CLOUD
ACCOUNTABILITY
PROJECT

D:B-3.2 Consolidated use case report

Deliverable Number:	D23.2
Work Package:	WP 23
Version:	Final
Deliverable Lead Organisation:	SINTEF
Dissemination Level:	PU
Contractual Date of Delivery (release):	30/09/2014
Date of Delivery:	03/10/2014

Editor

Karin Bernsmed (SINTEF)

Contributors

Karin Bernsmed (SINTEF), Vasilis Tountopoulos (ATC), Paul Brigden (ATC), Thomas Rübsamen (Furtwangen), Massimo Felici (HP Labs), Nick Wainwright (HP Labs), Anderson Santana De Oliveira (SAP), Jakub Sendor (SAP), Mohamed Sellami (Armines), Jean-Claude Royer (Armines)

Reviewer(s)

Melek Önen (EURECOM), Mario Südholt (Armines)

A4Cloud
www.a4cloud.eu
Accountability For Cloud and Other Future Internet Services

SEVENTH FRAMEWORK
PROGRAMME

List of Figures

List of Tables

Abbreviations

A4Cloud	Accountability For Cloud and Other Future Internet Services
AAL	Ambien Assistant Living
AAS	Audit Agent System
AccLab	Accountability Laboratory
A-PPL	Accountability Privacy Policy Language
AT	Assertion Tool
BPMN	Business Process Model Notation
BUC	Business Use Case
BYOD	Bring Your Own Device
CNIL	Commission Nationale de l'informatique et des Libertés
COAT	Cloud Offerings Advisory Tool
CRM	Customer Relationship Management
CSA	Cloud Security Alliance
CTO	Chief Technology Officer
DoW	Description of Work
DPA	Data Protection Authority
DPD	Data Protection Directive
DPIAT	Data Protection Impact Assessment Tool
DSART	Data Subject Access Request Tool
DT	Data Track
DTMT	Data Transfer Monitoring Tool
EU	European Union
ERP	Enterprise Resource Planning
GUI	Graphical User Interface
IaaS	Infrastructure as a Service
IRT	Incident Response Tool
ISV	Independent Software Vendors

NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
RRT	Remediation and Redress Tool
R&RT	*see "RRT"*
SaaS	Software as a Service
SME	Small and Medium-sized Enterprise
TL	Transparency Log
UML	Unified Modelling Language
XACML	eXtensible Access Control Markup Language
WP	Work Package

Executive Summary

The objectives of the A4Cloud project is to contribute toward an accountability-based approach enabling different mechanisms and tools that help cloud users, providers as well as regulators and auditors to make sure that the obligations to protect personal data and business confidential data are adhered too. The purpose of the *business use cases* in the A4Cloud project is to demonstrate how the accountability mechanisms and tools that are being developed in the project can be applied in three distinct domains, which involve generating, storing and processing of personal and business confidential data by different actors in cloud ecosystems. The business use cases are examples of services that will benefit strongly from being realized as cloud services but that will have stringent requirements for accountability and transparency in the cloud service provision chain.

This is the final deliverable describing the three different business use cases that have been developed in the A4Cloud project. These are:

- Business use case 1, which deals with the flow of healthcare information generated by medical sensors in the cloud. It focuses on the generation, processing, flow and traceability of sensitive personal information between a set of cloud providers. The case shows which accountability mechanisms and tools will be needed to protect sensitive personal data.
- Business use case 2, which deals with cloud-based Enterprise Resource Planning (ERP) software, which is extended with third party services. The purpose is to show how an enterprise cloud deployment that originally has been configured as an on-premises system can be extended with new capabilities by combining it with service extensions running in the cloud. This business use case demonstrates how personal information can be adequately protected across a chain of cloud service models (IaaS, PaaS, and SaaS), using accountability mechanisms and tools.
- Business use case 3, which deals with a multi-tenant cloud scenario. This business use case is concerned with challenges that arise when end users operate with cloud services for personal as well as business purposes on the same device. It shows how accountability mechanisms and tools can help solve the intersection of policy enforcements across different cloud domains. In contrast to business use case 2, which illustrates service chains in one domain, this business use case comprises multi-tenant service chains of different domains.

This deliverable gives an overview over each business use case, explains what are the roles and responsibilities of the actors involved in each case, and analyses the accountability obligations that exist in the service delivery chains. Furthermore, we relate the business use cases to the different phases in the A4Cloud conceptual framework and explain how the tools that are being developed in the project can be used to assist the involved actors in achieving accountability. The deliverable also includes an analysis of the interoperability requirements that arise from the business use cases.

In parallel with the business use case development, the work with creating a demonstrator for the A4Cloud tools has been started. In the last chapter of this deliverable we propose an approach to demonstrate the project results, which is based on characteristics from all the three existing business use cases.

The A4Cloud project is now moving into the implementation and demonstration phase. Until now the business use cases have been used to derive requirements for the A4Cloud tools and technologies, to investigate how the research done in the technical work packages will be applied in the business use case domains, and to validate that derived theory and models are applicable in real cloud service ecosystems. This deliverable marks the end of the requirements phase in the project. The characteristics of the business use cases will not be developed further in the project; however they are expected to remain useful for validation, demonstration and evaluation of the project results in the next few years.

Table of Contents

1 Introduction

The A4Cloud project deals with accountability for the cloud and other future Internet services. In the context of the project, accountability concerns data stewardship regimes in which organizations that are entrusted with personal and business confidential data are responsible and liable for processing, sharing, storing and otherwise using the data according to contractual and legal requirements from the time it is collected until when the data is destroyed (including onward transfer to and from third parties) [4]. A4Cloud contributes toward an accountability-based approach by enabling different mechanisms supporting the governance of personal and business confidential information in the cloud, hence accountability governance. This accountability governance concerns the chain of responsibilities that needs to be built throughout the cloud service supply network.

The purpose of the business use cases (BUCs)[1] in the A4Cloud project is to provide an understanding of real-world scenarios from three distinct user domains, to use them to derive requirements and to validate and demonstrate the research that is being performed in the project. The accountability challenges that we have identified for the business use cases may be also of interest to stakeholders outside the project. This deliverable contains the final descriptions of the three different business use cases. In the rest of this section we will explain how the business use cases relate to the accountability, concepts, models, technologies and tools that are being developed in the project, and explain what role they will have in the final implementation and demonstration phase.

1.1 Relationships with the other A4Cloud Work Packages and Deliverables

This deliverable is related to a number of other work packages in A4Cloud project. Here we list the most important relations.

- The goal of the **WP:B-2 (elicitation)** work package is to ensure that the project activities reflect the needs of the targeted stakeholder groups. So far this have been achieved through the organisation of stakeholder workshops, which gathered a broad spectrum of requirements, good practices and risks related to the cloud eco-system covering the diverse range of geographical (including legal) constraints and challenges, sector/industry-specific requirements and cloud models. We have engaged in WP:B-2 activities to derive accountability-related requirements for all the three business use cases. The result has been documented in the WP:B-2 deliverables [18][19] as well as in a scientific paper [1].
- The goal of the **WP:B-4 (socio-economic context)** work package is, amongst other things, to identify the needs of cloud stakeholders from a socio-economic behaviour. The *normative obligations* presented in Section 5 in this deliverable have been derived from the needs documented by WP:B-4 in one of their first deliverables [2].
- The goal of the **WP:B-5 (contractual & regulatory considerations)** work package is, amongst other things, to assess the legal responsibilities and regulatory implications for the different actors in the cloud ecosystem in the context of the project. WP:B-5 has provided an internal project report, which outlines a number of regulatory and contractual obligations that exist between different actors in a cloud ecosystem when processing of personal data takes place. This report has formed the basis for the set of *legal obligations* that have been derived in Section 5 of this deliverable. Moreover, WP:B-5 has contributed to a scientific paper [3], which analyses the legal and contractual obligations in the health care business use case.
- The goal of the **WP:C-2 (conceptual framework)** work package is to identify and describe a framework of concepts and the terminology that forms the basis for the accountability mechanisms and tools that will be developed in the project. We have used the concepts

[1] The term "business use case" (or simply just "BUC") was introduced in the first WP:B-3 deliverable [6]; with the purpose of making it easier to distinguish between a use case that is a description of a system at an organizational level (this is what we call a "business use case") and a detailed model of the system behaviour under certain conditions (such as a "UML use case").

described in [4] when describing, modelling and analysing the business use cases. Section 2 in this deliverable will give a further explanation of our use of the conceptual framework.

- The goal of the **WP:C-3 (interoperability of framework)** interoperability work package is to identify relevant interoperability requirements for the conceptual framework, reference architecture and tools that will be developed in the project. In order to contribute to this work, we have made a high-level analysis of interoperability seen from the business use case perspectives.
- The goal of the **WP:C-4 (policy mapping and representation)** work package is to define a framework for enforceable accountability policies. The framework has been validated by modelling the business use cases that are described in this deliverable. The results have been presented in a number of scientific papers [25][27][28][29].
- The goal of the **WP:C-6 (risk and trust modelling)** work package is to provide abstract models of risk and trust amongst the cloud stakeholders, and to create representations of these concepts. The risk and trust models have been validated by modelling one of the business use cases that have been defined in this deliverable. The result is documented in Section 9 of this deliverable.
- The goal of the **WP:D-2 (reference architecture)** work package is to define the A4Cloud architecture, which includes all the tools that will be developed in the project. This deliverable includes an analysis of all the three business use cases with respect to these tools.
- The goal of the **WP:D-6 (assertion framework and toolkit validation)** work package is to develop a framework for accountability assertion of individual toolkit components and assemblies of multiple components. The business use cases presented in this deliverable will be used to derive test case scenarios for validation of the proposed assertion framework.
- The goal of the **WP:D-7 (instantiation for use cases)** work package is to enable demonstration and evaluation through the use of the business use cases. The business use cases that are presented in this deliverable, together with the instantiated use case presented in Section 10, will hence serve as input to this work.

The A4Cloud deliverable DB-3.1 [5] contains a first description of the three business use cases. This deliverable provides an introduction and motivation of the three different BUCs and analyses them in terms of the system that is to be considered, the actors involved and their means of accountability. The deliverable also outlines as-is and to-be scenarios, which are textual descriptions of the need for and usage of the A4Cloud tools and services. Finally, the deliverable describes the accountability relationships that exist between the involved actors and summarizes what functionalities will be needed to achieve accountability in the to-be scenarios.

This deliverable builds directly on DB-3.1 [5]. The descriptions of the BUCs have been refined (Section 3) and we have clarified the roles of the involved actors (Section 4). The accountability relationships that we identified in DB-3.1 have not been used further, since we considered it more relevant to shift the focus from the, somewhat vaguely defined "accountability relationships" into clearly defined accountability obligations that arise from the legal/contractual and the normative perspective (Section 5). The scenarios from DB-3.1 have not been included in this deliverable, but we have used them to extend the high-level function analysis in DB-3.1 into a more detailed tool analysis (Section 7), and as a basis for doing a detailed process modelling of the business use cases (Section 8).

1.2 Business Use Case Consolidation and Refinement

The A4Cloud Description of Work (DoW) defines this deliverable to be "the final description of all three use cases" and it comprises work that has been done in two different tasks; namely "Task T:B-3.4 Use case consolidation and refinement" and "Task T:B-3.5 Use case model population".

The task T:B-3.4, Use case consolidation and refinement, consisted of a number of different activities, which were conducted in collaboration with other work packages in the project. During the last year, the initial business use case descriptions (see deliverable D:B-3.1 [5]) have been used by other

WPs in order to contextualize emerging issues in cloud service provisions. For instance, the business use case descriptions have been used in the WP:B-2 Elicitation Workshops (WS1 and WS2) in order to gather stakeholders' opinions on accountability (WS1) and emerging accountability issues in the cloud (WS2). In addition, a number of project partners involved in other WPs have reviewed the use case descriptions in D:B-3.1 in order to identify specific examples that they can use to describe their contributions and analyses (this is the case for the other WPs within the B and C streams).

In addition to the reviews and interactions by other WPs in the A4Cloud project, we would also like to mention some of the specific use case consolidation and refinement activities, which have been conducted by WP:B-3 (Task T:B-3.4):

- Cloud Actor Roles: the WP:C-2 Conceptual Framework [4] has identified and defined a Glossary of Terms and Definitions [11] in order to harmonize the discussion of accountability across WPs as well as with external stakeholders. Among the terms identified are those concerned with the cloud actor roles. Due to the particular project scope dealing with cloud computing as well as with data protection, the C2 Glossary of Terms and Definitions identifies specific Cloud Actor Roles. This enables a systematic identification and analysis of relevant roles for each cloud actor in the ecosystem. Section 4 in this deliverable introduces the Cloud Actor Roles, which have been used to review the use cases' description and discuss them with respect to accountability.
- Interoperability: an interoperability analysis (performed together with WP:C-3) [7] characterizes the interactions among the cloud actors in the three business use cases. The interactions between cloud actors must be seen at the specific time of the cloud service lifecycle that they are held in order to serve the respective business use cases. This supports gathering requirements on the way such interactions are enabled by accountability (as structured by WP:C-2 in terms of Accountability Model). In order to better understand the interoperability requirements, the business use cases have therefore been analysed from four distinct interoperability perspectives: regulatory, business, semantic and technical.
- Accountability Mechanisms: Obligations and Tools: the initial business use case descriptions in D:B-3.1 focused on the creation of so called "as-is" and "to-be" scenarios (see [5] for further details), that is, a functional characterization of the business use cases in terms of supported activities as understood from specific cloud actors. This report extends the original business use case descriptions by analysing them from the point of view of accountability mechanisms, in particular with a focus on obligations and (project) tools. In this deliverable the review of the business use cases in terms of obligations and tools highlights obligation requirements as well as mappings from tools to use case (to-be) scenarios (that is, how implemented tools address cloud actors' needs).
- Demonstrator: The initial business use cases allow the project to scope and analyse the various dimensions of the concept of accountability (as done by WP:C-2), leading to the generation of requirements and the identification of specific functionality to be implemented. For example, the set of policies supported by the project is directly derived from the analysis of the business use cases. The business use case and tool descriptions have been used as input to a Demonstrator Workshop[2], which purpose was to identify how an integrated and operational understanding of accountability could be achieved. In contrast, the purpose of the instantiation use case (the demonstrator use case) is to provide a scenario which will allow the practical demonstration of various concepts and tools developed by the project.

The task T:B-3.5, Use case model population, consisted mainly of two parts; applying the risk and trust models that have been developed in WP:C-6 to the business use cases and analysing the business use cases in order to derive requirements for the accountability policies that are being developed in WP:C-4. Most of the risk and trust modelling efforts have been done as a joint effort with WP:C-6.

[2] The demonstrator workshop took place in Bristol, UK, Jan 29th–30th 2014 and was attended by representatives from all the partners in the A4Cloud project.

Moreover, we have worked closely together with WP:C-4 in order to derive requirements for, and examples of, accountability obligations and their corresponding machine-readable policies.

The two tasks T:B-3.4 and T:B-3.5 have been running in parallel during the second year of the project. While the business use cases were equally specified and analysed during the first year of the project, they have, however, not received an equal share of attention during the second year[3]. As will be seen in this deliverable, most focus has been put on analysing BUC 1 (health care services in the cloud) and BUC 2 (cloud-based ERP software). Both these business use cases have also been used extensively by other work packages to validate and illustrate the work that have been done in stream C and D of the project.

According to the DoW, only one use case will be instantiated and used to implement a demonstrator for the project results. For reasons that will be explained in the last chapter of this deliverable (Chapter 10), the A4Cloud project partners have mutually agreed not to implement any of the already defined business use cases (as was stated in the Dow), but instead defined a new case that integrates the most interesting characteristics form the three existing BUCs and that at the same time is more concise and feasible to implement.

1.3 Outline

The deliverable is structured as follows. This section introduces the overall approach that has been followed in WP:B-3 and explains its relation to the other work packages in the project and to the DoW. Section 2 explains how the concepts, models, technologies and tools developed in stream C and D of the project have been adopted in the work with the business use cases. In Section 3 we provide an overview over the three business use cases. Section 4 analyses the BUCs in terms of what cloud actor roles are involved and Section 5 outlines what accountability obligations that apply to these actors. Section 5 also provides an example of the mapping of obligations to policies for one of the business use cases. Section 6 provides an interoperability analysis of the BUCs. In Section 7 we present the tools analysis that we have performed and in Section 8 we present some of the process modelling activities that have taken place in the context of WP:B-3. Section 9 includes some results from the risk and trust modelling activities. Finally, in Section 10 we present a first approach to define a demonstrator for the accountability tools that are under development in the project.

[3] For example, the analysis of accountability obligations in Chapter 5 focuses only on BUC1 and BUC2. Also, the process modelling in Chapter 8 uses BUC1 and the risk assessment in Chapter 9 uses BUC2 to illustrate the respective methodologies.

2 Accountability Framework and Governance in the Business Use Cases

The A4Cloud approach is to integrate legal, regulatory, socio-economic and technical approaches into a framework to provide accountability pre-emptively, to assess risk and avoid privacy harm and reactively to provide transparency, auditing and corrective measures for redress. This will enable organisations to implement chains of accountability, including interdisciplinary mechanisms to ensure that obligations to protect data are observed by all who process the data, irrespective of where that processing occurs [10].

To achieve this objective, the A4Cloud has adopted the different views of accountability, as illustrated in Figure 1. This figure shows that accountability can be analysed in a broad perspective; from a conceptual view (answering questions like; *What is accountability? How do we achieve it?*), to a much more concrete view (*Which processes do we adopt? What tools can we use?*). Eventually the instantiation of a use case will demonstrate how accountability can be achieved in a realistic setting.

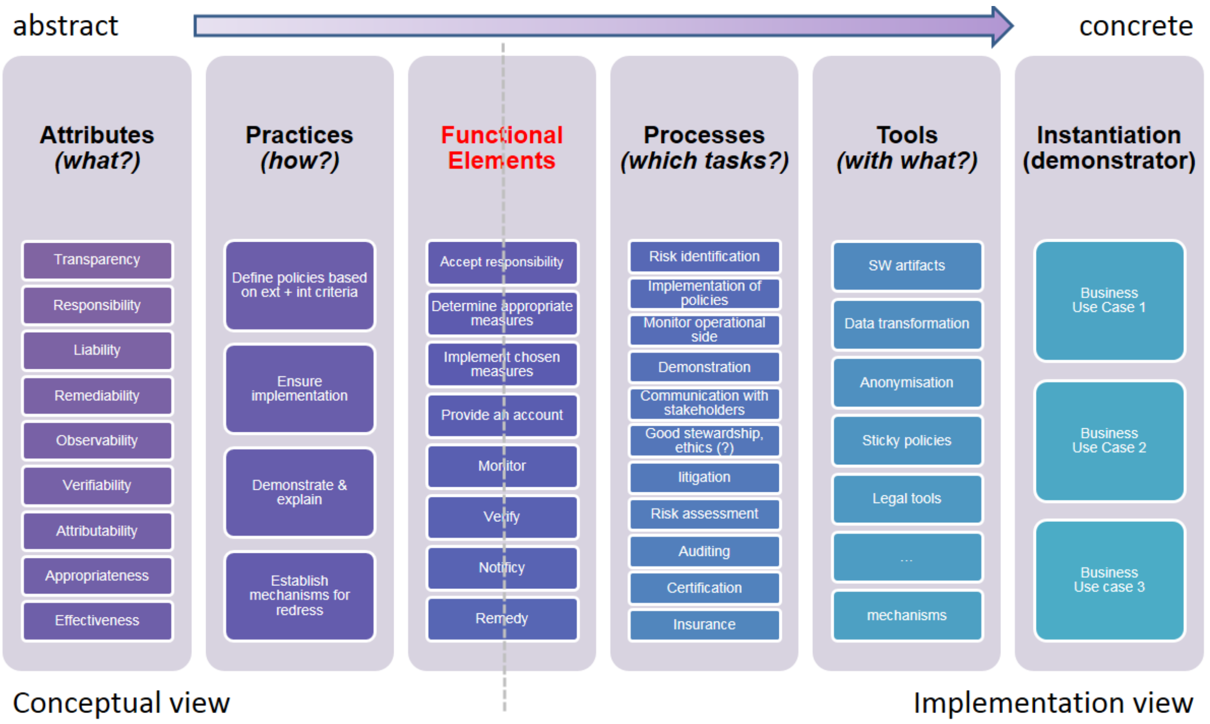


Figure 1 Different Views of Accountability [10].

The previous deliverable from WP:B-3 (DB:3-1 [5]) focused on the abstract views of accountability. In DB:3-1 we analysed each of the business use cases in terms of the **attributes** illustrated in the leftmost column in Figure 1; for each of the BUCs we suggested a number of accountability relationships that applied to the involved actors. We also presented a set of to-be scenarios that outlined how some of the **practices** (the second column in Figure 1) were applied in the three BUCs. Finally, this deliverable presented a high-level functional analysis of the to-be scenarios, which was a first attempt to map the practices in the second column in Figure 1 into the **functional elements** in the third column.

In this deliverable we take a more concrete approach. We use Business Process Modelling Notation (BPMN) to model the **processes** in Figure 1 (c.f. Chapter 8). We also analyse all three BUCs in terms of the **tools** that are used (c.f. Chapter 7). Finally we suggest a way to do the **instantiation** of a demonstrator, which is based on characteristics from all the three business use cases (Chapter 10). In this deliverable we also go back to the conceptual view and clarify the underlying relationships that affect the attributes in Figure 1 (c.f. Chapter 4 that analyses the roles of the actors in the BUCs and Chapter 5 that outlines a number of obligations that apply).

The rest of this section provides a brief introduction to some of the most important parts of the A4Cloud conceptual framework, which have been the foundation for the analysis and modelling activities presented in the rest of this deliverable. Note that we provide an overview only; more details about the A4Cloud conceptual framework can be found in the project documentation [4].

2.1 Functional Aspects of Accountability

According to WP:C-2 (and illustrated in Figure 1), an accountability-based approach can be broken down into the following key functional aspects of accountability:

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

The different functional elements of accountability bridging the conceptual and implementation views of accountability are visible in the third column of Figure 1. These functions are realised at different phases within an organisation's operational lifecycle (as explained in [10] and summarised later on in this deliverable).

Different accountability functions are triggered at different phases of an organisation's operational security lifecycle, and how some of these (namely attribution of failure, notification and remediation) are triggered within exception loops corresponding in this case to non-satisfaction of obligations, for example by a data breach. Thereby, it can be seen how there is involvement both of proactive elements (clarification and acceptance of responsibility, determination and implementation of appropriate measures and preparation of a demonstration that these meet the obligations involved for when it might be needed), as well as reactive elements (corresponding to detection and handling of data breaches or other non-satisfaction of obligations). At its core, in the sense that a data controller should be accountable for complying with measures which give effect to principles that have been set within a democratic context, and that they will be held to account in case of failure, as well as the provision of tools to help organisations to 'do the right thing' (including for better remediation, breach notification, etc.), accountability is obviously a good thing and not very controversial. The way in which accountability is achieved is key, which includes the need for adequate resources in checking and enforcing whether organisations are indeed using appropriate measures, involvement of different stakeholders, including the public (or representatives of the public) in data privacy regulation, provision of suitable accountability tools and help for organisations to form appropriate risk assessment mechanisms and policies.

2.2 The A4Cloud Mechanisms and Tools

The A4Cloud toolkit consists of a number of software tools that will be developed in the project. These will address the different functional aspects of accountability that were outlined in the previous subsection. The tools can be classified in terms of whether they are preventive, detective or corrective in nature, as illustrated in Figure 2. The preventive tools are related to contract and risk management (the Cloud Offerings Advisory Tool (COAT) and the Data Protection Impact Assessment Tool (DPIAT)). The detective tools are the tools intended for data subject controls (Data Track, the Data Subject Access Request Tool (DSART) and their associate plug-ins), policy definition and enforcement (Accountability Laboratory (AccLab) and the A-PPL Engine) as well as the tools related to evidence and validation (The Audit Agent System (AAS) and the Data Transfer Monitoring Tool (DTMT)). Finally the corrective tools are the tools that will address incident response and remediation (the Incident Response Tool (IRT) and the Remediation & Redress Tool (RRT)). In the A4Cloud project these tools are being developed in different technical work packages, however the overall architecture of the toolkit has been described in the WP:D-2 project internal milestone report [6].

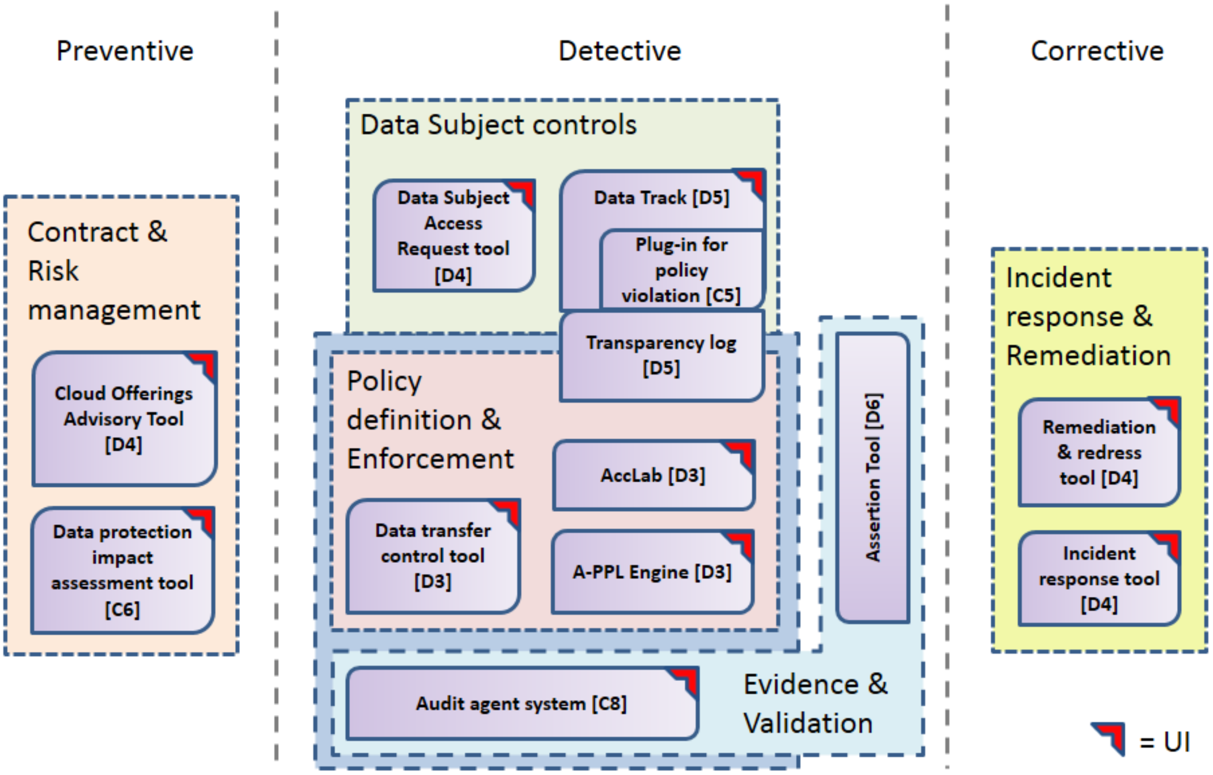

Preventive
Detective
Corrective
Contract & Risk management
Cloud Offerings Advisory Tool [D4]
Data protection impact assessment tool [C6]
Data Subject controls
Data Subject Access Request tool [D4]
Data Track [D5]
Plug-in for policy violation [C5]
Transparency log [D5]
Policy definition & Enforcement
AccLab [D3]
Data transfer control tool [D3]
A-PPL Engine [D3]
Assertion Tool [D6]
Audit agent system [C8]
Evidence & Validation
Incident response & Remediation
Remediation & redress tool [D4]
Incident response tool [D4]
= UI

Figure 2 Functional model of the A4Cloud mechanisms and tools [10].

