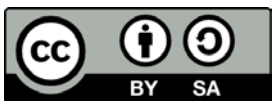
CLOUD
ACCOUNTABILITY
PROJECT

Cloud Accountability Reference Architecture

Project Release



This document has been edited by Frederic Gittler (HPE) and Siani Pearson (HPE)

Contributors to this document include Richard Mark Brown (ATC), Vasilis Tountopoulos (ATC), Jesus Luna (CSA), Alain Pannetrat (CSA), Mehdi Haddad (EMN), Jean-Claude Royer (EMN), Mohamed Sellami (EMN), Monir Azraoui (EURECOM), Kaoutar Elkhiyaoui (EURECOM), Melek Önen (EURECOM), Theo Koulouris (HPE), Niamh Gleeson (QMUL), Asma Vranaki (QMUL), Anderson Santana De Oliveira (SAP), Karin Bernsmed (SINTEF), Martin G. Jaatun (SINTEF), Lorenzo Dalla Corte (TiU), Carmen Gago (UMA), David Núñez (UMA)

We wish to acknowledge the reviews done by Christoph Reich (HFU), Rehab Alnemr (HPE), and Mickey Dichter (HPE)

This work has been partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no:317550 (A4CLOUD) Cloud Accountability Project.

Executive Summary and Reading Guide

The goal of the Cloud Accountability Reference Architecture is to provide an abstract but powerful model for designing accountability in modern cloud and future Internet ecosystems. It is an essential step towards addressing the requirements of target stakeholders by defining the architectural vision and capabilities and delivering a roadmap to implement such requirements in specific cases, aligned with selected business goals.

The context of our work is the cloud, with its associated ecosystem of customers, providers, auditors and regulators. Whilst we often refer to accountability in the context of data protection, our aim is to design an architecture which is agnostic of the particular domain of accountability.

Hence, we adopt a definition of accountability which can be applied to most enterprise operations, and most notably to information technology (IT)-supported functions, namely that:

accountability is the *state of*

- ***accepting*** *allocated responsibilities,*
- ***explaining*** *and* ***demonstrating*** *compliance to stakeholders and*
- ***remedying*** *any failure to act properly;*

where these responsibilities may be derived from

- *law,*
- *social norms,*
- *agreements,*
- *organisational values and*
- *ethical obligations*.

This document builds on the concepts and models developed in the Cloud Accountability Conceptual Framework[1], and most notably develops the mechanisms which provide the means to implement and deploy the practices specified in the accountability model shown in Figure 1 below (which provides an overview of the concept of accountability at different levels of abstraction):

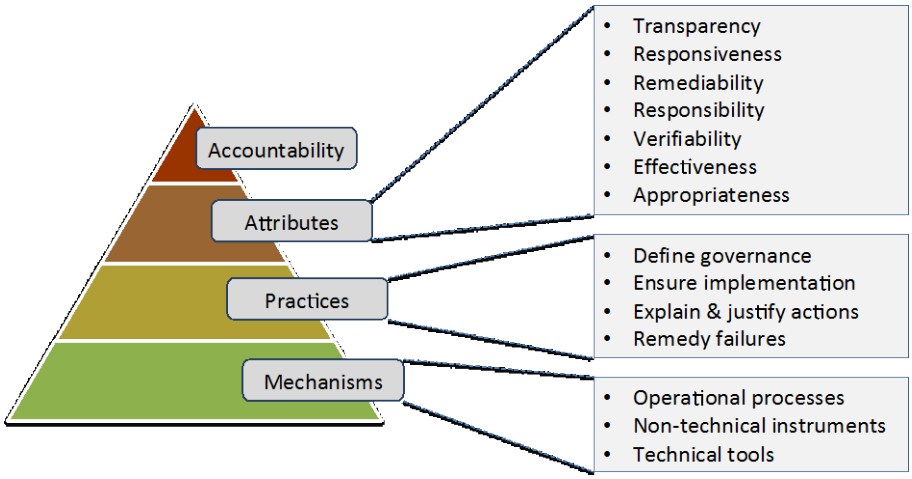


Figure 1: The Cloud accountability model.

We have identified six key groups of practices which must be addressed by accountable organisations, shown in Figure 2, where these are mapped onto an Accountability Lifecycle.

[1] S. Pearson, M. Felici and et al., "WP-32 Conceptual Framework," A4Cloud project, 2014

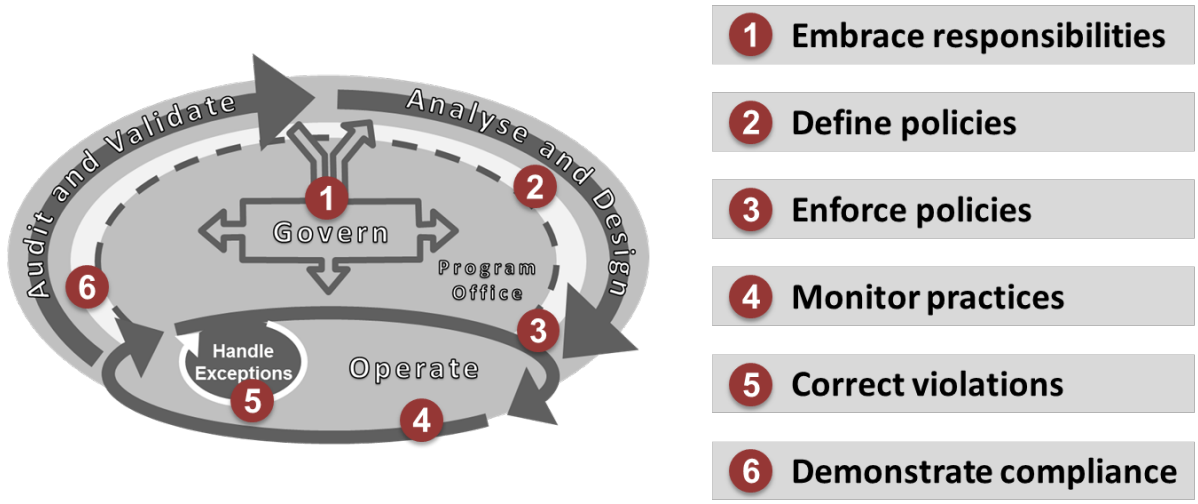


Figure 2: Accountability lifecycle and practices.

This lifecycle, presented in more detail in section 3, addresses both the governance programme of the organisation (Govern and Program Office elements), as well as the lifecycle for the services or applications to be developed (which comprises Analyse and Design, Operate, Handle Exceptions, and Audit and Validate phases).

We provide a Reference Framework that clarifies the functional elements and mechanisms of accountability. Figure 3 shows this information captured in an integrated diagram.

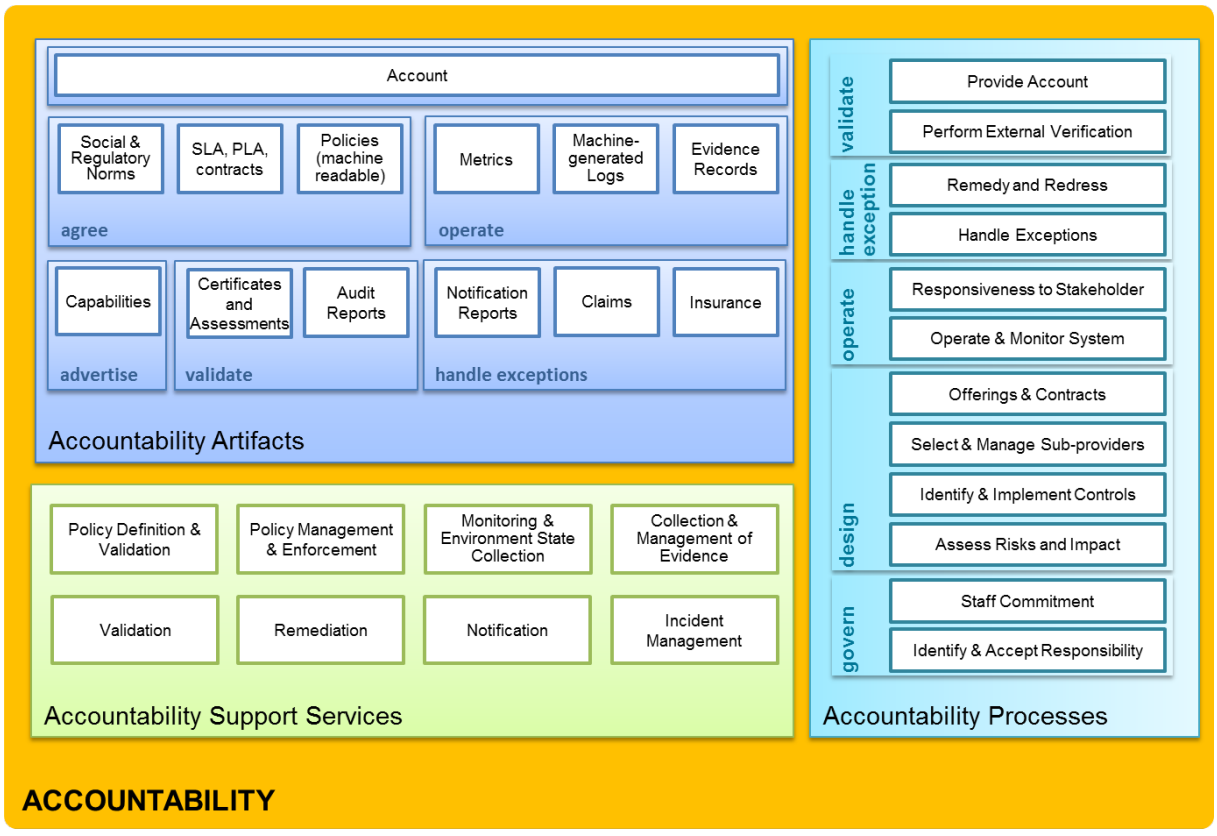


Figure 3: The accountability reference framework.

We discuss the elements of this framework throughout the document, building progressively towards the full picture. We start in section 2 by addressing how accountability applies to the cloud, focusing our analysis on the actors and how they interact. In section 2.4 we identify the various accountability artifacts which are exchanged between actors across the cloud provisioning chain.

In section 3, we shift our focus to the organisations that will be accountable to other stakeholders. After defining the lifecycle, we identify a series of process groups that map to this lifecycle. We are offering practical guidance to organisations that want to behave in an accountable manner at three different levels of abstraction:

- A set of principles for accountable behaviour, which we have designed specifically for use by small and medium sized organisations (SMEs) which do not have the organisational structure to adopt the more detailed recommendations
- A simplified control framework specific to accountable organisations, which leverages existing control frameworks to specifically address accountability
- A series of best practices which provide practical guidance about the governance and processes that accountable organisations need to deploy. This list can also be used in case of questions in the interpretation of the control framework

In section 4, we focus our attention on the various aspects of demonstrating accountability. We provide an in-depth analysis of the account, which is the core instrument to demonstrate accountability. An account is a report or description, which may be written and/or oral, of an event or process. It serves to report what happened, what has happened, or what might happen. It is produced on a schedule, on request, or as an answer to specific questions. Accounts are produced at various points of the service lifecycle: as a companion to service descriptions for the prospective customer, to communicate audit results and system state to existing customers, and to report on the handling of failures to continuously meet obligations. Accounts are primarily intended for customers and for auditors mandated by regulators, depending on the situation.

We also address other methods to complement the account when demonstrating accountability, either in a very dynamic context (section 4.6 on Metrics and Evidence) or being more effective in the use of resources (section 4.7 on Certifications and Continuous Compliance). The Accountability Maturity Model we present in section 4.8 focuses on capturing both the maturity of individual organisations in terms of accountability practices, as well as a measurement of the appropriateness of the measures used across the whole cloud provisioning chains, as a way to aid organisations (in particular, SMEs) to quantitatively assess their accountability practices as a first step to improving them.

Finally, in section 5, we propose a set of cloud accountability support services that are designed to offer an automated accountability interface to process the artifacts identified above.

Note to the Reader

We have structured the Cloud Accountability Reference Architecture document so that it offers two reading levels:

- CORE: central material that provides enough detail to obtain a general understanding of the Reference Architecture
- DETAILS: additional information that allows a deeper understanding of the selected topics

The Cloud Accountability Reference Architecture is structured to be accessed through a web interface, the PDF version being offered as a convenient option for those who prefer this medium. In order to present the same content in both versions, we have unified the structure across the two formats. Sections with a CORE reading level are intermixed with sections addressing DETAILS topics, organised in a logical flow of delivery. DETAILS sections are easy to identify, as:

- The section title starts with [DETAILS]
- The section is always a “level 2” text (e.g. N.NN section number)
- The colour of the text is **dark red**, not **black**
- The text starts with the following note:

> The information presented in this section represents details which may only be required if seeking an in-depth understanding of the Cloud Accountability Reference Architecture.

Table of Contents

1 Fundamental Concepts

We adopt a definition of accountability which can be applied to most enterprise operations, and most notably to IT-supported functions:

accountability is the *state of*
- *accepting allocated responsibilities,*
- *explaining and demonstrating compliance to stakeholders and*
- *remedying any failure to act properly;*

where these responsibilities are derived from
- *law,*
- *social norms,*
- *agreements,*
- *organisational values and*
- *ethical obligations*.

This section summarises the key concepts and models which form the foundation on which this Reference Architecture is built, including the accountability model below:

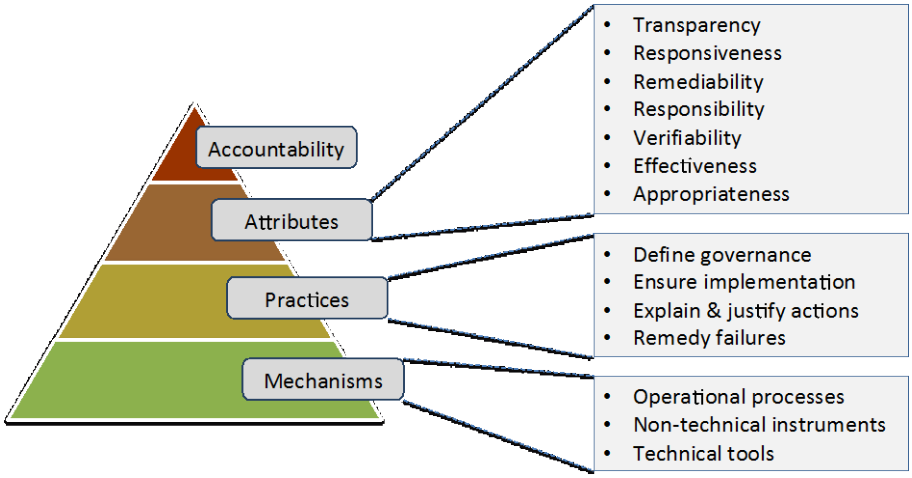


Figure 4: The cloud accountability model.

The context of our work is the cloud, with the associated ecosystem or customers, providers, auditors and regulators. While we often refer to accountability in the context of data protection, our aim is to design an architecture which is addressing the property of accountability rather than the topic to which it is applied (e.g. accountability for data protection or accountability for service availability).

1.1 Fundamental Concepts

Accountability in the context of handling personal and business confidential information 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. The perceived lack of transparency and control over data governance, inherent in complex cloud service provision chains, makes accountability a key market enabler which can help overcome barriers to cloud service adoption. Still, providing accountability both legally and technically in the cloud has proved to be very challenging.

In the A4Cloud project we propose a co-designed approach for accountability that combines a range of technological enhancements with legal, regulatory and governance mechanisms to 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.

Although the goal behind the A4Cloud Reference Architecture (the "RA" hereafter) is to propose a blueprint for end-to-end accountability across the entire cloud service provisioning chain, the starting point for a great many of the concepts and mechanisms discussed focus on making a single organisation accountable. The rationale is that the problem of creating accountable cloud provisioning chains becomes much more tractable if the actors chained together are accountable. Therefore, we begin by defining what it means for an organisation to be accountable. In this context, the A4Cloud project has developed a definition of "Accountability for Data Stewardship in the Cloud" and a corresponding model of how various elements of accountability can be combined to create a roadmap for accountability [1].

As illustrated in Figure 4, this A4Cloud accountability model consists of:

- **Accountability attributes:** central elements of accountability (i.e. the conceptual basis, and related taxonomic analysis of accountability for data stewardship in the cloud). These are transparency, responsiveness, remediability, responsibility, verifiability, effectiveness and appropriateness.
- **Accountability practices:** emergent behaviour characterising accountable organisations (that is, how organisations can incorporate accountability into their business practices). 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.
- **Accountability mechanisms:** operational processes, non-technical mechanisms and technical tools that support accountability practices. Operational processes operate at the organisational business process level, by extending existing processes like auditing and risk assessment to support accountability practices. Non-technical mechanisms consist of accountability-reinforcing mechanisms that are predominantly non-technical, such as contracts, policies, codes of conduct, and various legal safeguards and deterrents. Finally, technical tools comprise the various software systems and components an organisation may use to carry out various accountability-related operations. We may further classify the accountability mechanisms into three categories:
    1. Innovative mechanisms designed and built for purpose by A4Cloud (i.e. *"things we build"*).
    2. External mechanisms which are imported/utilised by A4Cloud mechanisms (i.e. *"things we import"*).
    3. External mechanisms with which A4Cloud mechanisms will co-exist (i.e. *"things we interface with"*).

This A4Cloud accountability model aims to model accountability at different levels of abstraction, from the abstract to the operational, and thereby it elucidates how accountability mechanisms support accountability.

Next we discuss several key concepts related to accountability, which are necessary to explain as background to the rest of this document. According to [1], *accountability 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.*

A core element of the concept of accountability is the "account". Within an accountable system, the "account" can be seen as an explanation or demonstration of the system's behaviour, norms or compliance. We identify three types of "account": proactive account, account of legitimate event(s) and account of incident(s) (see section 3.5 for details). The description of an "account"-related event provides answers to the six "reporters' questions":

- *Who*: identifies actors involved in the described event.
- *What*: describes what the account is about.

- *Where*: describes where the event related to the account occurs (not only physical location).
- *When*: depicts when the described event occurs.
- *Why*: presents why the event happened (to respect policies/obligations for instance).
- *How*: illustrates the used means (logs, encryption, etc.) for the described event.

An "account" also comes with evidence, when possible, associated with these different answers and means for remediation if adequate (the case of an account on an incident, for instance).

In the remainder of this document the core concepts of the accountability model (as summarised in Figure 4) will be utilised and explained further. In particular:

- The core *accountability attributes* (namely, transparency, responsiveness, remediability, responsibility, verifiability, effectiveness and appropriateness) will be related to the accountability metrics in section 4.6. Indeed, metrics constitute an instrument for verifying the compliance of non-functional requirements. Therefore, metrics offer a means to support accountability by privacy and security governance that is in use.

- The *accountability practices* are discussed further in section 4.1, where different notions of account and their properties are presented. Two main types of account are highlighted: evidence about compliance and data breach.

- The *accountability mechanisms* are detailed in section 2.4. In this section, it is explained how high-level goals need to be first decomposed into accountability artifacts and then recomposed to provide assurance and accounts. High-level goals express the privacy and security requirements as well as the laws and regulations that apply in a given context. Accountability artifacts (as discussed further in section 2.5) represent various accountability-related information (such as obligations, evidence records and notification reports).

1.2 [DETAILS] The Role of Standards

The information presented in this section represents details which may only be required if seeking an in-depth understanding of the Cloud Accountability Reference Architecture.

There are many ways to classify standards. For example, in the A-5 work-package (WP) of this project, we notably distinguish *real* standards, from *technical specifications* and *best practices*. In the C-3 work-package of this project, we make another type distinction regarding the scope of standards, based on the four categories of standards defined in CEN-CENELEC[2]. We will reuse this classification to structure the discussion of this section. If we restrict ourselves to the IT domain, these four categories can be expressed as follows:

1. **Fundamental standards** - *which concern terminology, conventions, signs and symbols, etc.*;
2. **Organisation standards** - *which describe the functions and relationships of a company, as well as elements such as quality management and assurance, maintenance, value analysis, project or system management*, *etc.*
3. **Specification standards** - *which define characteristics of a product or a service, such as interfaces (APIs), data formats, communication protocols and other interoperability features, etc.*;
4. **Test methods and analysis standards** - *which measure characteristics of a system, describing processes and reference data for analysis*.

In the following paragraphs we examine the role and value of each category of standards as a driver for accountability for organisations.

1.2.1 Fundamental Standards

Fundamental standards are like the foundation of a building; they are needed to create solid constructions. They play a role in setting the terminology and concepts that are used by organisations implementing IT systems and they influence other types of standards. From a strategic point of view, it

[2] http://www.cencenelec.eu/research/innovation/standardstypes/Pages/default.aspx

is therefore important to include accountability as a crosscutting concept in fundamental cloud standards where relevant and possible. So far, most of the standardisation initiatives in work-package A-5 has precisely been directed at putting accountability into core standards (see [2] for details).

1.2.2 Organisational Standards

Organisational standards and specifications standards form a complementary pair. In a simplified view, we can argue that organisational standards are useful for structuring the internal processes of an organisation in order to best take accountability practices into account. By contrast, we can also argue that specification standards, by promoting interoperability, enable accountability across the provisioning chain with external entities. We will first discuss the role of organisational standards.

Organisational standards are not strictly necessary to enable accountability practices within an organisation. In theory, this goal can be achieved by applying best practices that have been developed internally. Such practices could notably be inspired by the A4Cloud conceptual framework [1]. This approach has some important drawbacks however. First, it makes it complex for external entities to evaluate the quality of the accountability practices implemented by the organisation. Second, it makes comparison between organisations largely impossible, since each organisation will be using its own logic and criteria. Standardised approaches solve these two problems by structuring practices in a way that is recognised not only within an organisation but also across the whole industry. In addition, such standards can be used as a foundation to build certification schemes, with independent third-party auditors, with the benefit of recognition and enhanced trust. This could create a market for "accountability" certification, much like existing information security management system (ISMS) certification today.

There are essentially two competing approaches to embed accountability into organisational standards:

1. Take existing standards in security, governance and compliance, identify their gaps regarding accountability and extend them if needed to cover these gaps.
2. Build a new "accountability management standard", mirroring ISO 27001 for security for example.

Both approaches have advantages and drawbacks.

Taking an existing organisational standard and extending it to cover accountability practices allows organisations to re-use a framework they already know. This normally minimises the cost of "adding accountability" to current practices, which in turn facilitates adoption of accountability practices. The Cloud Control Matrix[3] (CCM) is an example of an organisational cloud control framework that uses this attractive approach: all CCM controls reference back to existing equivalent controls in other frameworks in which they exist (in other words, to ISO/IEC 27001, PCI-DSS, ISACA COBIT, NIST, etc.). Using this approach for accountability means however that accountability is "added" to current practices and is not the backbone of the organisational practices. Building a real accountability organisational standard from scratch would allow describing governance, risk and compliance processes that would be structured around accountability. Building such a standard with industry consensus is however a huge task in itself.

1.2.3 Specifications Standards

Specification standards allow accountability to be expressed and transferred along the provisioning chain, by promoting common metrics, common semantics and common data formats. This ultimately leads to automation of accountability interactions, in turn bringing cost reduction, which makes the value proposition of accountability more attractive. These points are extensively discussed in the project report on interoperability [3].

1.2.4 Test Methods and Analysis Standards

This last category can be exemplified through software testing standards such as [4], but is less relevant to our work on accountability, so we will not discuss it further.

[3] https://cloudsecurityalliance.org/research/ccm/

2 Accountability in the Cloud

This section considers accountability right across cloud service provision chains. In section 2.1, we examine and name the various roles of cloud actors which are either accountors (that should provide accounts) or accountees (who would be requesting and receiving accounts). The cloud operating model poses a number of challenges to achieve end-to-end accountability, which is the focus of sections 2.3 and 2.5. In section 2.4, we identify the accountability information which is exchanged across the service provisioning chain, and start populating the first block of the Accountability Reference Framework diagram (shown in Figure 5 below).

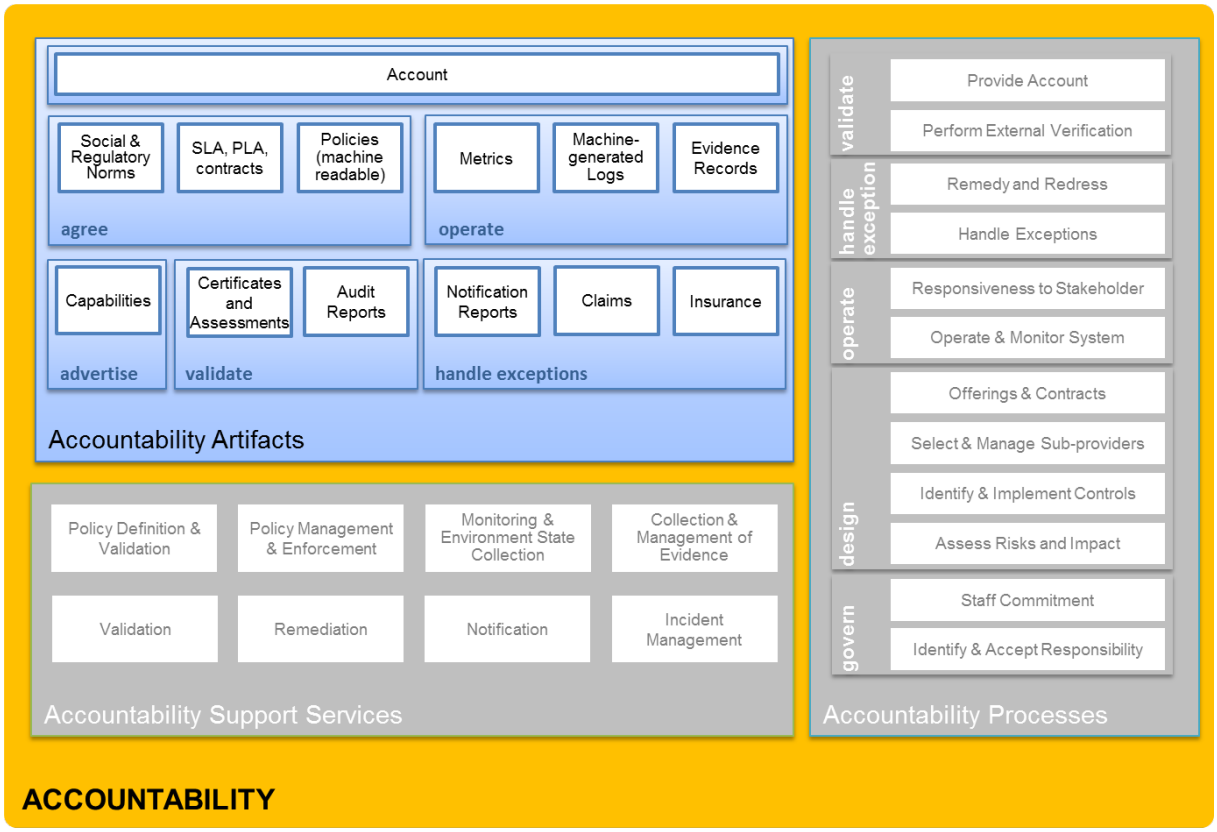


Figure 5: The accountability reference framework - artifacts.

2.1 Actors and Roles

A key challenge when reasoning about accountability in a cloud context is the adoption of a common vocabulary for expressing in a full and consistent way elements coming both from the world of technology and from the domain of data protection. The need for a common vocabulary is particularly relevant for the definition of actors and roles in the A4Cloud Reference Architecture (RA).

The NIST Cloud Computing Reference Architecture [5] defines five major actors:

- *Cloud Consumer*: "A person or organisation that maintains a business relationship with, and uses service from, cloud providers."
- *Cloud Provider*: "A person, organisation, or entity responsible for making a service available to interested parties."
- *Cloud Auditor*: "A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation."
- *Cloud Carrier*: "An intermediary that provides connectivity and transport of cloud services from cloud providers to 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."

Although these five roles are sufficient for representing the vast majority of interactions involved in a cloud service provision and procurement context, they do not effectively capture all the elements necessary to reason about accountability. Specifically, as it is, the NIST model cannot capture the following two roles:

- *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.

In the interest of maintaining maximum compatibility and alignment with the NIST model which appears to be well understood amongst cloud stakeholders, we chose to extend it to cover these roles and support accountability, as follows[4]:

1) **Cloud Subject**: An entity whose data is processed by a cloud provider, either directly or indirectly. When necessary, we may further distinguish between:
   a) Individual Cloud Subject, when the entity refers to a person.
   b) Organisational 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 between:
   a) Individual Cloud Customer, when the entity refers to a person.
   b) Organisational 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.

2.2 [DETAILS] Actors and Roles

The information presented in this section represents details which may only be required if seeking an in-depth understanding of the Cloud Accountability Reference Architecture.

The roles that we introduced (as an extension of the NIST model) share similarities and articulate differences with the cloud computing roles defined in the NIST model in the following way:

- We introduce a new role (Cloud Subject) to designate an entity that owns data (or in the case of personal data, that is the data subject i.e. identifiable by that 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 aligned with the NIST definition (as a synonym of cloud consumer) but we further introduce a distinction between individual cloud customers and organisational cloud customers.
- The roles of cloud provider and cloud broker are adopted without modification from the definition provided by NIST.

[4] For an extended discussion please refer to the A4Cloud Conceptual Framework document [1].

- The role of cloud auditor is based on the definition provided by NIST but was altered to better reflect the goals of accountability, by additionally referencing data protection as well as regulatory and 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 internet service provider). In the case where a cloud carrier takes a stronger role in terms of data stewardship, or if the routing of data traffic matters, we may consider it as a cloud provider instead without loss of generality.

Even in its extended form, however, the cloud role classification alone cannot provide all the information necessary to fully characterise an actor. For example, a cloud provider can be either a data controller, data co-controller, or a data processor, with fundamentally different responsibilities in each case. For that reason, the proposed model for fully specifying an actor's role in the A4Cloud RA is to provide both the (extended) cloud and the data protection (95/46/EC and 2002/58/EC) role classifications. Table 1 below presents all the possible combinations of cloud computing and data protection role classifications identified in the RA. In conclusion, to fully characterise an actor in the RA, and documents produced by the A4Cloud project in general, the proposed nomenclature combining cloud and data protection roles, as presented in Table 1, should be used.

Extended NIST cloud roles	Data protection roles
Cloud subject	Data subject
Cloud customer	Data (co-)controller[5] or Data processor
Cloud provider	Data processor or Data (co-)controller
Cloud carrier	Data processor or Data (co-)controller (unlikely) or Not applicable.
Cloud broker	Data processor or Data (co-)controller
Cloud auditor	(Not Applicable)
Cloud supervisory authority	Supervisory authority (DPA or NRA)
(Not Applicable)	Third party
(Not Applicable)	Recipient

Table 1: Cloud reference architecture roles.

2.3 Challenges in Implementing Accountability in the Cloud

Cloud computing describes a model for enabling ubiquitous, 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 [6]. Its key characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity, multi-tenancy (of users and/or applications) and measured service. Cloud computing can be provided via different service models, such as *Software-as-a-Service* (SaaS), *Platform-as-a-Service* (PaaS) and *Infrastructure-as-a-Service* (IaaS), as well as deployment models such as *private, hybrid* and *public* cloud [6].

[5] By data (co-)controller, we designate both the data controller and the data co-controller roles.

A major benefit of cloud computing is that it enables the flexible composition of powerful applications by chaining together functions provided by different cloud services and providers. For example, end-user-facing cloud applications may be composed from different service components packaged as SaaS offerings, themselves utilising cloud resources provided by different IaaS providers. Furthermore, the use of standard interfaces and technologies means that cloud services[6] along the service provisioning chain may be substituted with others of similar specification without radically altering the way the application is composed.

An implication of this model however is that separate, independent entities assume control, ownership and responsibility for different parts of the service provision chain, the latter constituting separate domains of control. This is illustrated in Figure 6 below, which presents a typical cloud service provisioning chain. Here, a cloud service provider is operating a datacentre to provide a public IaaS cloud offering. Numerous tenants utilise the cloud resources made available to provide applications to the general public in the SaaS model. Each tenant's virtual environment is isolated from all others' by means of the IaaS provider's virtualisation and management infrastructure. Finally, customers access tenant applications over the public Internet to support various business functions.

Clearly, different parts of this provisioning chain belong to different control domains. The IaaS cloud operator has administrative control (and responsibility) over the IaaS support infrastructure. This is indicated in the figure by the area marked by the red dotted line. Employees of the cloud operator may need to access privileged administrative interfaces to manage parts of the IaaS support infrastructure (for example to apply security patches). Naturally, access to those privileged interfaces will only be given to a select, vetted and authorised subset of the IaaS operator's staff and will never extend to outside its area of control due to their potential for catastrophic misuse.

Similarly, each of the IaaS tenants only controls the virtual environment made available to them, such as the green or blue areas in the diagram. IaaS tenants have privileged access to configuration and management controls of their SaaS applications which they will not make available to entities outside their own domains for security, liability or business confidentiality reasons.

Finally, an application user may be responsible for the handling of data processed by tenant applications as part of some business function. Such a user, especially if they are processing regulated data, may configure controls (such as at-rest encryption) to prevent upstream providers (e.g. the SaaS or IaaS provider in this example) from having non-authorised access to the raw data.

[6] This is especially common for services operating at the IaaS layer, as the functions supported by different vendors at this layer are generally uniform.

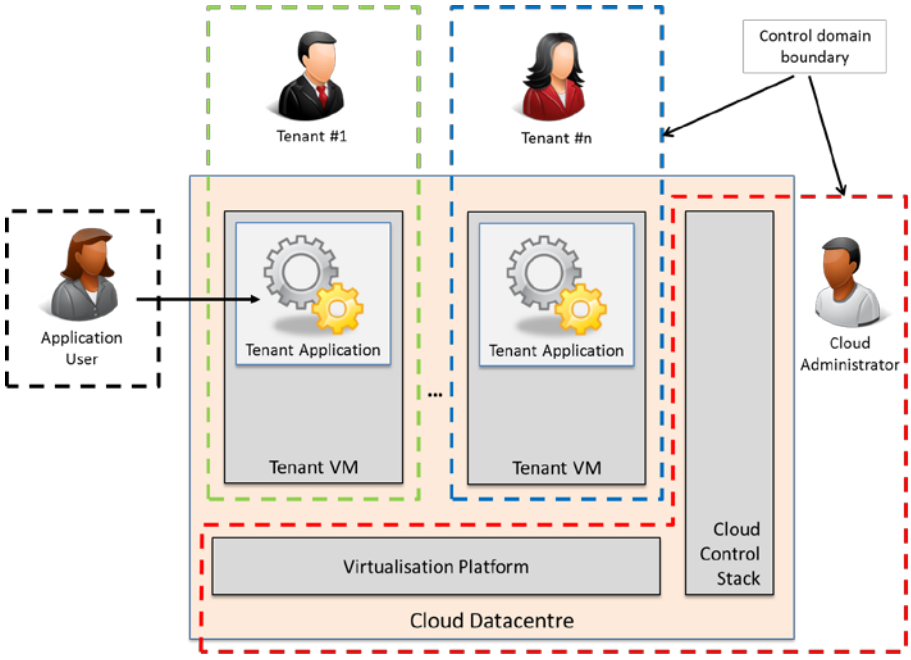


Figure 6: Separate domains of control in cloud service provisioning chains.

Based on the fundamental accountability practices identified in the A4Cloud conceptual model of accountability and discussed earlier in the text, being accountable largely means for an organisation to implement the controls appropriate for the service offered, demonstrate that obligations stemming from policies and regulations are met, and handle exceptions appropriately, remedying failures when applicable.

Even in the relatively simple example of a cloud service provisioning chain illustrated earlier, the challenges involved with achieving accountability end-to-end, across the entire chain, are evident. Since every part of the chain is separated by technical and organisational boundaries between domains, it is hard for any actor to establish whether the processes and operations executed beyond its own domain are according to the agreed rules and obligations. Thus, even if a number of actors have individually implemented accountability-supporting mechanisms inside their own domains (e.g. by implementing the accountability governance process described in section 3) there are no obvious means for accountability to be extended beyond the various domain boundaries to cover the entire provisioning chain.

The A4Cloud RA was developed to provide a method to tackle these challenges by designing mechanisms to support accountability both within an organisation and across cloud service provision chains. The accountability process described in section 3 focuses on the former task while the rest of this section addresses the latter. More specifically, the types of information artifact that need to flow across the provisioning chain to support accountability are identified. Next, a high-level view of the service-oriented approach for accountability in the cloud promoted by the RA is presented.

2.4 Flow of Accountability Information

As discussed in the previous section, control domains may be formed due to a combination of architectural, technical, organisational and economic reasons. A pragmatic approach to extending accountability beyond domain boundaries must reflect the way that clouds and cloud services are architected and operated, and thus focus on enabling the various domains to exchange the information necessary to establish, evaluate and exercise accountability while maintaining their structural separation.

