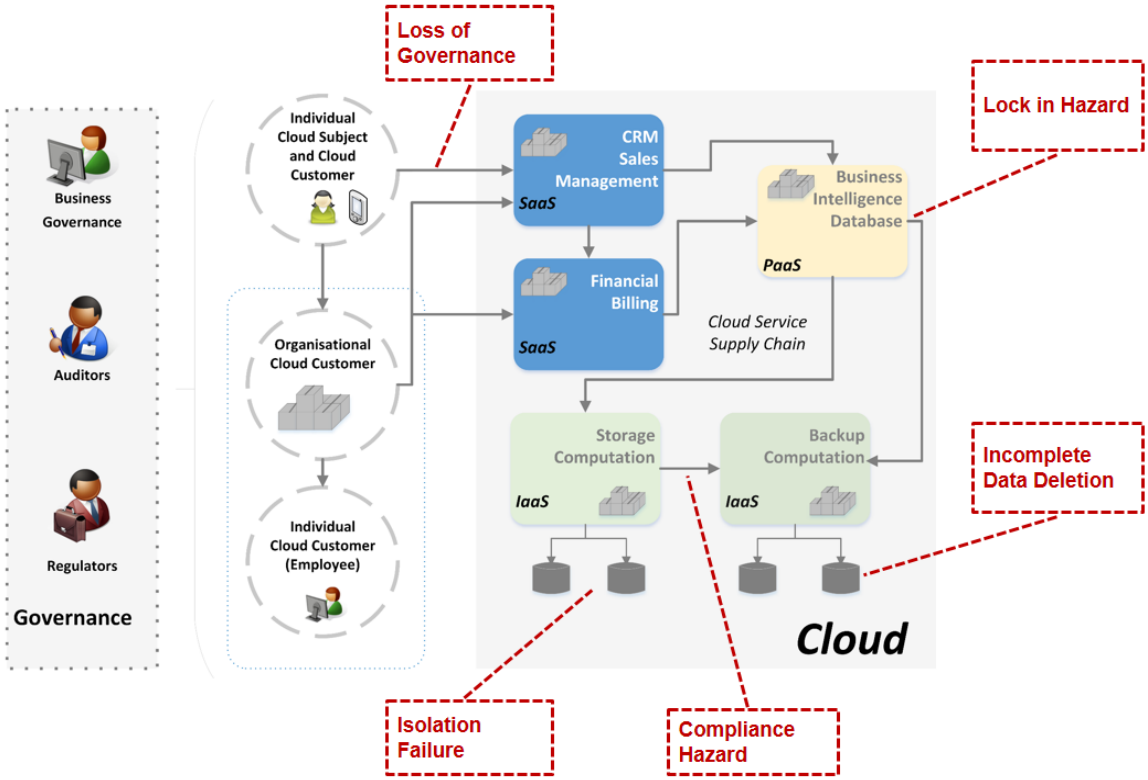


Figure 11 Ramifications of Cloud Failures

Loss of governance may arise in cloud computing for example as the client cedes control to the cloud provider, but SLAs may not offer commitment to provide such services on the part of the cloud provider, thus giving a gap in security. There are many ways in which there can be data loss or leakage involving IaaS, PaaS and SaaS providers: for example, unauthorised parties might gain access to sensitive data due to insufficient authentication and authorisation controls, or data might be stored in servers in India without appropriate governance mechanisms in place, causing a compliance hazard (for other examples see for instance (CSA, 2012)). Security and privacy threats of data breaches are the most severe types for cloud computing (CSA, 2013). Unfortunately, some of the measures (e.g. data encryption) that can address data breaches may exacerbate data loss (e.g. if the encryption key is lost all encrypted data will be lost too). Data can be exposed to different types of security and privacy concern, and these include internal cloud facing security issues such as security attacks exploiting vulnerabilities of virtualisation mechanisms and monitoring virtualised environments giving information about data usage by neighbouring users. Data breaches need to be addressed within specific provisions of service level agreements (SLAs) that clarify the respective commitments of the cloud provider and the client, as considered further in the following sections. Unfortunately, an analysis of cloud failures has identified further threats (i.e. hardware failure, natural disaster, service closure, cloud-related malware and inadequate infrastructure planning) specific to cloud computing (Ko, Lee, Rajan, 2012).

3.2.2 Lack of Transparency and Verifiability by cloud providers

The relative lack of transparency and verifiability by cloud service providers is a big issue, especially in relation to PaaS and IaaS providers. This is a potential show stopper for accountability-based approaches, in the sense that decisions made about stored locations, usage, sharing, duplication and sharing of information, etc. do have implications both with respect to risk of harms to the data subject and various forms of data exposure, as well as implications in terms of policy violations along the cloud service provision chain.

Given the global structure and shared environment nature of cloud services it is not feasible to allow customers to audit the service provider individually and subcontractors will have the same constraints. Making third party audit reports available to the customer is a viable alternative. The recent Dutch Central Bank case shows that service providers may need to permit customer audit in certain sectors if

they want to win business in that sector. In this case, Microsoft agreed to allow the bank to audit their facilities in order to meet the requirements of the local financial services regulator. This enhanced audit needs to be not only made available, but done in such a way that the verifiability is trustable, as discussed above in Section 2.

3.2.3 Complexity of Liability in Service Provision Ecosystems

An important issue in the cloud context is how cloud customers and end users can practically obtain redress in case of failure. One approach would be that through contractual agreements, all organisations involved in service provision could be made accountable to some person, by means of legally enforceable contractual obligations. Under data protection law, the primary user (for example: a corporate cloud user or government department) as the first entity in the cloud provision would be held legally accountable as a data controller. To manage this accountability obligation, the primary user would then hold the initial service provider accountable through contractual agreements, requiring in turn that it hold its SPs accountable contractually as well. In an accountability system of this kind, the transferor remains accountable to its regulators, even if it is the transferee whose actions cause a breach of the regulation (Pearson & Charlesworth, 2009).

However, this notion of legal accountability in the sense of formal obligations owed to another person is increasingly seen as too simplistic. There are a wide range of people who might have a legitimate claim that a service provider or data user should be accountable to them, but only a few of those people will be owed an obligation to account which is legally enforceable. Thus the modern conception of accountability recognises two related forms of accountability: compliance with legally binding obligations to account; and accountability to others through transparency. Transparency requires the disclosure of all the information which is necessary for those to whom account must be given to determine if the discloser is acting properly. It confers on those persons, at least in theory, *"the ability to know what an actor is doing and the ability to make that actor do something else"* (Hale 2008, 75). This more nuanced conception of accountability necessarily focuses attention on the persons to whom account must be given. Each has different interests which accountability aims to protect, and thus each group is owed different obligations. To take an example from data protection, the accountability obligations which a data controller owes to its data protection regulator are not the same as the obligations it owes to its commercial customers, and nor do these obligations derive from the same source. As a consequence, accountability is a complex, dynamic and dialectic activity, not a set of fixed obligations. There is no 'perfect' accountability solution, but rather an evolving process of improving accountability. Black points out that (Black 2008, 157):

> *"Actions that organisations may need to take to render them legitimate for one legitimacy community can be in direct opposition to those they need to adopt to satisfy another. Moreover, attempts to render them accountable may face an 'accountability trilemma:' they are ignored, co-opted, or destroy that which it is they seek to make accountable."*

3.3 Other Cloud Specific Issues Affecting Accountability

The established regulations set limitations and constraints in the further adoption of the cloud, since plenty of relevant issues are difficult to be accommodated within the currently configured cloud services. Such constraints may have an impact on the future accountability mechanisms for the cloud and are analysed in this section. The development of complex cloud service provision chains is, then, subject to the limitations of the legal framework and the inherit inability and/or unwillingness of the providers to faithfully support their security and privacy mechanisms. The adoption of an accountability based approach for efficient data governance in the cloud has to seriously consider these legal issues and propose pragmatic solutions to lower the legal barriers and encourage the proliferation on the use of cloud services.

3.3.1 Subcontracting of Services to Third Parties

EU regulators and new EU regulation require customer consent to all subcontractors (affiliates or third parties) processing personal data. Generic consent is permissible but the customer must be informed about the subcontractors and have the option to terminate if it objects. In complex subcontracting chains

it would be extremely difficult for cloud providers to manage the notification process with all customers. Flow down of terms to the subcontractors is also challenging, not because of the way the cloud services are set up, but because very few service providers will have the resources and expertise in their contract management department to do this effectively. Organisations' global procurement departments typically work on the basis of standard terms and have little meaningful engagement with the business units or reference to the contract terms actually signed with customers. If a customer contracts on non-standard terms this needs appropriate management to ensure compliance. The use of a digital portal for customers would be an effective way to manage notice of subcontractors to customers. Investment in contracts management is required to ensure appropriate contract management with non-affiliate subcontractors. Binding Corporate Rules (BCR) for processors is an effective way to manage internal subcontracting if a service provider has the time, resources and internal mechanisms to both apply for regulatory approval and then ensure compliance with BCRs.

3.3.2 Negotiation of Cloud Contracts

With respect to legal responsibilities, it is an issue that the majority of cloud agreements offered are in standard form contracts and users have very little power and influence over the terms of the contract and thus cannot ensure obligations within the legislation are being effectively enforced through the service chain. The lack of balance in negotiating power between the parties in cloud computing agreements and the implications it leads to for the protection of personal information, have been stressed within the stricter area of European data protection. The European Data Protection Supervisor (EDPS) in his Opinion issued on Cloud Computing (EDPS, 2012c) points out the stake involved, especially, for Small and Medium Enterprises (SMEs) by stating in this respect that: "*While governments and big companies may have the possibility to have private clouds established according to their requirements or to negotiate the service agreements with cloud providers at equal level, small and medium organisations from the public and private sectors and individual consumers will have to accept the terms and conditions as they are laid down by the service providers for public cloud services. This asymmetry could be exploited by service providers to set conditions for their services which are to the disadvantage of the clients by limiting providers' obligations and liability and restricting clients' rights, giving providers far reaching privileges and powers, even to unilaterally change terms and conditions of service to the disadvantage of the cloud client.*" Interestingly, the EDPS comments on the lack of power to negotiate security measures, in case of IaaS solutions by stating that the cloud client "*may not be in a position to negotiate security measures of the cloud service provider (…) In addition, the relationship between provider and client may not involve any direct negotiation and may amount to a simple registration process.*" (EDPS, 2012c). Note that a solution proposed to this asymmetry is the development and use of standard contractual terms and conditions, a detailed discussion of which falls outside the scope of the present section (EDPS, 2012c). However, cloud customers need to ensure that the cloud computing solution they select satisfies their organisational security and privacy requirements. In cloud computing, it is normally the case that non-negotiable service agreements are offered in which the terms of service are prescribed completely by the cloud provider, so the emphasis is on the cloud customer to just choose a suitable provider, or choose not to employ cloud services at all. However, negotiated service agreements are also possible in some cases. The circumstances in which this is most likely to be the case are shown in Figure 12 from (Catteddu & Hogben, 2009), in which the three main possibilities in terms of negotiating contracts and agreements between the customer and the cloud provider are summarised.

CLOUD PROVIDER	CUSTOMER
A) Large company – **strong ability to negotiate contract clauses**	SME – **Weak or lacking ability to negotiate contract clauses**
B) Both the customer and the provider have the **ability to negotiate contract clauses**	
C) SME – **Weak ability to negotiate contract clauses**	Large company or public administration - **may negotiate contract clauses**

Depending on the particular case (whether it is A, B or C), the way to tackle the issues identified in *subsection* I may differ significantly.

Figure 12 Negotiation of Cloud Contracts (Catteddu & Hogben, 2009)

In addition, negotiation is more likely to be needed where critical data and applications are involved, and where an agency might be used to negotiate a service level agreement in order for an organisation to use a public cloud. However, the process of negotiation will negatively affect economies of scale and may well not be feasible (for example, it may not be possible for an infrastructure provider to offer customised services to different consumers).

In a similar way to traditional information technology outsourcing contracts used by agencies, negotiated agreements can address an organisation's concerns about security and privacy details, such as the vetting of employees, data ownership and exit rights, breach notification, isolation of tenant applications, data encryption and segregation, tracking and reporting service effectiveness, compliance with laws and regulations and the use of validated products meeting federal or national standards. A negotiated agreement can also document assurances that the cloud provider must provide as evidence that certain requirements are being met (Jansen & Grance, 2011).

3.3.3 Growing Usage of Integrators

Since negotiated contracts are rare at least numerically, in cloud transactions there has been a growing trend especially by SMEs (although they are also used by larger organisations) in the use of integrators. *Integrators* are entities which contract with both end users and providers; essentially, they are very large users of IaaS and PaaS services, which they use to provide cloud services (mostly SaaS) to end users. Integrators play an important role in negotiated contracts as they can be seen to be in a better position to negotiate contract terms than end users, mainly due to existing relationships with cloud service providers and also integrators can have stronger bargaining positions since they may use the same provider to service many end users.

Since most cloud service agreements are in standard form, to ensure accountability is being imposed down the service chain, integrators can provide more contractual assurances than service providers, for example with respect to liability caps, support and security measures. It is important to note that such increased acceptance to negotiate terms and provide assurances has its limitations; the integrator is essentially taking a risk unless it knows it can negotiate similar terms from the service provider. For this reason some integrators are investing in infrastructure, which will give them more control and increase their ability to better meet specific customer/user needs.

Integrators that are willing to accept more risk are increasingly entering the market, seeing the opportunity to sell more robust, enterprise-grade services, with contract terms to match rather than the "as is, where is" services agreements which are offered by the majority of cloud service providers. In order to remain competitive, providers may have to be more aware of user concerns, more flexible in negotiations, and more willing to demonstrate the security of their services and ensure accountability obligations and assurances, which the user requires, are represented in agreements. Hence, we recommend that integrators should be taken account on in the taxonomy. They would come under the role of being a type of cloud broker.

3.3.4 Guaranteed Security Levels

Cloud providers may be constrained by the levels of security they can offer for different types of cloud. It may be difficult for a service provider to determine if the level offered is appropriate if it does not know what type of data may be stored in the cloud by the customer. Security levels will need to be enhanced to win business in certain industry sectors (e.g. financial services and health). Notification of modifications/enhancements to security levels during the term of the contract would be a very valuable accountability tool. Again, a digital portal may be the customer notification mechanism for this. Other potential business constraints relate to, for example, operational changes, back up and disaster recovery and service evolution and upgrade.

3.3.5 Data Transfers

Data transfers are more complex in cloud computing but the fundamental compliance issues remain the same for customers. Traditional compliance tools available to customers (e.g. model contracts) do not "fit" well in the dynamic world of cloud. Service providers need to adopt overarching compliance models involving either (i) the adaptation of model contracts into a workable contractual framework with internal and external subcontractors and/or (ii) apply for BCR for processors (to cover internal transfers) and ensure appropriate subcontracting terms with third party subcontractors. Customers need to know where their data is located. Again, it will be very difficult for service providers to meet this requirement particularly if service locations change during the term of the contract. A digital portal for customers could again be an effective way to manage notice to customers. "Sticky data" technologies may assist in populating a portal or otherwise be a means of data tracking for customers.

3.3.6 Type of License for Cloud Services

One of the most obvious distinctions to develop in cloud services is between services for which the customer pays a subscription or usage fee and those, which are, at least at first sight, provided free. Moreover, a number of Cloud providers offer both "free" and paid versions of products, which may differ only slightly. Free services include, for instance, email storage such as Gmail; Dropbox and also social networking sites such as Facebook, Pinterest, and many others. Paid services, for instance, such as Amazon Cloud and Sales Force, are generally aimed at commercial users. However, cheaper entry-level services are being offered to consumers. In view of one of the central attributes of cloud computing, namely the elasticity of resources, it is in principle just as easy for a provider to sell a time unit on a single processing or storage instance as it is to sell that instance as an incremental resource increase to a large existing customer. In relation to accountability, although the obligations imposed on the actors are the same with both free and paid cloud services, how these obligations are attributed and enforced depends on the negotiating power between the user and provider. Only in limited scenarios where the user is paying for a cloud service of very high value can it negotiate the agreement with the provider: examples include large financial institutions and government entities. Cloud services provided on an at least notionally free or low- cost, flat-rate basis are usually non-negotiable 'take it or leave it' agreements. (For further details see MS:B-5.3).

3.4 Summary

The problems presented by cloud service provision ecosystems, and how they may be addressed by an accountability approach, have been considered in this section; these include multi-tenancy, the dynamic, ever changing environment, data duplication, and easy access to data from multiple locations. This extends the related discussions already given in Section 1. Key points are that in the cloud context, the cloud client/controller may not be solely able to determine the purposes and the means of processing because the cloud service provider designs the infrastructure and also to some extent the services, in a way that depends upon the cloud model (namely, IaaS, PaaS or SaaS), as well as typically elaborating standard SLAs with little or no customisation possibility. In addition, lack of transparency and verifiability, especially at the PaaS and IaaS levels, is a major problem that needs to be addressed, and without which accountability-based approaches in the cloud just may not work. Finally, the complexity of the environment is a major challenge for solutions and indeed it still needs to be demonstrated that an accountability-based approach can really add value in a practical sense in this domain without adding to the complexity, although indeed it is the goal of the project's approach to help cut through the

complexity. This is discussed further in Section 6. In the next section we move on to consider in more detail accountability in cloud service provision ecosystems.

4 Accountability in Cloud Service Provision Ecosystems

This section takes into account cloud service provision ecosystems and provides an accountability analysis of some scenarios involving different cloud actors. As we shall consider further below, security and privacy requirements will vary widely from one scenario to the next, and be heavily dependent upon risks and responsibilities of actors in those scenarios, which again depend upon a combination of the service and deployment models used. Cloud computing creates new dynamics in that there is an additional role of cloud provider, and indeed there could be several such parties. Top barriers in providing cloud computing services include lack of customer trust and regulatory complexity in global business environments: cloud customers want data processors to respect their obligations and policies and be compliant (especially as they may be legally liable), but these are difficult issues to tackle, because of the underlying complexity across multiple dimensions and the interdisciplinary nature of the problem. For example, data location matters from a legal point of view and there are restrictions about how information can be sent and accessed across boundaries, but in cloud computing data can flow along chains of service providers both horizontally between SaaS providers and vertically, down to infrastructure providers, where the information can be fragmented and duplicated across databases in different jurisdictions. The remainder of this section provides an analysis of roles and responsibilities in various scenarios, in order to allow further analysis about accountability relationships in different cloud service provision ecosystems. This section describes the cloud service accountability ecosystem through the following components: Accountability Roles, Accountability Relationships and Accountability Graphs, which are graphs using roles as vertices and interactions as edges.

4.1 Cloud Computing Roles

This section discusses cloud actor roles. In particular, it takes into account cloud computing roles drawn from the NIST Cloud Computing Reference Architecture (Liu et al., 2011). It extends these roles in order to cover those situations in which individuals are indirectly involved in cloud ecosystems (that is, not directly using cloud services). We extend these roles and clarify their definitions in order to consistently describe cloud ecosystems. The A4Cloud project is extending the NIST taxonomy (Hogan, 2011) by accountability. That is, accountability (and its main elements or means to achieve accountability) will be considered as a principal conceptual viewpoint in order to analyse relationships among different roles in cloud ecosystems. This will result in extending and detailing the NIST taxonomy by accountability and actors (associated with specific roles) identified in cloud ecosystems.

4.1.1 NIST Cloud Roles and their Limited Applicability for Accountability

The NIST Cloud Computing Reference Architecture identifies the main roles in cloud computing (Liu et al., 2011), as:

- Cloud Consumer: "*Person or organisation that maintains a business relationship with, and uses service from, Cloud Service Providers"*
- Cloud Provider: "*Person, organisation, or entity responsible for making a service available to cloud consumer"*
- Cloud Carrier: "*The intermediary that provides connectivity and transport of cloud services between Cloud Providers and Cloud Consumers"*
- Cloud Broker: "*An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers"*
- Cloud Auditor: "*A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation".*

The roles defined by NIST are part of a cloud taxonomy, which consists of four different levels of abstraction (Liu et al., 2011): Level 1 Role, *"which indicates a set of obligations and behaviours as conceptualised by the associated actors in the context of cloud computing";* Level 2 Activity: *"which entails the general behaviours or tasks associated to a specific role";* Level 3 Component: *"which refer to the specific processes, actions, or tasks that must be performed to meet the objective of a specific activity"*; Level 4 Sub-component: *"which present a modular part of a component".* The four-level taxonomy identifies the main concepts underpinning the NIST Reference Architecture for cloud computing (Liu et al., 2011). Appendix C provides further information about cloud computing.

Taxonomies may be used to structure in a systematic manner the analysis of interactions and responsibilities among cloud actors in order to identify contingencies (CSA, 2011). They allow us to describe cloud ecosystems and to map actors to specific roles and responsibilities. Identifying roles and responsibilities in cloud ecosystems allows us to analyse relationships and dependencies between cloud services (and software) in order to understand emerging threats, e.g. data breaches and data loss (CSA, 2011). The roles defined by NIST have some limitations when dealing with accountability, in particular when it comes to data protection. Some essential actors in an accountability framework are not well characterised by the roles in the NIST model:

- **Data "owners"**: Individuals, in particular data subjects, or organisations who have some personal or confidential data processed in the cloud, and who may not necessarily be qualified as 'cloud customers' (or consumers) in the NIST taxonomy. Though more rarely, this also applies to businesses, which may have business confidential data processed by the cloud despite not being a cloud customer (rather customers of a cloud customer). They are essentially "invisible" in the NIST model, but represent the ultimate role in an accountability chain.
- **Supervisory authorities**: Data protection authorities or telecom regulators may be seen as auditors, but they also have the distinct characteristic of holding enforcement powers, which auditors lack.

Next, we extend the NIST model in order to address these issues and support accountability.

4.1.2 Extending the NIST Model for Accountability

We propose the following seven cloud accountability roles:

1. **Cloud Subject:** An entity whose data is processed[67] by a cloud provider, either directly or indirectly. When necessary we may further distinguish:
    a. **Individual Cloud Subject**, when the entity refers to a person
    b. **Organisation Cloud Subject**, when the entity refers to an organisation
2. **Cloud Customer:** An entity *that (1) maintains a business relationship with, and (2) uses services from a Cloud Provider*. When necessary we may further distinguish:
    a. **Individual Cloud Customer**, when the entity refers to a person
    b. **Organisation Cloud Customer**, when the entity refers to an organisation
3. **Cloud Provider:** An entity responsible for making a [cloud] service available to Cloud Customers
4. **Cloud Carrier:** The intermediary entity that provides connectivity and transport of cloud services between Cloud Providers and Cloud Customers
5. **Cloud Broker:** An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Customers
6. **Cloud Auditor:** "An entity that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation, with regards to a set of requirements, which may include security, data protection, information system management, regulations and ethics
7. **Cloud Supervisory Authority:** An entity that oversees and enforces the application of a set of rules.

These roles both share similarities and articulate differences with the cloud computing roles provided in the NIST model (Liu et al., 2011):

- We create a new role of Cloud Subject, which designates the entity that owns data, which is either directly transferred to a cloud provider for processing, or indirectly through a cloud customer. We further distinguish Cloud Subjects as individuals or organisations.
- The role of Cloud Customer is taken from the definition of the NIST (as a synonym of Cloud Consumer) but we further introduce a distinction between individual Cloud Customers or organisation Cloud Customers.

[67] Where processed means "*any operation or set of operations which is performed upon data*", "*such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*". (Inspired from article 2 of Directive 95/46).

- The roles of Cloud Provider and Cloud Broker are directly taken without modification from the definition provided by NIST.
- The role of Cloud Auditor is based on the definition provided by NIST but was altered in order to cover a scope in line with the goals of accountability with references to data protection and regulatory/ethical requirements.

We note that the role of Cloud Carrier defined by NIST is unlikely to be considered in the context of accountability, since a Cloud Carrier does not normally take any responsibility for data stewardship but merely acts as a neutral transporter (much like an ISP). In the case where a Cloud Carrier takes a stronger role in terms of data stewardship we may consider it as a Cloud Provider instead without loss of generality. Figure 13 lists the identified cloud computing roles.

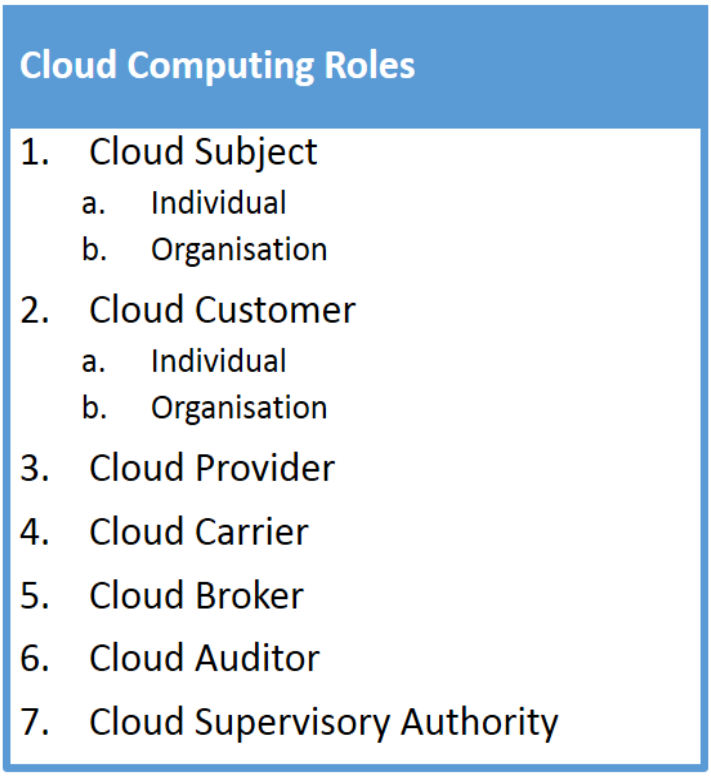


Figure 13 Cloud Computing Roles

As often the case with the definition of roles, a single actor (or entity) may have more than one role. For example:

- An actor may act both as a Cloud Provider and a Cloud Customer, providing a cloud service to customers and also using cloud services from another provider (e.g. a PaaS built upon a IaaS).
- Cloud Subjects are not always Cloud Customers. For example, a company “AcmeCorp” may collect data about individual Cloud Subjects and process them with a company “CloudPlus”, which is a cloud provider. These individual Cloud Subjects will have no business relationship with company “CloudPlus” and therefore do not meet the definition of a cloud customer but they still play a role in the accountability network.
- A Cloud Supervisory Authority may sometimes fit the definition of a Cloud Auditor when it conducts on-site inspections to verify compliance, or when it evaluates a privacy impact assessment provided by a provider in the context of Data Protection.

4.2 Cloud Accountability Scenarios

In the following paragraphs we describe four generic accountability scenarios. These scenarios are aimed to illustrate the diversity or accountability scenarios that bind together cloud subjects and cloud supply chains, with the potential intervention of other parties such as regulators or auditors.

The NIST model allows an infinite combination of cloud providers, customers and brokers. For the sake of simplicity, in order not to overload the generic accountability scenarios we describe in the following paragraphs, we will focus on the most basic supply chains (Figure 14).

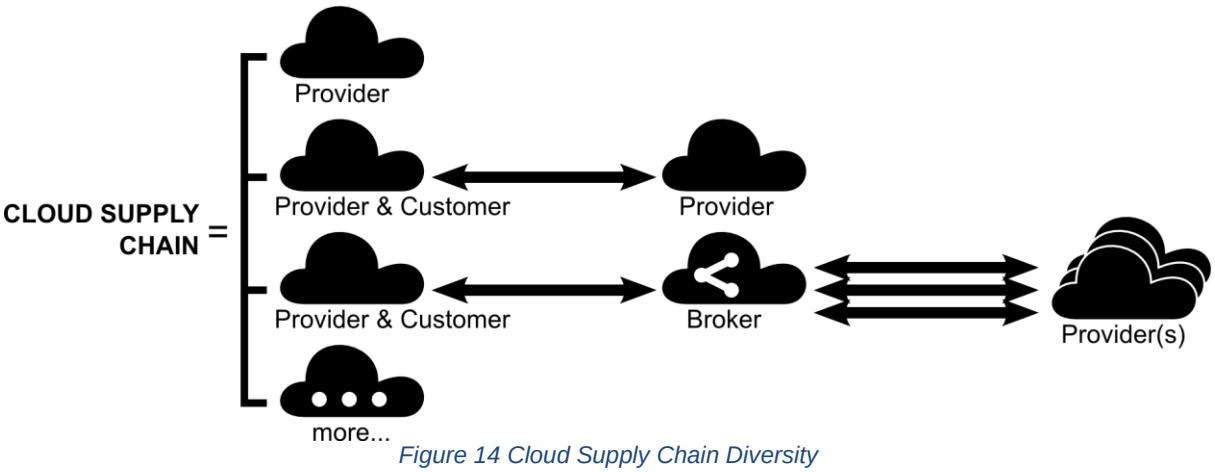


Figure 14 Cloud Supply Chain Diversity

In practice however, it should be clear that what we describe as the "cloud provider" entity in the following paragraphs may in fact represent several entities forming various possible supply chains as illustrated above, such as:

- A simple cloud provider (e.g. Amazon AWS).
- A cloud provider, acting as a cloud customer to another provider (e.g. DropBox using Amazon as IaaS).
- A cloud provider, acting as a cloud customer to a cloud broker, which itself interfaces with one or more cloud providers.
- A cloud broker, acting as a front-end to a pool of cloud providers (not shown above).
- Variations of the above.

Additionally, it should be noted that the scenarios below might be subject to further variations that are domain specific or technology specific. For example, in the data protection domain cloud auditors may never interact with data subjects (cloud subjects). The data protection domain might also involve additional actors such as "third parties" (see 4.3) who collect data on behalf on the data subject, and do not appear in the generic scenarios we describe below.

4.2.1 Scenario 1: Individuals using a Cloud Service

In this scenario, applications run on the cloud and are accessed by individuals, cloud subjects who have no idea how the underlying architecture works (which has implications in terms of transparency and what is appropriate in this case). This type of model would apply for email for example (e.g. Gmail, Facebook and LinkedIn), and thus would encompass persons communicating with each other via the cloud. Here, the Cloud entity is mainly accountable to the individual (Figure 15). In terms of roles, the individual is an **Individual Cloud Subject** and most frequently also an **Individual Cloud Customer**.

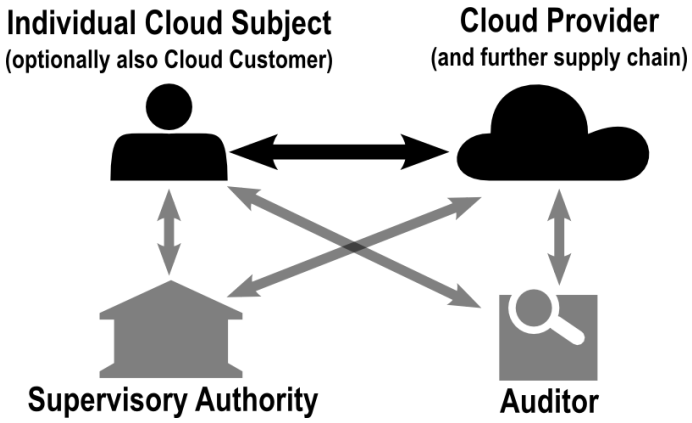


Figure 15 Individual to Cloud Supply Chain

The cloud supply chain can be simply a single cloud provider as illustrated in Figure 15, or a more complex chain mixing customer, broker and provider roles as discussed above – **Example:** A person using Google Drive to store personal documents and pictures.[68]

4.2.2 Scenario 2: Traditional Enterprise Moving to the Cloud

In this scenario, the person does not directly deal with a cloud provider, but with a traditional enterprise acting as a cloud customer, which itself uses some cloud provider. In some cases, the individual cloud subject may not even be aware that this enterprise is using a cloud service as a backend for some or all data processing (Figure 16).

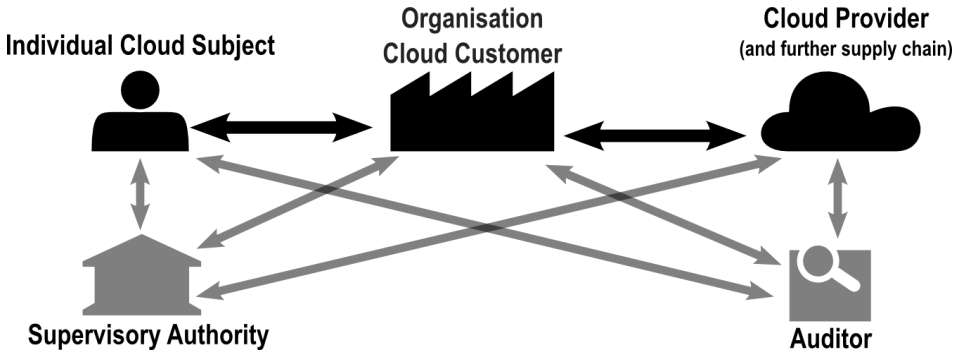


Figure 16 Individual to Cloud Supply Chain, through Cloud Customer

Here, the Enterprise is accountable to the Individual Cloud Subject, and the Cloud supply chain is accountable to the Cloud Customer (enterprise) – **Example:** This type of model would apply for example for a hospital storing health data in a secure cloud. Patients are Cloud Subjects in this case but not Cloud Customers.

4.2.3 Scenario 3: Organisation Storing Confidential Data in the Cloud

This scenario is the transposition of scenario 1 in the case where we are dealing with organisations as cloud subjects. This is the case for example when a business decides to use the cloud to process business confidential data. The Organisation Cloud Subject is also a Organisation Cloud Customer in this case, since it seems unlikely that an organisation would provide data to a cloud provider without defining a business relationship with the said provider. Here the Cloud supply chain is mainly accountable to the Cloud Customer (Figure 17) – **Example**: An enterprise uses Google Apps to elaborate its new marketing plan.

[68] Note however that regulators and auditors may have a direct link, both in Figure 15 and in Figure 16, as ultimately auditors should be supervised or certified by regulators – see the discussions in Section 2 about trustworthiness, verifiability and democratic accountability.

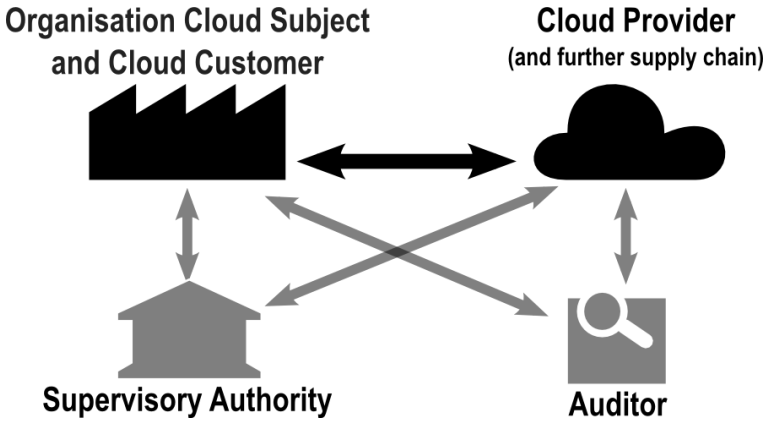


Figure 17 Organisation provides Data to Cloud Supply Chain

4.2.4 Scenario 4: Using a Broker

This scenario further complicates the previous one by involving a cloud broker. The Cloud Customer does not deal directly with a cloud provider but uses a cloud broker instead which acts as an intermediate between the customer and several provider in order to negotiate the best offering (Figure 18).

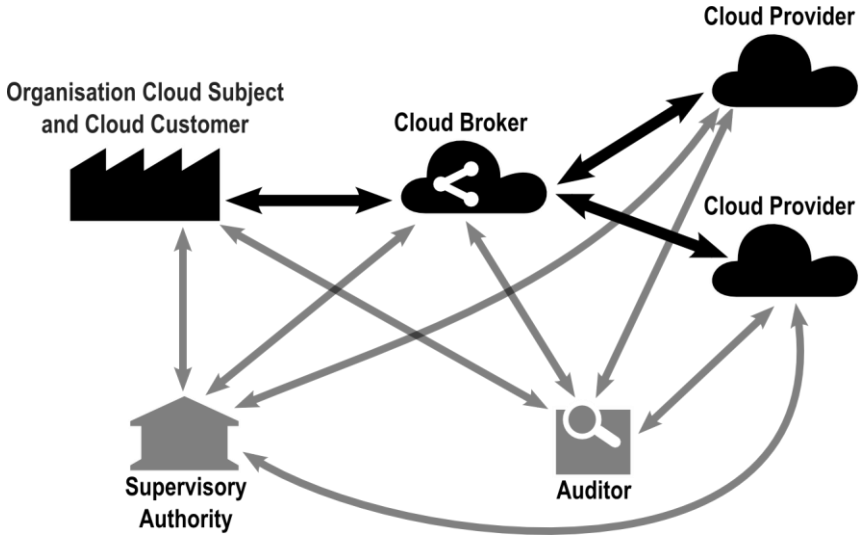


Figure 18 Using a Broker

As we did in scenario 2, we can also have situations where the Cloud Customer and the Cloud Subject are distinct entities. For example if an organisation collects data form individual cloud subjects, we may have the following variation presented in Figure 19.

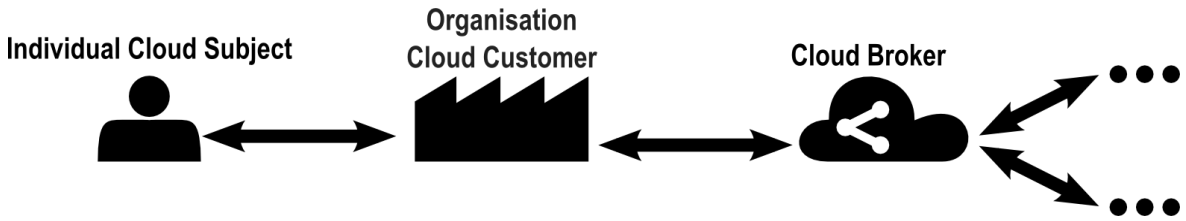


Figure 19 Using a Broker with Individual Cloud Subjects Involved (Partial View)

This type of scenario illustrates cases where accountability will be even more challenging due to the complexity of the supply chain – **Example**: A photo storage service uses a cloud broker to get the cheapest block storage offering on a daily basis. It encrypts the pictures before storing them with a provider and maintains a backup with a second one (encrypted as well) as a failsafe.

4.3 Regulatory Roles

The proposed EU regulation (GDPR) increases the responsibility and accountability of data controllers and processors, as assessed further within documentation provided by WP B-5. The Data Controller (DC) should implement appropriate procedures to ensure that the data processing carried out by the CSP complies with the GDPR – but it is difficult for a business customer (esp. SME) to influence the structure of cloud services, especially IaaS services. Clarification of DC and Data Processor (DP) responsibilities is key in cases where personal information is involved. The provider of cloud services can be a DP and/or a sole or joint DC. For analysis of how this is likely to change with respect to the forthcoming EU GDPR, see (EDPS, 2012). There can be multiple DPs in some scenarios (see (GSMA, 2012) for example, which defines an accountability framework for mobile environments). Contracts/SLAs define respective responsibilities, but some of the responsibility cannot be transferred to the CSP, both in terms of security responsibilities and legal responsibilities. An accountability-based approach should actually help clarify this situation.

This section reviews the roles drawn from the EU Data Protection Directive (DPD), which defines a specific regulatory regime. We then analyse cloud actors from a regulatory perspective and derive further relevant responsibilities. In our case, the DPD is the relevant regulatory regime we are considering in order to identify relevant roles and responsibilities. The same idea would work if considering other regulatory perspectives. The relevant regulatory roles are then used to analyse specific responsibilities and obligation for cloud actors. In particular, cloud actors have different responsibilities and obligations depending on being a data subject, data controller, data processor or data protection authority in relation to the processing of personal data. Note that this section has taken into account mainly two perspectives: cloud computing and data protection. These two perspectives allowed us to identify and define specific roles for cloud actors. However, the process of identify roles could be extended to other alternative regulatory regimes (business confidential data, intellectual property, etc.), which are relevant for the specific context. This would result in an extended schema of roles for cloud actors. Figure 20 lists the Data Protection roles we have identified.

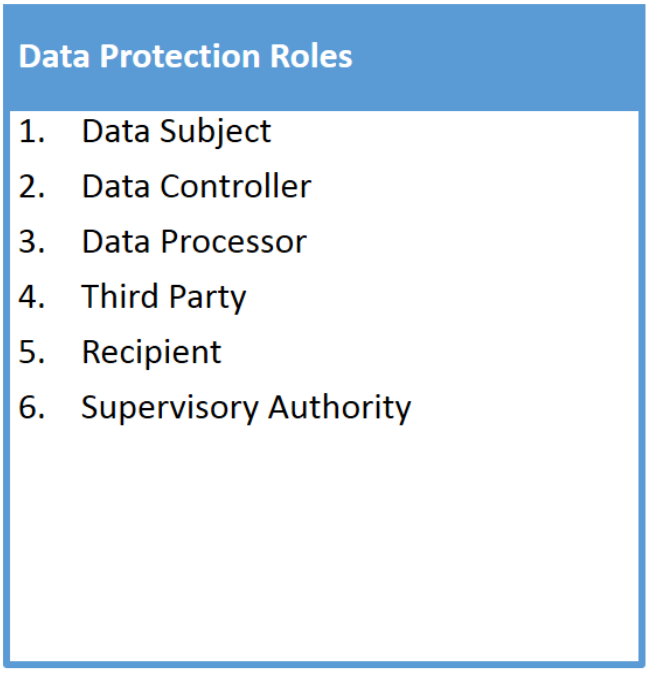


Figure 20 Data Protection Roles

Based on the directive 95/46/EC (DPD) and 2002/58/EC, we identify six roles in the data protection domain:

1. **Data subject**: an identified or identifiable natural person (i.e. living individual). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
2. **Data controller**: an entity *which alone or jointly with others determines the purposes and means of the processing of personal data*.
3. **Data processor**: an entity *that processes personal data on behalf of the controller*.
4. **Third party**: an entity *other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor,* is *authorised to process the data*.
5. **Recipient**: an entity to which *data* is *disclosed, whether a third party or not*; (excluding *authorities which receive data in the framework of an inquiry*).
6. **Supervisory authority**: an independent authority that enforces the application of the data protection regulations in member states, providing advice to the competent bodies with regard to legislative and administrative measures relating to the processing of personal data, hearing complaints lodged by citizens with regard to the protection of their data protection rights. The supervisory authority is either the Data Protection Authority or, less frequently, the National Regulatory Authority in the telecom sector in some member states.

An actor may play one or more data protection roles, in relation to distinct data processing. For example, an actor can be a controller with respect to one data processing and at the same time be a processor with respect to another data processing. Note that there are other terms that originate from the DPD, which we have been using in this report. These are:

- **Personal data** means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Recital 26 of the DPD, clarifies that this definition does not apply to data rendered anonymous in such a way that the data subject is no longer identifiable, taking account of 'all the means likely reasonably to be used either by the controller or by any other person' to identify the data subject. Data, which has been so rendered anonymous, is often termed 'anonymous data'.

- **Sensitive personal data** is not defined in the DPD, but the term "sensitive personal data", or "sensitive data", is often used to refer to certain special categories of data under Article 8 of that Directive, which refers to *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life*. By default, Member States must prohibit the processing of personal data falling within the special categories except in limited circumstances. These limited circumstances notably include the case where the data subject has given his explicit consent to the processing (except in cases where the law states that such consent is insufficient to lift the prohibition on processing), or the case where such data is necessary to protect the vital interests of the data subject or of another person in circumstances where the data subject is physically or legally incapable of giving his consent. Other exceptions exist both in the DPD and in member state legislation.

- **Processing** (of personal data) is *any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*.

Table 2 shows the possible mapping between the cloud roles we have identified in our extended NIST model and the data protection roles. Cloud customers, providers and brokers will be mapped to different roles on a case by case basis.

Table 2 Cloud Actor Roles

Extended NIST model role	Data protection possible roles
Cloud subject	Data subject
Cloud customer	Data controller or Data processor
Cloud provider	Data processor or Data controller
Cloud carrier	Data processor or Data controller (unlikely) or Not applicable.
Cloud broker	Data processor or Data controller
Cloud auditor	(Not Applicable)
Cloud supervisory authority	Supervisory authority (DPA or NRA)
(Not Applicable)	Third party
(Not Applicable)	Recipient

Cloud customer: When the Cloud Customer is a business or a legal person, it will be considered as a data controller, since the customer has the role of choosing the *means and the purpose* of data processing by selecting a particular cloud provider.

When the Cloud Customer is a natural person, it will likely be considered as a data subject. However, there are situations where a person uses a cloud service for professional purposes processing data of other data subjects and in that cases that person will be considered as a data controller as well (see opinion of WP29 on social networks[69], and see "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe" for examples).

Cloud provider: Cloud providers can be considered as data processors or controllers[70]. Broadly speaking we can differentiate three cases:

1. The cloud providers processes personal data which is not provided by a cloud customer, acting autonomously to define the "means and the purpose" of the processing. In this case, the cloud provider is a data controller.
2. The cloud provider processes personal data to provide a service requested by a cloud customer, and does not further process the data for its own purposes. In this case the cloud provider is a data processor.
3. The cloud provider processes personal data to provide a service requested by a cloud customer, and further processes the data for its own purposes (statistics, advertising, research, etc.). In that case the provider is a (joint) data controller.

In practice, the view established in the DPD that controllers are "in control" and that processors only act "based on the instructions" of the data controller is not well suited for the cloud. First, we can note that in most cases cloud customers have little leverage against cloud providers: they either accept the service conditions offered by the provider or they find another offering ('take it or leave it'). The cloud customer cannot notably change security measures or policies implemented by the provider. As noted by the Article 29 WP (Opinion 05/12, 2012) the cloud customer is then still considered as a Controller because he chooses among several offerings, thereby selecting the "means and the purpose" of the processing. However, cloud providers usually also allow themselves to change the conditions of the service unilaterally. This has caused in some cases customers and providers to wrestle over their

[69] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf

[70] Although a cloud provider (and a cloud broker) will more than likely have the role of a data controller for the cloud customer's data used for administrative purposes, the customer may not be a data subject and DP law may not apply; we focus our attention on the primary processing rather than the secondary processing (business client databases) which may or may not have personal data.

respective roles and responsibilities, as the providers typically refuse to accept the role of "joint-controller". This problem has been partially recognised in the current proposal for GDPR (European Commission, 2012). The proposal notably explicitly states that a processor who processes data beyond the controller's instructions is to be considered as a joint controller (Article 26.4). A cloud provider that would unilaterally change security measures or data handling practices would therefore be considered as a joint-controller in some cases.