2.3 The Organisational Accountability Governance Process

The functional aspects of accountability described in Section 2.1 will be realised within different phases of an organisation's governance lifecycle [4]. Figure 3 outlines how the functional aspects will be triggered at different phases in the lifecycle, and shows how exceptions, such as a security incident or a policy violation, will invoke an exception loop in the operating phase.

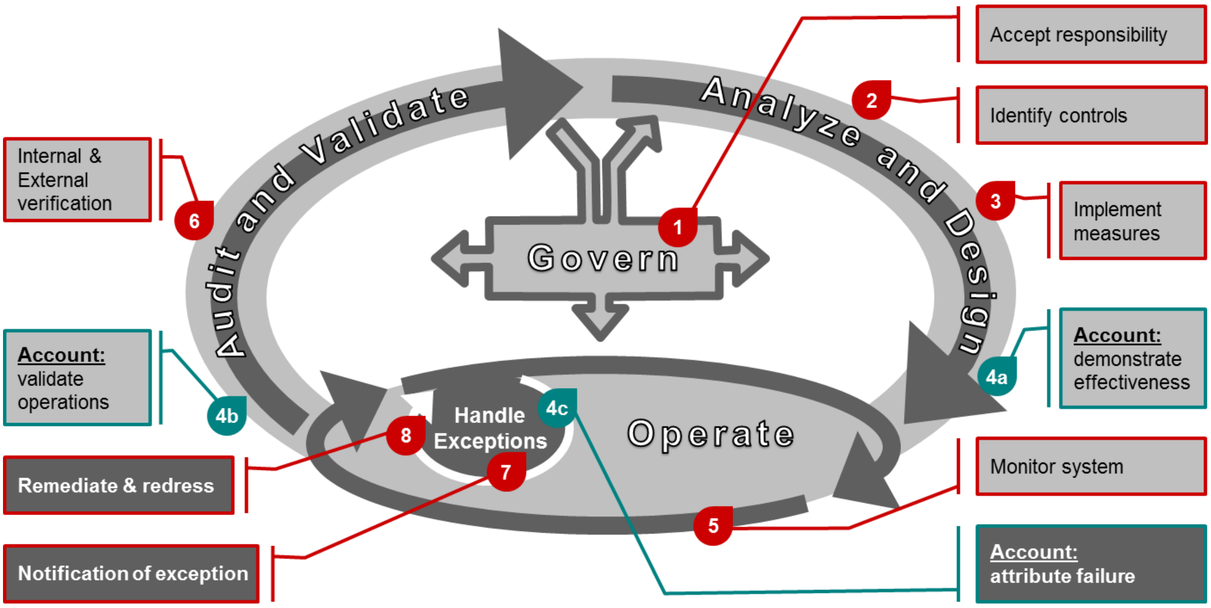


Figure 3 Functional aspects of accountability in an organisational lifecycle [10].

As pointed out in [6], accountability will not only be restricted to a set of tools; it will be necessary to adopt a holistic approach where goals and objectives are translated into controls that affect all dimensions of an organisation (social, business processes, IT processes etc.). However, since the purpose of refinement phase of WP:B-3 is to align the business use cases to the conceptual and technical work streams, the focus in this deliverable is largely technical and centred around the A4Cloud mechanisms and tools.

3 Business Use Case Overview

This section outlines the characteristics of the three Business Use Cases (BUCs) that have been developed in WP:B-3. For all three BUCs, we start by providing a brief summary of the BUC before providing a more technical description of how the BUC will be implemented. Note that this section serves as an introduction only; the three BUCs will be further analysed in the subsequent sections.

3.1 Business Use Case 1

The first business use case is about health care services in the cloud. In recent years there has been a significant growth in the use of wireless sensor networks in healthcare [9][10], which can be used for early detection of clinical deterioration through real-time patient monitoring in hospitals or at home, for improving the quality of life for the elderly through smart environments, and for monitoring of chronic diseases, to name just a few application areas. The cloud is a preferred solution for analysis and storage of data from medical sensor networks; not only because of cost advantages but also because of scalability and elasticity requirements. However, while implementing medical sensor networks in the cloud may be preferable from a technical point of view, the processing of sensitive personal data gives rise to a number of issues. To understand the accountability requirements in this business use case, it will be necessary to clarify what types of data will be collected, how they will be processed, shared and stored in the cloud and who will be responsible for them. Wireless sensor networks in the cloud will require particular attention to personal data protection in accordance to relevant legislation, as well as the support of strong privacy by design mechanisms. Medical data governance for access by multiple partners is a key issue in this business use case.

The healthcare system that we describe[4] will be used to support elderly people and other types of end users involved by making short-term and long-term analysis on the use of the behavioural and physiological data collected by wearable and environmental sensors. We investigate a case where medical data from the sensors will be exchanged between the elderly, their families and friends, caregivers, healthcare personnel, as well as a number of other actors and how the policies with respect to the protection of this data are defined and monitored during the provision of health care services. The proposed solution is the "M Platform" illustrated in Figure 4.

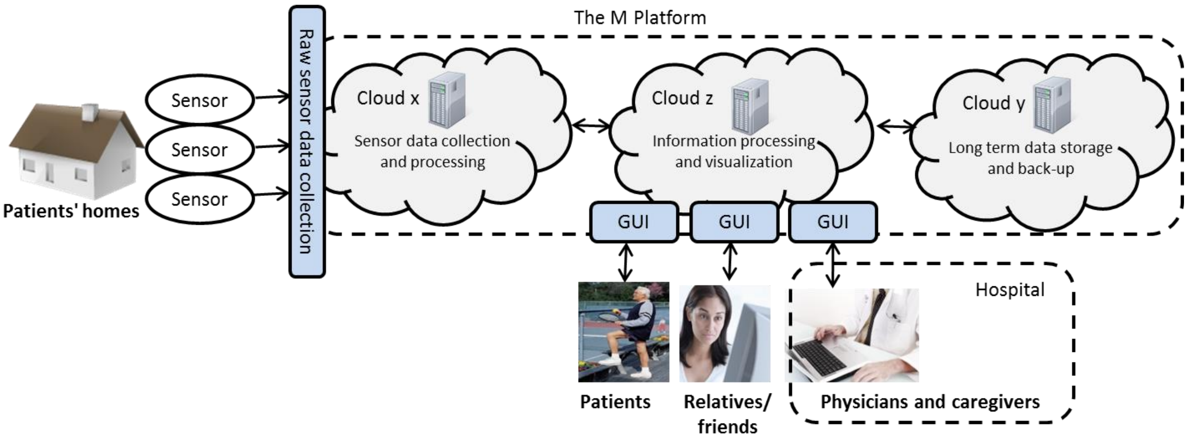

The M Platform
Patients' homes
Sensor
Sensor
Sensor
Raw sensor data collection
Cloud x
Sensor data collection and processing
Cloud z
Information processing and visualization
Cloud y
Long term data storage and back-up
GUI
GUI
GUI
Patients
Relatives/ friends
Hospital
Physicians and caregivers

Figure 4 A high-level conceptual view of the M Platform.

The M Platform is a cloud-based platform for medical sensor data collection, processing, storage and visualization. Patients will be connected to wireless sensors that monitor their vital signs (e.g., movement, blood pressure, pulse oximetry, temperature, position, etc.). The sensor data will be transmitted to the cloud where they will be further processed and stored, according to the specified policies and the established regulatory framework. The M Platform is assumed to be developed by an EEA-established software and service provider M, which will outsource to one or more external cloud providers both the sensor data collection and initial processing tasks (Cloud x, provided by X) as well

[4] Note that this is currently a theoretical study only; no implementation exists.

as the long-term data storage and back-up procedures (Cloud y, provided by Y). M therefore has a contract with X, and a separate contract with Y. The actual sensors themselves will be deployed by the hospital which engages M to provide the M Platform, under a contract between the hospital and M; the hospital has no direct contractual relationship with either X or Y. The information engine, which visualizes and displays information to the end users, will be implemented in M's own infrastructure (Cloud z). As can be seen in Figure 4, through graphical user interfaces (GUIs) the M Platform will interact with and provide services to a number of different users involved. Data that are being stored or processed in Cloud x or Cloud y are only accessible through using Cloud z, which provides GUIs for patients, relatives and friends, as well as selected employees (physicians and caregivers) at the hospital. Note that it is the hospital that provides accounts and logins to patients, relatives, staff etc., to enable them to access data through Cloud z.

Figure 5 outlines the technical landscape of a possible implementation of the health care business use case, including the possible use of a A4Cloud tools to achieve accountability in the cloud ecosystem[5].

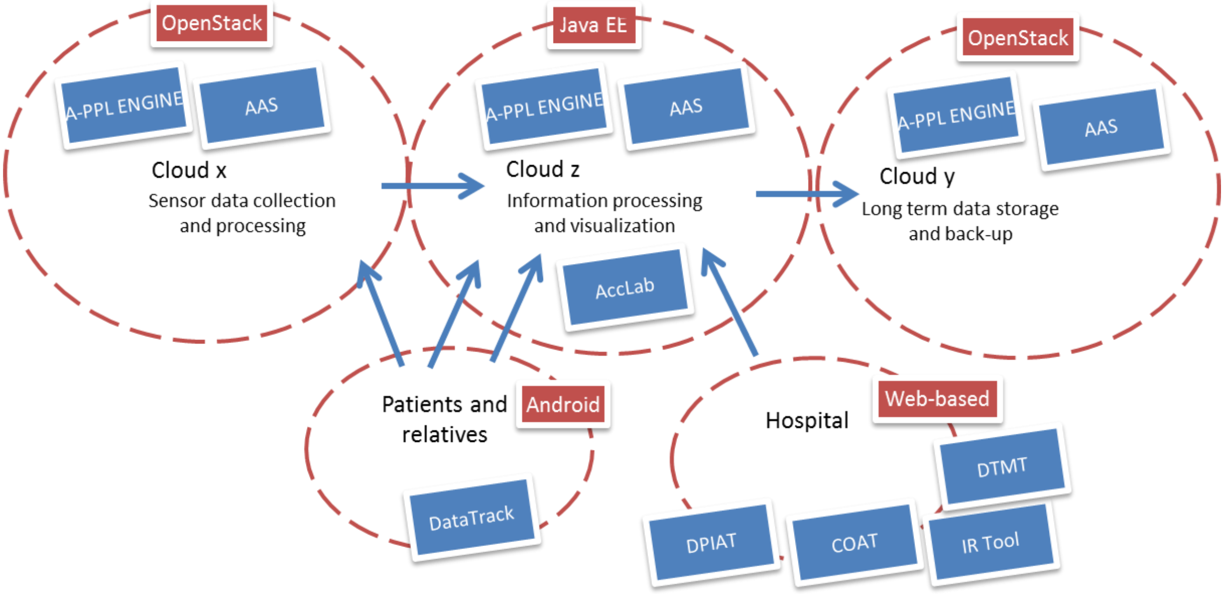


Figure 5 Business Use Case 1 Technologies Landscape

3.2 Business Use Case 2

The ERP (Enterprise Resource Planning) system that is the topic of this business use case is a cloud-based SaaS offering, capable of having its core functionality extended by third-party services. Personal data sharing that occurs during the communication between the primary and the third-party services are subject to specific obligations.

The SaaS ERP offering is used by a large supermarket chain operating in southern France. Among other business functionality it is also used to support the loyalty program that its customers can join to benefit from special product offers and discounts. The service offered by the supermarket tracks the customers' behaviour to determine their shopping habits and provides more personalized offers that customers are more likely to benefit from, respecting at the same time the customers' privacy.

The supermarket chain utilizes a PaaS cloud to deploy their loyalty program mobile application. Thanks to other services supplied by ISVs (Independent Software Vendors) on that platform, the application can directly use a mobile payment service supplied by a third party. The PaaS offering used in this scenario is on its own also deployed on an IaaS cloud, to leverage elastic infrastructure cloud capability.

[5] A more detailed mapping of how the A4Cloud tools can be used in the health care business use case domain is provided in Chapter 7 of this deliverable.

The landscape introduced in this business use case is depicted in Figure 6. MarchéAzur (the supermarket chain, SaaS provider), PaaSPort (PaaS provider) and InfraRed (IaaS provider) are all operating their cloud offerings, at the software, platform and infrastructure level respectively. In addition, Check-it-out (ISV) is offering platform extension in form of the SaaS offering that can be utilized by other cloud services.

MarchéAzur operates both a mobile application, which will be used by their customers in order to collect shopping information, as well as the back-office CRM (Customer Relationship Management) service operated by its business analysts. Data utilized by these applications is coming from the on-premise ERP system still operated by MarchéAzur. It is mainly information about the products offered in supermarket stores, information related to marketing campaigns and possible discount offers and other business data consumed by the analytics service.

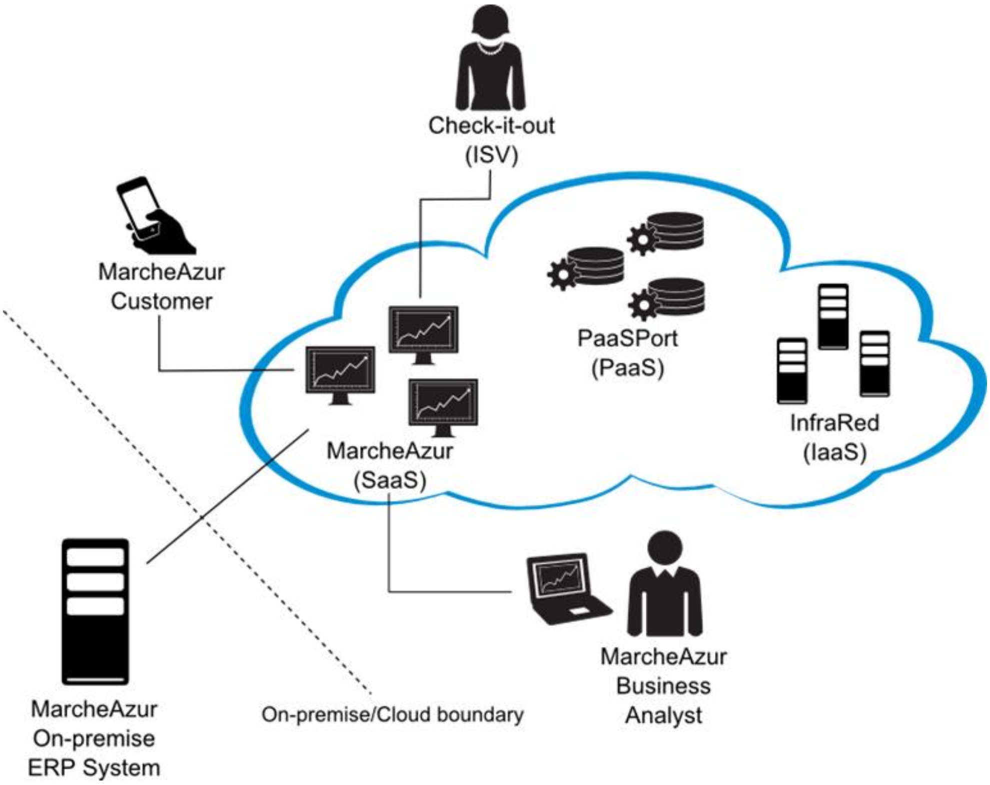


Figure 6 Conceptual overview of the cloud-based ERP business use case.

In this use case we plan to demonstrate how different cloud technologies are combined together to provide a business value for the individual end users and businesses. We have selected a set of technologies for SaaS and IaaS offerings that are standard and well-established industrial efforts. The technological landscape is depicted in Figure 7.

MarchéAzur CRM service is Java Platform, Enterprise Edition (Java EE)[6] application that runs as standalone web application deployed on the Apache Tomcat[7] servlet container. It utilizes a MySQL[8] database to provide persistency for its business and customer data.

Both the servlet container and the database are deployed on the computation node of the IaaS offering. The IaaS cloud platform selected for this use case is OpenStack[9]. The IaaS offering also uses back-up nodes that are managed by OpenStack.

[6] https://www.oracle.com/java/technologies/java-ee.html
[7] http://tomcat.apache.org/
[8] http://www.mysql.com/
[9] http://www.openstack.org/

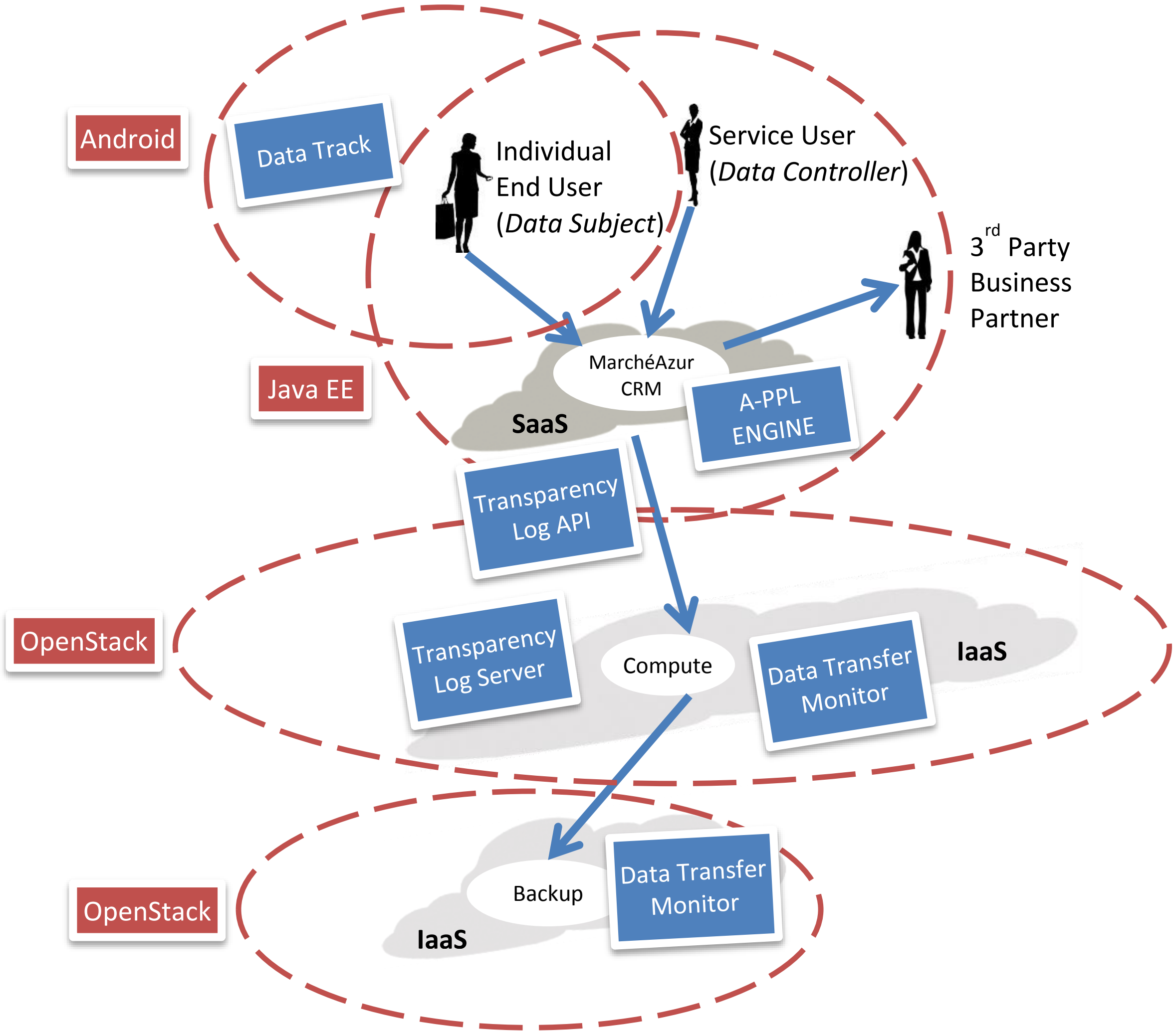


Figure 7 Business Use Case 2 Technologies Landscape.

In this business use case we primarily aim to demonstrate the following tools from the A4Cloud landscape: the A-PPL Engine, the Data Transfer Monitoring Tool (DTMT), the Data Track (DT), and the Transparency Log (TL). The A-PPL Engine will be used by the CRM service that is deployed as a SaaS offering while DTMT is meant to be used at the IaaS layer. DT will be used by the data subjects to receive notifications from MarchéAzur. TL serves as the communication channel between the A-PPL Engine and DT[10].

3.3 Business Use Case 3

This section describes the third business use case, which is called "Rights and relevant obligations in a multi-tenant cloud scenario". The cloud ecosystem we consider consists of a number of players that must interact in a very agile manner in order to both preserve the value of the cloud paradigm and its benefits for end users and also to ensure that providers can appropriately and independently manage policies, controls and users of cloud resources. Such an ecosystem may be relatively simple with a one-to-one chain, but it may become extremely difficult to manage in its complex forms. Multi-tenancy – *"the property of multiple systems, applications or data from different enterprises hosted on the same physical hardware"* [21] – exposes organisations as well as individuals to emerging issues in the cloud [22]. On the one hand, cloud computing is characterised by different features (i.e. on-demand service self-

[10] A more detailed mapping of how the A4Cloud tools can be used in this business use case domain is provided in Chapter 7 of this deliverable.

service, broad network access, resource polling, rapid elasticity and measured service) that enable complex Information and Communication Technology (ICT) deployments (exhibiting multi-tenancy, complex and dynamically changing environments, global and dynamic data flows, data duplication and proliferation, difficult to know geographic location and which specific servers or storage devices will be used, easy and enhanced data access from multiple locations). On the other hand, such cloud features expose organisations as well as individuals to cloud vulnerabilities that emerge at the governance level. Data duplication and proliferation (and its autonomic aspect) creates problems in terms of compliance. In addition, public cloud providers make it very easy to open an account and begin using cloud services, and that ease of use creates the risk that individuals in an enterprise will use cloud services on their own initiative, without due consideration of the risks and due governance process. There are also fears about increased access to data by foreign governments and other parties. Other issues include data lifecycle management across chains of suppliers, including data discovery and destruction, and legal risks that include security obligations, international transfers and the processing of sensitive data. For example, difficulties exist if users want to end a service, get their data deleted or export their data to another provider. Often, it is unclear who the data controller is and which parties have what responsibilities (MSC-2.2 [4] provides further analysis of emerging issues in cloud service provision). In particular, key issues (as highlighted by the Article 29 Working Party [23]) are the concerns regarding the loss of control and transparency (in the sense of insufficient information, thus making the task more difficult of selecting a suitable service from the vast choice of cloud offerings). The main features characterising this business use case are:

- **Personal and confidential data interaction:** individual cloud subjects or customers increasingly access cloud services both for personal and business purposes. The blurred boundaries between personal and business confidential data are difficult to draw. Governing data flows become very complicated and exposes cloud subjects (customers) as well as cloud providers to threats such as data breaches and data loss [24]. It is thus important to clarify rights and obligations of cloud customers and providers. Cloud subjects (customers) would benefit from awareness of how they comply with relevant policies while accessing cloud services in business contexts. Cloud providers would be able to adjust their services according to individual as well as organisational policies.
- **Bring Your Own Device (BYOD):** individual cloud customers increasingly access cloud services for personal use from within the enterprise domain. This trend is exposing organisations to security threats – *"Security challenges due to social computing and bring your own device (BYOD) policies will increase as new vulnerabilities walk in the door with employees"* [24]. Identifying suitable policies for using personal devices to access cloud services is a priority for most organisations. What is needed is the ability to verify whether or not specific data policies are satisfied while accessing cloud services for personal use within the enterprise domain.
- **Multi-tenancy:** the scenario focuses on data governance conflicts arising in the interaction between personal and confidential data flows. Conflicting and competing requirements are to a certain extent due to the nature of multi-tenancy – *"Multi-tenancy in its simplest form implies use of same resources or application by multiple users that may belong to same or different organization"* [24]. The challenge is guaranteeing policies throughout chains of accountability while services are accessed by multiple cloud users.
- **Data governance:** moving to the cloud introduces a separation between cloud subjects (customers) and the location where data is stored in the cloud. This separation between cloud subjects (customers) and their data increases the complexity of data governance as well as the risk of loss of governance. This is due to delegating responsibilities throughout cloud supply chains. Supporting data governance for cloud users and providers enhances cloud trustworthiness.

Figure 8 depicts the cloud ecosystem for the third business use case.