At the highest level, the exchange of accountability-supporting information between two accountable[7] actors[8] in the cloud provisioning chain may be viewed as supporting one of two purposes: the communication of the service consumer's *objectives* to the service provider as they pertain to the handling of data as part of the service provided and, in response, the provision of *assurance* that those objectives are appropriately met by the provider to the consumer. Figure 7 below illustrates this concept.

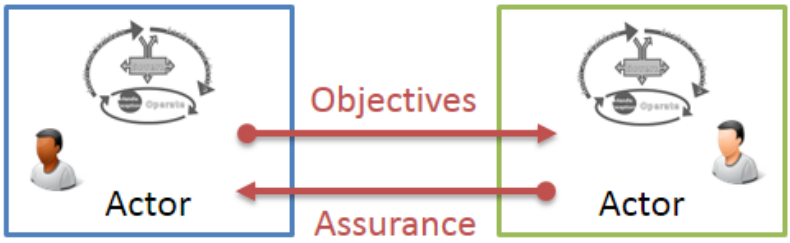


Figure 7: Exchange of accountability-supporting information between two actors.

The communication of objectives and provision of assurance encompass a number of different processes which result in the generation of various types of accountability-related information, called *accountability artifacts*. It is the exchange of these accountability artifacts over organisational boundaries at various phases of the service lifecycle that facilitates the establishment (and continuous evaluation) of accountability between actors. Figure 8 presents the full list of accountability artifacts.

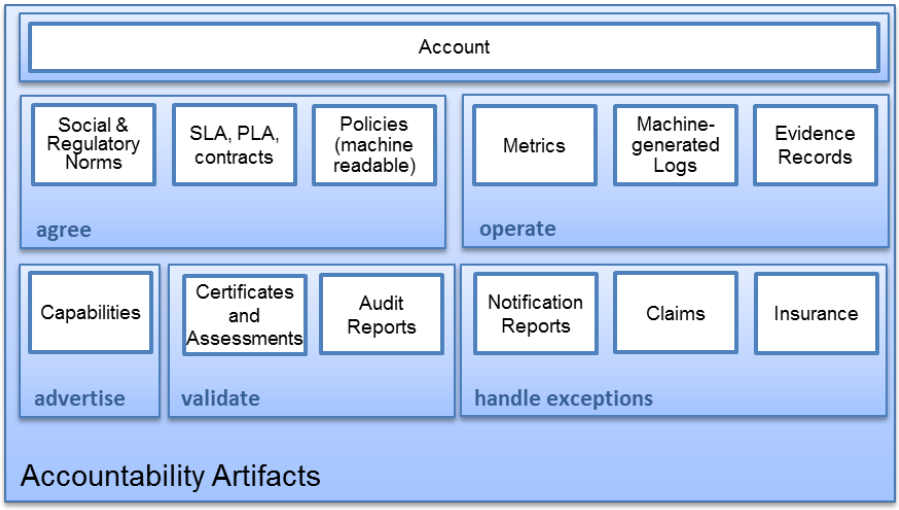


Figure 8: Accountability artifacts.

Objectives describe the high-level goals an organisation wishes to achieve through the use of an IT service. These objectives express the business (i.e. functional) needs of the organisation as a prospective cloud customer and may also contain elicited preferences of the cloud subjects it represents. Before a particular service is procured from the cloud, the prospective cloud customer needs to refine and reformulate these objectives so that they clearly capture its privacy and security requirements for the service. These requirements will encompass any requirements stemming from law and regulation, such as limitations on how personal data are collected and handled. The formulation and compilation of these requirements is part of the "analyse and design" phase of the accountability process lifecycle described in section 3.2, and comprises the necessary first step towards defining the scope for accountability in the sought-after service relationship. These requirements are (implicitly or explicitly) communicated to the selected cloud provider[9] as part of the service procurement process.

[7] An organisation or actor defined as "accountable" hereafter is one that has implemented the accountability process described in section 3.
[8] For the list of actors and roles identified in the RA, see section 2.1.
[9] To avoid unnecessarily complicating this example, we describe a process between two parties, a single cloud customer and a single cloud provider, which results in a straightforward agreement. Obviously, while searching

The cloud provider has requirements of its own, stemming from how its business operates and the constraints it has itself from law and regulation. These requirements inform the provider's service specification, which may be published in various forms ranging from documents outlining "terms and conditions" to machine-readable service description documents. In an accountability-based approach the process of publishing a cloud provider's service specification takes a more prominent role. The cloud provider is expected to *advertise* the capabilities of the service it offers with regards to handling of data, including providing information about what security and privacy controls it offers, what mechanisms it has deployed internally to preserve the security and privacy characteristics of the data as well as any certifications or other documents supporting these assertions. The advertisement of these **capabilities** comprises the first accountability artifact to be produced, which supports the service procurement phase between a customer and a provider of cloud services.

Cloud providers are, like all organisations, required to comply with applicable laws and regulations. Accountable cloud providers additionally commit to moral obligations dictating responsible behaviour. Most, but not all, of these obligations can be, and to the extent possible should be, documented and provided to the cloud customers, under the form of the **social and regulatory norms** artifact.

Typically, if the procurement process deems that the cloud customer's requirements are compatible to the cloud provider's service description (capabilities), a contract is formed between the two parties describing the service agreement and responsibilities of each party to the other. Service and Privacy Level Agreements (SLAs and PLAs respectively) are particular forms of such contracts or may be produced to supplement a general contract to more precisely define particular aspects of the service. **Contracts, SLAs and PLAs** collectively comprise the third type of accountability artifact. In an accountability-based approach this step is particularly important because it is where the cloud provider's obligations to the customer are defined and agreed upon with regards to the handling of data.

The agreed obligations at this stage may be expressed in a variety of forms, with natural language being the most common. These obligations need to be translated into specific policies to be enforced by the cloud provider. This necessitates a procedure for the translation of obligations into **machine-readable policies** that can be automatically monitored and enforced so that all handling of data is performed as per the agreed set of obligations. These (enforceable) policies comprise the fourth type of accountability artifact that must be generated. Machine-readable accountability policies may describe operations more verbosely or at a more granular level compared to obligations and their exact form may depend on the architecture and implementation specifics of the service provided.

During the operation of the cloud service, various elements of it will access, process or otherwise handle personal data at some capacity. While regular operations may be expected to handle the data as prescribed by the relevant policies, an accountability-based approach requires the explicit provision of evidence to demonstrate compliance and meeting of obligations. Furthermore, information on the internal workings of the service, such as machine-generated logs, may need to be provided for the purposes of auditing or to support transparency reports. Both **machine-generated logs** and **evidence records** are thus important accountability artifacts that need to be generated and exchanged between different actors[10]. In addition, as discussed in section 4.2, the evidence collection process drives the development of the "account", which is the principal means for supporting accountability at various phases of the accountability governance lifecycle in its own right.

While logs and evidence provide information about discrete actions and events that took place at specific instances during the operation of the service, the provider must also demonstrate how well it is meeting various accountability-related criteria during the continuous operation of the service, as these are determined by its stated obligations. The assessment of a provider's performance with

---

the market for the most appropriate service offering, the cloud customer may engage with multiple providers in parallel, expressing its requirements to each of them and evaluating all responses before selecting one. Additionally, it may engage in negotiation of terms, which will imply a number of out-of-band iterations before agreement is reached. These actions do not affect the ultimate outcome of this process, which is the acceptance of agreed obligations by the provider.

[10] Although in many cases evidence may include machine-generated logs, they can have different uses as well as different requirements for creation and handling. As such we consider them as two distinct classes of artifacts.

respect to such criteria is performed through the measurement of service-specific subjective and objective metrics over defined periods of time. The provision of **metrics** to enable the evaluation of how well a provider meets various accountability-related criteria thus comprises another important accountability artifact.

If during service provision an incident occurs or otherwise a failure to meet the agreed obligations is detected, the cloud provider must notify the affected parties, take steps to remedy the problem, and potentially offer redress. Thus, the construction of the **notification report** comprises an essential accountability artifact, containing besides a description of the incident, information on corrective actions or the proper remedial steps that have been taken.

When incidents occur or policy violations are detected, accountable service providers are expected to take steps to remedy their effects, and where appropriate offer redress. Affected parties must be given a mechanism to formulate **claims** in the form of artifacts and transmit them to the service provider for evaluation and processing in the context of the remediation and redress mechanisms.

There may be cases where remediation and redress cannot be fully handled by the particular service provider, either because the necessary process is such that it needs to be handled by third parties or because the liability involved is such that the provider cannot cover it on their own. In cases like these insurance can be a vital instrument to manage risk and offer additional assurance, even if it is not a compulsory requirement as it is in many industries and activities. **Insurance** is therefore another artifact that can be provided to establish and evaluate the accountability of a particular actor.

It is also important for the provider to demonstrate global compliance to best practice standards. This is typically achieved through an auditing process, which usually involves external auditors. The auditors produce detailed **audit reports** which are mostly used internally. The auditors also deliver more concise, summary-level **assessments** of the performance of the provider. The provider may also elect to be **certified** (or attested) against formal criteria defined in e.g. Cloud Security Alliance (CSA) Star Certification or Attestation [7]. These documents have historically been issued as paper reports, but are increasingly delivered as structured electronic documents protected against tampering.

Last but not least, the provider creates **accounts** to report on the state of what it is accountable for to stakeholders. In the case of interactions between the regulator and the data controller during an investigation, multiple accounts are created at the data controller level. Some accounts are oral ones (e.g. meetings with a data protection authority (DPA)) and others are written ones (e.g. document provision to the DPA or response to an investigation questionnaire). In cases of written accounts, they are produced by various teams (e.g. operations, public policy, security, engineering, advertising, platform etc.) and these are then aggregated by one senior (usually legal) officer to ensure that there are no inconsistencies between them and that all queries have been answered. These different accounts are then passed on to the DPA. The latter may come back with queries or requests for clarifications which are initially sent to the legal officer of the data controller who then passes it on to the relevant team who actions it.

In general, accounts can be in oral or written form, provided according to a schedule, on request or to answer specific questions, and are principally provided to customers, auditors, and regulators, at various phases of the lifecycle. Sections 4.1 to 4.5 present further details and an extensive analysis of the account.

Table 2 provides a summary of the various types of accountability artifacts discussed.

Accountability Artifact	Brief description
Capabilities	Document containing a description of the service in terms of the capabilities and controls it makes available to its user. The document may be presented in a machine-readable form to enable easier processing by software systems for analysis and comparison of service offerings.
Social and regulatory norms	Document(s) enumerating the legal and regulatory obligations and socially acceptable behaviour imposed on each party according to the

Accountability Artifact	Brief description
	business domain and service relationship in which they engage, represented in a human-readable form. Social norms might only be discussed rather than being clearly specified in documents; they are nonetheless imposed on each party.
SLA, PLA, Contract	Document(s) enumerating the binding contractual and normative obligations of each party engaging in a service relationship, represented in a human-readable (natural language) form. In most cases, they are either negotiated by the parties, or defined by one party and accepted by the other. They may also reference binding legal obligations.
Machine-readable policy	Document or set of documents expressing the obligations of a service provider to a service consumer with regards to data handling, in machine-readable form for automated processing.
Metrics	Measurements of various service-specific objective and subjective performance characteristics over defined periods of time.
Machine-generated logs	Machine- or human-readable objects, which are collected from various components of the cloud provider infrastructure (such as the network, hardware, the host operating system, hypervisor, virtual machines and cloud management systems, applications, etc.), detailing the actions and events that occurred during the execution of a service.
Evidence record	Structured information object which aggregates information from logs, documents and other sources with other metadata to demonstrate the occurrence of particular actions or events, in a provable and tamper-evident manner.
Notification report	Document or message meant to alert affected parties on the occurrence of an incident. It may contain relevant information on the incident, along with any potential corrective actions to be undertaken.
Claims	Document(s) or message(s) in which a party makes claims in the context of remediation and redress mechanisms available in case of discontinuity or breach in the service.
Insurance	Document which attests that the holder will be financially compensated if specific incidents or circumstances occur, which may be used to provide additional assurance that the holder has managed risk and will be in a position to honour its obligations in those cases.
Assessments and Certificates	Document(s) which attest to the assessment of compliance to good practice (e.g. performed by an external auditor) or to the certification or attestation against a formalised criteria (e.g. CSA Star Certification [37])
Audit report	Document which contains evidence records and related objects (i.e. logs, policies) obtained and compiled using a specific methodology to demonstrate compliance.
Account	Report or description which reports what happened, what has happened, or what might happen. An account generally addresses who, what, where, when and why. It may also include measures taken to address risks or to remedy prior failures.

Table 2: Accountability artifacts.

2.5 Artifacts across the Cloud Provisioning Chain

Our report on the Cloud Accountability Conceptual Framework [1] describes several cloud scenarios that are used as a basis for discussion. It is not infrequent to see provisioning chains where a single service offering depends on several SaaS, PaaS and IaaS providers, with a mix of small and large IT organisations. From the point of view of the cloud customer, this provisioning chain should behave as a single, coherent service, seamlessly integrated to the point of being an invisible integration.

The exchange of the accountability artifacts, described in section 2.4, at various phases of the service lifecycle enables the establishment and continuous evaluation of accountability between any two accountable cloud actors directly engaged in a service relationship. This model extends to cover cloud

service provisioning chains of arbitrary length and branching complexity, each actor exchanging accountability artifacts with its neighbours. Figure 9 illustrates how the process of exchanging accountability artifacts between pairs of actors in the provisioning chain can lead to accountability for the agreed context across the entirety of a given cloud service provisioning chain.

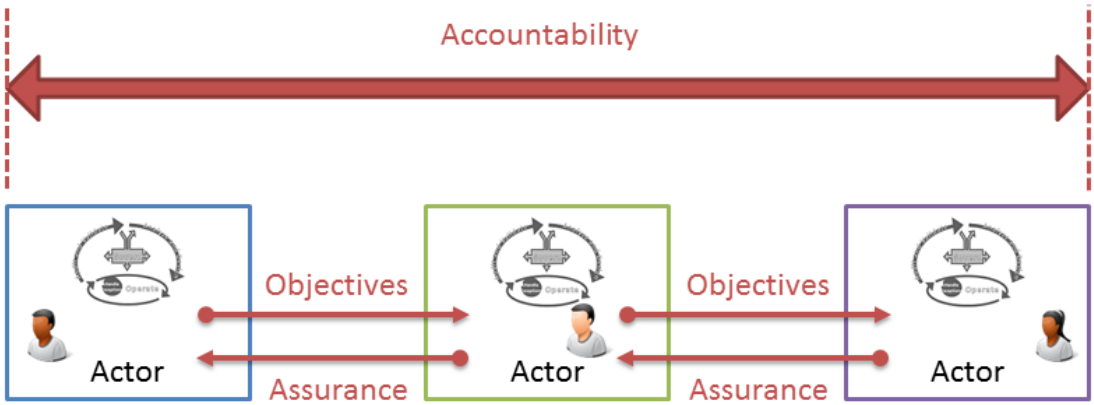


Figure 9: A model for end-to-end accountability in cloud service provisioning chains.

This flow of information is not a simple relay, store-and-forward structure. Artifacts are seldom transmitted unchanged across the provisioning chain. At each stage, artifacts are transformed based on the distribution of roles of each actor and the distribution of data processing functions across the provisioning chain.

To illustrate this point for artifacts flowing downstream (cf. objectives in Figure 9), we can take as an example the case of policies which specify limitations on where a data object classified as personal data can be stored and processed. These policies can be initially associated with the object instance as metadata, stored in a policy-aware object-oriented database, and processed by a policy-aware application. However, down the provisioning chain, a SaaS provider may elect to use a third party IaaS provider for the deployment of its application. In this case, the policies associated with all the personal data instances being processed will need to be aggregated into a policy which relates to the SaaS-IaaS interface, e.g. virtual machines and storage. This aggregated policy will specify the allowable location for servers and disk farms. Alternative models can be used in this case, such as a dynamic distribution of the processing jobs based on the policies associated with the personal data (matching data policies to IaaS capabilities), or a static selection of locations which comply with all personal data location policies the application will ever process (using static policies). This simple example demonstrates that the adoption of interoperability standards covering the specification and exchange of artifacts, which is in itself quite a complex and challenging task, is not enough. In order to automate the propagation of policies, the industry will need to converge on interoperable machine-readable functional descriptions which are suitable for automated reasoning. These are clearly topics of future research and effort.

The situation is similar for artifacts which are being exchanged upstream (cf. assurance in Figure 9), such as notification reports. As illustration, we can take as an example an IaaS provider which experiences a severe disk crash, leading to the temporary unavailability of data, until the faulty hardware is replaced and the data restored. Information on this outage is certainly relevant for the users of the affected services. But the question of *which* cloud subjects need to be notified about the incident depends on whether they are affected by the outage or not. This can only be determined based on mapping the distribution of the cloud subject data and processing onto the infrastructure. Furthermore, the data in the notification report will need to be modified to refer to the cloud subject data, as the cloud subject has no knowledge of storage volumes or virtual machines.

In current practice, the transformation of artifacts along the provisioning chain is performed by manual or static (hard-coded) processes.

3 Implementing Accountability

Good governance is a condition *sine qua non* to be accountable, and accountability must be a part of the DNA of the organisation. In section 3.1 we examine the recommendations issued from the data protection domain. In section 3.2 we identify the lifecycle for accountability, which addresses both core organisational processes and service-delivery processes.

In section 3.3 and the following subsections, we identify a control framework structured into functional areas, and then a series of best practices for each phase of the lifecycle. This is captured in the second block of the Accountability Reference Framework diagram (Figure 10).

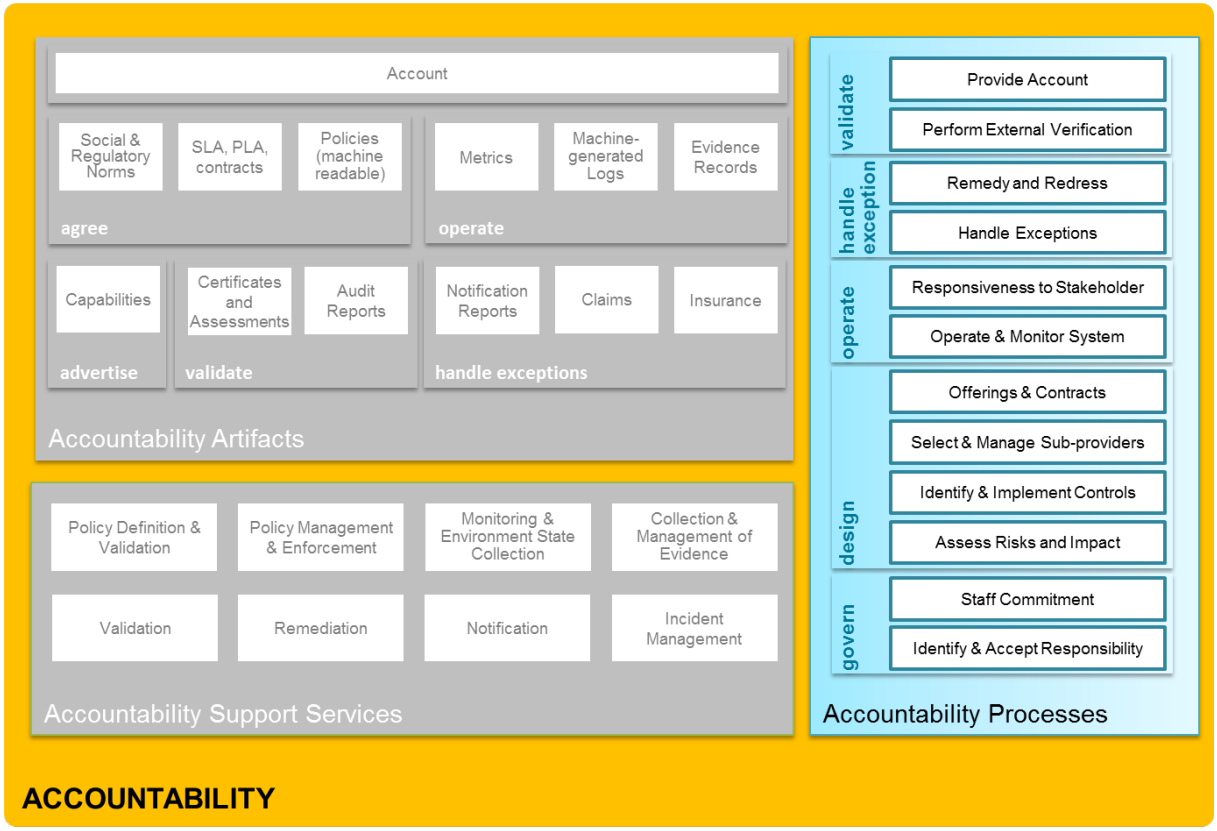


Figure 10: Accountability reference framework - processes.

In section 3.5, we revisit the question of end-to-end accountability, focusing on impact in regards to governance and organisations.

3.1 Introduction to Accountable Organisations

Operating in an accountable manner is not simply a matter of deploying tools to implement technical controls and to report on their behaviour. It actually starts at the very top of the organisation, with the Board of Directors, is embedded in the foundation values of the organisation ("organisational DNA"), and is transmitted through the whole organisation through governance. In the following sections, we will explore the practices required to operate in an accountable manner.

The Accountability for Cloud Conceptual Framework [1] defines an accountable organisation as being *one that takes an accountability-based approach, implying the adoption of the entire set of the accountability practices*. The Conceptual Framework then expands on accountability at an organisational level, focusing on the ways it could be implemented in practice. For the benefit of the reader, these conclusions are listed below:

The Galway project [8] *has defined the central elements that an accountable organisation (in the context of data protection) needs to address as being:*

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 [9]*:*

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 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*
   - *policies relating to: collection, use 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*
   - *risk assessment mechanisms*
   - *training and education*
   - *breach and incident management*
   - *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 proposed EU General Data Protection Regulation (GDPR) [10] *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 Assessments*
- *Prior authorisation/consultation by Data Protection Authorities (DPAs)*
- *Data Protection Officer*
- *If proportional, independent internal or external audits*

While we have adopted a "*focus on the data protection domain and on accountability of organisations rather than individuals*" [1], one of our main concerns is accountability in the context of IT supply chains based on the use of cloud services. End-to-end accountability, which is further analysed in section 3.5, requires all actors of the provisioning chain to be accountable organisations to a certain degree. However, the domain for which these organisations need to be accountable is not necessarily the data protection domain. For example, when an organisation implements a service which is handling sensitive data (in regards to the data protection regulations) through the use of an IaaS cloud service provider, the latter is typically accountable for providing adequate security, and not for implementing an accountability-based data protection program.

It should be noted that, even if the focus as stated above is on organisations, the role of individuals involved is also essential and that accountability must be ensured down to the employee level. Accountable organisations must provide individuals with the necessary tools and procedures to be individually accountable.

In the remainder of this section, we have defined the control objectives and associated measures that should be implemented by an accountable organisation in a manner which remains agnostic to the domain. The recommendations have been identified based on work done for both the data protection

domain, such as CNIL [11], ICO [12], and Nymity [13]. These have been augmented by more general organisational standards, such as COBIT [14] and ISO 27001 [15]. We have also leveraged the HP Security Handbook [16] as well as the professional experience of the authors.

3.2 Lifecycle for Accountability

The Conceptual Framework introduces the Organisational Lifecycle and introduces the Functional Elements of Accountability, which provides the reference model for this discussion.

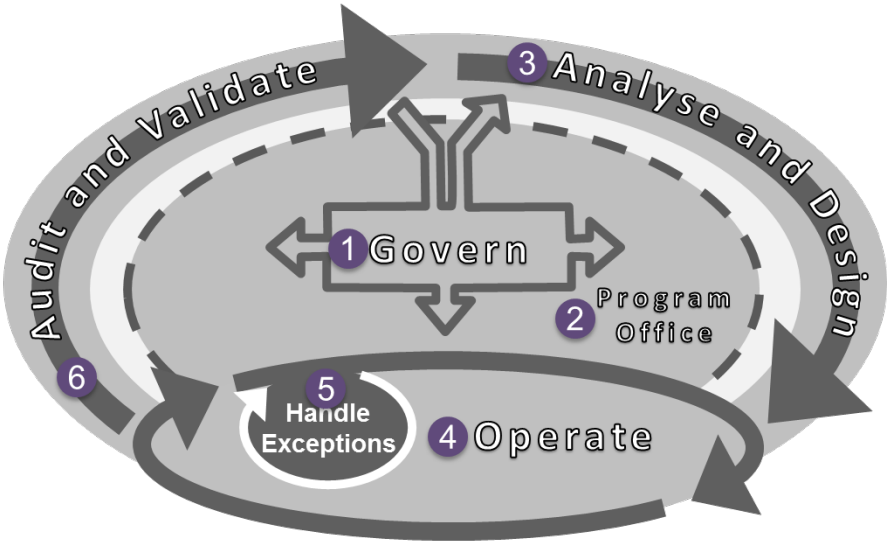


Figure 11: Accountability lifecycle.

This lifecycle (shown in Figure 11) is organised around five phases which provide a structure to the solution development, operation, and maintenance. Specific to the Corporate Accountability scope, we introduce a sixth element, the Program Office, which provides the operational support to the governance body. Note that the first two elements (Govern and Program Office) are strongly associated with organisational accountability, while the three first lifecycle elements (Analyse and Design, Operate, Handle Exceptions) describe the lifecycle for building and operating an "accountable solution". The last element (Audit and Validate) is applicable to both domains, as the assessments can be either focused on the organisation as a whole or on a particular solution or business service.

1. Govern – This corresponds to the executive roles in the organisation establishing and maintaining a framework and supporting management structure and processes, as well as accepting and providing assignment of responsibility, to meet the obligations of the organisation in an accountable manner.

2. Program Office – This is the operational body which supports the governance body in meeting its responsibilities in e.g. drafting guidelines, policies and procedures, defining the operational programs and infrastructure, and providing oversight and support for the implementation of the decisions of the governance body. This program office is typically in charge of both organisational accountability as well of the domain for which the organisation is accountable (e.g. the privacy program office or the security program office); it can either be an organisational or a logical structure.

3. Analyse and Design – This corresponds to the analysis and design phases related to the engineering of a solution. The work performed in this phase clearly separates identification of risks (based on business impact, not just technology), identification of controls, design of control implementation, and implementation of controls through technology and processes.

4. Operate – This corresponds to the operational (production) phase of the solution, and includes all the associated management processes.

5. Handle Exceptions – This set of activities, which could be considered as an integral part of operations, has been singled-out due to its specific nature and high relevance to accountability. It includes all processes for the handling of complaints and breaches related to accountability obligations.

6. Audit and Validate – This corresponds to the assessment of the effectiveness of the controls which have been deployed, the necessary reporting, and paves the way to the tuning (adaptation) of the measures deployed to ensure the obligations are being met.

Section 3.4 describes in more detail the content of each of these phases. More than a general discussion and framing of the scope, we want to provide practical guidelines for implementing accountability. We are providing a series of recommendations which can be used as a checklist. We do not claim this describes a specific methodology but provides a general guideline on integrating accountability within an organisation.

These lists are not comprehensive, and each of the points must be evaluated in regards to the size and structure of the organisation. The full list of recommendations may, in general, not be applicable to smaller groups such as SMEs. We acknowledge there are many common points between the recommendations identified below and the actions identified as required for topics like data protection, business continuity, disaster recovery, information security management, and trustworthy accounting. However our recommendations below are not intended to be a substitute for those lists of actions – an organisation must address all of them in order to have a comprehensive coverage and meet its obligations. The analysis focuses on the processes to be deployed by the accountor rather than those of the accountee.

3.3 Simplified Accountability Control Framework

Our investigation on best practices for accountability has led us to define a simplified control framework, associated with the more detailed measures presented in Section 3.4. In this section, we examine the key control objectives which are associated with operating an accountable organisation.

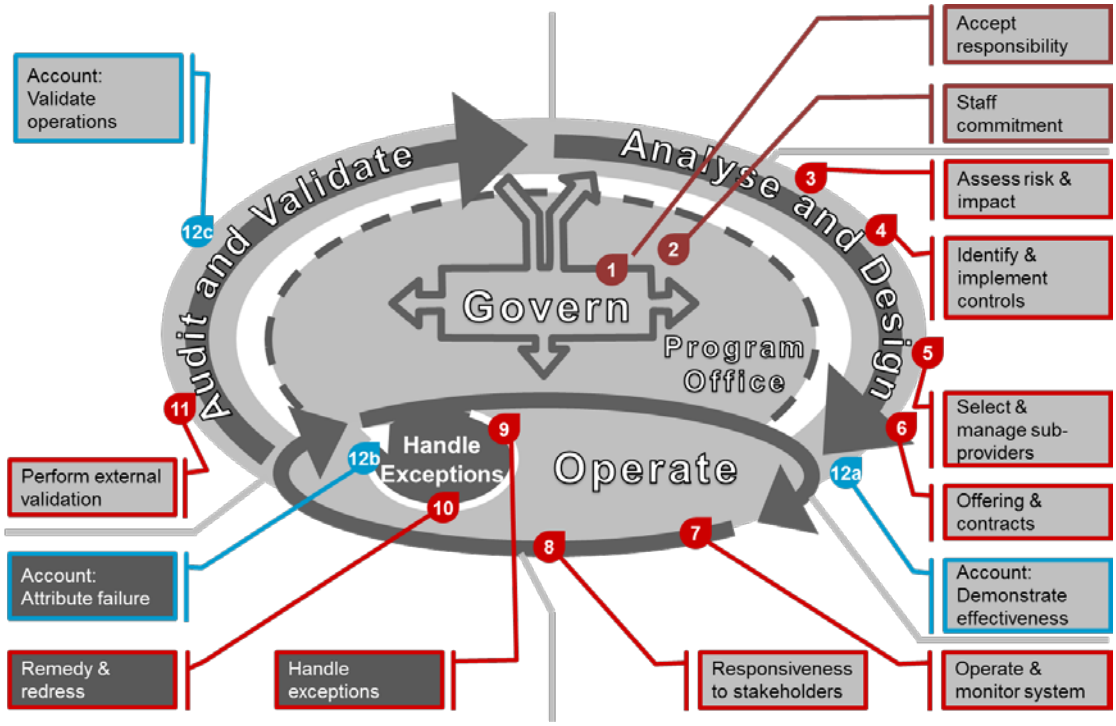


Figure 12: Key processes in the accountability lifecycle.

We have grouped the control objectives according to the main concerns they address. These groups map to the accountability lifecycle according to the phase in which they are primarily addressed. Most are addressed both in the Governance (and associated Program Office) phase of the lifecycle – typically to define the processes that will be used to address the concern in another phase of the lifecycle- and in one of the four phases of the "accountable solution" lifecycle, as shown in Figure 12[11]. In several cases, a process group maps to several areas.

Table 3 provides more details on the concerns corresponding to each of these groups:

Process Group	Description of Concern
(1) Identify and Accept Responsibility	Understand and accept responsibility for fulfilling obligations in an accountable and responsible manner; commitment to accountability.
(2) Staff Commitment	Adopt an accountability-driven culture for the whole organisation; ensure individual commitment to responsibilities
(3) Assess Risks and Impact	Identify and assess risks and impact for the organisation and its service offerings.
(4) Identify and Implement Controls	Mitigate risks and implement controls to ensure continuous compliance with obligations in an accountable and responsible manner.
(5)Select and Manage Sub-providers	Ensure that all third-party services are compliant with relevant obligations and can be properly accounted for.
(6) Offering and Contracts	Define the object of accountability, both in terms of documentation and of commitment to stakeholders. Establish contracts.
(7) Operate and Monitor System	Operate the system as intended and execute the processes to meet obligations.
(8) Responsiveness to Stakeholders	Take into account input from external stakeholders and respond to queries of these stakeholders; enable individual participation
(9) Handle Exceptions	Handle incidents related to obligations for which the organisation is accountable
(10) Remedy and Redress	Take corrective action and/or provide a remedy for any party harmed in case of failure to comply with its governing norms
(11) Perform External Verification	Regularly review the status in regards to accountability and compliance to the obligations; also includes the certification of the organisation.
(12) Provide Account	Provide an account to report what happened, what has happened, or what might happen and to demonstrate accountability.

Table 3: Process groups.

We recognise that there is a significant overlap between the controls we have identified and those listed in widely-accepted control frameworks, such as ISO 27002 [17], COBIT [14], or CSA's CCM [18]. To be accountable, an organisation must start by operating in compliance with a baseline set of practices expected from leading organisations, which is the object of these control frameworks. Accountability cannot be achieved independently, as a separate property; it mandates a baseline set of controls which are required as part of state-of-practice behaviours. We have found that the commonly-adopted control frameworks do not necessarily fully address a number of key behaviours which are at the core of accountability, most notably:

- Behave ethically: while the above control frameworks require operation in compliance with laws and regulations, organisation adopting a culture of accountability will also be guided by a strong set of ethical values. This is not consistently addressed by control frameworks.

- Comply with social norms: accountable organisations must accept the obligation to act as a responsible steward with respect to assets of others. This obligation is not only legally prescribed, but also implied by requirements or promises derived from social norms. Most control frameworks do not make provisions related on this topic.

[11] When a process group maps to several lifecycle phases, we are only showing the one with which it has the strongest ties.

- Perform due diligence: accountable organisations cannot simply transfer responsibilities and liabilities through the chain; the organisation remains accountable no matter where the information is processed. The acceptable level of risk and due diligence are key criteria for the associated liability. Most control frameworks do not model the transfer of responsibilities in this manner.

- Involve stakeholders: accountable organisations are bound to take into account input from external stakeholders and respond to queries of these stakeholders. Furthermore, 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. Most control frameworks cater to handling customer problems, not to the active involvement of stakeholders.

- Inform stakeholders transparently: accountable organisations are required to provide visibility of its governing norms, behaviour and compliance of behaviour to the norms, both in the context of incidents and of normal operations. While all control frameworks address incident management and resolution, most do not require informing stakeholders in a transparent manner, except if required by law.

- Accept liability and cover with insurance: accountable service providers must provide an appropriate remedy to customers in case of failure to achieve agreed service levels. While subject to contractual clauses limiting liability, behaving in an accountable manner requires that the liability be commensurate with expected usage. The associated liability is often beyond the organisation financial capabilities, and must therefore be covered by insurance.

- Explain and demonstrate compliance to stakeholders: the provision of an account to explain and demonstrate compliance to stakeholders is central to the concept of accountability. While most control frameworks mention accountability, they typically only address individual responsibility or keeping track of assets.

The control frameworks are intended to be used as a guide for the implementation of a coherent set of controls for providers and users of IT services. They are often coupled with a certification or attestation scheme, where certificates are delivered by accredited third-parties (e.g. certified auditors) after a detailed audit procedure. The certified organisation can then demonstrate compliance to the provisions of the control framework to third-parties (e.g. its customers or authorities). To achieve this, the provisions of the control framework have to be interpreted, both for the implementation (by the provider) and for the certification (by the auditor). The words which seem to be calling for an accountable behaviour by some, may be understood (and, hence, operationalised) quite differently by practitioners. In fact, one could argue that most of the accountability controls are already addressed in the control frameworks, including on the points above, while observation of the behaviour of certified parties shows the opposite conclusion.

A further discussion on this topic can be found in section 4.8 related to the Accountability Maturity Model.

3.3.1 Identify and Accept Responsibility Control Objectives

Being accountable starts with having an in-depth understanding of, and committing to, obligations derived from law, social norms, agreements, organisational values and ethical obligations. This applies to both the organisation as a whole, e.g. obligations related to the business domain in which the organisation is engaged, and to each offering, e.g. specific obligations associated with the profile contractual clauses of a service offering. The organisational level commitment must be taken by senior and executive management. The corresponding objectives are described in the table below:

Identifier[12]	Control Objective	Lifecycle Phase
1.01	The organisation must understand and document relevant obligations in breadth and in depth, whether from law, social norms, agreements, organisational values and ethical behaviour. Understand the impact of not fulfilling the obligations. Accept responsibility for fulfilling these obligations in an accountable and responsible manner.	1+2 - Governance
1.13	Compliance readiness: liaison to external agencies (domestic and foreign). Ensure the organisation tracks "external criteria" and reporting requirements – use a mix of specialised information services, industry associations, professional networks, specialised conferences, and consultants. Maintain the legally-required documentation.	1+2 - Governance
3.01	Define the accountability object: describe the functionality and associated non-functional requirements of the product or service, inventory the data stored and processed, inventory the obligations for which the organisation will be accountable, inventory the assets related to the functionality and obligations and perform an impact assessment. Keep and update a record of assets and impacts.	3 - Analyse and Design

Table 4: Identify and Accept responsibility control objectives.