Cloud broker: Cloud brokers are more likely to be considered as data processors than data controllers, because of their position as intermediaries. However, the reasoning applied above to data controllers is also valid for cloud brokers, which could be considered as controllers in some circumstances if they process the data for their own purposes. It may also be that they fall outside the controller/processor distinction because they not necessarily process any personal data in the line of their business.

Cloud carrier: The case of Cloud Carrier is complex as it may intersect several regulatory regimes and depends on the actual function of the Carrier, which could range from a CDN (content distribution network) to a specialised telecom operator, for example.

In the simplest case where the Carrier can be assimilated to a telecom provider, he will generally not be considered as controller (or even a processor). Their purpose is to transfer data between cloud entities regardless of the fact that this data is personal data or not. Recital 47 of the Directive 95/46 (DPD) clarifies that telecom service providers are not to be considered as Controllers for the transmission of electronic messages, except if they use additional personal data for the purpose of this service. In this case, we also note that Directive 2002/58 may place some specific and distinct regulatory obligations on Carriers, notably confidentiality of communication contents, if they are considered as providers of a publicly available electronic communications service.

In the case where the Carrier takes a more complex role, providing a value added service such as a CDN, it may be considered as a processor of another cloud entity. It is unlikely that the cloud carrier will be considered as a controller, but we cannot fully exclude this possibility if the carrier processes some data for its own purpose (advertising).

4.4 Actor Responsibilities

The risks, as well as responsibilities, will vary according to the combination of cloud service and deployment models. Correspondingly, security and privacy requirements will vary widely from one use case to the next. For example, an internal private cloud can potentially offer an organisation greater oversight and authority over security and privacy, and better limit the types of tenants that share platform resources, reducing exposure in the event of a failure or configuration error in a control (Jansen & Grance, 2011). In terms of service models, the security that the customer is responsible for implementing and managing will vary, as shown in Figure 21 (CSA, 2011).

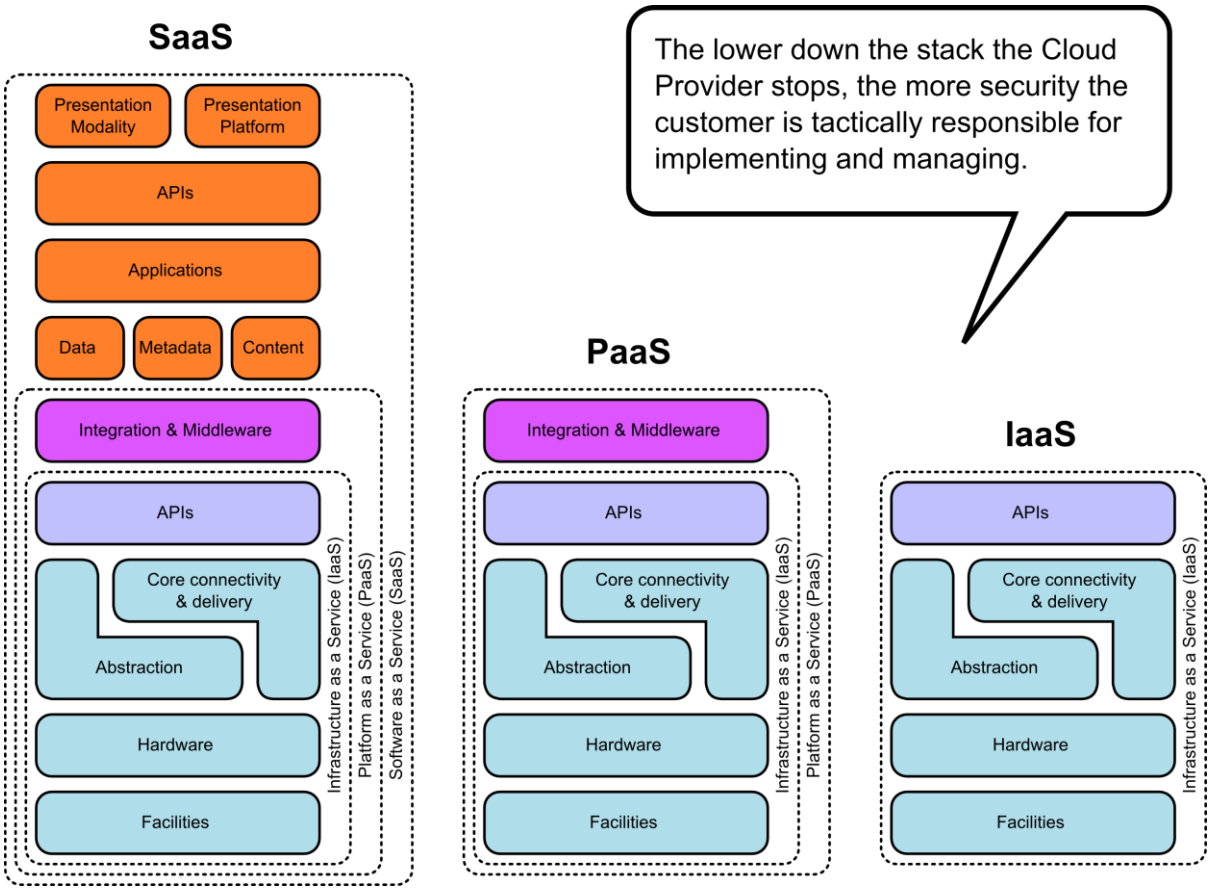


Figure 21 CSA Security Hierarchy (CSA, 2011)

IaaS customers are responsible for log collection, security monitoring, guest OS patch and hardening, guest security platform and guest system monitoring. PaaS providers are responsible for the security of the platform software stack. SaaS providers are responsible for security applications delivered to end users; the SaaS customers are normally responsible for operational security processes (i.e. user and access management), including identity management, authentication and compliance with data protection law.

In IaaS and PaaS, a great deal of orchestration, configuration and software development is performed by the customer, so much of the responsibility cannot be transferred to the CSP. Although the cloud provider bears most of the responsibilities for SaaS, the virtual machine that contains licensed software and works with sensitive data places many more responsibilities on the customer that builds and manages it. SLAs define the respective responsibilities. There is also potential for user responsibility to be outsourced to third parties who sell speciality security services, such as configuration management or firewall rule analysis. Further discussion about responsibilities is given in what follows, particularly in relation to legal obligations, and the way in which these might change over time.

4.5 Accountability Relationships and Graphs

So far, we have defined accountability actors by extending the NIST supply chain model, and we have shown some general rules for the mapping between these accountability roles and data protection roles. We may consider building accountability graphs, were:

- Vertices represent accountability roles endorsed by actors.
- Edges represent accountability relationships between actors.

This immediately raises the question of what constitutes an “accountability relationship”. The definition of accountability proposed in this document, as well as the definition of accountability attributes, shows that the notion of accountability is multidimensional. There are therefore multiple ways to envision

accountability relationships, which forms the edges of an accountability graph. We examine two approaches in this Section:

1. **Based on accountability "interactions"**: data exchanges representing the agreement, reporting, demonstration or remediation of data policies from one actor to another.
2. **Based on "providing account" obligations**: the obligation to demonstrate and provide assurance, from one actor to another.

4.5.1 Interaction Graphs

Accountability involves at least two entities A and B, where one entity is responsible to the other for the definition, implementation and/or demonstration of data stewardship practices. Following the definition of accountability used in this framework, this means for example that:

- Actor A will *define governance to comply with internal and external requirements*, some of which are expressed by actor B;
- Actor A will *implement appropriate actions* in response to these requirements, and will *explain and justify* these actions to B;
- Actor A will *inform* and possibly *provide remediation* to B in case of failure to implement the requirements.

These practices translate into interactions between actors. More precisely, based on the work we conducted in (C-3.1), we define 4 logical families of interactions between two actors for the purpose of accountability:

- **Agreement**: [actor A] takes responsibility for processing of data provided by [actor B] according to a data handling policy.
- **Reporting**: [actor A] informs [actor B] about status of data handling policies.
- **Demonstration**: [actor A] demonstrates to [actor B] compliance with data handling policy.
- **Remediation**: [Actor B] seeks (and receives) remediation from [actor A] for failure to implement data policy.

The four families of interactions are used to cover the seven core accountability attributes (defined in Section 5) as follows:

Agreement covers all interactions that lead to one actor taking responsibility for the handling of certain data provided by another party according to a certain policy. These interactions may include a negotiation phase. A policy may express requirements that apply to all core accountability attributes, and contribute to the implementation of the attribute of *responsibility* and *liability*. Agreement interactions requires both: means to express data policies; and, means to describe implementation of policies, potentially through a negotiation.

Reporting covers all interactions related to the reporting by an actor about current data handling practices (e.g. reporting incidents on customer data) and policies. This type of interaction mainly supports the implementation of the accountability attribute of *transparency* and *observability*.

Demonstration covers all interactions that lead to one actor demonstrating the correct implementation of some data handling policies. This includes external verifications by auditors or cryptographic proofs of protocol executions for example. This type of interaction mainly supports the implementation of the accountability attributes of *verifiability* and *attributability*. We emphasise that *Demonstration* is different from *Reporting* in that it implies some form of proof or provision of evidence.

Remediation covers all interactions that lead one actor to seek and receive remediation for failures to follow data handling policies. This type of interaction mainly supports the implementation of the accountability attribute of *remediability*.

We note that *Reporting*, *Demonstration* and *Remediation* are interactions that contribute to the implementation of requirements related to the core accountability attributes. By contrast, *Agreement* is a type of interaction that is used both for the expression of requirements that apply to the core accountability attributes, and the implementation of taking responsibility to implement the core attributes in accordance with policies, regulations and ethics, and defining corresponding liabilities.

As shown in (C-3.1), interaction graphs are useful to map out all interoperability requirements between roles in our accountability model. Their drawback is that they do not show obligations of actors towards each other, but focus on the implementation of these obligations in terms of communications between actors. Obligations and implementation do not always overlap. Indeed a cloud customer may have the obligation to inform data subjects about policies but may delegate the implementation to a cloud provider, resulting in interactions between the data subject and the provider.

4.5.2 Account Graphs

Another approach is to interpret accountability relationships as directed edges, form Role A to Role B, with the meaning that:

[Role A] must provide account to [Role B].

Therefore, we focus on the obligation to demonstrate and provide assurance, from one actor to another. Figure 22 based on this idea proposes a generic account graph applicable to the data protection domain.

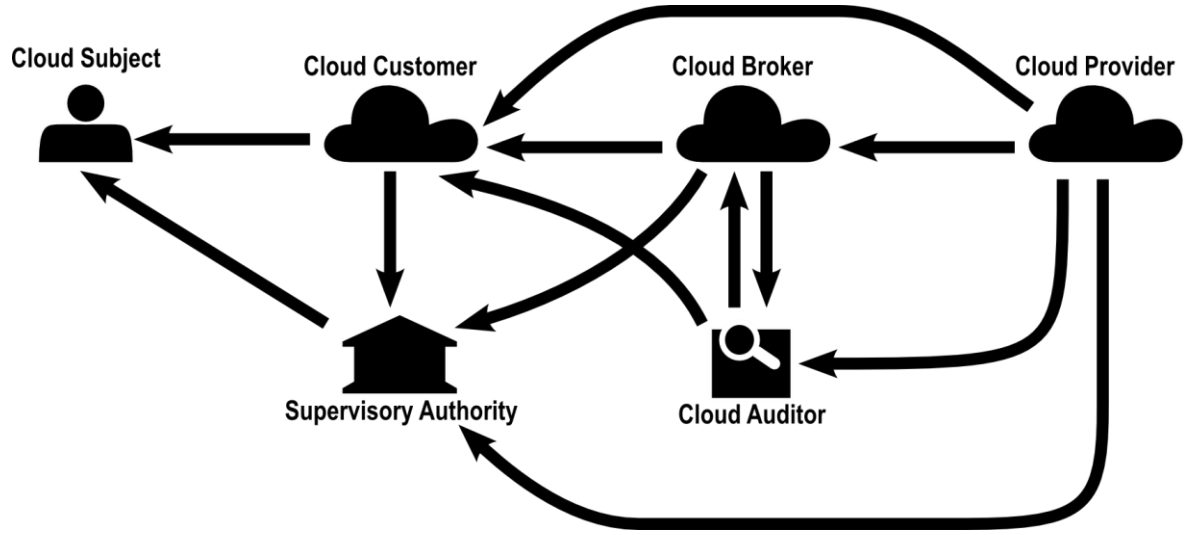


Figure 22 Account Graph

The above graph (Figure 22) can be detailed as follows:

- The cloud **provider** and the cloud **broker**
  - must provide account of compliance to an **auditor**.
  - must provide account of compliance to the **supervisory authority**
  - must provide account of compliance to cloud **customers**.
- The cloud **provider** must provide account of compliance to a **broker**.
- The cloud **auditor**
  - must provide confirmation that it audited a cloud service (provider or broker) to a cloud **customer**.
  - must provide confirmation that it audited a cloud service (provider) to a cloud **broker**.
- The cloud **customer**
  - must provide account of compliance to a **cloud subject**.
  - must provide account of compliance to the **regulator** (DPA or NRA).
- The **regulator** must provide account to the **cloud subject** that it processed its complaint.

4.6 Summary

This section is designed to provide a generic set of tools to discuss accountability in cloud supply chains. As a starting point, we established a taxonomy of seven cloud actors that we use in A4Cloud to describe accountability scenarios. This taxonomy is largely inspired by the ubiquitous NIST cloud actor taxonomy,

but extends it to take into account the scope of accountability, by notably adding the role of Cloud Subject, which is the actor to which all others are ultimately accountable. Armed with this set of cloud accountability actors, we are able to describe four canonical cloud supply chain scenarios in a way that is largely domain independent. The second scenario illustrates an important case that is often overlooked and which presents a challenge for accountability: when the cloud subject is distinct from the cloud customer. Since data protection is one of the central domains of investigation in the A4Cloud project, we show how our generic taxonomy can successfully be mapped to domain specific actors such as those found in the data protection domain, as defined in the EU data protection directive (DPD).

Finally, we take a closer look at accountability relationships between actors. We propose two types of accountability graphs that we consider useful to describe accountability networks. In both of these graphs, vertices represent actors, but the nature of edges differs. In the first graph, edges represent interaction between actors, which are classified in four categories: *agreement*, *reporting*, *demonstration* and *remediation*. This representation is used in the C3 work package to analyse interoperability requirements for accountability. In the second type of graph, an edge represents the fact that an actor A is accountable to an actor B. We call this representation, an “account graph”.

5 Accountability Model

Building on the concept of accountability presented in Section 2, we introduce a model of accountability for data stewardship. The model expands upon the definition of accountability by introducing accountability practices, attributes and mechanisms. Accountability attributes encompass the numerous elements and properties of accountability at the conceptual level. Accountability practices characterise organisational behaviour, and hence define what it means to be an accountable organisation. Diverse mechanisms are used in order to support such practices.

5.1 Description of the Model

Building on the definition and analysis of accountability in Section 2, we introduce a model of accountability. The model expands upon the definition using accountability attributes, practices and mechanisms. Accountability, a complex concept related to privacy and data protection, encompasses different attributes, hence accountability attributes. Accountability practices characterise organisational behaviour, hence what defines accountable organisations. Diverse mechanisms are used in order to support such practices. The A4Cloud accountability model consists of:

- **Accountability attributes** – conceptual elements of accountability applicable across different domains (i.e. the conceptual basis for our definition, and related taxonomic analysis)
- **Accountability practices** – emergent behaviour characterising accountable organisations (that is, how organisations operationalise 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 23 illustrates how attributes, practices and mechanisms form a model of accountability for cloud ecosystems. Accountability is interpreted in terms of *accountability attributes*. These accountability attributes are operationalised (that is, put into practices) by organisational *accountability practices*. Accountability practices need to comply with and mediate between external (drawn from relevant regulatory regimes and ethical attitudes) and internal criteria (characterising organisational culture). In order to implement such practices, organisations use different *accountability mechanisms* tailored to their domains. On the one hand, organisations adopt mechanisms in order to address their needs. On the other hand, they shape (that is, adapt or modify) them in order to embed organisational knowledge derived from experience. These mechanisms therefore constrain and support accountability practices, and the operational interpretation of the accountability attributes.

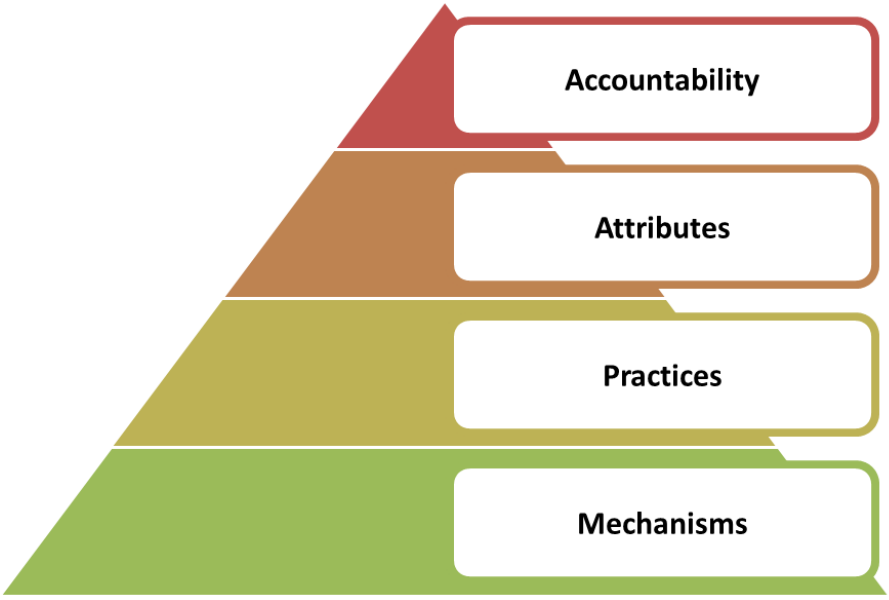


Figure 23 Accountability Attributes, Practices and Mechanisms

The emerging relationships between accountability attributes, practices and mechanisms give rise to an operational interpretation of accountability. This characterisation explains how organisations may attain accountability in different ways, that is, instantiate this accountability model differently according to their particular contexts. The remainder of this section describes the accountability attributes, practices and mechanisms.

5.1.1 Accountability Attributes

Accountability attributes capture concepts that are strongly related to and support the principle of accountability. We propose a number of attributes, coming from our analysis at the topmost layer, i.e. from our definition and related literature. The core (key) attributes are: transparency, responsiveness, responsibility and remediability. In addition, as we shall see, verifiability is a key property of an object of accountability, and accountability indicators about the measures used by an organisation include the key attributes of appropriateness and effectiveness.

We now consider these notions in more detail. We shall distinguish between attributes that we consider to be key to the concept of accountability, in the sense that they are most associated with our definition of accountability and related notions in the literature, and those that we consider to be of secondary relevance, in the sense that they are not necessary elements of accountability or have a strongly overlapping meaning to a key attribute.

Recall from Section 2 that we identify the objects that a cloud actor is accountable for within a cloud ecosystem to be:

- **Norms:** the obligations and permissions that define data practices; these can be expressed in policies and they derive from law, contracts and ethics.
- **Behaviour:** the actual data processing behaviour of an organisation.
- **Compliance**: entails the comparison of an organisation's actual behaviour with the norms.

From the definition of accountability given in Section 2, the core attributes are suggested in a direct way: 'commitment to norms' and 'demonstrating compliance' suggest that transparency is an important element; 'explaining to stakeholders' suggests responsiveness; 'accepting responsibility' suggests responsibility; 'remedying failure to act properly' suggests remediability.

More specifically, these key attributes refer to:

- **Transparency**: the property of a system, organisation or individual of providing visibility of its governing norms, behaviour and compliance of behaviour to the norms.
- **Responsiveness**: the property of a system, organisation or individual to take into account input from external stakeholders and respond to queries of these stakeholders.
- **Responsibility:** the property of an organisation or individual in relation to an object, process or system of being assigned to take action to be in compliance with the norms.
- **Remediability:** the property of a system, organisation or individual to take corrective action and/or provide a remedy for any party harmed in case of failure to comply with its governing norms.

By 'system' here we mean (parts of) the accountable cloud ecosystem, which could for example be a chain of cloud providers or an IT process, which should be accountable to humans. However, since in a legal sense the entities further down the chain are not accountable to cloud customers, but rather to the entity one step up the chain, often in our domain of interest the accountability property will relate to a single cloud provider.

Being transparent is required not only with respect to the identified objects of the cloud ecosystem (i.e. norms, behaviour and compliance) but also with respect to remediation. Hence transparency can be argued to be the most important attribute of accountability. A stronger definition would require demonstration of the governing norms, behaviour and compliance of behaviour as part of the definition of transparency; however, we hold that it is more natural for this aspect of demonstration to be captured mainly within the verification attribute given below. A weaker definition of transparency would only require visibility of the governing norms, but we consider this interpretation of the notion of transparency in the context of accountability to be too weak.

Responsiveness is a key element of the notion of accountability in the relation between government and electorate because ultimately, it is the electorate that mandates what happens (for example, via a social contract). In the context of cloud computing the providers are private entities that determine their own actions, between the boundaries set by regulation, and if users do not like this, they can refuse to use the service. However, even in the relation between cloud providers and their users, responsiveness is required. It refers to the two-way communication relation between cloud providers and external stakeholders (such as individual cloud customers and regulators) needed within the cloud ecosystem to define part of the governing norms. Generally speaking, the audience for an organisation's account should somehow be involved with the process by which the account is produced, and not only with the product.

Responsibility is revealed through being an attribute of the accountability objects, so is slightly different from the other attributes listed here, in that for each object, process or system within an accountable ecosystem a responsible entity (i.e. cloud actor that here would be the accountor) should be provided.

The remediability attribute provides assurance that being responsible, etc. is not sufficient and further action is required in order to be accountable; although legal responsibility, namely liability, leads to remedies, accountability equally puts emphasis not only on whom to blame but how to heal.

An attribute that is a property of the *objects* of accountability (i.e. norm, behaviour, compliance) is:

- **Verifiability:** the extent to which it is possible to assess norm compliance.

This is a property of the behaviour of a system, service or process that it can be checked against norms. We consider this to be a core attribute because of our explanation of accountability in terms of defining and displaying relevant norms, behaviour and compliance to the norms.

Other attributes that are properties of accountability objects but are of secondary relevance are:

- **Attributability**: the possibility to trace a given action back to a specific entity.

This is a property of behaviour or of a norm violation. Attributability is considered of secondary relevance as it is not explicit in our definition of accountability, but is implied in the notions of responsibility and transparency. For responsibility to materialise in a meaningful way, actions have to be attributable to those responsible for them. Furthermore demonstration of this responsibility through transparency allows for accountability.

- **Observability:** the extent to which the behaviour of the system is externally viewable.

This is a property of behaviour of a system, service or process which describes how well the internal behaviour of a system, service or process can be described by observing the external outputs of the system, service or process. Observability is considered of secondary relevance as it is not necessary for accountability (as observability implies transparency and verifiability but the opposite is not true), even though if organisations know that they are likely to be observed then they may be more likely to behave in a responsible manner. While transparency requires an actor taking actions to be transparent, observability is more passive and the actor may not even be aware of it. It is possible to be transparent (and accountable) and non-observable, by the intervention of a third party that can observe a party instead and transfer the element of transparency.

Accountability is not a binary state, but often has many factors indicating the extent of accountability of an organisation. If accountability is seen as a process in which an organisation can mature, accountability indicators can assess the maturity of the organisation, with a focus on the mechanisms used and resultant behaviour. Accountability attributes may be defined to capture the important aspect of deployment of 'appropriate and effective measures' that meet technical, legal and ethical compliance requirements, and act as this type of indicator:

- **Appropriateness:** the extent to which the technical and organisational measures used have the capability of contributing to accountability.
- **Effectiveness:** the extent to which the technical and organisational measures used actually contribute to accountability.

By 'contribute to accountability', we mean (in the light of the analysis above) contribute to defining and displaying relevant norms, behaviour and compliance to the norms. We believe that it is acceptable to refer to accountability within these definitions since they are accountability indicators (properties of the measures used to support organisational accountability).

The cloud ecosystem not only has internal factors steering accountability, there are also some external factors that have the ability or are needed to keep the process of accountability in motion. These external factors often relate to governance mechanisms that, for example, sanction when compliance is not met. Hence there are accountability attributes that relate to the process by which the accountee holds the accountor to account. One of these is punishability, which is achieved through sanctions. Another attribute relevant to this process is verifiability, which, as already considered above, allows for the provision of evidence that compliance to the norms is (or is not) met. A further relevant attribute is liability. When an actor becomes liable for his actions, one could perceive this as a form of sanctioning. Liability is the legal obligation (either financially or with some other penalty) in connection with failure to apply the norms. It is closely related to legal responsibility (although being held liable does not necessarily mean that the same entity is actually responsible[71]), and is not referred to directly in our definition, and so could be considered to be a secondary attribute.

- **Liability**: the state (of an organisation or individual) of being legally obligated or responsible in connection with failure to apply the norms.

There exist emerging relationships (e.g. implication and inclusion) among the concepts described above dependent on different viewpoints of analysis (which are related to societal, legal and ethical aspects of accountability). For example: from a legal perspective, responsibilities imply obligations, which consequently may involve sanctions; liability is based upon the establishment of norms, allowing the request for remedies and the imposition of sanctions should these norms not be met. If the norms are not met it is not necessarily the case that all related failures can be entirely remedied (e.g. in case of a data breach the "harm" resulting from the disclosure of information is done and that cannot be entirely corrected).

In summary, the *core accountability attributes* are:

ATTRIBUTES OF (ELEMENTS OF) ACCOUNTABLE SYSTEMS:
- **Transparency** is a property of a system, organisation or individual of providing visibility of its governing norms, behaviour and compliance of behaviour to the norms.
- **Responsiveness** is a property of a system, organisation or individual of taking into account input from external stakeholders and responding to queries of these stakeholders.
- **Responsibility** is a property of an organisation or individual in relation to an object, process or system of being assigned to take action to be in compliance with the norms.
- **Remediability** is a property of a system, organisation or individual of taking corrective action and/or providing a remedy for any party harmed in case of failure to comply with its governing norms.

ATTRIBUTES OF ACCOUNTABILITY OBJECTS:
- **Verifiability** is the extent to which it is possible to assess norm compliance.

ACCOUNTABILITY INDICATORS:
- **Appropriateness** is the extent to which the technical and organisational measures used have the capability of contributing to accountability.

[71] For example, according to the DPD, data controllers are always held liable towards data subjects, even in connection with a damage actually caused by data processors.

- **Effectiveness** is the extent to which the technical and organisational measures used actually contribute to accountability.

5.1.2 Accountability Practices

Accountability practices, derived directly from the given definitions, characterise emerging behaviour (highlighting operational and organisational objectives to be met) manifested in accountable organisations. Specifically, an accountable organisation:

- 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 organisational policies have been followed
- Remedies any failure to act properly, for example, notifies the affected data subjects or organisations, and/or provides redress to affected data subjects or organisations, even in global situations where multiple cloud service providers are involved.

5.1.3 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 organisations need to achieve). Organisations can adopt different available accountability mechanisms as appropriate for their contexts. They will use what is best for suits their particular processes best, demonstrating at the same time that the appropriate mechanisms have been selected. Accountability mechanisms focus on the core aspects of accountability (e.g. remediation, notification and risk assessment) and are expected to be used in conjunction with separate privacy and security mechanisms (Pearson, 2013).

Mechanisms (e.g. security controls, policies, tools, standards, legal mechanisms, penalties), from a social science viewpoint, are accountability objects *("that both inhabit several communities of practice and satisfy the information requirements of each of them"* (Bowker, Star, 1999). Accountability mechanisms (developed by the *Cloud Accountability Project*) will complement others that are available from third parties. They may be used individually or in combination. Organisations 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 (CSA, 2013) or the Cloud Trust protocol (Knode, Egan, 2010) to ask for and receive information from cloud service providers about the elements of transparency, or they may take another approach to do so.

5.2 Further Conceptual Analysis

We have already discussed the notion of account, evidence and obligations in Section 2. This section provides some further consideration of related conceptual aspects, including remediation and sanctions and the distinction between responsibility and liability.

5.2.1 Responsibility and Liability

This section discusses the relationship between the attributes Responsibility and Liability. We start this analysis by recalling the given definitions: Responsibility – *"the property of an organisation or individual in relation to an object, process or system of being assigned to take action to be in compliance with the norms"*, Liability – *"the state (of an organisation or individual) of being legally obligated or responsible in connection with failure to apply the norms*". An over simplistic view of these attributes might suggest that they, to a certain extent at least, correspond to each other and that they could be used interchangeably in regulatory, legal and/or other contexts. The short response to that view is yes (sometimes); no (other times), and yes and no (depending on the circumstances). Because of that confusion, it is worthwhile to further examine this issue and explain the distinction between these attributes of Accountability.

Liability can arise from regulations and/or contracts, so we determined that it is already implied and/or that such expansion of the definition is unnecessary. The definition of Liability highlights the legal perspective we are concerned with and why Liability can present itself as an important attribute of accountability, especially in light of the regulations and contracts which often dominate the realm of data protection and consequently, cloud computing. Responsibility also encompasses another important aspect of accountability in that it includes the moral, ethical and/or social obligation of acting in an acceptable manner and in conformance with standards of good practices that may or may not otherwise be part of the applicable regulations or contracts, and therefore not otherwise encompassed by Liability.

What the impact or effect of liability is another question (one which is addressed by B5 work package on Contractual and regulatory considerations and D4 work package on Redress and Remediation). However, such impact is irrelevant for the definition of liability itself and the distinction between responsibility and liability remains clear from a legal perspective (though, perhaps confusing the issue further, is that lawyers and regulators will themselves often use the two terms interchangeably). Nevertheless, there are often cases where it is possible to distinguish responsibilities from liabilities. It should be without any surprise that liability requires responsibility before it can be asserted/enforced, but one could also argue that the search of responsibility can be sometimes driven by a quest to assign liability. This is, for example, the case with man-made major environmental disasters, such as the shipwreck of the Erika in 1999, where the court held Total responsible "*in solidum*", citing imprudence as sole responsibility. This example is, of course, far from the scope of our project, but we are left wondering to which extent a large organisation (read: able to indemnify) could be held liable for sanctions and/or for damages in which it does not carry a (primary) responsibility.

Further, and although the adopted definition seems to imply that liability is more strongly associated with the attribution of a blame than with redress, most laymen do associate liability with redress in terms like 'liability insurance', 'liability cap', "liable for" which are all strongly associated with that use. There certainly can be an element of blame into liability, but it is not addressed, implicitly or expressly, in the definition (that is, there is no implication of blame in the definition and the definition presumes that "the state of being legally obligated or responsible" will be determined by the governing legal regulations and/or applicable contract(s)). Thus, when an organisation has breached its legal obligation, it could face repercussions for that breach, whether through the imposition of damages, sanctions, or some sort of remedial action such as an injunction. Thus, there are inherent connotations of blame and redress where there is a breach of a duty owed as a consequence of being liable.

In other words, there will always be responsibility within liability, but not always liability within responsibility (though most times there will be). As for indemnification, that will be determined by the contracts agreed to by the parties involved (this is however beyond the scope of the A4Cloud project). Let us consider an example in order to discuss and to clarify that concept. Every actor (in a cloud ecosystem) has a set of responsibilities (assigned by law or contract), and each may have a set of liabilities which often, but not always, match up with the responsibilities. But an actor can be liable but not responsible, or can be responsible but not liable, or can be both responsible and liable. Deciding which depends on the specific factual circumstances of any given circumstance, and the application of the governing law and contracts to that situation. Just to complicate things even further, it is possible to have legal liability without any responsibility for an action which gave rise to the liability (And, to add another layer to the confusion, lawyers often use the word 'responsible' as a synonym for "liable"). For example, imagine a UK data controller stores personal data with a cloud service provider. The service provider wrongfully discloses that personal data to a third party. In these circumstances the UK Information Commissioner will hold the data controller legally liable for the disclosure. But we would all accept that the data controller is not responsible for the disclosure (except in the sense that the law makes the controller responsible by imposing liability, which is not the common usage of the word). Of course, the service provider will also potentially have liability – in this case to the data controller under the service contract and (if it is a UK entity) liability to the Information Commissioner as well. But it is possible that the service contract validly excludes the service provider's liability, in which case it will be responsible but not liable. In our example, "who is at fault" means "failed to take action". Our point is that in this scenario the controller has not failed to take any assigned action, but is still legally liable. As such, the use of the term 'responsibility' in such an example is different from the one established within the A4Cloud project. Taking the A4Cloud definition, in our example both the data controller and the processor are responsible for something though likely with different scope (which is defined in the

contract they have with each other). As a side note, the third paragraph of Article 17 of Dir 94/46 EC imposes the same security obligations on the processor as the controller. So in our scenario, we might argue that there is a legal responsibility – a liability – for the processor as well (i.e. the processor is assigned by law to take action to secure data). As far as we can tell, member state legislations do not provide any tools to enforce this obligation on processors.

In conclusion, it is one of the goals, and hence the inclusion of both Responsibility and Liability as attributes of Accountability, that all actors assume responsibility for their acts and/or omissions, but also recognise that there may also be liability associated with those responsibilities. Likewise, that does not mean that all actors will be liable for those same acts and/or omissions, and such liability will again be determined by the applicable regulations and/or contracts between those actors.

5.2.2 Remediation and Sanctions

Remediation and sanctions fall under the broader scope of consequences accountability may entail (Bovens, 2007) in case certain obligations are not met. Colin Benett highlights the role of rectification in relation to accountability by stating that: "*accountability implies a process of transparent interaction, in which a body seeks answers and possible rectification*." (International Privacy Standards, 2010). Depending on the nature of these obligations (e.g. regulatory, contractual), the consequences may take various forms ranging from administrative measures issued by Data Protection Authorities to court decisions. The provisioning of legal consequences is based upon the prior allocation of liabilities upon the entities, who will essentially suffer the burden of consequences, should they fully or partly fail to meet their obligations. Liability triggers, therefore, legal consequences and may lead to remediation and sanctions. Taking into account that consequences resulting from non-compliance with legal obligations might not only be legal (e.g. damage of reputation), the discussion below focuses only on consequences provided by law. In general, the legal consequences aim – primarily – to serve as a threat, forcing accountable actors to comply with rules. Mulgan states: "*Admittedly, the prospect of sanctions has an important deterrent effect on those held accountable. In this respect, accountability, like any enforcement procedure, can be seen as designed to influence the future as much as to judge the past"* (Mulgan, 2003). Secondly, as soon as there is the legitimate ground for these legal consequences to be implemented, their enforcement might not only entail the punishment of the entity that did not meet its obligations, but also entail compensating the aggrieved party.

Oxford Dictionary of Law defines remedies as "*any of the methods available at law for the enforcement, protection, or recovery of rights or for obtaining redress for their infringement*." Remedies, however, might –or might not– lead to remediation, given that not all types of "failures" can be entirely corrected. In case of a data breach, for instance, remedies cannot ensure remediation; the data has been disclosed, and therefore, the right to private life and to personal data protection has been irreversibly infringed. Although from a technical point of view, remediation seems mostly feasible, from a legal point of view it depends largely on the type of infringement, which explains why A4Cloud considers remediability – rather than remediation – as an accountability attribute.

For remediation to be enforced, there must be a redress mechanism in place allowing for the exact process interested parties (i.e. cloud subjects) should follow in order to make right (i.e. process for filing complaints adapted to the types of the cloud clients or cloud offered service). Such a redress mechanism can either be established by law allowing for the external enforcement of remedies (i.e. by courts or by supervisory authorities) or be provided within a company's policies dictating the exact procedural steps that would allow for internal remedial actions within the accountable organisations.

Sanctions on the other hand may be considered as a punishment in case of an infringement, which – in the context of personal data protection – can be imposed either by supervisory authorities or through courts. Early termination of a contract between the data controller and the data processor, in case the latter does not meet his contractual obligations, is not really a sanction from a legal perspective, but rather a contractual right of termination based on an act or omission. Sanctions may therefore be regarded as purely regulatory and imposed by governing bodies such as DPAs and/or courts.

The relationship between remediation and sanctions is complementary based on the prior establishment of liabilities. The Data Protection Directive (DPD) dedicates a separate chapter (Chapter III) on

Remedies (Article 22), Liability (Article 23) and Sanctions (Article 24), providing for them in consecutive articles pointing out the underlying close link. The following scenario fleshes out roughly the relationship between the aforementioned concepts as they emerge in the field of European data protection law:

> A data subject files a complaint to the competent Data Protection Authority regarding the implementation of the appropriate security measures by the Data Controller. The Data Protection Authority issues a decision dictating the DC to proceed to corrective actions and imposing *a* fine to the Data Controller. The data subject can, also, go to court asking for damages as provided in the contractual agreement with the Data Controller. The court decides on compensative damages.
>
> The data subject files a complaint on the basis of the right to administrative remedies (Article 22 of the DPD), which leads to the imposition of sanctions –corrective measures, fine- to the Data Controller (Article 24) due to non-compliance with Article 17 of the DPD providing for the adoption of "appropriate security measures". Moreover, the data subject is entitled to judicial remedies allowing her to ask for compensation on the basis of the damage suffered from the data controller, given that data controllers are held liable towards data subjects even if the damage is actually caused by processing operations performed by data processors (Article 22 & 23).

The common understanding of the notion of accountability even in areas outside the project's scope explains why remedies and sanctions can be considered as conceptual elements of the accountability concept. R. Mulgan notes in this respect: "*Accountability', however, is more sensibly confined to its everyday sense of external scrutiny and sanctions*.[72]" A4Cloud does take into account how accountability is being broadly understood, and builds further on it by stressing out certain aspects of the accountability concept, such as the proactive approach implied or the emphasis on the role of the account *per se*.

5.2.3 Observability

Our definition of observability is given above as "the extent to which the behaviour of the system is externally viewable". From a computer science perspective, 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. Observability at first sight might seem to be an unnecessary characteristic of an accountable system, because a system can lack 'external' observability and still be accountable. For example, a system might have external outputs that provide no (or little) information on its internal actions, and yet be accountable by allowing a third party auditor to verify its internal actions (and certify their compliance). In other words, a system can be transparent (or verifiable) without being observable externally. Therefore, the rationale for observability is that we should be able to a certain extent to 'observe' the behaviour of a system/service. Of course, the observability *per se* can be operationalised in different ways. We should be able to 'observe' the behaviour based on the input/output observations. Just to draw some similarity with other engineering concepts, observability can capture a sort of 'black-box' analysis: that is, there may be little or no information about some internal system/service, but somehow it should still be possible to understand what the service/system is doing on the data. Observability enables most operational monitoring at the service/system level, as required in order to support evidence gathering (fundamental for providing an account to third parties).

5.3 Summary

The accountability model consists of: accountability attributes (that relate to accountability), accountability practices (that characterise accountable organisations) and accountability mechanisms (that support such practices). The main accountability attributes are: transparency, responsibility, responsiveness, remediability (core attributes); verifiability (attribute of accountability object); appropriateness and effectiveness (accountability indicators). Accountability practices are:

- defining governance to responsibly comply with internal and external criteria
- ensuring implementation of appropriate actions

[72]Mulgan, R. (2003): Holding Power to Account.

- explaining and justifying those actions
- remedying any failure to act properly.

Organisations identify and implement accountability mechanisms, as appropriate for their given context, in order to satisfy the accountability practices. A4Cloud is defining (and implementing) a range of accountability mechanisms and tools that can be used individually or in combination with each other or with other external mechanisms.

6 Accountability Framework

This section extends the concept of accountability to cloud environments. It explains accountability in the context of the A4Cloud project, that is, accountability for cloud service provision. It defines accountability for data stewardship in the cloud. Section 3 and Section 4 have highlighted the need for accountability in cloud ecosystems. This section uses the accountability model introduced in Section 5 for structuring the analysis of cloud actors in terms of accountability attributes, practices and mechanisms. It furthermore presents an accountability framework, which comprises preventive, detective and corrective mechanisms that are usable throughout the cloud service provision chain, hence enabling chains of accountability.

6.1 Accountability for Data Stewardship in the Cloud

A closely related notion to accountability is data stewardship. In a supply chain, cloud services are consumed from many different cloud providers in an ecosystem (as highlighted in Section 4). It is a challenge to understand such ecosystems, and a step change in thinking is required. Security and privacy management evolves into an information stewardship problem. In the cloud, it will be harder to establish the risks and obligations, implement appropriate operational responses and deal with regulatory requirements. The notions of transparency and assurance come in more strongly and it is necessary to ensure 'chains of accountability'. Accountability places a legal responsibility upon an organisation that uses personal information to ensure that the contracted partners to whom it supplies the personal information are compliant, wherever in the world they may be. So, the communities responsible for data stewardship (who are typically organisational IT security, legal, operations and compliance staff) place responsibilities/constraints on other individuals or on the way systems operate, and these constraints are met along the chain of provision. Applying the definition of accountability given in Section 2 to the project scope defined in Section 1, we obtain a revised definition of accountability that applies specifically to the case under consideration by the A4Cloud project that was given already in Section 2.2.1, namely:

> **Definition of Accountability for Data Stewardship in the Cloud:** *Accountability for an organisation consists of accepting responsibility for data with which it is entrusted in a cloud environment, for its use of the data from the time it is collected until when the data is destroyed (including onward transfer to and from third parties). It involves the commitment to norms, explaining and demonstrating compliance to stakeholders and remedying any failure to act properly.*

We also need to tailor the analysis given in the preceding sections to the cloud environment, and more specifically, the project scope. Our understanding of accountability (described in Section 2) and accountability model (presented in Section 5) are the result of critical (literature) analysis of accountability attributes (and their definitions), practices and mechanisms tailored to accountability. Appendix B reports our commented review of relevant literature and discussion within the *Cloud Accountability Project*. Structuring accountability (in terms of attributes) allows us to interpret relationships between actors in the cloud.

Figure 24 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 generalisations where one of the actors is actually an oversight or enforcement entity (e.g. regulator and auditor). Figure 24 highlights how the attributes fit together to enable (evidence of) accountability. Transparency relies on verifiability and attributability, which in turn rely on observability. Transparency, responsibility, responsiveness, remediability and liability characterise cloud-mediated interactions between actors in cloud ecosystems. Other aspects of accountability are also relevant. For instance, sanctions are (legal) consequences of failing to fulfil responsibilities. Assurance 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. Remediability is the act or process of correcting, for example, a failure or deficiency, whereas responsiveness is concerned with responding to external queries. Attributes like appropriateness and effectiveness are concerned with the contextual aspect of accountability (i.e. accountability indicators), measuring the organisational measures used.

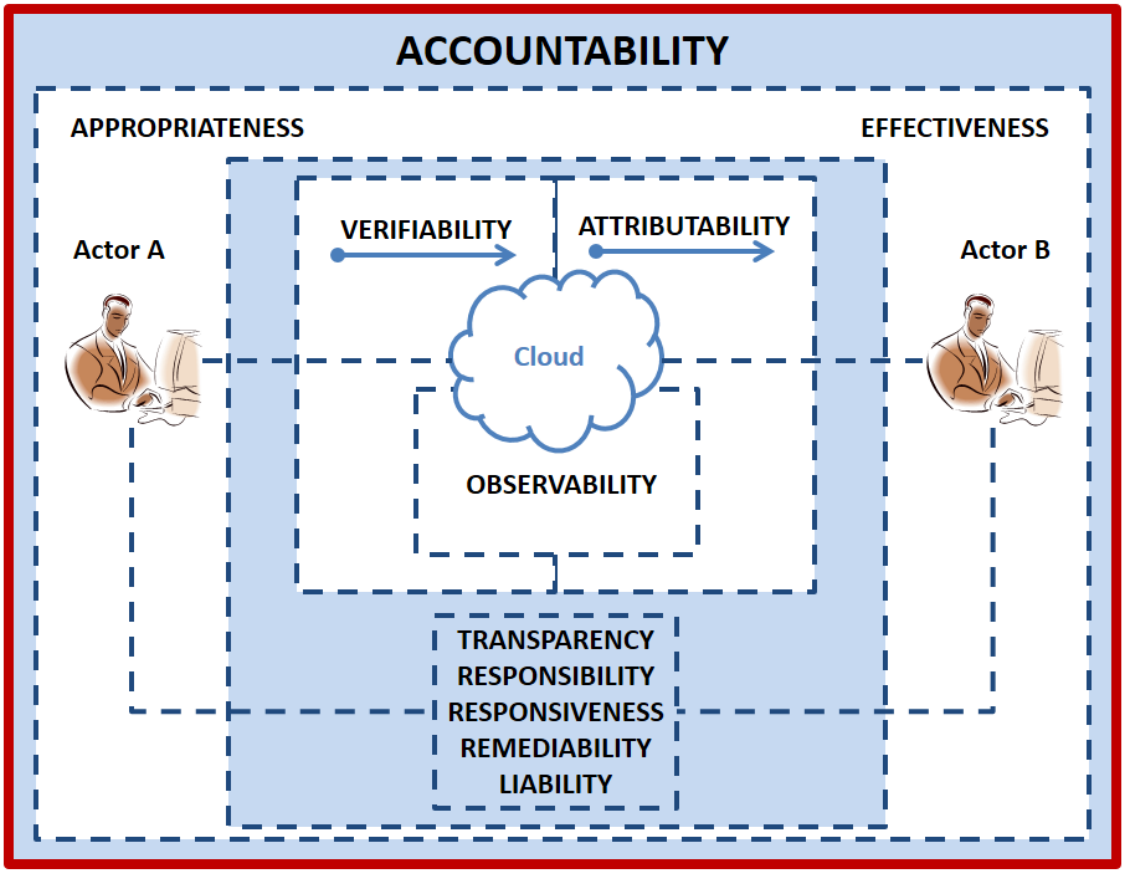


Figure 24 Accountability Relationships between Actors

Other relevant concepts such as obligations, sanctions and account have been already discussed in general accountability terms in Sections 2 and 5.