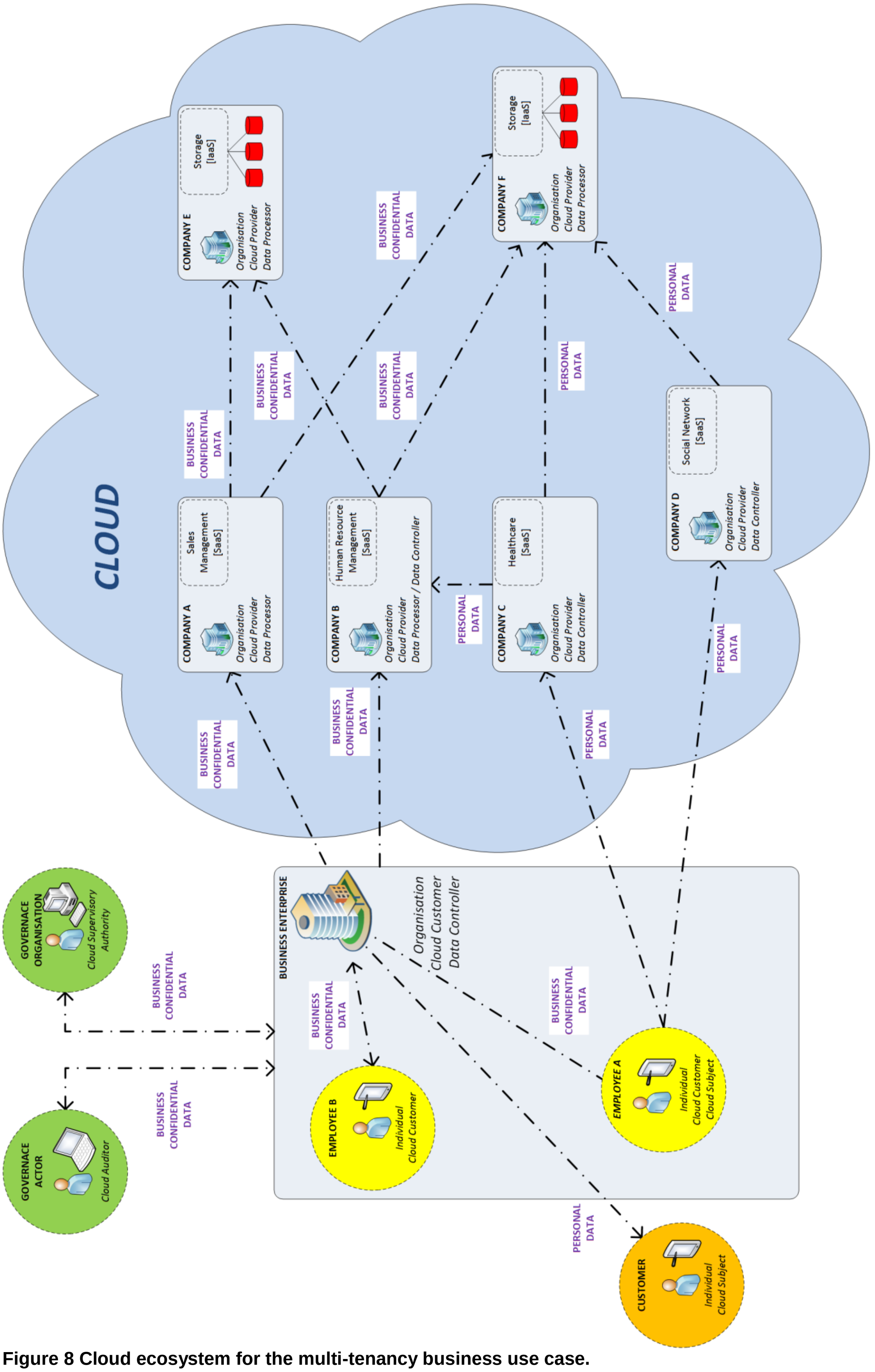


Figure 8 Cloud ecosystem for the multi-tenancy business use case.

4 The Actors Involved in the Business Use Cases Cloud Ecosystems

A cloud ecosystem is a complex system that consists of interdependent components that are composed in order to enable and deliver a cloud service. These components include not only a number of service delivery models where, for example, computing infrastructure, platforms and software are provided as a service, but also the different stakeholders (actors) that are involved, for example the users of the service and the providers of a service. Accountability in the context of a cloud ecosystem is concerned with correctly allocation of responsibilities amongst these actors. This section therefore identifies the actors involved in the different business use cases and classifies them in terms of the roles that have been defined in the project.

Our understanding and interpretation of the actors in a Cloud ecosystem is based on the reference architecture developed by NIST [8], which identifies the main actors and roles involved in a cloud ecosystem, as well as their activities and functions in terms of cloud computing. The NIST architecture takes a technical perspective, where roles are defined in order to clarify responsibilities on a system level, from an operational perspective. Their approach can be used to describe, discuss, and develop system specific architectures.

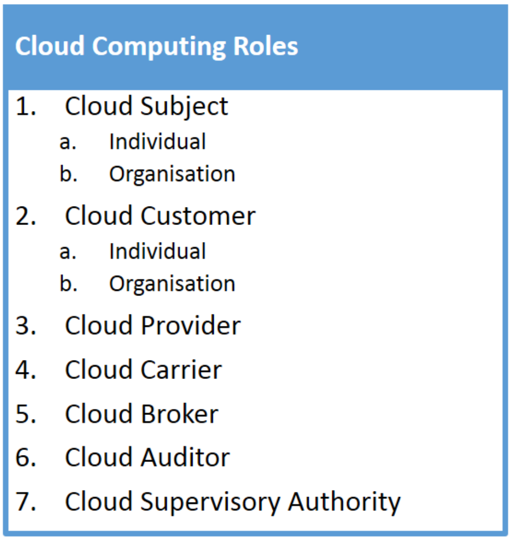
The NIST reference architecture allows us to analyse the business use cases from a technical perspective, however, in A4Cloud we need to take the legal and socio-economic perspective into account as well. The A4Cloud project has therefore proposed a revision to the NIST taxonomy, which includes with accountability. In the project documentation [10] the following seven accountability roles are identified:

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

In addition, six roles in the data protection domain have been defined:

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

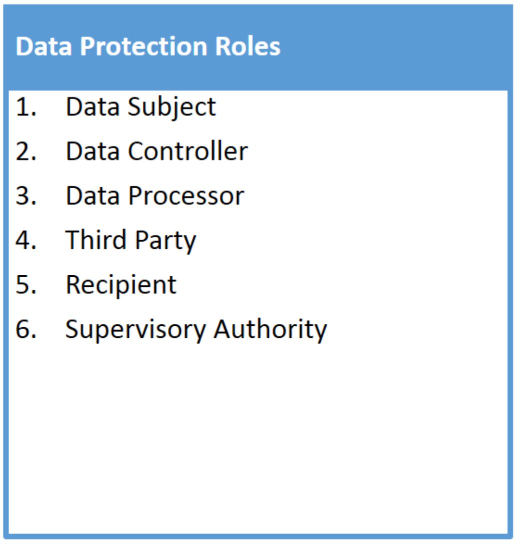
Hence two perspectives have been taken into account when defining the possible roles that an actor in the cloud ecosystem can take; cloud computing and data protection. These are summarized in Figure 9 and Figure 10. By correctly classifying each involved actor in a cloud ecosystem in terms of these roles, accountability relationships and responsibilities will become clear. More information can be found in the project documentation (see Chapter 4 in [10]). The rest of this chapter analyses each business use case in terms of these roles.



Cloud Computing Roles

1. Cloud Subject
   a. Individual
   b. Organisation
2. Cloud Customer
   a. Individual
   b. Organisation
3. Cloud Provider
4. Cloud Carrier
5. Cloud Broker
6. Cloud Auditor
7. Cloud Supervisory Authority

Figure 9 Cloud computing roles



Data Protection Roles

1. Data Subject
2. Data Controller
3. Data Processor
4. Third Party
5. Recipient
6. Supervisory Authority

Figure 10 Data protection roles

4.1 The Roles of the Actors Involved in Business Use Case 1

In the health care business use case, sensors communicating with the M Platform are used to collect sensor data from elderly persons who are suffering from dizziness, in order to help make a diagnosis. Here we describe the main characteristics of the actors involved and how they interact with the system. We then classify the actors using the method outlined in the beginning of this section.

- **The patients.** The patients are *Individual Cloud Subjects*, from whom the health care system collects personal data and sensitive personal data, including name, age, location, blood pressure, oxygen saturation, and more[11]. The patients will be able to access and review the data that have been stored about themselves and they will be able to check who has accessed or edited their personal data and when. Ultimately, patients also have the option of withdrawing from the system and having all their data expunged.
  According to the Directive, the patients will be *Data Subjects* since personal data will be collected from them, both through the use of sensors and when they log in to access and review their personal data as described above.
- **The relatives/friends.** The relatives/friends are *Individual Cloud Subjects* who upload further information about the patients and/or edit patients' data[12]. Also the relatives/friends will be able to access and review the data that have been stored about themselves[13] and they will be able to check who has accessed or edited their personal data and when. The relatives/friends can also access their respective patient's data and check who else has accessed the data and when. Ultimately, relatives/friends also have the option of withdrawing from the system and having all their data expunged.
  According to the Directive, the relatives/friends will be *Data Subjects* since personal data will be collected from them when they log in to access and review their or the patients' personal data as described above[14].
- **The hospital.** The hospital is the organization that diagnoses the patients and decides the appropriate treatment (through its staff, i.e., physicians and caregivers), and places sensors on or attaches sensors to the patients (or near the patients). The hospital has purchased access to the M platform from the M Platform provider. The hospital is therefore an *Organisation Cloud Customer* in the cloud ecosystem.
  According to the Directive, the hospital is a *Data Controller* of its patients' personal data, which it has chosen to process using M's cloud service. The hospital is also a controller over the personal data collected from relatives/friends as well as the personal data collected from hospital staff (see next bullet point). Note that it is each controller's responsibility to ensure that the relevant data subjects' personal data are processed in line with applicable legal requirements, including accountability obligations under the relevant data protection legislation.
- **The hospital staff.** The hospital staff (i.e. the physicians and caregivers) are *Individual Cloud Subjects* in the cloud ecosystem. The physicians and caregivers at the hospital will have the full picture of the patient's medical condition; being able to monitor the readings in real time as well as the patient's health record that is stored locally at the hospital. Hospital staff can access and edit data through the M Platform, are informed in advance that their operations are logged (and have consented to such logging), and logs are viewable by patients, relatives/friends as well as the hospital systems administrators.
  The hospital staff will also be *Data Subjects*. There will be logs of accesses and edits of patient data by identified or identifiable doctors, nurses etc., hence those individuals will be data subjects too and should consent to patients or relatives accessing those logs or some other legal basis should be found for allowing such access.
- **X.** X is the organization that operates the sensor data collection and processing cloud (Cloud x). X is a *Cloud Provider* (towards M) in the cloud ecosystem.
  X is a *Data Processor* of the personal data collected from the patients through the sensors.

[11] Note that the electronic health record itself is not part of the cloud solution.
[12] Note that allowing relatives to have control over patient data should be given careful attention since this scenario, while likely to occur, may give rise to many accountability challenges.
[13] Primarily this is related to the data about the patients, but metadata about relatives and their accesses and/or edits [and hospital employees and their accesses and/or edits] will also be available for review.
[14] Note that relatives/friends may also be characterised as controllers of the patients' personal data. See [3] for a further discussion on this.

- **Y.** Y is the organization that operates the long-term backup storage cloud (Cloud y). Y is a *Cloud Provider* (towards M) in the cloud ecosystem. Y is a *Data Processor* of the personal data that are stored in their data centres.
- **M.** M is the organization that delivers the cloud-based service (including software) for sensor data collection and processing to the hospital (the M Platform). M also operates Cloud z. M is both a *Cloud Provider* (towards the hospital) and an *Organisation Cloud Customer* (towards X and Y) in the cloud ecosystem. M is a *Data Processor* of the personal data collected from patients, relatives/friends and hospital staff[15].

Table 1 provides an overview over the involved actors and their roles, according to the classification provided in the beginning of this section.

Table 1: The roles of the actors in the health care business use case.

Cloud actor	Cloud computing role	Data protection role
Patients	Individual Cloud Subjects	Data Subjects
Relatives/friends	Individual Cloud Subjects	Data Subjects
Hospital	Organisation Cloud Customer	Data Controller
Hospital staff	Individual Cloud Subjects	Data Subjects
M	Cloud Provider; Organisation Cloud Customer	Data Processor
X	Cloud Provider	Data Processor
Y	Cloud Provider	Data Processor

In DB-3.1 we provided as-is and to-be scenarios for the following personas. We do not reproduce these scenarios in this report; however, for clarification we explain what roles these actors have in terms of the classification provided in the beginning of this section.

- **Kim** is a patient at the hospital. Kim is therefore an *Individual Cloud Subject* and a D*ata Subject* in the cloud ecosystem.
- **Sandra** is a relative of Kim. Also Sandra is an *Individual Cloud Subject* and a D*ata Subject*.
- **Michael** is a privacy officer at the IT department at the hospital. As an individual, Michael does not have any particular role in the cloud ecosystem. However, Michael is using the A4Cloud tools on behalf of the hospital, which (as explained above) is an O*rganization Cloud Customer* and *Data Controller* in the cloud ecosystem.
- **Peter** is a software architect at M. Similarly to Michael, Peter does not have any particular role in the cloud ecosystem. However, Peter is using the A4Cloud tools on behalf of M, which is an O*rganization Cloud Customer, Cloud Provider* and *Data Processor* in the cloud ecosystem.
- **Bruce** is an infrastructure manager at Y. Also Bruce does not have any particular role in the cloud ecosystem. However, Bruce is using the A4Cloud tools on behalf of Y, which is a *Cloud Provider* and *Data Processor* in the cloud ecosystem.
- **Leslie[16]** is a senior advisor at the Data Protection Authority (DPA). Leslie does not have any particular role in the cloud ecosystem. However, Leslie is using the A4Cloud tools on behalf of

[15] M (who is the primary service provider to the hospital) will be seen as the hospital's processor of the personal data, but would not be considered a controller in its own right unless, for example, it uses patients' personal data for its own (rather than the hospital's) purposes, such as by selling anonymized patient data to research companies.

[16] Note that Leslie, who is acting on behalf of a data protection authority, is not included in the list of actors described earlier in this section.

the DPA, which is a *Cloud Supervisory Authority* and *Supervisory Authority* in the cloud ecosystem.

4.2 The Roles of the Actors Involved in Business Use Case 2

We further describe the actors taking part in the ERP business use case as well as their relations towards each other in this enterprise cloud landscape. The roles are described in the same manner as in the health care business use case from the previous subsection.

- **The supermarket customers** are the individuals who are regularly shopping at MarchéAzur stores and who are enrolled in the supermarket loyalty program. The customers can receive personalized shopping deals thanks to constant monitoring of their shopping habits. The supermarket customers are *Individual Cloud Subjects* in the cloud ecosystem.
  The supermarket customers are sharing their personal data when they are subscribing to the loyalty program operated by MarchéAzur. As such, they are considered to be *Data Subjects* according to the Directive
- **MarchéAzur** is the supermarket chain and the SaaS provider, which offers its customers possibility to enrol into a loyalty program. The SaaS provided by MarchéAzur consists of a mobile application with an on-line shopping catalogue and the possibility to store shopping lists and to track the customers' habits related to their shopping behaviour. MarchéAzur is considered as a *Cloud Provider* (towards the supermarket customers) and an *Organisation Cloud Customer* (towards InfraRed, Check-it-out and PaaSPort).
  The MarchéAzur supermarket chain is a *Data Controller*, as it determines to collect information (including personal data) from their customers, which it uses to analyse customer shopping habits.
- **Check-it-out** is the Independent Software Vendor providing PaaS extensions, like mobile payment solutions. The SaaS provided by MarchéAzur offers the customers to finalize shopping deals on-line thanks to the payment via Check-it-out payment service. Check-it-out is considered as a *Cloud Provider* (towards MarchéAzur) and an *Organisation Cloud Customer* (towards PaaSPort).
  The mobile cloud application operated by the supermarket sends the customer information also to Check-it-out payment solution, so the ISV is considered a *Data Processor.*
- **PaaSPort** is the PaaS provider which is used by MarchéAzur and Check-it-out services for cloud deployment of their offerings. PaaSPort is considered as a *Cloud Provider* (towards MarchéAzur and Check-it-out) and an *Organisation Cloud Customer* (towards InfraRed).
  The platform provider PaaSPort is considered a *Data Processor*, as it does not directly collect the information from the data subjects, but nevertheless the supermarket customers' personal data is processed on behalf on the controller MarchéAzur in its cloud.
- **InfraRed** is the IaaS provider which is offering elastic cloud resources. The infrastructure provided by InfraRed is used by PaaSPort to deploy their PaaS offering. InfraRed is then considered as *Cloud Provider*.
  Also the infrastructure provider InfraRed is considered a *Data Processor*, as it does not directly collect the information from the data subjects, but nevertheless the supermarket customers' personal data is processed on behalf on the controller MarchéAzur in its cloud.

Table 2 summarizes the actors involved in the business use case and their subsequent roles according to the classification provided in the beginning of this section.

Table 2: The roles of the actors in BUC2.

Cloud actor	Cloud computing role	Data protection role
The supermarket customers	Individual Cloud Subjects	Data Subjects

Cloud actor	Cloud computing role	Data protection role
MarchéAzur	Organisation Cloud Customer	Data Controller
Check-it-out	Cloud Provider; Organisation Cloud Customer	Data Processor
PaaSPort	Cloud Provider; Organisation Cloud Customer	Data Processor
InfraRed	Cloud Provider	Data Processor

In DB-3.1 we provided as-is and to-be scenarios for the following personas. We do not reproduce these scenarios in this report; however, for clarification we explain what roles these actors have in terms of the classification provided in the beginning of this section.

- **Alice** is a customer at MarchéAzur and a loyalty program participant. Alice is an *Individual Cloud Subject* and a *Data Subject* in the cloud ecosystem.
- **Bob** is a business analyst at MarchéAzur. Bob does not have any particular role in the cloud ecosystem. However, Bob is using the A4Cloud tools on behalf of MarchéAzur, which (as explained above) is an O*rganization Cloud Customer* and *Data Controller* in the cloud ecosystem.
- **Charles** is a cloud software developer at PaaSPort. Charles does not have any particular role in the cloud ecosystem. However, Charles is using the A4Cloud tools on behalf of PaasPort, which (as explained above) is a *Cloud Provider*, O*rganization Cloud Customer* and *Data Processor* in the cloud ecosystem.
- **David** is a cloud software developer at Check-it-out. David does not have any particular role in the cloud ecosystem. However, David is using the A4Cloud tools on behalf of Check-it-out, which (as explained above) is a *Cloud Provider*, O*rganization Cloud Customer* and *Data Processor* in the cloud ecosystem.
- **Edgar** is a cloud infrastructure administrator at InfraRed. Edgar does not have any particular role in the cloud ecosystem. However, Edgar is using the A4Cloud tools on behalf of InfraRed, which (as explained above) is a *Cloud Provider* and *Data Processor* in the cloud ecosystem.
- **Frank** is a senior advisor at the CNIL (the French Data Protection Authority). Frank does not have any particular role in the cloud ecosystem. However, Frank is using the A4Cloud tools on behalf of CNIL who acts as a *Cloud Supervisory Authority* and a *Supervisory Authority* in the cloud ecosystem.

4.3 The Roles of the Actors Involved in Business Use Case 3

This section identifies the main cloud actors that are relevant for the cloud ecosystem that the third BUC is concerned with. From a business perspective, various stakeholders may be relevant depending on specific operational and deployment situations.

- **Cloud infrastructure provider (cloud provider):** a cloud infrastructure provider (IaaS provider) will manage and operate infrastructure resources on behalf of multiple cloud providers, and hence need to be able to enforce controls required by the end user.
- **Cloud service provider (cloud provider):** a cloud service provider (SaaS provider) will typically operate service level resources on behalf of multiple cloud service customers, and sometimes on behalf of other cloud service providers (service aggregation). Hence they need to be able to enforce controls as agreed with their customers. For example, a cloud service provider may be a SaaS provider, operating on an IaaS provider infrastructure, and delivering the SaaS service to many enterprises, businesses, or individual end customers.
- **Cloud service customer (cloud customer):** a cloud service customer could be an individual, or a business. When it is a business it adds another actor down the chain, typically a customer or employee of the cloud service customer. In addition, aggregation of cloud services at each layer

(e.g. IaaS, SaaS) means that the chain of actors can extend horizontally across providers before they reach a service user or an individual end customer.

- **Individual end customer (cloud customer):** an individual end user is usually the entry point to the chain and the provider (data subject) of the personal data which may be at risk along the processing chain.
- **Business end customer (cloud customer):** a business end customer may deserve a specified level of protection in terms of rights and obligations in order to preserve business confidential data. These rights and obligations may differ from applicable regulatory requirements due to data protection law. Moreover, some business domains (e.g. healthcare) may have additional regulatory obligations of confidence which need protecting. Note that for purely business confidential data (i.e. not personal data) there is no data protection role. In such cases a Business Enterprise will be a cloud customer but not a data controller (or anything else).

Table 3: The roles of the actors in BUC3.

Cloud actor	Cloud computing role	Data protection role
Business Enterprise	Organisation Cloud Customer	Data Controller
Employee A	Individual Cloud Subject	Data Subject
Employee B	Individual Cloud Subject	
Customer	Individual Cloud Customer	Data Subject
Company A	Organisation Cloud Provider (Cloud Customer)	Data Processor
Company B	Organisation Cloud Provider (Cloud Customer)	Data Controller; Data Processor
Company C	Organisation Cloud Provider (Cloud Customer)	Data Controller
Company D	Organisation Cloud Provider (Cloud Customer)	Data Controller
Company E	Organisation Cloud Provider	Data Processor
Company F	Organisation Cloud Provider	Data Processor
Governance Actor	Cloud Auditor	
Governance Organisation	Cloud Supervisory Authority	Data Protection Authority

In DB-3.1 we provided as-is and to-be scenarios for the following personas. We do not reproduce these scenarios in this report; however, for clarification we explain what roles these actors have in terms of the classification provided in the beginning of this section.

- **Sandra** is an employee and an end user of the cloud services that her organisation has purchased. She is a *Cloud Subject* and a *Data Subject* in the cloud ecosystem.
- **Paul** is a chief privacy officer at a SME. Paul does not have any particular role in the cloud ecosystem. However, Paul is using the A4Cloud tools on behalf of his employer, which (as explained above) will be an Organization Cloud Customer and Data Controller in the cloud ecosystem.
- **Roger** is the chief technology officer at a cloud service provider. Roger does not have any particular role in the cloud ecosystem. However, Roger is using the A4Cloud tools on behalf of his employer, which (as explained above) is a *Cloud Provider* and *Data Processor* in the cloud ecosystem.
- **Michael** is a cloud auditor in BUC3. Michael hence acts as a *Cloud Auditor* in the cloud ecosystem. (Michael does not have any data protection role.)

- **John** is a regulator, working at an (unnamed) data protection authority. John is using the A4Cloud tools on behalf of his employer, which acts as a *Cloud Supervisory Authority* and a *Supervisory Authority* in the cloud ecosystem.

4.4 Summary

In this chapter we have analysed the roles and responsibilities of all the actors involved in all the three business use cases that are described in the A4Cloud deliverable DB:3.1 [5]. Similar analysis can be made for any cloud ecosystem in order to clarify who is responsible for what and what accountability tools that will be appropriate to deploy in this context.

5 Obligations and Policies in the Business Use Cases

This section is devoted to an analysis of the business use cases from the point of view of accountability obligations, that is what the various actors in a cloud ecosystem will expect or will ensure related to accountability. In this section we take a dual perspective on accountability and look at obligations that come from both the legal perspective[17] as well as from the normative perspective.

5.1 Deriving Accountability Obligations

The work on **legal accountability** and obligations in WP B-5 [15] has identified two types of legal obligations: *regulatory obligations* and *contractual obligations*. In the scope of this project, regulatory obligations will arise from the current data protection directive [9] and from the proposed general data protection regulation [16].

Contractual obligations essentially take regulatory obligations, which may be at a high level, and translate them into specific binding obligations between the parties [15]. These obligations are also, in addition to regulatory obligations, based on non-legislative obligations such as industry standards and norms.

A4Cloud also considers the **normative** perspective. By this we mean that cloud service providers and their customers/users should not only behave according to certain rules because they (legally) have to but they also have a moral responsibility. As outlined in MSC:2.3, "accountability could encourage organisations to act as moral agents and adopt an ethical approach in regard to respecting and protecting the personal data and confidential information of customers, employees and partners, and encourage corporate responsibility" [10]. A normative obligation is a requirement, agreement or promise derived from social norms. Normative obligations hence imply for an organisation to act responsibly and to justify and explain ones conduct. In this section we outline a number of accountability obligations from the normative perspective, which will be necessary to meet the involved stakeholders' expectations on for example transparency and privacy.

The list of obligations that we have proposed in this section is based on the project's guiding light requirements[18] [17], the stakeholder requirements elicitation efforts in WP:B-2 [18][19] as well as an analysis of the characteristics and needs of actors involved in the three different business use cases.
Our approach is illustrated in Figure 11, which illustrates that accountability obligations stem from a combination of regulatory regimes, contracts, organisational policies and stakeholders' expectations.

[17] Note that the analysis of the legal perspective in this section focuses on obligations related to the processing of personal data; the scope of the A4Cloud project is also business confidential information but due to lack of harmonization of in the field of business sensitive information we only focus on obligations with respect to the processing of personal data as provided under the EU Data Protection Directive [9]. This directive regulates the processing of personal data within the European Union.

[18] In short, the guiding lights requirements states that an accountable organisation must 1) demonstrate willingness and capacity to be responsible and answerable for its data practices, 2) define policies regarding its data practices, 3) monitor its data practices, 4) correct policy violations and 5) demonstrate policy compliance.

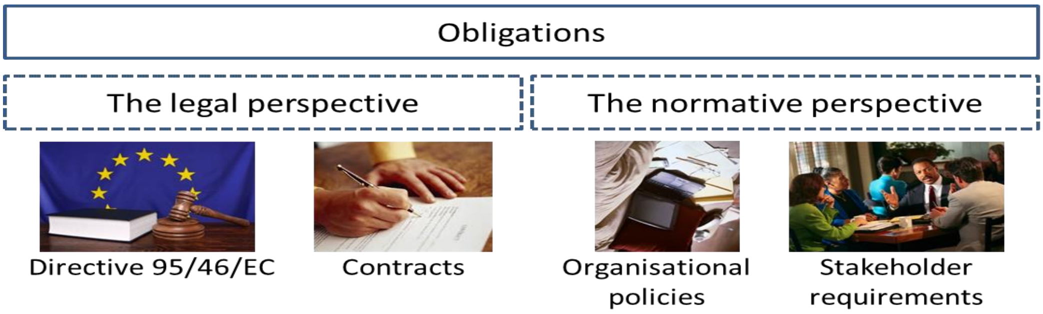


Figure 11 Accountability obligations can be derived from the legal and normative perspectives.

5.2 Obligations from the Legal Perspective

The regulatory perspective (i.e. the Data Protection Directive) provides us with a number of obligations, to which controllers and processors have to adhere to. Here we present an initial list of obligations, which have been directly derived from the accountability relationships outlined in [15]. These obligations are expressed in terms of *<actors 1> is accountable to <actor 2> for <doing something>*.

- **Obligation 1: informing about processing**. Data subjects have the right to know that their personal data is being processed. This means that *the controller is accountable to the data subjects for informing that their personal data is being collected and processed*.

- **Obligation 2: informing about purpose.** Data subjects also have the right to know why their personal data is being processed. This means that *the controller is accountable to the data subjects for informing about the purpose of collecting and processing their personal data*.