3.3.2 Staff Commitment Control Objectives

As highlighted above, the role of individuals involved is also essential and that accountability must be ensured down to the employee level. Accountable organisations must provide individuals with the necessary tools and procedures to be individually accountable. These control objectives correspond to that requirement.

Identifier	Control Objective	Lifecycle Phase
1.05	Ensure a proactive attitude towards the object of accountability across the organisation. For example, if the organisation aims to be accountable for its handling of private and confidential data, the staff must be specifically trained on the topic, and commitment to protecting the privacy and confidentiality of user data must be included as an expected behaviour for all staff members.	1+2 - Governance
1.06	Drive the adoption of an accountability-driven mindset. Ensure that it is integrated with the core values of the organisation (e.g. code of conduct, ethical guidelines, list of values) and committed at the individual level (signoff). Provide appropriate tools, training, processes, and instruments to report on the state of the accountability program (including a set of metrics).	1+2 - Governance

Table 5: Staff commitment control objectives.

3.3.3 Assess Risks and Impact Control Objectives

Understanding risks and assessing their impact is core to the accountability process – there would be no need for accountability if one could provide a total and absolute guarantee that all these obligations are met. These control objectives address the identification and understanding of risks and impact at both the level of the organisation and at the level of the offerings.

[12] The identifier is solely used as a means to easily cross-reference the control objectives in this and other documents. The control objectives may be organised by process group or by lifecycle phase; the identifiers correspond to the latter structure and have not been modified for this document.

Identifier	Control Objective	Lifecycle Phase
1.02	Define the "internal criteria" (e.g. criteria derived from ethics, morals, values, personal targets, professional norms, perceived social role [19]) for the organisation. Understand the risks associated with the operation of the business in regards to the obligations. Define a "risk appetite" used as guidance for operational decisions, taking into account the nature of the obligations. Perform the associated risk and impact assessments.	1+2 - Governance
1.10	Define organisational standards for the analysis processes (e.g. impact assessment, risk assessment) in regards to accountability and obligations, for use in the Analyse and Design phase of the lifecycle.	1+2 - Governance
3.02	Perform a risk analysis and associated impact assessment based on accountability requirements.	3 - Analyse and Design

Table 6: Assess risks and impact control objectives.

3.3.4 Identify and Implement Control Objectives

Once risks and impact are identified, they must be treated adequately, which is the object of these controls. The nature of the controls addressing the needs of the organisation is different from the ones addressing software or service offerings, but both are subjects to what must be transparently reported through the accountability process.

Identifier	Control Objective	Lifecycle Phase
1.03	Treat the organisational risks in an accountable and responsible manner, while keeping the ability to demonstrate due-diligence.	1+2 - Governance
1.04	Ensure the organisation deploys the necessary means for the fulfilment of the obligations, in terms of resources, personnel, funding, authority and executive leadership. Ensure the organisation is aligned on the objectives.	1+2 - Governance
1.07	Ensure that accountability principles and requirements are built in across all relevant organisational processes. Avoid operating the program as a "silo" or an afterthought.	1+2 - Governance
1.12	Maintain a registry of job (function) profiles in relationship with the obligation and identify "sensitive positions", define recruiting criteria and continuous training programs. Ensure legal compliance re. staff.	1+2 - Governance
1.14	Deploy techniques and tools supporting authorisation based on duty segregation. Use tools guaranteeing that all actions are logged and allow the identification of the agent and of the authoriser, within the constraints of the law.	1+2 - Governance
3.03	Define, maintain, and validate risk treatments and associated controls. Ensure continuous monitoring of the state and effectiveness of the risk treatment plan, e.g. with metrics and dashboards.	3 - Analyse and Design

Table 7: Identify & implement control objectives.

3.3.5 Select and Manage Sub-Providers Control Objectives

Using cloud services implies the coordinated involvement of multiple providers. Each of the providers in the provisioning chain carries a share of the responsibility for meeting the obligations which are the objects of accountability. These control objectives address the associated requirements. A coordinated program to manage sub-providers is an essential attribute of managing sub-providers.

Identifier	Control Objective	Lifecycle Phase
1.11	Ensure that all service and provisioning contracts are compliant with relevant obligations, define appropriate standards and practices in regards to engagement with third-parties. Maintain and update a registry of third-party engagements and their relationship with obligations. Ensure 3rd party providers are regularly reviewed and that non-compliance is dealt with.	1+2 - Governance
3.04	Identify assets handled by the 3rd parties, the related obligations and associated accountability requirements. Ensure continuous interoperability of policies, reporting, and incident management with the 3rd party. Identify the certifications and other levels of guarantees that must be offered by the provider. Ensure the proper contractual clauses are in place. Ensure the provider exploits the data only as intended.	3 - Analyse and Design
6.02	Audit third-parties, either directly as provisioned by contract or through the reports they provide. Validate functionality and compliance to obligations, at a frequency based on risks and sensitivity (normally yearly).	6 - Audit and Validate

Table 8: Select & manage sub-Providers control objectives.

3.3.6 Offering and Contracts Control Objectives

The process of accountability requires a clear definition of what is committed to and can be expected by stakeholders. This is the object of contract and service agreements, which can either be generic, or be negotiated on a case-by-case basis (enterprise agreements).

Identifier	Control Objective	Lifecycle Phase
3.05	Fully document the functionality, service levels and implementation of offerings and solutions. Ensure the terms of the contracts reflect what is actually implemented. Obtain executive signoff to ensure a commitment to the stated functionality and levels of service.	3 - Analyse and Design

Table 9: Offering & contracts control objectives.

3.3.7 Operate and Monitor System Control Objectives

This set of control objectives corresponds to the operation of the system, the reporting of metrics and the collection of evidence, as defined in the Analyse and Design phase of the lifecycle, in accordance with what is defined in the service agreement (or contract), and in compliance to the accountability expectations (e.g. ethical behaviour, social norms,…)

Identifier	Control Objective	Lifecycle Phase
4.01	Operate the system as intended.	4 - Operate
4.02	Gather and report on accountability and risk treatment metrics, keep the dashboards updated.	4 - Operate
4.03	Ensure collection and protection of evidence.	4 - Operate
4.05	Continuously monitor the system, the operating environment, and the ecosystem for signs of incident, breach or significant change. Trigger the exception handling processes as required, in case of a detected breach.	4 - Operate

Table 10: Operate and monitor system control objectives.

3.3.8 Responsiveness to Stakeholders Control Objectives

Being accountable requires having a privileged relationship with stakeholders, based on responsiveness and transparency. This is what is addressed by these controls.

Identifier	Control Objective	Lifecycle Phase
4.04	Proactively communicate and timely respond to stakeholders.	4 - Operate
5.01	Receive, handle, track, and respond to complaints and information requests from stakeholders in a timely manner as required by internal policies or legal requirements. Have a FAQ to anticipate the most frequent information requests.	5 - Handling Exceptions
5.02	Create a classification for requests and complaints. Define standard procedures for the handling of requests in each of the classes. Have defined escalation procedures.	5 - Handling Exceptions

Table 11: Responsiveness to stakeholders control objectives.

3.3.9 Handle Exceptions Control Objectives

“Remedying any failure to act properly” is an integral part of accountability. This starts with the need to plan beyond expected discontinuities and anomalies in the operation of services; accountable organisations must have a plan for large-scale issues. This set of control objectives deals with the ability to handle discontinuities in services.

Identifier	Control Objective	Lifecycle Phase
1.08	Ensure the organisation is ready to handle incidents related to obligations for which it is accountable (incident response). Preparedness for handling exceptional events (processes and procedures, allocate responsibility, deploy the staff, define a contingency plan, get retainer for external resources (e.g. forensics expertise), insure against risks, define metrics then track and report performance, test the system based on simulated incidents.	1+2 - Governance
5.03	Log and track the incidents in a secure, time stamped and reliable way.	5 - Handling Exceptions
5.06	Perform a root cause analysis.	5 - Handling Exceptions
5.07	Repair the affected services and restore the business processes based on recovery objectives (eg. tradeoff timeliness vs. completeness, ability to restore in full, …). This could be done in stages to minimise impact to stakeholders.	5 - Handling Exceptions

Table 12: Handle exceptions control objectives.

3.3.10 Remedy and Redress Control Objectives

This set of control objectives caters to the communication with stakeholders once an issue has been identified.

Identifier	Control Objective	Lifecycle Phase
5.04	Notify the stakeholders (affected parties) of the incident, providing remediation actions, as soon as those have been identified.	5 - Handling Exceptions
5.05	Report the incident to authorities when required by law or by the criticality of the incident – including both regulators and law enforcement.	5 - Handling Exceptions

Table 13: Remedy and redress control objectives.

3.3.11 Perform External Verification Control Objectives

This set of control objectives addresses the development of an oversight and review plan that describes how the organisation's program controls will be monitored and assessed and of its execution, both in regards to the organisation as a whole and to the offerings.

Identifier	Control Objective	Lifecycle Phase
1.09	Ensure that the accountability program is regularly reviewed, updated, and documented. Regularly review the status of the organisation in regards to accountability and compliance to the obligations, using internal and external audit.	1+2 - Governance
6.01	Regularly perform internal audits aimed at validating functionality and compliance to obligations, considering both internal and external criteria, at a frequency based on risks and sensitivity (normally yearly).	6 - Audit and Validate
6.03	Ensure that recommendations from previous external audits have been properly considered and dealt with.	6 - Audit and Validate

Table 14: Perform external verification control objectives.

3.3.12 Provide Account Control Objectives

Unique to accountability, this set of control objectives addresses the privileged communication instrument between the accountor and the accountees, and is the means of demonstrating accountability.

Identifier	Control Objective	Lifecycle Phase
3.06	Produce an account reflecting the analysis linking obligations with actual controls must be produced and made available to stakeholders.	3 - Analyse and Design
5.08	Build and distribute an account for the incident, which in particular attributes the failure corresponding to the incident.	5 - Handling Exceptions
6.04	Collect the material and perform the analysis which will allow to prepare updated accounts, to include actual indicators of effectiveness.	6 - Audit and Validate
6.05	Perform external audits as dictated by internal criteria, regulations of each domain of accountability, or customer contractual provisions. Certifications or attestations might be used as effective substitutes for client-directed audits.	6 - Audit and Validate

Table 15: Provide account control objectives.

3.4 [DETAILS] Accountability Best Practices

The information presented in this section represents details which may only be required if seeking an in-depth understanding of the Cloud Accountability Reference Architecture.

In this section, we present a list of measures, under the form of best practices, corresponding to the control objectives listed in Section 3.3 above. This list is organized by lifecycle phase (cf. Section 3.2). These measures are intended to be pragmatic recommendations, and are not uniform in nature, some representing specific objectives to achieve (e.g. understanding relevant obligations), while others are more action-oriented (e.g. Perform a root cause analysis). The list is neither comprehensive nor prescriptive: there are most often alternative ways to fulfil control objectives, the optimal choice depending on context. This list is best suited for large organisations; an alternative approach for smaller entities is proposed in Section 3.5.

3.4.1 Roles and Responsibility of Governance Bodies

In the scope of our analysis, we consider obligations which have to be met by the organisation as a whole and where the responsibility for fulfilling these obligations rests with the board members and executive managers, with some part of it being reflected down to the employees. In this context, being responsible often goes beyond civil responsibility (liability to be called upon to respond to an action at law for an injury caused by a dereliction of duty or a crime) as laws often assign penal sanctions for not meeting obligations and not performing due diligence.

The governance bodies are the owners of the strategic dimension of accountability. In order to fulfil this mission, the board and executive management must:

- Understand relevant obligations in breadth and in depth.
- Understand the consequences of not fulfilling the obligations.
- Accept responsibility for fulfilling these obligations in an accountable and responsible manner – this is applicable not only to the governance body as a whole, but must be an integral part of the mission of each member of the governance body, which must embrace the obligations, ensure support from each (relevant) functional area, and act as champions in the organisation.
- Define the “internal criteria” for the organisation, taking into account internal and external stakeholders’ ideas of what norms and behaviour one should account for.
- Understand the risks associated with the operation of the business in regard to the obligations. Define a “risk appetite” used as guidance for operational decisions, taking into account the nature of the obligations (ethical, social, or industry norm, contractual, regulatory, legal, etc.…). The acceptable level of risk acceptance delegated to the various levels of the organisation will typically increase with the management levels in the organisation.
- Appoint an executive-level owner who will oversee and be accountable for the fulfilment of the obligations. For example, this is typically the Chief Privacy Officer or the Chief Security Officer for (respectively) the data protection domain or the security domain.
- Ensure the proper integration of all responsibilities and actions across the whole organisation. Avoid operating the program as a “silo” or an afterthought.
- Ensure a proactive attitude towards the accountability domain (e.g. data protection) across the organisation.
- Drive the adoption of an accountability-driven mindset. Ensure that this becomes part of the culture, and is integrated with the core values of the organisation (e.g. code of conduct, ethical guidelines, list of values).
- Ensure accountability is properly integrated in all relevant processes (e.g. business management, risk management, compliance management, reporting).
- Ensure that employees are properly trained to understand the concept of accountability and their own obligations.
- Ensure that employees are provided with appropriate tools and processes to fulfil their own part of the accountability obligations.
- Ensure the organisation is ready to respond to discontinuities in compliance to obligations (incident response).
- Ensure the organisation has the adequate processes and attitude to seek, receive, and collect stakeholder comments and respond in a proactive and transparent manner.
- Regularly review the status of the organisation in regards to the compliance to the obligations.

In order to fulfil this mission, depending on the scope, the organisation’s high level management will typically create a Program Office to provide the operational support for the enactment of the governance decisions and more generally support the governance body in meeting its responsibilities. The Program Office will typically report to the executive-level owner. In relationship with this Program Office, the governance body will:

- Define the mission and charter of the Program Office.
- Define the level of authority of the Program Office.
- Ensure the Program Office is provided with the necessary means, in terms of resources, personnel, funding and authority so it can fulfil its mission.

- Support and champion the various policies, programs, processes and other actions identified by the Program Office as necessary to meet the obligations.
- Regularly review the work performed by the Program Office. Use external audits to get an external view on the performance of the Program Office.

3.4.2 The Program Office

The Program Office may be focused on accountability across the organisation, but will more typically be in charge of both the domain (or one of the principal domains) for which the organisation is accountable (e.g. the Privacy Program Office or the Security Program Office) and of accountability. The Program Office can either be an organisational or a logical structure.

In its role to support the governance bodies in fulfilling their responsibilities, the mission of the Program Office can be divided into eight main areas:

- Inventory Obligations, Risk Assessment and Risk Treatment
  - Maintain a registry of all obligations and associated operational standards.
  - Perform risk assessments and identify risks and exposure. This is focused on business and related (accounting) practices.
  - Identify how to treat the risk. The analysis must include cost, timing, alternatives, and comply with the “risk appetite” identified by the Board.
  - Create a rollout plan.
  - Create a set of metrics to report on the state of the accountability program.
  - Investigate best practices and compliance frameworks; consider adoption, attestation or certification based on benefits, costs, and risk.

  This sets the stage to perform due-diligence, which often defines the boundary where the responsibility of the officers of the organisation is engaged. Performing due-diligence is however not enough – it can only be used as defence if it can be demonstrated. The Program Office must be sure that this can be done.

- Company Culture, Practices and Standards
  - Review relevant company codes, operating guidelines, and standards with regard to obligations. This must take a holistic view and deal with all appropriate business functions: sales, marketing, business operations, IT, facility management, workplace solutions, finances, accounting…
  - Draft appropriate changes to these codes.
  - Rollout these changes and ensure effective change of the documentation throughout the organisation.
  - Notify staff of changes through adequate communication programs (awareness).
  - When none exist, foster organisation-level codes and standards creation by or in collaboration with businesses and functions when required for alignment of the internal business processes. Ensure compliance through checklists and metrics used for reviews at different levels.
  - Build templates for analysis (e.g. impact assessment, risk assessment) in regards to accountability and (domain specific) obligations, for use in the Analyse and Design phase of the lifecycle.
  - Define a sign-off process with responsible parties to validate the major milestones in the Organisational Lifecycle for Accountability.

  It is important to adopt the principle that all actions performed be traceable to the person or people performing and authorising it (attributability). This is to be used primarily for root-cause analysis, continuous improvement and individual accountability.

- Incident Recovery and Response

  This is a critical success factor. It is the responsibility of the Program Office to ensure that an adequate structure and set of processes is effectively implemented in the organisation. Considering the scope, this is often best implemented as a pan-organisation structure, rather than smaller teams dedicated to individual product offerings or, at a minimum, that such a structure exists to support dedicated product teams in case of an exceptional event. Details of this program are provided in section 3.4.5.

- 3rd Party Engagement
  - Ensure, with active involvement of procurement and contract negotiator, that all service and other provisioning contracts are compliant with relevant obligations.
  - If appropriate, define appropriate standards and practices in regards to engagement with third-parties.
  - Ensure that procurement or other relevant organisations maintain and update a registry of third-party engagements and their relationship with obligations.
  - Enforce strict compliance with the standards and practices, as well as reporting.
  - Monitor that procurement or other relevant organisations ensure that contract renewal and changes in terms are properly tracked.
  - Ensure 3rd party providers are regularly reviewed by procurement or other relevant organisations.
  - Ensure that processes are in place by procurement or other relevant organisations to deal with non-compliance of 3rd parties.

  The collection and archiving of contracts is required but not sufficient in most instances. It must be possible to get a quick understanding of the relationship of external engagements with obligations across all engagements (hence the need to maintain a registry). Also refer to the discussion on 3rd parties in section 3.4.3.

- Employee Skills and Awareness
  - Ensure the organisation maintains a registry of job (function) profiles in relationship with the obligation and identifies “sensitive positions”.
  - Ensure the organisation defines recruiting criteria for sensitive positions regarding obligations.
  - Ensure the organisation has specific training programs for sensitive positions regarding obligations.
  - Ensure compliance with legally-required training and certification.
  - Inject topics in the on-boarding and recurrent employee code of ethics and business training programs.
  - Ensure the organisation includes questions measuring accountability awareness and attitude in employee surveys.
  - Ensure the organisation organises and rolls-out specific accountability awareness campaigns, such as posters displayed on billboards and internal bulletins.
  - Ensure that management “state of business” (coffee talks) presentations regularly address accountability.
  - In more general terms, ensure the organisation addresses accountability in appropriate employee information vehicles with adequate messages for rollout through the organisation.
  - Ensure the organisation keeps skills of the specialised staff current – support staff to join industry associations, professional networks, specialised conferences, and get training as required.

  Accountability for one’s own actions, regardless of the domain to which it is applied, must become part of the culture of the organisation, must be embraced by all employees and contractors. Circumventing this must be treated as a serious performance issue. It must be noted that human interaction is one of the weakest points in the security of a system.

- Compliance Readiness
  - Appoint liaison to external domestic and regional compliance and regulatory agencies (as appropriate).
  - Appoint liaison to relevant foreign compliance and regulatory (as appropriate).
  - Ensure the organisation tracks “external criteria” – use a mixture of specialised information services, industry associations, professional networks, specialised conferences, and consultants.
  - Ensure the organisation understands reporting requirements and ensures compliance.
  - Maintain the legally-required documentation (or ensure it is maintained by the relevant departments).

- Deploy Individual Accountability Tools

  - Investigate and (if adequate) ensure deployment of techniques and tools supporting authorisation based on duty segregation.
  - Investigate and ensure deployment of tools guaranteeing that all actions are logged and allow the identification of the agent and of the authoriser (as appropriate). This must be done in compliance with legal constraints on the handling of individually identifiable information. Ensure that these tools bear a proper timestamp and are secured against tampering or destruction.

  There are some commercially-available tools which act as portals and allow the deployment of these types of controls even if the native applications do not support the functionality. In addition, using a uniform mechanism across the organisation allows for a streamlined management of the authorisation structure and of the audit logs. One must note that provisioning a trusted log with attribution is more important, less expensive, and less problematic than deploying an authorisation framework due to the complexity of modelling and allocating the correct structure for the roles, although the latter may reduce risks upfront.

- Ensure Continuity of the Accountability Program
  - Ensure that all the above documentation stays current.
  - Periodically review the various analyses performed.
  - Define and maintain a dashboard providing a synthetic view of the accountability program.
  - Define and track a set of metrics to measure effectiveness and progress. A significant part of these metrics must correspond to objective (as opposed to subjective) criteria.
  - Have the accountability program and the Program Office audited regularly (in the order of once a year) by external auditors.

3.4.3 Provisioning for Accountability – Analyse and Design

By its very nature, accountability identifies and addresses potential risks, harms and expectations – there would be no need for accountability if one could provide a total and absolute guarantee that all these obligations would be met. Designing for accountability is therefore naturally associated with the lifecycle dealing with security, data protection, and risk. There are many variants for this lifecycle – we will use the pragmatic model described in [16].

The main activities involved in this analysis and design phase are to:

- Understand the product or service and related assets
  - Have a description of the functionality and associated non-functional requirements.
  - Inventory the (related) obligations for which the organisation will be accountable.
  - Inventory the assets related to the functionality and obligations.
  - Perform an impact assessment for these assets in order to qualify the risk.
  - Keep and update a record of assets and impacts.

- Perform a risk analysis
  - Identify the position of the board and executive management.
  - Perform a risk analysis – in regards to accountability, this should focus on obligations and the contributing factors, as well as on the accountability support system. The nature of the obligations will influence this greatly. In the case of obligations regarding the handling of personal data, for example, the risk analysis must include an analysis of the potential harm to data subjects (which is not something usually included within a traditional organisational security risk analysis). The risk analysis must take into consideration all aspects impacting the organisation, including secondary impacts such as a loss of reputation, product or service implementation, slow down, regulator push back, and so on.
  - Keep and update the record of threats and vulnerabilities, qualified with probability and impact. Associate this record with the record of assets and impacts.

  Risk analysis is a complex process for which many methodologies and software support exist for traditional security related domains. Risk analysis related to accountability is only a part of the overall risk analysis process but there are few existing tools and practices for that part. As mentioned above, extensions to this process are needed for the domain area (i.e. to consider

data privacy, security, etc.), whereby tools and methodologies already developed for those areas (such as Privacy Impact Assessments) may be used, and ideally integrated at several points within the design lifecycle.

- Define the risk treatment
  - Define how risk will be handled as part of the investigation, design and engineering phases for the product or service.
  - For each risk, identify if it will be reduced, mitigated, assigned, transferred, or accepted. The residual risk must be understood and treated in a recursive manner until the constraints associated with the obligations are met (typically, the residual risk in the last iteration will be transferred or accepted).
  - Define the controls which will be deployed to reduce or mitigate each risk, and define how the risk will be assigned or transferred, as appropriate. These controls can be based on a mixture of technology and processes.[13] In this latter case, a link must be established with the inventory and operational programs defined at the global level for the organisation (see in particular sections 3.4.2 and 3.4.5).
  - Define the metrics and dashboard for continuous monitoring of the state and effectiveness of the risk treatment plan.
  - Augment the above record of threats and vulnerabilities with the record of risk treatment and associated measures. Include all steps in the recursive treatment of residual risk.
  - Validate that the risk analysis takes into consideration the selected implementation decisions. Update it as necessary.
  - Ensure that the accountability mechanisms are tested as part of the solution testing (in both regression and system tests). Validate the effectiveness of the measures.

  This step is tightly integrated with the solution design and engineering phase, and is recursive by nature as each implementation alternative has an impact on risk. The information obtained in this process provides the foundation for signoff and the creation of the first account.

  The result of this phase will be the definition of a technical solution to implement the solution or offering. The technical or procedural controls implemented correspond to a due-diligence and best effort coverage of the requirements. It is in general impossible to guarantee that the mechanisms and procedures effectively deployed guarantee that the obligations will be met. The accountability system must be able to handle the unexpected.

- Select 3rd party providers

  Special attention must be given to the selection of 3rd party providers. We will focus on the selection of cloud services. This section leverages the recommendations made in [20] and [11], but those have been considerably modified to address accountability in general as opposed to just data protection regulation.

  When selecting a cloud provider, the accountable organisation must:
  - Identify assets which will be processed or stored in the cloud environment.
  - Identify the related obligations and associated accountability requirements.
  - Based on the initial risk analysis, identify the risk profile of the provider, the set of security (and other relevant attributes) that must be supported.
  - Identify the links between the third-party accountability provisions and the accountability system of the organisation – list the associated requirements.
  - Based on compliance obligations, identify the certifications and other levels of guarantees that must be offered by the provider (most often including local constraints relating to the data centre and the IT staff).
  - Check internal policies and procedures in terms of selection, registration, and tracking of third party service providers. Comply once the provider is selected.
  - Review and select the provider based on a review of the offerings matching the above requirements. Validate that the costs are in line with funding expectations. Review the

[13] For example, the use of Privacy Enhancing Technologies (PETs) should be seriously considered as a way of mitigating privacy risks. Privacy by design is in general an important aspect of this accountability design process; the latter does not replace it, but augments it.

risk appetite and risk treatment plans if there is a gap. The practice of increasing the levels of risk acceptance to meet the cost expectation should be banned.
    - Ensure that proper contractual clauses are in place, especially as in regards to compliance to the requirements and the associated accountability measures. The contracts must be handled as per organisational policies (see section 3.4.2).
    - Ensure the provider exploits the data only as intended and defined by the Data Controller.
    - Exploitation for the benefit of the provider should be avoided, but if envisaged it must be carefully defined by contract, and its consequences (including liabilities, the Data Controller role and relevant obligations) must be clearly understood by the organisation and be compliant with the allowable use of the data and legal requirements.
    - Identify the metrics that will be used during the lifetime of the relationship to continuously assess the compliance of the 3rd party.
    - Track changes in the service provider operations.
    - Ensure there is an adequate link between the provider exception handling processes and those of the organisation (see section 3.4.5). The associated procedures must be tested regularly and readiness assessments must be performed.

- Provide documentation and signoff
    - The solution must be fully documented and placed under change management. Any evolution must be assessed against the requirement, obligations, and risks, and necessary adjustments must be performed.
    - The contracts associated with the solution must reflect what is actually implemented.
    - An account reflecting the analysis linking obligations with actual controls must be produced and made available to stakeholders. This account is to demonstrate, through a static analysis, the effectiveness of the controls as due-diligence to meet the obligations.
    - The solution must go through a signoff process that will validate that all internal requirements and obligations have been met.

3.4.4 Operating in an Accountable Manner

This phase covers the support, management, and day-to-day operations. For the purposes of accountability, it focuses on two aspects:

- Operate the system as intended:
    - Gather and report on accountability and risk treatment metrics, and keep the dashboards updated.
    - Communicate with stakeholders as intended.
    - Ensure that the collection of evidence is performed as intended.
    - Ensure that all logs are effectively backed-up and are protected against tampering.
    - More generally, ensure that all solution-specific processes and associated organisation-level processes are used and are operating with the intended effectiveness. This is also applicable to all processes related to 3rd parties.

- Look for signs of unexpected issues:
    - Continuously monitor the system, the operating environment, and the ecosystem for signs of incident, breach or significant change. Activate the exception handling processes as required (see section 3.4.5).

3.4.5 Handling Exceptions

It is critical to have a set of policies and processes to handle exceptions, along with the proper organisation to handle these exceptions quickly and completely. These exceptions can be significant, leading to a workload that cannot promptly be handled by an in-house structure of the organisation. Careful planning and coordination with external parties is therefore an important part of this process. In all cases, the organisation must ensure that the organisation and processes are defined with

scalability and prompt reaction in mind as this is required for due-diligence. The Program Office has a central role in organising this set of processes.

The core of the process is articulated via two series of coordinated suites of processes: the handling of complaints, which are externally generated, and the handling of incidents, which are detected by operational monitoring or are the result of complaints after investigation and qualification.

- Handling complaints: the organisation must be ready to:
  - Receive, handle, and respond to complaints and information requests in a timely manner as required by internal policies or legal requirements.
  - Use a case management system to support the handling of requests, track progress, and provide global statistics for use by both the operational management, the Program Office, and the Board.
  - Have a FAQ to anticipate the most frequent information requests.
  - Create a classification for requests and complaints. Define standard procedures for the handling of requests in each of the classes.
  - Have defined escalation procedures.

- Handling incidents and breaches: the organisation must be ready to (in sequential order):
  - Log and track the incidents in a secure, time stamped and reliable way.
  - Provide a prompt operational response to the incident ("stop the bleeding"). This can mobilise staff from all business and technical departments of the organisation as well as external experts.
  - Notify the stakeholders (affected parties) of the incident, providing remediation actions, as soon as those have been identified.
  - Report the incident to authorities when required by law or by the criticality of the incident – including both regulators and law enforcement.
  - Perform a root cause analysis.
  - Repair the affected applications and restore the business processes in full.
  - Build and distribute an account for the incident, which in particular attributes the failure corresponding to the incident.

- Preparedness: in order to be ready to perform the above mission, the organisation must:
  - Define the relevant processes and procedures.
  - Allocate responsibility and deploy the necessary staff.
  - Deploy the required tools (e.g. case management and incident tracking).
  - Have a contingency plan to deal with events of an exceptional magnitude.
  - Place required external resources on retainer, to handle incidents of an exceptional magnitude or the provide forensics expertise.
  - Get insurance against risks (based on a risk / cost analysis).
  - Define metrics for the various processes, track performance, and report to the responsible organisations.
  - Test the system based on simulated incidents.
  - Regularly update these various elements to ensure they are current.

3.4.6 Audit and Validate

It should be noted that audits focus, all or in part, on continuous improvement, providing a proactive view rather than solely looking to place blame. Audit requirements are typically mandated by the domains for which the organisation is accountable. There is however a pattern that can be identified:

- Internal audits
  - Regularly perform internal audits on the system.
  - Focus on both compliance to internal and external criteria.
  - Investigate the effectiveness of the risk treatment plan as implemented. Ensure that the objectives are being met.
  - Trigger a review and adjustment process when critical deficiencies (blind spots) are discovered.

  - Prepare for external audits. Ensure that recommendations from previous external audits have been properly considered and dealt with.
  - Collect the material and perform the analysis which will allow to prepare updated accounts, to include actual indicators of effectiveness rather than solely relying on the theoretical analysis used in the Analyse and Design phase (see section 3.4.3).

  The internal audits are performed by internal auditors, who work within the organisation and report to the audit committee.

- External audits
  - External audits are performed as dictated by the regulations of each domain of accountability.
  - External audits are also required in most compliance or attestation frameworks.
  - Customers may also place contractual provisions for realising audits. The industry trend, in particular as it regards cloud computing, is to define certification and attestation to best-practice frameworks which can be effective substitutes for client-directed audits.

  The external audits are performed by external auditors, which either perform on the basis of an auditing contract or are hired by an external party (e.g. stakeholder or certification authority).

3.5 Accountability Control Framework Alternative for SME

Typically, small businesses do not have a structured and formalised approach to dealing with governance and organisational processes. Likewise, medium enterprises that do not have a specific focus on delivering e-services or make an extensive use of IT, usually lack the staff and expertise to define an IT governance or formalise IT processes. Nevertheless, accountability is relevant for all businesses. We are therefore proposing an alternative to the governance-led approach defined in sections 3.3 and 3.4 above: this section proposes a set of guidelines that can be employed by SMEs. Note that, similarly to the control framework defined in section 3.3, the adoption of this set of guidelines does not mean that the business will be automatically in compliance with laws and regulations.

Our approach is to identify and make explicit key principles that underpin a simplified accountability control framework. This is not a simple mapping exercise: it is analogous to trying to identify the closed set of universal and unequivocal principles which are behind the rules of our society – an impossible task. The list we propose is only the result of a "best effort" pragmatic exercise, and is neither complete nor accurate. A sincere and proactive adoption of these principles, as opposed to just a tick-the-box checklist approach, should lead the organisation to operate in an accountable manner.

- Embrace responsibilities: Obligations are not limited to what is defined in the law or in contracts, as social norms, especially ethical behaviour and eco-responsibility, also result in obligations. Promises made publicly and "values" at the root of the business equally translate into obligations. Providers are also encouraged to undertake obligations that assist customers to achieve compliance. While creating and maintaining a document that lists this full set of obligations is not generally achievable, having a short document listing the categories of obligations and identifying the main ones is very useful to ensuring alignment across the whole organisation and providing consistency over time. Sectorial associations and specialised publications are a good source to identify the obligations specified in the law and in social norms.

- Promote transparency: An accountable organisation must be willing to explain and ready to demonstrate its practices to its customers and statutory stakeholders in a transparent manner[14]. This includes, but is not limited to, information on the financial and legal status,

[14] As an example, for the data protection domain, a cloud provider should, voluntarily and where possible in advance, make available to cloud customers all the information which the provider might reasonably expect a customer to be entitled to in order to be satisfied that personal data will be processed appropriately and that the customer can account to a cloud subject for that processing (cf. [21])

descriptions and terms of services, the supply chain, the technology used, operational processes, and safeguards deployed[15]. A service provider, acting in a chain of accountability, must also be willing to provide access to information and systems as required by their customers to comply with obligations and demonstrate accountability.

- Support participation: The organisation must have the mechanisms in place to allow the customer participation and consent, in particular over the use of protected information in the context of accountability for data protection. Hidden practices, such as the use of data beyond what is explicitly agreed with the customer, are not allowed for accountable organisations. Policies, as well as terms and conditions, must be clearly stated, in a manner which can be understood by non-experts. An organisation should not collect data beyond what it is required to collect to fulfil its obligations.

- Foster individual accountability: The organisation must adopt an accountability mindset. This in particular means that every staff member commits to an ethical behaviour and is both open (transparent) and ready to explain what has been done. To the extent possible, mechanisms should be in place to be able to trace actions to their authors. The organisation should deploy separation of duty authorisation profiles to the extent they do not create a significant point-of-failure due to limited staffing[16].

- Plan for contingencies: Handling contingencies is an integral part of the provided services. This implies that a 360-degree risk analysis and risk treatment plan has been performed, identifying the potential failure points and ensuring adequate remedies will be provided in case of failures[17]. These failures can be of an organisational nature (e.g. loss of staff), technological nature (e.g. software vulnerability, system crash), environmental nature (e.g. earthquake, flooding, storms, accidents), financial nature (e.g. inability to secure funding, loss of business), legal nature (e.g. litigation, change in laws and regulations), to cite just a few. When relevant, the risk analysis must be coupled with an impact assessment focused on impacts to the service customer and its clients. The mechanisms to receive, handle and respond to customer complaints must be in place. Communication with customers and other stakeholders in case of issues must be proactive.

- Commit responsibly: The organisation must ensure it has the means to fulfil its commitments and obligations prior to agreeing to provide a service. This means that adequate means are being deployed in areas such as staffing, training, production resources, technology maturity, service management and monitoring tools, etc. This does not exclude the use of emerging and non-mature techniques or technologies, but means that the customer is aware of the situation and has accepted the associated risks. The organisation must be ready and willing to respond and provide remedy in case of incident, breach, or other failure to render the promised service, whether originating internally or from a third-party. This might require securing a liability insurance cover when processing highly sensitive, valuable, or high-risk data, although remedies are not always in the form of a financial compensation. It may also require obtaining some retainers to mobilize external help in case specific high-impact events occur.

- Adopt best practices: Best practices on providing services are available from many sources, in many forms, from cookbook-style methodologies to complete frameworks associated with certification or attestations. The organisation should be aware of these various schemes and adopt those that are most applicable to their profile (line of business, size, market segment, etc.). These best practices provide a baseline service-level at a minimum cost compared to building a custom solution, as the later requires an often expensive analysis specific to the

[15] Trade-offs have to be considered because disclosing some information, such as the supply chain or safeguards, may lead to an increased operational risk (cf. [21])
[16] It is important to ensure that risks based on missing, ill or departing personnel are considered when defining separation-of-duty authorisation profiles for small organisations.
[17] It must be noted that, depending on the regulations specific to the domain, some risks cannot simply be accepted and must instead be treated.

organisation or the offering. Similarly, the adoption of model contracts, with well-defined properties and operational consequences leading to balanced responsibilities, is advisable.

- Manage the supply chain: Cloud-based solutions often involve a provisioning chain through which the services of many suppliers are composed to provide the solution. Being accountable for the solution means that the organisation is not only accountable for what it operates, but also for what is operated by third-parties. As a consequence, the organisation must understand the commitments of its third-parties, their level of accountability, and how these will compose to meet its obligations. The approach to risks and handling of incidents is a key factor to consider. A best practice consists in using a limited set of suppliers with blanket service agreements, used across the whole solution portfolio, hereby handling separately the design and implementation of the solution and the selection of the supplier. Contracts must be managed, regularly reviewed, and the third-parties must regularly provide evidence that they are operating in an accountable way (for example by means of audits or certifications). See [11] for additional recommendations.