6.2 Accountability Contexts

While all of the regulatory frameworks considered in Section 2 provide a foundation for data protection, none is specifically designed with managed services or cloud computing applications in mind. The Cloud Industry Forum has started looking at a governance framework for cloud[73] but this work is not yet mature. More fundamentally, either frameworks are defined at the regulatory level that do not encompass or describe how necessary change in underlying structures may be achieved, or else point solutions are developed technically without reference to a more generic framework. ENISA's analysis of trust, privacy and accountability[74] highlighted a number of missing elements, including that *"Research on information accountability technology should be promoted, aimed at the technical ability to hold information processors accountable for their storage, use and dissemination of third-party data."* (Recommendation #16). Our approach is to integrate legal, regulatory, socio-economic 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. This will enable us to implement chains of accountability, including interdisciplinary mechanisms to ensure that obligations to protect data are observed by all who process the data, irrespective of where that processing occurs. To achieve this for the cloud a *chain of responsibility* needs to be built through the cloud service supply network starting from the cloud service users, which can be overseen by regulators, auditors and business governance. This is achieved not only by legal means and contracts, but also by technology and well defined corporate governance rules together providing trusted services supporting

[73] http://www.cloudindustryforum.org/governance-framework
[74] http://www.enisa.europa.eu/act/it/library/deliverables/pat-study

accountability. These address stakeholder requirements. A4Cloud provides a framework and technologies enabling accountability for how personal and confidential data is used in the cloud.

Accountability is then the result of complying with a combination of public (external to ecosystems) and private (internal to ecosystems) accountability criteria. Public accountability criteria are derived from transparent interaction (between subjects of personal data, regulatory bodies and data controllers), legislation, regulation, on-going Privacy Impact Assessments (PIAs), audit, public policy, and other relevant aspects of regulatory regimes. Private accountability criteria are derived from interactions between data controllers and data processors (premised on contract law, technological processes and practical internal compliance requirements) in cloud ecosystems (Charlesworth & Pearson, 2012). The A4Cloud project is also concerned with the investigation of how the same mechanisms might apply for personal and confidential data (including sensitive 'special category' info, location info, etc.). On the one hand, regulatory regimens constrain governance. On the other hand, cloud ecosystems need to comply with different regulatory regimes. Accountability enables cloud ecosystems to comply with regulatory regimes while deploying services. Accountability enhances the confidence on compliance with respect to regulatory regimes as well as trustworthiness of cloud supply chains. Figure 25 shows how our model of accountability fits within the overall accountability model for cloud service provision. Actors within cloud ecosystems use mechanisms to support accountability practices, and thereby help them to comply with relevant regulatory regimes within specific application domains.

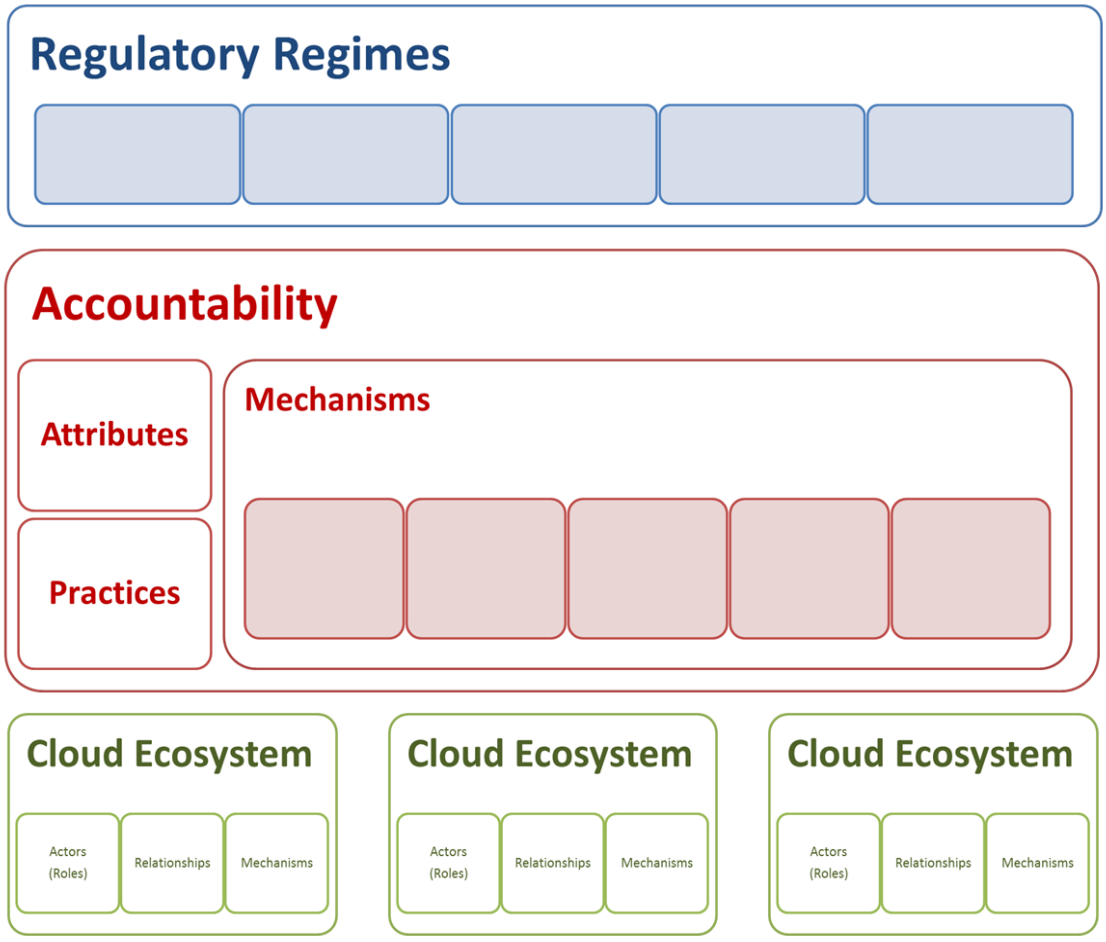


Figure 25 Context of Accountability Support for the Cloud

Accountability entrusts organisations with the practical aspects of complying with data protection obligations, and so there is this element of choice to help facilitate compliance, but also the necessity for proof that what has been done is both appropriate and is operating effectively. The legal and contractual context defines obligations, responsibilities and liabilities of actors in a given cloud ecosystem. Businesses need to meet these obligations, as well as obligations and requirements

imposed by other stakeholders that include customers and data subjects. Accountability can help them to mitigate risk and uncertainty in dynamic and global environments, clarify what their obligations are and help them meet these. It also helps provide transparency, including an account that is trusted in the sense that it provides improved evidence about the degree of compliance with these obligations. Achieving this is a challenging problem especially where service provision chains are complex. Figure 25 shows graphically the accountability model as supporting (compliance) relationships between regulatory regimes and cloud ecosystems. Note that the mechanisms within the accountability model here should be viewed as a kind of 'toolbox' from which organisations can choose in order to implement accountability, as ultimate practical means of accountability may differ according to the type of cloud, and indeed some cloud ecosystems will use certain mechanisms and not others.

Different domains adopting the cloud (which may be thought of in terms of cloud ecosystems in which multiple parties are interacting to provide cloud services, potentially including relationships between cloud ecosystems) would benefit from a general accountability framework, which enables them to address relevant regulatory regimes. Such a framework would support diverse mechanisms and technological artefacts throughout emerging chains of accountability. The next section introduces the A4Cloud's Accountability Framework. The Accountability framework enables organisations to operationalise accountability. It provides a systematic way of structuring different interventions supporting accountability in the cloud.

6.3 Accountability Framework for the Cloud

In this section an accountability framework for the cloud is presented that forms the basis of the research carried out within the A4Cloud project. It describes the project's high level approach and how a combination of legal, governance and technical measures are used to enable chains of accountability to be built along cloud service provision chains. The aim in particular is to strengthen the accountability of organisations that use cloud services and organisations that provide cloud services to data subjects and regulators (in conformity with the project scope as defined within Section 1.1). This section introduces an accountability framework that is based upon the accountability model defined in Section 5. The Accountability Framework supports:

- assessment of potential **co-design** of mechanisms from different disciplines (i.e. legal, regulatory, procedural and/or technical)
- provision of **flexibility** in our approach, including 'intelligent accountability' in complex environments and incorporation of varying degrees of accountability according to the context
- assessment of **accountability in different cloud delivery and deployment models**; possibly, this could include identification of patterns and capabilities that are suitable for specific cloud computing contexts (e.g. private cloud vs. public cloud, storage-based cloud vs. flexible computing ones, etc.)
- contribution towards high-level design and architecture– mapping across to **requirements for functional components** within systems that provide accountability and starting to build a high-level, logical design structure and explaining how the component parts work together.

This section highlights that the emerging A4Cloud's accountability framework enables cloud ecosystems to comply with relevant regulatory regimes within specific application domains. It clarifies what is considered to be beyond the scope of the A4Cloud's accountability framework. This makes any aspect of the project manageable (e.g. by focusing on the use cases). This section also explains how the emerging A4Cloud's accountability framework supports the analysis of cloud ecosystems and emerging issues (e.g. data protection issues), as considered further in the following section.

6.3.1 High Level Approach

Accountability promotes implementation of practical mechanisms whereby legal requirements and guidance are translated into effective protection for data. Legislation and policies tend to apply at the data level, but the mechanisms can be at various levels, including the system level and data level. A toolbox of measures could be provided for data controllers, to allow construction of custom-built solutions, whereby the controllers might tailor measures to their context (taking into account

consideration of the systems involved, type of data, data flows, etc.). We can co-design legal mechanisms, procedures and technical measures to support this approach. We may integrate design elements to support: prospective (and proactive) accountability, using preventive controls, and retrospective (and reactive) accountability, using detective controls.

- **Preventive Controls –** *Preventive controls* can be used to mitigate the occurrence of an action for continuing or taking place at all (e.g. an access list that governs who may read or modify a file or database, or network and host firewalls that block all but allowable activity). The cloud is a special example of how businesses need to assess and manage risk better (Baldwin & Shiu, 2010). Preventive controls for cloud include risk analysis and decision support tools (for example, Privacy Impact Assessments), policy enforcement (for example, machine readable policies, privacy-enhanced access control and obligations), trust assessment, obfuscation techniques and identity management.
- **Detective Controls –** *Detective controls* are used to identify the occurrence of a privacy or security risk that goes against the privacy or security policies and procedures (for example, intrusion detection systems, policy-aware transaction logs, language frameworks and reasoning tools). Detective controls for the cloud include audit, tracking, reporting, and monitoring.
- **Corrective Controls –** In addition, there are *corrective controls* (e.g. an incident management plan, dispute resolution), which are used to fix an undesired result that has already occurred. These controls complement each other: a combination of these would ideally be required in order to provide accountability.

Provision of accountability would not just be via procedural means, especially for cloud, which is such an automated and dynamic environment: technology can play an important role in enhancing the solution (by enforcing policies, providing decision support, assurance, security, etc.). Procedural measures for accountability include determining the capabilities of CSPs before selection, negotiating contracts and Service Level Agreements (SLAs), restricting the transfer of confidential data to CSPs and buying insurance. Organisations should also appoint a Data Protection Officer, regularly perform privacy impact assessments on new products and services, and put mechanisms in place to allow quick response to data subject access and deletion requests. Technical measures for accountability can include encryption for data security mitigation, privacy infomediaries and agents to help increase trust. We also need to be able to rely on infrastructure to maintain appropriate separations, enforce policy and report information accurately.

6.3.2 Description of Framework

It could be argued that the current regulatory structure places too much emphasis on remediation of problems (e.g. privacy breaches), and not enough on trying to get organisations to ‘do the right thing’ for data protection in the first place. Our approach in A4Cloud is the provision of a hybrid accountability mechanism via a combination of policies, regulatory and technical means. It is a co-regulation strategy based on a corporate responsibility model underpinned primarily by contract. This approach places the onus upon the data controller to take a more proactive approach to ensuring compliance, and encourages cloud service vendors and subcontractors to compete in providing services on the basis of evolving better privacy and security enhancing mechanisms and processes.

Correspondingly, in A4Cloud we build upon the accountability proposals discussed above and extend these to include prospective effects, that is to say, proactive rather than just reactive measures. This is because the policies by which we are judging our actors are constantly changing, the context and technological environment is changing and privacy-related harms to individuals (as for example detailed within (Solove, 2009)) are not equal. It is necessary to provide mechanisms to determine liability in the event of a breach, but we also (from the point of view of the data controller or PSP) build in processes and reinforce good practices such that the liability does not arise in the first place. Specifically, we suggest ways in which an organisation might take an ‘accountability’ approach further in order to develop a reflexive privacy process that is not simply a static compliance mechanism but rather that involves an on-going process of data protection monitoring and review and improvement throughout the contractual chain (Section 8 assesses what the contextual factors are and how variations can be taken into account in our model). Reflecting this approach, see Figure 26, services supporting accountability can be:

- **Preventive** – investigating and mitigating risk in order to form policies and determine appropriate mechanisms to put in place; putting in place appropriate policies, procedures and technical mechanisms
- **Detective** – monitoring and identifying policy violation; putting in place detection and traceability measures
- **Corrective** – managing incidents and providing notifications and redress.

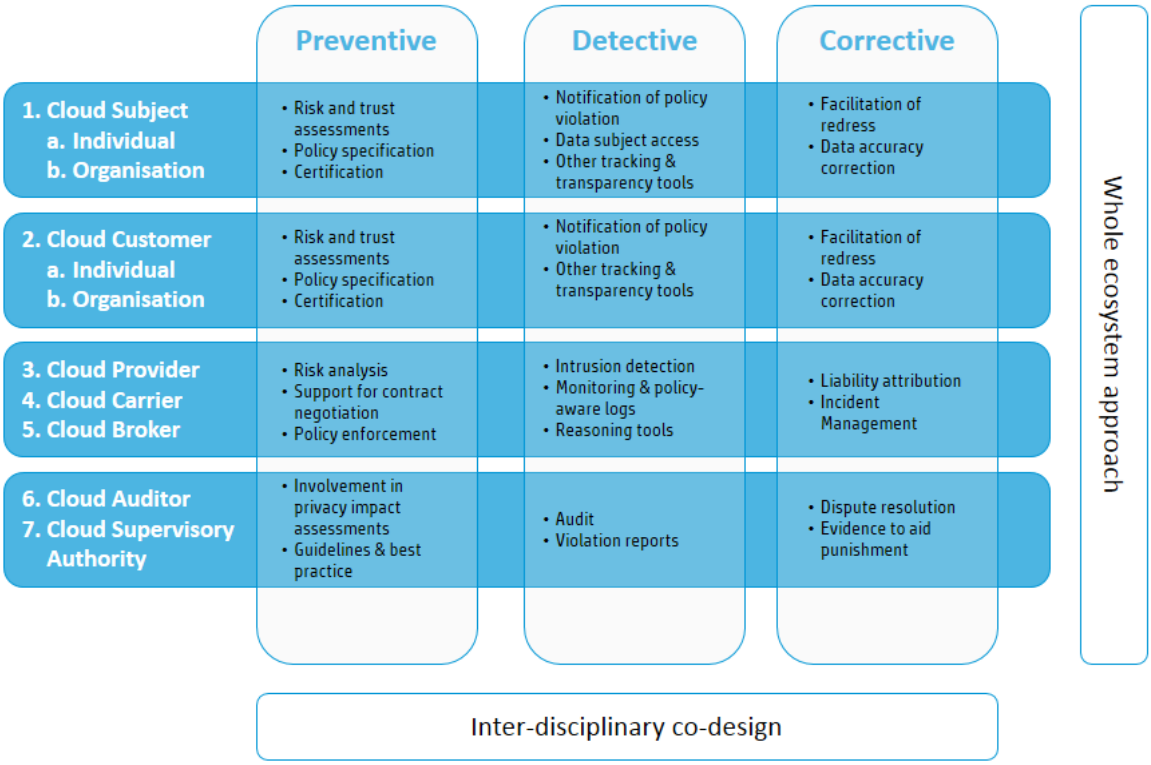


Figure 26 Accountability Framework

Figure 26 shows some examples of such services. These are not a complete set of accountability services, but broadly speaking map to the trusted services supporting accountability that are being developed within A4Cloud or that relate directly to those. Other services could be provided and would fit into this framework, such as incident management, identity management services and certification. We aim to provide benefits and tools for a range of different stakeholders, shown here in the rows of the grid of Figure 26. This would include:

- Technology-providers, e.g. partners, standards groups (like CSA and ENISA)
- Infrastructure providers, e.g. shared infrastructure CSP
- Service providers, e.g. SMEs acting as CSPs (data processor), primary service provider using CSPs (data controller), large companies acting as data processor, managed services
- Trusted third parties, e.g. TTP providing certification services
- Insurance providers
- Service users
- Auditors
- Data subjects, e.g. end users or. Employees
- Regulators, e.g. DPAs, EU Commission
- Other intermediaries, e.g. consumer groups, brokers.

In Section 8 we consider how this model would vary according to context, and what the relevant parameters would be. Related questions include investigating: to what extent the same mechanisms apply for personal data, confidential data, sensitive info, location info, etc.; how we can put intelligence into accountability; what should underlie all scenarios, and what should vary, in terms of accountability; what guidance can be given in terms of appropriate levels of external assessment and certification for

different contextual types. The functional aspects of accountability may be achieved by mechanisms in the following way:

- ***proper allocation of responsibilities*** – via management support, allocation of responsibilities for data protection within an organisation and clarification of responsibilities across supply chains
- ***definition of the contextual obligations to be followed*** (carried out by organisations and reflecting stakeholder and regulatory requirements)[75] – via formation of appropriate organisational policies, contracts, stakeholder engagement
- ***risk and trust assessment to decide which mechanisms to use in the given context to meet the policies*** – via risk identification/assessment, trust assessment, appropriate choice of business partners
- ***deployment of appropriate privacy and security controls*** (these are the mechanisms determined above and include means to make uses transparent to individuals and to assure that their rights are respected) – via security and privacy best practice, including transparency tools
- ***monitoring data practices*** (by organisations and by regulatory oversight)[76] – via tracking tools
- ***detection of policy violations*** – via audit and violation detection tools (e.g. evidence collection)
- ***correction of policy violations***[77] - via remediation and/or compensation[78]
- ***reporting of policy violations*** – via breach notification and transparency tools
- ***demonstration of policy compliance*** (including that policies defined by organisations are appropriate, the mechanisms used are appropriate for the context and that the operational environment is satisfying the policies)[79] – via provision of trustworthy account, verification (about appropriate use of privacy and security controls), certification, provision of evidence about satisfaction of obligations along service provision chains, transparency tools

Not only are mechanisms to achieve this run within different types of organisation, but others are kinds of meta-mechanisms that can bridge across organisations, for example helping with clarifying responsibilities, or with the verification process.

6.3.3 Co-Design

In order to realise accountability, we believe that there should be an interdisciplinary approach, which involves consistent and coordinated development across three main dimensions:

1. Responsible, ethical corporate governance
2. Innovative regulatory frameworks and
3. Supporting technologies.

Hence, legal mechanisms, procedures and technical measures need to be co-designed to support this approach. In particular, elements need to be designed to support retrospective (and reactive) accountability in addition to prospective (and proactive) accountability. Accountability can be retrospective in the sense that, if actor A performs action B, then we can review B against a predetermined policy to decide if A has done something wrong, and so hold A accountable; this is a mixture of detective and corrective aspects. Prospective accountability involves other aspects, such as achieving a proportionate and responsive process for reacting to context-dependent privacy risks. These elements will be designed such that they can be deployed individually, or in combination to greater

[75] These link to relevant external criteria and should correspond to organisational policies that are supported by senior management. The policies include specification of the entities involved in the processing of data and their responsibilities; the scope and context of processing data; the purposes and means of processing and data handling and data access policies. The policies need to take account of relevant external legal obligations. In addition, policies need to be defined related to risk monitoring and risk mitigation.

[76] This includes how organisations process data, evidence that the organisation has acted according to its policies, and a running account that is a record of the monitoring and its results. In particular, periodic internal reviews are needed to provide assurance that the mechanisms are working and improve over time.

[77] This includes both the effects of the violation that need to be addressed, as well as causes of the violation that need to be addressed, and the informing of appropriate stakeholders, who include authorities, customers and affected data subjects. The effects of the violation could involve errors that need to be corrected and damages that need to be compensated, financially or otherwise.

[78] Note the link also here to punishment.

[79] Policy violations need to be reported and compliance with policies needs to be demonstrated in a timely fashion, reactively and where possible, proactively. The organisation must demonstrate that the controls selected and used within the service provision chain are appropriate for the context and should provide evidence that the operational environment is indeed satisfying the policies. There must be openness to oversight by enforcement agencies, together with remediation if the goals of data protection have been abused in a harmful fashion.

effect. For example, an “accountability by contract” approach can be used in conjunction with machine-readable policies propagated with data through cloud as well as with integrated risk assessment that can help determine what the policies should be. In general, consumers of cloud services might (in some circumstances) define policies to include details relevant to the particular cloud service, namely:

- Type of data collected/uploaded
- The ways in which collected data will be used
- Location of processing
- Recipients
- Retention periods
- Backup
- Recovery/security.

There might also be policy obligations between providers in the cloud services chain, captured within the contractual agreements (and/or via machine readable policies, as considered further below), The idea is that the machine readable policy would be adapted to reflect the privacy and security requirements/restrictions that the PSP wants to ensure flow through the chain, such as:

- Limits on data collection from each user by a subcontractor
- Limits on permitted use
- Limits on the types of recipients/authorised recipients and notification of disclosures
- Limits on data transfers/location of processing
- Data retention requirements
- Data portability requirements
- Back up /recovery/security standards and controls.

More detailed human readable policies could be referenced in the contract. Technological means could be used to enhance this approach (as discussed at a high level in the following section, and as reflected within the work of D3 for example).

6.3.4 How Technology Can Strengthen the Notion of Accountability

Technology can provide assistance in ensuring proper implementation of accountability. In particular, technology can be used to strengthen the enforcement and monitoring of policies and to help provide evidence, assurance and transparency. Other technological means for accountability include policy-aware transaction logs; non-repudiation and immutability mechanisms; a language framework; reasoning tools; audit; obligation management; service level agreement (SLA), trust and incident management; selective information exchange. In this respect, A4Cloud is focused overall on the development of information accountability technology aimed at the technical ability to hold both data controllers and information processors accountable for their storage, use and dissemination of third-party data. In terms of the key elements of accountability identified in Section 2, technology can provide support in the following ways:

- *Responsibility and liability attribution* – e.g. revealing which component is responsible for automated notification
- *Transparency* – data tracking mechanisms, automated notifications, policy assessment tools, HCI, policy mapping, etc.
- *Assurance* – allowing users, operators and third parties to verify a posteriori if the system has performed a data processing task as expected (validation); providing evidence that can be used to convince a third party that a fault has or has not occurred; providing evidence as input to certification schemes.

Hence, in accordance with Recommendation 5 from (Castelluccia et al., 2011), our approach is that privacy assessment, assurance, verification or enforcement should be evidence-based, and that these evidences might be derived from a number of sources, events and traces at different architectural layers. One area where technology is very beneficial for privacy management in particular is in helping to provide risk assessment tools. An important part of any organisational privacy management programme is to conduct regular risk assessments to ensure compliance with applicable legislation and company policies. This is because privacy risks change over time, and new services might be provided that collect, use or disclose personal information and that have not been thoroughly vetted from a privacy

perspective — it is much better to minimise privacy impacts in this way before deploying or changing services rather than having to fix privacy problems after they have occurred. Some technological mechanisms for accountability that have already been developed are discussed in (Pearson & Wainwright, 2012), including privacy impact assessment systems that can help enterprises reduce privacy risks (Pearson, 2012). One specific example of how technology can strengthen the notion of accountability is that it can help enforce privacy obligations along the service provision chain. Furthermore, other technological approaches including Design for Privacy are complementary to accountability although not part of accountability in itself (Cavoukian et al., 2010).

6.3.5 Proactive Versus Reactive Measures

Weitzner and others have argued that to provide accountability, we must shift from hiding information to ensuring that only appropriate uses occur (Weitzner et al., 2008). Information usage should be transparent so that we can determine whether a use is appropriate under a given set of rules. A history of data manipulations and inferences can be maintained (providing transparency) and can then be checked against a set of policies that are supposed to govern them (providing accountability). This provides retrospective accountability, in the sense that if actor A performs action B then we can review B against a predetermined policy to decide if A has done something wrong, and so hold A accountable.

However, we do not adopt this approach as we consider it important to also include proactive measures for accountability that avoid transfer of personal data in risky situations. We want to extend this approach to include prospective effects, for example, because the environment may change. We want to reduce the risk of disproportionate harm to data subjects, and thereby reduce negative consequences for the data controller(s). To do this, we build in processes and reinforce good practices such that we can try to avoid liability arising in the first place (Pearson & Charlesworth, 2009), but nevertheless we still want the appropriate actors to be held liable in case of damages. This is a reflexive privacy process, which is not static and where there is an ongoing assessment of harm and process of privacy review throughout the contractual/service provision chain. Further discussion about the role of risk analysis as part of accountability is given below and in Section 2.

6.3.6 To what Extent should Good Practice reduce Penalties for Data Breaches?

There is an interesting distinction that can be made with respect to organisations putting mechanisms in place such that liability is very likely to be avoided (something that can be encouraged by accountability), versus holding an organisation to account if there is a privacy breach or similar violation (which is central to the notion of accountability). It seems that both aspects are important. However, there is a variation in opinion as to the extent to which good practice should reduce penalties if a data breach actually occurs: for example, Malcolm Crompton argues that the penalties should still be strong (Crompton, 2006), and rather having the mechanisms in place will reduce the risk of the beaches occurring, whereas others argue that the penalties should depend more on the mechanisms used rather than the degree of harm. In particular, Article 79 2a of the proposed GDPR says that “If the controller or the processor is in possession of a valid ‘European Data Protection Seal’ pursuant to Article 39, a fine pursuant to paragraph 2a(c) shall only be imposed in cases of intentional or negligent incompliance.”

Certainly, holding to account in the event of a data breach is a central part of accountability, so that someone essentially ‘carries the can’. Hence a person can be held accountable for some events that cannot easily be foreseen or controlled. Furthermore, within A4Cloud we hope to prove (given some base assumptions) that some systems that use the mechanisms provided by A4Cloud will behave in a particular way, and so are trustworthy/reliable to that extent. In the A4Cloud project, our framework assumes that it is very likely that there will be a data protection breach at some stage in the data management lifecycle, and that we are planning to reduce the risk, to enhance the observability and to enable the mechanisms for redress.

6.3.7 The Role of Risk Analysis

Risk assessment is particularly important for accountability, as it is a central part of the process used to determine and demonstrate that the policies that are signed up to and the corresponding practices that are implemented by an organisation are effective and appropriate to the context. On-going risk

assessment and mitigation relating to new products or processes, as well as regular risk assessment and validation of the accountability program, are core elements of implementing an accountability program within an organisation (Galway project, Canadian Privacy Commissioners). Moreover, the role of risk assessment is increasingly recognised as useful within global and dynamic environments in reducing risks (e.g. OECD). The type of procedures and mechanisms that would be appropriate vary according to risks dependent upon in particular the processing and the nature of the data.

As considered above, accountability, as articulated by the Article 29 Working Party (European DG of Justice, 2010), begins to shift our thinking from only having an obligation to comply with a principle, to an obligation to prove that you can put those principles into effect. Hence risk assessment (a core security process) is particularly important for accountability because it is a central part of the process used to determine and demonstrate that the policies (whether reflected in corporate privacy and security policies or in contractual obligations) that are signed up to and implemented by the organisation (that is taking an accountability-based approach) are appropriate to the context. The type of procedures and mechanisms vary according to the risks represented by the processing and the nature of the data (CNIL, 2012; Catteddu, Hogben, 2009; Castelluccia et al., 2011; Pearson, 2012). Automation can enhance this process (Pearson, 2011). Data impact assessment may also become an obligation for some high risk contexts within the GDPR (cf. Article 33: EU, 2012).

On-going risk assessment and mitigation relating to new products or processes, as well as regular risk assessment and validation of the accountability program, are captured within the core elements of implementing an accountability project within an organisation specified within the Galway and Paris projects, which were (CIPL, 2009; CIPL, 2010). These core elements of implementing an accountability project within an organisation (CIPL, 2010), are very similar to the guidance provided by the Privacy Commissioners of Canada, Alberta and British Columbia (Office of the Information and Privacy Commissioner of Alberta et al., 2012), which also emphasises the need for risk assessment, as does the revised OECD guidelines (OECD, 2013), which now recommend the practical implementation of privacy protection through an approach grounded in risk management and stress the need for improved global interoperability.

Risk assessment within an organisation can potentially be extended to encompass both pre-emptive approaches (to assess risk and avoid privacy harm) and reactive approaches that provide transparency and audit. And the privacy policies and mechanisms need to take into account the entire life cycle. Companies need to think about what data they will collect and how they plan to use it, but also what are the potential harms (or surprises) for individuals. It is the data subject that is the real owner of data, who ultimately is harmed in case of failure and who should be empowered and supported. For example, if you are tracking someone online then under an accountability approach you might include clear notice that tracking is happening, how the tracking data will be used, as a mechanism for individuals to choose not to be tracked and to request previous tracking data to be deleted. PIAs are regarded as an essential tool for implementing the Accountability Principle and demonstrating compliance, as espoused within the Art. 29 WP Opinion 3/2010 on the Principle of Accountability (DG of Justice, 2010) and the GDPR (EC, 2012), where PIAs based on self-verification by or on behalf of data controllers are proposed for higher risk data processing operations, The Art. 29 WP Opinion 3/2010 on the Principle of Accountability states that:

> *"As a complement to the principle, specific additional requirements aiming at putting into effect data protection safeguards or at ensuring their effectiveness could be set up. One example would be a provision requiring the performance of a privacy impact assessment for higher risk data processing operations"*

Furthermore, PIAs are encouraged within the Madrid Resolution 2009 (Int. Conf. of DP and Privacy Commissioners), the UK Information Commissioner's Office PIA Handbook (2007) and draft Code of Practice on Conducting PIAs (2013), the Art. 29 WP Opinion 9/2011 on a PIA Framework for RFID Applications, the European Commission's Recommendations on preparations for the roll-out of smart metering (2012).

In addition to this, data impact assessment may also become an obligation for some high risk contexts within the forthcoming GDPR (cf. Article 33: EC, 2012). In the proposed GDPR (2012), Art. 33 introduces

a risk-based approach to PIAs (DPIAs). Prior to processing of personal data, a DPIA is required if the processing is likely to present specific risks for the rights and freedoms of data subjects, taking into account the nature, scope and purpose of the data processing. However, there is still no consensus on the final legal provisions.

Existing organisational risk assessment processes need to be enhanced to meet the requirements above, or else supplemented with separate privacy-specific risk assessment (Trilateral, 2013). Privacy impact assessments are already being rolled out as part of a process to encourage privacy by design (ICO, 2007): in November 2007 the UK Information Commissioners Office (ICO) (an organisation responsible for regulating and enforcing access to and use of personal information), launched a Privacy Impact Assessment (PIA) (ICO, 2007) process (incorporating privacy by design) to help organisations assess the impact of their operations on personal privacy. This process assesses the privacy requirements of new and existing systems; it is primarily intended for use in public sector risk management, but is increasingly seen to be of value to private sector businesses that process personal data. Similar methodologies exist and can have legal status in Australia, Canada and the US (Tancock et al., 2010). The methodology aims to combat the slow take-up to design in privacy protections from first principles at the enterprise level. Usage is increasingly being encouraged and even mandated in certain circumstances by regulators (Tancock et al., 2010).

Risk assessment must be extended right along the service provision chain: in order to implement a chain of accountability for the non-functional attributes of an ICT system, it must be possible to measure those attributes in a meaningful way. However, this is non-trivial. For example, liability assignment is currently particularly difficult in an international context where business relations are negotiated and regulated by contracts, and there are differences among the countries with respect to legal framework and regulations. Furthermore, it is very difficult and resource-demanding to detect and then prove that electronic data has been compromised and to identify the perpetrator. What is reported to the police is just a small percentage of all violations detected[80]. In addition, risk allocation is (for large deals) negotiated individually in contracts, so that a single provider will have a different risk allocation scheme with each of its major customers. Law and regulation differs between countries, so that there is no single scheme of risks to be addressed, or single view on liability if those risks eventuate.

Current risk assessment methods have not been designed for use in a cloud computing setting, and there is at the moment no methodology or tool developed for assessing and predicting risks related to accountability of cloud services. Even in a non-cloud environment, automation of privacy impact assessment is not yet mature (Sander & Pearson, 2010; Pearson & Sander, 2011).

Practical challenges include whether objective or subjective harm can be used as a basis for evaluation, and how this could be encoded. For example, the classification of harm according to Richard Thomas (Centre for Information Policy Leadership) encompasses three different elements:

1. Material (tangible) harm to individuals
2. Moral (non-tangible) harm to individuals
3. Harm to democratic and societal values of a free society.

An additional challenge relates to what the **evidence** looks like that is provided by DPIAs to external parties, and how important organisational criteria and choices in this decision making process can get exposed to other parties. Related to this issue, self-verification through PIAs could involve a transparency duty with regard to the outcome of the PIAs (e.g., public PIA registers), but this is not even specified from the regulatory side and the situation is unclear. A further challenge relates to the way in which verification is provided that the measures used (potentially across a supply chain network) are appropriate for the context.

In A4Cloud, risk analysis is a preventative accountability measure that helps prevent risky actions happening. It is also used to demonstrate how the security and privacy mechanisms used are appropriate for the context. CSP chains should be taken into account within the analysis. Accountability functionality must also be part of the solution, so accountability requirements should be part of the output

of the DPIA, together with the demonstration above. The main challenges for A4Cloud with regard to risk assessment include: risk assessment across CSP chains; assessment of social harms; output as part of a design process and output as part of the account/verification process.

6.4 Functional Analysis of Accountability

As discussed above, organisations need to use privacy and security controls appropriate to the context, but they may also use a number of accountability tools that complement these. These accountability tools may form a toolbox from which organisations can select as appropriate. They can be (extensions of) existing business processes like auditing, risk assessment and the provision of a trustworthy account, or non-technical mechanisms like formation of appropriate organisational policies, remediation procedures in complex environments, contracts, certification procedures, and so on. Or they can be technical tools, which would include tracking and transparency tools, detection of violation of policy obligations, notification of policy violation, increased transparency without compromising privacy, and so on. The tools are targeted at different stakeholders, and some are designed for usage as a preventive measure (for example, to assess and reduce privacy harm before personal data is collected), some as a detective measure (for example, to assess the degree to which privacy obligations are actually being met) and others as a corrective measure (for example, to facilitate redress).

6.4.1 Key Functional Aspects of Accountability

A functional analysis of accountability may be derived from the definition of accountability given above in Section 2, which maps to what are called accountability practices in Section 5 and indeed to the Galway project elements of accountability. The core elements of implementing an accountability project within an organisation specified within the Galway and Paris projects were (CIPL, 2009; CIPL, 2010) (with our emphasis):

1. **Policies** that reflect current laws and relevant standards
2. **Executive oversight** and **responsibility** for privacy
3. **Delegation** of responsibility to trained resources**; education** of staff and suppliers
4. On-going **risk assessment and mitigation** relating to new products or processes
5. Regular risk assessment and **validation** of the accountability program
6. Policies to manage major privacy events or complaints
7. Processes to **enforce policies** internally
8. A method of **redress** if privacy rights are breached

These core elements of implementing an accountability project within an organisation (CIPL, 2010), are very similar to the guidance provided by the Privacy Commissioners of Canada, Alberta and British Columbia (Office of the Information and Privacy Commissioner of Alberta et al., 2012), as considered further within Section 2. An accountability-based approach can be broken down into the following **key functional aspects of accountability**:

1. Clarification and acceptance of responsibility for data protection obligations (in a given context)
2. Determination of appropriate measures, e.g. security and privacy best practices; risk identification and mitigation
3. Implementation of chosen measures
4. Provision of an account:
    a) Demonstration that measures used meet obligations
    b) Validation of the operation
    c) Attribution of failure
5. Monitoring what actually occurs – internally and externally
6. External verification (including assessment of the account in the context of the enforcement process in relation to the satisfaction of obligations)
7. Notification (e.g. of an incident or data breach)
8. Remediation (including punishment)

Figure 27 shows the different functional elements of accountability bridging the conceptual and implementation views of accountability – it emphasises how we moved from an abstract and conceptual analysis of accountability (in terms of attributes) towards a concrete implementation of tools and the demonstration of accountability. Transparency can be an aspect of many if not all of these elements.

These functions are realised at different phases within an organisation's operational lifecycle (as explained in Section 7).

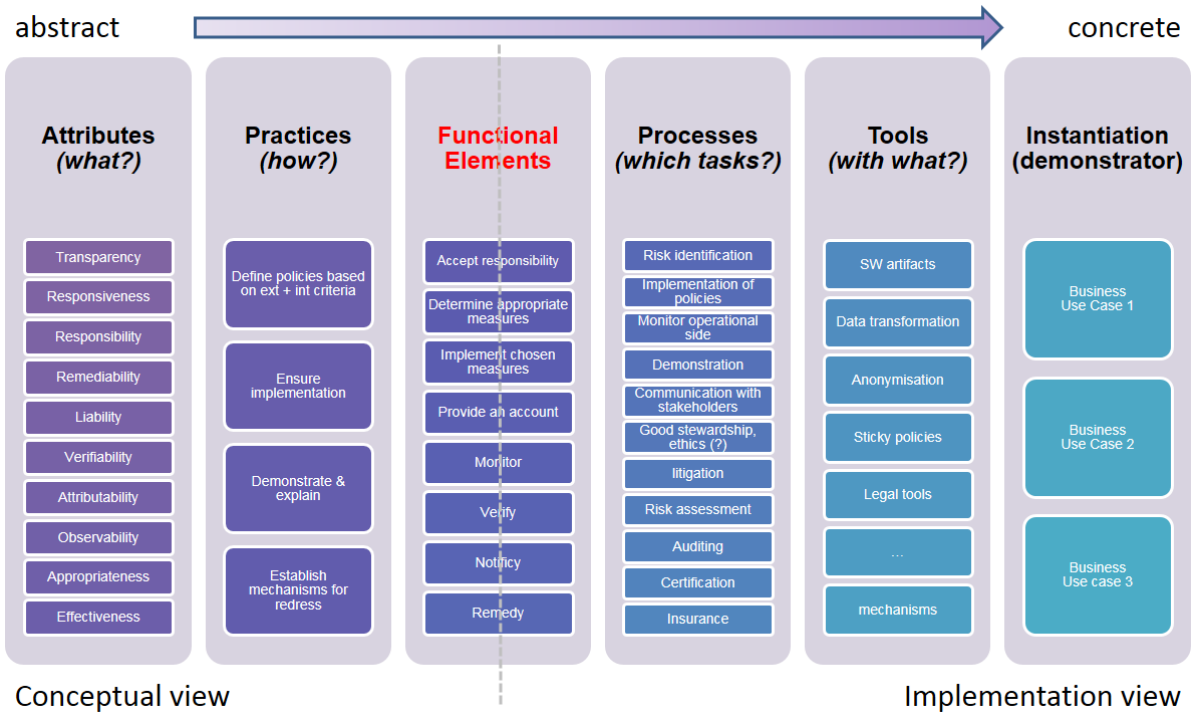


Figure 27 Different Views of Accountability

Different accountability functions are triggered at different phases of an organisation's operational security lifecycle, and how some of these (namely attribution of failure, notification and remediation) are triggered within exception loops corresponding in this case to non-satisfaction of obligations, for example by a data breach. Thereby, it can be seen how there is involvement both of proactive elements (clarification and acceptance of responsibility, determination and implementation of appropriate measures and preparation of a demonstration that these meet the obligations involved for when it might be needed), as well as reactive elements (corresponding to detection and handling of data breaches or other non-satisfaction of obligations). At its core, in the sense that a data controller should be accountable for complying with measures which give effect to principles that have been set within a democratic context, and that they will be held to account in case of failure, as well as the provision of tools to help organisations to 'do the right thing' (including for better remediation, breach notification, etc.), accountability is obviously a good thing and not very controversial. However, there are a number of different and even conflicting opinions related to additional (or even alternative) potential features of an accountability-based approach. Mainly these relate to how accountability can help address the issue of the lack of take up of privacy by design by organisations to date, the role of accountability in moving towards greater regulatory interoperability, the importance of measures that prevent privacy harm and the extent to which punishment for a privacy violation should be lessened by evidence that appropriate privacy and security measures have been taken by an organisation. The former can be done in particular by easing transborder data flow constraints and regulatory complexity in favour of a single set of organisational requirements that need to be adhered to that could apply globally (as is the case with Binding Corporate Rules for instance (ICO, 2012)), allowing differentiation in terms of privacy (so long as legal requirements are met), being less prescriptive in terms of the specification of regulatory requirements, encouraging (or even mandating) usage of privacy impact assessments to guide design and also of course increasing punishment in cases of non-compliance as well as taking into account the controls an organisation has used when determining punishment. Opinions about the relative merits of these approaches differ. In addition, Weitzner views accountability as retrospective (arguing that a shift is needed from hiding information to ensuring that only appropriate uses occur) (Weitzner et al., 2008) whereas preventive risk identification and mitigation is viewed as an essential element of accountability by others (CIPL, 2009; OICPA et al., 2012).

It is often regarded as underpinning an accountability-based approach that organisations should be allowed greater control over the practical aspects of compliance with data protection obligations in return for an additional obligation to prove that they have put privacy principles into effect (see for example (Weitzner et al., 2008). Hence, that whole approach relies on the accuracy of the demonstration itself. If that is weakened into a mere tick box exercise, weak self-certification and/or connivance with an accountability agent that is not properly checking what the organisation is actually doing, then the overall effecte could in some cases be very harmful in terms of privacy protection. As Bennett points out (p. 45: Bennett, 2012), due to resource issues regulators will need to rely upon surrogates, including private sector agents, to be agents of accountability, and it is important within this process that they are able to have a strong influence over the acceptability of different third party accountability mechanisms. This can be achieved via independent testing of practices, provision of evidence that is taken into account, including auditing against the ISO 27001 series and associated security standards. Hence, the way in which accountability is achieved is key, which includes the need for adequate resources in checking and enforcing whether organisations are indeed using appropriate measures, involvement of different stakeholders, including the public (or representatives of the public) in data privacy regulation, provision of suitable accountability tools and help for organisations to form appropriate risk assessment mechanisms and policies.

6.4.2 How A4Cloud Mechanisms and Tools Support Accountability in the Cloud

This section explains how the A4Cloud mechanisms, as results of research and development activities within the project, are aligned with the accountability framework (and hence capture the accountability definitions and model) and support accountability in practice. Based on the A4Cloud definition of accountability, the relevant implementations aim to support this definition and enable the involved stakeholders in addressing accountability at all levels of abstraction, thus mapping the accountability elements in a human readable form, a machine-readable code and a lawyer-readable terminology. Figure 28 shows a functional model of the A4Cloud mechanisms and tools forming together the reference architecture supporting and implementing the accountability framework.

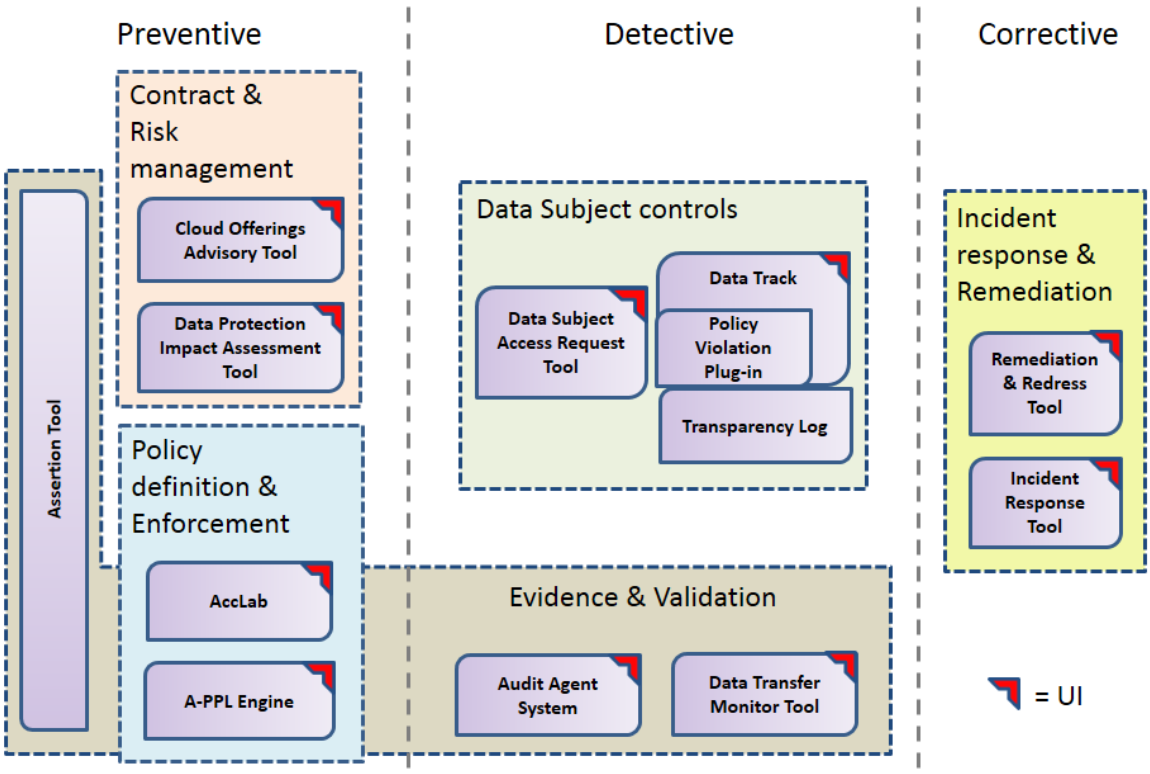


Figure 28 Functional Architectural Model of the A4Cloud Mechanisms and Tools

This figure shows how functional accountability elements, in the form of generic attributes of accountability and accountability practices bridge across to actual processes and techniques employed

within organisations, via functional building blocks of accountability (for data protection) defined at the organisational level. Thereby, the Accountability Conceptual Framework enables different mechanisms and tools, which combined together, form an architecture supporting chains of accountability in cloud ecosystems. This architecture is reflected along all the entities within the service provision chain. Note however, that it is not necessary that all of these functional elements are present in each organisation; these are just the elements needed in order for the A4Cloud accountability mechanisms to function in union. Furthermore, additional architectural elements will also be needed by the organisation in order to complement these, such as security functionalities, identity management, and others. Note that the same types of accountability mechanisms can be used by individuals as well as individuals (who may be cloud customers or cloud subjects who are interested parties without actually being directly users of cloud services) and organisational cloud customers. Appendix D provides further details about the way in which the A4Cloud tools relate to each other and support accountability, reflecting analysis carried out within the reference architecture (i.e. WP D-2). Policy configuration is used by cloud service users to define their accountability requirements in human readable forms, so that the proper privacy, confidentiality and data protection requirements can be expressed by non-ICT skilled users. These users are thus able to define their own policy preferences and communicate them to the cloud service providers. The latter can use policy configuration to extend specific policies on how their customers' data can be used in the cloud, as well as explain the responsibilities and obligations in policies following legal terminology.