- **Obligation 3: informing about recipients.** Data subjects have the right to know who will process their personal data. This means that *the controller is accountable to the data subjects for informing about the recipients of 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. This means that *the controller is accountable to the data subjects for informing about the existence of their rights to access and rectify the collected 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. This means that *the controller is accountable to the data subjects for collecting personal data only for specific, explicit and legitimate purposes*. Moreover it also means that *the controller is accountable to the data subjects for processing their personal data only for the stated 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[19]. These means that *that the controller is accountable to the data subjects for their rights to access, collect and rectify their personal data.* In practice this means that the controller must ensure that the data subjects have read and write grant access to their personal data and that there are means to enforce the deletion of such data, throughout the service delivery chain.

- **Obligation 7: data storage period.** Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which they were collected. This means that *the controller is accountable to the data subjects for keeping their personal data in a form which permits identification for no longer than necessary.* In practice this means that the controller must make sure that all personal data are either deleted or anonymized after the data collection purpose has been fulfilled.

- **Obligation 8: security and privacy measures.** Controllers are responsible to the data subjects for the implementation of appropriate technical and organizational security measures, which ensures an appropriate level of security in relation to the risk represented by processing their personal data. This means that *controllers are accountable to the data subjects for the security and privacy of the personal*

[19] Note that deletion is not an unconditional right. The data subject needs “compelling legitimate grounds“ to request deletion.

data they collect. The controller must therefore ensure that appropriate security and privacy preservation measures have been implemented throughout the service delivery chain.

- **Obligation 9: rules for data processing by provider.** Controllers are accountable to data subjects for how sub-providers process their personal data. Therefore the controllers must ensure that the processor(s) they engage does not process the personal data except on the controller's instructions (unless they are required to do so by law). Hence, *controllers are accountable to data subjects for how the processors process the data subjects' personal data*.
- **Obligation 10: rules for data processing by sub-providers.** For the same reason as the previous obligation, 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). Hence, *controllers are accountable to data subjects for how sub-processors process the data subjects' personal data*.
- **Obligation 11: provider safeguards.** *Controllers are accountable to data subjects for choosing data processors that can provide sufficient safeguards* concerning technical security and organizational measures. The controller therefore must ensure that the processor(s) they engage provide sufficient safeguards to protect the personal data that they process.
- **Obligation 12: sub-provider safeguards.** The previous obligation comprises all processors in a service delivery chain. Hence, *the controller is accountable to the data subjects for ensuring that all sub-providers involved in the service delivery chain provide sufficient safeguards* to protect the personal data that they process.
- **Obligation 13: informed consent to processing.** *Controllers are accountable to the data subjects for obtaining informed consent before collecting personal data*[20].
- **Obligation 14: explicit consent to processing.** *Controllers are accountable to the data subjects for obtaining explicit consent before collecting sensitive personal data.*[21]
- **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*[22].

In Table 4 the regulatory obligations are mapped to BUC 1 and BUC2.

Table 4 Regulatory obligations mapped to BUC1 and BUC2.

Regulatory obligations	BUC 1	BUC 2
O1:informing about processing	The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers
O2: informing about purpose	The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers
O3: informing about recipients	The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers
O4: informing about rights	The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers
O5: data collection purposes	The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers
O6: the right to access, correct and delete personal data	The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers

[20] Note that this only applies when consent is the legitimate basis for data collection.
[21] "Explicit consent" means that an individual is clearly presented with an option to agree or disagree to the collection of personal data. Explicit consent can be provided verbally or in writing.
[22] Note that this depends on the country. Some countries request notifications, others do not.

Regulatory obligations	BUC 1	BUC 2
O7: data storage period	The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers
O8: security and privacy measures	The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers
O9: rules for data processing by provider	The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers
O10: rules for data processing by sub-provider	The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers
O11: provider safeguards	The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers
O12: sub-provider safeguards	The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers
O13: informed consent to processing	The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers
O14: explicit consent to processing	The hospital is accountable to patients (when processing sensitive personal data)	N/A (there is no processing of sensitive data)
O15: explicit consent to processing by joint controllers	The hospital is accountable to patients (when allowing relatives to upload patient personal data)	N/A (there is no processing of sensitive data)
O16: informing DPAs	The hospital is accountable to the relevant DPA.	MarchéAzur is accountable to the relevant DPA.

In addition to the obligations that follow directly from regulation, the Directive requires certain clauses to be represented in the contracts between the service providers and the service customers, when personal data is being processed in the service that has been purchased. The most important obligations that can be derived from this perspective are:

- **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*. Sub-providers that process personal data (with or without their knowledge) will become processors too.
- **Obligation 18: security breach notification.** *Controllers are accountable to data subjects for notifying them of security incidents* that are related to their personal data[23].
- **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 informing them about the location of the processing of their personal data*. Cloud providers must therefore have contractual obligations towards their respective customers on the location of the infrastructure where they process personal data.

In Table 5 the contractual obligations are mapped to the different business use cases.

Table 5 Contractual obligations mapped to BUC1 and BUC2.

Contractual obligations	BUC 1	BUC 2
O17: informing about the use of sub-processors	M is accountable to the hospital for informing about their usage of X and Y.	Check-it-out is accountable to MarchéAzur for informing about their usage of PaaSPort.

[23] Not that this is not in the current Data protection Directive [9], but in the Proposed Regulation [16].

Contractual obligations	BUC 1	BUC 2
		PaasPort is accountable to Check-it-out for informing about their usage of InfraRed. PaasPort is accountable to MarchéAzur for informing about their usage of InfraRed.
O18: security breach notification	X and Y are accountable to M. M is accountable to the hospital. The hospital is accountable to the patients, relatives/friends and hospital staff.	Check-it-out is accountable to MarchéAzur. PaasPort is accountable to Check-it-out and MarchéAzur. InfraRed is accountable to PaasPort. MarchéAzur is accountable to their customers.
O19: evidence of data processing	X and Y are accountable to M. M is accountable to the hospital.	Check-it-out is accountable to MarchéAzur. PaasPort is accountable to Check-it-out and MarchéAzur. InfraRed is accountable to PaasPort.
O20: evidence of data deletion	X and Y are accountable to M. M is accountable to the hospital.	Check-it-out is accountable to MarchéAzur. PaasPort is accountable to Check-it-out and MarchéAzur. InfraRed is accountable to PaasPort.
O21: data location	X and Y are accountable to M. M is accountable to the hospital.	Check-it-out is accountable to MarchéAzur. PaasPort is accountable to Check-it-out and MarchéAzur. InfraRed is accountable to PaasPort.

5.3 Obligations from the Normative Perspective

In addition to the regulatory and contractual perspective, the A4Cloud project also aims to facilitate for service providers to implement accountability ethically, i.e. to "do the right thing". In this subsection we outline a set of obligations, which we consider to be important for the actors in cloud ecosystems to become accountable, from the security and privacy perspective. These obligations are expressed in terms of *<actors 1> should do something related to <actor 2>*. Since the normative perspective is based on the relations between a service customer and the service provider, these obligations are based on the cloud computing roles (cf. Section 2) rather than the data protection roles.

- **Obligation: informing about personal data processing.** Cloud customers should inform cloud providers that they will use their services to process personal data.
- **Obligation: personal data minimization.** Cloud providers should offer their customers services that have been designed to minimize the amount of personal data they collect from the service users (i.e. the end users).
- **Obligation: privacy-by-default**. Cloud providers should offer their customers services that have been designed in such a way that the strongest privacy settings are the default settings (seen from the service users' perspective).
- **Obligation: specifying user preferences**. Cloud providers should offer their customers services that allow the users to specify privacy preferences.
- **Obligation: monitoring of data practices**. Cloud providers should monitor their actual data practices and keep records of the monitoring and its results.
- **Obligation: compliance with user preferences**. Cloud providers should be able to provide evidences to their users that personal data is processed in accordance to their preferences.
- **Obligation: compliance with privacy policies**. Cloud providers should demonstrate to their customers and users compliance with their policies in a timely fashion “reactively” and where possible “proactively”.

- **Obligation: informing about policy violations**. Cloud providers should inform their customers and their users about any policy violations that are related to their personal data
- **Obligation: informing about privacy preferences violations**. Cloud providers should inform their customers and their users about any violations of their privacy preferences
- **Obligation: remediation in case of damages:** Cloud providers should provide remediation to their customers and their users in the case of damages caused to data subjects due to processing of personal data.

In Table 6 the ethical obligations are mapped to BUC 1 and BUC 2.

Table 6 Ethical obligations mapped to BUC1 and BUC2.

Ethical obligations	BUC 1	BUC 2
O: informing about personal data processing	The hospital is accountable to M M is accountable to X and Y.	MarchéAzur is accountable to PaaSPort. Check-it-out is accountable to PaaSPort. PaaSPort is accountable to InfraRed.
O: personal data minimization	The hospital is accountable to the patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers. Check-it-out is accountable to MarchéAzur's customers.
O: privacy-by-default	M is accountable to the hospital	MarchéAzur is accountable to their customers. Check-it-out is accountable to MarchéAzur's customers.
O: specifying user preferences	M is accountable to the hospital The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers. Check-it-out is accountable to MarchéAzur's customers.
O: monitoring of data practices	X and Y are accountable to M M is accountable to the hospital	InfraRed is accountable to PaaSPort PaaSPort is accountable to MarchéAzur and Check-it-out
O: compliance with user preferences	M is accountable to the hospital The hospital is accountable to patients, relatives/friends and hospital staff.	MarchéAzur is accountable to their customers. Check-it-out is accountable to MarchéAzur's customers.
O: compliance with privacy policies	X and Y are accountable to M M is accountable to the hospital The hospital is accountable to patients, relatives/friends and hospital staff.	InfraRed is accountable to PaaSPort PaaSPort is accountable to MarchéAzur and Check-it-out MarchéAzur is accountable to their customers.
O: informing about policy violations	X and Y are accountable to M M is accountable to the hospital The hospital is accountable to patients, relatives/friends and hospital staff.	InfraRed is accountable to PaaSPort PaaSPort is accountable to MarchéAzur and Check-it-out MarchéAzur is accountable to their customers.
O: informing about privacy preferences violations	X and Y are accountable to M M is accountable to the hospital The hospital is accountable to patients, relatives/friends and hospital staff.	InfraRed is accountable to PaaSPort PaaSPort is accountable to MarchéAzur and Check-it-out MarchéAzur is accountable to their customers.
O: remediation in case of damages	X and Y are accountable to M M is accountable to the hospital The hospital is accountable to patients, relatives/friends and hospital staff.	InfraRed is accountable to PaaSPort PaaSPort is accountable to MarchéAzur and Check-it-out MarchéAzur is accountable to their customers.

5.4 The Relation between Obligations and Policies

In the A4Cloud glossary [11], the term *obligation* is defined as: "A prescription that a particular behaviour is required". Simply speaking, an obligation is therefore a requirement that must be fulfilled. Obligations can be categorized depending of the context, as we did in the previous section with the legal, contractual and normative perspectives. As this term is referring to social, political, or general contexts, obligations are usually expressed in natural language.

Policy is a broad term denoting rules, principles or protocols established by an entity to guide its decisions and to achieve some effects or actions. In a computer science/security context, a policy refers to a sentence that can be executed (or enforced) by a policy engine. The A4Cloud glossary defines the term policy as: "A set of rules related to a particular purpose. A rule can be expressed as an obligation, an authorization, permission or a prohibition. Not every policy is a constraint. Some policies represent an empowerment." [11].

An exhaustive analysis of policy languages and obligation representations was performed in deliverable D34.1 [25]. Policies are usually written in some dedicated languages or domain specific languages. One of the most well-known policy languages is XACML [30], a standard XML-based language dedicated to access control. In deliverable D34.1 [25], accountability policies are viewed as a set of rules to (i) allow end users or businesses to define how personal and/or confidential data in cloud environments can be processed and (ii) allow cloud service providers to give an account for all operations. Thus, accountability policies will include not only obligations relating to security and privacy, but also obligations relating to the accountability attributes currently identified in WP:C-2 (i.e. assurance, verifiability, observability, etc.). In this analysis, we note that while existing policy standards are suitable for access and usage control, they do not cope with accountability and they are not close to natural language. Therefore, providing a direct mapping of regulations and legal texts to a machine-readable language can be a cumbersome task. We also studied existing work on formal and semi-formal approaches that can be used to map obligations to a human, and at the same time machine, understandable language (for instance, SecPal4P [31], or SIMPL [32]). However, these approaches do not consider accountability but only privacy concerns.

The term *enforcement* is defined in the New Oxford American Dictionary as: "*the act of compelling observance of or compliance with a law, rule, or obligation: the strict enforcement of environmental regulations*"[24]. In the A4Cloud context, enforcement can be seen as the process of making obligations (i.e. accountability obligations) machine understandable and executable. The work performed in WP:C-4 on policy representation distinguish between mapping and enforcement. The mapping is the translation of an obligation to another language in order to prepare it for enforcement. A policy is then the operational aspect of an obligation at the time of enforcement. This view has been further developed in deliverable D43.1 [26].

As stated before, obligations, either legal, contractual or normative, are natural sentences. They are written in some natural languages and only understandable by humans. It is rather difficult to make them executable or understandable by machines, thus enforcement is preceded by a mapping process. The mapping translates parts of an obligation into an executable language, and then the enforcement is able to understand the policy and to apply it on resources and agents involved in the context.

In A4Cloud, we propose to semi-automatically map textual obligations into concrete policies that are specified in A-PPL [25] [27]. A-PPL is an extension of PPL [34], which is in turn an XACML extension. A-PPL was introduced in A4Cloud by WP:C-4 in order to represent concrete accountability policies [25]. To simplify the translation and to automate it as long as possible, an intermediate language called AAL (Abstract Accountability Language) is also proposed [25] [28]. The process is illustrated in Figure 12.

To understand the enforcement process we should have in mind three different levels: Natural language (needs expressed as obligations), Abstract language (as clauses) and Concrete language (as policies).

- Obligations: they are written in natural language, English in this deliverable. They are coming from different areas: legal (regulatory and contractual), and normative.

[24] See http://www.oxforddictionaries.com/definition/english/enforcement

- Accountability clauses: they are written in AAL, a formal language with permission, interdiction and temporal modalities. They only capture some of the obligations taking into account an abstract operational design of the obligation context. More details and a first methodology are available in [28] [29].
- A4Cloud policies: they are written in A-PPL. They describe rules to execute the accountability clauses.

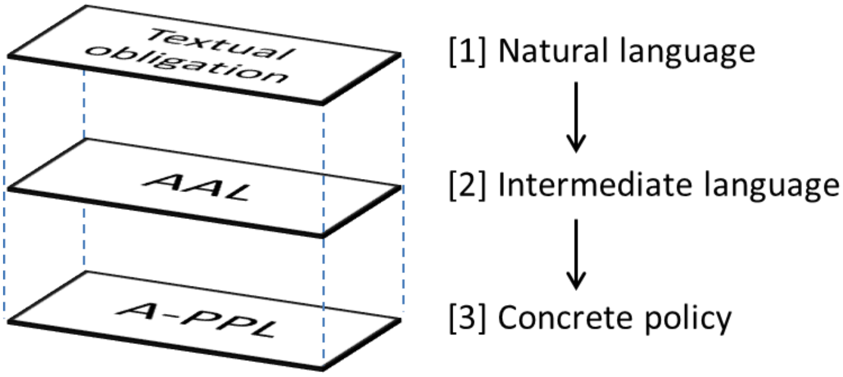


Figure 12 Mapping obligations from the legal terms expressed in a natural language to concrete policies expressed in machine-readable code.

Mapping and enforcement is a kind of refinement process. In software engineering, refinement is devoted to implement an abstract sentence into a more concrete one, adding implementation details. This is the usual process we run when we program an algorithm into a programming language. In computer science refinement is generally seen as a generic term that encompasses various approaches for producing correct computer programs and for simplifying existing programs in order to enable for example formal verification. In our case mapping is not a strict refinement since there are aspects of obligations we cannot implement in a machine or aspects we do not want to implement. For instance, some abstract obligations are not operational at all (the data controller is responsible of data management) and in other situations we do no aim at making it executable (the judge decides of the guiltiness of someone).

To precisely illustrate the three levels the next section provides some examples of obligations and their translation into AAL and in A-PPL or XACML.

5.5 Examples of the Mapping of Obligations to Policies in the Healthcare Domain

Figure 13 provides an overview over how obligations can be mapped to policies for the healthcare business use case (BUC 1). The mapping of most of the obligations identified in this chapter will fit into this approach. For example, consider Obligation 17 (informing about the use of sub-processors). This obligation implies that M is accountable to the hospital for informing about their usage of X and Y as sub-processors of the patients' personal data. This is a contractual obligation, which means that the Directive requires a clause about the usage of provider X and Y's services to be present in M's contract with the hospital. M will therefore express this obligation in terms of an AAL clause, which will be mapped into a machine-readable A-PPL policy. The A-PPL policy can then be further distributed to the sub-providers X and Y[25], in order to prevent them from doing any further outsourcing of the processing of the patients' personal data to other service providers, which are not present in the current configuration of the M platform.

[25] The A-PPL policy can either be distributed separately from the patient data (either by sending it directly to the sub-providers or by making it accessible from a policy repository), or it can be translated into a sticky policy that travels together with the patient data. Note that sticky policies are not part of the A4Cloud framework.

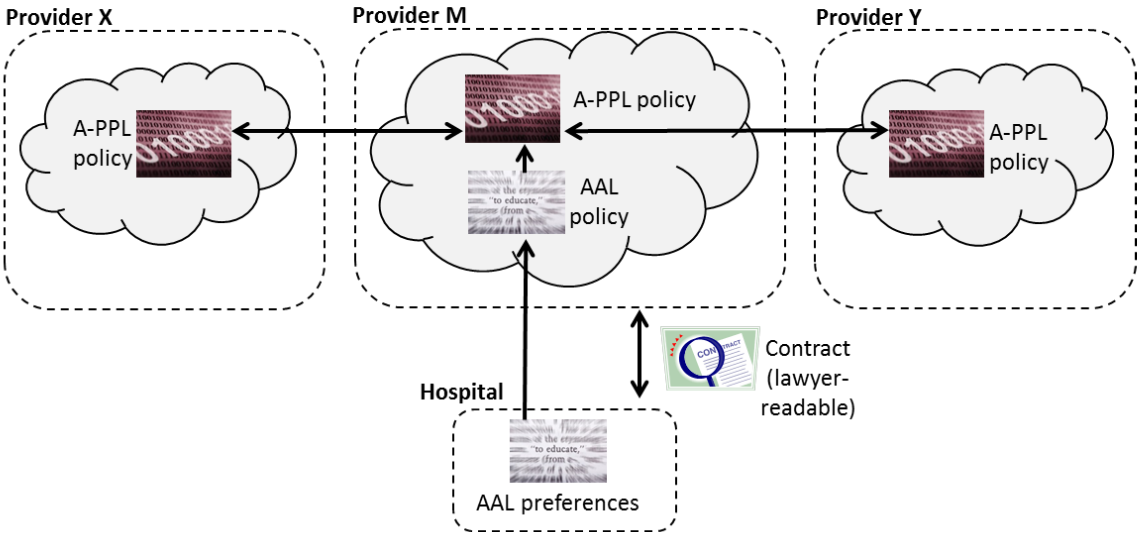


Figure 13 An overview over how obligations can be mapped to policies for BUC 1.

Note that (as implied in Figure 13) it is also possible that provider M can take the hospital preferences into account when defining the AAL policy.

More information on the mapping of obligations to policies for the A4Cloud business use cases, as well as a number of concrete examples, can be found in the WP:C-4 publications [25][27][28][29].

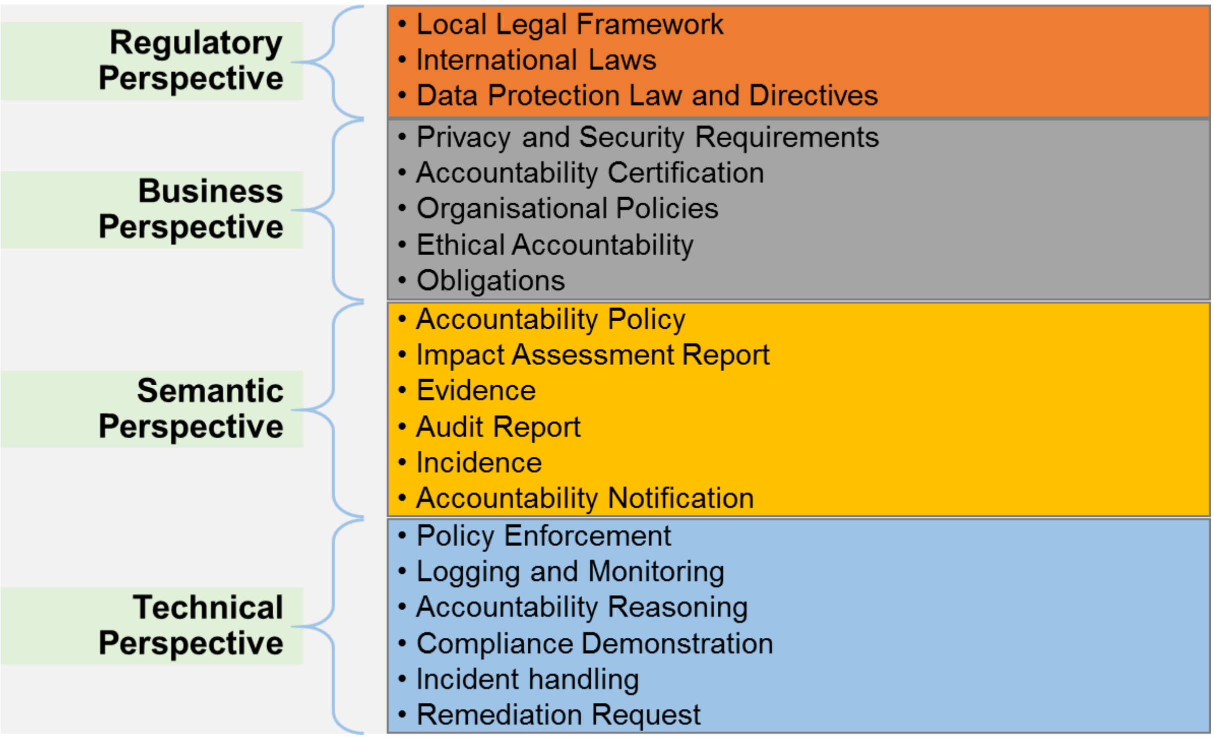
6 Interoperability Requirements for the Business Use Cases

Interoperability describes the ability of diverse systems and organizations to exchange and make use of information[26]. In the context of accountability, WP:C-3 has derived a set of logical requirements needed to support the accountability attributes in a cloud ecosystem. These have been documented in deliverable D:C-3.1 [7]. In this section we aim to contribute to this work by outlining some additional requirements that will arise from the business use cases perspective. The requirements have been derived from a high-level perspective, meaning that they are not specific to the different business use case domains.

The adoption of accountability in real business transactions being evolved in cloud environments introduces a set of requirements, which need to be fulfilled by the actors taking part in the relationships described in the business use cases and the tools used to accomplish these use cases. The accountability perspective is realised through the different accountability attributes that can be defined across complex cloud service chains and may lay on more than one accountability phases (i.e. as per work in D:C-3.1 [7], these phases can be named as agreement, report, compliance, remediation) during a cloud service lifecycle. In that respect, the interactions between the business use case cloud actors must be seen at the specific timing of the cloud service lifecycle (e.g. requirements, design, development, operation, etc.), in which they serve the needs of the respective business use case scenarios.

6.1 Introduction to the Interoperability Perspectives

The analysis of the interoperability requirements for the business use cases must be examined from four conceptually distinct perspectives, as they are depicted in Figure 14. This figure shows a hierarchical top down approach for realising the interoperability points in the A4Cloud business scenarios. As it can be seen, these points are shared among the A4Cloud business use cases, and they correlate the business level security and privacy requirements, which express the limitations of the business transactions involving personal and business confidential data, with the restrictions of the regulatory framework and the system level implementation mechanisms to achieve accountability.



[26] Oxford dictionary. http://oxforddictionaries.com/definition/english/interoperable

Figure 14: The cross layer interoperability perspectives of the A4Cloud business use cases.

Whether A4Cloud targets health, online shopping or any other domain, the scope is to make the involved stakeholders being accountable with respect to the data governance processes in the cloud. To achieve this in a multi-player environment, the involved actors, as they are assigned the respective cloud computing and data protection roles, should share common understanding on who is interacting with whom, for which purpose and through which means. The cloud ecosystem that hosts the development and the runtime invocation of the A4Cloud business use cases introduces additional interoperability requirements, as third parties are delegated with tasks related to the collection, management and processing of personal data, when building a complex chain of cloud service providers. As such, the business use cases would need for cross-layer interoperability concepts, accountability information and respective mechanisms, so that the involved actors efficiently interoperate and facilitate the business functionalities in an accountable manner.

In more details, the four perspectives for defining the accountability-based interoperability requirements for the A4Cloud business use cases are the following:

- The Regulatory Perspective includes the requirements introduced by the existing regulatory framework, the restrictions and the rules stemming for this framework and the provisions of the local and international laws and directives (such as the Data Protection Directive), with respect to the way that sensitive data should be collected, processed, analysed and stored from the various actors, in the cloud service provision chain.
- The Business Perspective includes the requirements to enable the various use cases actors to be attributed specific (cloud computing / data protection) roles and interact with each other in the cloud ecosystem, according to their assigned responsibilities. In this layer, we consider the organisational policies, which provide the framework for the interactions between the parties involved from a privacy and security point of view and the ethical perspective of accountability, as an inherent incentive to collaborate in a business context and from a societal perspective and comply with specific data governance and information security standards and provisions when executing any kind of business requiring interaction with other parties. This perspective, also, includes the need for an organisation to be accountable and establish business relations driven by the dimensions of the accountability framework (i.e. the accountability attributes)|, as it is defined in WP:C-2.
- The Semantic Perspective, in essence, consists of those commonly acceptable accountability information objects necessary to effectively draw and define the accountability relationships / interactions among the business use case actors. Such data objects involve the accountability policy specification, which comprises the means for a common way to formulate legal and moral obligations and business responsibilities, which extend the security and privacy requirements and providers' offerings in both human and machine readable interfaces, and the certificate of compliance, as the point of reference for rapid assessment on the compatibility and the level of maturity for meeting accountability requirements in the context of bilateral interactions between the cloud business actors. Furthermore, the semantic perspective includes the information, which is needed to build the interactions happen across all the stages of the accountability lifecycle, as it will be explained later.
- Finally, the Technical Perspective exhibits the mechanisms to deliver the interoperability semantics defined in the previous layer. In practice, this perspective hosts the means and protocols for enabling the mutual communication between the business actors. Many interactions are involved here, as shown in Figure 14.