- Collect and protect evidence: Providing an account to stakeholders relies on evidence gathered during the operational phase of the service. The collection, archival, and protection of evidence are therefore key to behaving in an accountable manner. This is not limited to application logs, but should also include the logs of the various management systems and the logs of non-IT processes, such as signup sheets or recording authorisations. While a simple verbal "yes" may be operationally sufficient, an accountable approach requires that this be documented. Likewise, interactions with customers, stakeholders and other third-parties must be documented and traceable. A service provider must also be willing to provide evidence as required by their customers to comply with obligations and demonstrate accountability.

- Demonstrate accountability: The SME must be able to demonstrate its compliance with obligations. This involves the creation of an account (see section 4.1) either at regular intervals (e.g. a yearly reporting cycle) or as required by contract or regulation (e.g. in case of the investigation of a breach by the DPA). Contracts and certification/attestation requirements will often mandate the use of external auditing services to perform an analysis of compliance.

The above list addresses the topic of accountability, but not what the organisation is accountable for. An additional set of principles and actions needs to be identified for that, and this list depends on the topic for which accountability is provided; e.g.:

- Accountability for availability – this caters to uptime service agreement, backup, resilience to natural disasters, etc.
- Accountability for security – this caters to the integrity and confidentiality of data and processes
- Accountability for data protection – this addresses the use and protection of confidential data, as defined by regulation, and includes privacy and security requirements applicable to that data.

Note that these additional sets of principles and actions are not in the scope of this architecture document, which solely focuses on accountability.

In addition, national or regional laws and regulations may define specific accountability responsibilities or mandate certain accountability controls when an organisation processes certain types of data or operates in certain sectors. The good faith application of the above list of principles cannot, in most cases, be a substitute for what is legally required. Refer to [21] for a further discussion of this topic in the data protection domain.

3.6 Implementing Accountability across the Cloud Provisioning Chain

Our report on the Cloud Accountability Conceptual Framework [1] and section 2.5 in this document discuss the complex service provisioning chains which are increasingly frequent in cloud ecosystems. This does not mean, however, that all actors along the provisioning chain have to be "strongly accountable" organisations and adopt the control objectives and best practices defined in this section. Some cloud providers along the chain may implement mitigating measures which remove (or reduce)

the dependency on 3rd-parties' high-grade quality of service (QoS) and ability to render account. For example, an intermediate SaaS service provider may use several IaaS 3rd-party providers for redundancy and workload balancing, effectively removing the dependency on the continuity of any one of these service providers. This means that the SaaS provider can source cheaper IaaS services, from providers with lower quality of service (QoS) commitments and lesser-grade accountability standards. This is however only true to a degree – we are in the domain of greater tolerance to risks, not of acceptance of careless behaviour; likewise we are referring to lesser-grade accountability, not elimination of accountability altogether. Furthermore, we cannot assume that the QoS requirements and level of accountability will become progressively lower across all branches of the provisioning chain – the tolerance for lower-grade services can only be determined through a thorough analysis of the dependencies.

Long and complex provisioning chains pose another challenge for QoS and accountability: the numerous customer-provider interfaces in the chain correspond each to a separate service contract, often pre-existing, with its own set of obligations and reporting requirements. Seamless integration does not exist in this regard. This poses a challenge with regard to the true realisation of each of the four main attributes of accountability:

- **Transparency**: transparency is never absolute. Even if an organisation intends to be genuinely transparent, the processes used to put transparency in motion have limitations, in particular as insiders will have a good knowledge of the situation but have an (involuntarily) biased view, while outsiders equally have a bias, of another nature, and only a limited ability to obtain a true understanding of the situation. Cost, resource, time, and contractual constraints compound these issues.
- **Responsiveness**: input and queries from external stakeholders may not always be received directly by the party which it relates to, and have to be propagated through the provisioning chain, with a transformation at each step according to the context of the customer-provider relationship. This will slow down or ultimately decontextualise the input or query.
- **Responsibility**: responsibility is to be considered in the context of the norms (to which an accountor is supposed to be compliant), which are not uniform across the provisioning chain. This means that an agreement relating to responsibility may not keep its nature along the whole provisioning chain.
- **Remediability**: remediability, like responsibility, is defined in the context of the governing norms, which vary across the whole provisioning chain. While the main service provider (data controller) can provide remedy to affected parties, corrective actions are subject to the customer-provider interfaces along the provisioning chain.

One way to deal with the challenges induced by the provisioning chain is to take a holistic approach, which addresses globally all actors. One of these approaches is Service Integration and Management (SIAM), which finds its sources in ITIL®[18] and its community. The intent of SIAM corresponds to "*the ability to manage the challenge of cross-functional, cross-process, cross-provider integration while finding an effective method for controlling this delivery environment and assuring 'value based' outcomes for the customer*" [22]. SIAM starts with understanding and enumerating the boundaries and dependencies between each of the services; and does not require the documentation of end-to-end transparent processes. SIAM is based on a three layer structure as depicted in Figure 13.

[18] ITIL® is a Registered Trade Mark of AXELOS Limited. ITIL is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. Further information on the ITIL methodology is available at https://www.axelos.com/best-practice-solutions/itil.

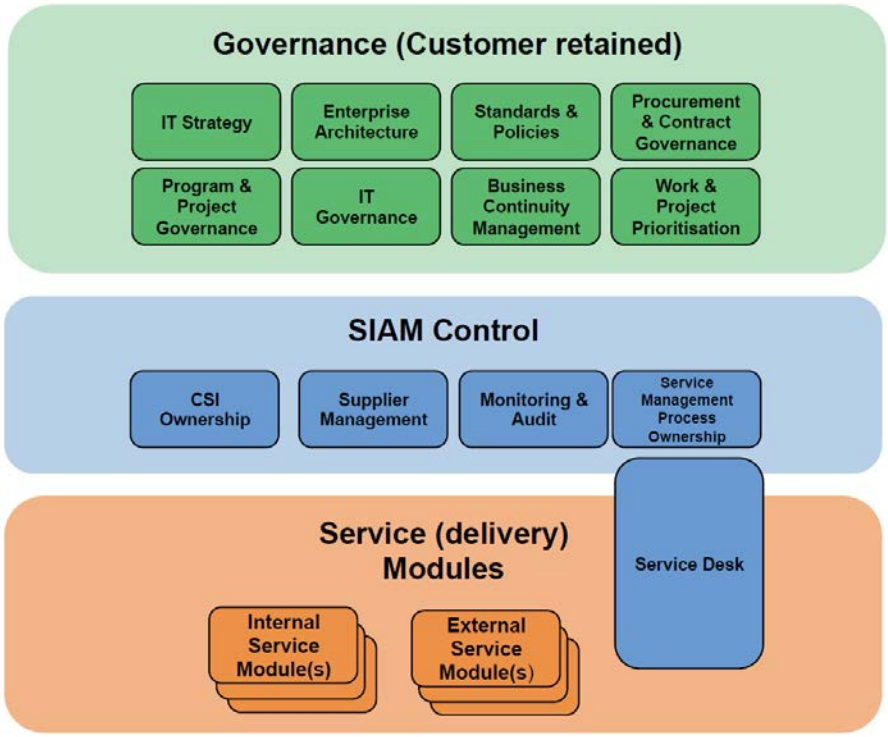


Figure 13: SIAM organisational layers and service modules (source: [22]).

While SIAM itself may be outsourced, this model presumes that all service providers integrate into SIAM. This means that service providers party to the "clumps" described above integrate with SIAM. As SIAM is based on the ITIL model, it means that each provider needs to operate in a manner compatible with an ITIL-based IT Service Management, and use a standardised approach to key processes, such as the exchange of service management information. The SIAM model recognises that some providers, most notably large commodity service providers, may not comply, and requires that the SIAM provider maps (translates) provider-specific information into the structure adopted by SIAM.

The SIAM approach provides a methodology for dealing with accountability in cloud provisioning chains. In an accountability-enabled SIAM, the analysis of boundaries and dependencies between services corresponds to the identification and distribution of responsibilities, which is the starting point of the accountability relationship between an accountor and its accountees. In this approach, each organisation must be accountable, and adopt the organisation-level control objectives and best practices (cf. sections 3.3 and 3.4).

SIAM is, however, not the ultimate solution as it requires that all all service providers integrate into the framework, something that can be mandated only by very large, institutional level actors like governments or similar entities. Only a few actors in the private sector have the purchasing power and competitive positioning to impose such a framework on all providers while remaining competitive. It seems likely that a solution based solely on regulations would not be adequate either due to the inherent dynamism and multi-jurisdictional nature of supply chains and long adaptation cycles of the regulation. A more promising approach could be in the adoption of industry-regulated sectorial compliance frameworks, which would practically translate into a requirement to only select providers which have adopted the compliance framework and been certified for it.

4 Demonstrating Accountability

In this section first we analyse what accounts are and we clarify the process around provision of accounts and their verification. After this, we discuss the relationship between evidence and metrics, and introduce a confidence model for metrics. Metrics are a foundation for continuously assessing compliance, with a strong relationship to accountability. This topic, and the role of certification as an accountability mechanism, is examined in section 4.7. We conclude this section by proposing an Accountability Maturity Model in section 4.8.

4.1 The Account

As discussed above in sections 1, 3.4.3 and 3.4.5, provision of *accounts* is an important part of the organisational lifecycle, and the means of demonstrating accountability. In this section it is explained what accounts are (in 4.1.1: general concepts); who produces them (in 4.1.2); how their properties can vary (in 4.1.4); how this analysis relates to the functional elements of accountability corresponding to section 3.1 (in 4.1.3). Examples of the two main types of account are given, namely evidence about compliance (in 4.3) and about data breaches or policy violations (in 4.4 and 4.5). Within this discussion, ways of improving account provision are given, and the process around the provision of accounts and their verification is clarified.

4.1.1 General Concepts

The form and content of accounts are contextually dependent. In this section the varying properties of accounts are considered.

What is an account?

An account is a report or description that may be written and/or oral, of an event or process. It serves to report what happened, what has happened, or what might happen. An account generally contains answers to the 'reporters' questions", i.e. who, what, where, when and why. It may also include measures taken to remedy prior failures. An account of the same event or process might be provided several times and vary in its format and information depending on the recipient.

Example

An example where accounts are needed is data breach notification. In this case, the following information should be provided:

- To explain who committed the breach (or if unknown, how investigation to discover perpetrator)
- What the breach consisted of
- When the breach occurred (and was discovered if different dates)
- How and why it occurred, extent of breach
- What measures are being taken to prevent any further such breaches in future
- Contact information for a department or person to respond to further questions (and maybe link to web page for updates)

Forms of account

There are two main forms of account: proactive or retrospective accounts.

Proactive accounts relate to reports before making services available. Provision of an account could be *proactive*, in the sense that the choice of accountability mechanisms and tools needs to be justified to external parties, and this could happen before any processing takes place (perhaps as part of a third party assurance review), when processing is particularly risky (e.g. before such processing, with documentation generated via Data Protection Impact Assessments), or using ongoing certification to provide flexibility (for example, as is the case with Binding Corporate Rules).

Retrospective accounts are reactive and can either describe a legitimate event - in which case they can be either periodic or produced upon request (e.g. triggered by a spot check by a regulator) – or an unexpected event, such as a data protection breach.

Furthermore, an interesting distinction can be made between what may be regarded as *static* accounts, as opposed to *dynamic* accounts. The former do not vary over time, whereas the latter take into account parameters that may change over time. For instance, an example of a dynamic account would be a CSA Open Certification Framework (OCF) level 3[19] account, which is an example of a dynamic certification. Indeed, it could be argued that yearly or monthly audits are irrelevant in an environment that changes completely on a daily or hourly basis, as is often the case with cloud computing. Continuous compliance monitoring is essential to securely delivering cloud services and ensuring compliance. Cloud services are inherently dynamic, because the dynamic provisioning and de-provisioning of resources is a key part of the cloud value proposition and business model. Hence, automation for operations and asset management are essential in this dynamic environment and verification of compliance with policy and legislation – such as the EU Data Protection Directive 1995 (Directive 95/46/EC), Gramm-Leach-Bliley Act (GLBA)[20], US federal Health Insurance Portability and Accountability Act (HIPAA) 1996, and export compliance controls like the International Traffic in Arms Regulations (ITAR)[21] – requires continuously running automation. Accounts can be also regarded as a process, for example a process of storytelling and explanation, and further detail about that is given below, later in this section.

Attributes of the account

Although the description of the event or process is an essential element, the account should also carry the following attributes:

- *Recipient*: This is the actor who receives the account. Depending on the recipient, the level of detail in the description of the event may change.
- *Event/Process description*
- *Evidence*: Relevant information to support explanation and justification about assertions (for further discussion see section 5.2.4).
- *Measures for remediation (if incident)*
- *Timestamp and signature*: The accountable organisation is of course responsible for producing the account and therefore should sign the entire report including the date. Accounts of legitimate events may be periodic and could sometimes be used as evidence for prior events whenever an incident happens in the future. A timestamp in the report hence becomes mandatory.

4.1.2 Interactions between Cloud Actors Related to Accounts

First we consider project framing (to set out the general context in which accounts are produced in areas of focus for A4Cloud project) and then the process of generating and verifying an account.

Project framing

As discussed further within A4Cloud deliverable D:32.1 [1], a cloud actor (accountor) is accountable to certain other cloud actors (accountees) within a cloud ecosystem for:

- **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.

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.

[19] https://downloads.cloudsecurityalliance.org/initiatives/ocf/OCF_Vision_Statement_Final.pdf
[20] https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act
[21] https://gov-relations.com/itar/

Contracts express legal obligations and business considerations. Also, policies may express business considerations that do not end up in contracts. 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. By the accountor exposing the norms it subscribes to and the things it actually does, via an *account*, an external agent can check compliance.

Accounts shown to different data protection roles

Generally speaking, the sort of information that an organisation needs to measure and demonstrate in such an account includes: policies; executive oversight; staffing and delegation; education and awareness; ongoing risk assessment and mitigation; program risk assessment oversight and validation; event management and compliance handling; internal enforcement; redress [23] [12]. Existing organisational documents can often be used to support this analysis [13]. Measurement of the achievement needs to be done in conjunction with the organisation and the external agents that judge it, which is dependent upon the circumstances, and to other entities that may need to be notified. Some examples of accounts that may be provided to cloud actors fulfilling certain data protection roles in a given context are shown in Table 16.

Type of Account	Data Protection Roles	Example Cloud Actor producing the Account
Account for self-certification/verification	Data Controller (DC), for Data Protection Authorities (DPAs) and their customers	Organisational Cloud Customer
Periodic internal reviews (to check that mechanisms are operating as needed and update if required)	DC or Data Processor (DP), for themselves or auditors	Organisational Cloud Customer, Cloud Provider
Evidence provided by risk analysis, PIAs and DPIAs (including assessment along the CSP chain and how this was acted upon)	DC, for DPAs and their customers	Organisational Cloud Customer
External certification e.g. BCRs, CBPRs, CSA OCF level 3, privacy seals, accountability certifications, security certifications	DC or DP, for certification bodies (evidence for certification) or for customers (evidence of certification)	Organisational Cloud Customer, Cloud Provider
External audit (ongoing)	DC or DP, for auditors (evidence) or customers (audit output)	Organisational Cloud Customer, Cloud Provider
Verification by accountability agents	DC to agent, output to DPA	Organisational Cloud Customer
Evidence about fault if data breach	DC to DS, DC to DPA, DP to DC, DP to DP	Organisational Cloud Customer, Cloud Provider

Table 16: Accounts provided by whom to whom and in what circumstances.

Verification of accounts

It is not just a question of interaction between actors in the provision of accounts, but also in the verification of accounts. Verification methods may differ across the different forms of account in the cloud, as considered further below. As briefly mentioned in section 3, the company Nymity [13] 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 [13].

There are different levels of verification for accountability, as proposed by Bennett [24], which correspond to policies (the level at which most seals programmes operate), practices and operations. It is very weak to carry out verification just at the first of these levels – instead, mechanisms should be provided that allow verification across all levels. 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 currently 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.

In terms of the verification process, there are various different options about how this may be achieved. 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. In general, 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. There could in some cases be certification based on verification, to allow organisations to have greater flexibility in meeting their goals.

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 [25]). 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 effect could in some cases be very harmful in terms of privacy protection. As Bennett points out ([26] p. 45), 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.

In particular, it is important that the verification is carried out by a trusted body that does not collude with the accountor, and that it is given sufficient resources to carry out the checking, as well as there being enough business incentive (for example, via large fines) that organisations wish to provide appropriate evidence to this body and indeed implement the right mechanisms in the first place.

The overall process around verification of an account is summarised within Figure 14.

First of all, there is a certain context in which the ‘start’ – labelled (1) within Figure 14 - would apply, in other words the context in which an organisation might need to give an account, or might wish to do this voluntarily. Broadly speaking, these situations requiring or involving production of an account may be characterised as follows:

- **Regulatory obligation:** The most typical situation where there is a legal obligation to produce an account is where governmental bodies or regulatory agencies enforce rights or obligations, by means of an investigation, a request for information or a spot check by a Data Protection Authority (DPA).
- **Contractual undertaking:** A legal obligation could instead come from the organisation itself, for instance from a contractual obligation to give an account. The cloud service provider may have given a contractual obligation in its terms of service or in a SLA that it would provide an account (for example, a data breach notification procedure) or that it would demonstrate compliance in some way. Another situation may be that the Cloud Service Provider (CSP) has undertaken to get third party certification for compliance or for some process and so is required by the third party to give an account of certain processes in order to get certification.
- **Voluntary undertaking to give an account:** The CSP may just state (in a policy published on its website for example) that it would provide an account in certain circumstances or make ‘best efforts’ to do so. Many policies published in this way are not legally binding or may not

be incorporated into the contract between the CSP or the customer, so the CSP can refuse to give the account or may claim that it cannot do so and has made a 'best effort'.

Next, supposing this context is in place, the organisation (as accountor) is supposed to give account of not only its actions, but also its results and intentions to the accountee cf. (2) in Figure 14. Exactly what must be provided will vary according to the context; for example, specific information will be expected in the case of the accountor wishing to be certified.

If an organisation gives no account in the first place, there should be repercussions about this that might include the obligation to give a refined account, defined according to the accountees' or assessors' needs, cf. (3) in Figure 14. For example, in the case of regulatory requests, the consequences could be fines. In the case of contractual undertakings, failure to produce an account would be a breach of contract that entitles the customer to damages, or service credits (for breach of SLA) or gives a right to the customer to terminate the contract without notice. Failure to produce an account needed for a third party certification of compliance would mean that the CSP could not obtain the certification. This may have direct legal consequences for the relationship between the CSP and its customer (depending on whether this was a condition of the contract) because the customer may decide to terminate or not to renew the contract. In the case of a voluntary undertaking, although there would be no legal redress for the customers, the consequences of refusal to give an account may involve damage to its reputation by disgruntled customers.

If the organisation does provide an account, this can result in one or more documents being provided, or information being captured by other means, as the account provided by the organisation could be written or oral, cf. (4) in Figure 14. For further information, see for example [27], which expands upon real life cases in which multiple accounts can be created by a Data Controller for presentation to a regulator.

The accountee then assesses the account (5), potentially making reference to additional information (6). The level of satisfaction with the account is gauged (7), in the sense that the account may be judged to show that the organisation is compliant (if appropriate), or else may be judged to provide a satisfactory explanation about a data breach event. On the other hand, the accountee may judge the organisation to not be compliant (and hence for example, not issue a certificate of compliance) (9), or wish to have additional information about the event. Especially in the case of a data protection report, the accountee probably requires more than just information, in other words clarification, explanation, updating and also most probably corrective action. Hence, even if the account process is complete in the sense that the accountee may accept the account is accurate and may be satisfied with it, it could be that they are not satisfied in the sense that the account shows that some action/omission has caused and is causing harm and needs additional action. For this reason, the '*End of account*' (10) may only be the start of another process, even if the accountee is satisfied with the account. 'Next steps based on account' reflects that this process may follow; it could include for example remediation, actions based on the account, further investigation, etc. After all, an account of a breach should contain something about ongoing corrective action.

Accountability agents or other third parties could be used to provide verification of accounts, and serve as an intermediary to the ultimate accountees, some of whom may impose sanctions (8). If, as considered within D:C-2.1, there is a good trust relationship between such an agent and the accountee, then the agent's account is likely to be directly accepted by the other accountees.

The account process is taken to finish (10) if either an account has been provided that is found to be satisfactory by the accountee or an agent acting on its behalf, or the account is not found to be adequate and appropriate actions are taken by the accountee against the accountor. However, this notion of 'finishing' is too coarse-grained, as discussed above. Furthermore, accountability is not a binary state, but has a certain level of maturity. Correspondingly, accounts have a certain effectiveness and appropriateness. Depending on the maturity an accountee may be satisfied or not, and the threshold of this maturity might differ depending on the accountees or the event about which one is asked to give an account. Hence, more mature account might be provided, or different ones for different accountees, events, etc., so this is another reason why '*End of account*' is not necessarily an end state, but the process might be repeated from the start with a different degree of maturity or threshold.

Sanctions might be applied at several points, notably if the organisation does not provide an account in the first place (3), if it fails to respond adequately to the dialogue with the assessor, or if the assessor is not satisfied in respect to the accounts produced (9). In fact, the use of the word 'sanction', here meaning a consequence of an inadequate or non-provision of an account, is avoided within Figure 8 because in legal terms 'sanction' refers to a punishment imposed by a legal or regulatory authority, for example fine, imprisonment of penalties for disobedience, whereas we also want to include non-regulatory actions imposed by the accountee, which is perhaps the customer, and this could for example mean contract termination or perhaps a contractual penalty for failure to produce a report. Such consequences or repercussions are therefore represented quite broadly in Figure 14 as *actions by the accountee against the accountor*.

The process of providing an account could be quite complex, and this is just a generic overview of that process. There could be multiple documents that in the form described here provide an account, but each of which may be viewed as an individual account, and perhaps even have a slightly different process flow. For example, MS:D-4.4 provides an example of how multiple accounts provided by different parties within an organisation are aggregated by a senior officer, who acts as a communication interface with the accountee (in this case, the regulator); this officer would interact further if needed with the various internal teams that produced the accounts if further information is required.

The element of responsiveness is not necessarily in the account itself, yet in the interaction between what the account should be about (and how it should be refined if deemed inappropriate) and in the establishment of the account objects, i.e. the norms that need to be compared with actual behaviour (compliance). Part of the norms to which actual (system) behaviour is compared should be defined in a two-way communication (dialogue) between cloud providers and external stakeholders, which includes cloud users, regulators and the public at large.

The process of generating and verifying accounts for certification could be more specialised than the flow shown in Figure 14 (for example, it could involve assessment by multiple parties) and would need to be adapted as the purpose of verification of the account and possible outcomes would differ, i.e. result in a certain level certification, or no certification being given.

This flow shown in Figure 14 is a generic flow that could apply in range of contexts and is not cloud-specific. With regard to cloud contexts, as with other service provision delivery contexts involving a chain of providers, provision of an account might involve chaining of accounts. For example, an account provided by an organisation using the cloud that is acting in the capacity of a data controller, to a data protection authority might be constructed using accounts that had previously been provided to it from the cloud service providers that it was using.

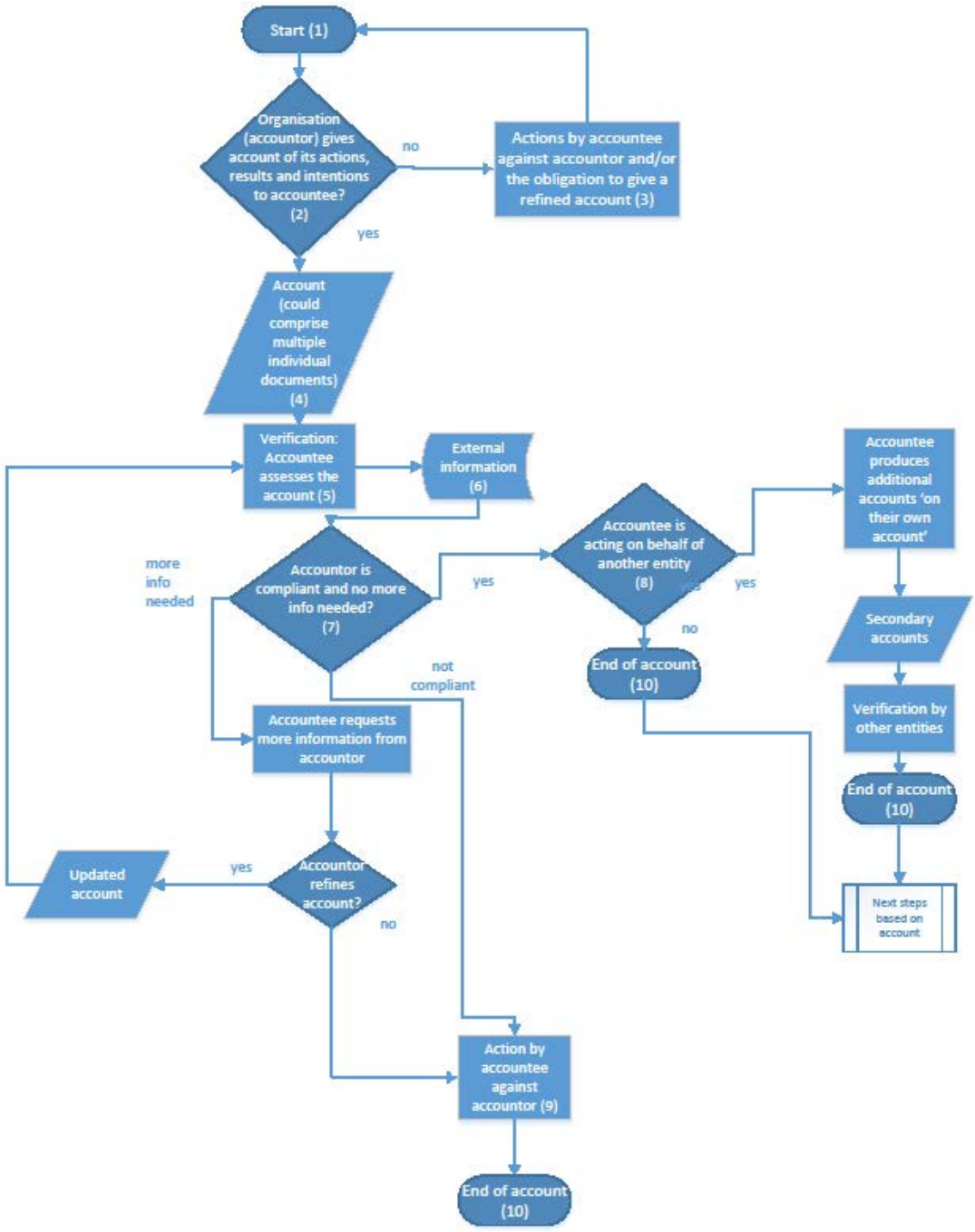


Figure 14: High level view of the provision and verification of an account.

4.1.3 Mapping Different Kinds of Account to Functional Elements of Accountability

In terms of the organisational lifecycle described above in section 3.1, provision of an account may take place in different phases, as shown in Figure 15. Example accounts corresponding to these four stages are shown in Table 17: Mapping of different kinds of account to functional elements.

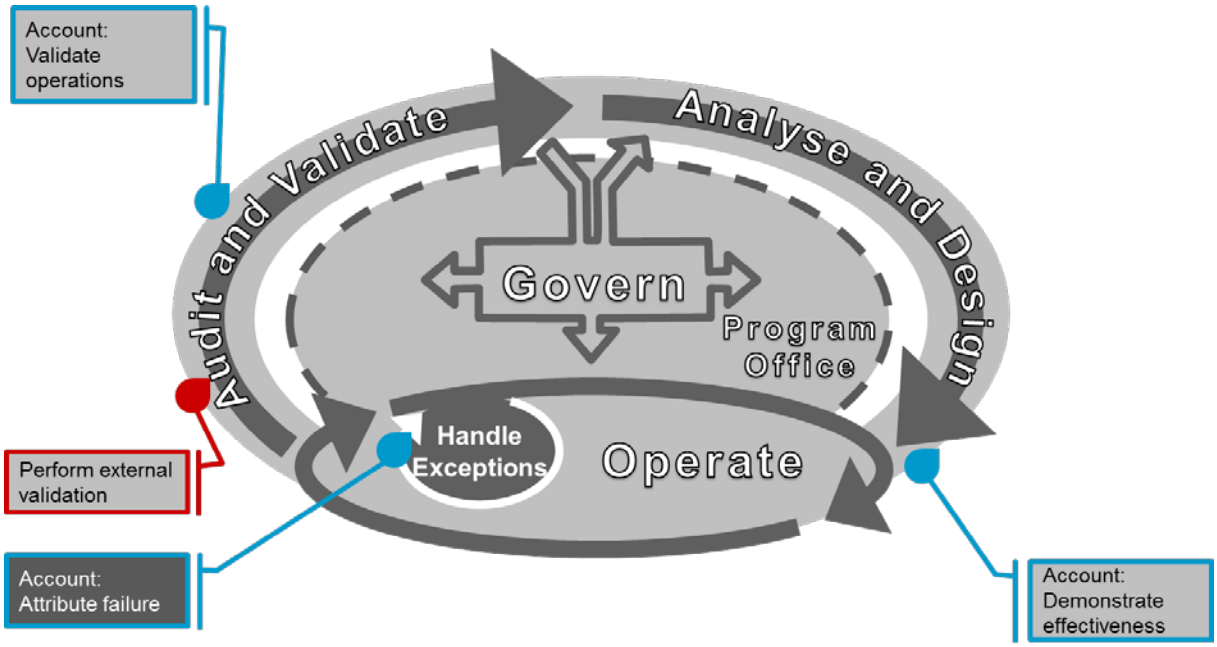


Figure 15: Functional elements of organisational account provision.

Functional Element	Types of Account
Demonstrate effectiveness	Data Protection Impact Assessment Notice to supervisory authorities (before processing) Documentation obtained, created and maintained by DC & DP
Validate operations (organisation)	Contractual compliance verification
Attribute failure (exception cycle)	Notification of data breach to data subjects Notification of data breach to supervisory authorities Notification from cloud provider to other cloud provider/organisation
Perform external validation - Output of third party checking (to be shared)	Certification & seals, e.g. OCF level 3 Audit reports Verification by third party accountability agent

Table 17: Mapping of different kinds of account to functional elements.

In our analysis we do not focus on records used for internal use (for example, risk reduction and self-improvement) within the organisational lifecycle shown in Figure 15, but instead those for external use, and in particular some cases of evidence provided for compliance and data breach notifications.

4.1.4 Summary of Core Properties

From the analysis above, we can identify what an account should include. An account can perhaps best be defined, though simply, as “a report or description of an event.” This means that an account should have a story or narrative that can be easily understood. This account or report can be presented at any time, not just when there has been a system failure. The report or description should sometimes include reasons or explanations, for example, if the event should not have occurred. It should sometimes also explain consequences, for example, what action will be taken to remedy a situation or what action will be taken in the future. It may also include justifications for actions taken or for omissions.

In light of the foregoing, an account, when required and/or provided, usually consists of the accountable actor providing a report or description 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. 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 Cloud Security Alliance.

Applying these principles in practice perhaps best demonstrates the notion of the account and what would be encompassed in an actual account. In sections 4.3 and 4.4, examples of giving an account are considered further.

4.2 **[DETAILS] Account**

The information presented in this section represents details which may only be required if seeking an in-depth understanding of the Cloud Accountability Reference Architecture.

4.2.1 Content of Accounts

In addition to proactive reports, the Accountable Organisation should also report while its services are operational. In this case, the Accountable Organisation will either validate its operations or inform on an incident. As explained in [1], while describing such an event, be it expected (i.e. a legitimate event) or unexpected (an incident), " *the account should generally include the answers to what are traditionally referred to as the reporter's questions […] backed up with as much evidence as possible to validate the account".* These questions are:

- *Who?* The account should provide information on all cloud actors involved in the actual event. This information will especially be very helpful for the Auditor or the Data Protection Authorities to identify the responsible or liable actor.
- *What?* The report should describe all actions taken with respect within this event or provide the details of the incident.
- *Where?* The answer to such a question is especially helpful while verifying the compliance with respect to data transfer policies.
- *When?* The account should mention the time (preferably a timestamp) and duration of the actual event.

While these four questions should definitely be answered in the case of both expected and unexpected events, the account on legitimate events may also include some more details about the process in order to demonstrate the compliance to the corresponding policy rule by answering the following two additional questions:

- *Why?* The answer to this question will simply be the obligation or policy rule the accountable organisation is aiming at enforcing.
- *How?* The report should include as much details as possible on the means used to achieve the corresponding action. For example, to demonstrate that a cloud provider implements security and privacy measures, it should provide details of the underlying functions such as the encryption algorithm, the size of the encryption key, etc.

On the other hand, although an account describing an incident cannot easily answer the previous two questions, it should nevertheless provide some information on remediation and hence answer the following question:

- *What Next?* In [1] authors note that an account is used in a *"prospective function"*; hence together with the description of the incident the account should ideally contain some additional information on future remedial actions and the adopted measures to prevent the recurrence of such an undesired event.

4.2.2 Legal Influence on Properties of Accounts

In this section we examine what an account should contain from a practical perspective, beginning with the obligations arising from legal and regulatory norms, contractual obligations and the opinions

of legal or academic commentators about the content of an account. From these sources, we identify what could or should be the content of an account in more detail than already considered in 4.1.1.

Legal or regulatory norms about the content of the account

There is no formal legal standard on the content of an account. Guidance about the content of the account given by regulatory bodies is typically very high level with little specificity provided by regulators as to what accounts must contain. For example, very little direction is provided in the Data Protection Directive, or even the proposed General Data Protection Regulation on this point.

The Article 29 Working Party ('Article 29 WP') has published its own opinion highlighting the importance of the notion of accountability in the field of personal data protection [28]. In its Opinion 3/2010 on the principle of accountability, the Article 29 Data Protection Working Party highlighted the importance of a concrete proposal for a general accountability principle. Specifically, the Article 29 Working Party found that accountability should focus on two main elements: "(i) the need for a controller to take appropriate and effective measures to implement data protection principles;" and "(ii) the need to demonstrate upon request that appropriate and effective measures have been taken. Thus the controller shall provide evidence of (i) above." [28]. From a data protection point of view, the account is the method of presenting such evidence and demonstrating such measures. The Article 29 Working Party also explained how the use of accounts will lead to greater enforcement by data protection authorities, and perhaps even increased accountability:

> *Furthermore, putting the accountability principle into effect will provide useful information to data protection authorities to monitor compliance levels. Indeed, because data controllers will have to be able to demonstrate to the authorities whether and how they have implemented the measures, very relevant compliance related information would be available to authorities. They will then be able to use this information in the context of their enforcement actions. Moreover, if such information is not provided upon request, data protection authorities will have an immediate cause of action against data controllers, independently of the alleged violation of other underlying data protection principles*. [28]

A similar approach is taken in the non-binding 2009 Madrid international privacy standard, which also addresses the need for organisations to provide an account:

> *The Responsible person shall: a) Take all the necessary measures to observe the principles and obligations set out in this Document and in the applicable national legislation, and b) Have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers, as established in section 23 (Monitoring).*

These documents are important to the process of devising accountability mechanisms in that they indicate how accounts could be used by data protection authorities, for example, to monitor compliance and to demonstrate to the relevant authorities that such measures are in place in the organisation. Therefore they implicitly indicate what types of information an account should contain: evidence of compliance with legal norms and information that demonstrates to authorities that relevant compliance has taken place. Nevertheless, these statements do not give a template of what exactly an account should contain. Rather, they are good practice guidance for accountability at quite a high level.

Contracts in the cloud and practical accountability

Contracts between data controllers and cloud users, and, to a lesser degree, contracts between data controllers and data processors, 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. 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. And even then, data controllers largely try to further limit their obligations, particularly their liability, in their contracts and/or terms of service [29].

As between data controllers and data processors, Article 17 of the Data Protection Directive requires data controllers to impose on data processors the same obligations regarding the implementation of security measures as those imposed on data controllers. The relationship between data controllers and data processors will normally be established via the prior conclusion of a contractual agreement (or other legal act).[22] The initial draft of the Proposed Regulation stipulated in Article 26(2) that such a contract or legal act should be obligatory and should require the processor to "make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article", or in other words to provide at least a partial account.

Finally, the one area where one would most expect an account to be provided would be where there has been a security breach, yet, even in negotiated contracts, as opposed to the standard, non-negotiated contracts which currently dominate the cloud computing landscape, "many providers' standard terms did not require reporting of security incidents and so on to users." [30]

It is noteworthy that even where accounts are imposed by law through legislation and contracts, there is mostly little to no express provision as to what the account must specifically include. If accountability is to be built into the cloud, an important element will be the inclusion of terms in contracts which require a proper account to be given.