Using policy enforcement, cloud service providers actually enforce the execution of the policies in the cloud and can compile logs of how policies are treated. This is achieved by translating policies in machine-readable code. As policies can be expressed in multiple machine-readable formats, interoperability must be supported in the policy specification part, which enables different kind of policy expressions to be mapped to each other. They can also exploit policy enforcement as a tool to control the delegation of accountability elements, as they are defined in the specific policies, in the supply chain. Contract support introduces mainly lawyer-readable terms to support users and service providers in identifying the contract terms that are appropriate to the context of use. Such a tool should also consider for mapping metrics for accountability, which will enable the evidence collection system to capture the most relevant information.

Accountability validation is exploited by cloud stakeholders as a tool to check that certain accountability elements are supported in a supply chain. Policies, which have been expressed by the policy configuration and are executed through the policy enforcement environment, have to be analysed and checked to specific accountability metrics so certain assertions over the support of accountability can be made.

Risk analysis offers assessment of the potential risks by using a cloud environment for a certain cloud service chain and the impact that these risks can have on this cloud service. A risk assessment tool can be based on risk models for the cloud, which combine the human readable risks identifications with the machine-readable policy specifications and risks' implications to a cloud service chain.

In order for accountability to be measured effectively, based on the relevant metrics, a system for evidence collection is provided, which can assess that privacy and confidentiality are preserved, and support audit and attribution. The evidence collection system is closely associated with the policy monitoring, which sniffs the cloud ecosystem transactions to verify that policy configuration is followed in the service chain and appropriate notifications are alerted when data usage is not compliant to contracts. When accountability metrics are not compliant with contracts, appropriate redress actions have to be adopted. A4Cloud provides remediation over loss of accountability, when the relevant metrics fall below the defined thresholds, as they agreed in contracts. Metrics are among the research developments from A4Cloud that will contribute to support accountability. From the perspective of the accountability framework, metrics are a means for demonstrating accountability practices, through the provision of quantifiable evidence of the application of such practices. In this case, accountability objects are the entities that are subject to measurement.

In other contexts, such as quality assurance, software development or project management, metrics are traditionally used as a tool for monitoring progress, assessing compliance, and facilitating and refining the decision making process within an organisation. Additionally, the adoption and systematic use of

metrics is an indispensable practice for organisations that strive to achieve a repeatable and optimising behaviour. Metrics also support accountability governance. The accountability process should assess accountability of an organisation in a systematic way, and the definition and use of specialised metrics are a means for achieving this. Measuring the behaviour of organisations is central to define an Accountability Maturity Model. In theory, a mature organisation (from the accountability perspective) should present a quantitative, and hence, measurable behaviour. Mature organisations are therefore characterised by an ingrained use of metrics within their internal processes.

6.5 Chains of Accountability in the Cloud

The principle of accountability needs to be supported across cloud supply chains. This requires establishing and supporting accountable relationships between cloud actors. Figure 29 highlights sample accountability relationships that arise due to the need to support accountability across cloud supply chains.

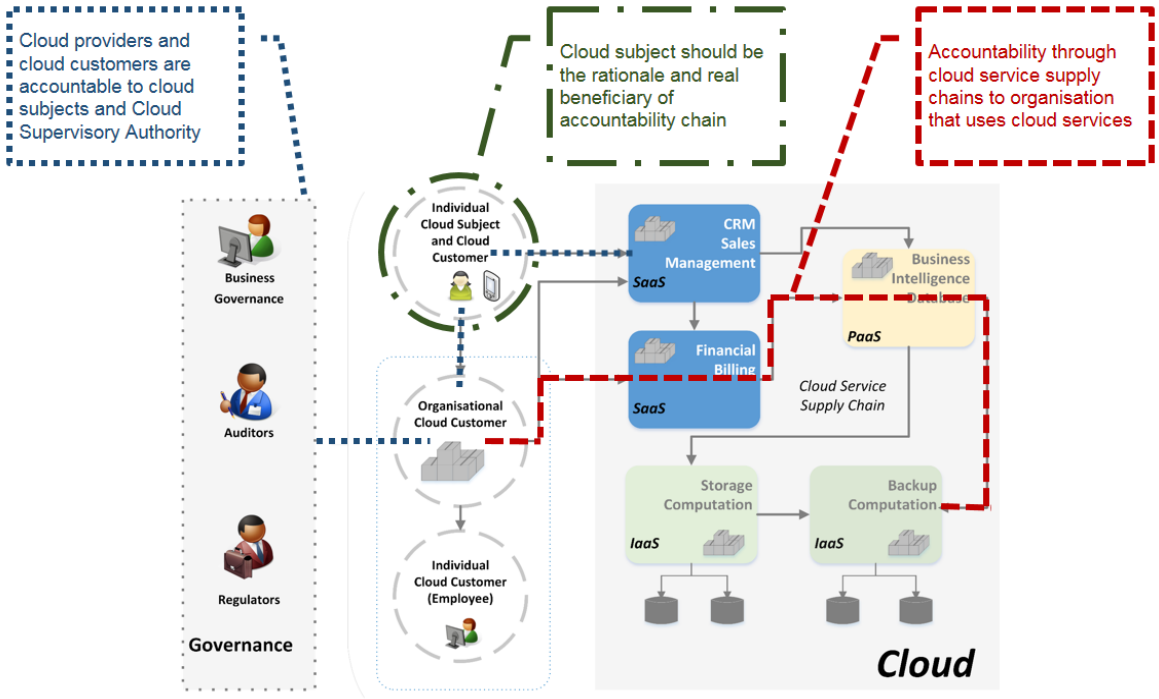


Figure 29 Emerging Accountability Relationships between Cloud Actors

First of all, it is necessary that accountability is supported throughout the cloud supply chain. Cloud providers nearly always act as Data Processor. They may need to assume co-controllership responsibilities, although they may not know who the users are or what their services are being used for. Data Processors are accountable for cooperation with Data Controllers to meet data subjects' rights, assist them (i.e. Data Controllers) in providing security measures, and act only on their behalf. Cloud Customers are in general considered Data Controllers, who are accountable to Cloud Subjects for applicable data protection measures. From a societal perspective, all actors involved in a cloud supply chain are ultimately accountable to Cloud Subjects. Appendix E provides further examples of accountability chains and mechanisms.

6.6 Avoidance of Potential Pitfalls of an Accountability-based Approach

There are a number of forces at work that can prevent a strong accountability-based approach, and a number of issues that have been raised around various aspects that could be associated with an accountability-based approach. In this Section we consider some of these, and how these objections might be mitigated or do not apply to our project approach.

6.6.1 Potential Issues

In this section we raise a number of potential issues that could be, or are already being, raised with respect to accountability-based approaches.

1. *The relationship of accountability with privacy:* The first viewpoint is that accountability shouldn't be viewed as a new principle that would reformulate the essential principles of privacy and data protection. A related concern by some people is the association of accountability with self-regulation, although this is not actually a necessary way of achieving accountability. The fear here is centrally about introduction of light-touch self-regulation by the back door, of data controllers promoting accountability in the hope of avoiding more constraining and comprehensive regulations, and of the proposal of accountability as a way to attack the notion of universal human rights espoused in EU and other countries.
2. *Trust in the verification process*: Another aspect to this concern relates to trying to avoid weak verification. As already considered earlier in this Section, there are trust issues if the levels of verification or certification are seen as low, in the same way as happened with the Safe Harbour programme, coupled with potential lack of trust in the verifier.
3. *Enforcement:* A third aspect is a worry about lack of enforcement that would make an accountability-based approach not work very well. This could be due to the fact that if there would be a lack of real consequences for the data controller breaching obligations then this would seriously weaken the approach: if an organisation wouldn't be caught then why would they pay to implement accountability measures? Currently there is rather a lack of funding for regulators to make the appropriate checks; there would also be a need for appropriate authority for any enforcement agencies involved.
4. *Increased risk:* It can be argued that the implementation of certain accountability measures themselves could introduce data protection risks, such as breach risks. For example, personal data would be included both in accounts and also in logs that are gathered for evidence. There are also risks related to falsification of information in accounts.
5. *Increased burden:* Due to greater costs and greater liability for organisations, especially those trying to use best practice, accountability may also impose unacceptable burdens on industry. This issue is addressed further in Section 10, as an 'intelligent' approach needs to be adopted to help avoid this.
6. *Social harm:* In terms of social harm, potentially there could be transfer of corporate responsibility to more junior staff, and it could be argued that there is a lack of role of individuals and public interest groups in the accountability process, except to make complaints. The wider scope of accountability and ethical organisational behaviour is considered further below.
7. *Cloud context:* Accountability is particularly hard to achieve in the cloud context, but that is actually a context where it is strongly needed. The main factors contributing to this are the current shallowness of transparency and verifiability in the cloud context (especially at the PaaS and IaaS layers), surveillance and potential weak links in dynamically formed cloud service provider chains.

The resultant objections culminate in a general *fear of a weak accountability approach* that can be characterised as 'privacy whitewashing', whereby accountability could encourage a false basis for trust by data subjects in data controllers. Accountability could be implemented by very light organisational measures that might just encompass something like appointment of a data protection officer together with executive oversight of a high-level plan. Such weak accountability could be adopted on a voluntary basis to avoid data protection obligations and keep costs down. Moreover, the basis for trusting self-verification or audits conducted by the organisation's business associates could be very weak: there could be inaccuracies and collusion, and even accounts that are forged by the controller to cover up privacy breaches or else that might be tampered with by other parties.

6.6.2 Required Characteristics

In order to address the points above, an accountability approach should be strengthened to have the following characteristics:

1. *The relationship of accountability to privacy:* Accountability should be viewed as a means to an end (i.e. that organisations should be accountable for the personal and confidential information that they collect, store, process and disseminate), not as an alternative to reframing basic privacy principles or to requirements in the GDPR, etc. Although the OECD principles already provide a 'one size fits all' approach for organisations to follow, further guidance about practices is nevertheless helpful, and the relationship between accountability and related concepts like privacy has been considered already in 2.2.3 above, where their potentially complementary nature is brought out.
2. *Trust in the verification process:* There needs to be a strong enough verification process to show the extent to which commitments have been fulfilled. Note however that missing evidence can pose a problem, and guarantees are needed about the integrity and authenticity of evidence supporting this verification and the account. In addition, the actor carrying out the verification checks needs to be trusted by the data subject and to have the appropriate authority and resources to carry out spot checking and other ways of asking organisations to demonstrate accounts. There are further related aspects supporting this approach in terms of responsibility and transparency, as listed below.
    a. *Clarity of responsibility:* The commitments of the data controller need to be well defined – this is (part of) the aspect of responsibility, that is an element of accountability. The commitments of the data controller should include all applicable legal obligations, together with any industry standards (forming part of the external criteria against which the organisation's policies are defined) and declarations made by the data controller in privacy statements (which may encompass any of the three types of obligations mentioned earlier in this Section). In the cloud context, this is particularly important as entities may have multiple roles, e.g. could be joint controller and processor. The responsibilities of the entities along the CSP chain need to be clearly defined, including relative security responsibilities.
    b. *Transparency:* The commitments of the data controller(s) need to be properly understood by the data subjects affected and other parties as appropriate – this is a key transparency aspect. In addition, the mechanisms used and relevant properties of the service providers in the provision chain need to be clarified as appropriate to cloud customers and regulators. Furthermore, DPIA/PIA is one form of verification for accountability (that should be used in conjunction with others!) that can be used to help provide transparency about the nature of the risk analysis, including the criteria used, how decisions are made to mitigate risk, and whether the mechanisms to be used/implemented are appropriate for the context
3. *Enforcement:* Strong enforcement, not only in terms of verification, but also in terms of the likelihood of being caught and strong penalties if caught, seems to be a necessary part of accountability.
4. *Increased risk:* Technical security measures can help prevent falsification of logs and privacy-enhancing techniques and access controls should be used to protect personal information in logs. In the project we are researching how to address the potential conflict of accountability with anonymity, but the issue is much reduced as our focus is not on the accountability of data subjects but of data controllers, who do not need to be anonymous.
5. *Increased burden*: Accountability must deliver effective solutions whilst avoiding where possible overly prescriptive or burdensome requirements.
6. *Social harm:* Accountability should have democratic and ethical characteristics. Related discussion is provided in Section 2.
7. Mechanisms should also be developed to help regulators do their job, notably with respect to enhancement of the verification process as discussed above.
8. *Cloud context*: With regard to the cloud context, addressing surveillance is largely out of scope of the project. If the data controller is ultimately made accountable for meeting obligations right along the service provision chain, they should try to obtain contractual assurances that lessen the risk of potential weak links in dynamically formed cloud service provider chains. The potential shallowness of transparency and verifiability in the cloud context, especially from Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) providers (Hon et al., 2011), is currently a problem but by development of solutions to provide an alternative and by market pressures it is hoped that this situation might be changed. Without this, it is indeed the case that accountability-based approaches in the cloud can only be relatively weak.

Butin and colleagues have introduced the notion of *strong accountability* (Butin et al., 2013), that: applies not only to policies and procedures, but also to practices, so that the effectiveness of the processing of personal data can be overseen; is supported by precise binding commitments enshrined in law and involves regular audits by independent entities. They assert that this should not be contradictory with the need for flexibility that is required by the industry. Our project approach is similar and is described further in the following section, and in Section 7.

6.6.3 A4Cloud's Strong Accountability Approach

In A4Cloud, we take a mixture of a strong and a soft accountability approach. The strong accountability approach is achieved in particular via:

- Being precise about what accountability means
- Moving beyond accountability of procedures, to accountability of practice
- Joining technical measures to enhance the integrity and authenticity of logs with enhanced reasoning about how these logs show whether or not data protection obligations have been fulfilled
- Including verification by independent, trusted entities (which could support external certification).

The soft approach relates to addressing how accountability can be achieved in a socially beneficial way, for example via democratic accountability considered in Section 2 above, the economic analysis as described in B-4 deliverable and the ethical governance considered in Section 2. Accountability then entails demonstrating what non-technical mechanisms are implemented in organisations to acknowledge societal norms and ethical issues related to cloud computing. The soft approach not only focuses on internal regulations (e.g. Codes of Conduct within organisations), but stimulates the externalisation of the internal regulatory work within these organisations (Codes of Conduct incorporate external stakeholders perspectives and are integrated in the entire organisation.

Overall, A4Cloud can provide greater analysis and evidence especially with regards to organisational risk assessment and analysis, and to demonstrating that what has been done is appropriate for the given context. It also needs to take into account reasoning about the service provision chains, and missing info. Metrics for accountability developed by the project can provide practical support for strong accountability via facilitating measurement of mechanisms, including both implemented controls and what is occurring operationally. They can raise the bar with regards to what is (or can be) in the account, help organisations produce evidence for the account and also helping third parties assess the account. In addition, better evidence and better analysis of evidence can be provided in particular via:

- Defining what evidence is needed for accountability
- Secure and trustworthy logs covering the evidence required
- A log analyser and framework that link obligations right through to lower level distributed evidence in cloud supply chains that show whether or not the obligations are met
- Incorporation of state of the art in distributed audit
- Tackling the issue of potential shallowness of evidence about treatment of personal data in the cloud, especially at the PaaS and IaaS levels .

The verification process for accountability can be enhanced via verification by third parties (about policies, practices and operational satisfaction of obligations), verification across service provision chains and input to appropriate certification schemes. For further details of the project's framework and approach, see Section 7.

6.7 Summary

Current regulatory structure places too much emphasis on recovering and not enough on trying to get organisations to proactively reduce privacy and security risks. New data governance models for accountability can provide a basis for providing data protection when cloud computing is used. Accountability is becoming more integrated into our self-regulatory programs as well as future privacy and data protection frameworks globally. If cloud service providers do not think beyond mere compliance and demonstrate capacity for accountability then there is a good chance that regulation may develop that will be difficult to follow and that may stifle innovation, or there could be a backlash from data

subjects. It is an upcoming challenge to strengthen this approach and make it more workable by developing intelligent ways in which accountability and information stewardship can be provided. This goes beyond traditional approaches to protect data, in that it includes complying with and upholding values, obligations, and enhancing trust. This section has introduced the A4Cloud Accountability Framework that addresses this need. The framework based on the accountability definitions and concepts enables different mechanisms and tools. These mechanisms and tools form together a reference architecture enabling cloud service provision and deploying accountability. This section shows how the A4Cloud Accountability Framework together with the mechanisms and tools supports chains of accountability in cloud service provision. It also discusses why and how the project takes a *strong accountability* approach.

7 Accountability Governance and Processes in the Cloud

This section builds upon the framework defined in the previous section, to explain further how organisations may implement accountability practices. While the benefits of using Cloud services in terms of flexibility and cost does not need to be demonstrated, the safe use of Cloud requires a strong set of policies, procedures, decision processes, guidelines, which must be coupled with a culture of responsibility. As identified by NIST, '*While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.'; in fact 'Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open deperimeterised organisational infrastructure – at the extreme, displacing applications from one organisation's infrastructure to the infrastructure of another organisation, where the applications of potential adversaries may also operate*' (Jansen & Grance, 2011).

7.1 Accountability Governance

Inspired by the definition adopted by NIST in regards to Information Security Governance (NIST, 2007), accountability governance can be defined as the process of establishing and maintaining a framework and supporting management structure and processes, as well as accepting and providing assignment of responsibility to:

- provide stewardship of personal and confidential data with which the organisation is entrusted,
- processing, sharing, storing and otherwise using said data according to contractual and legal requirements, from the time it is collected until when the data is destroyed (including onward transfer to and from third parties),
- comply with legal, ethical and moral obligations, policies, procedures and mechanisms,
- explain and demonstrate ethical implementation to internal and external stakeholders and remedy any failure to act properly.

In essence, accountability governance consists in accepting responsibility for accountability objectives, and in establishing and sponsoring the operational structure and process to meet these objectives. The board (or equivalent executive leadership) of the organisation is responsible for governance. It can (and usually does) create management structures to assign authority in the implementation of the oversight and processes identified, however it ultimately remains responsible and accountable for meeting these objectives (De Clercq). Nothing in this definition is dependent on the mechanisms used to store or process the data. The accountability governance objectives do not depend on whether data processing is based on the use of clouds or not. However, cloud has a strong impact on how governance is implemented. (Details of an accountability governance program are discussed in Section 6).

7.2 Governance and Span of Control in the Cloud

In a simplified view, accountability is modelled as a relationship between two parties: a party (the application provider) is accountable to another party (the customer) for something (handling data in a defined manner). These roles bear a strong relationship with the roles defined in data protection legislation: the first party being the data controller and the second being the data subject.

The use of cloud services to implement an application brings in another party: the cloud provider, which provisions and controls the resources used to provide the service. This creates a relationship between the above application provider – which is now a cloud customer – and the cloud provider (see Section 4 for a more complete analysis of these relationships). It must be noted that third-parties can also be involved around the relationship between the above parties; in fact all seven parties identified in Section 4 have a role to play in regards to accountability governance. Figure 30 shows the interaction between two organisations (as a continuous process) driven by *accountability governance* (constrained by external criteria and regulatory regimes but orchestrated independently by organisations). Organisation A could be part of a service provision chain that involves cloud service providers and Organisation B is actually an oversight and enforcement actor (e.g. regulators and accountability agents) in the chain. Organisation A defines and implements appropriate governance mechanisms, which enable to demonstrate governance. Organisation B, holding to account Organisation A, can ask for further clarification, engage in discussions and also apply sanctions. As a result, Organisation A may modify organisational governance.

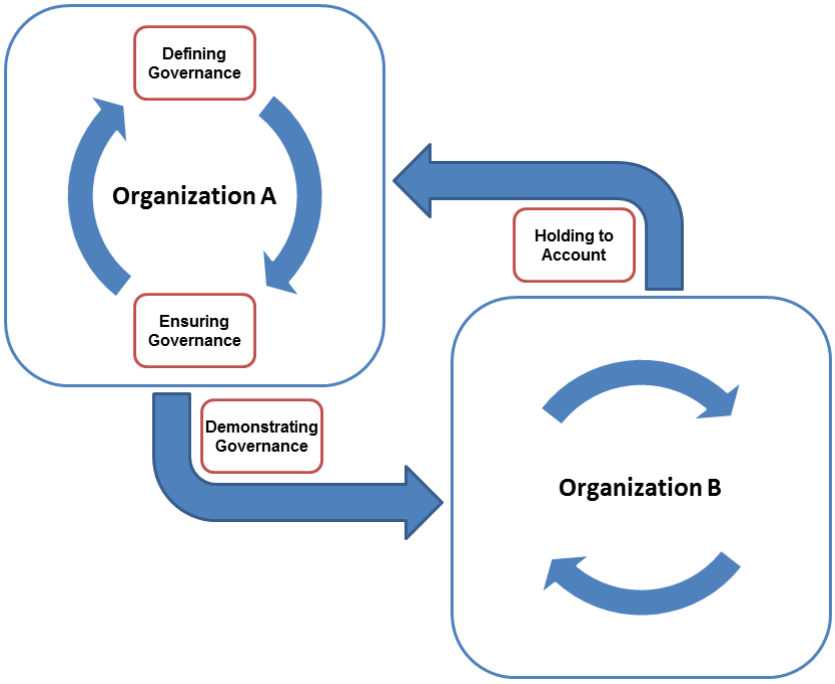


Figure 30 Accountability Governance

This relationship can be defined across multiple dimensions:

- ***Legal***: laws and regulations assign responsibilities and obligations to both parties.
- ***Contractual***: the use of cloud services is done in the context of an agreement between the cloud customer and the cloud provider. This agreement can take many forms; e.g. negotiated contract or terms and conditions applicable to all cloud users.
- ***Technical***: the cloud service offers a set of functionalities, which are accessed through a defined interface. This interface is provided by the cloud provider and is invoked by the cloud customer, hence creating the relationship.
- ***Administrative***: operators and administrators can only manage the resources placed under their administrative control. Administrative domains define which resources are in the control of which party.

Organisations need to provide transparency of those actions taken in order to show that stakeholders' expectations have been met and that organisational 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 organisational obligations that result from taking this approach represent a shift from reactive to proactive governance of personal and/or confidential data. Organisations commit to the stewardship of personal and/or confidential data by addressing legal, contractual and ethical obligations. In order to do so, organisations 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. While accountability may not typically be composed; i.e. it is primarily a bilateral relationship, the ability to behave in an accountable manner in the context of the cloud depends on cloud services supporting "deep" accountability attributes, such as transparency (Section 0 provides a more detailed analysis).

7.3 Accountability Process

This section describes an accountability process enabled by the accountability framework that is underpinned by the A4Cloud accountability model described in Section 2. This process bears many similarities to the process used for Information Security in general, and embeds nicely with it. In Section 2, there was a high level introduction of the functional elements of accountability mapped on that process, as shown in Figure 31.

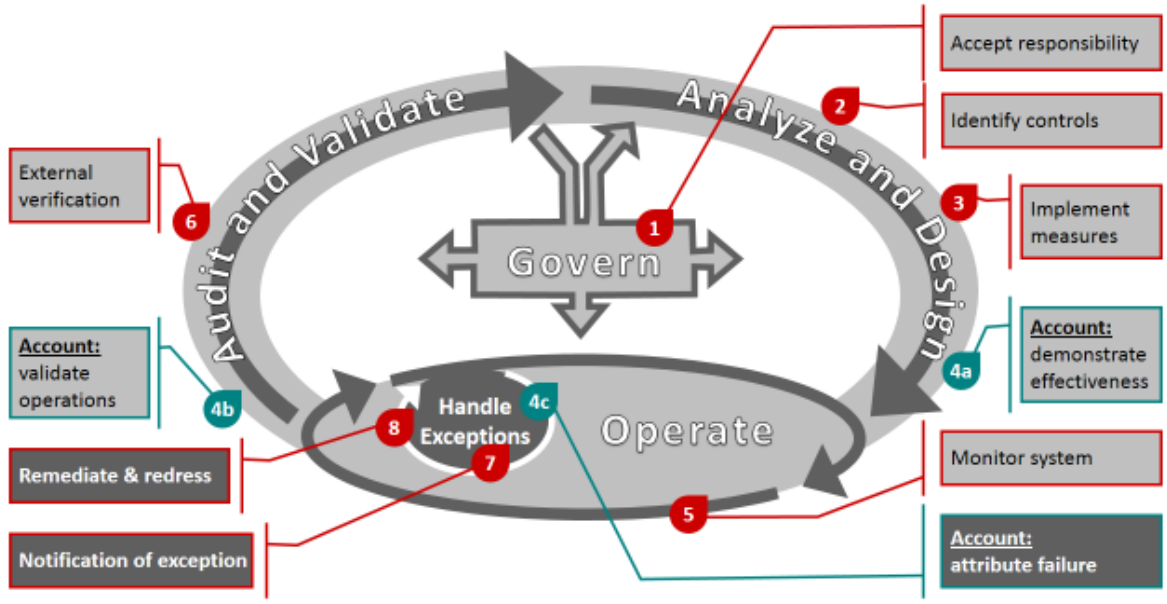


Figure 31 Functional Elements of Accountability in an Organisational Lifecycle

This process, described by (De Clercq), is orchestrated along a combination of lifecycles (phases), as follows:

- The information security governance lifecycle (marked Govern) corresponds to the processes that operate across the governance areas of corporate, business, IT, risk management, information security, and compliance. The purpose of this lifecycle is to allow executive officers to exercise their risk management oversight responsibilities. It interfaces with the risk mitigation lifecycle by setting the objectives for risk mitigation, including the definition of risk appetite and accountability objectives. Additionally, it interfaces with the risk mitigation lifecycle by consuming dashboards, Key Performance Indicators (KPIs), and audit reports. Beyond these specific interfaces, the two groups interact regularly on a more or less formal basis.
- The risk mitigation lifecycle transforms the risk management and accountability objectives set by the governance bodies into controls. It implements these controls and regularly reviews their effectiveness. This lifecycle clearly separates identification of risks (based on business impact, not technology), identification of controls, design of control implementation, and implementation of controls through technology and process. This lifecycle is typically iterated once a year.
- Daily operations (marked Operate) function continuously; this is where the IT system delivers its services to the business. This set of processes produces a massive volume of event data. The data is the base material for security audits and reports to the governing bodies.
- The incident response and mitigation lifecycle is a specialised part of the daily operations lifecycle. It is activated when an incident which requires a specific response is detected.

This process is applicable to each organisation party to the technical interactions along the provisioning chain; this is in particular the case for both the cloud customer and the cloud provider. The functional elements of accountability are as follows:

1) ***Accept responsibility:*** as part of the governance for the organisation, the management accepts responsibility for accountability objectives, and establishes and sponsors the operational structure and process to meet these objectives
2) ***Identify controls:*** This is the first step of the risk mitigation lifecycle. It starts with a risk analysis, which identifies all business processes related to the accountability objectives and documents the applications and people processes for each. Business management performs the risk analysis to ensure that the perspective is from a business view. These risks are then analysed and the proper treatment is determined. This treatment could correspond to

adaptations in the business processes, or a treatment through organisational or technical measures, the latter being rolled-out in terms of controls.

3) ***Implement measures*** which have been selected in the previous step.
4) ***Provide an account:*** the account plays a central role in accountability. Several steps in the overall lifecycle explicitly address the account:
   a) ***Demonstrate effectiveness:*** This is a static validation, based on the risk analysis and decisions taken for the risk treatment, with the objective of doing a first validation of the complete system and of validating what will be reported in the account
   b) ***Validate operation:*** This step of the Audit and Validate part of the risk mitigation lifecycle has for object the reporting of the operational aspects of the system to the party to which the account is owed.
   c) ***Attribute failure:*** In this step of the incident response and mitigation lifecycle, the provider reports to its customer the attribution of the failure corresponding to the incident
5) ***Monitor system:*** this groups all processes associated with the monitoring of the systems, collection of metrics, of logs and of other elements which constitute the foundation by which the organisation of the provider can demonstrate to its customers, auditors, and regulatory authorities that it meets its obligations. This is a continuous process which is part of the daily operations.
6) ***Externally verify:*** this is part of the audit and validate phases. Executed at regular intervals, it includes most of the processes involving external parties. This includes assessment of the account of step 4b, in the context of the enforcement process in relation to the satisfaction of obligations
7) ***Notify*** (e.g. an incident or data breach)
8) ***Remediate and provide redress***.

This accountability model can support an accountability process for organisational governance, as described below. The accountability process highlights different phases for an organisation to be accountable. The process can be presented in a schematic way, as follows:

1. Identify accountability attributes: organisations need to identify relevant accountability attributes and relate them to specific application domains
2. Operationalise accountability attributes: organisations implement these attributes by embedding accountability practices in their organisational/quality processes
3. Use accountability mechanisms and tools: organisations select, adapt and use specific accountability mechanisms and tools for their accountability practices
4. Assess accountability mechanisms and tools: organisations assess how accountability mechanisms and tools support their accountability practices
5. Interpret accountability attributes: organisations interpret accountability attributes and their emergent relationships as highlighted by their accountability practices and supported by specific accountability mechanisms and tools.

The above points identify an iterative accountability process consisting of cycles of operationalisation and interpretation of accountability attributes by practices, and cycles of adoption and assessment of accountability mechanisms and tools supporting accountability practices. The accountability process is an organisational process of governance that enables organisations to enhance accountability. That is, accountability is part of the emerging organisational culture resulting from following the accountability process. Accountability becomes a routine enhancing organisational trustworthiness (Möllering, 2006), that is, accountability is part of an organisational culture (how things normally get done within accountable organisations). At a high level, the focus will be on item 3, i.e. for the organisation to consider what mechanisms are appropriate for it to adopt in order to be able to adequately achieve the accountability practices defined within Section 2.

7.4 Accountability Process in a Cloud Context

The Accountability Process presented in Section 7.3 is described in the context of a single organisation. This process is not applicable as described to a “business” service provisioned through the composition of services offered by different organisations in a cloud model (which we will refer to as a cloud value chain); rather each organisation party to the value chain runs one distinct instantiation of such a lifecycle:

- The governance part of the lifecycle is directly tied with the (management of) each organisation. It refers to the definition of the organisation objectives, acceptance of responsibility, and mobilisation of forces to deliver. In a cloud value chain, there is however a relationship, albeit indirect, between the governance of all involved organisations: the responsibilities and objectives must have a degree of compatibility so the aggregates, i.e. the services provisioned through the cloud value chain, meets their requirements
- The risk mitigation part of the lifecycle has for object the service offered by the organisation. The decisions on how the service is to be implemented and delivered are taken in this lifecycle – this phase is therefore dependant on the characteristics (including the accountability properties) of the services which will be used. These services are themselves subject to an instance of this lifecycle, to define how it is to be implemented and operated – but the two instances are typically not connected, except when one service is specifically designed to support another (co-design). It is here important to note that, while the result of this composition includes an accountability chain, the obligations applicable to the services along the chain and the associated accountability properties are not necessarily (and not typically) identical across the whole value chain.
- There are strong dependencies between the various service providers when it comes to the daily operations. This dependency translates into a strong dependency on a service management chain, which must be designed-in, through the risk mitigation (and service design) part of the lifecycle. The services supporting accountability are part of this chain of services. In practice, this means that service management must be designed with the same degree of scrutiny as the functionality part "business" service, and that this design must take a holistic approach (considering all angles, including non-technical aspects such as the selection, training and management of administrative staff).
- Likewise, all aspects of exception handling are composite and follow a pattern similar to service management. Because the various elements required to provide an account are not under a single administrative domain, exception handling must be engineered as an integral part of the service and cannot be an afterthought.

The project approach to the mechanisms for accountability is based on a co-design approach, as presented in Section 6. This represents one extreme in the spectrum of possibilities to provision accountability chains. This means that the services supporting accountability properties are an integral part of each of the service offerings used in the cloud value chain. A variant of this approach is a model where the accountability tools and services are not implemented in a distributed manner across the various providers in the cloud value chain, but where tools are operated by one (or a few) actors. Instead of tools, the distribution is then on the control and reporting points across the value chain. The control points refer to the possibility to control the way services are rendered (such as the ability to specify policies associated with data handling, access control, and similar topics). The reporting points designate the ability to observe how services are rendered (such as trusted logs, metrics, tracing and attribution of actions…) The Reference Architecture for the project will explore in more details the implications of this approach in the context of the tools built by the project, in particular from functional and from a span-of-control viewpoints. The co-design approach can be realised either by the design of services for a specific use (bespoke services), or by the creation and widespread adoption of standards. This approach is one that has been followed by several initiatives investigating the subject of privacy, with varying degrees of success.

Accountable organisations do not necessarily require the use of co-designed accountability properties across the whole value chain. The relationship between the cloud customer and cloud provider can be classified in two broad categories: those where the customer data and processes have a semantic meaning for the cloud provider, and those where the cloud customer data is simply a "bag of bits". Examples of the former are where the cloud customer uses services of a higher-level of abstraction, typically offered under a SaaS model, such as a payment service, a social network platform, or an e-commerce platform. Because the data is in part processed under the control of the cloud provider, all obligations associated with this type of service are directly applicable – including all provisions applicable to the information provided to the cloud customer by its customers (which could be the data of cloud subjects or of cloud customers if the cloud customer acts as cloud provider for other entities). When the cloud customer data is simply a "bag of bits" for the cloud provider, the obligations of the cloud provider are typically simpler to enumerate, but may be more stringent. In this case, the cloud customer

controls the (algorithmic) processing of the data, and the cloud provider has simply the obligation to ensure that the data is only processed as intended by the cloud customer.

NIST, which is in charge of developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, has made specific recommendations in this regard (Jansen & Grance, 2011). It specifically lists a series of activities, in three phases (Table 3):

Table 3 Cloud Outsourcing Activities Recommendations (Jansen & Grance, 2011)

Areas	Recommendations
Preliminary Activities	• Identify security, privacy, and other organisational requirements for cloud services to meet, as a criterion for selecting a cloud provider. • Analyse the security and privacy controls of a cloud provider's environment and assess the level of risk involved with respect to the control objectives of the organisation. • Evaluate the cloud provider's ability and commitment to deliver cloud services over the target timeframe and meet the security and privacy levels stipulated.
Initiating and Coincident Activities	• Ensure that all contractual requirements are explicitly recorded in the service agreement, including privacy and security provisions, and that they are endorsed by the cloud provider. • Involve a legal advisor in the review of the service agreement and in any negotiations about the terms of service. • Continually assess the performance of the cloud provider and the quality of the services provisioned to ensure all contract obligations are being met and to manage and mitigate risk.
Concluding Activities	• Alert the cloud provider about any contractual requirements that must be observed upon termination. • Revoke all physical and electronic access rights assigned to the cloud provider and recover physical tokens and badges in a timely manner. • Ensure that organisational resources made available to or held by the cloud provider under the terms of service agreement are returned or recovered in a usable form, and that information has been properly expunged.

Even though the word "accountability" is not listed in these recommendations, it is clear that using an accountability approach addressing all dimensions (preventive, detective, and corrective) rather than solely relying on certifications and audits to "continually assess the performance of the cloud provider and the quality of the services provisioned to ensure all contract obligations are being met and to manage and mitigate risk" greatly reduces the risk of using Cloud services. The activities identified by NIST are an integral part of the risk mitigation lifecycle described above, extending in part to the daily operations lifecycle for the aspects related to continuous-compliance, proactive management, and gathering of evidence. Similar recommendations have been developed by other organisations. In regards to the Data Protection domain, one could refer to (CNIL, 2012b) and (ICO, 2012b), amongst others. Guidance also exists for other domains, such compliance to the Sarbanes-Oxley Act or the Health Insurance Portability and Accountability Act (HIPAA).

7.5 Summary

This section has discussed accountability governance in terms of controls as well as processes. It has also related these aspects of accountability governance to standard NIST activities. The accountability governance lifecycle is a means to operationalise accountability in cloud ecosystems. It enables us to move from accountability to being accountable. It also supports the orchestration of the different functional aspects of accountability, and the related accountability mechanisms. This is further detailed in the A4Cloud's reference architecture.

8 Contextual Accountability in the Cloud

In this section we introduce the idea of *adaptive* or *intelligent accountability.* We investigate how accountability may be introduced in distributed and cloud environments in an intelligent way, in order to avoid negative trade-offs between trust and generated administrative burden. Part of this analysis (considered within Section 8.1) relates to how what is appropriate to expect in terms of accountability may vary across different scenarios, and part (considered within Section 8.2) relates to definition of accountability maturity models that can capture both the maturity of individual organisations in terms of accountability practices, as well as a measurement of the appropriateness of the measures used across whole cloud supply chains. Finally, the analysis of evidence given in Section 2 is extended and more detail is provided about how evidence can support the strong accountability vision articulated in Section 6.6.

8.1 Adaptive Accountability

The idea of 'intelligent accountability' was first proposed by Onara O'Neill in her 2002 Reith Lectures on 'A Question of Trust', as a means to provide greater accountability without damaging professional performance (O'Neill, 2002). She argued that much that has to be accounted for is not easily measured and cannot be reduced to a set of stock performance indicators. She said that intelligent accountability "requires more attention to good governance and fewer fantasies about total control" and "good governance is possible only if institutions are allowed some margin for self-governance of a form appropriate to their particular tasks". The relation between accountability and good governance originates from the public sector (e.g. health care). One can speak of good governance when the interaction between A and B has such an institutional realisation it entails societal interests and moral values the best way possible. Good governance focuses upon the creation of conditions that allow collaborations, interactive processes or policy networks to function the best way possible. Moreover, these conditions do take into account the different stakeholder's responsibilities and societal interests. Good governance doesn't depart from the perspective of increased control and supervision. Instead, good governance of departs from the perspective of transparency, comprehensibility and taking account for one's conduct. Therefore one speaks of the chain of accountability and not a chain of oversight. Exactly here the Accountability model as provided in Section 5 and the notion of intelligent accountability are aligned. Despite the concern of the introduction of light-touch self-regulation by the back door or of data controllers promoting accountability in the hope of avoiding more constraining and comprehensive regulations, as discussed in Section 2.5.1, self-governance in the form of intelligent accountability would stimulate accountable behaviour as an intrinsic value of the cloud ecosystems from within. As relates to the cloud, intelligent accountability would involve:

- moving away from "box checking" and static privacy mechanisms;
- assessing potential harms to data subjects before exposing data to risks; this would be part of ongoing risk assessment and mitigation, for which privacy impact assessments (PIAs) are one important tool;
- allowing organisations more flexibility in how they provide data protection so that they can use internal mechanisms and controls that make the most sense for their business situation, rather than a one-size-fits-all prescriptive set of rules;
- employing various degrees of accountability; it might be that more stringent standards and tests for accountability could facilitate proof of CSPs' readiness to engage in certain activities (such as those that involve processing highly sensitive data) or even relieve them of certain administrative burdens (such as renotification of minor changes in processing); and
- developing clever, automated analysis, automated internal policy enforcement, and other technologies to enhance enforcement and avoid increasing the human burden. Examples of these techniques have already been considered within Section 7.

As an integral part of this approach, organisations will need to spend time and resource analysing what this means to them and gaining the management support to implement necessary changes, as described in Section 3. Much of this approach is actually included within the approach we suggest using in Section 7.

Contextual factors affect the degree of protection of personal data that is appropriate for a given context. Such factors include sensitivity of data, location of data (both the locations of stored data and the potential locations of transferred data), sector, whether an anonymous data set could be usable, contractual restrictions, cultural expectations, user trust (in organisations, etc.), trustworthiness of partners, security deployed in the infrastructure. etc. as well as potentially other factors that influence the solutions to be selected, such as expected number of users of the system and conformance to existing agreements between parties or compatibility with legacy systems. The relationship between these factors and privacy control measures (such as PETs) that should be deployed can be complex (Pearson & Shen, 2010), as suggestion of design patterns based upon contextual factors can be quite difficult. In the rest of this section we focus on the type of data and the risks involved as being the central factors influencing the suitability of accountability measures.

It is already part of the notion of accountability as considered within Section 2 that although some specific measures would have to be implemented for most processing operations, for reasons of flexibility (or as often referred to instead when making a similar point – scalability), the suitability of measures needs to be determined on a case-by-case basis, with particular reference to the type of data and to the risks involved as argued above. It is acknowledged that accountability could reduce and even replace some existing requirements, such as prior notification to DPAs (European DG of Justice, 2010).

The role of scalability and suitability of measures in achieving accountability is implied by the Galway project (CIPL, 2009). As it is provided, 'an accountability approach enables organisations to adopt methods and practices to reach those [common data protection] goals in a manner that best serves their business models, technologies and the requirements of their customers'. However, we believe that this should not be interpreted to mean that privacy and data protection should be defined in a way that best serves business models and technologies. Another danger is that the lack of precision about what adaptability means in practice could lead to a weakening of standards and to companies bending the rules (Bennett, 2012: p44). The issue of scalability, in particular, is really about how to develop workable rules that can apply both to small and to large organisations, and hence the accountability maturity model discussed in the next Section can be part of such a solution. In terms of privacy, however, we already have a broad consensus around what it means for a responsible organisation to protect personal data and respect the privacy of the individual (Bennett, 2010), and this centres around the standard set of fair information principles. Corresponding to this, all information privacy law across the world contains rights for data subjects and obligations for organisations, and these form a body of policy convergence. Specifically in terms of organisational obligations that should apply across all institutions and technologies, we can include the following key aspects:

- transparency about policies and practices
- collection of personal information only for defined and relevant purposes
- use and disclosure of personal information only in ways consistent with those purposes
- provision of access and correction rights to individuals
- security protection for the personal information
- data retention.

Corresponding to the organisational mechanisms needed to meet these obligations, some may be core (fundamental, mandatory activities that should be carried out by all organisations) and some may be elective (i.e. desired activities that are nevertheless optional). Core activities will vary from one organisation to the next and will be influenced by the industry/sector as well as jurisdiction (Nymity, 2013: p7). Such activities may even vary within an organisation. In the context of European Data Protection, Article 29 Woking Party has pointed out the tension between scalability and flexibility on the one hand and legal certainty on the other, within their Opinion on Accountability (para 50: European DG of Justice, 2010) arguing that the DPD cannot solve this issue and that the Commission could provide further guidance in this respect. Moreover, Article 29 Working Party has shed some light on the issue of the appropriateness of the measures implied by the enforcement of the accountability principle in practice. In particular, it argues that:

> "*Some of the measures are 'staples' that will have to be implemented in most data processing operations. Drafting internal policies and procedures implementing the principles (procedures to handle access requests, complaints) may constitute examples of appropriate measures for*

> *some processing of data. The suitability of measures will need to be decided on a case-by-case basis. It is up to data controllers to make such decisions, following guidance issued by national data protection authorities and the Article 29 Working Party where available (…) It follows from the above that in determining the types of measures to be implemented, there is no option but "custom built" solutions. Indeed, the specific measures to be applied must be determined depending on the facts and circumstances of each particular case, with particular attention to the risk of the processing and the types of data. A one-size-fits-all approach would only force data controllers into structures that are unfitting and ultimately fail."* (para 44-45: European DG of Justice, 2010)

In general, the principle of accountability – as being, also, understood in the field of European Data Protection Law, requires data controllers to go beyond mere compliance with the applicable law. For example, an organisation acting as a data controller may decide to appoint a data protection officer even through this is not mandatory under the DPD or the implementing laws at national level. The Article 29 Working Party applauds these initiatives and encourages the new data protection legal framework to provide incentives for data controllers to do so. To what extent, though, the proposed GDPR succeeds in doing so remains questionable.

8.2 Accountability Maturity Model

The notion of adaptive/contextual accountability presented in Section 8.1, rest on the assumption that organisations are able to assess their level of accountability. However, the evaluation of accountability is still an open problem in terms of state of the art. In this section we propose the adoption of an accountability maturity model (AMM) for the cloud, which can capture both the maturity of individual organisations in terms of accountability practices, as well as a measurement of the appropriateness of the measures used across whole cloud supply chains. The AMM seeks to aid organisations (in particular small and medium enterprises or SMEs), to assess their accountability practices by quantitatively evaluating the maturity of the mechanisms deployed to support accountability. The proposed AMM aims to be also context-aware by identifying the different stages by which an organisation would become accountable. It is not necessarily feasible and realistic for an organisation to commit to an accountability-based approach immediately: it would require organisations to gradually change their work practices and to change their culture (i.e., *adaptability*). Moreover, the size and type of an organisation needs to be taken into account – what is appropriate for an SME is not the same for example as for a larger enterprise (i.e., *context awareness*), and other factors including the sensitivity of information being handled must also be taken into account.

The proposed AMM is based on well-known security and privacy control frameworks (e.g. ISO/IEC 27002 and NIST 800-53), given the fact that both concepts (security and privacy) are close related to accountability (Bennett, 2012). This approach adopted for developing the AMM relies on the well-known notion of capability maturity models (CMM) as introduced by the Software Engineering Institute (SEI 2010). The CMM is generally context-aware, because it helps to understand the maturity of organisations through various characteristics. Such maturity models can help facilitate process development and enterprise evolution by identifying maturity milestones and benchmarks for comparison. In the state of the art, most maturity models consist of two basic elements:

- ***Control Framework:*** a set of controls that an organisation will apply to address requirements such as security, privacy or accountability.