In each perspective, the interactions of the business use case actors refer to four phases (as they have been introduced in WP:C-3), which are distinguished, according to whether they address the:

- Establishment of mutual agreements in the scope of data governance processes in the cloud (Agreement Phase)
- Monitoring of the proper execution of mechanisms to meet these agreements and the data handling processes stemming from them (Reporting Phase)
- Verification of the practices adopted by the business actors to show compliance with the accountability practices (Demonstration Phase)
- Support of remediation in case of failures to implement the specific data handling policies (Remediation Phase)

For each category, a set of specific interactions can be identified, which are attributed to the four interoperability perspectives, depicted in Figure 14.

6.2 The Regulatory Perspective

The established Legal Framework, at both national and international level, serves as the starting point, in order to explore the relationships and the interactions between the various actors in cloud ecosystems. At this point, the interoperability analysis of the business use cases focuses on how personal and business confidential data are to be protected when they are processed in the cloud in order to facilitate the execution of specific service and application business goals. Taking into account the domains under study and the envisaged cloud service paradigms, the regulatory perspective gives the basis for A4Cloud to define and implement the means for demonstrating accountability in the context of the relationships between all actors in the business use cases.

The regulatory framework governs the classification of the data involved in business transactions in the context of a specific business domain. Thus, personal and business confidential data can be considered as sensitive and, in that respect, they should be handled accordingly, when developing the needs of the domain specific scenarios. The Data Protection Directive provides for additional requirements with respect to the processing of sensitive personal information (for example information relating to health data). Therefore the processing of sensitive information as described in the HealthCare business use case, for instance, should take place following the explicit consent given by the data subjects. Sensitive personal data may also be subject to specific local laws and their management and processing should comply with them (for example, health data should not be processed outside the country boundaries that they are produced). However, when delivering such data in the cloud, different legal frameworks and regulatory rules might be applied, depending on the geographical boundaries of the data handling procedures, which introduce further complexity to the data governing practices in the cloud for the business use cases.

Thus, we can define a set of interoperability requirements in the Regulatory Perspective, which drive the classification of sensitive data involved in the A4Cloud business use cases and the respective data handling processes that should be implemented and supplement the security and privacy mechanisms. These requirements introduce specific legal restrictions and provide directives on the respective obligations that should be allocated to the business use case actors, depending on their assigned cloud computing and data protection role, as follows (the analysis refers to data protection roles):

- Establishment of agreements between the business use case actors, who are involved in the development of a cloud service chain, namely the data controllers, the data processors. These actors should make sure that the established agreements are in accordance to the local and international laws and the respective data protection directives.
- Establishment of agreements between the business use case actors, who are involved in the specification of the necessary type of personal and business confidential data that should be disclosed to the cloud service chain. The legal framework should define the identification of responsibilities of the data controllers towards the cloud subjects and the relevant legal obligations that should be in the form of legal bindings. The legal obligations should dictate the type and the security level of the data handling processes, which should be adequately explained and detail on the “who, when and for which purpose” of these processes.
- The allocation of responsibilities for the monitoring of the data handling processes among all the business actors to report on specific preventive mechanisms adopted against security breaches and other incidents.
- The compliance of the business actors to specific detective and corrective mechanisms, as they are obliged by specific legal rules. Such a capability implies demonstration of the appropriate actions, followed by the data controllers and processors, to authorised agents, such as the cloud auditors and the data protection authorities. During this Demonstration Phase, the Regulatory Perspective can offer insight on those data handling practices that the controllers and processors should showcase to the data protection authorities, based on the classification of the involved data.
- Definition and implementation of risk mitigation and remediation strategies, including the notification of the cloud providers and cloud customers about specific incidents being evolved in a business transaction and the communication of the adopted corrective mechanisms to the cloud subjects.

6.3 Business Perspective

From a business perspective, the interoperability aspects of the A4Cloud business use cases relate to the analysis of the user and legal driven security and privacy requirements and their integration into the typical business flow. These requirements are compiled into organisational level policies, which primarily identify the major interoperability points between the various actors involved in the execution of the business use cases. Depending on the scale of the envisaged use case, there might be necessary to establish a chain of cloud service providers, which are selected to be accountability certified and transparently offer the required level of security. The complexity of the chain and the allocation of responsibilities among the participants of the chain should be well defined in the organisational policies, along with the legal obligations residing in each cloud actor.

From an ethical point of view, the business actors are to adopt a societally friendly attitude to their collaborating parties, when delivering secure cloud services to their customers. The moral implications of this action are reflected in the form of normative obligations, which supplement the legal ones in terms of who is responsible to whom and for what. This ethical based accountability leads to completing the set of obligations defined in the previous perspective and both of them entail the appropriate level of commitment from the business actor's perspective to address certain accountability requirements and implement specific security and privacy mechanisms, which fulfil their assigned tasks across the four phases in a cloud-based business scenario.

Across the chain of actors involved in the A4Cloud business use cases, an accountability information flow is built, which drives the interactions between the cloud subjects and the data controllers and processors. This flow draws the path of interactions between the business actors and the processes that should be executed by them from a Business Perspective. In that respect, the following set of interoperability requirements can be defined:

- In the Agreement Phase, the cloud customers and providers should define their security and privacy provisions, along with their legal and moral obligations, using common objects from the Semantic Perspective (see Section 6.4). Each obligation is realised as a policy rule that corresponds to the respective accountability attributes of the accountability framework to be implemented across business practices for each actor (thus incorporating the concept of the accountability attributes in the definition of their business practices).
- In the Reporting Phase, both the controllers and the processors should be able to define the strategy for sharing evidence on the proper use of any kind of personal and business confidential data and reporting them to the cloud customers and the data subjects.
- In the Demonstration Phase, both the controllers and the processors should define the strategy to show compliance with the accountability policies and the rules defined in it with respect to data governance processes, as well as taking the responsibility for demonstrating their accountability maturity to the Cloud Auditors and Data Protection Authorities, upon request.
- Finally, in the Remediation Phase, from a Business Perspective, the interoperability should be achieved between all the business use case actors by defining the policies to incorporate within their business objectives the need for implementing risk mitigation strategies and undertaking appropriate corrective actions in case of security breaches. The actual receivers of these actions are the data holders of the business use cases. Furthermore, in this phase, all cloud actors should interface with the Cloud Auditors to demonstrate their capacity to implement any corrective actions taken on their behalf, as a result of remediation towards a detective security incident.

6.4 Semantic Perspective

In the Semantic Perspective, common data objects and accountability information are encompassed. These items are shared among the involved business actors, in order to effectively accomplish the operations and processes identified in the business perspective.

The accountability information stems from the implementation of the obligations and the privacy and security requirements. Such information is defined at the level of the interaction phases and takes the form of meaningful interoperability resources (i.e. human readable text and documents, machine readable data specifications), which are the main derivative of the communication and the interactions happen among the cloud business actors to support accountability.

Thus, the interoperability requirements in the semantic perspective are presented as follows:

- Generate an Impact Assessment Report to guide the Agreement Phase between the business actors that are assigned as cloud customer and the cloud providers, with respect to the risks involved in the disclosure of cloud subjects' data in a specific cloud service chain, exhibiting certain functional, privacy and security characteristics.
- Define the Accountability Policy to support the mechanism in the Agreement Phase. The policy is defined between the actors disclosing their data to the cloud ecosystem and the data controllers, along with any collaborating cloud third parties. Such a policy is supported by the individual agreements established among the business actors who are responsible for processing personal and business confidential data.
- Exploit the logs produced by the logging mechanisms of the various event generation tools in the Reporting Phase to provide a unified specification of the Evidence, elaborating on the occurred actions, the actors performed them and when, as well as any further information that can support the connection to the interoperability requirements of the Agreement Phase (namely the accountability policy)
- Analyse the types of evidences that can constitute an Incident, which should facilitate the Reporting Phase and the detection of abnormal behaviour from the business actors. An Incident should be communicated to all the actors in the cloud service chain.
- Facilitate the Demonstration Phase by specifying the form of an audit report, which should be exchanged among the business actors to show compliance with the required and agreed practices. Such a semantic object is, also, communicated to the Cloud Auditors and the Data Protection Authorities, including the previously mentioned Evidence.
- Define a common approach for servicing the Accountability Notification. Such data object needs to be semantically described, so that the business actors can efficiently implement the mechanisms both in the Reporting and the Remediation Phases.

6.5 Technical Perspective

From a technical perspective, interoperability refers to the channels used so that the business use case actors involved in the three domain specific studies can communicate and exchange the semantically enriched data streams, as they introduced in the previous Subsection 6.4. For each phase, a set of specific interactions is defined as interoperability requirements among the business actors.

The technical interoperability mechanisms that are needed from an accountability point of view are summarised in the following:

- Implementation of Policy Agreement and Enforcement mechanisms for the Agreement Phase to enable cloud subjects and data controllers to agree on an Accountability Policy and enforce it during the execution of the business scenarios in the cloud service chain.
- Deployment of Logging and Monitoring mechanisms for the Reporting Phase to facilitate the collection of the necessary logs from various sources of evidence.
- Implementation of Accountability Reasoning mechanisms to serve the interaction of the business cloud actors in the Reporting Phase towards exchanging the semantically described Evidence.
- Development of Compliance Demonstration mechanisms to facilitate the interoperability of the Cloud Auditors and the Data Protection Authorities with the business actors to showcase the way that accountability is supported in the business scenario execution.
- Implementation of the Incident handling mechanisms to enable cloud subjects and the providers in the cloud chain to be notified of failures and security breaches.
- Development of Remediation Request mechanisms to enable the business actors involved in the Remediation Phase to communicate the appropriate remediation actions in response to a detected incident.

7 A Tool Analysis of the Business Use Cases

This section provides an analysis of the business use cases *BUC1: Health Care Services in the Cloud*, *BUC2: Cloud-based ERP Software with Third-party Extensions* and *BUC3: Rights and Relevant Obligations in Multi-tenant Cloud*, especially the to-be scenarios described in the deliverable D:B-3.1 [5][27], with respect to the tools developed in the A4Cloud project. The to-be scenarios are mapped to a preliminary description of the tools that were made available by WP:D-2 (Architecture) for internal use in the project (the "Tool's specification handbook") and where necessary on other early design documents gathered throughout the project. Since the to-be scenarios are heavily based on the individual point-of-view of the cloud actor, the focus of the analysis is directed towards the tools' interfaces that the actor is using. Some functionality, which is described in the scenario, might not be provided by the mapped tool itself, but another A4Cloud tool that the mapped tool is interfacing with. Some of these connections between tools are already identified in the architecture described in WP:D-2. However, revealing these connections between tools is not the focus of this analysis. The goal is to identify functionalities described in the scenarios, which can be addressed by the A4Cloud tools and also to identify gaps, where there is currently no tool providing that functionality to stakeholders or missing to-be scenarios. The analysis has been performed solely in the context of WP:B-3, however, the results have been reviewed by some of the researchers who are responsible for the design and implementation of the actual tools.

To demonstrate the integration of the scenarios and tools within the organisational accountability governance process, the identified mappings are classified according to the functional accountability aspects of this process. As was mentioned in Section 2 of this deliverable, the functional elements of accountability identified by WP:C-2 are:

1. Accept responsibility
2. Identify controls
3. Implementation of measures
4. Provision of an account
    a. Demonstrate effectiveness
    b. Validate operation
    c. Attribute failure
5. Monitoring system
6. External verification
7. Notification
8. Remediate and redress

Figure 3 in Section 2 depicts the integration of the functional elements in an organizational lifecycle. The lifecycle has mainly two types of accountability elements: proactive elements, which are mainly part of the "analyse and design" phase and reactive elements, which are part of the "operate" and "audit and validate" phases.
The combination of tool/scenario mappings with an analysis regarding the functional accountability aspects enables a better understanding of the integration into the organizational lifecycle. In the following, we present an overview of the analysis results. For the complete mapping tables, refer to Appendix B. Note that all the scenarios that we refer to in this section are documented in deliverable D:B-3.1 [5].

7.1 Contract & Risk Management

Related Tools: Data Protection Impact Assessment Tool (DPIAT), Cloud Offerings Advisory Tool (COAT)

The tools provided in this category are the *Data Protection Impact Assessment Tool (DPIAT)* and *Cloud Offerings Advisory Tool (COAT)*. DPIAT enables SMEs to identify risks associated with particular cloud-

[27] Due to space limitation we do not reproduce the to-be scenarios from DB:3-1 [5] in this deliverable. However, the reader is recommended to have [5] in readiness when reading this chapter.

related business transactions. COAT tries to assist its users in understanding and comparing cloud offerings with respect to privacy, security, compliance and accountability. The user groups COAT addresses are SMEs and individual end-users planning to move to the cloud.

7.1.1 Scenario/Tool Coverage Analysis

Regarding BUC1 there are two scenarios, which can be addressed by using COAT and DPIAT, scenario 3.1.2a (Michael identifies risks in the service provisioning chain) and scenario 4.1.4a (Peter searches for alternative sub providers). However, regarding scenarios 4.1.1a-b (Peter drafts the contracts with St Olav hospital, Peter drafts the contracts with the sub providers) and 4.1.2a (Peter renegotiates a contract), which focus on contract negotiation support on the cloud provider side, it is currently unclear, whether or not COAT and DPIAT can be used in these scenarios. This is mainly due to COAT and DPIAT focusing on contract support for data subjects and other cloud customers, such as SMEs. Also, COAT and DPIAT may not be used for negotiating actual contract terms. Therefore, the extent to which these tools support contract negotiation for cloud providers (e.g., support for negotiating terms between cloud providers) is not clear. It is also possible that these scenarios will not be addressed by A4Cloud tools but rather describe common negotiation of contracts.

BUC2 scenarios 8.1.1b (Bob updates a risk assessment) and 10.1.1a (David assesses the privacy impact) are addressed by COAT and DPIAT, since the focus is on provider evaluation by cloud customers and risk analysis. The same applies for scenarios mapped to contract & risk management tools in BUC2 and BUC3. However, similarly to some of the BUC1 scenarios, these scenarios describe actions performed by a cloud provider. This is why careful attention has to be paid to whether or not the provider is an SME or not.

7.1.2 Functional Accountability Aspects

Scenarios relevant for contract and risk management, where DPIAT and COAT will be useful, can generally be connected to the “analyse and design”-phase and its accountability functions. Therefore, they can be characterized as enabling proactive functions. For instance, performing risk assessments along the provider chain (e.g., BUC1 – 3.1.2a) or a cloud provider selecting another sub-provider according to specific criteria (e.g., BUC1 – 4.1.4a). These scenarios and tools are clearly part of the “analyse and design” phase.

7.2 Policy Definition and Enforcement

Related Tools: Accountability Lab (AccLab), A-PPL Engine, Data Transfer Monitoring Tool (DTMT)

The tools provided in this category are the Accountability Lab (AccLab), the A-PPL Engine and the Data Transfer Monitoring Tool (DTMT). The A-PPL Engine is the core tool for privacy policy enforcement in the A4Cloud toolset. It is planned that the A-PPL Engine will provide a user interface for experts to interact with. Cloud customers and providers will interact with AccLab to define and update policies. The Data Transfer Monitoring Tool is a tool that provides data location and transfer monitoring. This enables users to query for evidence about whether or not obligations regarding personal data have been carried out properly. However, it does not interfere with data transfers, but analyses compliance of transfers retroactively.

7.2.1 Scenario/Tool Coverage Analysis

Since AccLab is the central tool for writing obligations, which can be checked and transformed into A-PPL policies, most scenarios that involve creating, updating, viewing and deleting policies can be mapped to this tool. However, depending on the different types of users (e.g., individuals, providers, data protection officers etc.), there might be the problem of overwhelming or requiring too much technical knowledge from the user. The planned A-PPL Engine GUI has been considered in scenarios, where substantial knowledge of the A-PPL can be assumed. This is not considered to be the case for individual end users, but for instance developers and data protection officers. The Data Transfer Monitoring Tool presents valuable functionality regarding data locality and data transfers. Scenarios, where such information has to be available on demand can be mapped to this tool.

7.2.2 Functional Accountability Aspects

The tool/scenario mappings in this area are mostly relatable to the “operate” and “audit and validate” phases of an organisational lifecycle.

DTMT is considered with observing data transfers that happen in the cloud. Users of this tool (data privacy officers, cloud auditors) try to uncover data transfer policy violations. Therefore, DTMT clearly fulfils a monitoring function in the operate phase as well as external verification and validation of operation in the audit and validate phase.

AccLab enables its users to express and define data processing policies, which the A-PPL Engine enforces. This can be categorized as being part of the provision of an account. AccLab allows its users to define and display policies in place at the provider, which is part of the demonstration of good practices regarding data processing by the CSP.

The A-PPL Engine fulfils a number of accountability functions. Monitoring of the enforcement of data processing policies is one of its most important functions, especially in scenarios, where this information is used for validation and external verification, such as when this information is evaluated during an audit by the Audit Agent System. Also, the A-PPL Engine fulfils notification functions in scenarios, where a stakeholder needs to be notified about any detected incidents (e.g., as stated in a privacy policy). Such incidents may be reported to the A-PPL Engine by other A4Cloud tools, which are concerned with the validation of operation and external verification, such as AAS, DTMT or IRT.

7.3 Evidence & Validation

Related Tools: Audit Agent System (AAS), Assertion Tool (AT)

The tools provided in this category are the Audit Agent System (AAS) and the Assertion Tool. AAS provides auditors with a means to automatically audit multi-tenant and multi-layer cloud infrastructures, including audits of policies along service provision chains. The Assertion Tool is used to validate the correctness of the other A4Cloud tools. As of now it is not supposed to be used in a live-system, but before shipment of the A4Cloud tools. Currently, there are no to-be scenarios, which can be linked with this tool, and therefore it is excluded from further analysis.

7.3.1 Scenario/Tool Coverage Analysis

The AAS is assigned to scenarios, which include aspects like periodical verification of policy compliance. Thereby, different groups of users (e.g., internal and external auditors with varying levels of technical expertise) are considered by providing audit reports containing compliance statements at varying levels of abstraction. User groups like providers and auditors are addressed. Notifications about detected violations are often linked with the monitoring of systems or audits in the BUC’s scenarios. However, AAS does not produce “notifications” to report violations in real-time but forwards detected violations to other tools for further processing (e.g., issuing of notifications or initiating remediation processes) There are also cases, where AAS interfaces with other A4Cloud tools, for example Data Track and its plugin for policy violations, to collect information for the audit reports.

7.3.2 Functional Accountability Aspects

Tools from this category are typically used during the audit and validate phase. AAS implements functions such as monitoring the system, validating operation and external verification by auditors. Additionally AAS plays an important role during the operation phase, where evidences are collected by the monitoring.

The Assertion Tool plays a somewhat different role, than the other A4Cloud tools, since it is only intended for validating the A4Cloud toolbox before shipping. It is not used during cloud deployment planning or operation. Because of this, it does not directly contribute to any of the lifecycle’s phases.

7.4 Data Subject Controls

Related Tools: Data Track (DT), Transparency Log (TL), Data Subject Access Request Tool (DSART)

The tools provided in this category are Data Track, Transparency Log and the Data Subject Access Request Tool. All of these focus on data subjects (e.g., individual end users) as the primary user. Data Track enables data subjects to be informed about the disclosure of their data to service providers. Additionally, Data Track provides a plugin, which informs the user about policy violations and enables him to assess such violations by presenting an ordered measurement (quantitative or qualitative) of the relevance of the event. The Transparency Log tool is also tightly coupled with Data Track. It provides a cryptographically secured channel from the provider to the data subject to transmit notifications and logs. Currently, there is not enough information available about the Data Subject Access Request tool, which is therefore excluded from this analysis.

7.4.1 Scenario/Tool Coverage Analysis

Since Data Track is designed with data subjects as the primary user group in mind, scenarios that address the issue of making transparent how and by whom data is collected, processed, shared and whether or not policy violations occurred can immediately be mapped to this tool. There are also scenarios, where the same functionality is required by other actors, such as BUC1 – 3.1.1a where a privacy officer uses a tool to track information in the cloud, which is not his own. DataTrack does not support these scenarios.

Transparency Log can be used in multiple scenarios, since it is generic enough to also be used outside its primary use in DataTrack. For instance, wherever a secure, one-way communication channel is needed, TL can be used. Since TL can be characterized as a drop-in replacement for other communication mechanisms, pointing out all possibly relevant scenarios has been omitted in this analysis.

7.4.2 Functional Accountability Aspects

Data Track is a tool specifically designed for allowing data subjects to access, modify and otherwise request and process information stored about them in the cloud. Transparency Log is a tool that supports scenarios, where a secure communication channel for submitting notifications is required. Therefore, from an accountability function perspective, it may be involved in handling exceptions, more specifically, in the notification of exceptions. However, Transparency Log will always be used in combination with another tool that generates these notifications and needs a means of transport to the recipient.

At this point, there is not enough information available to connect DSART to any of the functional aspects of accountability.

7.5 Incident Response & Remediation

Related Tools: Remediation & Redress Tool (R&RT), Incident Response Tool (IRT)

The tools provided in this category are the Remediation & Redress Tool (R&RT) and the Incident Response Tool (IRT). The R&RT can be used by individuals and SMEs to act upon the detection of incidents. These incidents can either be reported to the IRT by other tools such as the AAS or DTMT or other sources such as newspaper reports. In the latter case R&RT will engage in a dialogue with the user to establish their concern. R&RT then tries to guide the user through the actions he can undertake (such as filing complaints, requesting additional information etc.). IRT uses other A4Cloud tools to detect incidents (such as AAS), filters and presents them to the user. It also offers corresponding actions to respond to the incidents, such as invoking the R&RT tool. Both tools address individual end-users and SMEs as their main users.

7.5.1 Scenario/Tool Coverage Analysis

Scenarios, which are concerned with the response to incidents detected in the cloud, are connected to the tools in this category. For instance, any scenario that involves the notification of a cloud customer (cloud providers as cloud customers excluded, since both tools do not address this stakeholder specifically) about an incident, which could also be a policy violation, could involve IRT as a notification component (e.g., BUC1 – 3.1.3a, BUC2 – 11.1.1a, BUC3 – 13.1.1g, 14.1.1d, 14.1.1e, 15.1.1d if CSP is an SME). The R&RT tool support scenarios, where the response to an incident/violation is focussed. Examples include supporting the cloud customer to file complaints or report violations (see. BUC1 – 3.1.3b and 6.1.1b or BUC3 – 13.1.1f)

7.5.2 Functional Accountability Aspects

The main functional accountability aspects covered by tools and scenarios in this category are located in the operate phase of the lifecycle, more precisely: they are concerned with exception handling. Notification about incident is mainly done by IRT, whereas R&RT manages remediation and redress. However, the other important function "attribution of failure" in the exception handling process cannot necessarily be found in IRT or R&RT.

7.6 Scenarios without Corresponding Tools

Some scenarios have been identified, for which it might not be possible to map them to A4Cloud tools. These scenarios are described in the following:

- **BUC1, 2.1.1a:** This scenario describes changing a data upload policy in a mobile application. This functionality is not directly addressed in any A4Cloud tools, since none of those are envisioned to have a mobile user interface.
- **BUC1, 4.**1.1a-4.1.2.a: These scenarios describe contract negotiation support regarding the negotiation of contract terms. None of the contract and risk management tools are useful here, since the user (CSP acting as a cloud customer) is not addressed by any of those.
- **BUC2, 12.1.1b**: This scenario describes a tool, which enables data protection officers to identify responsibilities and liabilities and to send proper notifications to stakeholders. It is currently unclear, which tool (if any) will provide such functionality.
- **BUC3, 15.1.1f**: This scenario describes the ability of a CTO of a cloud provider to actively search for needs and concerns of cloud users. There is currently no tool, which addresses this functionality.

7.7 Summary

As has been demonstrated in this section, most of the scenarios that were described in deliverable D-B:3.1 [5] are concerned with accountability functions of the operational phase; most importantly with monitoring and notification. The provision of an account is also a very important aspect for most scenarios, especially the validation of the operation, which is concerned with reporting operational aspects. Also, as has been shown in this section, most of the scenarios in deliverable D-B:3.1 [5] will benefit from one or more of the tools that the A4Cloud project will develop.

8 Process Modelling of the Business Use Cases

This section outlines seven different business process models for accountable organisations, and map these to the accountability lifecycle that has been introduced in WP:C-2 [10]. The processes that we have identified are depicted in Figure 15 and they have been modelled using the Business Process Model and Notation (BPMN) graphical representation. The purpose of this chapter is to provide a first draft of how the A4Cloud tools can be used in a specific business domain in order to solve some of the accountability challenges that will arise[28].

Based on the stages of the accountability governance lifecycle, we model the processes that should be implemented with the involvement of all cloud computing and/or data protection roles. These processes are[29]:

1. Find a cloud service that fulfils a given set of security and privacy requirements
2. Perform a risk assessment for data that will be processed in a cloud
3. Define and enforce policies for data processing practices
4. Deploy accountability measures, including configuration of monitoring and auditing and providing accountability assertion to the selected tools
5. Gather evidences of the applied data processing practices
6. Track and verify the cloud provider's data processing practices
7. Detect and react to an incident

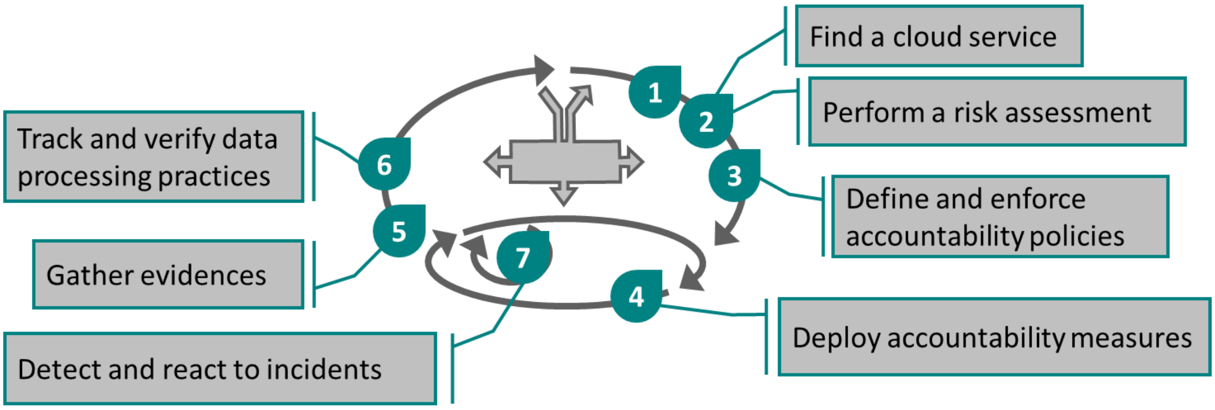

Find a cloud service
Perform a risk assessment
Define and enforce accountability policies
Deploy accountability measures
Detect and react to incidents
Gather evidences
Track and verify data processing practices
1
2
3
4
5
6
7

Figure 15 An overview of how the processes, which are modelled in this chapter, may fit into the accountability governance lifecycle defined by WP:C-2 [10].