It is not possible to draft model contract clauses for this purpose because what is proper in an account will vary substantially depending on the nature of the relationship between the giver and the recipient of the account. It is, however, possible to suggest some overriding principles which might guide the drafting of such clauses:

(a) The recipient of the account should be entitled to appropriate information about how its data will be stored and processed, updated as storage and processing methods change. The level of detail will depend on the nature of the relationship and the data. Thus a consumer user of a "free" cloud service should be content with quite general information, whereas a financial institution will require far more detail.
(b) There should be a suitable mechanism for checking that the actual operations on data match the information given under (a). Mechanisms might range from tools that allow customers to generate their own reports, through independent audit reports, to a right to inspect and audit a provider's systems.
(c) There should be an appropriate mechanism for reporting breaches to those whose interests are engaged, primarily customers, data subjects and regulators. What level of reporting, at what seriousness of breach, and to whom, again will depend on the nature of the relationships.
(d) The account should include explanations of the reasons for any failings, and the measures which will be taken to prevent future failure. The frequency, granularity and addressees of this part of the account are also relationship-dependent.

The content of an account

Since we have no clear stipulation from legal or regulatory sources about the content of the account, we therefore have to turn to statements by academic commentators who have studied or assessed the notion of the account or accountability and analyse what they suggest an account should contain.

As Prof. 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*

[22] Data Protection Directive 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,*

> *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.* [31]

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.* [31]

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 commentator opined:

> *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.* [32]

4.3 **[DETAILS] Accounts Relating to Compliance**

The information presented in this section represents details which may only be required if seeking an in-depth understanding of the Cloud Accountability Reference Architecture.

While an account is usually expected and more useful in the event of security breach or policy violation, an accountor, i.e. the organisation acting as a data steward, may report on events or operations that have taken place in accordance with pre-defined rules. For example, the process for providing information on the use of third parties in the cloud service chain is not adequately addressed in current practices, resulting in the bulk of end users not being aware of the complete cloud service delivery chain and their rights over data handling processes. In DB3.2 [33], several different obligations on informing different actors (Data Subjects or DPAs) about data processing practices have been enumerated (O1-O4, O13, O16).

Therefore, an account relating to compliance should demonstrate that the accountor fulfils the expected requirements regarding data processing practices usually defined through the obligations expressed in policies or in law. Such a report should generally describe the event in question and include the following information:

- *involved actor(s)*: the account should list all relevant actors who were involved in the event;
- *list of actions with **time** and **location** information*: the report should describe all relevant actions taken with respect to the event to be reported. Such a description should include information about time and location.
- *justification of the event*: the account should describe the reason of the event. This usually refers to the identification of the policy rule or obligation for which the accountor should comply with,
- *contact details* of the person or group who is responsible for the event in case further information is needed or an unexpected problem occurs.

The description of the event should further be completed with some additional evidence in order to achieve a certain level of confidence, indeed, as also stated in [13], it is more difficult to fully demonstrate compliance than to report on a security breach. Therefore an account of compliance should regroup all appropriate evidence.

In [13], Nymity divides their proposed *privacy compliance attestation methodology*, into two main steps: identification of the rules that require appropriate evidence and further demonstration of accountability. We propose to follow the same approach and to enrich this methodology by providing examples of forms of account by regrouping a list of potential evidence with respect to specific obligations derived from D23.2 [33]. We will consider in particular three different types of account, relating to secure data deletion, correct data storage and data location.

4.3.1 Account of Secure Data Deletion

An accountability policy may include obligations about data retention which include information about the data storage period. According to Obligation 7 in D23.2 [33], "the *data controller must make sure that all personal data are deleted (…) after the data collection purpose has been fulfilled*". Secure deletion of data is not straightforward and cannot be 100% guaranteed. Existing solutions either remove the link of the data to be deleted or overwrite the content with random data. Some other solutions use cryptography and for example propose encryption of data while storing it and then discarding the decryption key for deletion. It is therefore important to describe how data is deleted. An account of secure data deletion should include the following information:

- description of the deletion method (unlinking, overwriting, etc.);
- log traces on delete queries including information on time and location both from primary storage and backup servers;

In addition to this evidence, the account may also include the contact details of the person responsible for this action in case a further problem occurs.

4.3.2 Account of Correct Data Storage

Obligation 8 in D23.2 states that "*The controller must (..) ensure that appropriate security and privacy preservation measures have been implemented throughout the service delivery cha*in". Since the main service supplied by a cloud provider is data outsourcing, the cloud provider should ensure data availability and integrity. In order to prove the correct storage of data, the cloud provider can provide the following evidence:

- information about data handling practices;
- log traces with respect to the handling of the particular data;
- cryptographic proofs about the storage and integrity of the data.

4.3.3 Account of Data Location

Cloud adoption raises serious privacy concerns with respect to data residency. An accountability policy should express rules about the location of the data and the accountor should provide some evidence about the location of personal data either upon receiving a request or automatically whenever data is transferred. An account of compliance with respect to data location rules can regroup the following evidence:

- Binding Corporate Rules (BCR) approval: the number of multinational companies adopting Safe Harbor,Binding Corporate Rules [34] which define the rules with respect to international data transfer is increasing. Therefore, a BCR certification can be considered as important evidence for an account on compliance.
- information about the physical location of the servers: the accountor can provide such information with a third party audit report for example;
- log traces: data transfer logs can be obtained with a monitoring tool like A4Cloud's data transfer monitoring tool (DTMT).

4.4 [DETAILS] Handling a Data Breach

The information presented in this section represents details which may only be required if seeking an in-depth understanding of the Cloud Accountability Reference Architecture.

The most common situation where an account is required and provided is a data breach scenario. As part of an accountability policy, legal and normative obligations, with respect to the information of

associated parties in case of abnormal behaviour, such as data breach or policy violation, should be expressed in the form of rules. Currently, the requirement for information about such events is not explicitly derived from the regulatory framework, resulting in a lack of proper information about data leakage and violations happening in the cloud service provisioning chain. Further details are given about data breach reporting obligations in the following section (4.5).

In D23.2 [33], we have presented examples for the expression of the account relating to information about the resulting notification for an abnormal event. A4Cloud introduces am obligation for generating notifications about abnormal events (Obligation O18) – see Appendix 8.1. This type of account should be verified through the following information:

- The actor sending the notification
- The type of incident, detailing also which personal data was affected
- The actor by which the incident was raised
- Evidence in the form of logs traces, explaining the incident history
- Timestamp of generating the notification
- Contact details of the actor responsible to answer notification response
- Potentially the contact details for the responsible supervisory authority

In this section several different cases are illustrated in which an account is given in the event of a data breach. These examples also differ from each other with respect to the recipient of the account. The first example is where an account about unauthorised data access is provided to a data subject. Next, an example is provided in relation to a regulatory investigative process. Finally, we consider some examples of data handling within a service provision chain.

4.4.1 Account to Data Subject

This scenario below gives an example of how a data breach could be reported to a data subject. It hypothesises a breach of a cloud provider where data has been accessed and downloaded without authorisation. This breach notification is not required by law. Neither the Data Protection Directive, nor its implementation in national legislation in Member States of the EEA requires a notice of a security breach to be provided to either the Data Protection Authority or the data subjects. Regardless, we are giving an example of a scenario in which an accountable cloud provider, the provider here desires to provide an account to the user and the Data Protection Authority.

How the breach notice should be communicated

The question of how the breach should be communicated to data subjects is entirely at the discretion of the cloud provider since there is no legal obligation to provide an account. That said, it is most likely that the cloud provider would send the account by email to data subjects, in the first instance at least, 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.

What should be included in the breach notice

As noted above in section 4.2.2, there is no legal or regulatory template for such a communication but 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 do the following in its communication:

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 in a basic form, an account by a cloud customer and/or cloud provider to cloud subjects after a data breach may look like the letter or email shown in Figure 16.

Dear Data Subject:

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 February 1, 2015, 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 which 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.

We will release further pertinent information regarding our investigation on our website at www.cloudprovider.com/01022014breach, 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

Figure 16: Example data breach account (notification to end user).

To the data subject, the account will be general and use simple and non-technical language, without much of the technical information that would otherwise be available to the cloud provider. The cloud provider may decide to include more technical information on its website or upon request by the data subject, but the overriding objective to the end user should receive a clear explanation of the account.

What should not be included in the breach notice

The notice to the data subject is in contrast to the account of the same breach to the Data Protection Authority, discussed in the following section about investigations, section 4.4.2, where the account should contain more technical information, for example, the extent of the breach, a more technical overview of the breach, and the number of persons impacted by the breach. In addition, the account to the Data Protection Authority would 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. Providing

such information to a data subject, however, would be counterproductive since such detail could confuse them about the nature and extent of any breach. Therefore excessive technical detail or evidence should not be included in the initial breach notice to the data subject.

Updating and providing additional information after the breach notice

As more information is obtained by the cloud provider and/or business, such information could continue to be provided through updated accounts to the data subject. An example of this is the handling of the data breach by U.S. company Target, who established a webpage containing rather detailed information after its credit card processing systems were compromised[23]. It continued to update that page, providing its customers with information about the extent of the breach, measures that were being taken to prevent such breaches in the future, and other precautions end users should take to avoid damages and/or further damages. The account and updated accounts by Target provide an excellent template for companies facing similar data breaches and/or circumstances in the future.

4.4.2 Generating Accounts during Cloud Investigations by European Data Protection Authorities

In this subsection, we analyse how various accounts are produced during a specific regulatory process, namely, when European data protection authorities (EU DPAs) exercise their regulatory power of investigation in the context of the cloud. EU DPAs are the statutory independent public regulatory bodies which have various functions including applying and enforcing data protection laws in European member states. Investigations refer to the one of the enforcement powers of EU DPAs, namely, their power to investigate data controllers, such as companies which offer cloud computing services or technologies (Cloud Providers), in specific circumstances (e.g. when an individual complains). This analysis is generated from the qualitative socio-legal research as part of WP D4 within A4Cloud project, where we interviewed fifteen respondents including EU DPAs which have investigated cloud providers, and cloud providers which have been investigated by EU DPAs.

Our data analysis suggests that multiple accounts are generated by various actors during the different stages of an investigation of a cloud provider by an EU DPA ('Cloud Investigation'). Cloud investigation can be approached as a three-stage process which consists of the pre-investigative, investigative and post-investigative stage. The pre-investigative stage includes a plethora of circumstances, practices, and routines which lead to the investigative stage (e.g. email exchanges and conference calls between the EU DPA and the cloud provider). The investigative stage starts when the EU DPA initiates the cloud investigation (e.g. by sending a 'letter of intention to audit' to the cloud provider) and ends when the investigation report is finalised and/or published (depending on whether the report is published). The post-investigative stage refers to the stage following the publication (whether internal or external) of the investigation report.

During the pre-investigative stage, multiple accounts of compliance can be generated by different actors depending on the investigation in question. For example, a EU DPA that is unfamiliar with the data processing operations and business model of a cloud provider may engage in substantial discussions with various teams of the cloud provider (e.g. management, engineering, and legal) to know more about the entity it will regulate later on. Such requests for information also generate multiple accounts from the cloud provider such as account of compliance through internal and external policies. Here the types of account take various form such as exchanging relevant information through conversation or email or documents.

During the investigative stage, other accounts of compliance are generated by various actors. As with the pre-investigative stage, such accounts and the actors involved in generating these accounts are context-dependent. For example, subject to several factors such as financial pressures faced by EU DPAs, scope and aim of cloud investigations, different forms of accounts may be sought such as an account of how different technical functions operate in practice. Here the cloud provider often has to provide the EU DPA either with access to the algorithmic codes which implement these technical functions so that the EU DPA can test whether the algorithmic codes operate in the manner set out by

[23] https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ (last accessed on 29 January 2015).

the cloud provider in its policies (e.g. a cookie is deleted within a period of time specified in the cookie policy or the encryption methods used by the cloud provider operates in the manner specified in its privacy policy). Technical testing here often include other actors such as sub-contractors employed by EU DPAs that face financial constraints. Here, the account of compliance generated by the sub-contractor when s/he tests the relevant data processing operation of the cloud provider has to be compiled with other accounts of compliance generated by other employees of the EU DPAs (e.g. through analysis of privacy policies etc.).

Other compliance accounts can also be sought and produced such as accounts of compliance with the relevant data protection laws by providing the EU DPA with access to specific computer terminals when it inspects the premises of the cloud provider. Such accounts emanate from various sources and have to be managed at the cloud provider level before being passed on to the EU DPA for its review to ensure that these multiple accounts do not provide conflicting views of the compliance of the cloud provider with existing data protection laws. Here the generated accounts are questioned by the EU DPAs and can often be clarified by the cloud provider in cases of confusion.

These multiple accounts are examined by the EU DPA at the end of the investigation to determine to what extent the cloud provider complies with the relevant data protection laws. Here, there is evidently a very close link between the accounts produced during the cloud investigation and the outcome of the cloud investigation (e.g. the recommendations of the EU DPA to bring the operations of the cloud provider in line with the relevant data protection laws). This does not mean that accounts of compliance cannot be constructed in specific ways so that a particular version of compliance is generated, especially when the report produced at the end of the cloud investigation is published. We have explored this point further in the deliverable D: D-4.11.

Finally at the post-investigative stage, other accounts of compliance are sought and generated by specific actors. For example, the EU DPA seeks account of how the cloud provider is implementing its recommendations. Additionally, the cloud provider can also seek advice from the EU DPA about the compliance of its proposed future innovations with existing data protection laws. Here accounts of compliance are generated through informal interactions such as face-to-face meetings.

4.4.3 Accounts within the Service Provision Chain

A number of incident scenarios are being studied by work package D4. Some incident categories can be identified by the A4Cloud detective tools and other categories would fall outside the scope of the description of work, but standard techniques and tools can be used to detect them. For instance, non-compliance with respect to data location constraints can be detected by the Data Transfer Monitoring Tool (DTMT)[24], but a machine infected with malware allowing a malicious external agent to have unauthorised access would not be the main focus of our tools. Once a potential data breach has been notified to the data controller (via e.g. the A-PPL Engine), evidence needs to be analysed to confirm the breach. This later step can be achieved with the help of the techniques devised in work package C-8 and the Audit Agent System (AAS), for instance, which will help to identify where failures occurred in the cloud service provisioning chain. Finally, the data subject notification can be handled as described above, possibly with the support of the Incident Response Tool, which has been developed in the context of work package D-4.

Remedial actions can be imposed by the DPAs upon data subject complaint fillings. For a detailed legal analysis of remediation and redress mechanisms, please see MS:D4.1 [35]. The search of an arrangement to remediate damages caused by a breach can be facilitated by the Remediation and Redress Tool, also under consideration in D-4.

For a more precise incident please consider the following scenario from D-4:

"Misconfiguration of services and failing to patch software quickly can lead to severe security problems such as being vulnerable to exploits and violating security requirements. Recent SSL vulnerabilities such as POODLE, BEAST and Heartbleed are prime examples for the need to patch as soon as fixes become available. However, patching may not be enough in some cases. For instance, to mitigate the

[24] This tool is discussed in the A4Cloud Toolkit Architecture companion document.

Heartbleed vulnerability, certificates need to be replaced, old certificates revoked and private keys changed. Besides that, problems can arise from service misconfiguration. The recently discovered POODLE vulnerability is closely linked to obsolete protocols being allowed (which is an SSL configuration problem). Also, in cases where strong cryptography is required, specific SSL configuration is required (protocol versions, available cipher suite, cipher order, algorithms, key length, certificate status…)."

An attacker can gain access to personal data by exploiting this kind of vulnerability. In some cloud provisioning chains, it can be complex to identify whose responsibility it is to apply the necessary patches and updates to the software. This will depend on the service model and on the contractual agreements in place. The A4Cloud approach and tools help to clarify these situations: from detection until the remediation phase.

Another example from D4 of a data breach has to do with a data holder's right to have access to a set of data (right to know). In such a case, individuals are granted access to specific data, but in case of a contextual change in the individual's behaviour over such access rights (such as a large number of access requests in a short period of time), this may imply a potential violation (need to know property). An example like this is common in today's security systems, which adopt intrusion detection mechanisms or perform log and error analysis to monitor malicious intruders and discover misbehaviour, which can result from e.g. the loss of credentials from the data subject's side. If an intrusion is detected, then the responsible system administrator is informed of the timestamp of the event and the details of intrusion attempt (e.g. who, what, reason for alarm, etc.). The relevant data subject will occasionally be informed, but this is subject to the responsible behaviour of the service provider, while the notification of the breach will be mainly handled in a manual way (such as by mail). As happens with the previous example, in this example the handling of the breach involves multiple notification recipients, each of whom should receive a different level of informed actions to respond to. In case of the data subject, as mentioned earlier, this actor will occasionally be notified that their credentials have been compromised, in a way that could enable hackers to enter the system with their digital identity. On the other hand, the DPA may also be informed in case of these events, since this actor has to be told the details of this breach if the damage is severe, including the affected personal data and the respective data subjects and the actions undertaken to mitigate the risks from the exposure of the breach.

4.5 **[DETAILS] Data Breach Reporting Obligations**

The information presented in this section represents details which may only be required if seeking an in-depth understanding of the Cloud Accountability Reference Architecture.

In this section we provide background information on obligations to report data breaches, as ancillary information to the section above, in which accounts for data breach reporting are discussed.

This section provides a brief overview of current and forthcoming EU data breach notification requirements, focusing on the Framework Directive, the ePrivacy Directive, the General Data Protection Regulation (GDPR) and the upcoming Network and Information Security (NIS) Directive. Currently, the telecommunications sector aside, before the GDPR comes into force, data breach notifications are in general not mandatory in most countries in the European Union; nonetheless it is important to note that some countries (e.g. in Spain and Germany) have introduced data breach notification requirements into local legislation and regulatory codes of practice (e.g. Ireland). Different data breach notification requirements (personal data breaches and breaches involving operators in critical sectors and public operators) are foreseen in both the upcoming GDPR and in the NIS Directive. Bear in mind that national legislation or sector-specific regulations might be applicable as well in some specific cases, even if not considered in this overview.

4.5.1 Framework Directive

Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended by Directive 2009/140/EC and Regulation 544/2009, deals with data breach notifications in its Article 13, which states that

> "*Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.*
>
> *Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and the European Network and Information Security Agency (ENISA). The national regulatory authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest.*
>
> *Once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph*".

Article 2 provides some definitions that are adopted in other directives as well, such as the ePrivacy Directive. For clarity and convenience the most relevant ones are reported below:

'*Electronic communications network'* means transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

'*Electronic communications service'* means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;

'*Public communications network'* means an electronic communications network used wholly or mainly for the provision of electronic communications services available to the public which support the transfer of information between network termination points.

4.5.2 ePrivacy Directive

The ePrivacy (2002/58/EC) Directive was reviewed in 2009 in the frame of the reform of the regulatory framework on electronic communications by the Citizens' Rights Directive (2009/136/EC).

Its Article 3, titled "*Services concerned*", states that it

> "*shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the*

> *Community, including public communications networks supporting data collection and identification devices*".

The Directive applies therefore to communications providers or Internet service providers (ISPs) involved in the processing of individuals' personal data, and not to Information Society Services (e.g. SaaS providers) tout court.

The Directive deals with the security of the communications in Article 4[25], whose first paragraph mandates the provider of a publicly available electronic communications service to undertake

> "*appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented*".

Moreover, its second paragraph states that

> "*(i)n case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved*".

In 2009, as mentioned, the ePD was amended by Directive 2009/136/CE, which modified Article 4: aside from renaming the title (now "Security of processing"), it added additional paragraphs which clarify on one hand the concepts of technical and organisational measures and of data breach, and on the other the obligations deriving from them.

Paragraphs 3 and 4 of the amended Directive deal with data breach notifications, obliging the provider of publicly available electronic communications services to notify the personal data breach to the competent national authority without undue delay; moreover,

> "*(w)hen the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach*[26] [27]".

The paragraph continues, however, with an exception: the provider shall not be required to notify individuals of a personal data breach if it

> "*has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it*[28]".

The paragraph ends with a vague description of the content of the notification with regards to individuals

> ("*(t)he notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach*")

and relevant authorities

[25] Originally entitled "Security", after 2009 "Security of processing".
[26] Art. 4, par. 3 ePD as amended by Dir. 2009/136/CE.
[27] The national authority is empowered by the same article to require the provider to notify individuals and subscribers concerned in case it did not previously do that: Art. 4, par. 3 ePD as amended by Dir. 2009/136/CE.
[28] Art. 4, par. 3 ePD as amended by Dir. 2009/136/CE.

("*(t)he notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach*").

4.5.3 GDPR

The Commission's proposal

The provisions concerning data breach notifications are Articles 31 and 32. Article 31 concerns the notification to the supervisory authority: In the case of a personal data breach, the controller shall – without undue delay (not later than 24 hours after having become aware of it) and where feasible – notify the personal data breach to the supervisory authority. In cases where it is not made within 24 hours, the delay has to be justified.

The notification to the individuals affected is disciplined by Article 32, whose first paragraph states that

> "*(w)hen the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay*".

The article's third paragraph, however, exempts from the notification duty

> "*if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach*"[29]

so that the data results would be unintelligible to unauthorised persons. In any case, according to Article 32's fourth paragraph, if the controller did not notify the affected individuals, the national authority may compel it to do so.

The Parliament's version

The Parliament slightly modified Article 31, substituting the 24 hour time requirement to notify the national authority with a broader "*without undue delay*". Article 32, which concerns the notification to the data subject, was amended as well: the notification has to be done

> *"(w)hen the personal data breach is likely to adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject*"

(instead of the mere "*the protection of the personal data or privacy*") and it needs to be comprehensive and use clear and plain language and provide information about the rights of the data subject, including redress .

The Council's latest version

The Council's version of Artt. 31 and 32 arguably imposes a less stringent obligation than both the Commission's and the Parliament's one. The notification to the data subject *ex* Art. 32 is due only when the breach is likely to result

> "*in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of (…) pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage*",

and the data controller is exempt from the notification duty in four distinct (and broad) cases:

> "*a. the controller (…) has implemented appropriate technological and organisational*[30] *protection measures and those measures were applied to the data affected by the personal*

[29] Note the similarity of wording compared to the exemption related to security breaches with respect to the ePrivacy Directive discussed above.

> *data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption; or*
> *b. the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; or*
> *c. it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner; or*
> *d. it would adversely affect a substantial public interest*".

The notification to the national authority *ex* Art. 31 turned out a weaker requirement as well. The data controller, according to the Council, shall be obliged to notify to the competent authority only a breach

> "*which is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, [breach of (…) pseudonymity], damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage*",

and in a longer maximum time span – namely 72 hours. Moreover, according to the Council's Article 31, par. 1a, if the controller has implemented appropriate technological and organisational protection measures and those measures were applied to the data or it has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialise then the notification to the national authority is no longer due.

The Consolidated version

On 15th December 2015, the EU Commission, Parliament and Council of Ministers reached agreement after months of "trialogue" negotiations. This will soon be adopted most likely in Spring 2016 and come into force across the EU two years later on in mid-2018. Under this consolidated version of the GDPR [36] a "personal data breach" is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" and is associated with the requirement of a 72 hours notification period. A notification by the data controller to the data protection authority must be provided that "at least":

(1) describes the nature of the personal data breach, including the number and categories of data subjects and data records affected;
(2) provides the data protection officer's contact information;
(3) describes the likely consequences of the personal data breach, and
(4) describes how the controller proposes to address the breach, including any mitigation efforts.

Notification is not required however if "the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals". When a data processor experiences a personal data breach, it must notify the controller (and not necessarily the data protection authorities). If the data controller has determined that the personal data breach "is likely to result in a high risk to the rights and freedoms of individuals," it must also communicate information regarding the personal data breach to the affected data subjects.

4.5.4 NIS

On the 7th of February 2013 the European Commission published its "*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*" [37] ("the Cybersecurity Strategy") along with a proposal for a Network and Information Security (NIS) Directive. [38] The Directive is a minimum harmonisation[31] one, which aims at ensuring a higher level of data security across the whole

[30] "Organisational" being a notable addition by the EU Council.
[31] See Art. 2, [35]. See also [53].

EU by setting a threshold that national laws must meet, while still having the possibility to exceed the minimum mandatory level.

The proposal represents the EU's first attempt to enact a comprehensive set of cybersecurity related norms that are not restricted to a particular area or regulatory sector. It is a polar shift towards a mandatory framework for cooperation and incident notification, which sharply differentiates itself from the voluntary cooperation, and data breach reporting mechanisms with which the EU is familiar.[32]

Despite the widespread view that cybercrime and the lack of cybersecurity represent a major threat[33] for public safety, economic well-being and national security, the legislative proposals generated a significant amount of concern, both from economic actors and Member States. Some actors indeed worry that this proposed top-down, cross-sectorial, mandatory form of regulation could ultimately hinder European businesses. The imposition of burdensome and static administrative requirements and the increased coefficient of reputational risk all companies bound by mandatory data breach notification requirements would be subject to led the European Parliament – guided by the Internal Market and Consumer Protection (IMCO) Committee – to significantly amend and water down the original NIS Directive proposal. Ultimately, a final parliamentary version was voted on the 13th of March 2014.

The Strategy enumerated the cyber-security priorities of the EU,[34] amongst which NIS naturally assumes a prominent position. The Commission's proposal for a NIS Directive, published along with the Strategy, addresses this priority pursuing a triple order of objectives:[35]

1. Having the Member States reach a high[36] level of national information security capabilities "*by establishing competent authorities for NIS, setting up Computer Emergency Response Teams (CERTs), and adopting national NIS strategies and national NIS cooperation plans*[37]"
2. Stimulating cooperation at a communitarian level "*within a network enabling secure and effective coordination, including coordinated information exchange as well as detection and response at EU level […] to counter NIS threats and incidents on the basis of the European NIS cooperation plan.* [38]"
3. Mandating operators in critical sectors[38] and public operators to adhere to stringent risk assessment and management practices, adopting appropriate and proportionate security measures and reporting the NIS incidents that are deemed sufficiently serious.

Those objectives reflect on the proposed Directive's structure. The proposal is divided in five sections, respectively titled "*General Provisions*", "*National Frameworks on Network and Information Security*", "*Cooperation Between Competent Authorities*", "*Security of the Networks And Information Systems of Public Administrations and Market Operators*" and "*final provisions*". The Directive contains also two

[32] "The current situation in the EU, reflecting the purely voluntary approach followed so far, does not provide sufficient protection against NIS incidents and risks across the EU. Existing NIS capabilities and mechanisms are simply insufficient to keep pace with the fast-changing landscape of threats and to ensure a common high level of protection in all the Member States": [35], p. 3.
[33] A research study conducted on U.S. companies by the Ponemon Institute in 2012, for instance, framed the cost for a single lost or stolen record in the order of $194, the average size of breached records being 28,349 in the sample considered: [54]. Another research study conducted by PwC U.K. quantified the mean cost of the single most expensive breach in a single year's span: between 15.000 and 30.000 pounds for a small business and between 110.000 and 250.000 pounds for a large organisation, totalling billions in damages for the whole U.K.'s PLCs [55].
[34] Achieving cyber resilience, reducing cybercrime, developing cyber defence policy and capabilities and industrial and technological resources for cyber-security, establishing a coherent international cyberspace policy for the European Union and promoting core EU values [56].
[35] See Art. 1, par. 2, [35].
[36] See Art. 4, [35].
[37] [35] p. 4.
[38] As defined and enumerated by the proposed Directive and its annexes.

annexes, containing respectively a list of tasks and requirements for CERTs and a (non-exhaustive) list of market operators covered under the scope of the Directive.

As to the first area, which regards future Member States' frameworks for NIS, Article 5 would mandate Member States to adopt a "national NIS strategy,"[39] comprising a "NIS cooperation plan[40]", to be communicated to the Commission within one month from its adoption. Member States, according to the following Article 6, would also have to designate a competent national NIS authority tasked to monitor the Directive's application and contribute to its coherent implementation across the EU. Moreover, Article 7 sanctions Member States to setup a CERT "*responsible for handling incidents and risks according to a well-defined process*" under the supervision of the Authority *ex* Art. 6; the CERT would need to have enough technical, financial and human resources to be effective in responding to incidents as set out in its tasks, and Member States would need to allow it to rely on a secure information-sharing system as set out in Article 9 of the NIS proposed Directive.

Its third section tackles the second objective of the NIS Directive – the development of a solid cooperation system between the competent authorities mentioned above. Setting up a cooperation network would logically be the first step, and indeed Article 8 states "*the competent authorities and the Commission shall form a network ("cooperation network") to cooperate against risks and incidents affecting network and information systems*".

The network's members shall:

(a) Circulate early warnings on risks and incidents;
(b) Ensure a coordinated response in accordance with Article 11;
(c) Publish on a regular basis non-confidential information on on-going early warnings and coordinated response on a common website;
(d) Jointly discuss and assess, at the request of one Member State or of the Commission, one or more national NIS strategies and national NIS cooperation plans referred to in Article 5, within the scope of this Directive.
(e) Jointly discuss and assess, at the request of a Member State or the Commission, the effectiveness of the CERTs, in particular when NIS exercises are performed at Union level;
(f) Cooperate and exchange information on all relevant matters with the European Cybercrime Center within Europol, and with other relevant European bodies in particular in the fields of data protection, energy, transport, banking, stock exchanges and health;
(g) Exchange information and best practices between themselves and the Commission, and assist each other in building capacity on NIS;
(h) Organise regular peer reviews on capabilities and preparedness;

[39] The NIS national strategy shall address, as a minimum:
- The definition of the objectives and priorities of the strategy based on an up-to-date risk and incident analysis;
- A governance framework to achieve the strategy objectives and priorities, including a clear definition of the roles and responsibilities of the government bodies and the other relevant actors;
- The identification of the general measures on preparedness, response and recovery, including cooperation mechanisms between the public and private sectors;
- An indication of the education, awareness raising and training programmes;
- Research and development plans and a description of how these plans reflect the identified priorities.

[40] The NIS cooperation plan shall address, as a minimum:
- A risk assessment plan to identify risks and assess the impacts of potential incidents;
- The definition of the roles and responsibilities of the various actors involved in the implementation of the plan;
- The definition of cooperation and communication processes ensuring prevention, detection, response, repair and recovery, and modulated according to the alert level;
- A roadmap for NIS exercises and training to reinforce, validate, and test the plan. Lessons learned to be documented and incorporated into updates to the plan.

(i) Organise NIS exercises at Union level and participate, as appropriate, in international NIS exercises.

A secure information-sharing infrastructure, like the one national CERTs have to be provided by Member States, is foreseen in Article 9, in order to allow the members of the cooperation network to communicate through a secure system.

The Directive highlights also the importance of early warnings (Art. 10) and coordinated responses (Art. 11), clearly signalling the weight coordination mechanisms have during the whole lifecycle of the incident – from its detection to the response phase.

The setup of such a network would imply a high level of cooperation and information sharing throughout the EU and possibly on a global level as well, due to the transnational, borderless nature of NIS threats and incidents. In order to achieve such a cooperation level, Article 12 empowers the Commission to adopt a "Union NIS cooperation plan", no later than one year after the Directive's adoption, which aims to coordinate Member States' NIS action; Article 13, on its hand, affirms that the EU may conclude international agreements with third countries or with international organisations partly or fully integrating them in the Union's cooperation plan.

The Directive's fourth section deals with public administrations' and market operators' NIS requirements and incident notification. Both are to undertake appropriate technical and organisational security measures[41] in order to manage the NIS risks relating to their operations. Those measures are to be appropriate in relation to the state of the art, and guarantee a level of security tuned to the risks foreseen:

> "*In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems*[42]".

Both, moreover, shall notify to the competent authority incidents having a significant impact on the security of the core services they provide[43]. Neither the NIS mandatory measures nor the notification requirement foreseen in Article 14's first two paragraphs apply, though, according to its last paragraph, to micro-enterprises, as defined in Commission Recommendation 2003/361/EC of 6 May 2003. Moreover, Article 1, paragraph 3, clarifies that

> "*(t)he security requirements provided for in Article 14 shall apply neither to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC, which shall comply with the specific security and integrity requirements laid down in Articles 13a and 13b of that Directive, nor to trust service providers*".

The Parliament, mainly steered by its IMCO Committee, in its first reading [39] significantly amended the Commission's proposal for a NIS Directive, arguably watering down its scope and effectiveness.

As mentioned, the security and reporting requirements of the Directive would have applied, according to the Commission's version, to public administrations and market operators, defined as either (a) providers of information society services which enable the provision of other information society

[41] "'Security' means the ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system": Art. 3 point 2, [35].
[42] Art. 14, par. 1, [35].
[43] Art. 14, par. 2, [35].

services" or (b) operators of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health. Annex II concretely specifies, albeit in a non-exhaustive way, which categories of undertakings qualify as market operators for the purposes of the Directive.

The Parliament's version removes public administrations from the scope of the Directive, and amends the list of market operators excluding providers of information society services (as defined by the e-Commerce Directive) such as e-commerce platforms, internet payment gateways, social networks, search engines, cloud computing services and application stores, focusing instead on energy, transports, financial markets infrastructures, water and food production and supply, and internet exchange points[44]. A new Article 13a, moreover, allows Member States to determine the level of criticality of market operators, taking into account an array of considerations, such as the specificities of sectors, the importance of the particular market operator for maintaining a sufficient level of service, the number of parties supplied by the operator, the time period until the discontinuity of the core services of the market operator has a negative impact on the maintenance of vital economic and societal activities, and so on.

The Parliament also clarifies the incident reporting obligation set in Article 14. The notification, it specifies, shall be done *without undue delay* when incidents dent the *continuity* of the core services in a significant manner[45]; the significance of the incident shall be determined taking into consideration the number of users affected, its duration and its geographic spread. A newly introduced paragraph 2a specifies moreover that the authority to be notified is the one of the country of the affected core service. Finally, Article 1a's fifth paragraph states that the incident notification foreseen in Article 14 shall be without prejudice to the provisions regarding personal data breach notifications set out in Article 4 of Directive 2002/58/EC and in Regulation (EU) No 611/2013.

Despite narrowing the scope of the original Commission's proposal, the Parliament's text highlights the connection between NIS measures, notification to the competent authority and individuals' rights to privacy and data protection introducing Article 1a, titled "*Protection and processing of personal data*", that binds the processing of personal data in the NIS context to the respect of Directive 95/46/EC, Directive 2002/58/EC, Regulation (EC) No 45/2001, and Decision 2009/371/JHA. The same article specifies that

> "*(t)he processing of personal data shall be fair and lawful and strictly limited to the minimum data needed for the purposes for which they are processed*" and that the data "*shall be kept in a form which permits the identification of data subjects for no longer than necessary for the purpose for which the personal data are processed*".

The text supported by the Parliament would need approval by the Council before it could be converted into law, since they both must back proposed EU legislation before it can be introduced through the ordinary procedure. Discussions on how to balance the Commission's proposal with the Parliament's amendments are currently being held by Member States representatives46. The European Parliament, Council and Commission agreed on the NIS Directive on December 8th 2015, but the final text will not be available before it enters into force.[47]

At the time of writing, therefore, the exact content is unclear, but some information has been made available. In particular, the press release45 specifically lists the following sectors:

- Energy: electricity, oil and gas
- Transport: air, rail, water and road

[44] Ibid., Annex II.
[45] "Incident having a significant impact' means an incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions": Art. 3 point 8a of [35].
[46] See for instance [57].and [58]
[47] http://europa.eu/rapid/press-release_IP-15-6270_en.htm

- Banking: credit institutions
- Financial market infrastructures: trading venues, central counterparties
- Health: healthcare providers
- Water: drinking water supply and distribution
- Digital infrastructure: internet exchange points (which enable interconnection between the Internet's individual networks), domain name system service providers, top level domain name registries

Member states will identify these operators on the basis of criteria, such as whether the service is essential for the maintenance of critical societal or economic activities. The directive will also cover:

- Online marketplaces
- Cloud computing services
- Search engines

ENISA will be the secretariat of a new CSIRT network tying together all national CSIRTs.

The NIS Directive, overall, is expected to create a positive impact for EU cybersecurity in general and for the A4Cloud project in particular. The shift from a generalised voluntary approach to a mandatory framework is timely and opportune; the main issue, rather than the opportunity of the Directive's enactment, seems to be balancing the Directive's scope and obligations in order not to unreasonably hinder economic operators' ordinary activities, burdening them with too many obligations. As for the Project's scope, the adoption of a mandatory data breach notification mechanism and the imposition of a stricter minimum level of security measures could boost the usefulness – and therefore, potentially, the demand – of the A4Cloud toolset. The concordance between the NIS Directive's *ratio legis* and the A4Cloud's tools results clearly from the Project's definition of accountability, "*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*" [1].