- ***Scoring Methodology:*** a technique used to assign a quantitative or qualitative value that rates the level of implementation of the control framework. The assigned value is known as a "maturity level": the score typically increases with the level of sophistication of control implementation. .

This differentiation is important from the perspective of the methodology adopted to develop the proposed AMM (Figure 32).

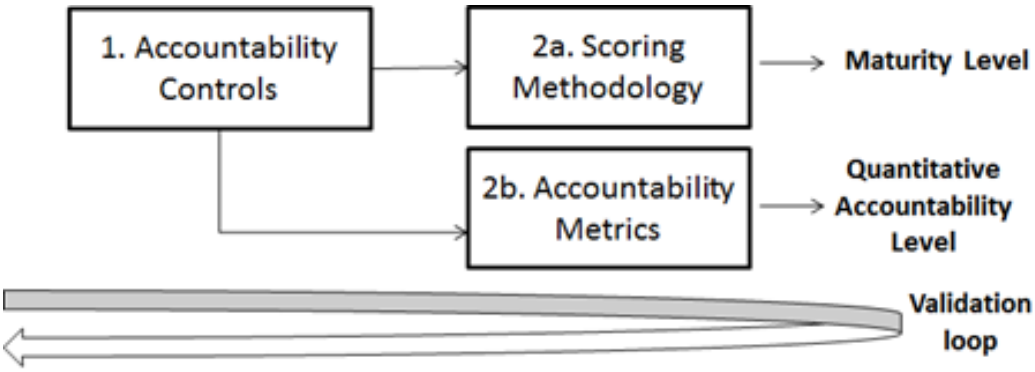


Figure 32 Stages Involved in the Development of the AMM.

8.2.1 Developing the Accountability Maturity Model: Overview

As mentioned in the previous section, the development of the contributed AMM rests on well-known cloud maturity models (e.g. Oracle Capability Model[81], Cloud Maturity Model[82,83,] Cloud adoption model[84]) which are strongly related to previous works carried out in the context of Capability Maturity Model Integration (SEI 2010). Most of these works imply that for achieving cloud maturity, some factors are likely to exist accumulatively as maturity grows. As suggested in (Bennett, 2012), the AMM is based on relevant maturity models developed in the areas of security and privacy. Security related maturity models for traditional ICT (i.e. non-cloud) (e.g. Information Assurance Maturity Model[85], Cybersecurity capability model[86], CSEAT IT Security Maturity Model[87], COBIT Maturity Model[88], CITI-ISEM[89], CERT/CSO[90]), and cloud systems CSA STAR Certification are common in current practice. Most of these rely on control frameworks based on standards like ISO/IEC 27002or best practice like the Cloud Controls Matrix (CCM) (CSA 2014). In the privacy domain it is worth mentioning maturity models like the AICPA/CICA Privacy Maturity Model (PMM) (AICPA 2014), and Nymity's Privacy Management Accountability Framework. The analysis presented in this Section will show the gaps in selected security and privacy controls frameworks from the accountability perspective.

A high-level view of the process to develop the AMM is shown in Appendix E where three stages are required to create both the control framework and associated quantifiers comprising the AMM. The empirical validation of developed controls and metrics is out of scope in this deliverable, but will be part of future activities. The following subsections detail each step of our methodology.

8.2.2 Stage 1: Defining the Accountability Controls

As mentioned in the previous section, our effort to develop an AMM rests in the analysis of relevant security and privacy maturity models. The ones analysed in this document were selected based on the criteria defined by A4Cloud's WP A-5 (Standardisation), in an effort to contribute obtained results in the area of AMM to the respective standardisation bodies.

[81] Oracle cloud computing capability model, http://www.oracle.com/technetwork/topics/entarch/oracle-wp-cloud-maturity-model-r3-0-1434934.pdf
[82] A maturity model for cloud computing, http://news.cnet.com/8301-19413_3-10122295-240.html
[83] Maturity models for the cloud, http://blog.gardeviance.org/2008/12/maturity-models-for-cloud.html
[84] The cloud computing adoption model, http://www.ddj.com/architect/211201818
[85] Information Assurance Maturity Model, http://www.cesg.gov.uk/publications/.../iamm-assessment-framework.pdf
[86] Cybersecurity capability model, http://energy.gov/oe/downloads/cybersecurity-capability-maturity-model-february-2014
[87] CSEAT IT Security Maturity Model, http://www.acsac.org/2001/case/Wed_C_1030_Burke_NIST.pdf
[88] COBIT Maturity Model, http://archive.adaic.com/ase/ase02_01/bookcase/se_sh/cmms/systems_security_engineering/SSEovrw_lkd.pdf
[89] Information Security Evaluation Model (CITI-ISEM), http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981
[90] CERT/CSO Security Capability Assessment, http://www.cert.org/archive/pdf/05tn023.pdf

Our research proposes two possible approaches for eliciting the controls that are relevant to cloud accountability:

1. It is possible to start from scratch developing customised controls, possibly based on the notion of accountability attributes presented earlier in this Deliverable.
2. We can also start by applying a gap analysis to relevant security/privacy controls frameworks in order to select those individual controls relevant for cloud accountability.

Both approaches have their pros and cons e.g., starting from scratch will provide accurate accountability controls but they might be more difficult to integrate into existing/standardised frameworks. The rest of this section focuses on our initial approach i.e., analysing existing controls frameworks to identify accountability-related controls.

Based on A4Cloud's notion of accountability attributes, we proceed to identify the gaps related with the surveyed security/privacy control frameworks. The gap analysis is based on a set of mapping rules (Table 4) to relate individual controls to each one of the accountability attributes introduced in this Deliverable. At a glance, the proposed rules consider that the ultimate goal of accountability is to provide information to external stakeholders, therefore only if information to internal stakeholders is provided then a gap is identified.

Table 4 Analysing Accountability Gaps in Security and Privacy Control Frameworks

General rule: If the control does not concern data stewardship practices, it is ignored.		
Accountability Attribute	***To whom information is provided?***	
	Gap identified if…	***Relevant to the AMM if…***
Transparency Does the control require or enable the dissemination of information describing how the organisation conforms to rules, policies and requirements? Note: the fact that a control requires the definition of rules, policies and requirements is not enough. Some provision must be included in the control to make sure that info is made available to stakeholders.	Only to internal stakeholders	Also to external stakeholder
Verifiability Does the control require a test or enable the construction of a proof that a rule, policy or requirement regarding data stewardship has been implemented? Note: the adoption of standards, or the documentation of policies & requirements may facilitate verifiability, but is not enough. An actual test or proof must be enabled by the control.	A test or proof examined by internal stakeholder	A test or proof examined by external stakeholder
Attributability Does the control enable to link individuals with the actions they performed on a system? Or does it contribute to the security or trustworthiness of that link? Note: Controls related to identity assurance and logging are in scope.	For individuals representing internal stakeholders.	For individuals representing external stakeholders
Remediability Does the control enable corrective measures related to non-compliance with a rule, policy or requirement? Note: Detective and preventive controls are not enough. We target corrective controls here.	Measures involve internal stakeholders	Measures explicitly involve external stakeholders, through compensations and/or information
Responsibility Does the control require an analysis resulting in the assignment of a task, or the oversight of a task, to an individual, group, or organisation? Or does the control	With assignments disclosed internally	With assignments disclosed to

participate in the enforcement of the assignment of a task to an individual, group or organisation? Notes: -The fact that a control says "X shall do Y" is not enough. The control must describe a process that results in the determination of responsibilities. -One of the difficulties is that some processes implicitly involve the determination of responsibilities, without making this explicit in the wording of the control. For example, if a control suggests the creation of an Information Security Management framework normally this also means that relevant responsibilities will assigned within the organisation. This allows some space for interpretation.		external stakeholder
Liability Does the control evaluate or attribute risks/costs legally related to failures to comply with rules, policies or requirements?	With scope limited to internal stakeholders	With scope including external stakeholders
Observability Does the control enable both (1) monitoring of policies, rules or requirements implemented by a system and (2) assurance that the monitoring provides a truthful representation of the internal compliance state of the system.	Monitoring is available to internal stakeholder	Monitoring is available to external stakeholder

Based on the proposed approach, as a proof of concept we analysed the accountability gaps in two relevant security controls frameworks and one privacy-related framework. The analysed frameworks were:

- CSA's Cloud Controls Matrix, CCM (CSA 2014): a control framework specifically designed for the purposes of cloud security. CCM strengthens existing information security control environments by delineating control guidance by service provider and consumer, and by differentiating according to cloud model type and environment. The CCM is one of the pillars in CSA's Open Certification Framework.
- NIST 800-53 rev. 4: despite not being formally considered a maturity model, NIST 800-53 provides a controls framework widely used by the US government agencies (i.e., FedRAMP). This framework has been mapped to other well-known ones like CSA's CCM and ISO/IEC 27001.
- AICPA/CICA Privacy Maturity Model, PMM (AICPA): a maturity model for assessing an organisation's privacy program and practices for handling personal information. The PMM is in turn based on the "Generally Accepted Privacy Principles" (GAPP), a set of privacy-related principles for guiding the definition and management of privacy programs. For the purposes of our gap analysis, GAPP is considered the control framework for PMM.

In Appendix F the initial results of the performed gap analyses are presented, showing the actual coverage of the respective control frameworks with respect to the accountability attributes. We can observe that in general GAPP and NIST show a better coverage in all aspects, given the fact that they were designed from a privacy and data protection perspective (contrary to CCM, which is security-focused). Actually, few controls in both GAPP and NIST are not related at all with accountability (approx.19% in GAPP versus CCM's 53%). With respect to the attributes covered, in all cases the "Transparency" attribute was the most relevant. In all the control frameworks "Liability", "Observability" and "Attributability" showed the smallest coverage. In particular, "Liability" is not covered at all in GAPP; in CCM, the attribute "Observability" is not covered by the current set of controls; and in NIST, there are no controls related to "Attributability". Note that the figures given in Table 5 are intended as an idea of the direct relevance of Accountability in the analysed control frameworks, but not as a means for comparing them to each other, as they have different total number of controls (CCM has 136 controls, GAPP has 73 and NIST has 27).

Table 5 Security and Privacy Maturity Models – Gap Analysis

Controls Framework	% of Controls unrelated to accountability	% of Controls mapped to Accountability Attributes (possibly overlapping)						
		Observability	Verifiability	Attributability	Transparency	Responsibility	Liability	Remediability
Cloud Control Matrix v3.0	53,67%	**0%**	1,47%	3,67%	11,76%	5,14%	0,73%	3,67%
GAPP	19,17%	3%	7%	4%	42%	4%	**0%**	10%
NIST 800-53 rev 4	19,2%	4%	27%	0%	42%	23%	**4%**	12%

It is worth noticing that from a very broad perspective, we can find some similarities among the GAPP principles and A4Cloud's accountability attributes, just as shown in Table 6.

Table 6 GAPP Principles and Accountability Attributes

GAPP principle	Description (extracted from (AICPA))	Related to Accountability Attribute
Management	The organisation defines, documents, communicates and assigns accountability for its privacy policies and procedures. Criteria: • privacy policies define and document all ten GAPP • review and approval of changes to privacy policies conducted by management • risk assessment process in place to establish a risk baseline and regularly identify new or changing risks to personal data • infrastructure and systems management takes into consideration impacts on personal privacy • privacy awareness training	Responsibility, Remediability
Notice	The organisation provides notice of its privacy policies and procedures. The organisation identifies the purposes for which personal information is collected, used and retained. Criteria: • communication to individuals • provision of notice • use of clear and conspicuous language	Transparency
Choice and consent	The organisation describes the choices available to the individual. The organisation secures implicit or explicit consent regarding the collection, use and disclosure of the personal data. Criteria: • communicating the consequences of denying/withdrawing consent • consent for new purposes/uses of the personal data • explicit consent for sensitive data consent for online data transfer	Transparency

Collection	Personal information is only collected for the purposes identified in the notice. Criteria: • document and describe types of information collected and methods of collection • collection of information by fair and lawful means, including collection from third parties • inform individuals if information is developed or additional information is acquired	Transparency
Use, Retention and Disposal	The personal information is limited to the purposes identified in the notice the individual consented to (as related to the EU Data Directive). The organisation retains the personal information only for as long as needed to fulfil the purposes, or as required by law. After this period, the information is disposed of appropriately. Criteria: • systems and procedures in place to ensure personal information is used, retained and disposed appropriately	-
Access	The organisation provides individuals with access to their personal information for review or update. Criteria: • confirmation of individual's identity before access is given to personal information • personal information presented in understandable format • access provided in reasonable time frame and at a reasonable cost • statement of disagreement; the reason for denial should be explained to individuals in writing	Transparency
Disclosure to third parties	Personal information is disclosed to third parties only for the identified purposes and with implicit or explicit consent of the individual. Criteria: • communication with third parties should be made known to the individual • information should only be disclosed to third parties that have equivalent agreements to protect personal information • individuals should be aware of any new uses/purposes for the information • the organisation should take remedial action in response to misuse of personal information by a third party	Transparency, Remediability
Security for privacy	Personal information is protected against both physical and logical unauthorised access. Criteria: • privacy policies must address the security of personal information • information security programs must include administrative, technical and physical safeguards • logical access controls in place • restrictions on physical access • environmental safeguards	Attributability

	• personal information protected when being transmitted (e.g. mail, internet, public or other non-secure networks) • security safeguards should be tested for effectiveness at least once annually	
Quality	The organisation maintains accurate, complete and relevant personal information that is necessary for the purposes identified. Criteria: • personal information should be relevant for the purposes it is being used	-
Monitoring and Enforcement	The organisation monitors compliance with its privacy policies and procedures. It also has procedures in place to address privacy-related complaints and disputes. Criteria: • individuals should be informed on how to contact the organisation with inquiries, complaints and disputes • formal process in place for inquires, complaints or disputes • each complaint is addressed and the resolution is documented for the individual • compliance with privacy policies, procedures, commitments and legislation is reviewed, documented and reported to management	Remediability, Verifiability

The detailed results of the gap analysis performed on the three controls frameworks are shown in Appendix F. It is worth to highlight that our approach does not aim for completeness, but seeks to elicit an initial set of controls for the proposed AMM. These initial findings still need to pass through a validation stage (out of this document's scope) before being e.g., contributed to their respective standardisation bodies. Once the accountability-related controls have been developed it is required to provide a methodology to quantitatively assess them. Our research proposes two different approaches to perform this quantification, just as explained in the next sections.

8.2.3 Stage 2a: Scoring Methodology

Despite its inherent subjectivity, human stakeholders (e.g., cloud auditors, decision makers) are nowadays quite familiarised with the use of high-level quantifiers known as *maturity levels* while assessing an organisation with respect to a control framework. The developed AMM proposes two different methodologies for assigning maturity levels:

1. The first methodology (cf., Section 8.2.3.1), uses a generic scoring system that rates the quality of implementation of controls independently of the notion of accountability. Accountability itself is provided by the selection of appropriate controls, while the scoring methodology rates the level of sophistication in the implementation the controls.
2. The second methodology (cf. Section 8.2.3.2), which was developed in the context of this project, proposes a scoring methodology consisting of maturity levels designed for the purposes of accountability. Here, controls are classified according to both an accountability function domain and an accountability sophistication level.

The first approach is more generic, and is easy to integrate with existing security and privacy management frameworks, like (CSA, 2013b). However it requires the selection of an adequate set of underlying accountability controls. The gap analysis we conducted previously and summarised in Appendix F shows that current control frameworks do not yet provide such a foundation. The second approach does not fully fix this problem but makes it much more visible: if the underlying control framework does not contain controls that match a particular function domain and accountability sophistication level, then that particular level of maturity is evidently unattainable. The rest of this section presents both approaches.

8.2.3.1 Assigning Maturity Levels based on Existing Frameworks

In this section are presented our views on assessing the AMM's accountability controls with existing state of the art maturity level methodologies. For the sake of comparability, we analyse the scoring methodologies used for assigning maturity levels in both CCM (as used in the Open Certification Framework (CSA, 2013b)) and GAPP (related to PMM (AICPA)). Most of the surveyed security maturity models (cf., Section 8.2.1), adopt a non-accountability specific scoring methodology similar to CCM and GAPP[91].

Assessing the Cloud Controls Matrix (CCM)
Despite that the CCM does not propose per-se a scoring methodology for assigning maturity levels, a suitable procedure for assigning maturity levels based on a CCM assessment has been developed in the context of the Open Certification Framework (OCF) (CSA, 2013b). The purpose of this "companion" methodology is to assess how well-managed are the activities described in CCM's control areas. Therefore, when an organisation is audited, a *Management Capability Score* (i.e., maturity level) will be assigned to each of the control areas on the CCM. For the sake of usability, the management capability of the *domains (not the individual controls*[92]*)* is scored on a scale of 1-15. These scores have been divided into five different categories that describe the type of approach characteristic of each group of scores:

a) 1-3: No formal approach.
b) 4-6: Reactive approach.
c) 7-9: Proactive approach.
d) 10-12: Improvement-based approach.
e) 13-15: Optimising approach.

These categories resemble the commonly used scale of five maturity levels (see PMM analysis below), although in the case of CCM/OCF the overall objective is to perform the assessment of each control domain. When assigning a score to a control domain, the following five factors below will be considered (all or any applicable combination of them):

1. Communication and Stakeholder Engagement.
2. Policies, Plans and Procedures, and a Systematic Approach.
3. Skills and Expertise.
4. Ownership, Leadership, and Management.
5. Monitoring and Measuring.

The lowest score against any one of those five factors will be the score awarded for the control domain. The organisation under evaluation will be awarded the lowest score it achieved for any of the factors assessed against the CCM domains (e.g., if they score 11 for leadership, 9 for communication and 4 for skills, the score for the domain is 4). Of course, in order to achieve a certain score, all of the lower levels must be achieved first. For example, if an organisation misses a vital element at the lower levels of the model, they will receive a low score even if they have some of the higher level attributes in place. The person in charge of performing the assessment will look for *evidence* of the organisation's capability to manage these factors. Once the assessor has assessed all of the control domain, there will be 16 scores (one per-domain of the CCM). The average score will be used to assign the overall Management Capability Score (or *award*) for the organisation, according to the following rules:

- If the organisation has an average score of less than 3, it will receive a certificate with *no award*.
- If the organisation has an average score between 3 and 6, it will receive a *bronze award*.
- If the organisation has an average score between 6 and 9, it will receive a *silver award*.
- If the organisation has an average score greater than 9, it will receive a *gold award*.

Assessing the Privacy Maturity Model (PMM)
PMM describes the characteristics of an organisation's privacy program at each maturity level. PMM does not propose an explicit scoring methodology, but actually for every control on the framework PMM

[91] As mentioned in the previous section NIST 800-53 only defines a controls framework, but does not specifies any particular scoring methodology.

[92] According to (CSA, 2013b), individual controls are too granular for assigning a level to them in isolation.

describes the characteristics that the organisation should fulfil at each level. PMM assigns a qualitative value corresponding to any of the following five maturity levels:

a) Ad Hoc
b) Repeatable
c) Defined
d) Managed
e) Optimised

It is worth to notice the analogies between the maturity levels of both PMM and CCM (i.e., *No formal approach, Reactive approach, Proactive approach, Improvement-based approach, Optimising approach*). Once all the controls have been assessed, the overall maturity level can be computed by a weighted average. The recommended value of the weights is 1 for all the controls, but the scoring methodology permits to use different weights if the rationale for such decision is documented and these weights are used in a consistent way in case of future benchmarking. A summary of the analysis performed on both CCM and PMM is shown in Table 7.

Table 7 Maturity Models - Scoring Methodologies

Control Framework	Granularity (Domain/Control)	Non-aggregated score	Aggregated score (Maturity Level)	Aggregation rule
Cloud Control Matrix v3.0	Domain	Quantitative (1-15)	Qualitative (None, bronze, silver, gold)	Average
Privacy Maturity Model	Control	Qualitative (1-5)	Qualitative (1-5)	Weighted average

The main conclusion drawn from the surveyed models is that the actual semantic of the assigned maturity levels is not accountability-related. On one hand, this "generic nature" allows for assessing most frameworks without considering the nature of their controls (e.g., security, privacy, or accountability). This feature clearly benefits standardisation, by easing the adoption of new controls (e.g., the ones from the AMM) into existing frameworks (e.g., CCM).

On the other hand, this generic nature dilutes the notion of accountability from the resulting AMM's maturity levels. This might be an issue for organisations willing to apply the proposed AMM as a stand-alone tool for assessing their accountability practices. The next section proposes a solution to this identified issue.

8.2.3.2 Using Accountability-Specific Maturity Levels

The novel AMM we contribute in this project proposes a scoring methodology that is *accountability-aware*. The proposed scoring methodology provides a scale with three different "accountability maturity levels" (Defined, Managed, and Optimised), which are assigned depending on the implementation of the individual control for each functional domain of accountability (cf. Figure 31). In order to provide some initial guidance to organisations willing to adopt this approach, in Appendix F is shown the proposed criteria for assessing individual accountability controls. In order to compute the overall maturity level, the following steps should take place:

1. The control is assessed with respect to each functional domain, and a level (1-3) is assigned.
2. The total score of the control, is the lowest score against any one of the eight functional domains.
3. Once all controls of the AMM have been assessed, the overall maturity level will correspond to the smallest score among all.

The rationale for our scoring approach is that in order to achieve a certain maturity level, all of the lower levels must be achieved first. This is similar to the methodology used by OCF (CSA, 2013b).

For example, let us suppose that an assessor is evaluating the implementation of AMM's control "Encryption & Key Management Entitlement" (EKM-01 as seen in Appendix F). This control is evaluated with the following functional domain's scores:

- 1. Accept responsibility: 3

- 2. Identify controls: 2
- 3. Implement measures: 3
- 4a. Provide account (demonstrate effectiveness of measures): 3
- 4b. Provide account (validate operations): 2
- 4c. Provide account (attribute failure): 3
- 5. Monitor system: 2
- 6. External verification: 2
- 7. Notify exception: 3
- 8. Remediation and redress: 2

In this case the overall maturity level for EKM-01 will be 2 (Managed).

The criteria we propose in Appendix F for this scoring methodology are in effect very close to a set of high-level accountability controls, classified in 8 domains. As such, this maturity model could serve as a canvas for the definition of an accountability control framework, by taking each one of the criteria and developing them into a set of accountability controls.

The next section proposes the use of fine-grained quantifiers as a more rigorous approach for quantifying the AMM controls, with the purpose of enabling realistic levels of automation during the accountability lifecycle.

8.2.4 Stage 2b: Accountability Metrics

Evaluating the controls of the proposed AMM in a quantitative way is central for organisational maturity models because of their role in quality assessment, monitoring of processes performance and support of management decisions. Beyond that, useful metrics are highly relevant when addressing the definition of cloud maturity models. In theory, a mature organisation (from the perspective of maturity models) should present a quantitative, and hence, measurable behaviour. Mature organisations are therefore characterised by an ingrained use of metrics within their internal processes. The adoption and systematic use of metrics is an indispensable practice for organisations that strive to achieve a repeatable and optimising behaviour.

Despite the quantification features enabled by the use of the scoring methodology presented in the previous section, the obtained maturity level is usually too high-level (and often subjective) so it cannot be directly used to automate the organisation's accountability management (e.g., adaptation of data protection mechanisms in case of cyber-incidents). In this case, the usage of fine-grained metrics capable of providing useful and low-level accountability information to automated systems is a clear benefit.

In order to elicit meaningful metrics for accountability, a possible approach jointly developed by WP:C-2 and WP:C-5 consists in eliciting quantitative/qualitative metrics through an iterative refinement process of the accountability controls presented in Section 8.2.2. At a glance, the proposed approach consists of the following steps:

1) Study the nature of the accountability control in order to identify whether there is any quantifiable element in the description of the control that is susceptible to being measured. Qualitative elements may be identified too, if they have at least an ordinal nature.
2) Define a metric that measures the identified elements.
3) Validate the metric with respect to the concept of Accountability and, in particular, to the Accountability Attributes.

A comprehensive explanation of the accountability metrics, and its relationship with the AMM is presented in Deliverable D:C-5.2 “Metrics for Accountability”.

8.2.5 Next Steps

We have presented our ideas for intelligent accountability as well as progress related with the creation of an Accountability Maturity Model (AMM) for the cloud, taking as starting point the notion of accountability attributes proposed by A4Cloud. Despite the obvious lack of both a control framework and scoring methodology focused on accountability, it is true that the highest impact will come from an

AMM that departs from existing and widely adopted frameworks. Taking this into account, we have shown in this section a preliminary analysis of three well-known maturity models.

An interesting initial conclusion *is the lack of both Observability and Liability controls in existing frameworks.* Therefore these might be relevant to start studying in further detail along with other WPs in A4Cloud*. We have also observed that privacy control frameworks are closer to accountability than security control frameworks*. This conclusion will help us to prioritise efforts for analysing other control frameworks being provided by WP A-5.

Given the identified gaps in existing security and privacy controls frameworks, by considering an accountability maturity model for cloud exploitation we hope to identify the key developmental stages for a number of organisational characteristics, which in turn will have implications for information security and data protection strategies. Hence it may be possible to anticipate future needs and begin delivering techniques for designing data-protection aware clouds.

The contributed AMM aims to be particularly useful for SMEs, which need to avoid complex approaches for assessing (and improving) accountability practices e.g., when considering migrating to the cloud. This vision is achieved through (i) the use of accountability controls based on widely-used security/privacy frameworks, and (ii) adopting and scoring mechanism that is easy to apply and interpret by humans (e.g., decision makers). These features of the proposed AMM are compatible with self-assessment approaches suitable for SME, just like the business continuity management (BCM) documented by the European Network and Information Security Agency (ENISA, 2010).Through the AMM, it is possible for organisations (including SMEs) to plan, prioritise and invest in order to progress along the maturity model until the most effective and beneficial state is achieved for the enterprise.

Nevertheless, the contributed AMM also recognises that some organisations might require in the short-term realistic levels of automation for their accountability practices, which can be achieved through the low-level metrics also proposed in this paper. As future work we plan to continue with the elicitation of new accountability controls, and to contribute the AMM notions to relevant standardisation bodies through A4Cloud's WP:A-5.

8.3 Evidence-based Accountability

This section introduces chains of evidence and evidence practices in terms of organisational practices. In particular it discusses three main perspectives, i.e., evidence as supporting risk management and governance, evidence in the cloud, and evidence practices. From a technical viewpoint, evidence is considered among the three fundamental capabilities of an accountable system (ENISA, 2011):

- **Validation:** *"It allows users, operators and third parties to verify a posteriori if the system has performed a data processing task as expected"*
- **Attribution:** *"In case of a deviation from the expected behaviour (fault), it reveals which component is responsible"*
- **Evidence:** *"It produces evidence that can be used to convince a third party that a fault has or has not occurred"*.

The first two capabilities relate directly to the accountability attributes of verifiability and attributability (as identified by the Accountability Model in Section 5). The third capability of evidence is the combined result of observability (what can be monitored) and transparency (what would be shared about what is happening with the data). This section highlights how evidence is part of accountability governance. That is, the provision of evidence characterises an accountability-based approach. It discusses three main perspectives of evidence. The first one is concerned with evidence as supporting assurance within enterprise information risk management. The second perspective is concerned with the problem of gathering evidence in cloud ecosystems. In particular, it discusses practical issues of collecting evidence across cloud supply chains and multi-tenant domains. The final discussion reviews a framework of evidence for accountability. This section therefore considers the provision of evidence as part of the account. Accountability evidence, taking into account an operational viewpoint of accountability, is defined (by the C8 work package) as follows:

Accountability Evidence as collection of data, metadata, routine information and formal operations performed on data and metadata which provide attributable and verifiable account of the fulfilment of relevant obligations with respect to the service and that can be used to support an argument shown to a third party about the validity of claims about the appropriate and effective functioning (or not) of an observable system.

8.3.1 Gathering Evidence

Evidence gathering is just one aspect of managing risk. Within organisational risk management processes, security and privacy policies are translated into implementable solutions that make use of specific mechanisms (e.g. security controls) in order to monitor operationally the implementation of such policies. Any policy violation detected is then assessed as part of risk management. Therefore, the gathering of evidence is critical for several reasons. First, evidence gathering would reflect organisational policies as they are implemented by means of specific mechanisms, for instance, such as security controls. Second, evidence gathering will inform organisational risk management. The gathering of evidence then is critical for mitigating operational risks, supporting information sharing and building trustworthiness. From a practical viewpoint, it is therefore necessary to clearly define what evidence to gather and what evidence to share.

This is also relevant in the case of supply chain risk management (NIST SP 800-161, 2013). In a cloud supply chain, the problem of gathering evidence becomes more complex (than gathering and sharing evidence within a single organisation). First of all, most of the mechanisms deployed across supply chains belong to different organisations with different access rights. Therefore, monitoring and gathering evidence would be constrained by many proprietary, contractual and legal aspects of cloud supply chains - for instance, cloud providers' own resources and services that are offered to and managed on behalf of cloud customers. Therefore, despite the fact that cloud providers might own resources and services, they nevertheless might be limited in what they can actually monitor and collect as evidence. Vice versa, in some cases cloud providers might manage proprietary resources and services that belong to cloud customers (this could be the case of Private Clouds). Another practical problem in a cloud supply chain is due to multi-tenancy. The gathering of evidence in a multi-tenancy context might be concerned with confidential information of neighbour tenants. This gives rise to many security and privacy concerns with cloud services. Therefore, the gathering of evidence in a cloud supply chain faces different operational issues that need to be addressed in order to effectively support risk management as well as trustworthy cloud. Having a well-defined framework of evidence is accordingly the first step towards gathering evidence supporting accountability in cloud services. Note that gathering evidence in this section is mainly concerned with an organisational perspective. However, gathering of evidence can be analysed from three main viewpoints (Ruan et al., 2011): legal, organisational, technical. The legal perspective of gathering evidence deals mostly with multi-jurisdiction, multi-tenancy, multi-ownership and Service Level Agreement. Technical aspect of evidence encompasses the procedures and tools that are needed to gather evidence in a cloud computing environment. Organisational aspects of evidence involve at least two entities: the CSP and the cloud customer. However, the complexity (e.g. segregation of duties, collaborations, policies, etc.) widens when a CSP outsources services to other parties.

8.3.2 Supporting Assurance

Gathering evidence is central for organisational risk management processes (ENISA, 2011). Risk management intends to mitigate risks and identify operational trade-offs, that is, what it is reasonably feasible to achieve in terms of protections with respect to emerging security and privacy threats (CSA, 2013). Therefore, gathering evidence has a critical role in supporting risk management as well as assurance. On the one hand, evidence provides valuable information to risk management. On the other hand, evidence would support assurance – "Assurance is about providing confidence to stakeholders that the qualities of service and stewardship with which they are concerned are being managed and maintained appropriately" (Baldwin, Pym, Shiu, 2013). This is also particular important while dealing with emergent digital risk (Lloyd's, 2010) due to a certain extent to the shift required while deploying new technological paradigms like cloud computing. For instance, monitoring security events (and alerts) and the collection of relevant information are critical phases of security analytics (Casassa Mont et al., 2012). Figure 33 shows common Security Event & Incident Management Processes. All processes are

influenced and driven by the collection of events and alerts, and subsequently by the collection of further information of such events and alerts. The analyses of the collected events and alerts, and related evidence, and the identification of suitable incident remediation complete SIEM (Security Information & Events Management) processes.

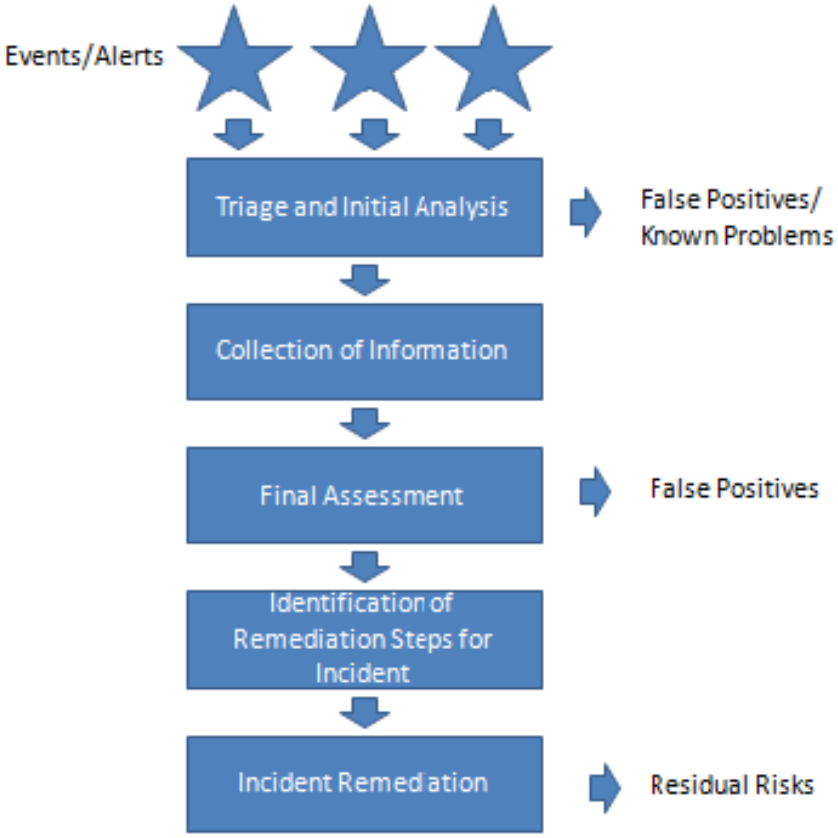


Figure 33 Security Event & Incident Management Processes (Casassa Mont et al., 2012)

The ability to collect evidence is constrained by the SIEM solutions that are deployed and actively monitored, e.g. Gartner provides a review of relevant SIEM technologies (Gartner, 2013). For instance, cloud security controls would enable monitoring of relevant events and security threats deployed in cloud ecosystems. The gathered evidence would also inform relevant metrics (e.g. risk and performance indicators) providing quantitative operational accounts of relevant events. Policy violation is an example of relevant information to be monitored for accountability.

8.3.3 Framework of Evidence for Accountability

Defining what type of evidence is critical in order to have effective governance of threats affecting cloud ecosystems. The deployments of specific mechanisms (e.g. cloud security controls) would enable monitoring of security and privacy threats mitigated by such mechanisms. Identifying and organising what mechanisms are deployed and monitored is part of organisational governance. This also highlights what information needs to be monitored in order to gather evidence supporting accountability. From a privacy perspective, the Nymity's Privacy Management Accountability Framework (Nymity, 2014) identifies thirteen different Privacy Management Processes (each consisting of multiple Privacy Management Activities). The privacy management processes (activities) are monitored and assessed in order to support accountability. Monitoring and assessing such processes (activities) is based on the collection of evidence, which is considered among the key elements of data privacy accountability (i.e. responsibility, ownership and evidence). An analysis of data privacy accountability emphasises the need for supporting evidence, in particular: the provision of evidence is necessary for supporting

organisational accountability (being able to demonstrate evidence on request); organisations manifest willingness to provide and demonstrate evidence; evidence needs to be demonstrable to third parties.

8.3.4 Account from Metrics Perspective

Initial work in deliverable D:C-5.1 on metrics for accountability identified “evidence” as a central concept for the process of eliciting metrics (Nuñez, Fernandez-Gago, 2013). From the metrics point of view, not all forms of account as perceived from a legal perspective are actually measurable, any assessment or evaluation of a property or attribute can only be made using as input some tangible information. The term “evidence” was used in this context to refer to the information used to support the assessment within a metric. Examples of “evidence” are an observation of a system, a system log, a certification asserted by a trusted party, a textual description of a procedure, etc. Hence, a metric does not directly measure a property of a process, a behaviour, or a system, but the evidence associated to them. It can be seen that the notion of evidence in this context is very broad and it is not limited to computerised data (such as a system log), but can be applied to more general information (e.g. the description of a process within an organisation, a certification, etc.). Note that it is unfeasible to measure any evidence highlighted from a legal point of view. Our analysis is concerned with “measurable forms of evidence”. In parallel to this definition of “evidence”, we find a preliminary definition of the notion of “account”: *"Account is a report or description of an event through the use of measurable forms of evidence".* That is, the notions of Account, Evidence and Event share the following relation (Figure 34):

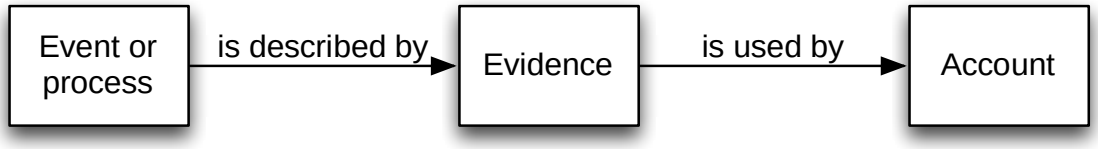


Figure 34 Relation between the Notions of Account, Evidence and Event

Building on top of the analysis performed in Section 4.1, we distinguish two types of accounts:

- Declarative account: The account consists of a description, such as a report, of a process or event. The account has primarily a retrospective function. It is important to note that not all forms of account as perceived from a legal perspective are actually measurable.
- Evaluative account: In this case, the account takes the form of an assessment of a process or an event, through the use of evidence. Same as above, “evidence” from a legal point of view does not necessarily relate to something measurable. Thus, evaluative accounts are restricted to measurable forms of evidence.

Taking into consideration this distinction and the concepts developed in deliverable D:C-5.1 (Nuñez, Fernandez-Gago, 2013), we note two main findings:

- There is a parallelism between the notion of "evidence" and declarative accounts. In some sense, we could argue that the notion of evidence is analogous to a declarative account (when related to measurable aspects).
- Metrics are of relevance for evaluative accounts during the assessment or evaluation procedure.

In Section 2, an account (from a legal perspective) is said to be a means for demonstrating accountability. Hence, metrics for accountability, supported by Declarative Accounts, could be considered as instruments to this end, by measuring how well accountability attributes are achieved in a particular context. The result of the application of metrics could be used by Evaluative Accounts to demonstrate compliance and fulfilment of accountability obligations. The relation among these concepts is depicted in Figure 35.

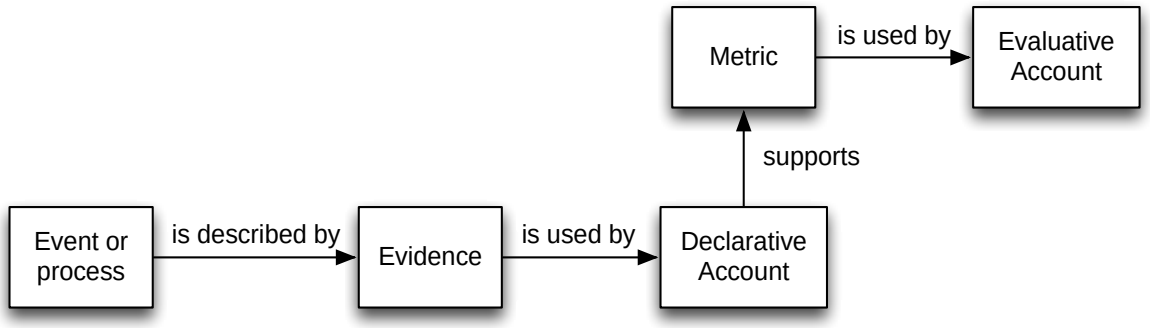


Figure 35 Metrics Meta-Model of the Account

8.4 Summary

This section has provided an operational analysis of accountability. In particular, the main contributions are: 1) Clarifying the notion of adaptive accountability, 2) Defining an Accountability Maturity Model, based on the quantitative assessment (that is, Accountability Metrics) of the maturity of an organisation in implementing specific mechanisms, and 3) Explaining an approach for evidence-based accountability. These contributions identify directions supporting the adoption of the A4Cloud's accountability-based approach of data governance in the cloud.

9 Conclusions

This document is an external A4Cloud project report that sets out the general approach of the A4Cloud project to providing a framework for trustworthy services supporting accountability in the cloud.

New data governance models for accountability, such as those underpinning Binding Corporate Rules in Europe and Cross Border Privacy Rules in Asia-Pacific Economic Cooperation (APEC) countries, can provide a basis for providing protection of personal data and confidential information when cloud computing is used. Accountable organisations ensure that obligations to protect such data are observed by all who process the data, irrespective of where that processing occurs. The A4Cloud project supports this vision by developing:

- *A framework for accountability*: a comprehensive specification for accountable service provision in the cloud and other future internet service provision models, spanning regulatory, legal, technical, business and user issues.
- *Trustworthy tools to support accountability* (for a variety of different stakeholders). These are largely based upon contractual assurances from cloud service providers to the accountable organisation and enhanced by a number of approaches including enforcement of the corresponding machine-readable policies, greater transparency, assurance and audit, with a role also for decision support.

However, we have also seen how the cloud is an incredibly complex and challenging domain. In the cloud context, the cloud client/controller may not be solely able to determine the purposes and the means of processing because the cloud service provider designs the infrastructure and also to some extent the services, in a way that depends upon the cloud model (namely, IaaS, PaaS or SaaS), as well as typically elaborating standard SLAs with little or no customisation possibility. In addition, lack of transparency and verifiability is a major problem that needs to be addressed. Furthermore, it needs to be demonstrated that an accountability-based approach can really add value in a practical sense in this domain without adding to the complexity.

It is the goal of the A4Cloud project's approach to help cut through this complexity and help provide more workable, effective solutions for data protection in cloud environments. This document serves towards that end by providing a conceptual model and framework for accountability in the cloud, together with a glossary of related terms.

References

Abadi M. (2003). “Logic in access control”. In *Proc. Symposium on Logic in Computer Science*, pp. 228-233.

AICPA, http://www.cica.ca/resources-and-member-benefits/privacy-resources-for-firms-and-organisations/item47888.aspx

Alhadeff, J., Van Alsenoy, B. & Dumortier, J. (2012). “The accountability principle in data protection regulation: origin, development and future directions”. In *Managing Privacy through Accountability*, ed. D. Guagnin et al., MacMillan, pp. 1-27.

APEC Data Privacy Sub-Group (2011). “Cross-border privacy enforcement arrangement”. San Francisco, 18 September, available at http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_010.pdf (accessed on 2 July 2012).

Baldwin, A. (2004). “Enhanced accountability for electronic processes”. In Christian Jensen, Stefan Poslad, and Theo Dimitrakos, editors, *Trust Management* , 2995, Lecture Notes in Computer Science , pp. 319-332. Springer Berlin Heidelberg, http://dx.doi.org/10.1007/978-3-540-24747-0 24.

Baldwin, A., Pym, D., Shiu, S. (2013). “Enterprise Information Risk Management: Dealing with Cloud Computing”. In S. Pearson and G. Yee (eds.), *Privacy and Security for Cloud Computing*, Springer-Verlag.

Baldwin, A., Shiu, S. (2010). “Managing Digital Risk: Trends, issues and implications for business”. Lloyds 360 Risk Insight.

Badger, L. et al. (2012). “Cloud Computing Synopsis and Recommendations”. NIST Special Publication 800-146, May.

Beiter, M., Casassa Mont, M., Chen, L., Pearson, S. (2012) “End-to-End Policy Based Encryption Techniques for Multi-Party Data Management”. *Computer Standards and Interfaces*, Special Issue, ISI Journal Citation Reports, D.G. Rosado (ed.).

Bella G, & Paulson L. C. (2006). “Accountability protocols: Formalised and verified”. *ACM Trans. Inf. Syst. Secur.* , 9(2):138161, May. http://doi.acm.org.gate6.inist.fr/10.1145/1151414.1151416.

Bennett, C.J. (2012) “The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats”. In *Managing Privacy through Accountability*, ed. D. Guagnin et al., MacMillan, pp. 33-48.

Bennett, C.J. (1995). “Implementing privacy codes of practice”, PLUS 8830, Canadian Standards Institution

Bennett, C.J. & Raab, C.D. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. MIT Press, Cambridge, Massachusetts

Bernheim B. D. & Whinston M. (1999). “Incomplete contracts and strategic ambiguity”. *Amer. Econ. Rev.*, 88, pp. 902–932.

Black, J. (2008). “Constructing and contesting legitimacy and accountability in polycentric regulatory regimes”. *Regulation & Governance* 137.

Bovens, M. (2007). “Analysing and Assessing Accountability: A Conceptual Framework”. *European Law Journal, 13(4),* pp. 447–468.

Bovens, M., Schillemans, T. (2009). *Handboek publieke verantwoording*. Den Haag: LEMMA.

Bovens, M. (2010). “Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism.” *West European Politics* 33 (5) (August 10) pp. 946–967. doi:10.1080/01402382.2010.486119.

Boyens, J., C. Paulsen, R. Moorthy, N. Bartol & S. A. Shankles (2013). “Supply Chain Risk Management: Practices for Federal Information Systems and Organisations”, NIST SP 800-161.

Bowker, G.C. & S.L. Star (1999). *Sorting things out: classification and its consequences*, The MIT Press, Cambridge.

Bradshaw, S., Millard, C., and Walden, I. (2013). “Standard Contracts for Services”, *Cloud Computing Law*, ed. Millard, C., pp. 37 – 72.

Brownsword, R. (2008). *Rights, Regulation and the Technological Revolution.* Oxford University Press.

Bull J. & Watson J. (2004). "Evidence disclosure and verifiability", *Journal of Economic Theory*, 118(1), September, pp. 1-31, ISSN 0022-0531

Burmester M., Desmedt Y., Wright R. N., Yasinsac A. (2006). “Accountable Privacy”. *Proc. Security Protocols*, Springer, pp. 83-95.

Butin D., Chicote M., Le Métayer D. (2014). “Strong Accountability: Beyond Vague Promises”. *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges,* Serge Gutwirth and Ronald Leenes and Paul de Hert Eds., Springer, pp 343-369.

Casassa Mont, M., R. Brown, S. Arnell, N. Passingham (2012). “Security Analytics: Risk Analysis for an Organisation’s Incident Management Process”. HP Laboratories, HPL-2012-206.