In this section, we will present the BPMN models for these processes from a general perspective and we will then apply these models to the BUC1 to showcase how these processes can be mapped to the actual accountability implementation in a specific business context.

8.1 Modelling of Accountability Processes

We start the accountability lifecycle with the process called "Find a cloud service", which is illustrated in Figure 16. This process refers to the selection of the cloud service providers to constitute the respective service chain, which is compliant with the scope of the business transaction and the respective security and privacy requirements. This figure shows the tasks that should be performed by the cloud customer, acting as the data controller, in order to assess the offerings of the candidate cloud providers, using the

[28] The process have been defined and modelled based on WP:B-3's current understanding of how the tools may be used and how they will interact with each other. The proposed processes will therefore most likely be subject to changes in the coming year.

[29] Note that WP:C-2 [10] maps one accountability lifecycle to each of the organisations that are involved in the cloud ecosystem. For simplicity, in this chapter we only use a single lifecycle to show all the processes for all the actors that are involved in the service delivery chain.

Note also that WP:C-2 [10] recommends the risk assessment (step 2 in this list) to be done before the selection of a suitable cloud service provider (step 1 in this list).

COAT tool. The process is fed with the set of obligations, deriving from the regulatory framework and the implementation of the ethical accountability (normative obligations), along with the privacy and security requirements constituting the organisational level policies of the cloud customer. The outcome of the process is a report on the available cloud offerings.

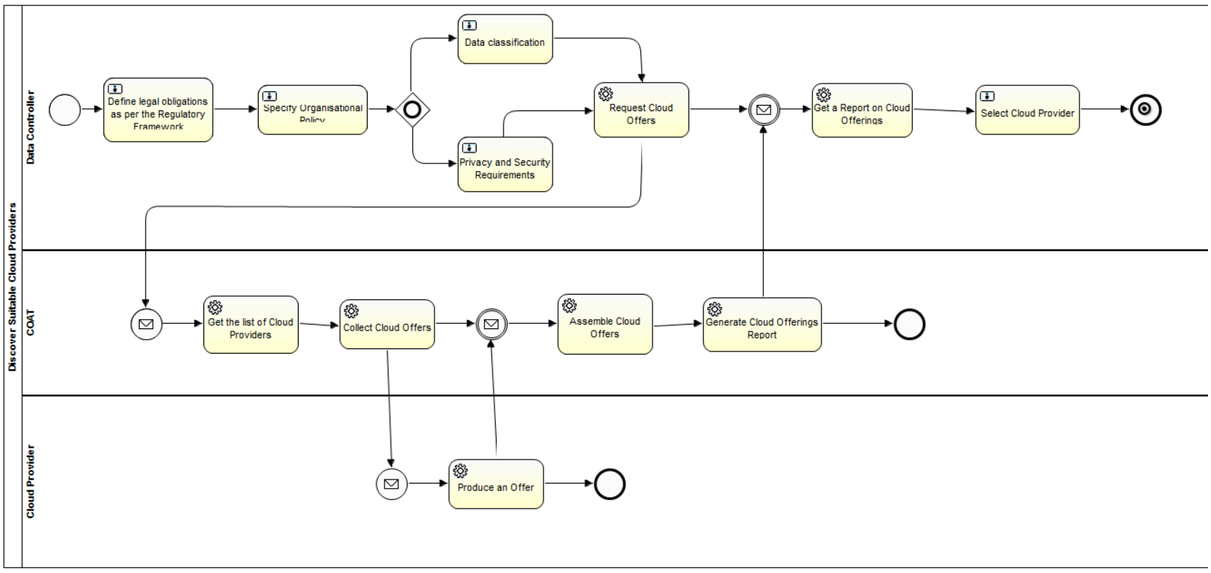

Discover Suitable Cloud Providers
Data Controller
COAT
Cloud Provider
Define legal obligations as per the Regulatory Framework
Specify Organisational Policy
Data classification
Privacy and Security Requirements
Request Cloud Offers
Get a Report on Cloud Offerings
Select Cloud Provider
Get the list of Cloud Providers
Collect Cloud Offers
Assemble Cloud Offers
Generate Cloud Offerings Report
Produce an Offer

Figure 16: The "Find a cloud service" BPMN process

Figure 17 shows the process for assessing the risks involved in the disclosure of personal and business confidential data in the cloud. The data controller decides on the data to be requested from the data subjects, subject to the obligations assigned to it and the organisational level policies, which take the form of privacy and security requirements. After analysing the risk and trust models of the specific cloud configuration, the process uses the DPIAT to generate the impact assessment report.

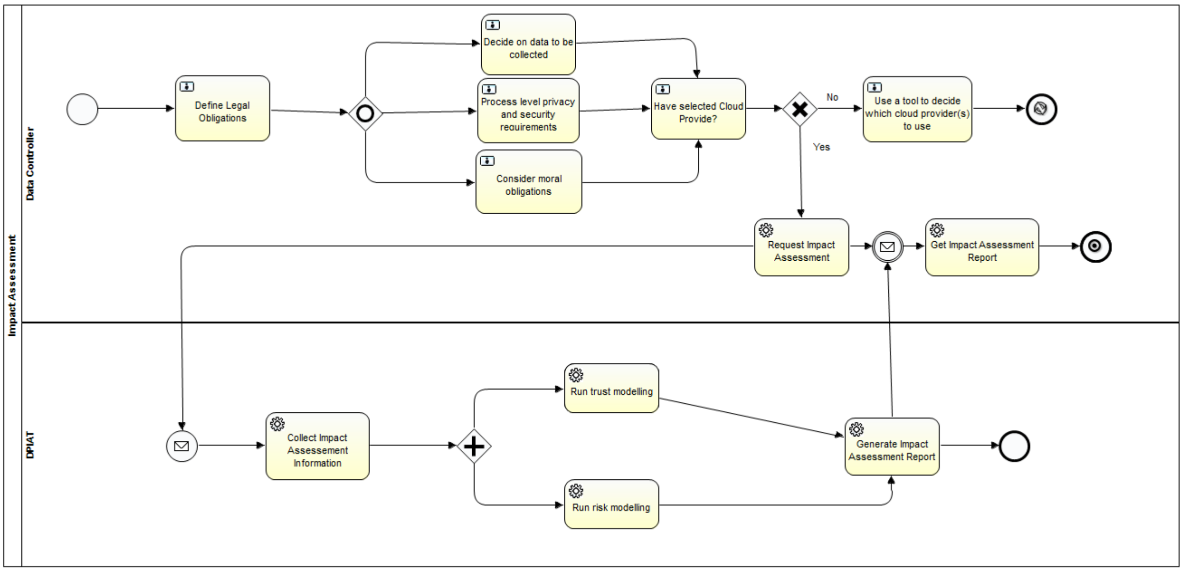

Impact Assessment
Data Controller
DPIAT
Define Legal Obligations
Decide on data to be collected
Process level privacy and security requirements
Consider moral obligations
Have selected Cloud Provide?
No
Yes
Use a tool to decide which cloud provider(s) to use
Request Impact Assessment
Get Impact Assessment Report
Collect Impact Assessment Information
Run trust modelling
Run risk modelling
Generate Impact Assessment Report

Figure 17: The "Perform a risk assessment" BPMN process

Then, the Data Controller maps the obligations to accountability policies, using the AccLab tool. These policies should be enforced through the A-PPL Engine and drive the establishment of agreements with the providers in the selected cloud service chain. This is shown in Figure 18.

The policies enforced by the A-PPL Engine drive the deployment of the necessary accountability measures that should be implemented across all the providers in the cloud service chain. Thus, the data controller and the data processors deploy the audit level rules and the data transfer monitoring rules, through which the AAS and the DTMT respectively activate and configure the relevant log collection mechanisms. The enforcement of these rules on the data controller side is then populated to the collaborating data processors, which install the corresponding AAS and DTMT instances, as shown in Figure 19. It must be noted that the developers of the data controller accountability measures use the AT to assert the proper deployment of an accountability solution in the service chain.

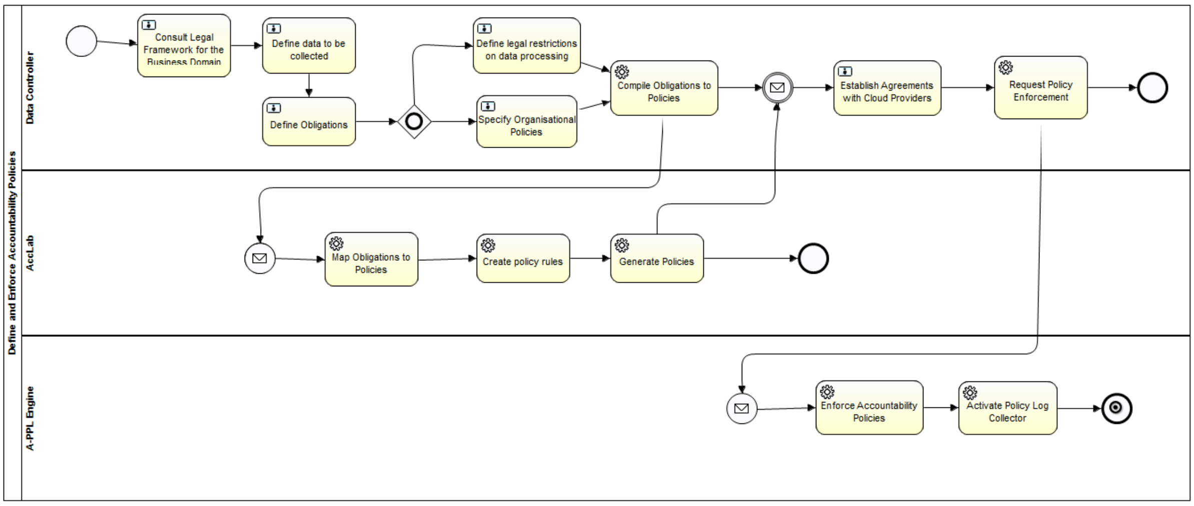

Define and Enforce Accountability Policies
Data Controller
AccLab
A-PPL Engine
Consult Legal Framework for the Business Domain
Define data to be collected
Define Obligations
Define legal restrictions on data processing
Specify Organisational Policies
Compile Obligations to Policies
Establish Agreements with Cloud Providers
Request Policy Enforcement
Map Obligations to Policies
Create policy rules
Generate Policies
Enforce Accountability Policies
Activate Policy Log Collector

Figure 18: The "Define and enforce accountability policies" BPMN process

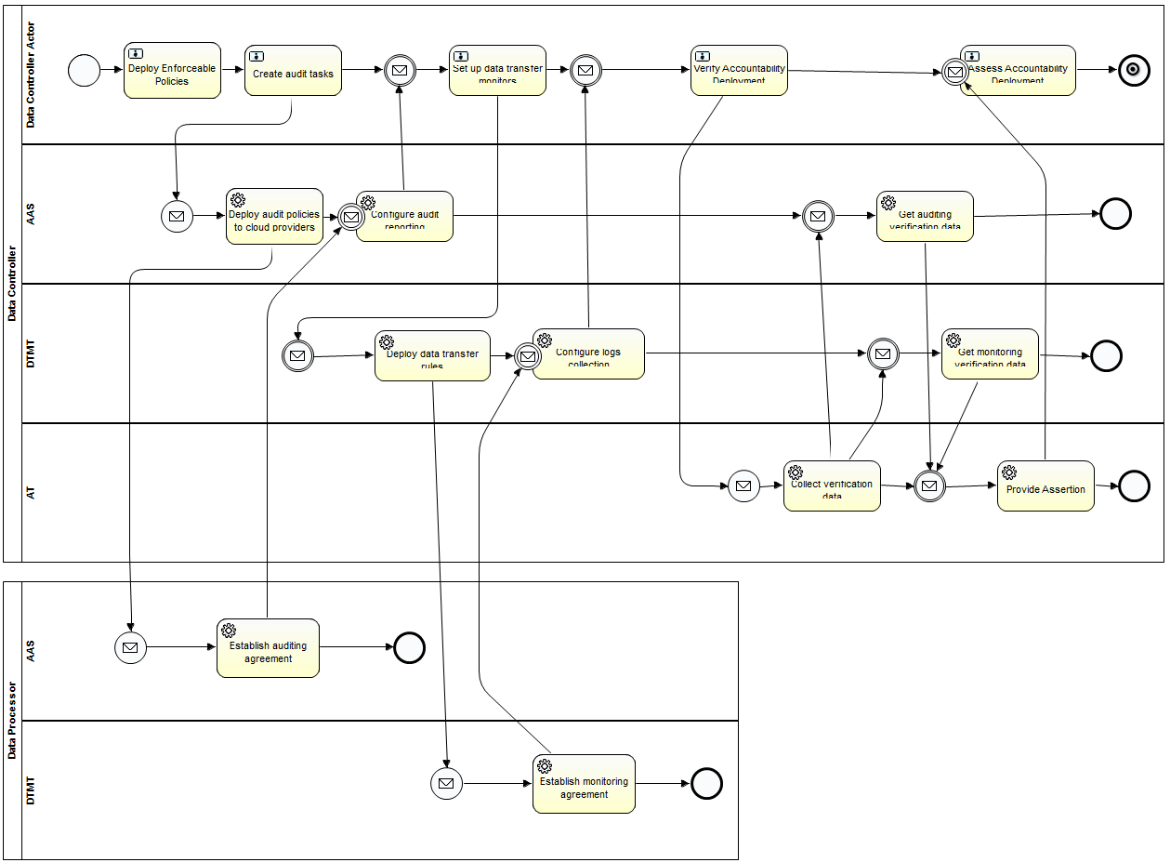

Data Controller
Data Controller Actor
AAS
DTMT
AT
Data Processor
AAS
DTMT
Deploy Enforceable Policies
Create audit tasks
Set up data transfer monitors
Verify Accountability Deployment
Assess Accountability Deployment
Deploy audit policies to cloud providers
Configure audit reporting
Get auditing verification data
Deploy data transfer rules
Configure logs collection
Get monitoring verification data
Collect verification data
Provide Assertion
Establish auditing agreement
Establish monitoring agreement

Figure 19: The "Deploy accountability measures" BPMN process

Figure 20 shows the accountability tasks adopted in the process of collecting evidence during the execution of business level transactions. The runtime phase involves the processing of personal data, provided by the data subjects and the collection of logs to log the actions performed by each business actor. At this level, data transfer and audit logs are collected, along with logs generated by the A-PPL Engine, as this tool enforces the proper implementation of the accountability policies, when business level data access is performed.

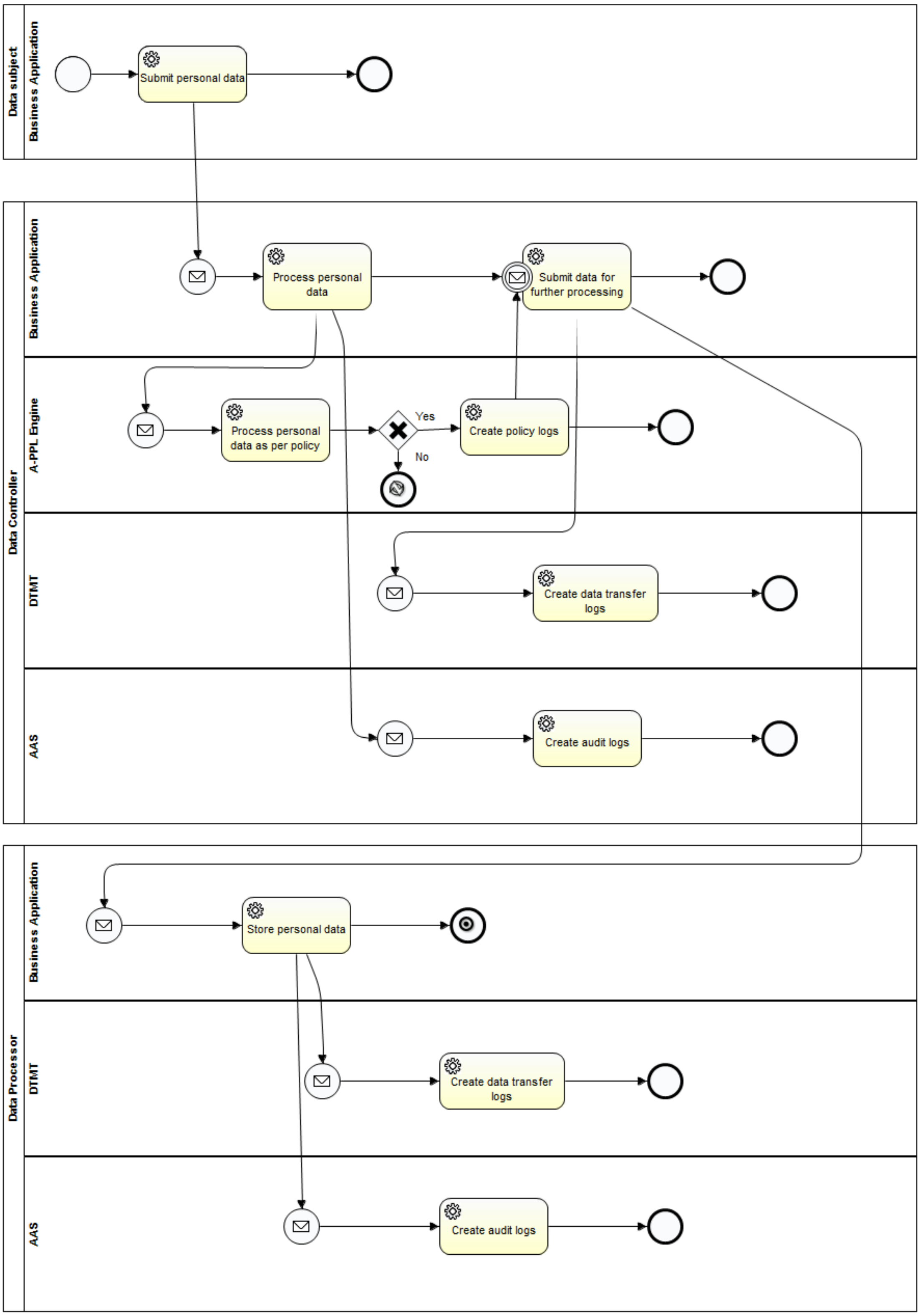


Figure 20: The "Collect Evidence" BPMN process

A4Cloud offers data subjects the ability to track and verify the data handling and processing practices of their data controllers, as shown in Figure 21. Using the Data Track (and the encrypted communication between the business actors through the Transparency Log), the data subjects can request an analysis of the disclosures of their personal data in the cloud. Thus, this process enables collecting evidence from the data controller (which in turn has had requested relevant evidence to be provided by the other cloud providers in the chain) and demonstrating how data are disclosure in the cloud. Through this process, the data subjects can discover any abnormal behaviour of the cloud service chain and receive a list of violations occurred.

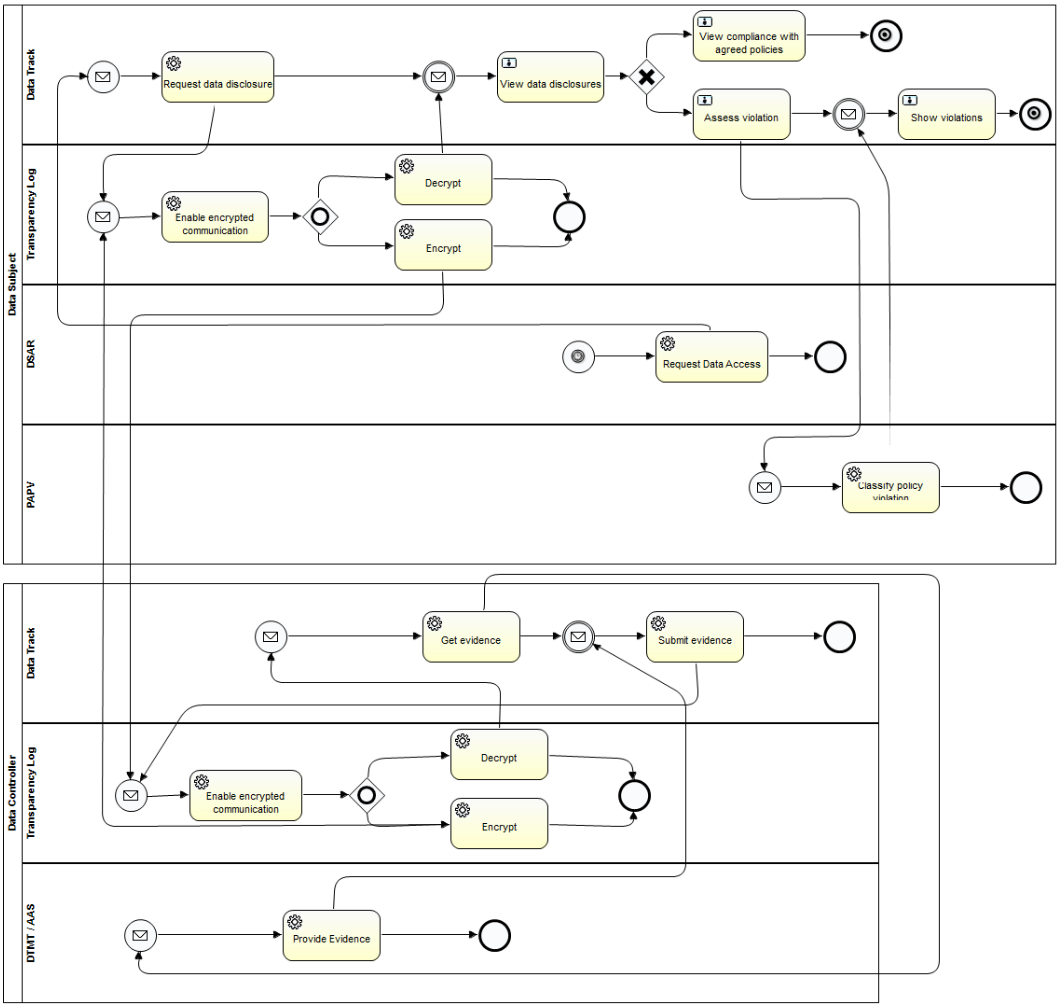


Figure 21: The "Track and verify data processing practices" BPMN process

The detection of an incident can be performed from the analysis of logs on the cloud providers' side, as shown in Figure 22. Depending on what toolset has been deployed, either AAS or DTMT will be used to discover incidents and will allocate their management to the IRT instances, in order to generate notifications for the collaborating actors, and the RRT instances to consult on the appropriate remediation. In this process, the Auditor role is also involved to consume the remediation complaints submitted by the data subjects.

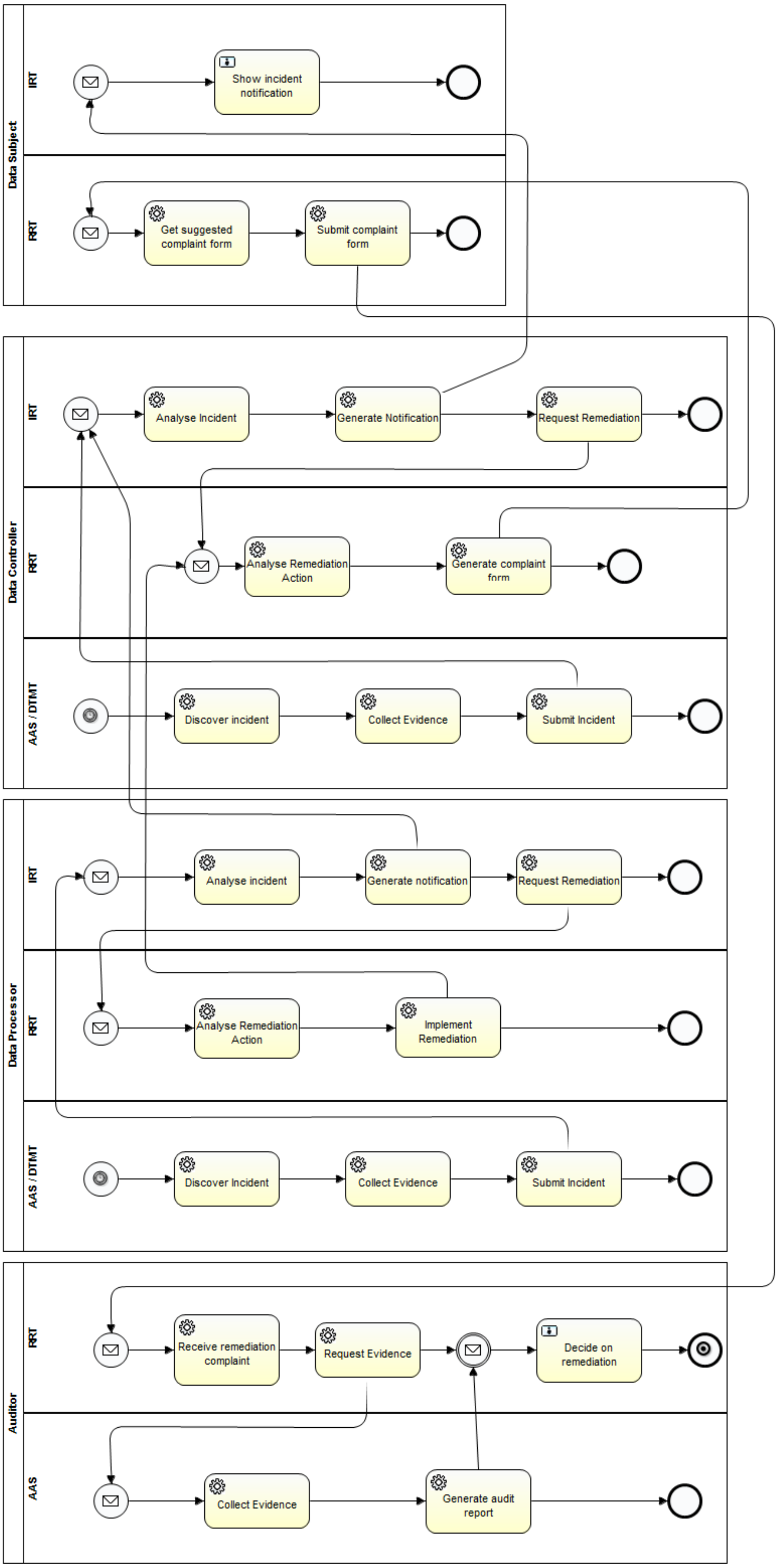


Figure 22: The “Detect and react to an incident” BPMN process

8.2 Instantiating the Accountability Processes for the Healthcare Business Use Case

This section demonstrates how the general accountability processes introduced in the previous Section 8.1 are instantiated to the A4Cloud healthcare business use case (BUC1). The processes for the other BUCs can be instantiated in a similar manner (to save space we chose not to include them in the deliverable).