In the first place, the scope of the NIS Directive would be significantly restricted if the final version will turn out to adhere to the Parliament's amendments: as for the Projects' interest, maintaining information society services – cloud services included – in the list of operators bound by NIS obligations would increase the relevance of the project's tools, making them go along with hard-coded legal obligations. In particular, having CSPs mandatorily subject, on one hand, to the security requirements set out by the Directive, and on the other to the notification obligation would significantly boost the tools' usefulness. In any case, the adoption of the A4Cloud toolset by the economic operators to whom the Directive will eventually apply is likely to be a meaningful help in compliance practices, and even if public administrations and some economic operators will be eventually excluded from the scope of the Directive, the Project's tools could still be adopted on a voluntary basis.

On the other hand, the Parliament's amendments show a closer connection and integration with both the existing data protection framework and the upcoming General Data Protection Regulation (GDPR) – a welcome approach, considering how the obligations set out in the NIS Directive could turn out to have a stark privacy-invasive side.

4.6 **Metrics and Evidence**

In accountable organisations, the evidence element can be used to indirectly assess the suitability of organisational policies, IT controls and operations. In this sense, the usage of accountability metrics capable of performing such indirect assessment throws light on the existing relationship between accountability metrics and evidence. The following example illustrates this relationship:

> *Let us consider an accountability metric that computes the percentage of customer PII[48] records with a timestamp out of all the customer PII records kept by an organisation. This metric can be used, in combination with additional relevant metrics, to indirectly evaluate how*

[48] Personally Identifiable Information.

well the organisation meets the verifiability attribute of accountability with respect to the fulfilment of a data retention policy by disclosing how long (data retention period) the PII will be kept before being deleted. Verifiability requires the "behaviour" of the process in place for data retention be verifiable against the policy. In this case the timestamp held by a PII record allows the verification of whether the storage of the record is conforming to data retention policies by comparing it with the data retention period and the current date. Furthermore, the PII creation date is used as body of evidence to perform the actual measurement based on the metric definition.

Based on the previous example and from the perspective of the accountability framework, metrics are a means for demonstrating accountability through its attributes using the notion of *quantifiable evidence* of the application of proper practices and the performance of operational processes. Based on this notion, A4Cloud proposes the following definition for the evidence element in the context of accountability metrics:

Evidence: collection of information, with tangible representation, that can be used for assessing a cloud service attribute.
Note 1 to entry: A metric does not measure directly an attribute of a given cloud service, but rather it measures the attribute indirectly through the evidence associated with that cloud service. Therefore, the evidence element supports the measurement result and the repeatability of the measurement.
Note 2 to entry: Evidence may come from sources with different levels of certainty and validity, depending on the method of collection or generation. All these sources can be analysed and be used as body of facts for assessing a given attribute.

The proposed definition of evidence is broad enough to encompass not only experimental observations, but also system logs, certifications asserted by a trusted party, or textual descriptions of a procedure. Therefore, e*vidence can take different forms and can be provided at different levels: at (i) the organisational level, to demonstrate that the policies are correct and appropriate for the context; at (ii) the operational level, to demonstrate that the right practices and mechanisms have been deployed to implement the policies; at (iii) the technical level, to demonstrate that systems and processes in place are behaving as planned.*

The evidence element also contributes to the S.M.A.R.T. characteristic of an accountability metric, namely:

- S - Specific (or Significant) – Evidence allows metrics to be specific and targeted to the area being measured. For example, evidence provides information about the actors involved on the measurement, the purpose or benefits of the metrics, etc.
- M - Measurable (or Manageable, Meaningful) – Evidence supports the elicitation of "meaningful metrics", by providing clear information about the input parameters.
- A - Achievable (or Appropriate, Attainable) – Metrics should not be developed if one cannot collect accurate or complete data. Evidence in this case helps stakeholders to assess the quality of the inputs, and ultimately to evaluate the assurance associated to the measurement result.
- R - Repeatable – Provided evidence is essential to trace the measurement process applied by the assessor to obtain the result. Evidence should provide enough information to repeat the measurement, as many times as required, in order to validate the obtained measurement result.
- T - Timely – Timely metrics are those for which data are available when needed, and this feature is directly related to the quality of provided evidence.

Depending on the characteristics of the evidence associated to each metric, it is possible to derive a "level of confidence" that indicates the assurance on the result of the metric. This confidence is based on two factors:

- Consistency, which indicates how systematic and regular the evaluation process is. This dimension is directly related to the "Repeatable" characteristic of accountability metrics. This level can vary depending if the evidence indicates an informal assessment where no formal procedure for the evaluation is defined (level 1), a structured but manual assessment (level 2), or an automated and systematic evaluation (level 3).

- Source of Assessment, which indicates how independent the metric's evaluation with respect to the object of assessment is. Self-provided assessments are considered of low value (level 1), while third party assessments, or even user/publicly verifiable evaluations, are considered of high value (levels 2 and 3, respectively).

Based on these two dimensions, an aggregated measure of the level of confidence can be constructed, according to the Metrics Confidence Matrix, in Figure 17. This measure indicates the confidence in the metric's results according to the following levels:

- **Level 0 (Unreliable).** There is no confidence in the metrics results, since both the independence and the consistency of the assessment are very low.
- **Level 1 (Insufficient).** In this case, one of the two factors only achieves the lowest level, so the global confidence value will be considered as insufficient. It is clear that confidence in metrics is insufficient when the assessment is self-made or the process is informal.
- **Level 2 (Essential).** This level is the minimum desired level of confidence. The assessment guarantees an acceptable level of independence and consistency.
- **Level 3 (Maximum).** This is the preferable level of confidence. However, achieving this level is presumably a costly procedure, since it implies automating the evaluation and making it publicly verifiable.

It is clear that both self-assessed and informally performed evaluations are not sufficient for providing a reliable metric; thus, the maximum attainable level of confidence for these two levels is 1. In particular, when the evaluation is both informal and self-assessed, the confidence is considered to be non-existent (level 0). Once both factors reach a level of 2, then an acceptable level of confidence is achieved (level 2). For the particular case when the evaluation is both publicly verifiable and automated, a maximum level of confidence is reached (level 3). Note that the confidence level defined above is only a coarse-grained indicator of the aggregation of the two factors of confidence. A finer grained indicator could be possible, but it would have more levels, which complicates its interpretation. Thus, the selection of this scale was done for the sake of simplicity and clarity.

Source of Assessment \ Consistency	Informal (Level 1)	Structured (Level 2)	Automated (Level 3)
Self-assessment (Level 1)	**0**	**1**	**1**
Third party assessment (Level 2)	**1**	**2**	**2**
User/Publicly Verifiable (Level 3)	**1**	**2**	**3**

Figure 17: Metrics confidence matrix.

The degree of confidence associated with accountability metrics becomes useful for mechanisms like certifications, where multi-assurance schemes like the CSA Open Certification Framework (OCF) have been proposed by the industry. The idea behind CSA OCF is to offer three levels of assurance (Level 1 – self assessment, Level 2 – third party attestation, and Level 3 – continuous monitoring/continuous audit), with different degrees of confidence related to the provided evidence. A more detailed discussion related to certifications and accountability is presented in the next section.

4.7 Certifications and Continuous Compliance

In addition to producing an account during the operational phase, the accountor can deliver a report to proactively demonstrate the effectiveness of the provided service. Important evidence to be included

in the account/report are for instance the company policy and/or the binding corporate rules (BCR), that could be used by DPAs to verify how a certain organisation is dealing with data protection across all business processes. For example the DPA can verify whether the actual policy rules, terms and conditions are governed by law.

The reference to Certifications and Attestations that the organisation holds can be also included in the report. A certification is typically an assessment / audit conducted by a third party to verify that a specific product, service or process satisfies the requirements/controls included in standard of reference. From a high-level perspective a certification entails the following actions:

1) *Identification of the relevant certification or attestation scheme to be used* (ISO 27001, SOC 2, CSA STAR Certification, Common Criteria, etc.). The selection of the scheme depends of the objective of certification (does the company want to certify a product or service/process? Does the company want to satisfy specific sectorial requirements? Does the company need to follow an international standard or want to obey to a code of practice / conduct? etc.)
2) *Definition of the scope.* The identification of the object of the certification, e.g. which process(es), which components, etc. A company can decide to certificate the overall organisation or just a specific process, units, or products. What is necessary though is that the scope is relevant.
3) *Identification of the controls that are relevant and applicable in the scope of the certification.* In an ISO and CSA context this exercise is called definition of the "Statement of Applicability" (SoA). Often the SoA is defined based on the results of a risk analysis that identifies the potential security, governance or general compliance risks and the controls necessary to mitigate them.
4) *Audit* the assessment of the controls, to verify that they have been implemented and that are able to mitigate to an acceptable level the risks to which the organisation is exposed.
5) *Monitoring* and periodically updating the whole process, potentially starting again from step 2.

These steps can be conducted internally by an organisation in the form of a self-certification. However a higher level of assurance is always obtained when the assessment of these steps is conducted by an independent third party (auditors).

Well-known certification schemes that relate to security and privacy include:

- ISO 27001[49], which certifies information system management practices.
- PCI DSS[50], which focuses on the secure processing of bankcard data.
- Service Organisation Control Reports[51] (SOC 1, 2 or 3), which is also about information system management.
- CSA STAR Self Assessment[52], which is a self-assessment regarding best practice governance, risk and compliance.
- CSA STAR Certification[53], which is a third-party assessment based on the CSA Cloud Control Matrix, ISO 27001 and ISO 2706.
- EuroPriSe[54]: , which certifies compliance with data EU protection rules (limited to Directive 95/46/EC) for products and services.

Certification can be used to support the "account" as defined in A4Cloud in two ways.

4.7.1 Certification as an Account

First, when an organisation obtains a certification to demonstrate compliance with a set of rules, whether they relate to security, privacy or governance in general, they are fully applying the notion of a "proactive account" (see section 4.1).

[49] Please refer to http://www.iso.org/iso/home/standards/certification.htm.
[50] Please refer to https://www.pcisecuritystandards.org/security_standards/index.php.
[51] Please refer to http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/ServiceOrganisation%27sManagement.aspx.
[52] Please refer to http://www.cloudsecurityalliance.org/star/self-assessment/.
[53] Please refer to https://cloudsecurityalliance.org/research/ocf/#_resources.
[54] Please refer to https://www.european-privacy-seal.eu/.

With the notable exception of CSA STAR Self -Assessment, which is a self-certification, whereby all findings are published in a public repository, none of the certification schemes listed above requires the results of the evaluation to be made available to outside worlds (for customers and data subjects). Sometimes the results of the assessment are made available to interested parties upon request and based on a Non -Disclosure Agreement. It should be noted that arguments against the disclosure of assessment results exist, e.g.:

- The documented account contains descriptions of security measures and processes that could provide information to adversaries.
- The documented account contains intellectual property or other confidential business data.

The result of this lack of visibility into audit results is that in many cases, certified companies will merely highlight that they hold a certification, and will not disclose details of the process. In most cases the certified company does not even state the scope of the certification, which results in customers not receiving any relevant information with regard to the actual value of the achieved certification. This is not possible under the CSA STAR Certification, where the publication of assessment's scope is mandatory.

While this principle is valid for the reason stated above, it contradicts the principle of transparency that is central to accountability. There should be therefore a middle ground that distinguishes a "detailed proactive account" (which is only provided to the auditors), from a "public proactive account" (which is provided to all interested stakeholders). The example of the CSA STAR Registry[55], which currently has reached 140 entries, shows that companies are willing to provide information describing on a high-level how they implement certain controls addressing risk, compliance and governance issues in cloud services. Therefore there is room for the notion of a "public proactive account" in certified cloud services.

4.7.2 Certification of the Account

Second, in order to build the account, a certain number of processes need to be in place. For example, incident reporting and analysis processes need to be defined, tested and implemented and evidence collection procedures need to be verified. Like any other organisational and technical processes, these elements are certifiable, provided that a reference organisational standard exists. These elements would have a place within an "accountability management standard" as we suggested in 1.2.2.

4.8 The Accountability Maturity Model

A4Cloud has identified the need to aid organisations (in particular, SMEs) to quantitatively assess their accountability practices as a first step to improve them. The proposal was to develop an Accountability Maturity Model (AMM) that could be used to assess the maturity of the mechanisms deployed to support accountability. This practice is not new in ICT, where maturity models have existed for several years (for example [40]).

In analogy to widely used maturity models, the AMM proposed by A4Cloud is composed of two elements:

- ***Control Framework:*** a set of controls that an organisation will apply to address requirements such as security, privacy and/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". This score typically increases with the level of sophistication of control implementation.

[55] https://cloudsecurityalliance.org/star/?r=4615#_registry.

The novelty of the AMM is its focus on capturing both the maturity of individual organisations in terms of accountability practices, as well as an assessment of the appropriateness of the measures used across whole cloud provisioning chains.

Based on the control framework proposed in section 3.3, the rest of this section further develops and instantiates the notion of AMM by:

- Mapping the accountability controls (cf., section 3.3) to a real-world control framework, and eliciting the associated accountability metrics in order to allow the implementation of semi-automated accountability assessment/certification processes.
- Associating the assessment of controls and metrics from the AMM to both the CSA's cloud reference architecture.

With respect to the mapping process mentioned above and in order to align the AMM to A4Cloud's standardisation efforts (being performed by WP:A-5), the control framework to be used in the rest of this section will be the Cloud Security Alliance's Cloud Control Matrix[56] (CSA CCM).

4.8.1 Instantiating the Accountability Control Framework

The accountability control framework elicited in section 3.3 can be mapped into well-known frameworks like CSA CCM to provide the foundations of the proposed AMM. A4Cloud followed two complementary approaches to perform the suggested mapping namely (i) mapping of CSA CCM v3.01 controls to Accountability Attributes, and (ii) mapping of CSA CCM v3.01 controls to the accountability controls shown in section 3.3.

Summary of results: mapping CSA CCM to A4Cloud Accountability Attributes
The mapping between CSA CCM and A4Cloud Accountability Attributes resulted on a coverage of approximately 46%, meaning that only 62 controls (out of 136 CSA CCM controls) were mapped to at least one accountability attribute. Furthermore, the highest "accountability coverage" related to the Transparency attribute (11,5%) followed by Responsibility (5%) and Remediability (4%). These results mostly relate to the fact that CSA CCM was designed as a security control framework, where accountability in data protection (i.e., the A4Cloud perspective) does not have a central role. Further information and results associated to the CSA CCM – Accountability Attributes mapping can be found in section 4.9.

Summary of results: mapping CSA CCM to A4Cloud Accountability Controls
A second mapping process took place between CSA CCM and the Accountability Controls (cf. section 3.3) to also realise the degree of accountability that is provided by the CCM controls and domains. An immediate result of this analysis is that certain domains of the CCM are particularly aligned with the accountability controls and best practices. The domains "Audit Assurance & Compliance" (AAC) and "Security Incident Management, E-Discovery & Cloud Forensics" (SEF) are fully covered by accountability controls (100% coverage). The former domain is intimately related to the Governance and Audit & Validation phases of the Accountability lifecycle, whereas the latter is associated to the Handling Exceptions phase, which explains their strong degree of relevance. Other domains, such as "Supply Chain Management, Transparency and Accountability" (STA), and "Governance and Risk Management" (GRM) also present high rates of coverage (between 80% and 90%).

At the other end of the spectrum are those domains that are fully devoted to the specifics of security tasks, and which, therefore, are not mapped to any accountability control. These domains are "Datacenter Security" (DCS), "Encryption & Key Management" (EKM), "Mobile Security" (MOS) and "Threat & Vulnerability Management" (TVM). As in the case of the CSA CCM – Accountability Attributes mapping, this result is understandable because the Accountability lifecycle does not deal with particularities of technical mechanisms and CCM is strongly security-focused. Other CCM domains tightly related to technical security measures are "Application & Interface Security" (AIS), "Identity and Access Management" (IAM) and "Infrastructure & Virtualisation Security" (IVS), and therefore, present a low coverage with respect to accountability controls (lower than 25%).

[56] Please refer to https://cloudsecurityalliance.org/research/ccm/.

The remaining CCM domains present a medium level of coverage. For example, "Data Security & Information Lifecycle Management" (DSI) is devoted to mechanisms for ensuring the protection of customers' data, which is explained given the fact that accountability and data protection are both in the scope of this project. Other domains of relative importance are "Business Continuity Management & Operational Resilience" (BCR), due its role in accountability functions such as Handling Exceptions, Remedy and Redress, and Risk Assessment, and "Human Resources" (HRS), which can be associated to Staff Commitment and Governance for Accountability. Finally, "Change Control & Configuration Management" (CCC) and "Interoperability & Portability" (IPY) are relevant to the Risk Assessment function.

The next sections further discuss the quantitative scoring and metrics associated to the elicited AMM controls, which allow for some realistic level of automation to be adopted by the assessment process.

4.8.2 AMM Scoring Methodology

In the proposed AMM, the set of accountability controls (cf., section 3.3) is complemented with a scoring methodology to (quantitatively) represent how well all of these controls have been implemented by the organisation under assessment. It is worth highlighting the fact that there is no standard scoring methodology adopted by state of the art maturity models; in many cases even the semantic associated with the numeric output (and also the actual number of maturity levels) is different. In order to align the proposed AMM with relevant industrial practices, the rest of this section leverages the scoring methodology used by CSA CCM. A suitable procedure for assigning maturity levels based on a CCM assessment has been developed in the context of the Open Certification Framework (OCF). 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)* 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.

When assigning a score to a control domain, the following five factors are 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. Once the assessor has assessed all of the control domains, 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*.

A typical (state of the art) maturity model would only implement the two elements discussed above (controls and scoring methodology); however, two limitations appear in relationship to (i) the subjectivity associated with the underlying assessment process, and (ii) the level of automation that

could be achieved. In order to overcome these limitations, EU projects like CIRRUS[57], CloudWatch[58], SPECS[59] and Cumulus[60] have been looking at potential mechanisms to implement the continuous assessment of security/privacy in a semi-automated manner for cloud systems. A promising solution is based on the use of metrics, just as proposed also by A4Cloud. The next subsection elaborates the relationship between the AMM and the accountability metrics.

4.8.3 Measuring the AMM Controls

Metrics are defined by NIST [41] as *"a standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of a measurement."*, and keep a close relationship to the concept of accountability being developed by A4Cloud. From a technical viewpoint, metrics are widely used as an instrument for verifying/monitoring the compliance of non-functional requirements, such as those related to security, privacy, or accountability. Metrics are also a tool that facilitates the decision-making process, since they can be seen as an input of the management review process of an organisation [42]. In this context, *accountability metrics* become an important aspect of the proposed AMM, since they can be considered as a means for showing that proper mechanisms for privacy, security and information governance are in place and indeed support accountability. However, in order to fulfil with this vision, it is necessary to relate the accountability controls from the AMM to the accountability metrics developed by A4Cloud. This is possible thanks to the approach proposed by A4Cloud to develop meaningful accountability metrics (please refer to details in section 4.9).

The elicited accountability metrics cover approximately 32% (10) of the CSA CCM controls resulting of the mapping to attributes. The other 21 controls do not have any metric associated to them. Obtained results also show that out of 39 accountability metrics, only 14 different metrics (approx. 35%) were actually related to the mapped CSA CCM. The resulting 10 measurable CSA CCM, are associated with metrics that can be assessed either automatically (e.g., Metric 26 Mean time to revoke users) or through human intervention (e.g., Metric 38 Total expenses due to compensatory damages).

The fact of having "non-measurable CSA CCM controls" does not mean that these cannot be assessed at all; on the contrary, in these cases the "traditional" audit practice will prevail and the control(s) will be evaluated through provided evidence while applying self-assessments or third-party assessments. Next we elaborate about the usage of these metrics from the perspective of the CSA cloud reference architecture (CSA EA).

4.8.4 Accountability Assessment from a Cloud Reference Architecture Perspective

In order to provide *useful* information about the accountability level achieved by an organisation, both the AMM and accountability metrics must be applied to a specific cloud context. This context might refer for example to some particular cloud deployment/service model, possibly resulting from a preliminary risk analysis or an existing set of security/privacy requirements. In any case, the proposed AMM/metrics cannot be applied on an isolated manner. This section elaborates on using the AMM[61] for the quantification of organisational accountability levels based on a cloud reference architecture (CRA). A CRA is typically comprised of a framework (i.e., methodology and tools) that enables security architects, enterprise architects, and risk management professionals to leverage a common set of solutions (patterns). These solutions fulfil a set of common requirements that risk managers must assess regarding the operational status of internal IT security and CSP controls (e.g., from AMM). The controls are expressed in terms of "security capabilities" and designed to create a common roadmap to meet the security needs of their business. NIST Special Publication 500-299 (draft) [43] and CSA Enterprise Architecture (CSA EA, formerly known as Trusted Cloud Initiative[62]) are two commonly referenced state of the art CRAs. For the sake of A4Cloud standardisation, the discussion presented in the rest of this section will be focused on CSA EA.

[57] Please refer to http://www.cirrus-project.eu/.
[58] Please refer to http://www.cloudwatchhub.eu/.
[59] Please refer to http://specs-project.eu/.
[60] Please refer to http://www.cumulus-project.eu/.
[61] In this section, the term AMM will also refer to the associated accountability metrics.
[62] Please refer to https://cloudsecurityalliance.org/research/eawg/.

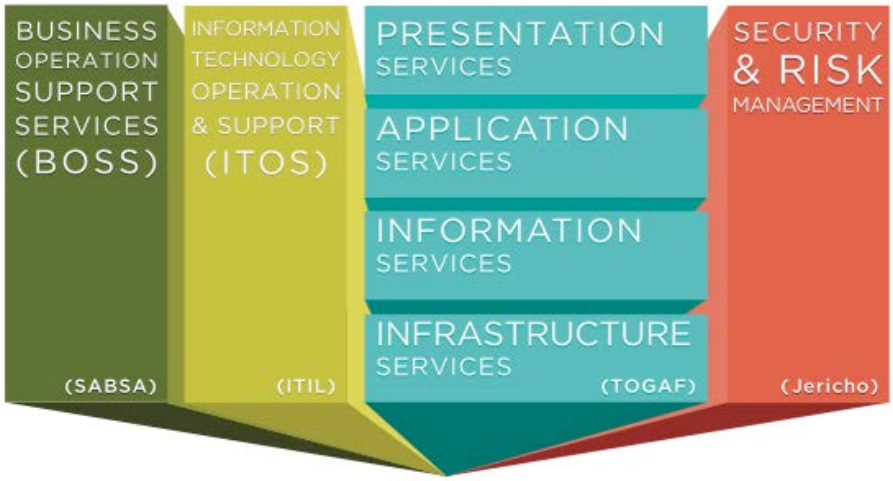


Figure 18. CSA Enterprise Architecture[63].

The CSA EA (shown in Figure 18) is structured in a hierarchical manner. Eight domains exist at the top level, which are composed of containers, and in turn these are comprised of one or more capabilities.

Within A4Cloud, the CSA EA capabilities were related to the mapped CSA CCM controls (please refer to section 4.9) in order to develop an approach to quantitatively assess the accountability level of an organisation through the following sequence of steps:

1. Map the organisation's security architecture components to the CSA EA's capabilities. Additional guidance to perform this mapping can be found on the CSA EA specification (please refer to footnote 17).
2. Based on the previous mapping, select the AMM controls (resulting from the CSA CCM mapping) that correspond to each component's capability.
3. Using the related set of metrics classify the AMM controls from Step 2 into "Quantifiable" (C_Q, if at least one accountability metric is associated to them) and "No Quantifiable" (C_{NQ}, if the control is not associated to any accountability metric).
4. Evaluate the accountability controls in the following manner:
    a. The C_Q controls should be measured according to the respective metric definition also developed by A4Cloud.
    b. The C_{NQ} controls should be assessed (e.g., by a human auditor) according to the applicable practice (for example, in the case of CSA CCM please refer to [18]).
5. Aggregation of results (out of scope in A4Cloud):
    a. The measurement results associated to the controls C_Q can be aggregated by using state-of-the-art techniques like [44] or [45].
    b. The assessment results obtained for C_{NQ} can be scored to an overall maturity level, following the rules presented in section 4.8.2.

The final result from Step 5, is the actual maturity level associated with the architectural component being evaluated. The accountability quantification process described above is shown in Figure 19.

Figure 19. Steps for evaluating the accountability level (architectural approach).

[63] extracted from https://research.cloudsecurityalliance.org/tci/

A4Cloud's notion of *appropriateness*[64] is closely related to Step 2 shown in the previous figure, where the set of accountability controls that are required by the organisation are selected from the CSA CCM mapping (possibly through a risk management process). Realistic levels of automation related to the process shown in Figure 19 would allow the organisation to periodically assess whether the selected controls are actually appropriate, by periodically computing the achieved Level of Accountability. This is a core idea in continuous certification schemes like CSA OCF – STAR[65].

4.9 [DETAILS] Details about the Accountability Maturity Model

The information presented in this section represents details which may only be required if seeking an in-depth understanding of the Cloud Accountability Reference Architecture.

This section reports in detail the analysis of mapping the CSA CCM version 3.01 to the accountability attributes proposed by the A4Cloud project. In order to start with the proposed analysis, criteria were developed to find out the relationship among individual controls from the CSA CCM and the accountability attributes proposed by A4Cloud [1]. The proposed criteria are shown in Table 18.

General rule: If the control does not concern data stewardship practices, it is ignored.		
Accountability Attribute [1]	***To whom information is provided?***	
	Internal stakeholders (I)	***External stakeholders (E)***
Transparency Does the control require or enable the dissemination of information describing how the organisation conforms to governing norms, behaviour and compliance of behaviour to the norms? 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 an assessment, test or enable the construction of a proof of norm compliance (i.e. checking the behaviour of a system, service or processing against norms)? 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
Remediability Does the control enable corrective action and/or providing a remedy for any party harmed in case of failure to comply with its governing norms? Note: Detective and preventive controls are not enough. We target corrective controls here.	Measures involve internal stakeholders	Measures explicitly involve external stakeholders, through compensation, punishment and/or information
Responsibility Does the control require an analysis resulting in the	With assignments disclosed internally	With assignments

[64] Defined by the project as „The extent to which the technical and organisational measures used have the capability of contributing to accountability."
[65] Please refer OCF – STAR Level 3: Continuous in https://cloudsecurityalliance.org/star/

General rule: If the control does not concern data stewardship practices, it is ignored.		
Accountability Attribute [1]	***To whom information is provided?***	
	Internal stakeholders (I)	***External stakeholders (E)***
assignment of a task, or the oversight of a task, to an individual, group, or organisation? Or does the control participate in the enforcement of the assignment of a task to an individual, group or organisation? The tasks here contribute towards norm compliance (and together should enable norms compliance). 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.		disclosed to external stakeholder
Responsiveness Does the control take into account input from external stakeholders and respond to queries of these stakeholders?	Not applicable	With scope including all involved external data subjects

Table 18: Criteria for mapping the CSA CCM to A4Cloud's accountability attributes.

At a glance, the applied criteria considered that the goal of accountability is to provide information to external stakeholders. In consequence, a gap was identified if the analysis finds out that only information to internal stakeholders is provided. The results of the analysis are shown in the table below.

No.	Control name (CCM v3.01)	Control code	V	T	R	Rem
1	Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02				
2	Business Continuity Management & Operational Resilience Impact Analysis	BCR-09				
3	Business Continuity Management & Operational Resilience Management Program	BCR-10				
4	Change Control & Configuration Management Unauthorised Software Installations	CCC-04				
5	Change Control & Configuration Management Production Changes	CCC-05				
6	Data Security & Information Lifecycle Management Classification	DSI-01				
7	Data Security & Information Lifecycle Management Data Inventory / Flows	DSI-02				
8	Datacentre Security Asset Management	DCS-01				
9	Encryption & Key Management Entitlement	EKM-01				
10	Encryption & Key Management Key Generation	EKM-02				
11	Governance and Risk Management Management Support/Involvement	GRM-05				
12	Identity & Access Management	IAM-02				

No.	Control name (CCM v3.01)	Control code	V	T	R	Rem
	Credential Lifecycle / Provision Management					
13	Identity & Access Management Trusted Sources	IAM-08				
14	Identity & Access Management *User Access Authorisation*	IAM-09				
15	Identity & Access Management *User Access Reviews*	IAM-10				
16	Identity & Access Management *User Access Revocation*	IAM-11				
17	Identity & Access Management *User ID Credentials*	IAM-12				
18	Identity & Access Management *Utility Programs Access*	IAM-13				
19	Infrastructure & Virtualisation Security Audit Logging / Intrusion Detection	IVS-01				
20	Security Incident Management, E-Discovery & Cloud Forensics *Incident Management*	SEF-02				
21	Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting*	SEF-03				
22	Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Legal Preparation*	SEF-04				
23	Supply Chain Management, Transparency and Accountability *Data Quality and Integrity*	STA-01				
24	Supply Chain Management, Transparency and Accountability *Incident Reporting*	STA-02				
25	Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-04				
26	Supply Chain Management, Transparency and Accountability *Supply Chain Agreements*	STA-05				
27	Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews*	STA-06				
28	Supply Chain Management, Transparency and Accountability *Supply Chain Metrics*	STA-07				
29	Supply Chain Management, Transparency and Accountability *Third Party Assessment*	STA-08				
30	Supply Chain Management, Transparency and Accountability *Third Party Audits*	STA-09				
31	Threat and Vulnerability Management Anti-Virus / Malicious Software	TVM-01				

Table 19: Mapping between CSA CCM and A4Cloud accountability attributes Legend: (V)erifiability, (T)ransparency, (R)esponsibility, (Rem)ediability.

The mapping between the accountability controls shown in section 3.3 and the CSA CCM v3,01 controls is shown in
Table 20 below:

Control Domain	CCM V3.01 Control ID	Governance	Lifecycle
Application & Interface Security Customer Access Requirements	AIS-02		3.01
Audit Assurance & Compliance Audit Planning	AAC-01	1.09	6.01
Audit Assurance & Compliance Independent Audits	AAC-02	1.09	6.01 6.03 6.05

Control Domain	CCM V3.01 Control ID	Governance	Lifecycle
Audit Assurance & Compliance Information System Regulatory Mapping	AAC-03	1.01 1.09 1.13	6.01
Business Continuity Management & Operational Resilience Business Continuity Planning	BCR-01	1.08	5.04
Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02	1.08	
Business Continuity Management & Operational Resilience Equipment Maintenance	BCR-07	1.10	
Business Continuity Management & Operational Resilience Equipment Power Failures	BCR-08		5.07
Business Continuity Management & Operational Resilience Impact Analysis	BCR-09		5.07
Change Control & Configuration Management New Development / Acquisition	CCC-01		3.05
Change Control & Configuration Management Outsourced Development	CCC-02		3.04
Data Security & Information Lifecycle Management Classification	DSI-01		3.01
Data Security & Information Lifecycle Management Data Inventory / Flows	DSI-02	1.10	3.01 3.05
Data Security & Information Lifecycle Management Handling / Labeling / Security Policy	DSI-04	1.10	
Data Security & Information Lifecycle Management Ownership / Stewardship	DSI-06	1.04	3.05
Governance and Risk Management Baseline Requirements	GRM-01	1.01 1.09 1.13	3.01
Governance and Risk Management Data Focus Risk Assessments	GRM-02	1.02	
Governance and Risk Management Management Oversight	GRM-03	1.01 1.04	3.05
Governance and Risk Management Management Program	GRM-04	1.04 1.07 1.09	4.01
Governance and Risk Management Management Support/Involvement	GRM-05	1.01 1.04 1.09	
Governance and Risk Management Policy Impact on Risk Assessments	GRM-08	1.02 1.03	6.03
Governance and Risk Management Policy Reviews	GRM-09	1.04 1.09 1.13	

Control Domain	CCM V3.01 Control ID	Governance	Lifecycle
Governance and Risk Management Risk Assessments	GRM-10	1.02 1.03 1.09	3.02 6.01 6.03
Governance and Risk Management Risk Management Framework	GRM-11		3.03
Human Resources Employment Agreements	HRS-03	1.06 1.12	
Human Resources Roles / Responsibilities	HRS-07	1.04	
Human Resources Technology Acceptable Use	HRS-08	1.06	
Human Resources Training / Awareness	HRS-09	1.06	
Human Resources User Responsibility	HRS-10	1.06	
Identity & Access Management Credential Lifecycle / Provision Management	IAM-02	1.14	
Identity & Access Management Policies and Procedures	IAM-04	1.14	
Identity & Access Management Segregation of Duties	IAM-05	1.14	
Infrastructure & Virtualisation Security Audit Logging / Intrusion Detection	IVS-01	1.14	4.03
Interoperability & Portability Policy & Legal	IPY-03		3.01 3.04
Interoperability & Portability Standardised Network Protocols	IPY-04		3.01
Security Incident Management, E-Discovery & Cloud Forensics Contact / Authority Maintenance	SEF-01	1.08 1.13	5.05
Security Incident Management, E-Discovery & Cloud Forensics Incident Management	SEF-02	1.08	4.02 4.05 5.02 5.07
Security Incident Management, E-Discovery & Cloud Forensics Incident Reporting	SEF-03	1.08	4.04 4.05 5.04
Security Incident Management, E-Discovery & Cloud Forensics Incident Response Legal Preparation	SEF-04	1.08	3.04 5.04 5.06 5.08
Security Incident Management, E-Discovery & Cloud Forensics Incident Response Metrics	SEF-05	1.08	

Control Domain	CCM V3.01 Control ID	Governance	Lifecycle
Supply Chain Management, Transparency and Accountability Data Quality and Integrity	STA-01	1.11	3.06
Supply Chain Management, Transparency and Accountability Incident Reporting	STA-02		3.04 4.04 4.05
Supply Chain Management, Transparency and Accountability Provider Internal Assessments	STA-04		6.02
Supply Chain Management, Transparency and Accountability Supply Chain Agreements	STA-05		3.05 3.06
Supply Chain Management, Transparency and Accountability Supply Chain Governance Reviews	STA-06		3.04
Supply Chain Management, Transparency and Accountability Supply Chain Metrics	STA-07		3.04
Supply Chain Management, Transparency and Accountability Third Party Assessment	STA-08	1.11	
Supply Chain Management, Transparency and Accountability Third Party Audits	STA-09	1.11	3.04 6.02

Table 20: Mapping between the CCM and the cloud accountability control frameworks.

In order to elicit the accountability metrics corresponding to the AMM controls, A4Cloud contributed with the following methodological approach:

1. Conceptual analysis. The first step is the modelling and decomposition of accountability attributes into simpler properties. In order to do this we use the A4Cloud Metamodel for Accountability Metrics, which enables for a top-down decomposition of attributes and the identification of practices and mechanisms that support accountability.
2. Analysis of control frameworks. The goal of this step is to select the controls from relevant control frameworks that can influence accountability. This analysis allows us to identify assessable factors.
3. Definition of metrics. The assessable factors identified by the analysis of the controls leads us to define metrics for them.

Applying the previously described approach, the A4Cloud project elicited a total of 39 accountability metrics (cf.
Table 21).

Metric	Name	T	V	Rem	R
	Verifiability and Compliance				
1	Authorised collection of personal data		X		
2	Privacy Program Budget		X		
3	Privacy Program Updates		X		X
4	Periodicity of Privacy Impact Assessments for Information Systems		X		
5	Number of privacy audits received	X	X		
6	Successful audits received	X	X		
7	Record of Data Collection, Creation, and Update		X		
8	Data classification		X		
9	Coverage of Privacy and Security Training		X		
10	Account of Privacy and Security Training		X		
11	Level of confidentiality		X		
12	Key Exposure Level		X		
13	Data Isolation Testing Level		X		
	Transparency, Responsibility and Attributability				
14	Type of Consent	X			

Metric	Name	T	V	Rem	R
15	Type of notice	X			
16	Procedures for Data Subject Access Requests	X			
17	Number of Data Subject Access Requests	X			
18	Responded data subject access requests	X			
19	Mean time for responding Data Subject Access Requests	X			
20	Readibility (Flesch Reading Ease Test)	X			
21	Rank of Responsibility for Privacy				X
22	Certification of acceptance of responsibility				X
23	Frequency of certifications		X		X
24	Log Unalterability		X		
25	Identity Assurance		X		
26	Mean time to revoke users				X
	Remediability and Incident Response				
27	Mean time to respond to complaints	X		X	
28	Number of complaints	X		X	
29	Reviewed complaints	X		X	
30	Number of privacy incidents	X			
31	Coverage of incident notifications	X		X	
32	Type of incident notification	X		X	
33	Privacy incidents caused by third parties	X		X	
34	Number of Business Continuity Resilience (BCR) plans tested		X	X	
35	Maximum tolerable period for disruption (MTPD)			X	
36	Sanctions	X		X	
37	Incidents with damages	X		X	
38	Total expenses due to compensatory damages	X		X	
39	Average expenses due to compensatory damages	X		X	

Table 21: Catalogue of accountabiliy metrics. Legend: (V)erifiability, (T)ransparency, (R)esponsibility, (Rem)ediability.