Castelluccia, C., Druschel, P., Hübner, S., et al. (2011). “Privacy, Accountability and Trust - Challenges and Opportunities”, ENISA Report.

Catteddu, D. & Hogben, G. (eds.) (2009). “Cloud Computing: Benefits, Risks and Recommendations for Information Security”. ENISA Report, November.

Cavoukian, A. (2012). “Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era”. *Privacy Protection Measures and Technologies in Business Organisations: Aspects and Standards*, G. Yee (ed.), IGI Global, pp. 170-208.

Cavoukian, A., Taylor, S., and Abrams, M. (2010). “Privacy by Design: Essential for Organisational Accountability and Strong Business Practices.” *Identity in the Information Society* 3(2), pp. 405–413.

Cederquist J.G., Corin J.G., Dekker M.A.C., Etalle S., and Den Hartog, J.I. (2005). “An audit logic for accountability”. *Policies for Distributed Systems and Networks*. pp. 34-43. IEEE, http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1454301.

Charlesworth, A. & Pearson, S. (2012). “Developing Accountability-based Solutions for Data Privacy in the Cloud”. 26 (1), Innovation, Special Issue: Privacy and Technology, *European Journal for Social Science Research*, pp. 7-35. Taylor & Francis, UK.

Center for Information Policy Leadership (CIPL), Accountability Project (Galway Project). http://www.informationpolicycentre.com/accountability-based_privacy_governance/.

Center for Information Policy Leadership (CIPL) (2009). “Data protection accountability: the essential elements. A document for discussion”.
http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

Center for Information Policy Leadership (CIPL) (2010). “Demonstrating and measuring accountability: a discussion document”. Accountability Phase II – The Paris Project. http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF

Center for Information Policy Leadership (CIPL) (2011). “Accountability: A compendium for stakeholders”. The Galway Project.

Centre for Information Policy Leadership (2012). “Accountability: Data Governance for the Evolving Digital Marketplace.”

Cloud Computing Use Case Discussion Group (2010). “Cloud Computing Use Cases White Paper”. v4.0.

Cloud Security Alliance (CSA) (2010). “Top Threats to Cloud Computing”. v1.0, March, Cloud Security Alliance.

CSA (2011). “Security Guidance for Critical Areas of Focus in Cloud Computing”, v3.0, Cloud Security Alliance.

CSA (2013). “The Notorious Nine Cloud Computing Top Threats in 2013”. Top Threats Working Group, Cloud Security Alliance.

CSA (2013b). “STAR Certification Guidance Document: Auditing the Cloud Controls Matrix (CCM)”. https://cloudsecurityalliance.org/download/star-certification-guidance-document-auditing-the-cloud-controls-matrix-ccm/

CSA (2013c). “Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union”, Cloud Security Alliance, Privacy Level Agreement Working Group.

CSA (2014). “Cloud Controls Matrix”. v3. https://cloudsecurityalliance.org/research/ccm/

CSA (2012a). “Privacy Level Agreement (PLA)”, PLA Working Group. https://cloudsecurityalliance.org/research/pla/

CSA (2012b). “Cloud Trust Protocol (CTP)”. https://cloudsecurityalliance.org/research/ctp/

CSA (2013). “STAR Certification Guidance: Auditing the Cloud Controls Matrix (CCM)”. https://cloudsecurityalliance.org/download/star-certification-guidance-document-auditing-the-cloud-controls-matrix-ccm/

CNIL (2012). “Methodology for Privacy Risk Management”. http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

Council of Europe (1981). “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”.

Creese, S., Hopkins, P., Pearson, S., Shen, Y. (2009). “Data Protection-Aware Design for Cloud Computing”, *Proc. 1st CloudCom 2009*, ed. M.G. Jaatun, G. Zhao, C. Rong, Beijing, Springer LNCS 5931, pp. 119-130, December.

Crispo, B., and Ruffo, G. (2001). “Reasoning about accountability within delegation”. pp. 251-260. Springer-Verlag.

Crompton, M. (2006). “APEC Privacy Framework: Review, impact and progress”. International Transfer of Personal Data Conference. http://www.iispartners.com/downloads/apec_belgium.pdf

De Clercq, J *et al.* (2008). ‘The HP Security Handbook’, HP publication 4AA1-7729EEW. http://www.filibeto.org/unix/hp-ux/lib/security/misc/HP%20Security%20Handbook.pdf

De Colle, S., and C. Gonella (2002). “The Social and Ethical Alchemy: An Integrative Approach to Social and Ethical Accountability.” *Business Ethics: A European Review* 11 (1), pp. 86–96. doi:10.1111/1467-8608.00261.

De Hert, P. and Gutwirth, S. (2006). “Privacy, data protection and law enforcement. Opacity of the individual and transparency of power”. E. Claes, A. Duff and S. Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerpen/Oxford, Intersentia.

De Hert, P., Papakonstantinou, V., Wright, D., Gutwirth, S. (2013). "The proposed Regulation and the construction of a principles-driven system for individual data protection". Innovation: The European Journal of Social Science Research 6(1-2):133-144.
DOI:http://dx.doi.org/10.1080/13511610.2013.734047

Department Of Defense (1985). *Trusted computer system evaluation criteria*. 5200.28-STD, DoD, December 1985.

Dubnick, M.J. and J.B. Justice (2004). "Accounting for Accountability". In *Proc. 2004 Annual Meeting of the American Political Science Association.*

European Data Protection Supervisor (EDPS) (2012). *Glossary of terms*. http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/71#accountability.

EDPS (2012b). "Opinion on the Data Reform Package", 7th of March 2012.

EDPS (2012c). "Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the potential of Cloud Computing in Europe'".

EDPS (2012d). "Responsibility in the Cloud should not be up in the air". Article EDPS/12/15. http://europa.eu/rapid/press-release_EDPS-12-15_en.htm

European Network and Information Security Agency (ENISA) (2009). "Cloud computing: benefits, risks and recommendations for information security".

ENISA (2011). "Privacy, Accountability and Trust – Challenges and Opportunities".

ENISA (2010). "IT Business Continuity Management: An Approach for Small Medium Sized Organisations". Technical Report. January. http://www.enisa.europa.eu/act/rm/risk-management-for-smes-and-micro-enterprises/business-continuity-for-smes/at_download/fullReport

ENISA (2012). "Appropriate security measures for smart grids: Guidelines to assess the sophistication of security measures implementation".

European Commission (EC) (1995). "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data". http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

EC (2005). "The New SME Definition". http://ec.europa.eu/enterprise/policies/sme/files/sme_definition/sme_user_guide_en.pdf

EC (2012). "Proposal for a directive of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data". January. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf

EC (2012b). "Digital "to-do" list: new digital priorities for 2013-2014". http://ec.europa.eu/information_society/newsroom/cf/dae/itemdetail.cfm?item_id=9309

EC (2012c). "Digital Agenda Pillar III: Trust and Security". Available at: http://ec.europa.eu/digital-agenda/en/our-targets/pillar-iii-trust-security

EC (2012d). "Unleashing the Potential of Cloud Computing in Europe". http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF (2012)

EC (2013). "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". http://ec.europa.eu./information_society/newsroom/cf//document.cfm?doc_id=1667

EC (2013b). “Directive on Network and Information Security”. http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

European DG of Justice (Article 29 Working Party) (2009). “The future of privacy: joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (WP168)”. December.

European DG of Justice (Article 29 Working Party) (2010). “Opinion 3/2010 on the Principle of Accountability (WP 173)”. July. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

European DG of Justice (Article 29 Working Party) (2010). Opinion 1/2010 on the concepts of "controller" and "processor", WP 169. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

European DG of Justice (Article 29 Working Party) (2012). “Opinion 05/12 on Cloud Computing”. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

European Parliament (2012). “Fighting Cyber Crime and Protecting Privacy in the Cloud”. Directorate-General for Internal Policies. http://www.europarl.euopa.eu/RegData/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_EN.pdf

European Parliament (2013). “The US surveillance programmes and their impact on EU citizens' fundamental rights”. Directorate-General for Internal Policies, PE 474.405.

Federal Trade Commission (FTC) (2012). “Protecting Consumer Privacy in an Age of Rapid Change: Recommendations for Business and PolicyMakers”. FTC Report, March

Feigenbaum, J., Jaggard, A.D. and Wright, R.N. (2011). “Towards a Formal Model of Accountability”. Sean Peisert, Richard Ford, Carrie Gates, and Cormac Herley (eds.), *NSPW* , pp. 45-56. ACM. http://dl.acm.org/citation.cfm?id=2073276.

Felici, M., Koulouris, T, & Pearson, S. (2013). “Accountability for Data Governance in Cloud Ecosystems.” *Proc. IEEE CloudCom 2013*, 2, pp. 327-332. IEEE.

Filiz-Osbay, E. & Osbay, E.Y. (2012). “Effect of an Audience on Public Goods Provision”. May. http://econweb.umd.edu/~ozbay/audience.pdf

Forrester Research, Inc (2011). “Ignoring Cloud Risks: A Growing Gap between I&O and the Business”. March.

Galway Project (2009). “Introduction”, *Proceedings to Plenary Session*, April 28th, p. 5.

Generally Accepted Privacy Principles (GAPP) (2014). http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/GENERALLYACCEPTEDPRIVACYPRINCIPLES/Pages/default.aspx

Gartner (2013). “Magic Quadrant for Security Information and Event Management”.

Gellert, R., & Gutwirth, S. (2012). “Beyond Accountability, the Return to Privacy?” *Managing Privacy through Accountability*, D. Guagnin et al. (eds.), MacMillan, pp. 261-284.

Gellman, R. (2009) “Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing”. World Privacy Forum.

Georgia Tech Information Security Center (GTISC) and Georgia Tech Research Institute (GTRI) (2013). “Emerging Cyber Threats Report 2014”. Georgia Institute of Technology, Georgia Tech Cyber Security Summit.

Gershoni, T., Mowbray, M. & Pearson, S. (2013). “Mechanisms for protecting sensitive information in cloud computing”. Secure Cloud Infrastructure, Special Issue, *International Journal of Computer Systems Science and Engineering* 28 (6), November.

Goodin, R. E. (2003). “Democratic Accountability: The Distinctiveness of the Third Sector.” *European Journal of Sociology/Archives Européennes De Sociologie* 44 (3), pp. 359–396. doi:10.1017/S0003975603001322.

Gray, A. & Jenkins, W. (1985). *Administrative Politics in British Government*, Brighton: Wheatsheaf Books, p. 138.

GSMA Mobile and Privacy (2012). “Accountability Framework for the implementation of the GSMA Privacy Design Guidelines for Mobile App Development”. February. http://www.gsma.com/publicpolicy/wp-content/uploads/2013/01/Accountability-framework-final.pdf

Guagnin, D., Hempel, L., Ilten, C. (2012). “Bridging the gap: We need to get together”. Guagnin, D. *et al.* (eds.), *Managing Privacy through Accountability*. Palgrave, pp. 102-124.

The Guardian (2013). “NSA Prism program taps in to user data of Apple, Google and others”. June 7. http://www.guardian.co.uk/world/2013/jun/06/us-techgiants-nsa-data

Haeberlen A., Aditya P., Rodrigues R., & Druschel P. (2010). “Accountable virtual machines”. *Proc. 9th {USENIX} Symposium on Operating Systems Design and Implementation*, pp. 119--134, http://www.usenix.org/event/osdi10/tech/full_papers/osdi10_proceedings.pdf.

Hale, T. (2008). “Transparency, Accountability, and Global Governance”. *Global Governance* 73.

Help Net Security (2012). “The threat landscape continues to expand rapidly”. http://www.net-security.org/secworld.php?id=14166

Help Net Security (2012b). “Guidance on cybersecurity, private clouds and privacy”. http://www.net-security.org/secworld.php?id=14155

Hildebrandt, M. (2009). *Biometric Behavioural Profiling and Transparency Enhancing Tools*. FIDIS Project Deliverable 7.12. http://www.scribd.com/doc/72120638/Fidis-wp7-Del7-12-Behavioural-biometric-Profiling-and-Transparency-Enhancing-Tools

Hijmans, H. (2011). “Principles of Data Protection: Renovation Needed?” Presentation held during the International Data Protection Conference, Budapest, 16-17 June.

Hogan, M. et al. (2011). *NIST Cloud Computing Standards Roadmap*, NIST Special Publication 500-291, v1.0.

Hon, K., Kosta, E., Millard, C., Stefanatou, D. (2014). “White Paper on the Proposed Data Protection Regulation”, D25.1, v1.0, A4Cloud Deliverable, Kuan Hon (ed.), March.

Hon, W.K., Millard, C. & Walden, I. (2011). “The Problem of “Personal Data” in Cloud Computing - What Information is Regulated? The Cloud of Unknowing”, Part 1. *SSRN Electronic Journal*, International Data Privacy Law 1(4) pp. 211–228.

Hon, W.K., Millard, C. & Walden, I. (2012). “Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing”. Part 2. *International Data Privacy Law* 2(1) pp. 3-18.

Hon, W. K., Millard, C, & Walden, I. (2013). “Negotiated Contracts for Cloud Services”. *Cloud Computing Law*, C. Millard (ed.), pp.. 73 – 107.

Horwath, C. (2012). “Enterprise Risk Management for Cloud Computing”. COSO, June. http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf

Hunt, G. (2006). “The principle of complementarity: freedom of information, public accountability and Whistleblowing”, p. 11.

Howell, J. and Kotz, D. (2000). “End-to-end authorisation”. In *OSDI 2000*, pp. 151-164.

International Conference of Data Protection and Privacy (ICDPP) (2009). “31st International Conference of Data Protection and Privacy ‘Data protection authorities from over 50 countries approve the “Madrid Resolution” on international privacy standards’”. http://www.gov.im/lib/docs/odps//madridresolutionpressreleasenov0.pdf

International Data Corporation (IDC) (2012). “Removing Barriers to Cloud Computing in Europe Through Policy Action Could Generate up to €250Bn EU GDP Growth in 2020, says IDC”. Press Release. http://www.idc.com/getdoc.jsp?containerId=prIT23744212#.UUl3jVdI20p

Information Commissioner’s Office UK (ICO) (2007). “Data protection guidance note: Privacy enhancing technologies”.

ICO (2010). “The Privacy Dividend: The Business Case for Investing in Proactive Privacy Protection”. March http://www.ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_DIVIDEND.ashx

ICO (2012a). “Binding corporate rules”. http://www.ico.gov.uk/for_organisations/data_protection/overseas/binding_corporate_rules.aspx

ICO (2012b). “Guidance on the Use of Cloud Computing”. http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

Institute of Internal Auditors (2012). *Managing and Auditing Privacy Risks.* Available at: http://www.theiia.org/download.cfm?file=33917

International Privacy Standards (2010): Can Accountability be Adequate?” Privacy Laws and Business International, 106:21-23.

International Organisation for Standardisation (ISO) (2011). “Information technology – Security techniques – Privacy framework”. Technical report, ISO/IEC 29100, ISO JTC 1/SC 27.

ISO (2014). “Information Technology, Security Techniques, Code of Practice for Information Security Management”. Technical report, ISO-IEC 27002.

Jagadeesan, R., Jeffrey, A., Pitcher, C., & Riely, J. (2009). “Towards a theory of accountability and audit”. Michael Backes and Peng Ning (eds.), *Computer Security ESORICS 2009*, 5789, Lecture Notes in Computer Science, pp. 152-167, http://dx.doi.org/10.1007/978-3-642-04444-1_10.

Jansen, W. & Grance, T. (2011). “Guidelines on Security and Privacy in Public Cloud Computing”. Special Publication 800-144, NIST, December.

Jasanoff, S. (2009). “Governing Innovation”. http://www.india-seminar.com/2009/597/597_sheila_jasanoff.htm.

Jos, P. & Tompkins, M. (2004). “The Accountability Paradox in an Age of Reinvention: The Perennial Problem.” *Administration & Society,* 36 p. 255.

Kalman R. E. (1961). "On the General Theory of Control Systems". *Proc. 1st Int. Cong. of IFAC*, Moscow 1960 1 p. 481, Butterworth, London.

Kapiriria, L., Norheimb, O.F., & Martinc, D.K. (2009). “Fairness and accountability for reasonableness. Do the views of priority setting decision makers differ across health systems and levels of decision making?” *Social Science & Medicine* 68(4) pp. 766–773.

Kessler, G.C. (2012). "Advancing the Science of Digital Forensics," *Computer*, 45(12), pp. 25-27, Dec.

Knode, R., Egan, D., (2010). “Digital Trust in the Cloud: A Precis for the CloudTrust Protocol”. v2.0, Computer Science Corporation, 2010.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2010). “Ein modernes Datenschutzrecht für das 21. Jahrhundert”. 18 March.

Koppell, J. (2005). “Public administration review,” *Public Administration Review*, 65, pp. 94–108.

Kuan Hon, W., Millard, C. (2013): Control, Security and Risk in the Cloud, In Cloud Computing Law, Oxford University Press, p. 27.

Küsters R., Truderung T., and Vogt A. (2010). “Accountability: definition and relationship to verifiability”. pp. 526-535. ACM, http://dl.acm.org/citation.cfm?id=1866366.

Ko, R.K.L., Lee, S.S.G., & Rajan, V. (2012). “Understanding Cloud Failures”. *IEEE Spectrum* 49(12) p.84.

Lake, R. (1999). “Social Accountability, the OECD Guidelines for Multinational Enterprises and the OECD Principles of Corporate Governance”. http://www.oecd.org/investment/mne/2089880.pdf

Lampson B., (2004). “Computer security in the real world”. *IEEE Computer*, 37(6) pp. 37-46, June.

Law, J., & Hassard, J. (1999). *Actor network theory and after*. Oxford: Blackwell.

Lin K., Zou J., & Wang Y. (2010). *Accountability computing for e-society.* pp. 34-41. IEEE, http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5474671.

Liu, F. *et al.* (2011). “NIST Cloud Computing Reference Architecture”. NIST Special Publication 500-292, September.

Le Métayer, D. (2009). “A formal privacy management framework”. *Formal Aspects in Security and Trust*, pp. 1-15, http://www.springerlink.com/index/q7505648948p9710.pdf.

Le Métayer, D. (2011). “Formal methods as a link between software code and legal rules”. *Software Engineering and Formal Methods*, pp. 3-18, http://www.springerlink.com/index/980H052715W527GQ.pdf.

Lloyd’s (2010), *Lloyd’s 360° Risk Insight Managing Digital Risk: Trends, Issues and Implications for Business.*

Locke, G. (2013). “Recommended Security Controls for Federal Information Systems”. Tech. Rep. NIST 800-53v4, National Institute of Standards and Technology. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Macnaghten, P. Kearnes, M.B. & Wynne, B. (2005). “Nanotechnology, Governance, and Public Deliberation: What Role for the Social Sciences?” *Science Communication,* 27 p. 268.

McQuay, T. (2013). “Data Privacy Accountability Scorecard”, Nymity Research Initiative.

Mell, P. & Grance, T. (2011). “The NIST Definition of Cloud Computing.” NIST Special Publication 800-145, September.

Millard, C. (ed.). (2013) *Cloud Computing Law.* Oxford University Press.

Möllering, G. (2006). *Trust: Reason, Routine, Reflexivity*. Elsevier, Oxford.

Moerel, L. (2011). *Binding corporate rules*. PhD thesis, Tilburg University.

Mulgan, R. (2003). *Holding power to account: accountability in modern democracies*. Basingstoke: Palgrave MacMillan.

National Institute of Standards and Technology (NIST) (2007). "Information Security Handbook: A Guide for Managers." NIST Special Publication 800-100. http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

Nissenbaum H. (1994). "Computing and accountability". *Communications of the ACM*, 37(1), pp. 72-80.

Novotny, A., & Spiekermann, S. (2013). "Personal Information Markets AND Privacy: A New Model to Solve the Controversy". *Proceedings of the 11th International Conference on Wirtschaftsinformatik* (WI 2013), 26 Feb - 1 Mar, Leipzig, Germany, pp. 1635-1649.

Nuñez, D., Fernandez-Gago, C. (eds.) (2013). Metrics for Accountability, A4Cloud D.35.1, v1.0.

Nymity Research (2014). "Implementing and Demonstrating Accountability." http://www.pcpd.org.hk/privacyconference2014/files/9_booklet_guide.pdf

Organisation for Economic Co-operation and Development (OECD) (1980). "Guidelines for the protection of personal data and transborder data flows." http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html

OECD (2013). "Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Data." http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner for British Colombia (2012). "Getting Accountability Right with a Privacy Management Program." http://www.oipc.bc.ca/guidance-documents/1435

Office of the Privacy Commissioner of Canada (2007). "Privacy Impact Assessments." February. http://www.priv.gc.ca/fs-fi/02-05-d-33-e.cfm

Omand, D., Bartlett, J. & Miller, C. (2012). "A balance between security and privacy online must be struck…" DEMOS Report. http://www.demos.co.uk/files/_Intelligence_-_web.pdf?1335197327

O'Neill, O. (2002). www.bbc.co.uk/radio4/reith2002

OpenGroup (2009). "A Maturity Model for SOA." http://www.opengroup.org/projects/soa-book/page.tpl?CALLER=faq.tpl&ggid=1319

Parris K. (1996). "Implementing Accountability." *IEEE Software*, 13(4), pp. 83-93.

Pearson, S. (2011). "Toward Accountability in the Cloud." *Internet Computing*, IEEE, July/August issue, 15(4), pp. 64-69.

Pearson, S. (2012). "Privacy Management in Global Organisations." B. De Decker and D.W. Chadwick (eds.): *CMS 2012*, LNCS 7394, pp. 217–237, IFIP.

Pearson, S. (2012b). "Privacy, Security and Trust in Cloud Computing". Pearson, S., Yee, G. (eds.), *Privacy and Security for Cloud Computing*, Computer Communications and Networks. Springer pp. 3-42.

Pearson, S. (2013). "On the Relationship between the Different Methods to Address Privacy Issues in the Cloud." *OTM 2013 Conference*, R. Meersman, H. Panetto et al (eds.), Springer, LNCS, pp. 414-433.

Pearson, S. (2014). "Privacy Management and Accountability in Global Organisations." *Proc. IFIP Privacy Summer School 2013*, Springer. IFIP AICT 421, pp. 33–52.

Pearson, S. & Charlesworth, A. (2009). "Accountability as a Way Forward for Privacy Protection in the Cloud". *Proc. IEEE CloudCom*, M.G. Jaatun, G. Zhao, C. Rong (eds.), Beijing, Springer LNCS 5931, pp. 131-144.

Pearson, S. & Sander, T. (2011). "A decision support system for privacy compliance." *Strategic and Practical Approaches for Information Security Governance*, IGI Global.

Pearson, S. & Shen, Y. (2010). "Context Aware Privacy Design Pattern Selection." *Trust, Privacy and Security in Digital Business*, LNCS 6264, pp. 69-80, Springer.

Pearson, S. & Tsiavos, P. (2014). "Taking the Creative Commons beyond Copyright: Developing Smart Notices as User Centric Consent Management Systems for the Cloud". *International Journal of Cloud Computing*, 3, pp. 94-124.

Pearson, S. et al., (2012). "Accountability for Cloud and Other Future Internet Services." *Proc. CloudCom 2012*, IEEE, pp. 629-632, December.

Pearson, S. & Wainwright, N. (2012). "An Interdisciplinary Approach to Accountability for Future Internet Service Provision." *International Journal of Trust Management in Computing and Communications (IJTMCC)*, 1(1) pp. 52-72.

Philp, M. (2009). "Delimiting democratic accountability". *Political Studies*, *57*(1), pp. 28-53.

PIPEDA (2000). Personal Information Protection and Electronic Documents Act. http://laws-lois.justice.gc.ca/eng/acts/P-8.6/

Pinch, T. J., and W. E. Bijker (1984). "The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other." *Social Studies of Science* 14 pp. 399–441.

Project Management Body of Knowledge (PMBOK) (2011). "Adoption of the Project Management Institute (PMI(R)) Standard: A Guide to the Project Management Body of Knowledge." 4th edition, IEEE.

Ponemon Institute (2013). "Security of Cloud Computing Users Study." http://www.ponemon.org/blog/new-security-of-cloud-computing-users-2013-study-confirms-conflicting-views-on-cloud-security-responsibility

Pym, D. & Sadler, M. (2010). "Information Stewardship in Cloud Computing", *International Journal of Service Science*, Management, Engineering and Technology, 1(1), January-March, pp. 50-67.

Raab, C. (2012). "The Meaning of 'Accountability' in the Information Privacy Context". *Managing Privacy through Accountability,* D. Guagnin et al. (eds.), MacMillan, pp. 15-32.

Radack, S. (ed.) (2012). "Guidelines For Improving Security And Privacy In Public Cloud Computing." ITL Bulletin, March. http://csrc.nist.gov/publications/nistbul/march-2012_itl-bulletin.pdf

Regan, Priscilla M and Johnson, Deborah G. (2012). "Privacy and Trust in Socio-technical Systems of Accountability". *Managing Privacy through Accountability*, D. Guagnin et al. (eds.), MacMillan. pp. 125 – 142.

Rodriques, T. (2012). "Mitigating Cloud Security and Privacy Risks." *Computing Now Blog.* http://www.computer.org/portal/web/computingnow/cloud/content?g=53319&type=article&urlTitle=mitigating-cloud-security-and-privacy-risks

Romzek, BS and Dubnick, MJ. (1987). "Accountability in the Public Sector: Lessons from the Challenger Tragedy." *Public Administration Review*. http://www.jstor.org/stable/10.2307/975901.

Ruan , K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). "Cloud forensics: An overview". *Proc. IFIP International Conference on Digital Forensics*, 7.

Sander, T. & Pearson, S. (2010). "Decision Support for Selection of Cloud Service Providers." *International Journal on Computing (JoC)*, GTSF.

Schedler, A. (1999). *Self-Restraining State: Power and Accountability in New Democracies*. Lynne Reiner Publishers, pp. 13–28.

Schillemans, T. & Bovens, M.A.P. (2009). "Publieke verantwoording 2.0: sober maar scherp." In: Bovens, M.A.P., Schillemans, T., (red). Handboek publieke verantwoording. Den Haag: Lemma, pp. 275-294.

Schneider, F.B. (2009). "Accountability for perfection". *Security & Privacy*, IEEE, http://ieeexplore.ieee.org/xpls/abs all.jsp?arnumber=4812145.

Schütz, P. (2012). "Accountability and Independence of Data Protection Authorities – A Trade-Off?" *Managing Privacy through Accountability*, D. Guagnin et al. (eds.), MacMillan, pp. 233-260.

Schweiker, W. (1993). "Accounting for Ourselves: Accounting Practice and the Discourse of Ethics." *Accounting, Organisations and Society,* 18 (2–3) pp. 231 – 252.

Sekar V. and Maniatis P., (2011). "Verifiable resource accounting for cloud computing services." *Proceedings of the 3rd ACM workshop on Cloud computing security workshop,* CCSW '11, p. 2126, New York, NY, USA, ACM, http://doi.acm.org/10.1145/2046660.2046666.

Shearer, T. (2002). "Ethics and Accountability: From the For-itself to the For-the-other." *Accounting, Organisations and Society* 27 (6) (August) pp. 541–573.

Smith, R. (2008). "Cloud Maturity Models Don't Make Sense." http://www.informationweek.com/blog/main/archives/2008/12/cloud_maturity.html;jsessionid=OL1NSZLUOGDMCQSNDLPCKHSCJUNN2JVN
Solove, D. (2009). *Understanding Privacy*. Harvard University Press.

Software Engineering Institute (SEI) (2010). "CMMI for development: Improving processes for developing products and services." Technical Report, v1.3, November. http://www.sei.cmu.edu/reports/10tr033.pdf

Sorofman, J. (2009). "The cloud computing adoption model." http://www.ddj.com/architect/211201818

Szolovits P. (1996). "Sources of error and accountability in computer systems: Comments on "accountability in a computerised society"", *Science and Engineering Ethics*, Springer, 2(1), pp. 43—46.

Sundareswaran S., (2012). "Ensuring distributed accountability for data sharing in the cloud." *Dependable and Secure Computing*, 9, http://ieeexplore.ieee.org/xpls/abs all.jsp?arnumber=6165313.

Tancock, D., Pearson, S., & Charlesworth, A. (2010). "Analysis of Privacy Impact Assessments within Major Jurisdictions." In *Proc. PST 2010*, Ottawa, Canada. IEEE.

Thomas, R. (2009). Foreword of RAND study "Review of Data Protection Directive Summary." http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf

Trilateral Research and Consulting (2013). "Privacy Impact Assessment and Risk Management." ICO report, May http://www.ico.org.uk/~/media/documents/library/Corporate/Research_and_reports/pia-and-risk-management-full-report-for-the-ico.pdf

Tsoukas, H. (1997). "The Tyranny of Light". *Futures*, 29(9), Elsevier Science Lts, pp. 827-843.

Urquhart, J. (2009). "A maturity model for cloud computing." http://news.cnet.com/8301-19413_3-10122295-240.html

Van Alsenoy, B. (2012). "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC." *Computer Law & Security Review*, 28, pp. 25-43.

Wang, Y., & Lin, K.-J. (2008). “Reputation-Oriented Trustworthy Computing in E-Commerce Environments”. *Internet Computing*, IEEE, 12(4), pp. 55–59.

Wang, C. and Zhou, Y. (2010). “A collaborative monitoring mechanism for making a multitenant platform accountable”. *Proc. 2nd USENIX conference on Hot topics in cloud computing*, HotCloud'10, p. 1818, Berkeley, CA, USA, USENIX Association, http://dl.acm.org/citation.cfm?id=1863103.1863121.

Wardley, S. (2009). “Maturity models for the cloud.” http://blog.gardeviance.org/2008/12/maturity-models-for-cloud.html

Watson, G. (1996). “Two Faces of Responsibility”. *Philosophical Topics* 24, pp. 227–248.

Wei W., Du J., Yu T., & Gu X, (2009). “SecureMR: a service integrity assurance framework for MapReduce”. *Proc. 2009 Annual Computer Security Applications Conference,* ACSAC '09, p. 7382, Washington, DC, USA. IEEE Computer Society. http://dx.doi.org/10.1109/ACSAC.2009.17

Weitzner, D. et al. (2006). “Transparent Accountable Data Mining: New Strategies for Privacy Protection.” *Proc. Spring Symposium on The Semantic Web meets eGovernment*, AAAI Press.

Weitzner, D.J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G.J. (2008). “Information accountability.*” Communications of ACM* 51(6), pp. 82-87, June.

White House (2012). “Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.” http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

Wynne, B. (1988). “Unruly technology: Practical rules, impractical discourses and public understanding.” *Social Studies of Science* 18(1) pp. 147–167.

Xiao Z., Kathiresshan N. & Xiao Y., (2012). “A survey of accountability in computer networks and distributed systems”. *Security and Communication Networks.* http://dx.doi.org/10.1002/sec.574.

Zabczyk J. (1992). *Mathematical Control Theory: An Introduction*. Birkauser Boston.

Appendices

A. A4Cloud Project Objectives

As presented in (Pearson et al, 2012), the project objectives are to:

1. develop tools that enable cloud service providers to give their users appropriate control and transparency over how their data is used, confidence that their data is handled according to their expectations and is protected in the cloud, delivering increased levels of accountability to their customers.
2. create tools that enable cloud end users to make choices about how cloud service providers may use and will protect data in the cloud, and be better informed about the risks, consequences, and implementation of those choices.
3. develop tools to monitor and check compliance with users' expectations, business policies and regulations.
4. develop recommendations and guidelines for how to achieve accountability for the use of data by cloud services, addressing commercial, legal, regulatory and end user concerns and ensuring that technical mechanisms work to support them.

B. Prior Analysis of Accountability

In developing the model of accountability presented in Section 5, we have taken into account the way in which this concept is being used in different communities. In particular, in data protection regulation since the 1980s, accountability has been used in the sense that the Data Controller is responsible for complying with particular data protection legislation and, in most cases, is required to establish systems and processes which aim at ensuring such compliance. In IT governance, accountability is used in the sense that the information security management system of an organisation is meant to generate assurance, transparency and responsibility in support of control and trust. For corporate governance, accountability is viewed as an organisational privacy management program. There are also other types of usage coming from social science and computer science. In this section we provide an analysis of this historical and current usage as background to our novel contributions towards conceptual analysis given in Section 2 (where we presented the concept of accountability), Section 5 (a model of accountability) and in Sections 6 and 7 (where we discuss a framework of accountability, and how to achieve this in practice).

Evolution of the Concept

We consider a selection of definitions of accountability, starting with high-level conceptual definitions and proceeding toward a more organisational, governance-related view. We will look at conceptions of accountability from diverse disciplines.

Webster's dictionary of 1828 defines accountability thus:
"1. The state of being liable to answer for one's conduct; liability to give account, and to receive reward or punishment for actions. 2. Liability to the payment of money or of damages; responsibility for a trust."

This definition has changed in the latest version of the dictionary to exclude the reward and punishment aspects, which nevertheless are relevant to our present purpose. Key ingredients of this definition include attribution of responsibility ('being liable to answer for…'), giving explanations, receiving a penalty for any misconduct (especially, being financially liable for damages). These same ingredients are echoed in Schedler's definition (Schedler, 1999):

"A is accountable *to B when A is obliged to inform B about A's (past or future) actions and decisions, or justify them and to be punished in the case of misconduct."*

Taking an organisational perspective, Koppell (2005) identifies five dimensions of accountability:

"1. Transparency: Did the organisation reveal the facts of its performance?
2. Liability: Did the organisation face consequences for its performance?
3. Controllability: Did the organisation do what the principal desired?
4. Responsibility: Did the organisation follow the rules?
5. Responsiveness: Did the organisation fulfil the substantive expectation?"

Note that Koppell's definition identifies performance as the principal concern around which accountability is centred. Accountability is understood in relation to performance, which is the objective for which managers are held accountable. Jos and Tompkins (2004) explain that accountability processes can either be performance-based or compliance-based; most of the definitions of interest to us are geared towards compliance with prevailing laws and regulations.

The distinction between accountability and responsibility is made in the following definition (Galway, 2009): *"Accountability is the obligation and / or willingness to demonstrate and take responsibility for performance in light of agreed upon expectations. Accountability goes beyond responsibility by obligating an organisation to be answerable for its actions"*.

From the social sciences we have, among others, Romzek and Dubnick's typology (1987) of public sector accountability; this is a classification of the different ways in which public sector officials are held accountable, and emphasises the responsibility and liability aspects of the concept of accountability.

The typology distinguishes between legal, political, bureaucratic and professional accountability regimes, each representing a form of responsibility to a particular audience (e.g. bureaucratic accountability being defined as responsibility to those higher up in a bureaucratic hierarchy).

The privacy-oriented definition of accountability given in ISO standard 29100 (ISO, 2011) expresses accountability in terms of the practices associated with it in organisations:
"Accountability: document policies, procedures and practices, assign the duty to implement privacy policies to specified individuals in the organisation, provide suitable training, inform about privacy breaches, give access to effective sanctions and procedures for compensations in case of privacy breaches."

This definition clearly picks out privacy breaches as being the problem that accountability as a whole is intended to address, and identifies specific ways to respond to the problem. It gives clear guidance on how to actualise accountability, avoiding what it is. Clearly it is desirable to combine some of the operational aspects with a high-level conceptual description of the concept, in order to produce a definition that meets the needs of researchers and practitioners alike.

We mention here the Galway project's definition of accountability, which refers specifically to the handling of personal data, and to which we will refer to frequently below:
"Accountability is the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information beyond mere legal requirements, and to be accountable for any misuse of that information."

Accountability concepts are evolving as the current legal framework responds to globalisation and new technologies, and indeed the current drafts of the proposed EU Data Protection Regulation (EC, 2012) and US Consumer Bill of Rights (The White House, 2012) include this concept, at least at a conceptual level (see further discussions in Section 3.2 below). Region block compliance tools such as the EU's binding corporate rules (BCRs) (ICO, 2012) and APEC's cross border privacy rules (CBPRs) (APEC Data Privacy Sub-Group, 2011) are being developed to provide a cohesive and more practical approach to data protection across disparate regulatory systems (Moerel, 2011). See also 'The future of privacy', from the Article 29 Working Party (EC, 2009; Article 29 Working Party, 2012), its opinion of July 2010 (EC, 2010), and the Madrid resolution's global data protection standards (ICDPP, 2009), which the International Conference of Data Protection and Privacy Commissioners adopted in October 2009. The Galway/Paris project started by privacy regulators and privacy professionals has been defining the concept of accountability for the last four years in the context of these latest regulations (CIPL, 2009) and refining its implementation, measurement and scalability.

Accountability is a tool being used by more and more regulators around the world, especially as privacy legislation is enacted or changed in response to technical change and globalisation. It is increasingly popular in common law jurisdictions such as Australia, Canada and US and has gained more visibility and acceptance in places governed by civil law. It is not only in the legislation referred to above but also a concept included within enforcement powers in Canada and in new laws being introduced in Latin America (see for example, Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner for British Colombia, 2012).

Accountability as a notion established in guidance such as OECD (OECD, 1980), APEC (APEC Data Privacy Sub-Group, 2011) and PIPEDA (PIPEDA, 2000) essentially means placing a legal responsibility upon an organisation that collects and uses personal data to ensure that contracted partners to whom it supplies the personal data are compliant and equally accountable, wherever in the world they may be. Its notion as a data protection model is evolving towards being an 'end-to-end' personal data stewardship regime in which the enterprise that collects the data from the data subject is accountable for how the data is shared and used throughout its journey across the global and its lifecycle from collection to disposal.
There is a slightly different element highlighted by Weitzner and others, who argue that a shift is needed from hiding information to ensuring only appropriate uses occur. They describe the ability to maintain a history of data manipulations and inferences (their interpretation of transparency) which can then be checked against a set of policies that govern them (their interpretation of accountability). For them,

accountability is retrospective, in the sense that if actor A performs action B then we can review B against a predetermined policy to decide if A has done something wrong, and hence hold A accountable.

Regulatory Frameworks

The A4Cloud project will focus on personal data and on information that is not personal, but for which there is an obligation to some person or organisation to keep that information confidential. However, as the A4Cloud project will primarily deal with personal data, it is important to look into the regulatory framework relating to accountability in the data protection context.
The concept of accountability is enshrined in regulatory frameworks for data protection across the globe. The Organisation for Economic Cooperation and Development privacy guidelines (OECD, 1980) do not only embrace the concept but also take a step forward, addressing it quite clearly by considering the data controller as accountable with regard to compliance with measures implementing the established principles. The concept of accountability is also present in the Asia Pacific Economic Cooperation's privacy framework (APEC, 2005), as well as in Canada's Personal Information Protection and Electronic Documents Act (PIPEDA, 2000). Basic elements of the concept can also be found in Convention 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data (Council of Europe, 1981). One expression of accountability that is common in all aforementioned documents are the obligations posed to the data controller for complying with that particular data protection legislation and, in most cases, the establishment of systems and processes which aim at ensuring such compliance.

Although the Data Protection Directive does not introduce explicitly the principle of accountability, it does embrace it in several provisions. The text of the Data Protection Directive as such is structured on the acceptance of relationships between the different entities involved in the processing of personal data. The relationship between data controllers and data subjects constitutes the main relationship provided on which further relationships are built. The Directive also addresses relationships from which accountability obligations derive between data controllers-data processors and data controllers-supervisory authorities. These relationships are characterised by a substantial imbalance of powers in practice in the course of processing between the data subject and the data controller, which justifies protection through accountability provisions (De Hert and Gutwirth, 2006). In his Glossary, the European Data Protection Supervisor (EDPS) has defined accountability as follows: "accountability intends to ensure that data controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice (....)" (EDPS, 2012).

In January 2012 the European Commission presented a proposal for a draft Regulation that is suggested to replace the Data Protection Directive. Although the draft Regulation does not include the term accountability in its text, the Explanatory Memorandum explains that Article 22 of the draft Regulation, entitled 'Responsibility of the controller' "takes account of the debate on a 'principle of accountability' and describes in detail the obligation of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance".

The Article 29 Working Party in its opinion on accountability made use of the term 'accountability', but explained the reasons why it may be difficult to use the term in all European languages:

"21. The term "accountability" comes from the Anglo-Saxon world where it is in common use and where there is a broadly shared understanding of its meaning –even though defining what exactly "accountability" means in practice is complex. In general terms though its emphasis is on showing how responsibility is exercised and making this verifiable. Responsibility and accountability are two sides of the same coin and both essential elements of good governance. Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed.

22. In most other European languages, due mainly to differences in the legal systems, the term "accountability" cannot easily be translated. As a consequence, the risk of varying interpretation of the term, and thereby lack of harmonisation, is substantial. Other words that have been suggested to capture the meaning of accountability, are "reinforced responsibility", "assurance", "reliability", "trustworthiness" and in French "obligation de rendre des comptes" etc. One may also suggest that accountability refers to the "implementation of data protection principles".

23. In this document, therefore we focus on the measures which should be taken or provided to ensure compliance in the data protection field. References to accountability should therefore be understood as the meaning used in this Opinion, without prejudice to finding another wording that more accurately reflects the concept given here. This is why the document doesn't focus on terms but pragmatically focuses on the measures that need to be taken rather than on the concept itself." (European DG of Justice, 2010)

The Article 29 Data Protection Working Party, national Data Protection Authorities (Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 2010), the European Data Protection Supervisor (EDPS), as well as the data protection and privacy regulators at the 31st International Conference of Data Protection and Privacy Commissioners – see reference (ICDPP, 2009) - have paid special attention to the principle of accountability. The common ground of these approaches has been the need to "reinforce" (EDPS, 2012b) accountability implying clearly its existence under the Data Protection Directive. The Article 29 Data Protection Working Party has made use of the term "*reinforced responsibility*" in order to describe the meaning of accountability (European DG of Justice, 2010), implying both "responsibility" and "action" with respect to the specific responsibility. Both in the Opinion on the Future of Privacy (European DG of Justice, 2009) and in the Opinion on Accountability (European DG of Justice, 2010), the Article 29 Working Party examines primarily the "conformity in practice" of the processing conducted by data controllers with the applicable rules laid in the Directive. In this way, accountability seems to link the responsible actors with the implementation of certain measures.

Information Technology (IT) Management

Business process and project management best practices such as Information Technology Infrastructure Library (ITIL) and Project Management Body of Knowledge (PMBOK) include a responsibility attribution method called the RACI model which specifies a mapping of roles and activities within a project, process, service management activity to who is Responsible, Accountable, Consulted and Informed.

Governance and compliance frameworks such as ISO/IEC 27001/02 contain many of the elements of accountability defined above: the information security management system of an organisation is meant to generate assurance, transparency and responsibility in support of control and trust. For instance controls within 27002 require attribution and separation of responsibility (e.g. ISO 27001 Section A.8.1.1 states that "Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organisation's information security policy."). Moreover, the increasing use of contractual arrangements and frameworks for monitoring the fulfilment of commitments made in those contracts affects liability (as breach of contract entitles the other party to some remedy at law. These remedies include payment of damages to compensate for the breach, termination of the contract, the ability to seek court orders requiring compliance, and a range of internal remedies such as reduction in charges, processes for negotiating consensual remediation without seeking court action, and so on).
A related concept (often used in assurance frameworks such as ISO 27K) is authentication, authorisation, and accounting (AAA). This is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security. The accounting component is strongly related to the notion of accountability since it includes the notions of transparency and providing account.
Accountability can be provided within an organisation by means of the organisation identifying risks and harms, having appropriate policies that mitigate risks, mechanisms for enforcement internally and for monitoring that these are effective within the enterprise, and for internal and external validation of this. In addition, provision of transparency and redress to customers and end users is also very important.

There is few literature describing real experiences around accountability in IT management. One early experiment is Parris (1996), where the author presents the use of an accountability model in a software management process. The experience was conducted during five years in the Modular Mission Computer team at Lockheed Martin Tactical Aircraft Systems. "The model views accountability as a proactive coprocess, not as a vague concept of obligation, nor as a reporting relationship on an organisation chart." "It lives behind the scenes as an aid to the design and troubleshooting of

management systems." The author claims that a management process based on a rationale handling of accountings and consequences enforces the team behaviour and is a key to empower itself. An accountability model is sketched based on accounting and consequences. Accounting is a report about end results, planning, performance for plan and their justifications, while consequences describe feedbacks from stakeholders in term of information, rewards or penalties. This model enables the following conceptual elements: attributability, transparency, responsibility, liability, and remediability.

Social Science

Social science, simply said, is the science of society. “Social science historically developed alongside the new industrial order, which was based on novel technologies of steam-based power, the railways, and the factory system” (Macnaghten, 2005). Social science’s aim is to provide intelligent and reflexive analysis of the implications of new emerging technologies such as nanotechnology or cloud computing. However, there are different ways of ‘doing’ social science.

Social science exists of multiple academic disciplines. These disciplines vary from economics, political science to sociology and its different sub-disciplines. The issues surrounding accountability have been generating a growing literature within a number of these social science disciplines (e.g., political science, public administration, management, accounting, education, social psychology) for at least two decades.

Moreover within these multiple academic disciplines different approaches to accountability have been taken, allowing for the different frames to be employed, different measuring techniques and varying conditions that lead to accountability either on macro-, meso- or micro-level. For example, whom to involve and for what purpose seems to differentiate within the social sciences. Below we will provide a review of accountability in social science, that is, how the different social science communities interpret accountability and what measuring techniques they use and conditions for accountability they define. We do not intend to provide a complete overview of all social science disciplines and their views on accountability as this simply is not feasible, yet the disciplines of economics, political science, psychology and sociology provide a good overview of the different approaches to accountability within the social sciences.

Economics seeks to analyse and describe the production, distribution, and consumption of wealth. Accountability, within economics, is about transactional relationships between stakeholders (e.g. within the A4Cloud project between cloud providers and cloud users). These relationships are conceptualised as ‘account giving’, ‘excuse-making’, and ‘image managing’. Within economics modelling is one of the most prominent measuring techniques.

The political science deals with the description and analysis of political systems and political behaviour. The ideas of Foucault with regard to surveillance and control of work has a tremendous influence on thinking about accountability, in the sense of understanding accountability as a form of governance with a moral pull for responsiveness and a moral push of amenability.