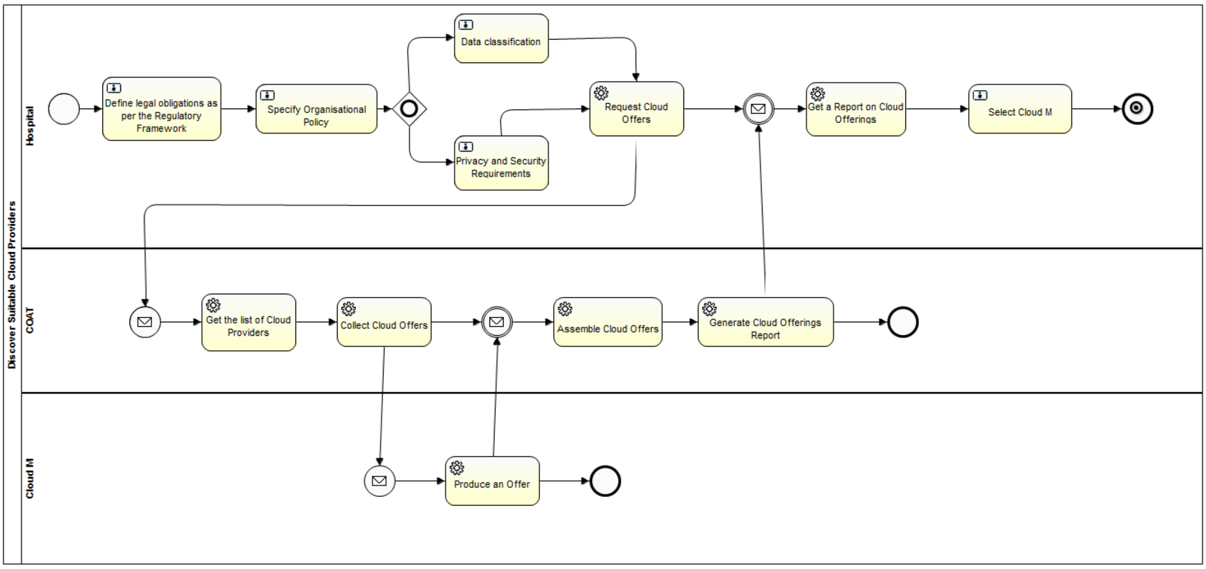

Discover Suitable Cloud Providers
Hospital
Define legal obligations as per the Regulatory Framework
Specify Organisational Policy
Data classification
Privacy and Security Requirements
Request Cloud Offers
Get a Report on Cloud Offerings
Select Cloud M
COAT
Get the list of Cloud Providers
Collect Cloud Offers
Assemble Cloud Offers
Generate Cloud Offerings Report
Cloud M
Produce an Offer

Figure 23: Instantiating the "Find a cloud service" process for the health care BUC

Figure 23 shows how the process of finding a cloud service provider is instantiated to BUC-1. Compared to Figure 16, the data controller is now the hospital, which receives cloud offers from providers collecting and processing patients' data in the cloud, like service provider M. Through this process, M is selected to drive the collection and processing of the data of the hospital patients in the cloud environment.

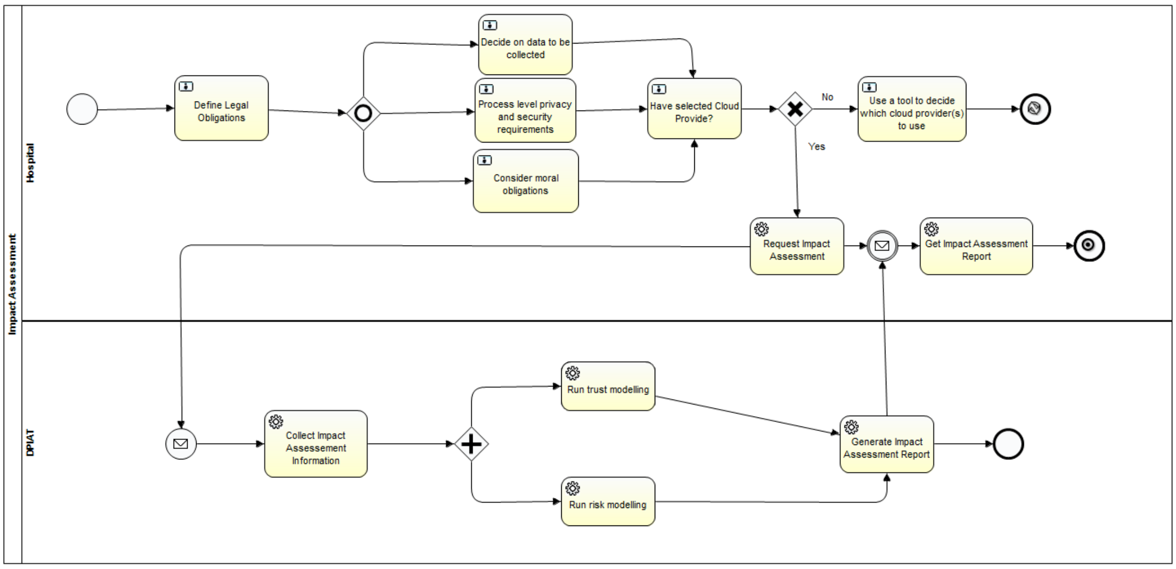

Impact Assessment
Hospital
Define Legal Obligations
Decide on data to be collected
Process level privacy and security requirements
Consider moral obligations
Have selected Cloud Provide?
No
Yes
Use a tool to decide which cloud provider(s) to use
Request Impact Assessment
Get Impact Assessment Report
DPIAT
Collect Impact Assessement Information
Run trust modelling
Run risk modelling
Generate Impact Assessment Report

Figure 24: Instantiating the "Perform a risk assessment" process for the health care BUC.

In BUC1, Michael (who is acting as the legal representative of the hospital), performs a risk assessment in order to determine which patients' data will be collected and how they will be disclosed across the cloud service chain. In that respect, the process for performing a risk assessment in Figure 17 can be instantiated in BUC1 as illustrated in Figure 24. Through this process, Michael can assess the impact from using the chain consisting of provider M, cloud provider X and cloud provider Y to process the patients' personal data.

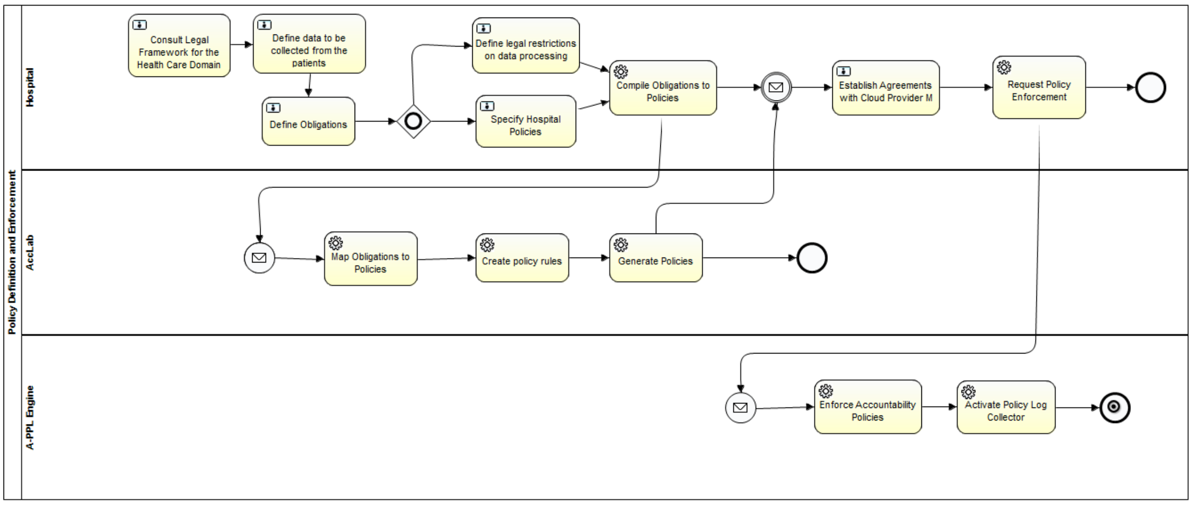

Policy Definition and Enforcement
Hospital
AccLab
A-PPL Engine
Consult Legal Framework for the Health Care Domain
Define data to be collected from the patients
Define Obligations
Define legal restrictions on data processing
Specify Hospital Policies
Compile Obligations to Policies
Establish Agreements with Cloud Provider M
Request Policy Enforcement
Map Obligations to Policies
Create policy rules
Generate Policies
Enforce Accountability Policies
Activate Policy Log Collector

Figure 25: Instantiating the "Define and enforce accountability policies" process for BUC1

Figure 25 shows the process for defining and enforcing accountability policies for BUC1. As shown there, Michael, as the Privacy Officer at the hospital, uses the AccLab tool to map the legal and normative obligations for the hospital (that is the data controller) to accountability policies, which are enforced at the hospital and in the M Platform.

In order for the accountability measures to be deployed properly, the involved cloud providers in the service chain of BUC1 also need to exploit the previously defined accountability policies and configure the auditing and monitoring tools. Thus, all the cloud providers acting as data processors, namely provider M, cloud provider Y and cloud provider X, deploy the appropriate solutions for logging collection from AAS and DTMT. The respective actors, such as Peter and Bruce (who are described in the to-be scenarios in D:B-3.1 [5]), verify that the deployment of the accountability measures is correct. Especially, Peter uses the AT to provide assertion over the proper configuration of these measures and communicates the result to Michael. This is reflected in Figure 26, which instantiates Figure 19 for BUC1.

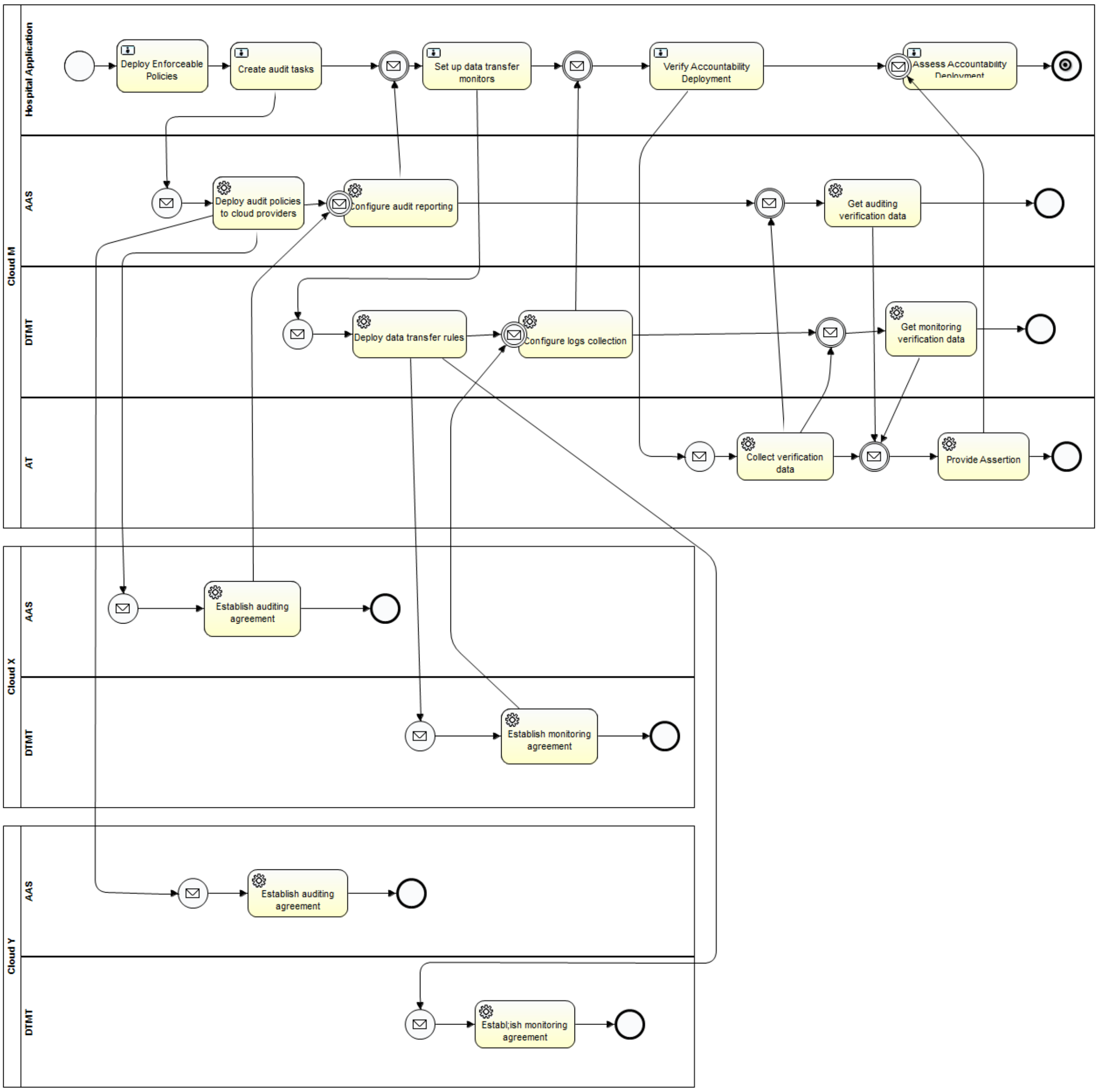

Hospital Application
Deploy Enforceable Policies
Create audit tasks
Set up data transfer monitors
Verify Accountability Deployment
Assess Accountability Deployment
Cloud M
AAS
Deploy audit policies to cloud providers
Configure audit reporting
Get auditing verification data
DTMT
Deploy data transfer rules
Configure logs collection
Get monitoring verification data
AT
Collect verification data
Provide Assertion
Cloud X
AAS
Establish auditing agreement
DTMT
Establish monitoring agreement
Cloud Y
AAS
Establish auditing agreement
DTMT
Establish monitoring agreement

Figure 26: Instantiating the "Deploy accountability measures" process for the health care BUC

During the execution of BUC1, personal data are collected from the hospital's patients by the M Platform, which are exploited by the hospital staff to assess the health care treatment for their patients. All the business transactions occurred from the application perspective must be logged to generate evidence of compliance with the agreed accountability policies. The evidence collection process for this business scenario is shown in Figure 27. Compared to the general case of Figure 20, we see here that all cloud providers, acting as data processors, implement their own log collection mechanisms, through which the evidence is produced. The logging mechanisms are attributed at three different levels, namely logging the matching of a business action with the policy rules, logging any data transfer actions on the cloud providers side and logging the actions referring to the audit tasks that have been enforced during the deployment of the relevant accountability measures.

Both the hospital's patients and their relatives (who also are data subjects) can request from the hospital, which is the data controller in BUC1, to track the data processing practices adopted in the hospital and subsequently by provider M, X and Y. They can then use the Data Track to verify that these practices adhere to the data disclosure agreements that they have agreed to and, in case of any violation, they will receive information about and assessment of the violation severity, so that they can request actions against it. This is depicted in Figure 28.

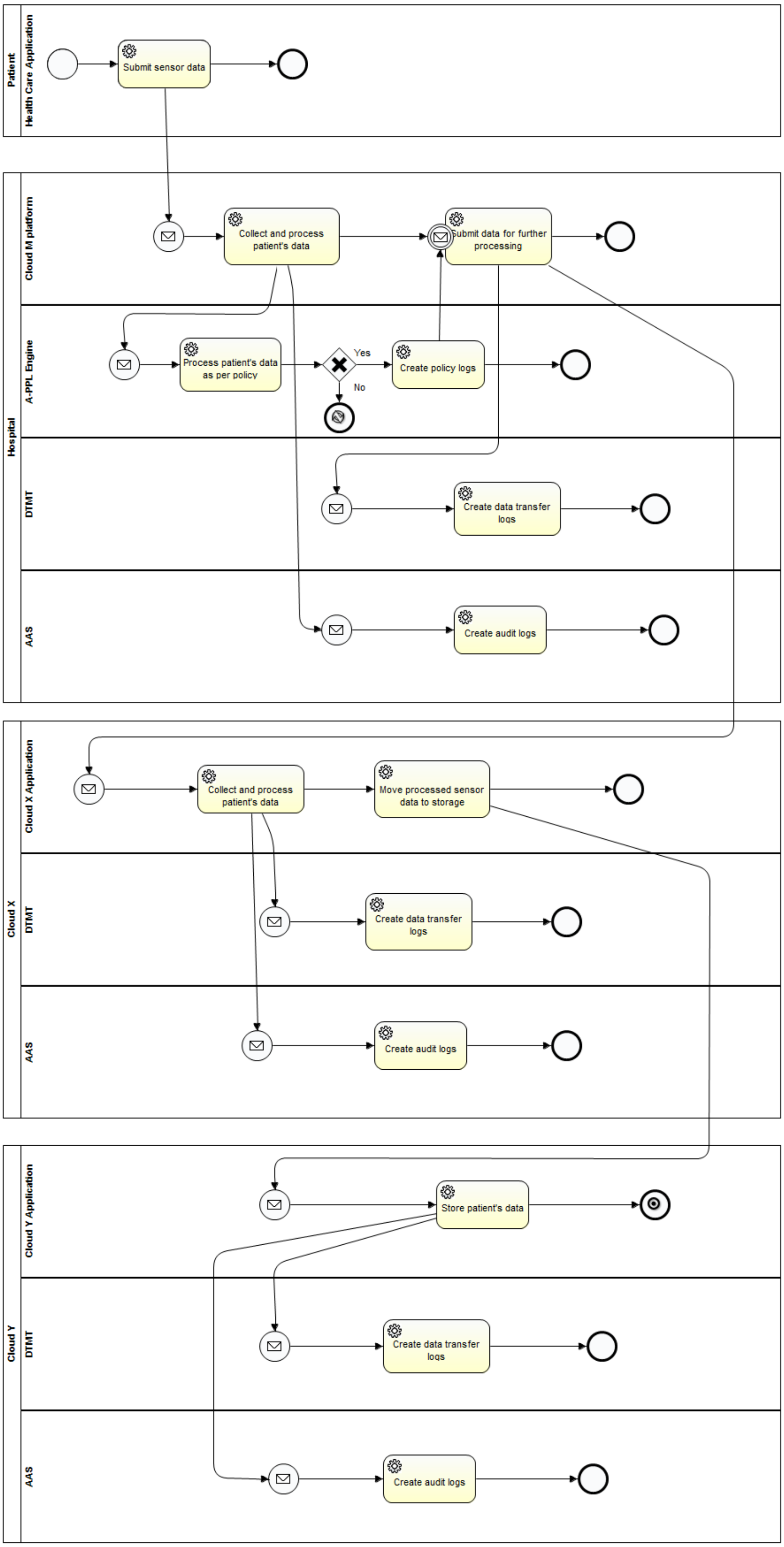


Figure 27: Instantiating the “Collect Evidence” process for the health care BUC

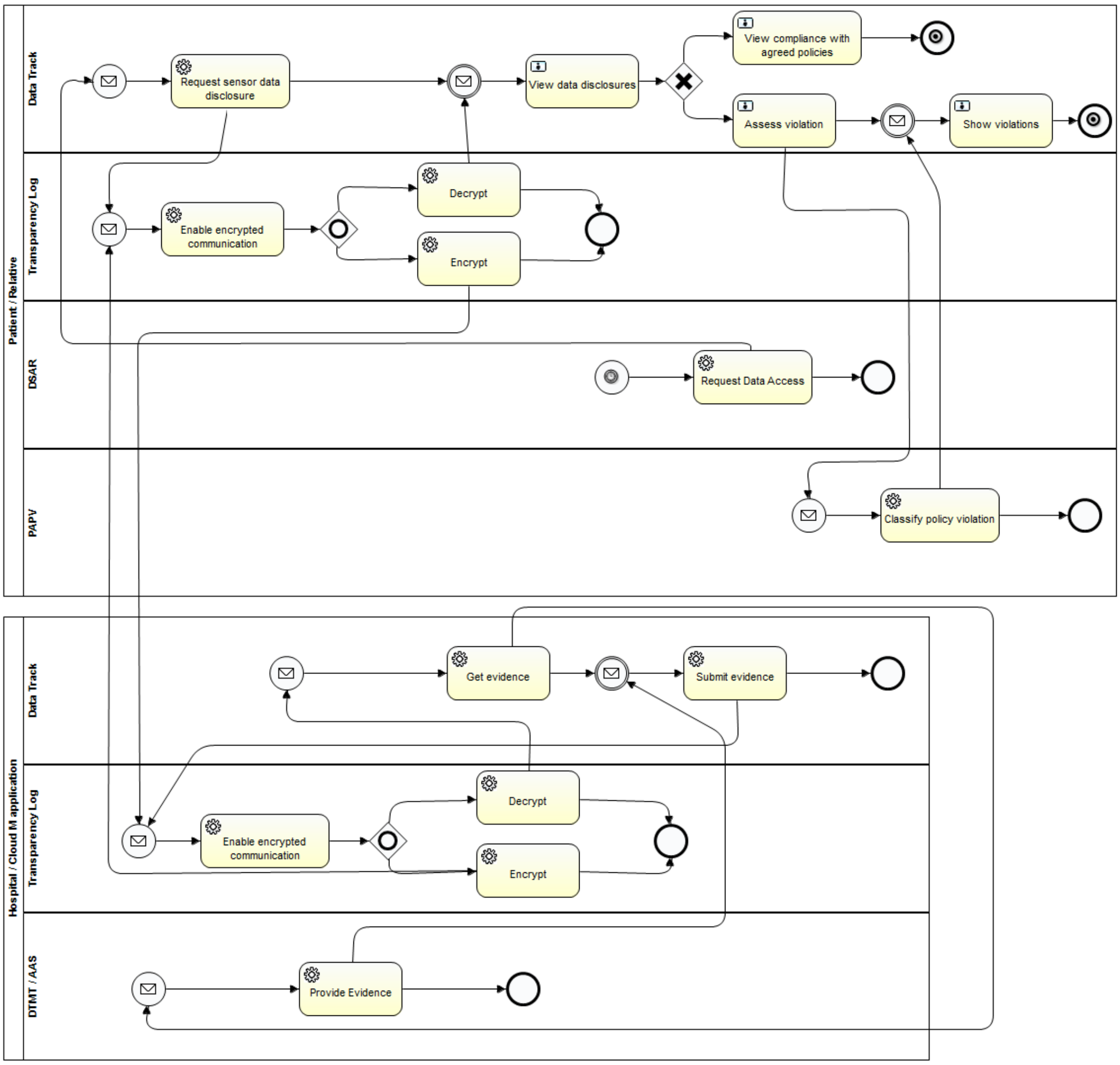


Figure 28: Instantiating the "Track and verify data processing practices" process for BUC1

Figure 29 shows how the process for incident management of Figure 22 is instantiated in BUC1. All cloud providers analyse the logs collected from the implemented detective mechanisms (as well as other possible sources of evidences) and produce evidence. The analysis of these evidences may generate incidents, which should be communicated to the affected data subjects and data controllers through the IRT and be remedied through the RRT. For example, as shown in Figure 29, an incident discovered in cloud X or Y shall produce a notification, which is communicated to the associated primary cloud provider (provider M). This actor, in turn, populates the notification to the data controller (the hospital) and all the involved data subjects (the patients, their relatives and/or the hospital staff), depending on whose data have been affected by the incident. At any stage, all the parties handling a notification can request for the respective corrective mechanisms to be enforced providing remediation on this incident.

Upon receiving remediation information, the data subject can also communicate with a representative of the Data Protection Authority, and submit a complaint form. The latter actor will then act accordingly to request from the cloud providers to demonstrate their compliance to the policies.

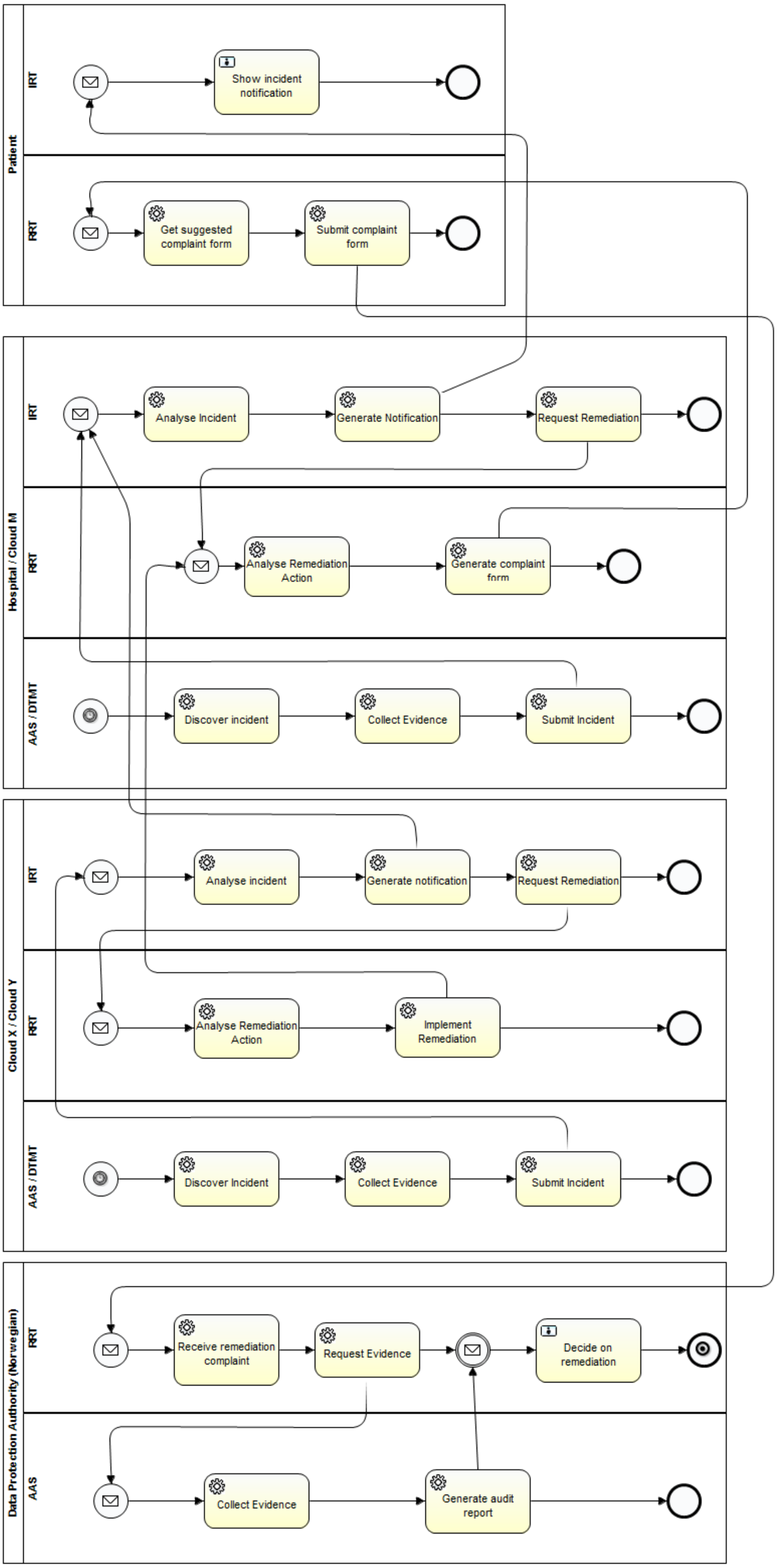


Figure 29: Instantiating the “Detect and react to an incident” process for the health care BUC

8.3 Summary

This section has outlined seven different business processes, which will help organizations that consumes or provides cloud services to become accountable, and showed how these processes can be mapped to the accountability governance lifecycle defined by WP:C-2. We have then showed how these seven processes can be instantiated into one of the business use cases that are described in this deliverable. As can be seen, the processes will involve interactions with A4Cloud tool by, not only data controllers and data processors, but also data subjects and data protection authorities.