Based on the developed accountability metrics, in
Table 22 the specific set associated with the elicited CSA CCM controls that map to the Accountability Attributes is shown.

Control group	Control name (CCM v3.01)	Control code	Accountability Metric
Business Continuity Management & Operational Resilience	Business Continuity Testing	BCR-02	Metric 34. Number of Business Continuity Resilience (BCR) plans tested
	Impact Analysis	BCR-09	Metric 35. Maximum tolerable period for disruption (MTPD)
	Management Program	BCR-10	n/a
Change Control & Configuration Management	Unauthorised Software Installations	CCC-04	n/a
	Production Changes	CCC-05	n/a
Data Security & Information Lifecycle Management	Classification	DSI-01	Metric 8. Data classification
	Data Inventory / Flows	DSI-02	n/a. Metric 7. Record of Data Collection, Creation, and Update
Datacentre Security	Asset Management	DCS-01	n/a
Encryption & Key Management	Entitlement	EKM-01	Metric 11. Level of confidentiality Metric 12. Key Exposure Level
	Key Generation	EKM-02	n/a
Governance and Risk Management	Management Support/Involvement	GRM-05	n/a

Control group	Control name (CCM v3.01)	Control code	Accountability Metric
Identity & Access Management	Credential Lifecycle / Provision Management	IAM-02	Metric 25. Identity Assurance Metric 26. Mean time to revoke users
	Trusted Sources	IAM-08	n/a
	User Access Authorisation	IAM-09	n/a Metric 16 Procedures for Data Subject Access Requests Metric 17 Number of Data Subject Access Requests Metric 18 Responded data subject access requests Metric 19 Mean time for responding Data Subject Access Requests
	User Access Reviews	IAM-10	n/a
	User Access Revocation	IAM-11	Metric 26. Mean time to revoke users
	User ID Credentials	IAM-12	n/a
	Utility Programs Access	IAM-13	n/a
Infrastructure & Virtualisation Security	Audit Logging / Intrusion Detection	IVS-01	n/a
Security Incident Management, E-Discovery & Cloud Forensics	*Incident Management*	SEF-02	n/a
	Incident Reporting	SEF-03	Metric 22. Certification of acceptance of responsibility Metric 23. Frequency of certifications Metric 27 Mean time to respond to complaints Metric 28 Number of complaints Metric 29 Reviewed complaints
	Incident Response Legal Preparation	SEF-04	Metric 31. Coverage of incident notifications Metric 32. Type of incident notification Metric 33. Privacy incidents caused by third parties Metric 39. Average expenses due to compensatory damages
Supply Chain Management, Transparency and Accountability	*Data Quality and Integrity*	STA-01	n/a
	Incident Reporting	STA-02	Metric 36. Sanctions Metric 37. Incidents with damages

Control group	Control name (CCM v3.01)	Control code	Accountability Metric
			Metric 38. Total expenses due to compensatory damages
	Provider Internal Assessments	STA-04	n/a
	Supply Chain Agreements	STA-05	Metric 31. Coverage of incident notifications Metric 32. Type of incident notification Metric 33. Privacy incidents caused by third parties
	Supply Chain Governance Reviews	STA-06	n/a
	Supply Chain Metrics	STA-07	n/a
	Third Party Assessment	STA-08	n/a
	Third Party Audits	STA-09	n/a
Threat and Vulnerability Management	Anti-Virus / Malicious Software	TVM-01	n/a

Table 22: Metrics associated with the CSA CCM controls related to accountability.

As a final step, the CSA EA (Cloud Reference Architecture developed by CSA) can be also mapped to the resulting set of CSA CCM v3.01 controls related to accountability attributes. The results are presented in the following table.

A4Cloud AMM		CSA EA		
Control name (v3.01)	**Control code**	**Domain**	**Container**	**Capability**
Business Continuity Testing	BCR-02	BOSS	Operational Risk Management	Business Continuity
Impact Analysis	BCR-09	ITOS	Service Delivery	Information Technology Resiliency - Resiliency Analysis
Management Program	BCR-10	SRM	Policies and Standards	Operational Security Baselines
Unauthorised Software Installations	CCC-04	ITOS	Service Support	Configuration Management - Software Management
Production Changes	CCC-05	ITOS	Service Support	Release Management
Classification	DSI-01	BOSS	Data Governance	Data Classification
Data Inventory / Flows	DSI-02	BOSS	Data Governance	Handling / Labelling / Security Policy
Asset Management	DCS-01	ITOS	Service Support	Configuration Management - Physical Inventory
Entitlement	EKM-01	SRM	Cryptographic Services	Key Management
Key Generation	EKM-02	SRM	Cryptographic Services	Key Management
Management Support/Involvement	GRM-05	SRM	Governance Risk & Compliance	Compliance Management
Credential Lifecycle / Provision Management	IAM-02	SRM	Policies and Standards	n/a

A4Cloud AMM		CSA EA		
Control name (v3.01)	**Control code**	**Domain**	**Container**	**Capability**
Trusted Sources	IAM-08	Information Services	User Directory Services	Active Directory Services, LDAP Repositories, X.500 Repositories, DBMS Repositories, Meta Directory Services, Virtual Directory Services
User Access Authorisation	IAM-09	SRM	Privilege Management Infrastructure	Identity Management - Identity Provisioning
User Access Reviews	IAM-10	SRM	Privilege Management Infrastructure	Authorisation Services - Entitlement Review
User Access Revocation	IAM-11	SRM	Privilege Management Infrastructure	Identity Management - Identity Provisioning
User ID Credentials	IAM-12	SRM	Policies and Standards	Technical Security Standards
Utility Programs Access	IAM-13	SRM	Privilege Management Infrastructure	Privilege Usage Management - Resource Protection
Audit Logging / Intrusion Detection	IVS-01	BOSS	Security Monitoring Services	SIEM
Incident Management	SEF-02	ITOS	Service Support	Security Incident Management
Incident Reporting	SEF-03	BOSS	Human Resources Security	Employee Awareness
Incident Response Legal Preparation	SEF-04	BOSS	Legal Services	Incident Response Legal Preparation
Data Quality and Integrity	STA-01	SRM	Governance Risk & Compliance	Vendor Management
Incident Reporting	STA-02	ITOS	Service Support - Incident Management	Cross Cloud Incident Response
Provider Internal Assessments	STA-04	SRM	Governance Risk & Compliance	Vendor Management
Supply Chain Agreements	STA-05	BOSS	Legal Services	Contracts
Supply Chain Governance Reviews	STA-06	SRM	Governance Risk & Compliance	Vendor Management
Supply Chain Metrics	STA-07	ITOS	Service Delivery	Service Level Management - Vendor Management
Third Party Assessment	STA-08	SRM	Governance Risk & Compliance	Vendor Management
Third Party Audits	STA-09	BOSS	Compliance	Third-Party Audits
Anti-Virus / Malicious Software	TVM-01	SRM	Infrastructure Protection Services	Anti-Virus

Table 23. Mapping the AMM to CSA's Cloud Reference Architecture (CSA EA)

5 Cloud Accountability Architecture

In section 5.1 we extend the NIST cloud reference architecture conceptual model [5] with accountability.

In section 5.2 we then identify the accountability support services to be implemented by cloud providers in order to exchange the accountability artifacts (cf section 5), and discuss the specifics of each service.

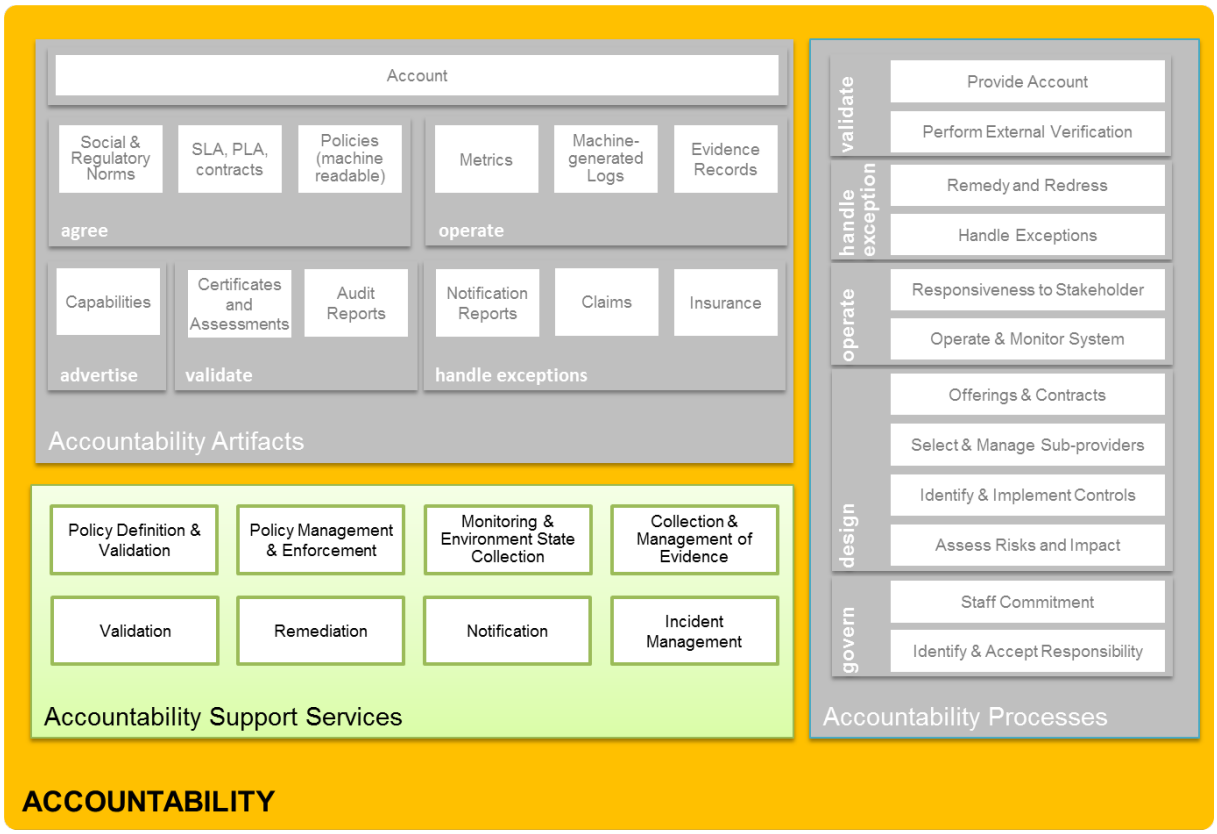


Figure 20: Accountability reference framework – support services.

In section 5.3, we offer a practical approach to the adoption of the Accountability Framework by identifying patterns, which respect to the integration of A4Cloud approach to the existing capabilities of a cloud environment and the adoption of this approach by the identified stakeholders.

5.1 Conceptual Model of the Reference Architecture (RA)

With the essential actors and roles necessary to describe accountability relationships identified, the building blocks of the RA model can now be examined. Again, emphasising the importance of building upon established and standardised concepts instead of “re-inventing the wheel”, we base the RA conceptual model on the corresponding NIST cloud reference architecture conceptual model [5]. Figure 21 below illustrates how the RA adapts and extends the NIST cloud reference architecture to support accountability.

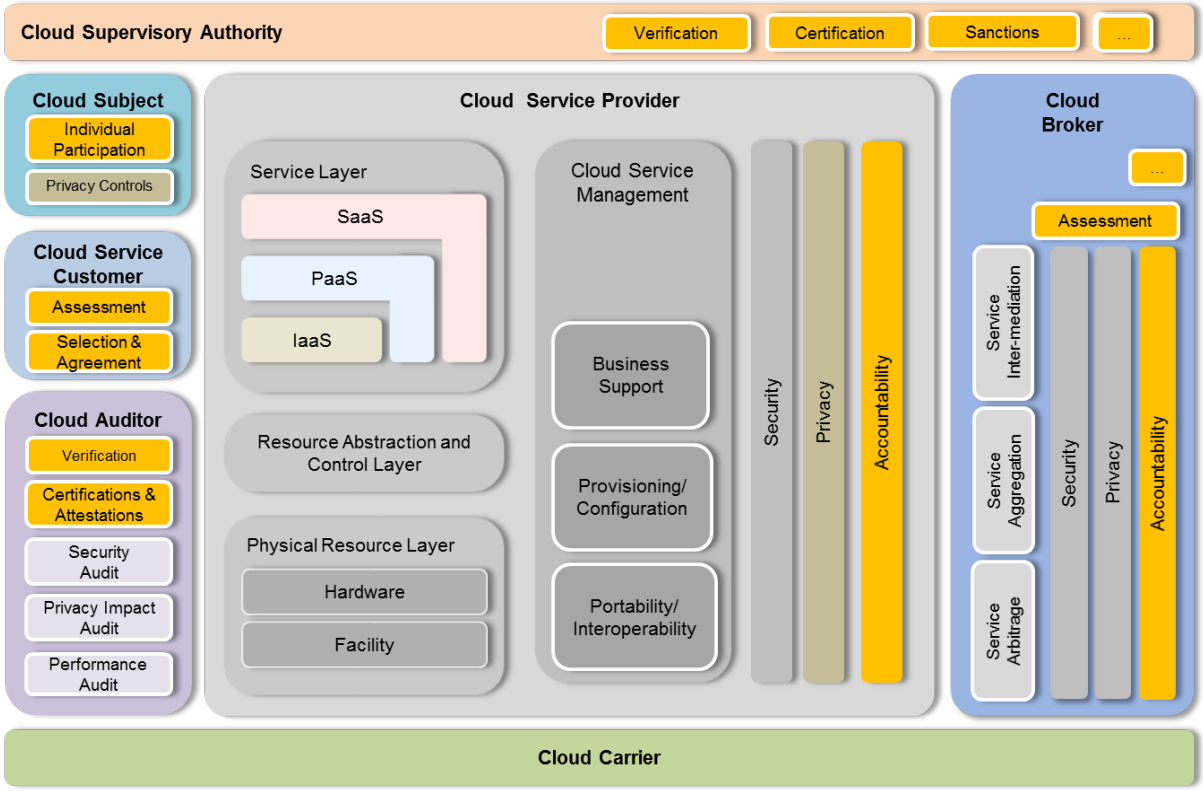


Figure 21: A4Cloud reference architecture conceptual model.

Our amendments to the NIST RA can be organised into three different classes:

- *Actors*: the focus on accountability for data protection has led us to add two actors those identified by NIST: the cloud subject and the cloud supervisory authority (refer to section 2.1 for details).
- *Architectural Components*: We have introduced a third cross-cutting aspect of the architecture: accountability. We have elected to add accountability as a separate aspect as it is not restricted to any particular cross-cutting aspect already identified. Indeed, cloud providers are typically held accountable for performance and availability, security, and data protection, making accountability cross-cutting other cross-cutting concerns. The NIST diagram does not show explicitly the security and privacy aspects for the cloud broker. We believe NIST did not intend to exclude these aspects for that actor and have consequently introduced these aspects alongside accountability as concerns, mirroring what is done for the cloud service provider.
- *Stakeholder Functions*: Actors perform selective functions corresponding to their roles in the cloud ecosystem. NIST lists a few such functions for cloud auditors; we have identified the key accountability functions for the various actors acting as accountees. More specifically:
    - *Cloud Auditors*: as part of their audit responsibilities, cloud auditors perform the verification of the accountability claims of accountors (cloud service providers and cloud brokers in this architecture). The auditors are also in charge of evaluating compliance to certification and attestation schemes related to accountability, such as ISO 27001, SOX2, or CSA STAR Certification.
    - *Cloud Customers*: before using cloud services, cloud customers go through a selection and agreement process during which they select a suitable CSP for their needs. The also assess the suitability of the CSP to their needs based on the accountability information provided.
    - *Cloud Subjects*: in regards to data protection, the relationship between the data (cloud) subject and the data controller (cloud service customer or provider, depending on the solution architecture) goes beyond one where the customer provides statically requirements *up-front*; accountability principles recognise the importance of the

dialogue (under the form of an individual participation) between the data subject and the data controller, where the data subject has the ability to issue queries to the data processor, requesting explanations and clarification of how its data is protected, and with the ability to clarify its requirements in terms of data handling requirements.

- *Cloud Supervisory Authority*: in the context of data protection regulations, the DPA has the ability to verify, investigate, and to issue sanctions against data controller and processors when they are not in compliance with the regulations.
- *Cloud Brokers*: the NIST RA identifies a variety of services provided by the Cloud Broker. In its role as an intermediate between the Cloud Customer and the CSP, the broker must assess how accountable the CSP is to its accountees.

In the remainder of this section we will focus on the accountability part of the architecture. We start by describing a service-oriented approach for accountability which enhances cross-domain interactions between the architecture components. We then list a set of capabilities that need to be implemented to achieve accountability. These capabilities (e.g., policy definition, incident management) could be viewed as autonomous building blocks that interact with each other to perform common goals.

5.2 **Service-Oriented Approach for Accountability in the Cloud**

In section 2.3 it was established that cloud service provision chains are composed from heterogeneous elements which reside in separate control, trust and ownership domains. This creates challenges to establishing accountability across the chain, as strong accountability cannot be achieved without cross-domain access to certain controls and views of information, typically only available to the administrative entities inside each domain. To overcome this problem we have identified in section 2.4 a set of accountability artifacts that can be exchanged across domain boundaries to support accountability in a controlled manner without interfering with the structural properties of the boundaries themselves.

This approach achieves two critical goals:

1. It promotes a model for accountability across cloud provisioning chains which is pragmatic, technology-agnostic and does not make unrealistic assumptions about the cloud environment. By developing a framework for evaluating accountability based only on the exchange of information in the form of accountability artifacts instead of requiring changes in the way clouds are architected, the desirable properties of cloud computing that emerge from the ability to flexibly compose services and abstract lower-level complexity are fully preserved. Overall accountability is achieved by establishing accountability over each direct service relationship formed.
2. It does not dictate a “one-size-fits-all” approach. Every cloud actor can individually apply the accountability governance process in the way that makes sense to their business domain, organisational setup, capabilities and resources, as long as they can provide (and operate on) the required accountability artifacts in an interoperable way.

Accountability attributes can be generated via multiple combinations of potentially already-in-place and purpose-built systems and workflows of operations (e.g. existing logging systems re-configured to provide accountability-supporting machine-generated logs). In the A4Cloud Accountability RA we propose a technology-agnostic service-oriented approach to carry out the accountability functions and generate (or compile) and exchange the accountability artifacts. As illustrated in Figure 22, sets of services collectively designated as “accountability support services”, are operated internally by the various actors involved in a cloud service provisioning chain to support each actor’s primary operations by generating (or compiling) at the various phases of the lifetime of a service the necessary accountability artifacts that can be allowed to traverse control domain boundaries.

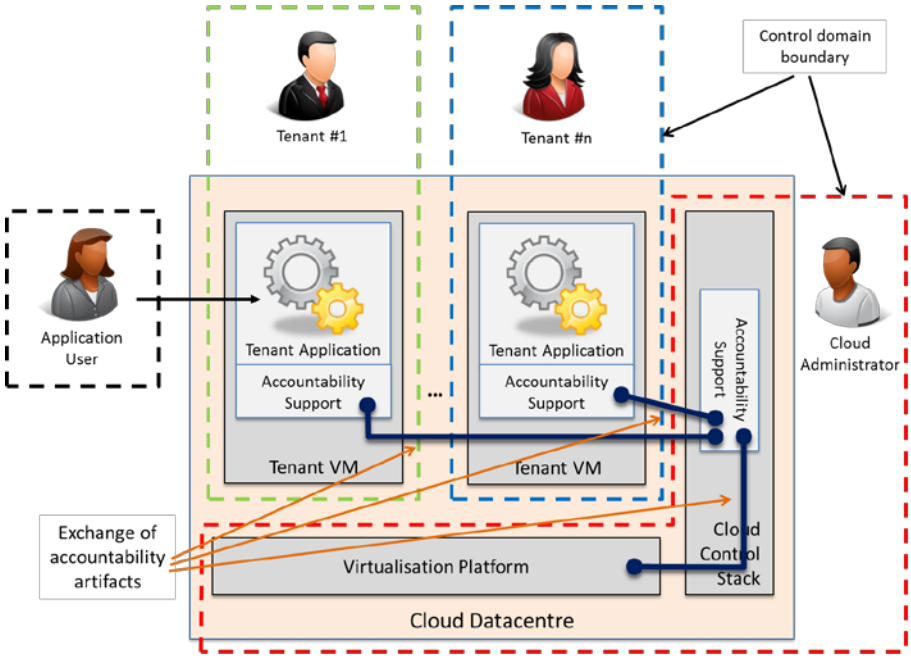


Figure 22: Supporting accountability via a service-oriented approach.

The A4Cloud RA does not dictate specific implementation requirements for the accountability support service model. Instead, we have identified a set of capabilities which participants must implement and integrate with their systems in a context-specific manner to develop the accountability support service suite that is suitable for their environment.

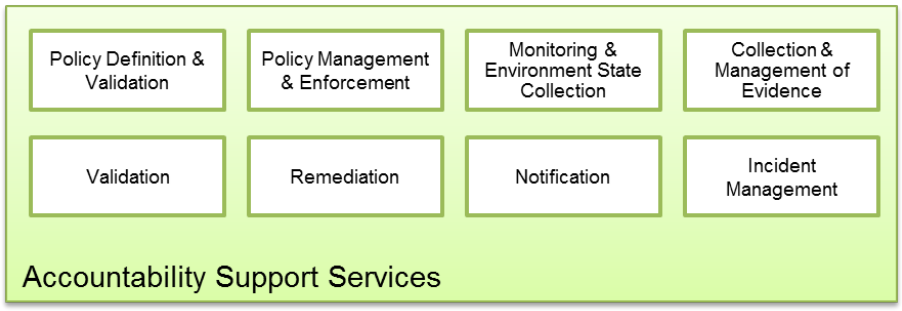


Figure 23: Accountability support services.

As illustrated in
Figure 23, the RA Accountability Support Services are shown and then defined in
Table 24:

Accountability Support Service	Brief description
Policy definition and validation	Systems that enable and facilitate the definition and configuration of policies and validate that policy terms have been extracted properly from higher-level, human-readable documents such as SLAs, PLAs and contracts.
Policy management & enforcement	Enforcement covers systems that ensure operations (such as handling of data) are performed exclusively according to defined policies. Management covers systems that support the lifecycle of policies themselves, such as versioning, editing, testing, updating and deleting.

Accountability Support Service	Brief description
Monitoring & environment state collection	Systems that monitor, collect and store information on the state and operation of the various systems and components that comprise a particular cloud service.
Collection & management of evidence	Systems that collect and compile evidence records about the state and operation of designated elements of a cloud service, and manage their full lifecycle according to specific integrity, confidentiality and access control requirements.
Incident management	A collection of systems tasked with supporting and coordinating the incident management process. The exact capabilities and level of integration of systems comprising this accountability support service will vary between organisations but at the very least they will include functions such as recording and tracking incident management cases, compiling and processing information obtained from various databases and data stores (including monitoring data and evidence records), updating status of various processes and managing the content of notifications.
Notification	Systems that enable the formation, population and transmission of notification reports to authorised parties.
Remediation	Systems that assist in compiling and communicating remediation options to affected parties.
Validation	Systems that validate the extent of the ability of the systems (and their configurations) in place to support accountability assertions.

Table 24: Accountability support services.

The rest of this section will focus on analysing these classes of accountability support services in more detail.

5.2.1 Policy Definition and Validation

In general terms, policies in IT systems specify sets of rules related to a particular purpose, such as defining the security credentials one must possess to access a particular data object and the actions to be taken under various conditions. In the scope of the A4Cloud policy representation framework [46], the obligations an organisation must fulfil and hence express in policies are classified as follows:

- **Data handling obligations**: policies should express which rights should be granted or revoked regarding any action taken on the data in cloud infrastructures including its access, its distribution to third parties and its deletion. Such data handling rules should not only support the definition of roles as specified in the Data Protection Directive, e.g. data controller and data processor but should also capture data subjects' preferences, express time and location constraints (ie. data retention periods).
- **Logging and monitoring obligations**: accountability policies should express the rules defining the way to verify compliance with data handling obligations. These include the rules specifying which events have to be logged what information should be part of the logs. Such rules enable the auditability of the different actors in the accountability chain. The policies should also incorporate notification rules which will enable cloud providers to notify end-users and cloud customers in case of policy violation or incidents, for instance.
- **Incident management obligations**: policies should also express recommendations for redress in the policy in order to define the set of actions that need to be taken to handle or recover failures.

Organisations that are subject to obligations need not only to meet their obligations, but also to ensure that their business partners and sub-contractors do not invalidate them. In particular, an accountable organisation needs to make sure that their obligations to protect personal data are adhered to all across the service provisioning chain.

An important aspect of governance in an accountable organisation is to define and deploy policies for their data processing practices and to make sure that they are followed by all the involved service providers. The policies should ideally travel with the data, and they should be used as input to monitoring of data processing practices, to generate evidence that policies are fulfilled, to correct policy violations that may occur and in general to demonstrate policy compliance.

Therefore, an accountability-based approach requires services via which to express accountability obligations using a common policy specification language (or standard interoperable policy specification languages) and to distribute them throughout the cloud provisioning chain. An additional component of policy definition support is the checking of compliance between the original obligation or law and the actual set or rules and actions defined in the policy.

In an accountability policy framework, the cloud customer must define the high-level data-handling requirements and obligations in human readable language. These rules should further be translated into machine-readable policies. These policies can be communicated and agreed with potential cloud providers.

If the cloud provider uses subcontractors, then it must check the conformance of the cloud customer policy with the practices of the actors further down the chain. In
Figure 24 we illustrate a cloud service chain. The SaaS provider must propagate *Policy 1* from the cloud customer to an adapted form to manage the resources it uses from its subcontractor. Hence, a machine-readable policy language helps in the definition and verification of these dependencies.

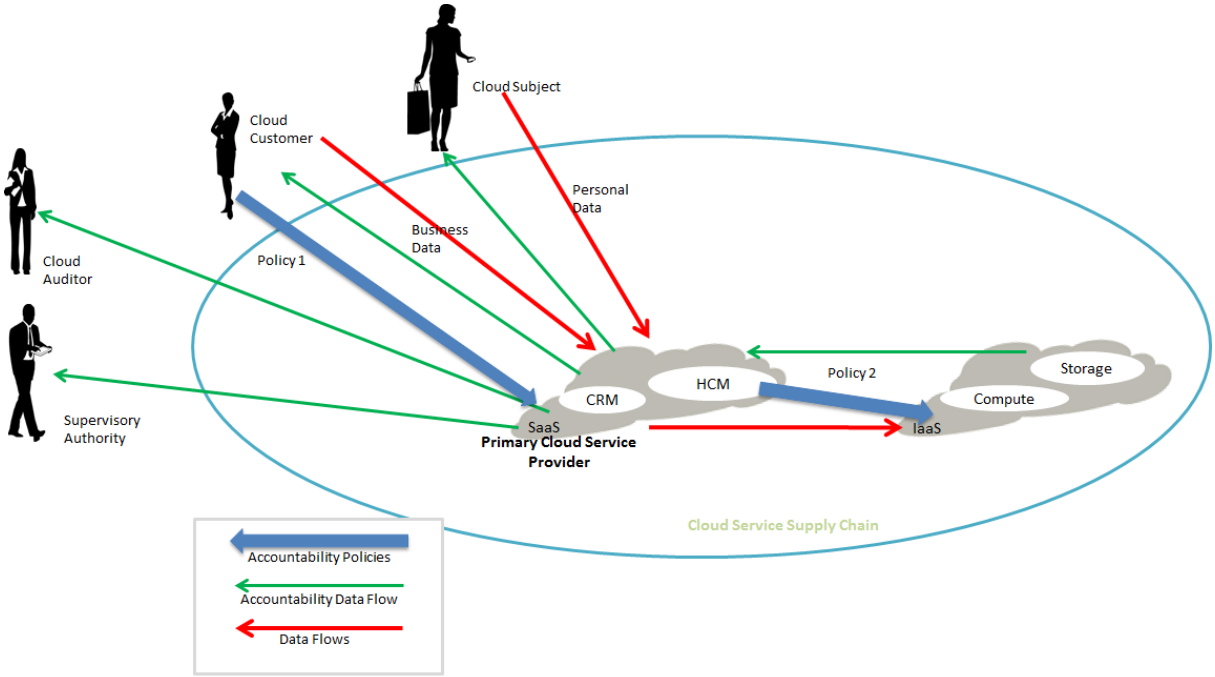


Figure 24: Accountability policy distribution and data flows.

However the framework should be flexible enough to accommodate further source and target languages. For instance, the Privacy Level Agreement (PLA[66]) is emerging as a federating initiative to make cloud privacy statement declarations clearer and to allow the assessment of the level of privacy disclosure associated with a given service.

5.2.2 Policy Management and Enforcement

Once policies are expressed into machine readable format, an accountable system should implement an automated enforcement framework in order to fulfil the requirements defined through policy rules.

[66] https://cloudsecurityalliance.org/research/pla/.

According to the nature of the obligations, different enforcement mechanisms can be integrated within this framework. This section first discuss the main components of the enforcement framework and further suggests some relevant enforcement techniques.

A policy enforcement framework should at least define two main components: the Policy Control Point (PCP) where policies are defined and decisions are taken, and, the Policy Enforcement Point (PEP) which enforces policies through different technologies. The PCP first maps each policy rule to a specific set of actions/operations and takes decisions on when and how to perform such operations. The PEP executes the actions upon PCP's decisions (such as data handling operations based on access control decisions) or continuously monitor some events (logging).

The PEP can implement different enforcement techniques: while preventive solutions such as privacy based access control solutions are implemented to meet data handling obligations, detective solutions help in order to verify the compliance with such data handling obligations. Specifically:

- **Privacy enhanced data access control**: personal data can be protected through well configured privacy-enhanced solutions. While encryption techniques become mandatory for the protection of the data stored in the cloud, a well-defined access control framework combined with a secure identity management system will help to meet data handling obligations. The new enforcement framework should also allow data subjects to have full access over their data (read, update, delete). Another way to enforce such rules is to implement sticky policies whereby rules and constraints travel with the data. This is especially beneficial in a cloud environment where data can travel.
- **Monitoring/logging solutions**: ensuring compliance with respect to data handling obligations is not always an easy task; the enforcement framework should therefore implement some dedicated logging solutions. There is a specific need for data transfer monitoring since controlling the location of data can remain difficult; data transfer monitoring tools may help to discover unexpected events. The integrity of logs is considered as the critical functionality of a secure logging solution.

Reliable policy enforcement requires a number of trust assumptions to be made:

- The cloud service provider wants to demonstrate accountability at a reasonable cost, therefore it would have no interest to tamper with the accountability enforcement engine.
- Access to personal data will not circumvent the accountability enforcement engine. Note that the engine by itself cannot guarantee this, since it cannot control the entire environment it is part of (operating system, network, etc).
- Further providers in the cloud service chain provide assurance about the security and privacy procedures and controls such that data subject rights can be guaranteed.

5.2.3 Monitoring and Environment State Collection

The ability to collect evidence of the events and actions that take place inside a cloud environment is absolutely reliant on the ability to observe and monitor the state of all systems that operate in this environment. Clearly, this requires that all systems are instrumented and monitored so that information about their state and inner workings is extracted and made available for analysis at various levels of granularity. Because most cloud services are implementation-specific and involve customisations, we do not propose a specific architecture for environment state information collection services. Nonetheless, we assume that capabilities to monitor the state of the cloud environment are in place.

Using the Cloud Trust Protocol (CTP)

The Cloud Trust Protocol (CTP) is a project currently being developed by CSA (a partner in A4Cloud). It aims to create a RESTful Application Programming Interface (API) that will allow cloud customers to query cloud providers about the security/privacy/compliance level of their service in near real-time. In the next paragraph, we analyse the potential use of this new tool for the purpose of providing the "account".

It should be highlighted that CTP does not define a monitoring architecture or framework but only defines an API to present the result of the monitoring in a standardised way.

In CTP the level of security of a cloud service is expressed through the measurement of "security attributes", which apply to "cloud resources". More precisely, CTP has adopted the following data model:

- A cloud service is divided into a set of resources (e.g. a VM, an API call, a database)
- Each resource has a set of attributes (e.g. "uptime", "confidentiality at rest", "incident response performance")
- Each attribute has a set of measurements, where a measurement is a process that enables to quantify or qualify an attribute, according to a specific metric (e.g. "percentage of failed requests per hour").
- Each measurement produces a value called "measurement result" (e.g. "99.98637 % / hour")
- Each measurement can also be associated with an objective, which represents what is typically described in a SLA by describing a constraint on the measurement result (e.g. "result > 99.95 % / month")

This data model enables cloud customers to get precise information about the security level of a service, and compare these levels with the security objectives that have been defined by the provider (provided of course that the provider is willing to provide a valuable set of attributes and measurements). In addition to these elements, the CTP API also proposes:

- *Triggers*: these are conditions (like objectives) that will generate an alert, sent to the customer.
- *Logs*: logs that are stored by the provider, for each trigger event.

With the high-level presentation of CTP we can examine how closely it can be related to the notion of the account. First, we can observe that:

- By construction, CTP triggers provide a mechanism to be notified of events, whether these events are "legitimate" or "incidents" depends solely on the choice of the trigger conditions formulated by the customer. CTP triggers and logs therefore provide a vehicle for *'a report or description of an event',* which defines the notion of the account (see 4.1).
- CTP "objectives", which describe obligation of the organisations, are closely linked to the notion of "proactive report".
- The account is expected to answer a certain number of question: notably who, what, where and when. By construction, the CTP data model:
    - Provides clear identification of "who" (via service-units).
    - Describes partially "what" through measurement results, but does not identify "root cause"
    - Describes "where" in the sense of identifying the "resources" to which attributes apply. Moreover "location" can be an attribute of a resource in itself.
    - Describes when through timestamps.
- The CTP standards envision explicitly the possibility to add a digital signature to measurement results, though this feature is not standardised at the time of writing.

However, we can also argue that CTP is not designed to present all the features that are expected of an "account" in the sense defined in A4Cloud:

- CTP does report "evidence" in the strict sense but only "results". Logs in CTP only allow deduction of the fact that a result failed to match a condition but they do not provide support for the results themselves.
- CTP does not describe actions taken to deal with an incident, but only describe that the incident occurred.

One last aspect to consider is that CTP targets mainly security/privacy attributes that can be minored in an automated way. This does not cover all elements that an organisation should monitor as part of an accountable process.

In summary, the CTP API can be used by organisations as a tool to provide an "account" of technical and measurable attributes related to security, privacy and compliance in general. However, the CTP API does not provide a mechanism to support the presentation of evidence in relation with incidents but only a mechanism to report that a specific incident occurred.

5.2.4 Collection and Management of Evidence

The provision of evidence is an essential element of an accountable system, enabling demonstration, verification and the construction of the account, while motivating and guiding a range of other functions and procedures important for accountability. Evidence contributes to the detective controls inherent to accountable systems. In particular, it supports the account by providing arguments to show whether policies, norms and regulations are satisfied at any stage of the service delivery. Therefore, the A4Cloud project proposes an account-oriented definition of accountability evidence: "*a collection of data, metadata, and 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 convince a third party of the veracious (or not) functioning of an observable system*" [47].

As shown in
Figure 25, the project determines three verification levels where accountability evidence should be provided in order to verify the correct operations of the system:

- *Organisational policies*: At this layer, evidence supports the correct definition of policies for the context.
- *Mechanisms and procedures*: This involves the provision of evidence that appropriate mechanisms and controls are deployed in accordance with the obligations defined at the policy layer.
- *Operational practices:* The evidence from this level should reflect that operations (what is actually happening) satisfy the requirements expressed in the policies (what is supposed to be happening). This may need continuous monitoring, recording and analysis of the activities in the service delivery.

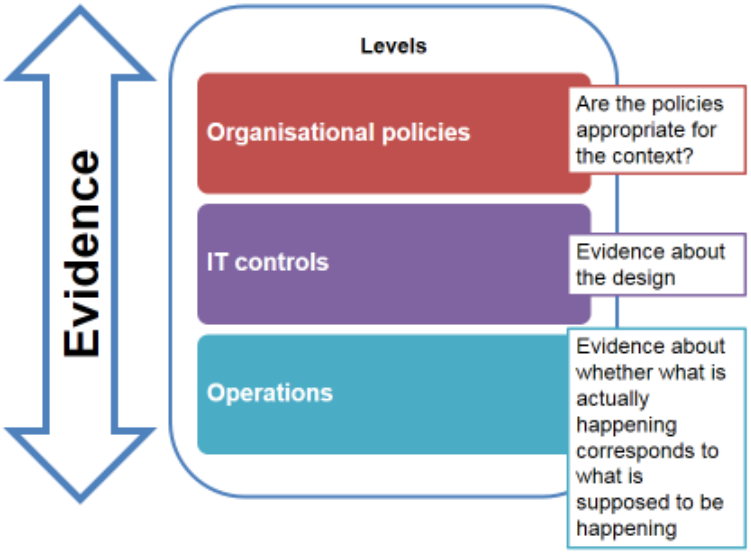


Figure 25: Accountability evidence.