(Social) psychology focuses on the mental and behavioural processes of individuals. The work of Michel Foucault is influential in gaining understanding of accounting and the control of work. “A Foucaultian analysis of accountability would focus attention on three dimensions: knowledge (how individuals understand the world in which they are operating), power (the techniques and technologies of control used in that domain), and ethos (the ways through which we adapt ourselves to the expectations generated by the knowledge/power arrangements)” (Dubnick and Justice, 2004). With regard to accountability the mechanisms of oversight provide insight in the accountable behaviour of individuals, or in the A4cloud project about being a good cloud provider. It is the responses of the cloud providers to surveillance that steers them towards this good behaviour. In (social) psychology accountability will be conceptualised as a role identity making uses of measuring techniques as experimental and field observations of individual subjects.

Sociology entails the systematic study of society and human social action. Within sociology accountability often is framed within the boundaries of public or social accountability. Accountability then is conceptualised as the rules, norms and grammars of society. Public or social accountability can be gained through accessibility, dialogue and relevance. In other words, being responsive to (one’s chosen)

publics' viewpoint and debates, being familiar with its key influences and styles, and aware of its ideas and frames of reference are conditions for demonstrating accountability. Other conditions are the timely involvement of stakeholders and the elicitation of (civil) stakeholders impacted by cloud computing's concerns and needs. The parameters for social accountability are largely determined by existing contextual and cultural conditions. To a large extent, social accountability action must respond to and operate within the larger context and framework of a sector, nation, or region. In the case of A4Cloud, transnational boundaries are in place. Lastly, transparency is a condition for accountability as transparency entails that the decisions and the reasons behind the decisions are communicated to the people affected by the decisions, so as to facilitate clear understanding of the process (Kapiriri 2009). Measuring techniques in place are for example indices constructed from multiple surveys and polls.

The social studies of science can be regarded as a subfield of sociology with more emphasises on the mutual shaping of technology and society. In the past social science "…framed technology as "black-boxed" and well defined, with an independent asocial logic that results in "impacts" or "effects" (Macnaghten, 2005). This places social science at the end of innovation processes. However, since the 1980s "various approaches in science-and-technology studies have shown how technologies cannot be black-boxed and separated from sets of constitutive social relations (see Law and Hassard 1999; Pinch and Bijker 1984; Wynne 1988)" (MacNaghten, 2005). Therefore, new emerging technologies such as cloud computing are in need of responsible governance. Responsible governance makes use of the notion of democratic accountability. This type of accountability goes beyond calling companies to account, and emphasises the need for the public to be involved in accounting mechanisms. Democratic accountability, according to Jasanoff, (Jasanoff, 2009) is needed since increasingly complex questions of responsible governance no longer can built on traditional accountability structures ("command and control" and inherent authority of science). Instead, the principles and practices of accountability by which democratic societies seek to ensure that the knowledge they pay for will serve desirable public ends need to be revisited. Therefore, to learn what governing mechanisms might contribute to gaining grip on the distribution and regulation of accountability in cloud computing, it is important to distinguish the underlying different types of problems, risks and concerns that ideally these governing mechanisms will address.

Computer Science

Our interest is in bridging the gap between the high-level definitions and views of accountability that are found in legal, regulatory, and management texts, and those found in the computer science literature, in which there is to be found a stronger link to security controls and means of automating such aspects as assignment of blame, enforcement of policies and more. We first look at some historical references and we review the main survey and analyses of accountability in computer science. This survey is completed with few practical approaches, a comparison with digital forensics and concluded with a summary.

The notion of accountability cuts across many domains of computer science, such as: digital forensics, computer security, distributed systems in general (including grid and cloud computing, the Internet and network applications) and natural language processing. Except for a few references, esp. (Weitzner et al., 2008; Le Métayer, 2011; Pearson and Wainwright 2012), in computer science, there is not a general and interdisciplinary view of accountability. Most of the papers, due to the complexity of the concept, only address some properties or specific mechanisms related to accountability. One thing does become obvious though – namely the view that the preventive controls used extensively in classical IT security are not sufficient to achieve accountability. Full accountability requires mechanisms for information transparency, checking misbehaviour and responsibilities and then proceeding to punishment. There are already some proposals for frameworks integrating these aspects (Pearson and Wainwright, 2012; Butin et al., 2013) and formal models or logics for accountability (Cederquist et al., 2005; Jagadeesan et al., 2009; Küsters et al., 2010; Feigenbaum et al., 2011).

The first reference about accountability in computer science seems Nissenbaum (1994). Accountability is mainly undetermined in computerised systems, and this is rather different from practices in other engineering domains. After presenting some generalities about responsibility, liability and accountability she discusses four barriers regarding accountability in computerised systems. The barriers are explained in details: the problem of many hands, bugs, the computer as Scapegoat, and ownership

without liability. The author argues that those who are responsible for harms and risks are also the most suitable to drive them. She emphasises responsibility and liability and she notes that ownership responsibility is often absent in the debates around software. A general trend is that licence agreements often include a detailed section about the producer's right but nothing or few about its accountability or its liability. She proposes four recommendations to maintain accountability in computer systems.

Later, the paper from Szolovits (1996) is a reply to this first paper, mainly the author considers that Nissenbaum missed the most significant source of errors. These errors are due to the large-scale, complexity and openness of the software systems. The author claims that new programming languages, component-based architectures and formal verifications are good ways to improve the quality of software applications. This paper was representative of the resistance from the computer community face to accountability. The above desirable features have been prove their suitability but they cannot solve the problems raised by the loss of accountability. More recent papers on accountability in computer systems recognise the complexity of modern software systems and the failure of the strict preventive approach. To the contrary they consider that accountability is a strong requirement to improve modern software trustworthiness.

In Burmester et al. (2006) the author explains that while privacy and accountability seem to be in contradiction, they could be balanced to offer more trustworthy systems. The paper proposes a first pragmatic view where accountability is accomplished with a combination of authentication, action binding, monitoring and trust infrastructure. The document discussed several examples focusing on the potential conflicts between privacy and accountability, and argues for good models of accountability. But a holistic definition for accountability was not achieved at this time. The author mainly reduces accountability to attributability.

Weitzner et al. (2008) consider that the usual "hide-it-or-lose-it" perspective on information is dominating but not adequate in a world where information should be communicated. They argue that a shift is needed from hiding information to ensuring only appropriate uses occur.

Lin (2010) claims that the key elements of accountability are: disclosure, liability and non-repudiation, and that the notion also includes collective responsibility and policy. Le Métayer (2011) discusses the interplay between legal and technical means to risks for citizens and consumers. Laws and contracts provide assurances and technology can help enforce legal commitments. Pearson and Wainwright (2012) take a global and interdisciplinary approach, which encompasses legal, regulatory and technical aspects. The principle is to provide a rich toolset rather than define a general, catch-all solution for all aspects of accountability. A distinction is made between *preventive*, *detective* and *corrective* mechanisms which can help in understanding, organising and implementing accountability. Xiao (2012) is a comprehensive survey of research related to accountability in the computer science domain. The author does not give a precise definition for accountability but relates it to a number of uses in various areas of computer science. End-to-end accountability is generally not accomplished; these systems have four key characteristics: identities of events, a secure record of events, auditing and evidence.

Recently Butin, Chicote and Le Métayer advocate for strong accountability in Butin et al. (2014). They propose a critical review of the concept and analyse a significant part of the existing literature from different point of views (regulations, laws and computer science). They put forward strong accountability as a set of precise legal obligations supported by an effective software tool set. They demonstrate that the state of the art in term of technology is sufficient to implement a notion of accountability by design.

Surveys and Analyses

A first interesting point of view about accountability is from Lampson in (Lampson 2004). The author reviews the requirements for security, recalls the basic principles and reasons about whether or not to focus on security in software development. He proposes to mirror classic terms in software engineering with those in security. Thus it is possible to see a policy as a specification (abstract, formal, etc.), a mechanism or a concrete policy as an implementation of the policy and finally the notion of assurance is related to the correctness of the mechanism. From the author’s point of view in that paper, security policies essentially aim to fulfil three objectives: usage control, availability and accountability. Mechanisms for usage control and accountability can be broadly classified into three categories:

authentication, authorisation and audit. Authentication and authorisation mechanisms allow usage to be controlled while audit mechanisms lead to accountability. In a distributed context, where applications span security boundaries, authorisation and audit mechanisms are related: an end-to-end authorisation cannot be granted without auditing capacities (Howell and Kotz, 2000). Indeed, delegation is needed in order to generate a chain of trust between two endpoints. An audit applied to this chain supposes means for investigating and reasoning about past events, saved in a log file for instance. From this work it is clear that formal logic is essential to define chains of trust and auditing. This conclusion may also be derived from (Abadi, 2003). Even if the focus is on authentication, the delegation mechanism (the *says* operator) is a cornerstone in this paper.

The authors (Weitzner et al., 2008) consider that the usual "hide-it-or-lose-it" perspective on information is dominating but not adequate in a world where information should be communicated. They argue that privacy means and access control over personal data are insufficient to guarantee the protection of privacy since the same information can be duplicated on the web or it is possible to infer some accurate details from other public information. The paper explains why privacy means, digital rights management and other techniques fail in assuring a transparent and responsible use of personal information. "*Individuals should not have to agree in advance to complex policies with unpredictable outcomes. Moreover, they should be confident that there will be redress if they are harmed by the improper use of the information they provide.*" They argue that we should move to accountability where the circulation and usage of information is transparent and then misuse and responsibilities can be defined. They assert that a technical architecture supporting accountability should support three features: policy-aware transaction logs, a policy-language framework and policy-reasoning tools. Their definition of accountability is mainly focused on transparency and attributability,
while the proposed framework suggests also verifiability.

Schneider (2009) discusses why perfection in preventing defects and attacks is so difficult to achieve in computer science. The main reason is that computing systems are very complex and often they are not provided with a precise specification of what they are doing, assumptions of the environment and an analysis of threats. Holding software producers accountable for their software systems needs an important effort in forensics for computing systems. The author argues that ensuring the responsibility in case of misbehaviour is simpler than preventing misbehaviour in a perfect manner. But this should increase the effort in auditing mechanisms. This will have also some strong consequences in society, in laws and in the cooperation between foreign countries.

The goal of Lin (2010) is to provide an understanding of accountability in service-oriented computing. The paper reviews the state of the art in this domain and proposes an accountability framework. This framework provides a dynamic and efficient e-service accountability infrastructure for monitoring, analysis, and reconfiguration of service processes. The paper discusses some general acceptations of accountability in quality management process, management literature, and regulatory compliance. In particular the paper emphasises definitions from Schedler and from Kopell. From Schedler : disclosure and liability, are the most essential attributes for accountability in any context. Koppel adds three managerial concerns namely, controllability, responsibility and responsiveness. However, the authors consider them not be essential for all domains. The author also consider the accountability definitions from information technology. "*Accountability is a term loosely used in the IT literature, referring to a variety of desired attributes in various aspects of IT*." They identify three levels: technical protocol, architectural and organisational. The first of these provides technical means to ensure some attributes of accountability. The architectural level promotes automation of accountability tasks in business processes. The last level considers overall accountability in a system and its governance.
The view is still partial both regarding technical and global aspects, as it is a business-oriented view of accountability. They claim that the key elements of accountability are: disclosure, liability and non-repudiation, and that the notion also includes collective responsibility and policy consideration. The last occurring as a more technical concern than a conceptual attribute. The term transparency in also used in the framework described but the connection with disclosure is not clearly stated. The work also discusses accountability in IT and its relations with other concerns of the domain such as security, trust and QoS. The authors observe that security, privacy and Quality of Service (QoS) are required for accountability but alone cannot achieve full accountability while trust and reputation are indirect measurements for accountability.

Le Métayer (2011) discusses the interplay between legal and technical means to risks for citizens and consumers. Laws and contracts provide assurances which are out of the technical means and technology can help enforcing legal commitments. The general goal of the research is to contribute, in partnership with lawyers, to the development of new methods for a better integration of technical and legal means. This work covers much more than accountability, since digital rights management, protection of privacy rights, cybercrime, Internet regulation and so on, are overviewed. The author argues that the use of formal (in the sense of fundamental and practical) methods can help to reduce the gap between legal and technical means. Regarding accountability, he considers that the focus is on responsibility and verifiability, and on the technical side, the concept involves transparency and security. The author considers that more research is needed to clarify the technical definition of accountability and associated requirements and to provide practical and trustworthy implementation methods and associated tools. He asserts that an interdisciplinary collaboration between lawyers and computer scientists is required and he gives some preliminary features of a precise methodology to follow.

In (Pearson & Wainwright 2012) a review of the notion of accountability is carried out and a global and interdisciplinary approach is promoted taking into account legal, regulatory and technical aspects. The proposed approach is to define an accountability framework which interoperates with existing mechanisms such as SLA management, incident management and audit. The focus is made on complementary mechanisms for accountability: risk management, data obfuscation, consent management, sticky policy and information monitoring. The principle is rather to provide a rich toolset than to define a general and unified solution for all aspects of accountability. "*There are a number of existent mechanisms to help technologically, but none of these provide a comprehensive or interdisciplinary framework and approach.*" A distinguished point is the distinction between preventive, detective and corrective mechanisms which can help in understanding, organising and implementing accountability.

(Xiao, 2012) is a comprehensive survey of research related to accountability in the computer science domain. The author does not give a precise definition for accountability but relates it to a number of uses in various areas of computer science. The considered attributes and characteristics are oriented to technical means without reference to legal or business aspects. A first table gives seven domains where accountability was considered and technical solutions have been proposed. Several of these domains are overlapping A4Cloud; at least: the Internet and network, distributed systems and cloud applications. Two notable properties, which were defined in previous related work, are fairness and completeness. Fairness means that no honest principal will be blamed while completeness implies that a misbehaving principal will be blamed. Numerous Internet techniques to provide properties linked to accountability have been explored and are reviewed in this survey. The main techniques are based on message authentication code, specific architecture, monitoring of systems, specific network, firewalls, packet authentication, or logging mechanisms. However end-to-end accountability is generally not accomplished. Digital signatures are essential but alone they cannot provide full accountability. Distributed systems are faced with a large number of threats and accountability is a main concern. Managing faults is a strong requirement implemented either by masking, fault tolerance or detection and removal. There is a specific section on cloud computing: the loss of control is critical
There are various kinds of problems from classic bugs, to attacks, loss of data, deny of services and lack of resources. The authors adopt an operational view and consider the following features for an accountable cloud system: identity of event originator, secure record of events, auditing, and production of evidences. They conclude with “The fundamental concept of accountability is to let every entity (internal or external) be held responsible for its behaviour with undeniable evidence.” Finally, the authors note that while accountability is studied in the previous domains, in other areas like wireless sensor networks, cellular systems or operating systems, consideration of this notion is still in its infancy.

Recently Butin et al. advocate for strong accountability in Butin et al. (2014). They propose a critical review of the concept and analyse a significant part of the existing literature from different point of views (regulations, laws and computer science). The authors consider that the view from normative text put too much emphasis on accountability of policy and procedure while computer scientists have a too narrow approach of accountability by practice. They put forward strong accountability as a set of precise legal obligations supported by an effective software tool set. They demonstrate that the state of the art in term of technology is sufficient to ensure the notion of accountability by design. The authors while they promote a precise and operational approach think that a multidisciplinary view of accountability is

fundamental. The authors detail pro and cons regarding the use of accountability in software applications dealing with private data. Accountability should be viewed as the needed requirement in case of the loss of controls resulting to vulnerabilities of systems. The authors also analyse three objections against accountability and explain that accountability must meet an absolute requirement of precision to effectively play its role. They analyse the case of the Prime Life Policy language as a support for accountability and illustrate the critical design of the logging system. Except the reference of the Colin Benett's taxonomy there is no explicit and general attributes for accountability.

Formal Logics and Models

The authors of (Crispo & Ruffo 2001) propose a framework to analyse how accountability is transferred among principals. They consider the following definition for accountability: "*The property whereby the association of a principal with an object, an action or a right can be proved to a third party*". They are interested in protocols with delegation of accountability: that is, a principal can exercise some rights resulting from the delegation of another principal. They want to differentiate delegate and delegator: the delegate must be accountable for its misbehaviour while the delegator is accountable only for its proper actions. The paper provides a formal logic framework for accountability with principals, messages and statements about rights, authentication and signatures. Then the authors use the framework to analyse two accountability protocols to see their differences regarding the delegation of accountability. The authors do not try to characterise general accountability. But starting from a precise notion of verifiability (provability) they show how to reason on tracing accountability in case of delegation, that is achieving a form of transparency.

In some situations, classic access controls or digital rights management fail and enforcing policy is often impossible. Agents may misbehave but at the risk of being blamed by an external auditor. Thus the authors of (Cederquist et al. 2005) consider a decentralised system in which data and usage policies can be delegated to other principals. The focus of the paper is on auditing: how to prove the obligations of an agent by an auditor. This work proposes a policy language with conditions, obligations and refinement of policies. A reasoning system is provided allowing checking of the formal behaviour of an agent by the auditor. A precise notion of agent accountability is provided: an honest agent should log its actions if it is authorised to process them. The notion of delegation of accountability is slightly different from (Crispo & Ruffo 2001). This work does not make explicit general attributes but it is linked to verifiability and attributability.

Le Métayer (2009) presents a formal framework to enhance privacy protection by linking legal privacy requirements and technical ones. The first idea is to consider that each physical person has a software agent which represents him. Software agents act as representative or proxy for the real agents. There are subject agents which own data and controller agents which use these data. The framework defines a simple privacy language similar to legal requirements for privacy protection. Software agents are formally described with an abstract model and communication events, for instance to request or to allow disclosure of some data. When a data is disclosed a sticky policy is attached to the data and describes the constraints on the use of these data. A trace semantics is then proposed and allows the precisely statement of a notion of compliance. A first desirable property is that a data in the space of the controller should have a sticky policy and that this policy was permitted by its subject owner. A second property is that data should be forwarded to controllers only if the subject has allowed it. Thanks to the formal framework, a notion of global correctness can be achieved and can be proved.

In (Jagadeesan et al., 2009) the authors state that the accountability approach to security lacks general foundations for models and programming. From that they propose a theoretical model for accountability in a distributed system with definitions of honest agent, auditor, and responsiveness. This allows them to discuss the power of the auditor and the constraints placed on agents and on the communication infrastructure. The model is based on point to point communications providing integrity and authenticity guarantees. The behaviour of agents is expressed *via* process algebra and discrete time. They use a game-based method and model-checking to check related accountability properties. For example, they are able to consider properties like: "*Every agent guilty of a dishonest action is blamed by the auditor*", "*At least one of the agents blamed by the auditor is guilty*", or "*The auditor is always successful in blaming a non-empty subset of agents*". It is not a general discussion on accountability but it provides a formal framework for it thus crosscutting verifiability, attributability and a limited form of remediability.

In (Küsters, 2010), new definitions for accountability and verifiability are proposed and shown to be connected together. The author demonstrates the applicability of this approach by analysing several cryptographic protocols. He provides two accountability interpretations: a symbolic one in the Dolev-Yao style and a computational one with a cryptographic model. The abstract symbolic definition "*reads as follows:*
(i) (fairness) Judge (almost) never blames protocol participants who are honest, i.e., run their honest program.
(ii) (completeness, goal-centred) If, in a run, some desired goal of the protocol is not met - due to the misbehaviour of one or more protocol participants - then Judge blames those participants who misbehaved, or at least some of them".
The subtle point is the completeness condition which should be carefully defined. It should take into account that "*misbehaviour that cannot be observed by any honest party may still be very relevant and harmful*". This definition left open the question "*who should be blamed*" since in some protocols individual accountability is impossible to achieved. It strongly links accountability and verifiability in a computer science view for protocols. As with (Jagadeesan et al., 2009) our acceptation of accountability here is related to verifiability, attributability and remediability.

Feigenbaum et al. (2011) claim to provide a more general and more widely applicable definition of accountability. They explain that existing approaches have been mainly preventive which is inadequate: it is generally impossible to*, a priori*, differentiate an honest user from a pirate. They argue that an *a posteriori* or corrective approach is more suitable to accountability. They provide a formal model of accountability based on event traces and utility functions taking into account anonymous agents, automatic and mediated enforcement of accountability. Their definition of accountability is: "*An entity is accountable with respect to some policy (or accountable for obeying the policy) if, whenever the entity violates the policy, then with some non-zero probability it is, or could be, punished*". The definition strongly relies on the notion of punishment which is extensively discussed in the paper. Several variations are formally presented (automatic/mediated, probabilistic/typical). We note that they want to de-correlate identity and punishment, as punishment can arise without explicitly identifying the violator. Indeed, this work is an original piece of work which proposes interesting ideas about formal definitions of punishment and accountability. As other formal computer model for accountability is only tar getting some of our attributes. However, it is the first to focus on punishment (attributability, remediability) to note that numerous notions are related including compensation and answerability.

Practical and Specific Approaches

This section describes some related work dedicated to prior consideration of accountability for protocols, distributed systems or the cloud. They are often technical or specific solutions which do not consider accountability with a wide and multidiscplinary acceptation.

Baldwin (2004) considers an interactive evidence store as a way to promote transparency and thus to increase accountability between parties. A Section is devoted to the description of accountability and its connections with authentication, evidence, transparency, judgment and detection. This definition is expressed as: "*Accountability is the concerned with an entity taking responsibility for its actions in performing a particular task or against a particular plan*." This work focuses on transparency and evidence of actions as an obvious aid for accountability. The author argues for an interactive evidence store and describes the characteristics of the event information to be stored. The main part of the work is to describe the architecture for such a framework and to justify the integrity and confidentiality of the information.

Bella and Paulson (2006) compare a non-repudiation protocol and a certified email protocol. They establish a general technique to model and verify accountability protocols inductively. The formalisation is based on the Isabelle theorem prover and the above properties:
"*Correctness of accountability protocols involves two concepts:*
1. Validity of evidence: an agent is given evidence sufficient to convince a third party of his peer's participation in the protocol
2. Fairness: both agents obtain the promised items, or neither do".

The authors prove both protocols to be correct: they are fair and deliver valid evidence. Mainly this work covers aspects of verifiability and transparency for specific protocols.

MapReduce is a parallel data processing model and in order to provide service integrity, Wei (2009) proposes the SecureMR approach. Using the MapReduce model in an open environment leads to the question of service integrity. SecureMR solves this problem using a scalable and decentralised replication-based integrity verification scheme. SecureMR was experimented with and evaluated in the open source Hadoop implementation of MapReduce. This work does not use the term “accountability” but “service integrity” and addresses verifiability and transparency issues.

The Accountable Virtual Machine (AVM) proposed in (Haeberlen et al., 2010) provides the capability to audit the execution of a system in a distributed context. AVM is able to detect errors and to identify faulty nodes, providing verifiable evidence of the fault. The technique wraps the client software in a virtual machine which records the execution into tamper-evident logs. The logs contain enough information to reproduce the complete execution of the embedded binary image and it links output messages with cryptographic information to the log action responsible for the message. This work covers observability, verifiability, transparency and attributability.

Wang and Zhou (2010) describe a mechanism to support accountability for a multitenant database with a centralised external service. The authors propose an accountability service, namely, a third party service which allows clients to verify the correctness of the data and the execution of their business logic in the cloud platform. The third-party service is responsible for intercepting endpoints interfacing the client and the service. It captures data relevant to the SLA contract and uses the Merkle B-tree method to authenticate the data stored in the database. The initial proposed service is centralised but the paper also considers a distributed version. This approach was experimented and evaluated with the Amazon EC2 cloud service. This work covers observability, verifiability, and transparency.

The purpose of (Sekar and Maniatis, 2011) is to allow cloud customers to verify that their applications physically consume the resources that they were charged for and that this consumption conforms to the agreed policy. This is contract verification, but it is complicated due to the black-box nature and the high dynamicity of the cloud context. This position paper considers a simple abstract model with a client, a provider and a verifier. The authors raised two questions: *“Did I consume what I was charged? Should I have consumed what I was charged?*” Then, the paper discusses challenges and possible solutions for verifiable resource accountability. It is specific in resource consumption but intersects verifiability and transparency attributes.

Sundareswaran (2012) proposes an end-to-end decentralised accountability framework (called *Cloud Information Accountability* or CIA) to keep track of the user data usage in the cloud. They suggest an object-centered approach that packs the logging mechanism together with users' data and policies. Thus a data owner can track whether or not the service-level agreements are satisfied, but also can enforce access or usage control. They consider two possible modes for auditing: push mode (where owners receive logs) and pull mode (where auditors extract logs). The CIA framework was tested and the experiments show efficiency, scalability and granularity of the approach. There is not an explicit accountability definition; the paper focuses on data accountability and a technical framework to achieve it. The author considers it is essential to provide such an effective mechanism in the cloud. There is not an explicit relation with legal or socio-economic requirements in this work and the focus is on the observability, verifiability and transparency attributes.

Accountability and Forensics

With respect to the notion of evidence, it is important to differentiate between accountability and forensics. Digital forensics looks for unintended evidence, i.e. evidence that some party was not planning to leave and which collection was not planned ahead (at least for the purpose of forensics) (Kessler 2012). Accountability, as defined by the authors mentioned in earlier Sections, is a planned process. Evidence collection is defined upfront and based on a carefully designed framework and metrics. This way the evidence is available at any time instant of the service delivery process. This allows for a much wider spectrum of actions (e.g. prevention) and shorter reaction time. The evidence can be used to support that policies were complied with, or to show that they were not complied with.

Accountability does not replace or directly contain digital forensics; however there might be an important body of knowledge available in the forensics field particularly to help in the definition of accountability metrics, and indeed to enhance evidence in the case of detection of non-compliance with policies in serious or contested cases.

Summary

In this appendix we have reviewed existing definitions of accountability from the literature and discussed related concepts and their interrelationships; the way that accountability has been interpreted in regulatory frameworks has been reviewed in some depth, and various interpretations of the concept from different disciplines, from law to computer science, have been presented. Thus we have seen some related perspectives, such as Weitzner's view of information accountability, and formal models of accountability that can be used in IT systems.

Taking this analysis into account, as discussed in Section 2 we think of accountability as encompassing the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information beyond mere legal requirements, to adequately anticipate risks and harm potentially created and to provide transparency, assurance and remediation. However, accountability does not apply to just personal information but also to other forms of information that may need protection, and so within A4Cloud we consider a broader scope of usage that also encompasses that protection. For a good overview of the context and meaning of accountability that is very relevant for the way in which we are considering it within A4Cloud, see (CIPL, 2009; Raab, 2012; Alhadeff et al, 2012). For background on privacy and related definitions, see (Pearson, 2012) and related terms in the Glossary of Terms and Definitions.

C. Cloud Computing

The NIST definition of cloud computing (Mell, Grance, 2011) identifies, as shown in Figure 36, the essential characteristics (i.e. on-demand self-service, broad network access, resource pooling, rapid elasticity and measured services), the service models and deployment models (i.e. private, community, public and hybrid clouds). . Furthermore, NIST also provides a well-accepted definition of cloud computing as *a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*. The combination of such cloud computing features enables different business models, and hence different cloud ecosystems involving various stakeholders (e.g. cloud customers and cloud service providers).

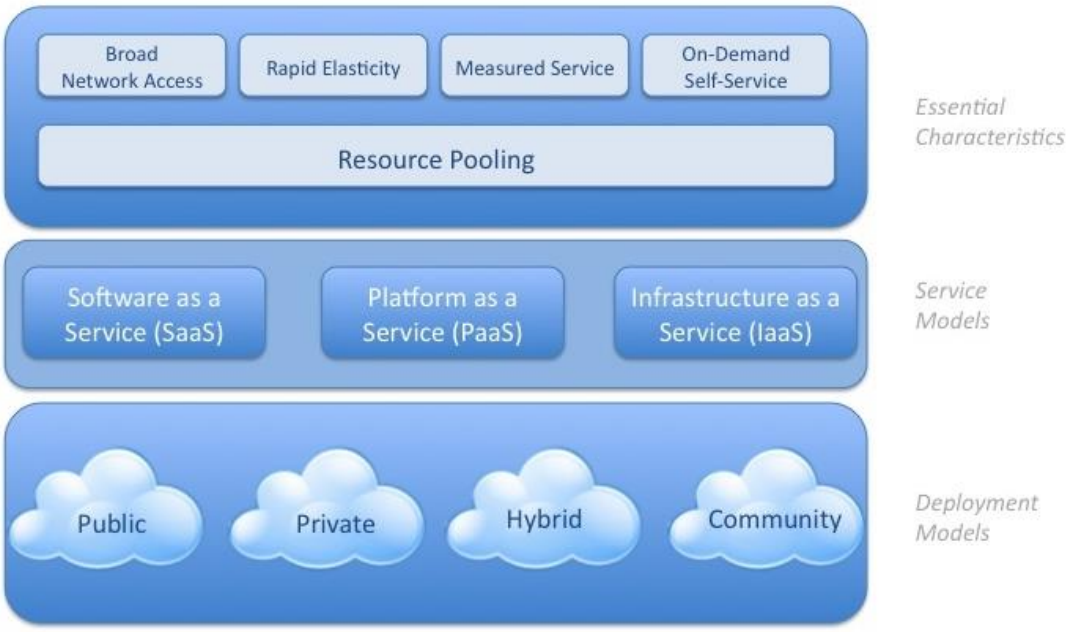


Figure 36 NIST Visual Model of Cloud Computing (CSA, 2011)

The service models defined by NIST are as follows:

1. *Software as a Service (SaaS):* consumers use CSPs' applications running on a cloud infrastructure
2. *Platform as a Service (PaaS):* consumers deploy (onto a cloud infrastructure run by a CSP) applications that have been created using programming languages and tools supported by that provider
3. *Infrastructure as a Service (IaaS)*: consumers deploy and run software, with a CSP controlling the underlying cloud infrastructure.

Private cloud is operated solely for an organisation, whereas public cloud is owned and managed by a third party. Community cloud is consumed only by a particular group of trusted users, and hybrid cloud is a combination of public and private clouds, connected in an interoperable way.

D. Accountability Functions and Mechanisms

Table 8 Accountability Practices, Functions and Mechanisms

Practice	Function	Mechanisms
Define governance	Policy definition (governance)	• Compliance frameworks (to ensure legal obligations are addressed)
Ensure implementation	Policy definition (implementation)	• AccLab • A-PPL language • 3rd party policy definition tools & frameworks
	Data subject preference elicitation and management	• AccLab • Data Track
	Cloud contract management	• COAT • 3rd party cloud specification & analysis tools (+ SLAs, contracts)
	Risk assessment	• DPIAT • 3rd party risk assessment tools & methodologies • Privacy Impact Assessment • Insurance • Certification
	Policy enforcement	• A-PPL Engine • 3rd party policy enforcement frameworks
	Secure logging	• 3rd party secure logging systems
	Evidence collection	• Audit Agent System • Data Transfer Monitor Tool
	Evidence management	• A4cloud framework of evidence
	Incident management	• Breach and incident management response protocols
	Internal monitoring, review, auditing, validation (internal audit and assurance programs to monitor compliance with privacy policies)	• Audit Agent System • Assertion Tool • 3rd party auditing tools and methodologies • Certification frameworks • Reporting (for governance to audit effectiveness of programme) • Testing of procedures & infrastructure
	External (supply-chain) monitoring, review, auditing, validation	• Audit Agent System • 3rd party auditing tools and methodologies • Certification frameworks
	External policy definition and contract requirement specification for supply chain	
	Elicitation and collection of feedback from customers & employees	
	Training, education & awareness	
Explain & Justify actions	Evidence presentation/association	• Data Track • Audit Agent System
	Evidence provision	•
	(external) Auditing	• Audit Agent System
	Information & Awareness	• Data Track • Transparency reports

		• Various public education & communication schemes
Remedy failures	Notification	• Data Track • Other notifications means & systems
	Incident response	• Incident Response Tool • Sanctions • Litigation
	Policy revocation	• A-PPL Engine
	Remediation mechanisms	• Remediation Tool • Other remediation options (litigation, etc.)

Table 9 Preventive, Detective and Corrective Mechanisms

	Preventive	Detective	Corrective
Cloud Subject	• AccLab	• Data Track • Transparency Log • Policy Violation Plug-in • DSART	• RRT • IRT
Cloud Customer	• DPIAT • COAT • AccLab		• RRT • IRT
Cloud Provider **Cloud Broker** **Cloud Carrier**	• A-PPL Engine • AccLab • Assertion Tool	• AAS • DTMT	
Cloud Auditor **Cloud Supervisory Authority**	• Assertion Tool	• AAS • DTMT	

E. Examples of Accountability Chains and Mechanisms

This appendix provides examples of how accountability mechanisms (in particular, the ones developed by A4Cloud) support emerging relationships between cloud actors across cloud supply chains (D:B-3.2 provides also an analysis of the A4Cloud tool in the contexts of the use cases).

Examples of Accountability Chains

The different A4Cloud mechanisms and tools support accountability throughout cloud service provision. In particular, they enable chains of accountability by supporting the interactions among cloud stakeholders. Figure 37 shows an example of chains of accountability supported by different mechanisms and tools. A4Cloud delivers a set of tools, which support stakeholders to address accountability in the cloud in a co-design fashion. The A4Cloud mechanisms, in this case, operate in a preventive, detective and corrective way. Thus, the different tools aim to support stakeholders at all stages of the service engineering chain, from the design of accountability to the monitoring of the evidence that accountability is actually met at runtime and the potential handling of incidents, which can lead to the loss of accountability, due to the dynamic nature of the cloud ecosystems. The tools delivered in A4Cloud span across these three dimensions and aim to control the responsibility for stewarding data in the cloud, as well as ensuring that the obligations derived from the legal and regulatory framework and the stakeholders' governance model as well are maintained.

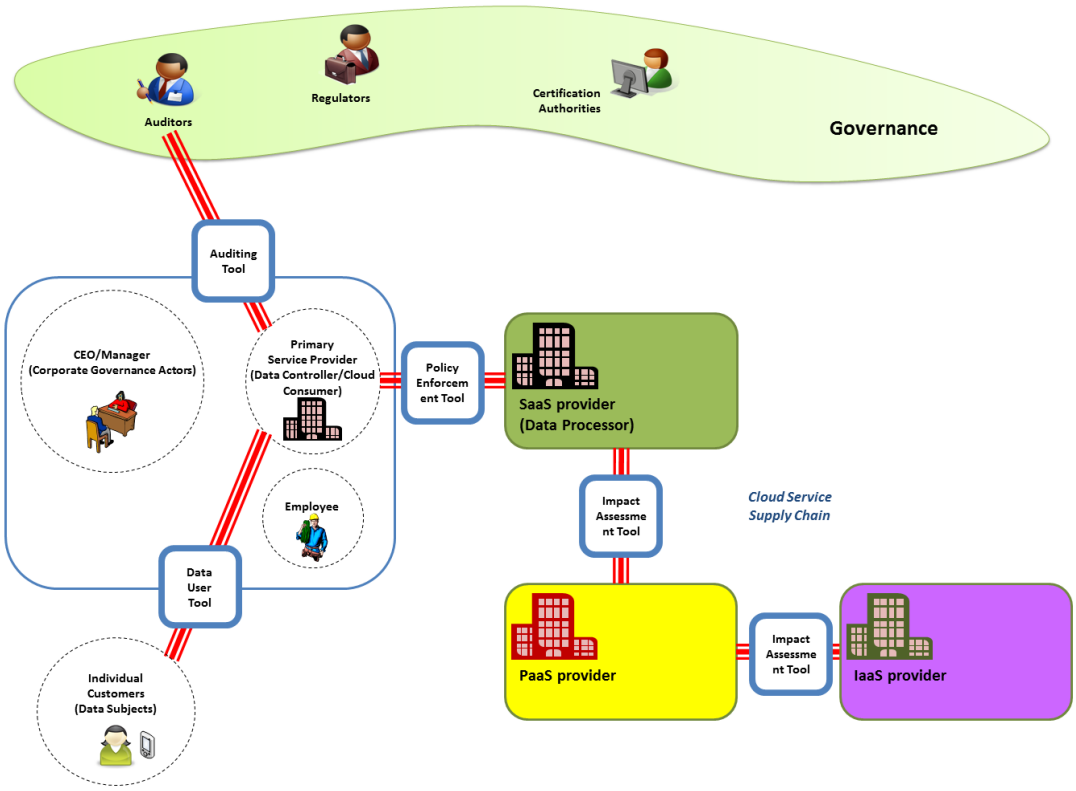


Figure 37 Chains of Accountability Supported by Different Mechanisms and Tools

A4Cloud mechanisms act as an on-demand service for accountability. Different mechanisms refer to different roles in the cloud ecosystem and as such facilitate various interactions in the relationship landscape of a cloud service chain. An example of how A4Cloud mechanisms might work together so that chains of accountability are supported as follows. Based on the recommendations and guidelines on data governance from the Accountability Framework a cloud subject can express their policies (expressed in natural language) for governing the use of their personal data in the cloud, using the Policy Configuration Tool, or an organisational cloud customer might use the Risk Assessment Tool to evaluate the impact of the risks identified with selection of suitable cloud service providers, and to help generate appropriate policies.

The policies are then compiled on the Cloud Service Provider (CSP) side to incorporate the lawyer-readable terms for conformance to the regulatory framework. Through the Policy Enforcement System, the CSP translates the policies to machine-readable forms, so that they can be conveyed to the other involved cloud providers in the service chain. In order for the specific cloud relationships to be effective, certain contracts are established through the Contract Support Tool, which should facilitate the provisions of the policies initiated by the cloud customer. The contracts, as well as the policies, are based on the models for risks, trust, human understanding and economic data governance in cloud ecosystems and they are mapped to the metrics of accountability, which should be monitored in order for compliance to be assessed. This process for the co-design approach of preventive mechanisms towards accountability is reflected in Figure 38.

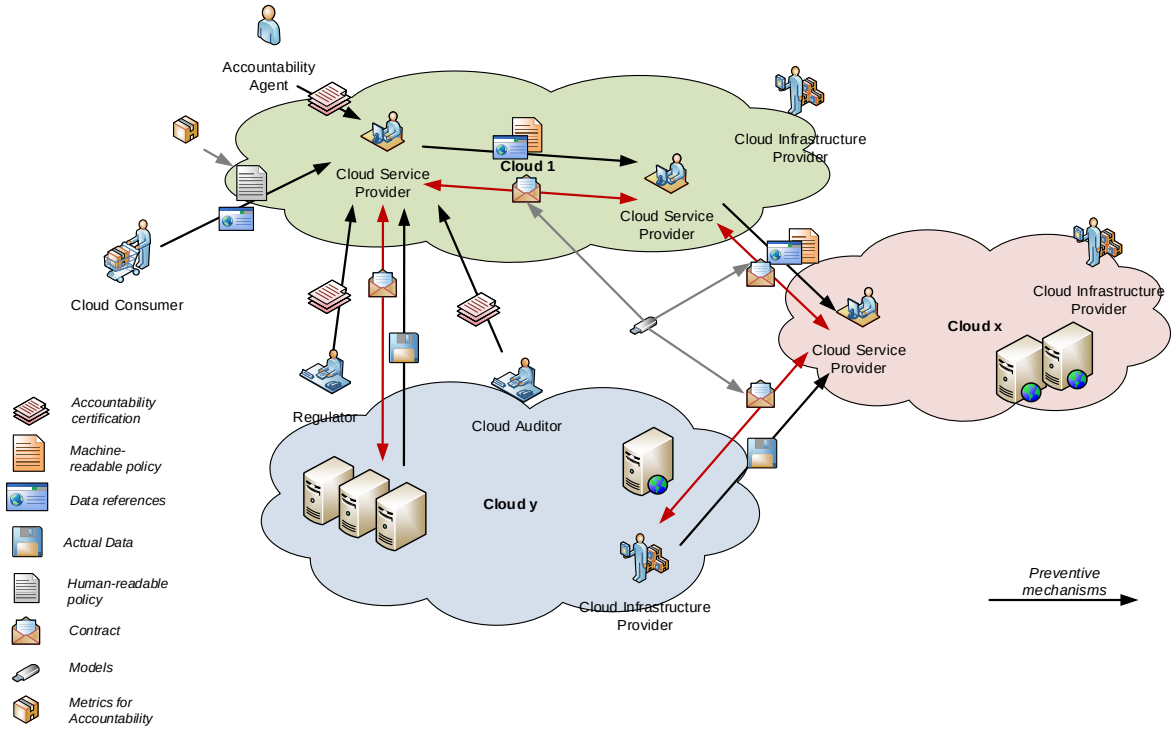


Figure 38 Preventive Mechanisms for Supporting Accountability in Cloud Service Chain

Moving to the actual monitoring of accountability so that detection of accountability violations is enabled, the CSP uses the Evidence Collection System to gather all this information, which is essential on making assertions on the provided accountability. The information collected from the cloud ecosystem is analysed based on the accountability metrics, which should be associated with specific thresholds detailing the provisions of the supported policies and contracts in technical terms. The Accountability Validation Tool assists the CSP to form assertions over the accountability support. The cloud user is always in the information chain by receiving notifications on the way that the defined policies and their data are handled in the cloud. This is reflected in Figure 39.

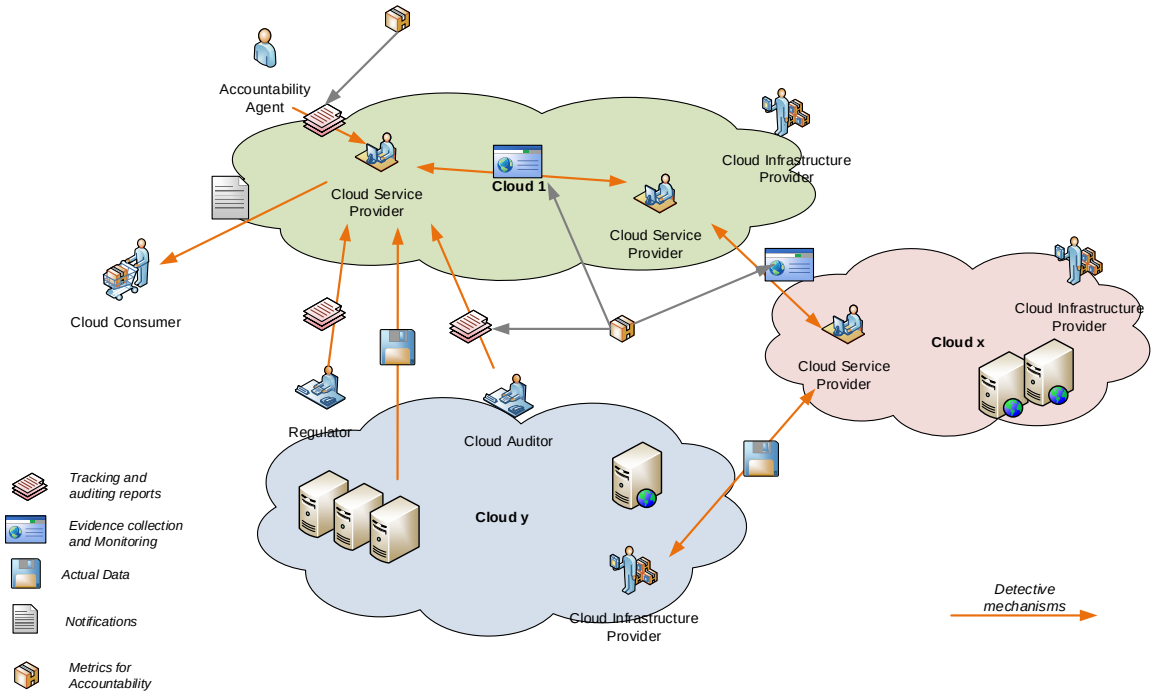


Figure 39 Detective Mechanisms for Supporting Accountability in Cloud Service Chain

Upon the detection of deficiencies in the support of accountability, the A4Cloud corrective mechanisms support the CSP and the cloud customer to perform remediation actions to redress the breach. These actions may refer to policy reconfiguration and contract modifications in accordance to the data governance models and the metrics for accountability. This is reflected in Figure 40.

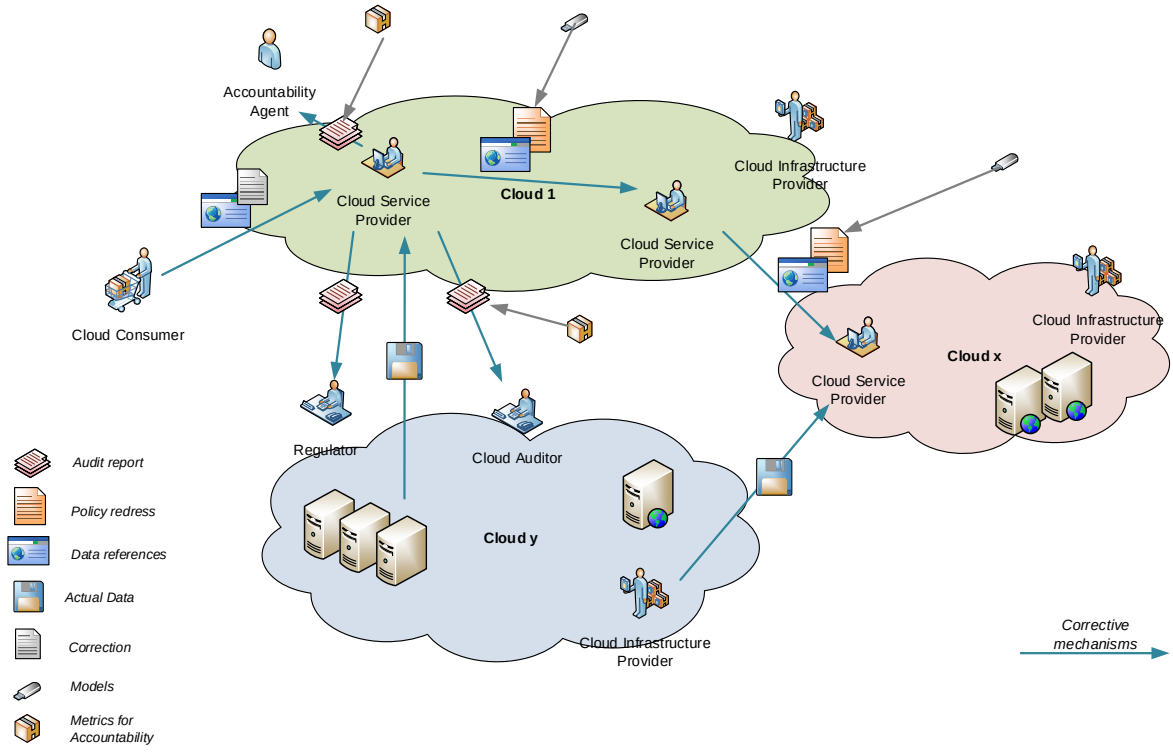


Figure 40 Corrective Mechanisms for Supporting Accountability in Cloud Service Chain

Examples of Mechanisms

One way to realise chains of accountability is shown in Figure 41 by extending the current notion of 'Binding Corporate Rules (BCRs)'. BCRs are a mechanism, adopted by the Article 29 Working Party, by which a corporate group ensures legal compliance and adequate protection for transfers of personal information between EU and non-EU members of the group in compliance with the EU Data Protection Directive.

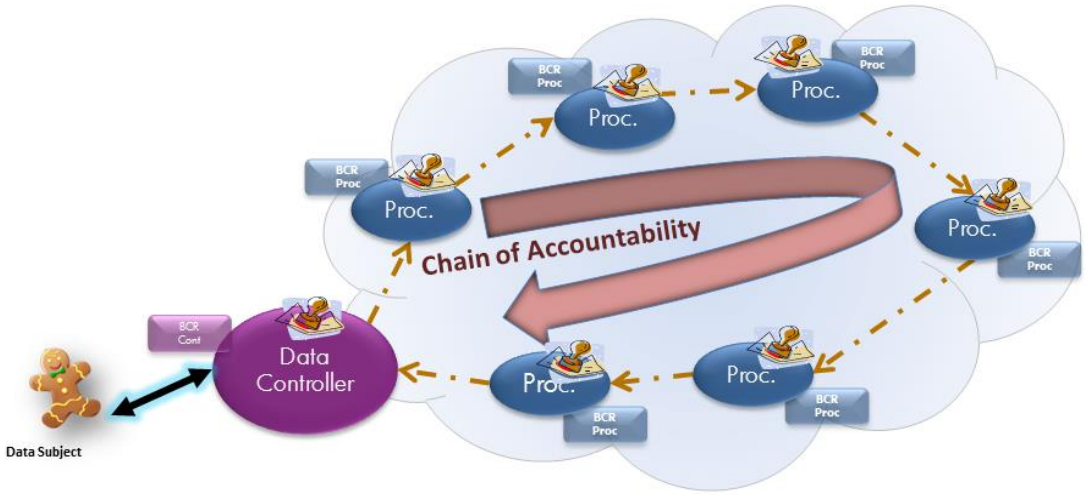


Figure 41 A Vision of Governance Continuity

Specifically, the BCR is a binding internal agreement/contract that obligates all legal entities within a corporate group that will have access to personal information to adhere to all obligations of the DPD, and that provides evidence of supporting measures to ensure compliance. It is used in order to meet the adequacy standards under the DPD for transfers of personal data outside EU and is an alternative to model contracts and US Safe Harbor membership. Without BCR, it is often necessary, due to trans-border data flow restrictions, to use many different model contracts (some setups may require hundreds even), and these are very cumbersome to set up, taking 1-6 months each, and to maintain along the lifecycle of the processing; hence not being well suited to global and dynamic business environments. Binding Corporate Rules (BCRs) apply to data controllers, only to movement within a company group and solely addressing trans-border flows. We extend this to the notion of BCR for processors supported by the EU Article 29 Working Party, extend their scope to a demonstration of overall compliance and not only to trans-border flows and then link these frameworks via appropriate legal agreements in order to allow a chain of accountability, as shown in Figure 41. Penalties can be built into these new BCRs so that it becomes easier to identify who needs to carry out remediation and be penalised in case of non-compliance. We can apply analogous techniques to other jurisdictions and not just EU, e.g. by extending the APEC Cross-Border Privacy Rules concept in a similar way. Such a vision of governance continuity, which will need further work to achieve, can be underpinned by technological mechanisms, for example in order to provide assurance that appropriate mechanisms are being used by the processors. Furthermore, such contractual and regulatory-based approaches could be enhanced by technological means. The co-designed elements could be as follows:

- Natural language policies in a contract associated with lower-level machine-readable policies that define usage constraints of the associated personal data, are transmitted through the cloud associated with the personal data and are acted upon automatically within the cloud without the need for human intervention.
- Privacy protecting controls built into different aspects of the business process, such that there is an on-going process of privacy review throughout the contractual chain and integrated risk assessment and decision support to assess harm.

One example of this is sticky policies, which bind usage controls to sensitive data as it is shared and processed around the cloud (Beiter et al., 2013). Indeed, in A4Cloud we intend to integrate mechanisms for legal enforcement and redress with corresponding machine readable representations of obligations

that can be automatically enforced and audited. This might build on for example an initial proposed approach illustrated in Figure 42, in which Creative Commons was used as the basis for provision of different types of policies (legal, human readable and machine readable) that were then enforced (Pearson & Tsiavos, 2014), such that the machine readable part of a contract generated by a smart notice is bound to data as it travels around the cloud and access is only allowed to that data if the policy is satisfied.

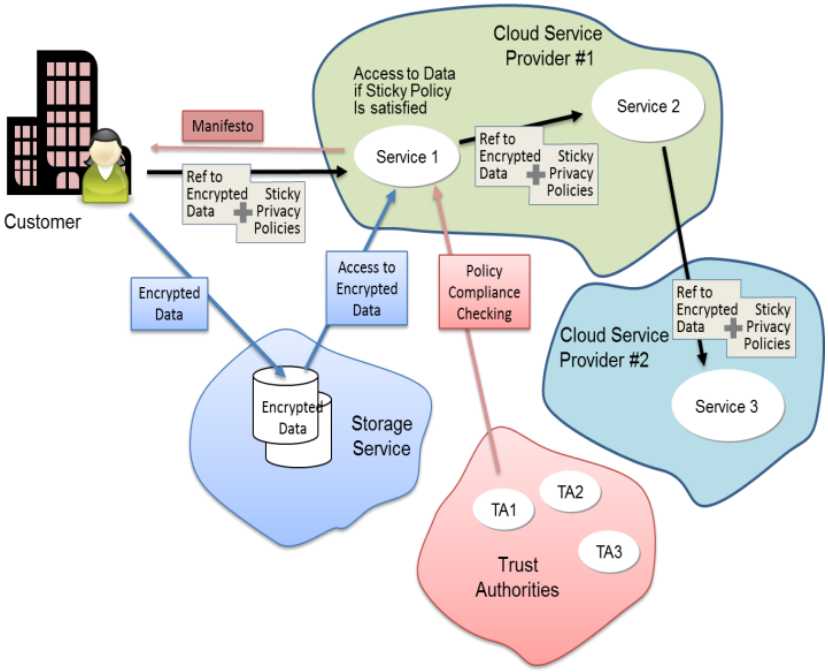


Figure 42 Chains of Accountability Using Sticky Policies

The accountability definitions map directly into the accountability practices. Accountability practices are implemented using accountability mechanisms and tools. We can model the accountability mechanisms at a number of levels, for example generic approach vs. instances, or more general versus more specific (e.g. policies versus IT policies). For some policies, it can be possible to map from a human readable form to a machine readable form, and even to a form for lawyers – legal policies or legal terms Figure 43, as in the Creative Commons approach (Pearson & Tsiavos, 2014).

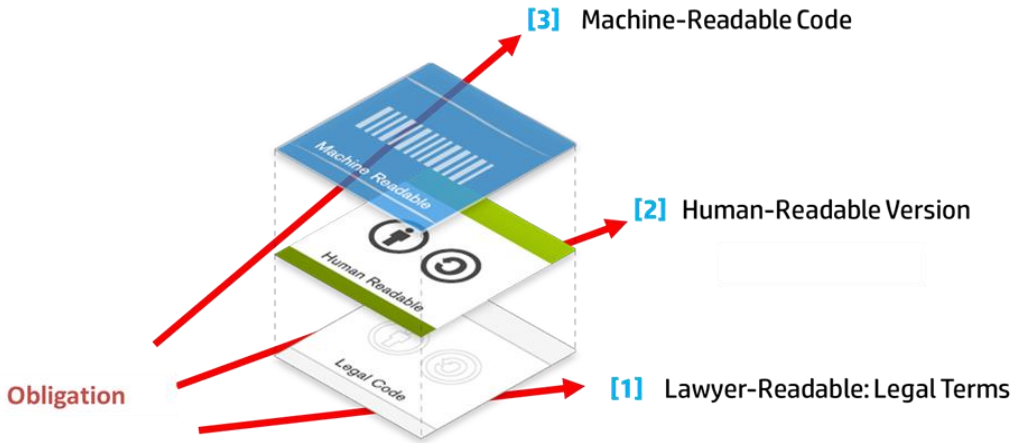


Figure 43 Mapping between Different Objects

Normative obligations relate to societal requirements and self-assessment obligations, thus giving the ethical dimension that maps across to the ethical element within the accountability definitions, and correspondingly for the need for organisations to take ethical considerations into account in their

decision-making processes that are part of the accountability practices. Different obligations will apply in different situations. It might be that a framework similar to that proposed in (Novotny & Spiekermann, 2013) could be useful in determining obligations in different spheres of the marketplace, including a sphere in which there would be an obligation to anonymise data. We might consider using this type of approach in future when modelling cloud service ecosystems. Different kind of accountability mechanisms can be used by different types of users/stakeholders. The accountability mechanisms could have certain properties, and be used at different times operationally. This is reflected within the accountability framework, where we can also show how A4Cloud mechanisms relate to such framework.

F. Accountability Maturity Model

The following table shows the security and privacy controls (column “Control Name”) related to accountability, following the criteria (gap analysis based on accountability attributes)) defined by the Accountability Maturity Model (AMM) presented in Section 8.2. These controls were extracted from well-known security and privacy frameworks (columns “Framework” and “Control Code”).

Control name	Control code	Framework	Observability	Verifiability	Attributability	Transparency	Responsibility	Liability	Remediability
Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02	CCM V3				■			■
Business Continuity Management & Operational Resilience Impact Analysis	BCR-09	CCM V3				■			
Business Continuity Management & Operational Resilience Management Program	BCR-10	CCM V3							■
Change Control & Configuration Management Unauthorised Software Installations	CCC-04	CCM V3				■			
Change Control & Configuration Management Production Changes	CCC-05	CCM V3					■		
Data Security & Information Lifecycle Management Classification	DSI-01	CCM V3				■			
Data Security & Information Lifecycle Management Data Inventory / Flows	DSI-02	CCM V3					■		
Data Center Security Asset Management	DCS-01	CCM V3					■		
Encryption & Key Management Entitlement	EKM-01	CCM V3				■			
Encryption & Key Management Key Generation	EKM-02	CCM V3					■		
Governance and Risk Management Management Support/Involvement	GRM-05	CCM V3				■			
Identity & Access Management Credential Lifecycle / Provision Management	IAM-02	CCM V3			■		■		
Identity & Access Management Trusted Sources	IAM-08	CCM V3				■			
Identity & Access Management *User Access Authorisation*	IAM-09	CCM V3			■				
Identity & Access Management *User Access Reviews*	IAM-10	CCM V3				■			
Identity & Access Management *User Access Revocation*	IAM-11	CCM V3			■				
Identity & Access Management *User ID Credentials*	IAM-12	CCM V3		■	■				
Identity & Access Management *Utility Programs Access*	IAM-13	CCM V3							
Infrastructure & Virtualisation Security Audit Logging / Intrusion Detection	IVS-01	CCM V3				■			
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management*	SEF-02	CCM V3				■			
Security Incident Management, E-Discovery & Cloud Forensics	SEF-03	CCM V3					■		

Control name	Control code	Framework	Observability	Verifiability	Attributability	Transparency	Responsibility	Liability	Remediability
Incident Reporting									
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	CCM V3							
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity*	STA-01	CCM V3							
Supply Chain Management, Transparency and Accountability *Incident Reporting*	STA-02	CCM V3							
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-04	CCM V3							
Supply Chain Management, Transparency and Accountability *Supply Chain Agreements*	STA-05	CCM V3							
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews*	STA-06	CCM V3							
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics*	STA-07	CCM V3							
Supply Chain Management, Transparency and Accountability *Third Party Assessment*	STA-08	CCM V3							
Supply Chain Management, Transparency and Accountability *Third Party Audits*	STA-09	CCM V3							
Threat and Vulnerability Management Anti-Virus / Malicious Software	TVM-01	CCM V3							
Privacy Incident and Breach Management	1.2.7	GAPP							
Communication to Individuals	2.1.1	GAPP							
Provision of Notice	2.2.1	GAPP							
Entities and Activities Covered	2.2.2	GAPP							
Clear and Conspicuous	2.2.3	GAPP							
Communication to Individuals	3.1.1	GAPP							
Consequences of Denying o withdrawing Consent	3.1.2	GAPP							
Consent for New Purposes and Uses	3.2.2	GAPP							
Types of Personal Information Collected and Methods of Collection	4.1.1	GAPP							
Collection Limited to Identified Purpose	4.1.2	GAPP							
Privacy Policies	4.2.4	GAPP							
Communication to Individuals	5.1.1	GAPP							
Use of Personal Information	5.2.1	GAPP							
Retention of Personal Information	5.2.2	GAPP							
Communication to Individuals	6.1.1	GAPP							
Access by Individuals to their Personal Information	6.2.1	GAPP							
Confirmation of an Individual's Identity	6.2.2	GAPP							
Understandable Personal Information, Time Frame, and Cost	6.2.3	GAPP							
Denial of Access	6.2.4	GAPP							
Updating or Correcting Personal Information	6.2.5	GAPP							
Statement of Disagreement	6.2.6	GAPP							
Communication to Individuals	7.1.1	GAPP							

Control name	Control code	Framework	Observability	Verifiability	Attributability	Transparency	Responsibility	Liability	Remediability
Communication to Third Parties	7.1.2	GAPP							
New Purposes and Uses	7.2.3	GAPP							
Misuse of Personal Information by a Third Party	7.2.4	GAPP							
Communication to Individuals	8.1.1	GAPP							
Logical Access Controls	8.2.2	GAPP							
Testing Security Safeguards	8.2.7	GAPP							
Communication to Individuals	9.1.1	GAPP							
Communication to Individuals	10.1.1	GAPP							
Inquiry, Complaint and Dispute Process	10.2.1	GAPP							
Dispute Resolution and Recourse	10.2.2	GAPP							
Ongoing Monitoring	10.2.5	GAPP							
Purpose specification	AP-2	NIST80053R4							
Privacy-enhanced system design and development	AR-7	NIST80053R4							
Accounting of disclosures	AR-8	NIST80053R5							
Consent	IP-1	NIST80053R6							
Individual access	IP-2	NIST80053R7							
Redress	IP-3	NIST80053R8							
Complaint management	IP-4	NIST80053R9							
Privacy notice	TR-1	NIST80053R10							
System of records notices and privacy act statements	TR-2	NIST80053R11							
Dissemination of privacy program information	TR-3	NIST80053R4							

G. Accountability Maturity Model Scoring

Functional Domain	Level 1 Defined	Level 2 Managed/Proactive	Level 3 Optimised
1. Accept responsibility	Define governance policies, and Responsibilities. Might include self-certification based on compliance frameworks.	Third party verification that organisational policies comply with appropriate legal obligations.	Enhancement of policies to include ethical aspects reflecting social values.
2. Identify controls	Use risk assessment tools and methodologies, obtain insurance and obtain certification. Usage of “controls cards”.	Use Privacy Impact Assessment throughout design lifecycle	Deploy automated policy definition tools & frameworks.
3. Implement measures	Define policies for implementation of controls, and deploy selected and privacy controls.	Policies are periodically reviewed.	Deploy automated policy enforcement tools.
4a. Provide account (demonstrate effectiveness of measures)	Provide public accounts.	Demonstrate effectiveness of mechanisms through impact assessments.	Use automated tools for demonstrating effectiveness.
4b. Provide account (validate operations)	Report operational aspects to the party which account is owed.	Reported operational aspects are reported and analysed.	Use data tracking systems. Automated collection of evidence tools.
4c. Provide account (attribute failure)	Report to the customer attribution of the failure corresponding to the detected incident.	Analyse reported incident information.	Use automated tools and interoperable format for reporting the incident information.
5. Monitor system	Deploy SIM/SIEM solutions. Regular audits.	Deploy agents to gather evidence in a continuous manner. Right to audit clauses included within contracts	Use automated tools for allowing customer to perform monitoring on demand.
6. External verification	Ability to provide accounts on demand.	Periodically maintain the processes to communicate with external entities.	Tools to support contractual transparency.
7. Notify exception	Notify supervisory authorities if there is a data breach. Notify data subjects where legally necessary if there is a data breach.	Deploy incident response tools.	Higher levels of transparency about data breaches.
8. Remediation and redress	Define policies and procedures for remediation and redress.	Deploy decision support systems to aid operators performing the remediation and redress actions. Periodically revise defined policies and procedures.	Deploy automated support for remediation and redress.

Glossary of Terms and Definitions

Term/Acronym	Brief Description/Definition	Source Reference
A4CLOUD	Accountability for Cloud and Other Future Internet Services	[A4CLOUD DoW] A4CLOUD, Accountability For Cloud and Other Future Internet Services, Annex I - Description of Work, Grant agreement 317550, 2012.
Access Control	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.
Access Control Policy	The set of rules that define the conditions under which an access may take place.	[NIST IR 7316] Hu, V. C., Ferraiolo, D. F., Kuhn, D. R., Assessment of Access Control Systems, NIST Interagency Report 7316, September 2006.
Accountability Attributes	Conceptual elements of accountability as used across different domains.	[A4CLOUD Conceptual Framework]
Accountability Evidence	Accountability Evidence as collection of data, metadata, routine information and formal operations performed on data and metadata which provide attributable and verifiable account of the fulfilment of relevant obligations with respect to the service and that can be used to support an argument shown to a third party about the validity of claims about the appropriate and effective functioning (or not) of an observable system.	[A4CLOUD Conceptual Framework]
Accountability Mechanisms	Diverse processes, non-technical mechanisms and tools that support accountability practices.	[A4CLOUD Conceptual Framework]
Accountability Model	Accountability attributes, practices and mechanisms.	[A4CLOUD Conceptual Framework]
Accountability Practices	Emergent behaviour characterising accountable organisations.	[A4CLOUD Conceptual Framework]
Accountability, Conceptual Definition	Accountability consists of defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly.	[A4CLOUD Conceptual Framework]
Accountability, for Data Stewardship in the Cloud Definition (A4CLOUD Definition)	Accountability for an organisation consists of accepting responsibility for data with which it is entrusted in a cloud environment, for its use of the data from the time it is collected until when the data is destroyed (including onward transfer to and from third parties). It involves the commitment to norms, explaining and demonstrating compliance to stakeholders and remedying any failure to act properly.	[A4CLOUD Conceptual Framework]
Accountability-based Approach	An accountability-based approach to data governance is characterised by its focus on setting privacy-protection goals for organisations based on criteria established in current public policy and on allowing organisations discretion in determining appropriate measures to reach those goals.	[CIPL 2011] Accountability: A Compendium for Stakeholders, The Centre for Information Policy Leadership, 2011.
Accountable Organisation	An accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognise outside criteria, and establishes performance mechanisms to ensure responsible decision-making about the management of data consistent with organisation policies.	[CIPL 2011] Accountability: A Compendium for Stakeholders, The Centre for Information Policy Leadership, 2011.
Appropriateness	The extent to which the technical and organisational measures used have the capability of contributing to accountability.	[A4CLOUD Conceptual Framework]
Assessment	see Security Control Assessment	
Asset	Any item that has value to the organisation.	[ISO/IEC 27000:2009(E)] ISO/IEC 27000:2009(E) Information Technology - Security techniques - Information security management systems - Overview and vocabulary.

Assurance	Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass.	[NIST SP 800-27 Rev. A] Stoneburner, G., Hayden, C., Feringa, A., Engineering Principles for Information Technology Security (A Baseline for Achieving Security), NIST Special Publication 800-27 Rev. A, June 2004.
Attributability	The possibility to trace a given action back to a specific entity.	[A4CLOUD Conceptual Framework]
Attribution	In case of a deviation from the expected behaviour (fault), an accountability system reveals which component is responsible (attribution).	[ENISA 2011] ENISA, Privacy, Accountability and Trust – Challenges and Opportunities, 2011.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures.	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.
Audit Log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period.	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.
Audit Trail	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.
Authorization	A prescription that a particular behavior shall not be prevented.	[ISO/IEC 15414:2006] ISO/IEC 15414:2006 Information technology - Open distributed processing - Reference model - Enterprise language.
Availability	The property of being accessible and usable upon demand by an authorized entity.	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.
Behaviour	The actual data processing behaviour of an organisation.	[A4CLOUD Conceptual Framework]
Binding Corporate Rules (BCRs)	Binding corporate rules (BCRs) are a legal tool that can be used by multinational companies to ensure an adequate level of protection for the intra-group transfers of personal data from a country in the EU or the European Economic Area (EEA) to a third country. The use of BCRs requires, in principle, the approval of each of the EU or EEA data protection authorities from whose country the data are to be transferred.	[EDPS Glossary] European Data Protection Supervisor (EDPS) Glossary - accessed online.
Broad Network Access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).	[NIST SP 800-145] Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.
Chain of Evidence	A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence. The "sequencing" of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner.	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.
Cloud Auditor	An entity that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation, with regards to a set of requirements, which may include security, data protection, information system management, regulations and ethics.	[A4CLOUD Conceptual Framework]

Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Customers.	[NIST SP 500-292] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., Leaf, D., NIST Cloud Computing Reference Architecture, NIST Special Publication 500-292, September 2011.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.	[NIST SP 500-292] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., Leaf, D., NIST Cloud Computing Reference Architecture, NIST Special Publication 500-292, September 2011.
Cloud Computing	Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.	[NIST SP 800-145] Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.
Cloud Consumer	see Cloud Customer	
Cloud Customer	An entity that (a) maintains a business relationship with, and (b) uses services from a Cloud Provider. When necessary we may further distinguish: a) Individual Cloud Customer, when the entity refers to a person. b) Organisation Cloud Customer, when the entity refers to an organisation.	[A4CLOUD Conceptual Framework]
Cloud Distribution	The process of transporting cloud data between Cloud Providers and Cloud Consumers.	[NIST SP 500-292] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., Leaf, D., NIST Cloud Computing Reference Architecture, NIST Special Publication 500-292, September 2011.
Cloud Ecosystem	A cloud computing business ecosystem (cloud ecosystem) is a business ecosystem of interacting organizations and individuals - the actors of the cloud ecosystem - providing and consuming cloud services.	[FG-Cloud-TR-1] ITU-T, FG Cloud TR, Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements, Version 1.0 (02/2012), ITU, 2012.
Cloud Governance	Cloud governance encompasses two main areas: internal governance focuses on a provider's technical working of cloud services, its business operations, and the ways it manages its relationship with customers and other external stakeholders; and external governance consists of the norms, rules, and regulations which define the relationships between members of the cloud community and attempt to solve disputes between them.	[Ree2013] Reed, C., Cloud Governance: The Way Forward. In Millard, C. (Ed.), Cloud Computing Law, Oxford University Press, 2013.
Cloud Provider (CP)	An entity responsible for making a [cloud] service available to cloud customers.	[A4CLOUD Conceptual Framework]
Cloud Service Management	Cloud Service Management includes all of the service-related functions that are necessary for the management and operation of those services required by or proposed to cloud consumers.	[NIST SP 500-291] Hogan, M., Liu, F., Sokol, A., Tong, J., NIST Cloud Computing Standards Roadmap Working Group, NIST Cloud Computing Standards Roadmap, NIST Special Publication 500-291, Version 1.0, July 2011.
Cloud Service Provider (CSP)	see Cloud Provider	
Cloud Subject	An entity whose data are processed by a cloud provider, either directly or indirectly. When necessary we may further distinguish: a) Individual Cloud Subject, when the entity refers to a person. b) Organisation Cloud Subject, when the entity refers to an organisation.	[A4CLOUD Conceptual Framework]
Cloud Supervisory Authority	An entity that oversees and enforces the application of a set of rules.	[A4CLOUD Conceptual Framework]
Cloud User	see Cloud Customer	
Community Cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).	[NIST SP 800-145] Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.
Compliance	Compliance entails the comparison of an organisation's actual behaviour with the norms.	[A4CLOUD Conceptual Framework]
Confidential	Class of information that is sensitive and/or business critical and therefore needs to be protected to a reasonable extent. It is intended for limited distribution within the organization or	[ISO27k] ISO27k implementers' forum, Hyperlinked information security glossary, 2007.

	to specially designated third parties, on a need-to-know ('default deny') basis.	
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	[NIST SP 800-53A] Joint Task Force Transformation Initiative, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, NIST Special Publication 800-53A, Revision 1, June 2010.
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature.	[ISO/IEC 27000:2009(E)] ISO/IEC 27000:2009(E) Information Technology - Security techniques - Information security management systems - Overview and vocabulary.
Data Controller	The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.	[Directive 95/46/EC] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281/31, 23/11/1995.
Data Integrity	The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.	[IETF RFC4949:2007] IETF, Internet Security Glossary, Version 2, RFC 4949, Internet Engineering Task Force (IETF), August 2007.
Data Processor	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.	[Directive 95/46/EC] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281/31, 23/11/1995.
Data Protection Agency (DPA)	see Data Protection Authority	
Data Protection Authority (DPA)	A data protection authority is an independent body which is in charge of: monitoring the processing of personal data within its jurisdiction (country, region or international organization); providing advice to the competent bodies with regard to legislative and administrative measures relating to the processing of personal data; hearing complaints lodged by citizens with regard to the protection of their data protection rights. According to Article 28 of Directive 95/46/EC, each Member State shall establish in its territory at least one data protection authority, which shall be endowed with investigative powers (such as access to data, collection of information, etc.), effective powers of intervention (power to order the erasure of data, to impose a ban on a processing, etc.), and the power to start legal proceedings when data protection law has been violated.	[EDPS Glossary] European Data Protection Supervisor (EDPS) Glossary - accessed online.
Data Protection Impact Assessment (DPIA)	A systematic process for evaluating the potential impact of risks where processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes to be carried out by the controller or the processor acting on the controller's behalf.	[Article 29 00678/13/EN WP205] Article 29 Data Protection Working Party, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force, 00678/13/EN WP205, 22 April 2013.
Data Protection Officer (DPO)	Each Community institution and body shall have a data protection officer (DPO). The DPO shall ensure the internal application of the Regulation and that the rights and freedoms of the data subjects are not likely to be adversely affected by the processing operations. The DPO shall also keep a register of processing operations that have been notified by the controllers of the institution or body where he or she works.	[EDPS Glossary] European Data Protection Supervisor (EDPS) Glossary - accessed online.
Data Security	Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.

Data Subject	An identified or identifiable natural person ('data subject') to whom 'personal data' relate to; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;	[Directive 95/46/EC] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281/31, 23/11/1995.
Data Subject Consent	Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.	[Article 29 01197/11/EN WP187] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 01197/11/EN WP187, 13 July 2011.
Data Transfer	Data transfer refers to the transmission / communication of data to a recipient in whatever way.	[EDPS Glossary] European Data Protection Supervisor (EDPS) Glossary - accessed online.
Directive 2009/136/EC	Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.	[Directive 2009/136/EC] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Official Journal of the European Communities L 337/11, 18/12/2009.
Directive 95/46/EC	European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This directive defines the overall concept of data protection in the Europe. Under this directive, individual personal data has to be collected openly and fairly with a clear explanation of the purpose for its collection.	[Directive 95/46/EC] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281/31, 23/11/1995.
Due Process	A moral claim to provide fair and equal treatment, and incorporates rights to full information, the right to be heard, to ask questions and receive answers, and the right to redress.	
Effectiveness	The extent to which the technical and organisational measures used actually contribute to accountability.	[A4CLOUD Conceptual Framework]
Ethical Accountability	It is the practice of taking responsibility of own's actions and to be accountable to one's self not only to others. It ensures: 1) the practice of sustainable development, 2) democratic accountability where all stakeholders are involved in the decision making process, 3) self-monitoring and self-auditing.	[A4CLOUD Conceptual Framework]
Event	Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.
Evidence	An accountability system produces evidence that can be used to convince a third party that a fault has or has not occurred (evidence).	[ENISA 2011] ENISA, Privacy, Accountability and Trust – Challenges and Opportunities, 2011.
Governance	Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services.	[NIST SP 800-144] Jansen, W., Grance, T., Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, December 2011.
Hybrid Cloud	The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).	[NIST SP 800-145] Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.

Individual Cloud Customer	see Cloud Customer	[A4CLOUD Conceptual Framework]
Individual Cloud Subject	see Cloud Subject	[A4CLOUD Conceptual Framework]
Information Accountability	Information accountability means that information usage should be transparent so it is possible to determine whether a use is appropriate under a given set of rules.	[Wei2008] Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., Sussman, G. J., Information accountability. Commun. ACM 51(6):82-87, June 2008. DOI=http://doi.acm.org/10.1145/1349026.1349043
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.
Information Technology (IT)	IT encompasses all technologies for the capture, storage, retrieval, processing, display, representation, organization, management, security, transfer, and interchange of data and information.	[NIST SP 500-291] Hogan, M., Liu, F., Sokol, A., Tong, J., NIST Cloud Computing Standards Roadmap Working Group, NIST Cloud Computing Standards Roadmap, NIST Special Publication 500-291, Version 1.0, July 2011.
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.	[NIST SP 800-145] Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.
Integrity	see Data Integrity	
Liability	The state (of an organisation or individual) of being legally obligated or responsible in connection with failure to apply the norms.	[A4CLOUD Conceptual Framework]
Measured Service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).	[NIST SP 800-145] Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.
Multi-tenancy	A characteristic of cloud in which resources are shared amongst multiple cloud tenants.	[FG-Cloud-TR-1] ITU-T, FG Cloud TR, Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements, Version 1.0 (02/2012), ITU, 2012.
Non-repudiation	The property whereby a party in a dispute cannot repudiate or refute the validity of a statement or contract.	[ENISA 2009] Catteddu, D., Hogben, G. (Eds.), Could Computing: Benefits, risks and recommendations for information security, European Network and Information Security Agency (ENISA), 2009.
Norms	The obligations and permissions that define data practices; these can be expressed in policies and they derive from law, contracts and ethics.	[A4CLOUD Conceptual Framework]
Obfuscation	The production of misleading, ambiguous and plausible but convincing information as an act of concealment or evasion.	[BN2013] Brunton, F., Nissenbaum, H., Political and Ethical Perspectives on Data Obfuscation, In Hildebrandt, M., de Vries, K., (Eds.) Privacy, Due Process and the Computational Turn, New York: Routledge, pp. 164-188, 2013.
Obligation	A prescription that a particular behavior is required.	[ISO/IEC 10746-2:2009] Information technology - Open Distributed Processing - Reference Model: Foundations.
Obligation, Legal	A legal duty.	
Observability	The extent to which the behaviour of the system is externally viewable.	[A4CLOUD Conceptual Framework]
On-demand Self-service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.	[NIST SP 800-145] Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.
Organisation Cloud Customer	see Cloud Customer	[A4CLOUD Conceptual Framework]
Organisation Cloud Subject	see Cloud Subject	[A4CLOUD Conceptual Framework]
Permission	A prescription that a particular behavior is allowed to occur.	ISO/IEC 10746-2:2009 Information technology -- Open Distributed Processing -- Reference Model: Foundations.

Person Pseudonym	A substitute or alias for a data subject's civil identity (name) which may be used in many different contexts.	[PRIME Framework V3] Fischer-Hübner, S., Hedbom, H., (Eds.), Framework V3, D14.1.c, PRIME, 2008.
Personal Data	'Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.	[Directive 95/46/EC] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281/31, 23/11/1995.
Personally Identifiable Information (PII)	Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.	[NIST SP 800-145] Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.
Policy	A set of rules related to a particular purpose. A rule can be expressed as an obligation, an authorization, a permission, or a prohibition. Not every policy is a constraint. Some policies represent an empowerment.	[ISO/IEC 15414:2006] ISO/IEC 15414:2006 Information technology - Open distributed processing - Reference model - Enterprise language.
Policy Enforcement	The execution of a policy decision.	[IETF RFC3198:2001] IETF, Terminology for Policy-Based Management, RFC 3198, Internet Engineering Task Force (IETF), November 2001.
Policy Violation	see Violation	
Primary Service Provider (PSP)	see Cloud Provider	
Privacy	The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. The ability to control the collection and sharing of information about oneself.	[Wes1967] Westin, A. F., Privacy and Freedom, New York: Atheneum, 1967.
Privacy by Design	Privacy by Design (PbD) is an approach to protecting privacy by embedding it into the design specifications of information technologies, accountable business practices, and networked infrastructures, right from the outset.	[Cav2011] Cavoukian, A., Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers, Information and Privacy Commissioner, Ontario, Canada, August 2011.
Privacy Enhancing Tool (PET)	It refers to a coherent system of information and communication technology (ICT) measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system.	[EDPS Glossary] European Data Protection Supervisor (EDPS) Glossary - accessed online.
Privacy Impact Assessment (PIA)	An analysis of how information is handled 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) t determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential risks.	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.
Privacy Impact Audit	Systematic evaluation of a cloud system by measuring how well it conforms to a set of established privacy-impact criteria.	[NIST SP 500-292] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., Leaf, D., NIST Cloud Computing Reference Architecture, NIST Special Publication 500-292, September 2011.
Privacy Policy Language (PPL)		

Privacy Preferences		
Private Cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units).	[NIST SP 800-145] Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.
Processing of Personal Data	Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.	[Directive 95/46/EC] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281/31, 23/11/1995.
Processor Agreement	Transfers of personal data from a data controller to a data processor must be secured by a contractual agreement. The contract must stipulate that the data processor shall act only on instructions from the data controller. The data processor must provide sufficient guarantees in respect of the technical security measures and organizational measure governing the processing to be carried out, and must ensure compliance with such measures.	[EDPS Glossary] European Data Protection Supervisor (EDPS) Glossary - accessed online.
Prohibition	A prescription that a particular behavior must not occur.	[ISO/IEC 10746-2:2009] Information technology - Open Distributed Processing - Reference Model: Foundations.
Proof of Retrievability (POR)	Protocol that allows a client that has stored data at an untrusted store to verify in an efficient way that the verifies has means to retrieve the original data without actually retrieving it.	[JK2007] Juels, A., Kaliski, B. S. Jr., Pors: proofs of retrievability for large files. In Proceedings of the 14th ACM conference on Computer and communications security (CCS '07), ACM, New York, NY, USA, pp. 584-597, 2007. DOI=http://doi.acm.org/10.1145/1315245.1315317
Pseudonym	A pseudonym is an identifier of a subject other than the subject's civil identity.	[PRIME Framework V3] Fischer-Hübner, S., Hedbom, H., (Eds.), Framework V3, D14.1.c, PRIME, 2008.
Public Cloud	The cloud infrastructure is provisioned for open use by the general public.	[NIST SP 800-145] Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.
Rapid Elasticity	Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.	[NIST SP 800-145] Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.
Recipient	A natural or legal person, public authority, agency, or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.	[Directive 95/46/EC] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281/31, 23/11/1995.
Relationship Pseudonym	A pseudonym that is used in regard to a specific communication partner (e.g., distinct nicknames for different communication partners).	[PRIME Framework V3] Fischer-Hübner, S., Hedbom, H., (Eds.), Framework V3, D14.1.c, PRIME, 2008.
Remediability	The property of a system, organisation or individual to take corrective action and/or provide a remedy for any party harmed in case of failure to comply with its governing norms.	[A4CLOUD Conceptual Framework]
Remediation	The act of mitigating a vulnerability or a threat.	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.
Remedy(ies)	Any of the methods available at law for the enforcement, protection or recovery of rights or for obtaining redress for their infringement (judicial/administrative).	
Reputation	An expectation about an entity's behavior based on information about or observations of its past behaviour. It is a form of social control in the context of trust propagation. In a multi-agent system, reputation is the voice the agent is spreading which is not necessarily the truth while image is the actual reputation the agent has for the subject.	[ARH2000] Abdul-Rahman, A.; Hailes, S., Supporting trust in virtual communities. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, vol.1, pp. 1-9, 2000. DOI: http://dx.doi.org/10.1109/HICSS.2000.926814 [CP2002] Conte, R., Paolucci, M., Reputation in Artificial Societies: Social Beliefs for Social Order.

		Multiagent Systems, Artificial Societies, and Simulated Organizations series, Vol. 6, Kluwer Academic Publishers, 2002.
Resource Pooling	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.	[NIST SP 800-145] Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.
Responsibility	The property of an organisation or individual in relation to an object, process or system of being assigned to take action to be in compliance with the norms.	[A4CLOUD Conceptual Framework]
Responsiveness	the property of a system, organisation or individual to take into account input from external stakeholders and respond to queries of these stakeholders.	[A4CLOUD Conceptual Framework]
Right of Access	It is the right for any data subject to obtain from the controller of a processing operation the confirmation that data related to him/her are being processed, the purpose(s) for which they are processed, as well as the logic involved in any automated decision process concerning him or her.	[EDPS Glossary] European Data Protection Supervisor (EDPS) Glossary - accessed online.
Right of Information	Everyone has the right to know that their personal data are processed and for which purpose. The right to be informed is essential because it determines the exercise of other rights. The right of information refers to the information which shall be provided to a data subject whether or not the data have been obtained from the data subject. The information which must be provided relates to the identity of the controller, the purpose(s) of the processing, the recipients, as well as the existence of the right of access to data and the right to rectify the data. The right of information for the person concerned is limited in some cases, such as for public safety considerations or for the prevention, investigation, identification and prosecution of criminal offences, including the fight against money laundering.	[EDPS Glossary] European Data Protection Supervisor (EDPS) Glossary - accessed online.
Right of Rectification	The right of rectification is the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data. The right of rectification is an essential complement to the right of access and is important to maintain a high level of data quality. To exercise the right of rectification, the data subject usually has to contact the controller of the processing operation.	[EDPS Glossary] European Data Protection Supervisor (EDPS) Glossary - accessed online.
Right of Rectification	It is the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data.	[EDPS Glossary] European Data Protection Supervisor (EDPS) Glossary - accessed online.
Right to Object	The right to object has two meanings. First, it is the general right of any data subject to object to the processing of data relating to him or her, except in certain cases such as a specific legal obligation. Where there is a justified objection based on legitimate grounds relating to his or her particular situation, the processing in question may no longer involve those data. It also refers to the specific right of any data subject to be informed, free of charge, before personal data are first disclosed to third parties or before they are used on their behalf for the purposes of direct marketing, and to object to such use without justification.	[EDPS Glossary] European Data Protection Supervisor (EDPS) Glossary - accessed online.
Risk	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	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.

	event occurs; and 2) the likelihood of occurrence.	
Risk Analysis	Systematic use of information to identify sources and to estimate risk.	[ISO/IEC 27000:2009(E)] ISO/IEC 27000:2009(E) Information Technology - Security techniques - Information security management systems - Overview and vocabulary.
Risk Assessment	Overall process of risk analysis and risk evaluation	[ISO/IEC 27000:2009(E)] ISO/IEC 27000:2009(E) Information Technology - Security techniques - Information security management systems - Overview and vocabulary.
Risk Estimation	Activity to assign values to the probability and consequences of a risk.	[ISO/IEC 27000:2009(E)] ISO/IEC 27000:2009(E) Information Technology - Security techniques - Information security management systems - Overview and vocabulary.
Risk Evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.	[ISO/IEC 27000:2009(E)] ISO/IEC 27000:2009(E) Information Technology - Security techniques - Information security management systems - Overview and vocabulary.
Risk Management	Coordinated activities to direct and control an organization with regard to risk.	[ISO/IEC 27000:2009(E)] ISO/IEC 27000:2009(E) Information Technology - Security techniques - Information security management systems - Overview and vocabulary.
Role Pseudonym	A pseudonym that is chosen for the use in a specific role (e.g., patient or customer).	[PRIME Framework V3] Fischer-Hübner, S., Hedbom, H., (Eds.), Framework V3, D14.1.c, PRIME, 2008.
Role-Relationship Pseudonym	A pseudonym that is used for a specific combination of a role and communication partner.	[PRIME Framework V3] Fischer-Hübner, S., Hedbom, H., (Eds.), Framework V3, D14.1.c, PRIME, 2008.
Rule	A constraint on a system specification.	ISO/IEC 10746-2:2009 Information technology -- Open Distributed Processing -- Reference Model: Foundations.
Sanction(s)	A measure taken against an entity to compel it to obey to data protection legislation or to punish it for a breach of a contractual clause.	
Security	see Information Security	
Security Breach	A breach of security occurs where a stated organizational policy or legal requirement regarding information security has been violated. However, every incident which suggests that the confidentiality, integrity or availability of the information has been compromised can be considered a security incident. Every security breach will always be initiated by a security incident which, only if confirmed, may become a breach.	[EDPS Glossary] European Data Protection Supervisor (EDPS) Glossary - accessed online.
Security Control Assessment	The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.	[NIST SP 800-53] Joint Task Force Transformation Initiative, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, Revision 4, April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4
Service Level Agreement (SLA)	An SLA represents the understanding between the cloud consumer and cloud provider about the expected level of service to be delivered and, in the event that the provider fails to deliver the service at the level specified, the compensation available to the cloud consumer.	[NIST SP 800-144] Jansen, W., Grance, T., Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, December 2011.
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.	[NIST SP 800-145] Mell, P., Grance, T., The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011.
Stakeholder	Individual, group, or organization who may affect, be affected by, or perceive itself to be affected by a decision or activity.	[ISO/IEC 38500:2008] ISO/IEC 38500:2008 Corporate governance of information technology.
Standard Contractual Clauses	Standard contractual clauses are legal tools to provide adequate safeguards for data transfers from the EU or the European Economic Area to third countries. The European Commission has adopted three Decisions declaring Standard Contractual Clauses to be adequate, and therefore, companies can incorporate the clauses into a transfer contract. In principle no authorization is required from data protection	[EDPS Glossary] European Data Protection Supervisor (EDPS) Glossary - accessed online.

	authorities to be allowed to use these clauses. A formal notification to the authority might nevertheless be necessary.	
Third country	A third country is a country which has not adopted a national law for the implementation of Directive 95/46/EC - as opposed to the 28 Member States of the EU and the three European Economic Area (EEA) countries Norway, Liechtenstein and Iceland. Third countries need to ensure an adequate level of protection for personal data in order to enable transfers of personal data from the EU and EEA Member States to them. The effect of such a decision is that personal data can flow from the EU and EEA Member States to that third country (within the limit of the material scope as described by each Decision) without any further safeguards.	[EDPS Glossary] European Data Protection Supervisor (EDPS) Glossary - accessed online.
Third Party	Any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.	[Directive 95/46/EC] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities L 281/31, 23/11/1995.
Threat	Potential cause of an unwanted incident, which may result in harm to a system or organization.	[ISO/IEC 27000:2009(E)] ISO/IEC 27000:2009(E) Information Technology - Security techniques - Information security management systems - Overview and vocabulary.
Transaction Pseudonym	A pseudonym that is used for a specific transaction only, i.e., for each transaction, a different pseudonym is used.	[PRIME Framework V3] Fischer-Hübner, S., Hedbom, H., (Eds.), Framework V3, D14.1.c, PRIME, 2008.
Transparency	The property of a system, organisation or individual of providing visibility of its governing norms, behaviour and compliance of behaviour to the norms.	[A4CLOUD Conceptual Framework]
Transparency Enhancing Tool (TET)		
Transparency, ex ante	it is concerned with the anticipation of consequences before data is actually disclosed (e.g. in the form of a certain behaviour).	[FIDIS 2009] Mireille Hildebrandt (Ed), D 7.12: Behavioural Biometric Profiling and Transparency Enhancing Tools, FIDIS 2009.
Transparency, ex post	It is concerned with informing about consequences if data already has been revealed.	[FIDIS 2009] Mireille Hildebrandt (Ed), D 7.12: Behavioural Biometric Profiling and Transparency Enhancing Tools, FIDIS 2009.
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.	[Gam1988] Gambetta, D., (Ed.) Trust: Making and Breaking Cooperative Relations. Oxford: Basil Blackwell, 1988.
Trustworthiness	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.	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.
Unauthorized Disclosure	An event involving the exposure of information to entities not authorized access to the information.	[CNSSI 4009:2010] National Information Assurance (IA) Glossary, Committee on National Security Systems (CNSS), CNSS Instruction No. 4009, 2010.
Unauthorized Information Disclosure	see Unauthorized Disclosure	
Usability	Extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.	[ISO 9241-11:1998] ISO 9241-11:1998 Ergonomic requirements for office work with visual display terminals (VDTs) - Part 11: Guidance on usability.
Usage control	Usage control is an extension of access control that covers not only who may access which data, but also how the data may or may not be used	[Hil2007] Hilty, M., Pretschner, A., Basin, D., Schaefer, C., Walter, T., A Policy Language for Distributed Usage Control. In Biskup, J., López, J., (Eds.), Computer Security – ESORICS 2007,

	afterwards. Thus it comprises: Managing reading, writing and other operations we could do on data, controlling data distribution in the network, and furthermore constraining what happens after redistribution to the data.	Proceedings of the 12th European Symposium On Research In Computer Security, Springer-Verlag, LNCS 4734, pp. 531-546 2007. DOI: http://dx.doi.org/10.1007/978-3-540-74835-9_35
Validation	An accountability system allows users, operators and third parties to verify a posteriori if the system has performed a data processing task as expected (validation).	[ENISA 2011] ENISA, Privacy, Accountability and Trust – Challenges and Opportunities, 2011.
Verifiability	the extent to which it is possible to assess norm compliance.	[A4CLOUD Conceptual Framework]
Violation	A behavior contrary to that required by a rule.	ISO/IEC 15414:2006, Information technology — Open distributed processing — Reference model — Enterprise language.
Vulnerability	Weakness of an asset or control that can be exploited by a threat. Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.	[ISO/IEC 27000:2009(E)] ISO/IEC 27000:2009(E) Information Technology - Security techniques - Information security management systems - Overview and vocabulary. [ENISA 2009] Catteddu, D., Hogben, G. (Eds.), Could Computing: Benefits, risks and recommendations for information security, European Network and Information Security Agency (ENISA), 2009.