In line with the above levels, the project identifies the following five major types of evidence relevant for accountability:

- **Data processing practices**: evidence of operational practices such as replication, storage, deletion, copy, access, optimisation, consent, security, segregation, proofs of retrievability, etc.
- **Data collection practices**: evidence of data collection practices such as policy compliance, privacy issues, security breaches, etc.
- **Notification**: evidence that notifications were sent to the interested stakeholders in case of privacy issues (unauthorised access, etc.), policy violations, security breaches (data leakage, data lost, corrupted or tampered, etc.) and services or policy modifications, as well as service practices and users rights;

- **Remediation**: evidence related to remediation to customers in case of security breaches, privacy issues and policy violations.
- **Organisational practices**: evidence of requirements related to employees' training, system certifications, privacy policies, etc.

The provision of evidence is a complex process that entails: identification, association and collection of information that will constitute evidence from various sources; processing and use of cryptographic techniques to ensure integrity; secure storage; and presentation for the various different stakeholders, auditors and regulators. Specifically, the process must be designed in such a way as to:

- Give account of events and occurrences within the services of cloud providers in a non-invasive manner to the customers' privacy and without exposure of sensitive material from the inside of organisations;
- Ensure information is collected securely in a tamper-evident process, which however may allow verification checks from different services, tools and trusted third parties (e.g. auditors);
- Avoid excessive data collection, minimising privacy issues and ensuring scalability of evidence storage with time, even with growing user bases and multi-tenancy scenarios.

To address this challenge the A4Cloud project has designed a Framework of Evidence (FoE) consisting of a set of mechanisms for extracting evidence in typical scenarios encountered in cloud services and managing their full lifecycle [47]. The FoE provides automated support to all the phases of the evidence lifecycle: monitoring, collection, storage, verification and presentation. The FoE considers four main types of sources:

- Internal data as logs, metadata SIEM outputs, etc., collected from monitored operations and services;
- Data from end-users or from a cloud service to another, or internal data as customers' or employees' lists, training certificates, seals, etc.;
- Documentation of the service's practices, contracts and organisational policies that relate to accountability and for which implied obligations can be expressed (manually or by other A4Cloud tools like AccLab or COAT – discussed later in the document) in machine-readable policies;
- Cryptographic proofs that are generated upon request at a particular point of time.

Using the FoE, the collected and processed evidence are assembled and stored as *records*. These records contain elements supporting a claim such as the actions that the evidence records, a timestamp, the identity of the authenticated agent that performed the recorded action and a reference to the policy that the action may or may not comply with. Among the supporting elements included in the records, audit logs and cryptographic proofs are of particular interest in the proposed Framework of Evidence. Audit logs provide documentary evidence of a sequence of events, actions and changes observed in the accountable service. They support the occurrence (or not) of an operation and demonstrate compliance or non-compliance with the policies. Audit logs must be protected against adversarial tampering or deletion to provide a non-disputable record of events. Logs also enforce the correct system behaviour since the latter is held accountable for the events, changes and actions that are logged in the audit logs. Cryptographic proofs provide an instantaneous assurance of correct (or not) behaviour of the accountable system, verifiable at any point of time. They are intended to convince any entity verifying them that the system provides the appropriate safeguards when processing and storing data. As an example of such proofs, in the project we focus on a particular cryptographic proof of storage called proofs of retrievability. They ensure with high probability that the accountable system stores the outsourced data as expected in policies, contracts and regulations and that this data is retrievable at any point of time.

Evidence contributes to account definition, attribution of responsibilities and policy violation reports.

Therefore, to support accountability across the provisioning chain, services providing the following high-level functions need to be provided for evidence provision:

- Support for the extraction of evidence targets (i.e. what to monitor, when, etc.) from policies, ensuring compliance and full coverage (i.e. no obligations described in policies are left unmonitored);
- Support for collection of logs from different sources and parts of the infrastructure;

- Support for full lifecycle of evident management (i.e. mechanisms to extract, assemble, secure, store evidence, etc.), ensuring privacy, integrity, verifiability;
- Support for enforcing access rights with regard to evidence;
- Support for context-specific presentation of evidence to different parties possessing different access-rights and privileges.

Evidence also supports elements for the provision of the account. The C-2 conceptual framework [1] defines three types of accounts that can be provided. We outline here some examples of evidence that can be provided to support these three different types of accounts:

- *Proactive account*: This kind of account may report the quality and security levels of the services provided by the cloud. Evidence in this case may consist of certification of the compliance of the offered data processing and storage services with regulations and contracts. The certificates should designate the party that provides the service, the issuer of the certificate, the validity period of the certificate, the level of security guaranteed by the certified service, etc. Additionally, proactive accounts can be supported by consistency checking reports that act as evidence of contractual obligations agreed between the cloud provider and its customer.
- *Account of compliance*: Evidence should be collected to provide an account of a legitimate event to demonstrate that the cloud provider complies with regulations and contracts. Logs are the most relevant sources of evidence to prove policy compliance. However, the integrity of logs may not be always easy to verify. Hence, there may also be additional cryptographic proofs for some cases such as proofs on data storage: for example, Proofs of retrievability, such as the one presented in [47], are cryptographic proofs that verify whether or not a data storage service actually stores the outsourced data. Collected on a periodic basis, these proofs of retrievability enable an auditor to check the correct storage of the data, meaning that the service stores the data as expected by regulation and contracts. Therefore, the proofs of retrievability can support this kind of account.
- A*ccount of security breach*: In case of the occurrence of an incident, evidence should demonstrate that the fault actually occurred, identify the actors and the environmental settings that lead to the incident, assign time and date to the event, and have a reference to the particular policy rule(s) that the reported event infringes. Logs can be an example of such inculpatory evidence to provide an account in case of an incident and to attribute the responsibility of that incident to a particular actor in the cloud. Indeed, logs report the actions performed by a particular entity and record the identity of that entity and the timestamp corresponding to the reported event.

The RA does not prescribe a specific method for providing an account, recognising that in many cases the form and contents of the account as well as the context of its provision are specific to the particular circumstances of the actors involved. For example, a particular account may consist of highly structured and annotated information allowing it to be transmitted electronically in an automated fashion, or may be an e-mail containing textual information that is not organised in a specific way.

However, given that the construction and provision of the account requires the provision of evidence, the RA notes that in order to support accountability across the provisioning chain via the construction and provision of the account, actors need to implement the services supporting evidence provision outlined above, as well as implement services supporting context-specific presentation of the account to different parties possessing different access-rights and privileges, in cases where the account can be processed automatically by computers.

5.2.5 Notification

Notification is an essential element of accountability. A strong accountability-based approach requires cloud providers to notify all affected parties of the occurrence of an incident or discovered policy violation within a reasonable timeframe. Notifications can be provided through common means such as e-mail or letters to the relevant parties, or dedicated communication channels designated for the purpose (usually between cloud providers).

The RA does not prescribe particular methods for notification recognising the fact that the circumstances around each incident rarely are the same and flexibility should be allowed in which

mechanisms to mobilise during response. However, the following functions should be implemented for a strong accountability-based approach:

- Obligations about providing notification within a predefined, reasonable timeframe should be reflected in the policies enforced. As such, any policy-support services implemented (discussed in section 5.2.1) should ensure that this element is explicitly supported.
- An automated approach to transmission of notifications can reduce the burden of operating this part of the accountability lifecycle. As such, organisations may opt to implement services supporting the exchange of machine- and human-readable notifications based on a predefined protocol that has provisions for the inclusion of information about the incident (including evidence of which subset of a subject's personal data were involved in the incident) and, where possible, links to an automatic remediation management system, discussed next.

5.2.6 Remediation

Like notification, remediation is also an essential element of accountability, referenced directly by the fourth and final accountability practice in the accountability model presented in section 1. Again, the specifics of a particular remedial action in response to a specific violation depend on the circumstances of the violation itself, and many may be enacted ad-hoc. As such, the RA does not propose a particular mechanism for remediation. We do, however, note that a framework for the systematic addressing of violations and provision of remedies depends on the proper implementation of the accountability-support services described in the previous sections. Specifically, service functions should be in place to facilitate:

- The ability to detail the origin of policy violations in order to provide appropriate responses. Customers need to know whether the policy violation occurred as the result of an attack, a deliberate action by the provider, an unintended alteration or any other means, in order to make an educated decision about the efficacy of the proposed remediation or request additional redress.
- The ability to suggest response actions to ease the process for customers responding to the event. Customers could get assistance from the service provider in performing any necessary step on their part to handle the event. This would include any remediation action deemed appropriate.

Accountability support tools facilitate notification and remediation processes in the cloud. Starting from the filling of complaints towards incident detection (AAS, DTMT), incident handling (IRT), automated notification (A-PPL-E, DT) and remediation and redress, the workflow across these phases and tools can provide much more assurance that corrective actions have been taken in accordance with contracts and regulations.

5.2.7 Data Subject Enablement

The final necessary element for end-to-end support of accountability across cloud provisioning chains is the provision of services aimed at enabling data subjects to consent, control, review and correct their personal data held in the cloud. Unlike all other functions in this section, data subject enablement is not a provider-side accountability support service, but rather is to be provided to the data subject as a separate tool, hosted in an environment hosted by the data subject or a trusted third party. As such, this tool does not appear in
Figure 23 or
Table 24.

Specifically, the Data Subject should be provided with facilities to:

- Provide consent about the use of their data;
- Request from a data controller access to their data stored in the cloud for review;
- Request from a data controller to correct or delete their data stored in the cloud;
- View detailed information about how the data has been shared and used by the data controller;
- Receive notifications of incidents affecting them;
- Receive assistance in requesting remediation and redress.

To support these functions, actors along the chain (excluding data subjects) should therefore implement services that implement the following functions:

- Track and produce evidence of all data uses;
- Provide means for data subjects to view their personal data held, along with meaningful metadata (e.g. time of data disclosure, etc.);
- Provide means for data subjects to amend or request deletion of their personal data held;
- Since almost all data subject controls will only interact with the data controller and not the actual data processors along the provisioning chain, services should be in place to facilitate the passing of data subject requests in an appropriate form to the relevant processors. Clearly, to support this capability the functionality provided by the accountability-support services described in previous sections (such as services to exchange enforceable policies and provide evidence) will be required.

One tool to consider in order to receive information about incidents occurring in the provisioning chain is the Cloud Trust Protocol (CTP). As described in 4.3.4, the CTP can be used to report alerts regarding the measured security level of a service, or more precisely the measured attribute of a specific resource. For example, if the availability of a disk resource falls below a user defined threshold, an alert can be sent to a user. This works also across a provisioning chain where one cloud provider can send an alert to another provider, which in turn sends an alert to another provider. In the case of a provisioning chain, the alerts might change in nature: an availability issue with a disk might become an availability issue with a database for the next provider in the chain. Importantly, CTP is agnostic to the notion of “data subject” and only reports security levels and the resources they affect. CTP is a protocol designed to be used between cloud customers and cloud providers, not between data subjects and providers. As such it is the responsibility of the “customer facing” provider to identify which cloud subjects are affected by an incident and to notify them appropriately.
.

5.3 Integration and Adoption Patterns

This section aims to offer a practical approach to the adoption of the Accountability Framework by identifying patterns, which respect to the integration of A4Cloud approach to the existing capabilities of a cloud environment and the adoption of this approach by the identified stakeholders.

5.3.1 Integration Patterns

In this section, we introduce the concept of integration patterns for accountability, which is inspired by the existing attempts of several software vendors and IT system and solution providers to provide some common ways to facilitate integration in multi-scaled and multi-oriented systems. From an accountability perspective, the integration patterns refer to the interaction of the accountability mechanisms with each other and with the external world. By saying so, we emphasise the need for interoperability among the different layers of a cloud ecosystem in order to achieve accountability, as this is described in the four phases, namely agreement, reporting, demonstration and remediation. The integration patterns may go beyond the strict boundaries of the technical details of an accountability solution and analyse the integration requirements along processes (or even other non-technical mechanisms, such as legal contracts) as well.

In the context of the A4Cloud Reference Architecture, we will introduce the following integration patterns:

- Agreement patterns: this family of patterns analyses the integration patterns to serve the agreement practices of the Accountability Framework and involve:
    - Capability pattern: this pattern integrates the way that the different cloud providers can advertise their offerings, by describing their function, security and privacy provisions to their clients in a structured template.
    - Policy specification pattern: this pattern integrates the various types of data handling procedures that reflect the accountability dimensions of a data protection problem (for example, the specification of data access, data retention or data transfer rules).
    - Policy enforcement pattern: this pattern describes the common functions for a policy decision point.

- Reporting patterns
  - Metrics pattern: this is a pattern to maintain a certain level of conformance along the cloud providers on the appropriate assessment of the environment state. This pattern needs more investigation in the sense that it should be considered from two different perspectives: i) a pattern on metrics description for monitoring, and ii) a pattern on assembling individual metrics patterns for assessing the state of a provider in an aggregated manner (for example the combination of metrics for delivering the accountability maturity score).
  - Log communication pattern: this pattern describes the way that the collected logs are communicated with a specific transformation model to serve an integrated approach for log reasoning and analysis.
  - Incident messaging pattern: this pattern is used to communicate incidents via a point to point approach.
- Demonstration patterns
  - Evidence building pattern: this pattern provides the way to build an evidence shared repository from multi-source log listeners and collectors.
- Remediation patterns
  - Incident response pattern: this pattern defines a communication path for enabling the exchange of incident management and remediation actions.

As an example of the log communication pattern, we consider the actions of the cloud provider which offers the infrastructure. In another case, this infrastructure is based on OpenStack **[48]** and, thus, the relevant pattern refers to the integration of the OpenStack services with the accountability ones to collect the appropriate logs. This integration includes the monitoring and analysis of the events referring to the traffic realised in the OpenStack network and, especially, the Controller Node. An accountability service should implement a pattern to log the events collected in this part of the OpenStack infrastructure and parse these logs to identify the type of actions happened and filter them, based on policies. The pattern should, then, implement a protocol so that the collected logs can be communicated to other referring accountability services (e.g. evidence).

5.3.2 Adoption Patterns

This section introduces the concept of the adoption patterns of the A4Cloud Reference Architecture for the different cloud service models and cloud computing and data protection roles. This approach is inspired by the IBM handbook on the Cloud Computing Reference Architecture (CCRA) version 4.0[67]. As reflected there, an adoption pattern is "*a collection of commonly observed functions and features that customers desire in their solution, where a customer starts to solve a specific business problem, typically driven by the same business motivation*". In IBM CCRA 4.0, the adoption patterns are solely driven by the adopted cloud service model that a specific cloud provider wants to adopt. In A4Cloud, the adoption pattern takes the form of guidance for the different actors in the cloud service provisioning chain in order to follow the accountability lifecycle and be accountable to their collaborating providers.

In more detail, the A4Cloud adoption patterns do not focus only on the cloud provider perspective, but try to capture the operational needs and the respective accountability requirements for the end-to-end chain in the cloud service provision. As such, these patterns should investigate the responsibilities and obligations of the actors, according to their position in the cloud computing/data protection role matrix and offer a guided roadmap for the adoption of the Accountability Framework in their cloud-based business model. From an accountability perspective, the position of an actor in data processing is very important, which raises various security and privacy requirements that should be addressed and a number of legal and normative obligations that should be implemented. In that respect, we can distinguish among the following A4Cloud adoption patterns:

67 https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Wf3cce8ff09b3_49d2_8ee7_4e49c1ef5d22/page/IBM%20Cloud%20Computing%20Reference%20Architecture%204.0.

- The Accountable Cloud Customer and Controller (ACCC) Adoption Pattern: this pattern refers to cloud customers, who act as data controllers and regulate the type of data to be collected from data holders and the purpose for doing so.
- The Accountable Cloud Provider and Controller (ACPC) Adoption Pattern: this pattern refers to cloud providers, who act as data controllers and regulate the type of data to be collected from data holders and the purpose for doing so.
- The Accountable Cloud Provider and Processor (ACPP) Adoption Pattern: this pattern refers to cloud providers, who act as data processors.
- The Accountable Cloud Customer and Processor (ACCP) Adoption Pattern: this pattern refers to cloud customers, who act as data processors.
- The Cloud Subject Enabling (CSE) Adoption Pattern: this pattern refers to a set of guidelines, through which the cloud subjects could be benefit from the mechanisms being implemented by the cloud providers and offered by the cloud customers with respect to how they could track the disclosure of their personal data in the cloud environments and respond to perceived and/or reported incidents about the way that this data is handled in the cloud.

Such adoption patterns aim to address the principal question for the cloud actors about “how am I going to be accountable to my customers?”, while providing informed guidance to the data owners on how they can take control over the results and the impact of the data processing procedures followed by the cloud providers to their data that has been disclosed in the cloud service provisioning chain. In general, the A4Cloud Adoption Patterns should provide a roadmap for the adoption of the Accountability Framework in all the respective lifecycle phases. Each pattern should, then, instantiate these general principles for the case of each target stakeholder, by detailing on the following items:

- The security and privacy requirements that drive the definition and the specification of the intended cloud-based business;
- The actors that are involved and how they relate with the primary actor of the adoption pattern;
- The accountability use cases and the respective accountability functions for this pattern;
- The roadmap to adopt the Accountability lifecycle;
- The instantiation of the A4Cloud RA, highlighting the intended use of each A4Cloud tool and any external tools that serve application specific functions, making references to target AMM;
- The realisation of the operational model for the A4Cloud components and the external tools and the respective information models.

In case of the instantiation of the RA, the adoption patterns describe the association of the accountability support services and the involved artifacts with the implementation of certain tool support functionalities to be addressed from the specific cloud computing and data protection roles. Thus, in Table 25, we analyse which are these functionalities that should be operated by each role, considering the use of software tools that should be accessible by the indicated roles and software tools running in the background that need to be deployed on the specific role machine to implement the respective accountability support service. This table does provide an exhaustive mapping of all the roles, since we skip the cloud carriers and brokers, who mainly act as data processors (and in some case as controllers), since they are seen in the same situation as for cloud providers.

Required functions	**Expected usage of tools for Cloud Subjects**	**Addressing Accountability Support Service**	**Involved Accountability Artifact or relevant object**
Cloud Subject Enabling (CSE) Adoption Pattern			
Track personal data	Tools to control the disclosure of personal data in the cloud	Validation	List of data disclosures from providers
Receive and manage incidents	Tools to allow the collection of violations from the cloud, against agreed data handling processes,	Notification and Validation	Notification Reports, Ranked incidents

Required functions	Expected usage of tools for Cloud Subjects	Addressing Accountability Support Service	Involved Accountability Artifact or relevant object
	and managing their severity level		
Manage remedies	Tools to suggest remediation, such as to complete and submit complaints form to a DPA, enforce the selected remediation/ redress actions	Remediation	List of data disclosures, Claims
Support data integrity	Tools for secure communication with Data Controller	Validation	Any type of artifact
Accountable Cloud Customer and Controller (ACCC) Adoption Pattern			
Select a cloud provider	Tools to get a guided selection of a cloud provider, according to functional, security and privacy requirements	Policy Definition and Validation	Capabilities, Social and Regulatory Norms, SLAs, PLAs, Contracts
Perform a DPIA	Tools to assess the impact of the cloud provider selection on the data protection aspects, and get the requirements to follow specific privacy, security and functional steps	Policy Definition and Validation	Capabilities, Social and Regulatory Norms, SLAs, PLAs, Contracts. Certificates and Assessments
Match policies to capabilities	Tools to perform policy matching between abstract policy statements and preferences	Policy Definition and Validation	Capabilities, machine readable Policies
Run audits	Tools to perform internal and external auditing	Validation	Audit Reports, Evidence Records
Manage incidents	Tools to assess the type of the perceived and/or reported incidents and generate notification alerts	Incident Management and Notification	Notification Reports
Accountable Cloud Customer and Processor (ACCP) Adoption Pattern			
Enforce policies	Tools to enforce accountability policies for the management of personal data	Policy Management and Enforcement	Machine readable Policies (including the personal data under consideration)
Produce logs	Tools to generate logs on the data handling processes with respect to data access, retention and integrity properties for monitoring and auditing purposes	Monitoring and Environment State Collection	Machine-generated Logs
Create evidence	Tools to collect and create evidence	Collection and Management of Evidence	Machine-generated Logs, Evidence Records
Run audits	Tools to perform internal and external auditing	Validation	Audit Reports, Evidence Records
Securely store evidence	Tools to securely store logs and evidence records	Collection and Management of Evidence	Machine-generated Logs, Evidence Records, machine readable Policies
Create incidents	Tools to raise incidents on an abnormal behaviour of the environment	Incident Management	Notification Reports
Manage incidents	Tools to assess the type of the perceived and/or reported incidents and generate notification	Incident Management and Notification	Notification Reports

Required functions	Expected usage of tools for Cloud Subjects	Addressing Accountability Support Service	Involved Accountability Artifact or relevant object
	alerts		
Accountable Cloud Provider and Controller (ACPC) Adoption Pattern			
Select a cloud provider	Tools to get a guided selection of a cloud provider, according to functional, security and privacy requirements	Policy Definition and Validation	Capabilities, Social and Regulatory Norms, SLAs, PLAs, Contracts
Perform a DPIA	Tools to assess the impact of the cloud provider selection on the data protection aspects, and get the requirements to follow specific privacy, security and functional steps	Policy Definition and Validation	Capabilities, Social and Regulatory Norms, SLAs, PLAs, Contracts. Certificates and Assessments
Match policies to capabilities	Tools to perform policy matching between abstract policy statements and preferences	Policy Definition and Validation	Capabilities, machine readable Policies
Develop policies	Tools to create accountability policies	Policy Definition and Validation	Capabilities, Social and Regulatory Norms, SLAs, PLAs, Contracts, machine readable Policies
Enforce policies	Tools to enforce accountability policies for the management of personal data	Policy Management and Enforcement	Machine readable Policies (including the personal data under consideration)
Produce logs	Tools to generate logs on the data handling processes with respect to data access, retention, transfer and integrity properties for monitoring and auditing purposes	Monitoring and Environment State Collection	Machine-generated Logs
Collect evidence	Tools to collect and create evidence	Collection and Management of Evidence	Machine-generated Logs, Evidence Records
Run audits	Tools to perform internal and external auditing	Validation	Audit Reports, Evidence Records
Create incidents	Tools to raise incidents on an abnormal behaviour of the environment	Incident Management	Notification Reports
Manage incidents	Tools to assess the type of the perceived and/or reported incidents and generate notification alerts	Incident Management and Notification	Notification Reports
Securely store evidence	Tools to securely store logs and evidence records	Collection and Management of Evidence	Machine-generated Logs, Evidence Records, machine readable Policies
Support data integrity	Tools for secure communication with Data Controller	Validation	Any type of artifact
Validate functions	Tools to validate the proper implementation of the accountability support services	Validation	Any type of artifact
Accountable Cloud Provider and Processor (ACPP) Adoption Pattern			
Enforce policies	Tools to enforce accountability policies for the management of personal data	Policy Management and Enforcement	Machine readable Policies (including the personal data under consideration)

Required functions	Expected usage of tools for Cloud Subjects	Addressing Accountability Support Service	Involved Accountability Artifact or relevant object
Produce logs	Tools to generate logs on the data handling processes with respect to data access, retention, transfer and integrity properties for monitoring and auditing purposes	Monitoring and Environment State Collection	Machine-generated Logs
Collect evidence	Tools to collect and create evidence	Collection and Management of Evidence	Machine-generated Logs, Evidence Records
Run audits	Tools to perform internal and external auditing	Validation	Audit Reports, Evidence Records
Create incidents	Tools to raise incidents on an abnormal behaviour of the environment	Incident Management	Notification Reports
Manage incidents	Tools to assess the type of the perceived and/or reported incidents and generate notification alerts	Incident Management and Notification	Notification Reports
Securely store evidence	Tools to securely store logs and evidence records	Collection and Management of Evidence	Machine-generated Logs, Evidence Records, machine readable Policies
Validate functions	Tools to validate the proper implementation of the accountability support services	Validation	Any type of artifact

Table 25: An example depiction of the adoption patterns for the instantiation of the Cloud Accountability Reference Architecture.

The adoption of one of the patterns from a business actor strongly depends on the role that this actor plays in the context of a business scenario. The further analysis of the required functionalities and their implementation details through ICT tools is provided in a separate document, which describes the A4Cloud toolset.

6 Concluding Thoughts

The A4Cloud Reference Architecture (RA) presented in this document covers a spectrum of topics, including the lifecycle, the artifacts, the processes, and the services. This is much wider than the technically-oriented domain of more traditional reference architectures, which in our case would be a service-oriented architecture. We were led to take this approach as strong accountability requires a holistic approach. In addition, accountability is a property which is applied to a defined set of commitments (or obligations): being accountable *for something* is a practical topic which can be associated with specific measures and processes, whereas simply "being accountable" remains an abstract topic and the associated artifacts, processes and services are only helpful as tools to frame, analyse, design and implement a solution when associated with an objective (or purpose).

In this report, we propose processes and mechanisms to address the accountability practices defined in the Conceptual Framework [1], i.e.:

- defining governance to responsibly comply with internal and external criteria
- ensuring implementation of appropriate actions
- explaining and justifying those actions
- remedying any failure to act properly.

We do so while remaining agnostic to the purpose to which accountability is to be applied, using the data protection domain as a "privileged use case". We also refrain from adopting a specific compliance baseline. This limits us in the level of practical details we can provide, but keeps the results relevant for a large spectrum of scenarios.

Therefore, this report can be used as a guide to determining what must be done, and not as a specification of what must be done. This opens up the possibility to instantiate a set of Reference Architectures with more actionable processes and mechanisms to address a specific combination of baseline compliance standards with a specific purpose.

Accountability in the context of the cloud is an emerging concern. Cloud service providers are not yet ready to commit to it, especially as it relates to transparency. The market requirements are however evolving, driven in part by the regulators which mandate an increasingly high level of accountability in the handling and protection of personal data. Cloud service providers will have no choice but to become accountable if they want to remain competitive, as their customers - the data controllers - will require this level of service. This is not the only driving force: commoditisation of cloud services will lead providers to increase the feature sets and quality of service they provide, first in order to gain a competitive advantage, and then to meet what has become a baseline requirement. At some point in this journey, accountability controls will be integrated in control frameworks, such as the CSA CCM, and accountability services will be defined to ensure interoperability. This RA provides the foundation for these two evolutions.

7 References

[1] S. Pearson, M. Felici and et al., “WP-32 Conceptual Framework,” A4Cloud project, 2014.

[2] J. Luna and D. Cattedu, “Report on A4Cloud contribution to standards,” A4Cloud project, 2014.

[3] A. Pannetrat and et al, “The interoperability of A4Cloud Framework,” A4cloud project, 2014.

[4] ISO/IEC/IEEE, “ISO/IEC/IEEE 29119 Software and systems engineering - Software testing,” 2013.

[5] F. Liu and et al, “NIST Cloud Computing Reference Architecture,” NIST Special Publication 500-292, 2011.

[6] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” NIST Special Publication 800-145, 2011.

[7] Cloud Security Alliance (CSA), “CSA Security, Trust & Assurance Registry (STAR),” [Online]. Available: https://cloudsecurityalliance.org/star/.

[8] CIPL - Galway Project, “Data Protection Accountability: The Essential Elements,” 2009.

[9] 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, “Getting Accountability Right with a Privacy,” 2012.

[10] European Commission, “Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation),” 2012.

[11] CNIL, “Recommendationds for companies planning to use cloud services,” 2012.

[12] Information Commissioner's Office, “Guidance on the use of cloud computing,” 2012.

[13] Nymity Inc., “Privacy Management Accountability Framework,” 2014.

[14] IT Governance Institute, “COBIT: Control Objectives for Information and related Technology,” 2000.

[15] ISO/IEC, “ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems — Requirements,” 2013.

[16] J. De Clerq and et al, The HP Security Handbook, Hewlett Packard, 2008.

[17] ISO/IEC, “ISO/IEC 27001:2013: Information technology — Security techniques — Code of practice for information security controls,” 2013.

[18] Cloud Security Alliance (CSA), “Cloud Controls Matrix,” 2014.

[19] H. Bergsteiner and G. Avery, “Responsibility And Accountability: Towards An Integrative Process Model,” 2011.

[20] UK Information Commissioner's Office, “Guidance on the use of cloud computing,” 2012.

[21] C. Reed and D. Stefanatou, “Final Report on Legal and Regulatory Dependencies: embedding accountability in the international legal framework,” A4Cloud Project, 2015.

[22] M. M.-G. S. R. Simon Dorst, “Who is the King of SIAM?,” AXELOS, 2015.

[23] CIPL Paris Project, “Demonstrating and measuring accountability: a discussion document,” 2010.

[24] C. Bennett, “Implementing privacy codes of practice,” Canadian Standards Association, 1995.

[25] D. A. H. B.-L. T. F. J. H. J. &. S. G. Weitzner, “Information accountability,” *Communications of ACM 51(6),* no. June 2008, pp. 82-87, 2008.

[26] C. Bennett, “The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats,” in *In Managing Privacy through Accountability*, D. G. e. al., Ed., MacMillan, 2012, pp. 33-48.

[27] A. Vranaki, “Learning Lessons from Cloud Investigations in Europe: Bargaining Enforcement and Multiple Centers of Regulation in Data Protection,” 2015.

[28] European DG of Justice (Article 29 Working Party), “Opinion 3/2010 on the Principle of Accountability (WP 173),” 2010.

[29] S. Bradshaw, C. Millard and I. Walden, “Standard Contracts for Cloud,” in *Cloud Computing Law*, C. Millard, Ed., Oxford OUP, p. 37 – 72.

[30] K. W. Hon, C. Millard and I. Walden, “Negotiated Contracts for Cloud,” in *Cloud Computing Law*, C. Millard, Ed., Oxford OUP, 2013, pp. 73-107.

[31] C. Raab, “The Meaning of ‘Accountability’ in the Information Privacy Context,” in *Managing Privacy through Accountability*, D. e. a. Guagnin, Ed., MacMillan, 2012, pp. 15-32.

[32] Hunton & Williams LLP, “Data Protection Accountability: The Essential Elements – a Document for Discussion,” 2009.

[33] K. Bernsmed and e. al., “D:B-3.2 Consolidated use case report,” A4Cloud Project, 2014.

[34] European DG of Justice (Article 29 Working Party), “Binding Corporate Rules,” [Online]. Available: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm.

[35] E. Kosta and e. al., “MS:D-4.1 “Internal report on legal analysis relating to redress mechanisms and remediation”,” A4Cloud Project, 2014.

[36] Presidency of the Council of the European Union, “Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [first reading] - Analysis o,” Council of the European Union, Brussels, 2015.

[37] European Commission, joint communication to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,” Brussels, 7.2.2013.

[38] European Commission, “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,” Brussels, 7.2.2013.

[39] European Parliament, “Legislative resolution of 13 March 2014 on the 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,” 2013.

[40] Software Engineering Institute (SEI), “CMMI for development: Improving processes for developing products and services.,” 2010.

[41] NIST Public RATAX WG, “Cloud Computing: Cloud Service Metrics Description,” 2014.

[42] ISO/IEC, “Information Technology – Security techniques – Information Security Management – Measurement,” 2009.

[43] NIST, “NIST Cloud Computing Security Reference Architecture,” 2013.

[44] A. Taha, R. Trapero, J. Luna and N. Suri, “AHP-Based Quantitative Approach for Assessing and Comparing Cloud Security,” in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2014.

[45] J. Luna, R. Langenberg and N. Suri, “Benchmarking Cloud Security Level Agreements Using Quantitative Policy Trees,” in *ACM Cloud Computing Security Workshop*, 2012.

[46] W. Benghabrit and et al, “A cloud accountability policy representation framework,” A4Cloud project, 2014.

[47] T. Wlodarczyk and et al, “D:C-8.1 Framework of Evidence,” A4Cloud project, 2014.

[48] “OpenStack: Open source cloud computing software,” [Online]. Available: https://www.openstack.org/.

[49] K. Bernsmed and et al., “MSB-3.1 Use Case Descriptions,” A4Cloud project, 2014.

[50] P. Krutchen, The Rational Unified Process: An Introduction, Reading : Addison-Wesley, 2000.

[51] V. Tountopoulos and et al, “Architecture guidelines and principles (internal report),” A4Cloud project, 2013.

[52] M. Azraoui and et al, “A-PPL: An Accountability Policy Language for Cloud Computing,” in *DPM / SETOP*, Wroclaw (Poland), 2014.

[53] W. Benghabrit and et al, “Abstract Accountability Language,” in *8th IFIP WG 11.11 International Conference on Trust Management*, Singapore, 2014.

[54] T. Pulls and et al, “Distributed privacy-preserving transparency logging,” in *Proceedings of the 12th annual {ACM} Workshop on Privacy in the Electronic Society*, Berlin, Germany, 2013.

[55] S. Trabelsi and et al, “PPL: PrimeLife Privacy Policy Engine,” in *IEEE International Symposium on*

Policies for Distributed Systems and Networks (POLICY), Pisa, 2011.

[56] European Commission, “Proposed Directive on Network and Information Security – frequently asked questions,” Brussels, 7.2.2013.

[57] Ponemon Institute LLC, “2011 Cost of Data Breach Study,” March 2012.

[58] PwC U.K., “Information security breaches survey,” 2012.

[59] European Commission, *EU Cybersecurity plan to protect open internet and online freedom and opportunity,* Brussels, 2013.

[60] Council of the European Union, “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 – progress report,” Brussels, 22.5.2014.

[61] Council of the European Union, “3318th Council meeting. Transport, Telecommunications and Energy,” Luxembourg, 5/6.6.2014.

8 Appendices

8.1 [DETAILS] List of Obligations

The information presented in this section represents details which may only be required if seeking an in-depth understanding of the Cloud Accountability Reference Architecture.

The following list of obligations was extracted from the WP B-3 MSB-3.1 report [49]. We point to that report for a full list of those obligations that provides extended details, including legal perspectives.

The following is a list of obligations from the regulatory perspective (Data Protection Directive), to which Cloud actors must adhere:

- **Obligation 1: informing about processing**. Data subjects have the right to know that their personal data is being processed.
- **Obligation 2: informing about purpose.** Data subjects also have the right to know why their personal data is being processed.
- **Obligation 3: informing about recipients.** Data subjects have the right to know who will process their personal data.
- **Obligation 4: informing about rights.** Data subjects have the right to know their rights in relation to the processing of their personal data.
- **Obligation 5: data collection purposes.** Personal data must be collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
- **Obligation 6: the right to access, correct and delete personal data.** Data subjects have the right to access, correct and delete personal data that have been collected about them.
- **Obligation 7: data storage period.** Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purpose for which they were collected.
- **Obligation 8: security and privacy measures.** Controllers are responsible to the data subjects for the implementation of appropriate technical and organisational security measures.
- **Obligation 9: rules for data processing by provider.** Controllers are accountable to data subjects for how sub-providers process their personal data.
- **Obligation 10: rules for data processing by sub-providers.** The controller must also ensure that all sub-providers involved in the service delivery chain do not process the personal data, except on the controller's instructions (unless they are required to do so by law).
- **Obligation 11: provider safeguards.** Controllers are accountable to data subjects for choosing data processors that can provide sufficient safeguards concerning technical security and organisational measures.
- **Obligation 12: sub-provider safeguards.** The previous obligation comprises all processors in a service delivery chain.
- **Obligation 13: informed consent to processing.** Controllers are accountable to the data subjects for obtaining informed consent before collecting personal data.
- **Obligation 14: explicit consent to processing.** Controllers are accountable to the data subjects for obtaining explicit consent before collecting sensitive personal data.
- **Obligation 15: explicit consent to processing by joint controllers.** Controllers are accountable to the data subjects for obtaining explicit consent before allowing joint data controllers to process their sensitive personal data.
- **Obligation 16: informing DPAs.** Controllers are accountable to the data protection authorities to inform that they collect personal data.
- **Obligation 17: informing about the use of sub-processors.** Processors are accountable to the controllers for informing about the use of sub-providers to process personal data.

- **Obligation 18: security breach notification.** Controllers are accountable to data subjects for notifying them of security incidents that are related to their personal data.
- **Obligation 19: evidence of data processing.** Processors are accountable to the controllers for, upon request, providing evidence on their data processing practices**.**
- **Obligation 20: evidence of data deletion.** Processors are accountable to the controllers for, upon request, providing evidence on the correct and timely deletion of personal data.
- **Obligation 21: data location.** Data controllers are accountable to the data subjects for the location of the processing of their personal data.

9 Index of Figures

10 Index of Tables