9 Business Use Case Risk Assessment

Moving business processes to the cloud is associated with a change in an organisation's risk landscape. Unfortunately, most organisations currently lack adapted methods to perform trust and risk management for the cloud. Data controllers, processors, or more generally cloud customers must be aware of specific risks for business confidential, personal and other kinds of sensitive data subject to regulatory restrictions when using cloud services. To fill these gaps, the work performed by WP:C-6 introduces a methodology, which is called the Cloud Adoption Risk Assessment Model (CARAM), which goal is to assess the various business, security and privacy risks that cloud customers face when moving to the cloud. In this chapter we analyse the risks from the cloud customer's standpoint, explaining how the methodology and the tool developed in WP:C-6 can be used when they perform the risk assessment and how it can help in their the decision making process.

9.1 The Cloud Adoption Risk Assessment Model (CARAM)

CARAM is based on the ENISA Risk Assessment Model [36] and the Cloud Assessment Initiative Questionnaire (CAIQ) [37]. CARAM, which is described in detail in [38], consists of the following "components":

- A questionnaire for cloud customers that allows them to identify the impact to their assets during the risk assessment, hence taking the customs' preferences into account.
- A tool and an algorithm that maps the answers to the Cloud Assessment Initiative Questionnaire (CAIQ) to discrete values. Compared with conventional information technology (i.e., other than cloud), risk assessment of cloud services is particularly challenging. One of the main reasons is that cloud providers usually keep the locations, architecture and details about the security of their server farms and data centres confidential from their customers. Therefore, it is often difficult for a cloud customer to assess all the threats and vulnerabilities associated with a cloud service. CARAM addresses this problem by using the most transparent and reliable data source available today[30], in order to extract statistics of the cloud providers' practices in security management (and many other control areas extracted from multiple security standards).
- A model that maps the CAIQ answers of both these questionnaires to risk values. The cloud customer then has elements to compare multiple cloud providers by analysing the exposure of the providers to vulnerability thanks to the classification generated by the tool.
- A multi-criteria decision approach with posterior articulation of the cloud customer's preferences for relative risk analysis. The cloud customer can therefore use the information to support its decision in the provider selection process with its own risk profile at hand, taking the accountability for making an informed decision.

In the next section we describe how CARAM can be applied to the cloud-based ERP offering described in Business Use Case 2. Due to space limitations (and to avoid duplications in the WP:B-3 and WP:C-6 deliverables) we do not give any further details of the inner workings of the CARAM methodology itself; the reader is referred to the WP:C-6 deliverable [35], which provides a detailed description and explanation of the risk assessment model.

9.2 Risk Assessment of the Cloud-based ERP Service Offering

Recall the cloud-based ERP offering described in Section 3.2 of this deliverable. The organisations that are involved in this business use case are MarchéAzur (i.e. the supermarket chain, which is a cloud customer and a data controller), Check-It-Out (the SaaS provider), PaaSPort (the PaaS provider) and InfraRed (the IaaS provider), whereof the latter three are operating their cloud offerings at the software, platform and infrastructure level respectively. In addition, Check-it-out (ISV) is offering a platform extension in the form of a SaaS offering that can be utilized by other cloud services. We conduct the risk assessment from the point of view of MarchéAzur, as the data controller, to illustrate our approach.

For MarchéAzur the first step would be to define the importance of the data assets to its project. The ENISA Risk Assessment Model [36] lists the most important assets that may be exposed to risks in the cloud. MarchéAzur would need to point out the relevant ones as shown in the Table 7. This corresponds

[30] The STAR registry provided by the Cloud Security Alliance (CSA). See footnote 32.

to setting up the impact parameter in CARAM – the “Gamma” collum is set to one for the sensitive assets to MarcheAzur. The justification for the selection is to concentrate on the ones that would threat compliance to data protection regulation, or to the personal data itself. In this sense, physical items (assets 17 and 18) are not relevant, since MarchéAzur is dematerializing its systems to use cloud services. It will on the other hand, require from the provider that physical security is in place when analysing the cloud providers' CAIQ.

Table 7 Asset relevance for personal data processing in the cloud.

Asset Id	Description	Gamma
A-01	A1. Company reputation	1
A-02	A2. Customer trust	1
A-03	A3. Employee loyalty and experience	1
A-04	A4. Intellectual property	0
A-05	A5. Personal sensitive data	1
A-06	A6. Personal data	1
A-07	A7. Personal data: critical	1
A-08	A8. HR data	1
A-09	A9. Service delivery: real time services	0
A-16	A16. Network (connections etc.)	0
A-11	A11. Access control / authentication / authorization	1
A-12	A12. Credentials	1
A-13	A13. User directory (data)	1
A-14	A14. Cloud service management interface	1
A-15	A15. Management interface APIs	1
A-17	A17. Physical hardware	0
A-18	A18. Physical buildings	0
A-19	A19. Cloud Provider Application (source code)	0
A-10	A10. Service delivery	0
A-20	A20. Certification	1
A-21	A21. Operational logs (customer and cloud provider)	1
A-22	A22. Security logs	1
A-23	A23. Backup or archive data	1

The next step for MarchéAzur is to define its preferences with respect to the risk categories in order to determine what the most relevant risk scenarios for their business are. Indeed, the ENISA’s risk assessment recommendation describes 35 distinct scenarios (see Appendix C.1 ENISA's List of Risk Scenarios and Their Categories), which can require time and expertise to analyse. Not all risk scenarios should be seen with the same importance by the cloud customer; it is more pragmatic to define the weights each incident scenario would have to the MarchéAzur business, creating what we call a "relative risk" analysis. Table 8 summarizes how the policy and organizational, technical, legal, and other risks would impact the privacy, security and the quality of service for MarchéAzur’s activities. These weights need to be decided with a panel of responsible stakeholders of an organisation: its privacy officer, chief security officer and at least one project manager. It can be adjusted for each different project in order to analyse cloud risks. Often these roles overlap for SMEs and they can of expertise. We suggest using the table below for cases similar to MarchéAzur. We are currently conducting evaluations to better prune these values.

Table 8 Weights for the different incident scenarios for data protection in the cloud.

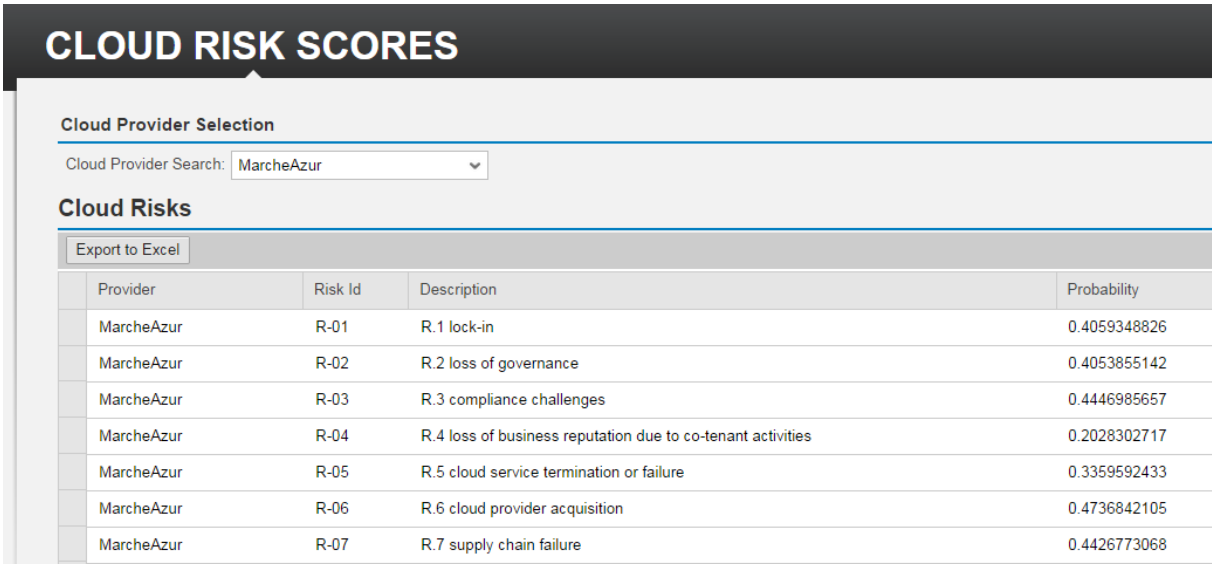
Relative risk	Scenario Category	Weight
Privacy	Policy & Organisational	1
Privacy	Technical	0.5
Privacy	Legal	1
Privacy	Non-cloud specific	0.5
Security	Policy & Organisational	0.2
Security	Technical	1
Security	Legal	0.1
Security	Non-cloud specific	1
Service	Policy & Organisational	0.5
Service	Technical	0.7
Service	Legal	0.2
Service	Non-cloud specific	1

The next step for the cloud customer is to calculate the vulnerability exposure of the providers under consideration. The current implementation of the Cloud Risk Assessment plugin[31] contains a database of all control groups of the CAIQ and a mapping of how they contribute to mitigate the vulnerabilities enumerated for each of the 35 different incident scenarios that have been identified by ENISA [36]. The database is also pre-filled with information obtained from the CSA STAR[32] about 60% of the providers in the list. We suggest the plugin to be used internally by cloud consumers that want to know the risk exposure of the providers. The database can be extended and updated under their discretion using the supervised machine learning process, as explained in the WP:C-6 deliverable [35] and in the paper [38].

The Cloud Risk Assessment plugin calculates the probabilities must proceed for all 35 different incident scenarios upon the selection of a cloud provider. The screenshot in **Error! Reference source not ound.** presents the output of the tool developed by SAP, with the values for the vulnerability index (see Appendix C.2) for all the risks concerning this fictitious service from MarchéAzur that are described in BUC2.

[31] Currently accessible under https://s3hanaxs.hanatrial.ondemand.com/i061767trial/a4cloud/shine/ui/caram/WebContent/caram.html
In order to access the application, it is necessary to create an account at https://scn.sap.com/ and request access to a4cloud@a4cloud.eu

[32] https://cloudsecurityalliance.org/star/#_registry



CLOUD RISK SCORES

Cloud Provider Selection

Cloud Provider Search: MarcheAzur

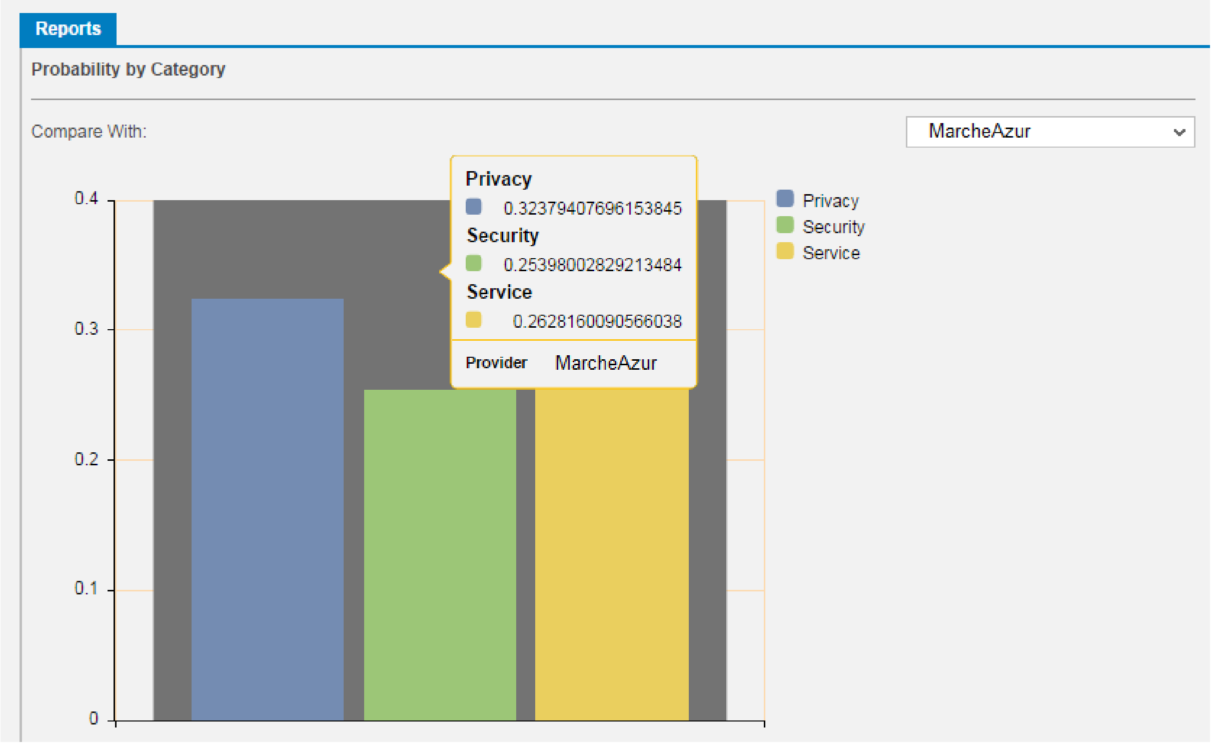
Cloud Risks

Provider	Risk Id	Description	Probability
MarcheAzur	R-01	R.1 lock-in	0.4059348826
MarcheAzur	R-02	R.2 loss of governance	0.4053855142
MarcheAzur	R-03	R.3 compliance challenges	0.4446985657
MarcheAzur	R-04	R.4 loss of business reputation due to co-tenant activities	0.2028302717
MarcheAzur	R-05	R.5 cloud service termination or failure	0.3359592433
MarcheAzur	R-06	R.6 cloud provider acquisition	0.4736842105
MarcheAzur	R-07	R.7 supply chain failure	0.4426773068

Figure 30 Cloud Risk Assessment plugin screenshot.

The last step consists in assessing the relative probabilities of privacy, security and service incidents, as explained in Section **Error! Reference source not found.** of [35]. The values for security and service isks will then be generated by the Cloud Risk Assessment plugin[33], shown in Figure 30. The user will conclude from this assessment that the service and security risks of the selected provider fall in the “Low” Probability range. On the other hand, as can be seen from the figure the probability of a Privacy incident is “Medium” according to the CARAM methodology. The cloud costumer may easily compare these indicators with those of other providers. The customer may also require more detailed information and further guarantees from the provider in order to make a decision, given that the cloud customer now has an increased awareness of cloud computing risks, adapted to the characteristic of its own project.

[33] The corresponding web service can be accessed under https://s3hanaxs.hanatrial.ondemand.com/i061767trial/a4cloud/shine/services/relativeRisks.xsodata/RELATIVE_RISKS/



Probability by Category

Compare With: MarcheAzur

Privacy
🟦 0.32379407696153845
Security
🟩 0.25398002829213484
Service
🟨 0.2628160090566038

Provider MarcheAzur

Figure 31 Relative Risks Screenshot.

CARAM is a qualitative and relative risk assessment model for assisting potential cloud customers to select a CSP that fits their risk profile best. It is based on the existing frameworks by ENISA, CAIQ and CNIL [39], which have been developed in Europe for the last decade, and complements them to provide the cloud service customers with a practical tool. In contrast to most other risk assessment methods, which are generic in nature and not specific to any particular service, CARAM is designed such as the evaluation will be carried out for a specific cloud service provider. Hence the model will help potential cloud customers to estimate and compare the risks associated with different service offerings.

This section has presented how a potential cloud customer (using MarchéAzur in BUC 2 to concretise the example) can use the CARAM methodology to assess the risk of selecting a specific cloud provider. As illustrated in Figure 30 and Figure 31, the tool asks its user to select a cloud service provider from a given list of around 50 providers, which have answered the CAIQ, and evaluates a risk landscape of 35 risks, which are grouped into 3 categories: service, security and privacy. In this section, the application of the approach to BUC2 shows the practicality of the process. CARAM is currently being integrated into the A4Cloud Data Protection Impact Assessment tool (DPIAT).

10 Selected Cases for Instantiation

This section in essence summarises the activities performed in WP:B-3 to draft the specifications of the use cases that will be implemented in the context of WP:D-7 use case instantiation to demonstrate the concepts, the accountability framework and the respective tools.

10.1 Introduction

The analysis of the three business use cases described in this deliverable and the previous deliverable from WP:B-3 [5] has served as a baseline for research on the accountability issues in business environments which make use of complex cloud service provision chains and raise as fundamental requirement the protection of personal and business confidential data.

The purpose of the use case for instantiation and demonstration is fundamentally to integrate the results of the project and to provide a means to demonstrate the concept of accountability and how the results of the project support that.

This leads to a set of differences between the business use cases analysed for the requirements phase and that selected for demonstration, which is outlined in Table 9 below.

Table 9 Instantiation use case compared with initial business use cases.

Aspect	Initial Business Use Case(s)	Instantiation Use Case
Headline	Articulate the purpose and value of accountability in the provision of cloud services	To demonstrate the practice of accountability for cloud services and the interactions and obligations between actors
Scope	Understand & identify accountability dimensions and requirements	Provide a practical demonstration of our accountability framework, architecture and tools
Value-chain	As complex as needed to explore many situations & interactions	As simple as possible in order to provide a clear demonstration using resources available
Construction	Description of the use case and a detailed description of the interactions between the various actors	An implementation in software of a conceptual prototype of the business application integrated with the actual tools developed by the project
Lifecycle	Focus on the exploitation of a business value chain (run-time)	Integrate both construction of the cloud services and exploitation of the business service
Coverage	Breadth – seeking wide coverage of all the dimensions of accountability in cloud services	Depth – aiming to incorporate the results of the project (concepts, architecture and tools)
Result	Build list of roles and obligations	Demonstrate how to go about accountability to potential adopters

This analysis of the initial business use cases leads to the conclusion that any one of these initial use cases on its own does not lend itself to demonstrating all the results of the project; they are either too complex to implement, individually they do not cover the whole space, or (in the case of healthcare) may become entangled with another regulatory domains outside the scope of the work.

Therefore we have chosen not to implement any of the three business use cases that the project has explored through the requirements phase. Instead we will implement a use case based around wearable computing in a “fitness and wellbeing” scenario. The wearable’s use case is in an area with significant business growth potential. Wearable computing was highlighted in DA2.1 – The Project Horizons Report - as an emerging technology that will generate huge challenges for data governance in cloud services in the future. Section 10.2 further articulates the objectives for the demonstrator; subsequent sections define the use case that will be instantiated.

10.2 The Objectives of the Use Case Instantiation

The synthesis of an appropriate use case for instantiation should target to fully cover the objectives of the use case instantiation task (WP:D-7). As such, we hereby briefly introduce these objectives to showcase the parameters that are exploited to define a new use case that will be instantiated. Here we refer to this new use case as "*the synthesised use case*".

The scope of the A4Cloud project is to cover the accountability issues considering fundamental features of the cloud deployment business paradigms. As such, we want to define a scenario that reflects the following cloud specific aspects:

- **Building a supply chain of cloud providers**. As shown in business use case 1, the provision of sophisticated business scenarios can be enabled through the exploitation of multiple cloud providers, who effectively cooperate in the cloud environment to deliver added value services to cloud customers and cloud subjects. The collaboration of multiple cloud providers builds service provision chains, which can handle different types of personal and confidential data in order to produce a value added result. The scope of the use case instantiation in this case is to demonstrate the stewardship of these data along the service chains and how the chain can provide the envisaged result in an accountable approach.
- **Operating at different layers**. Cloud offers can take the form of at least three different business service models; namely SaaS, PaaS and IaaS. As shown in business use case 2, the combination of these models in a cloud ecosystem can raise issues on the proper stewardship of personal and business confidential data across these layers. Thus, the synthesis of the envisaged use case should consider for demonstrating the accountability practices when moving from one layer to another.
- **Multi-tenancy**. An important aspect of a cloud ecosystem is the multi-tenancy of resources that can be accessed from different service instances of various business contexts and be shared in a fair and balanced way. The adoption of such a cloud feature means that security and privacy mechanisms are enacted. But this is not adequate to ensure protection of personal and confidential data, since, as shown in business use case 3, all the involved providers need to show compliance with accountability practices and offer the means to define and implement the relevant accountability mechanisms.

The synthesised use case should be specified so that it exhibits the problems and the concerns highlighted by the three domain-specific business use cases. These concerns relate to the way that the involved actors make sure that personal and business confidential data are handled in an accountable way in the cloud, irrespective of the number of cloud providers involved in the service chain or the cloud service model that is developed or the deployment of multi-tenancy applications and service instances in the same cloud. Such concerns and problems have already been emphasised in the analysis of the business use cases in this and the previous deliverable of WP:B-3 [5] and they have been specialised in terms of accountability requirements and relevant obligations assigned to the involved cloud and data protection roles.

The instantiation of the synthesised use case should consider for showcasing how the involved cloud providers are set as accountable by operating the complete phases of the accountability lifecycle and demonstrating the provisions of the accountability maturity model defined in WP:C-2 [10].

From a technical point of view, the synthesised use case must be designed so that the architectural aspects of the A4Cloud accountability framework and mechanisms can be easily demonstrated. In that respect, an important dimension during the design of the synthesised use case should be the fact that the new use case scenarios make use of the complete set of the A4Cloud tools. These tools should be consumed by all the potential cloud actors and data protection roles of the use case, aiming to demonstrate the accountability aspects towards data protection and efficient cloud data governance.

10.3 The Definition of the Synthesised Use Case Setup

(One of) the simplest combination of roles and actors in a Cloud context is a value chain composed of three actors:

- A customer (typically consumer) which access a service and entrust the provider with some private or confidential data. For the sake of this scenario, this actor has the role of Data Subject and is defined by our model as a Cloud Subject
- A service provider which implements its services using a Cloud service provider. In our scenario, this actor has the role of Data Controller and of Cloud Customer
- A SaaS, PaaS or IaaS Cloud provider which provides the services used by the above party. In our scenario, this actor has the role of Data Processor and is a Cloud Provider

The use-case we have selected for the instantiation use case is built on this model, extending it to allow the objectives for the demonstrator described in Section 10.2 above to be addressed. We assume a workflow that facilitates a "Wearables" service by gathering, managing and storing customers' personal data, which are used to keep track of customers' health status over time. This information is recorded by wearable devices provided by "Wearable Co.", and transmitted to CardioMon. This data is then used by the Map-On-Web to provide visualisations of this data to the customers, via the web platform provided by CardioMon.

- The client of Wearable Co. is a consumer and has the role of data subject and cloud subject.
- Wearable Co. is an SME business with the roles of data controller (as it controls the handling of the consumer personal data through the configuration of the SaaS application) and cloud customer.
- CardioMon is a SaaS provider operating as a Cloud provider. It has the roles of data processor and Cloud provider.
- Map-On-Web is another SaaS provider that provides a service which allows the creation of maps overlaid with annotated itineraries based on annotated GPX traces. These images can be incorporated by reference in any web page. The service provider stores the data which is associated with the itinerary.
- The IaaS Cloud Provider is a cloud provider that processes and hosts customer data. It has the role of data processor and Cloud provider.
- Incidentally, CardioMon uses the same IaaS Cloud Provider as Map-On-Web to implement the SaaS they offer (see below).

In the Cloud environment, the negotiation of contracts varies significantly according to the profiles of the Cloud customer and provider. The "by default" situation, which is most often the only situation of small and medium size customers, is the one where the terms of the service contract between the Cloud customer and provider are fixed and non-negotiable – it is the "take-it-or-leave-it" approach of the public cloud providers. For this reason, we have selected to model CardioMon as an SME which will use an IaaS service provider for computation and storage facilities. Adding this fourth actor to the value chain will also allow us to demonstrate how policies are translated through the value chain.

The instantiation of the scenario defined in the use-case is progressive and allows us to conduct a walkthrough of the processes and tools defined in the A4Cloud Reference Architecture. The addition of additional actors allows us to explore additional dimensions constraining accountability. In this use-case, we are focusing on the translation of obligations (through policies) at the application level and multi-tenant scenarios. The provisioning of the Map-on-Web service using the same IaaS provider allows us to build such a value chain.

The demonstration of remediation and redress includes an additional step: the triggering of an incident. We have elected to do so and to involve an external actor (DPA Investigator), who will be using the relevant tools and processes across the value chain

Wearable Co exploits the cloud by offering their customers a Web-based application that will enable them to automatically control the collected data and get customisable visualisations of their status, according to the analysis of their data. The application of this business service will be called the *Wearables Service* and it will interface with existing SaaS providers which store, retrieve and process the customers' personal data and offer them added value functionalities.

In more detail, the "Wearables" service aims to provide the functionalities to their customers. For example – the Wearable Co provider could provide the following functionalities to its customers:

- Enable customers to build their profile by supplying their age, height, weight and everyday activities (such as the duration of a running /walking exercise, etc.);
- Enable customers to provide their heart beat rate, blood pressure, sugar blood level and other human body monitoring metrics on a daily basis;
- Enable customers to inform about their stated allergies and any medical treatment followed in a specific period of time;
- Capture the location of the customers;
- Calculate aggregated statistics for the customers' metrics on a monthly or annual basis;
- Analyse customers' data on a daily basis to automatically build wellbeing training programs;
- Communicate with a health advisory to retrieve the thresholds for the typical values of the human body metrics per age group;

In cases of human body metrics getting exceptional (beyond thresholds) values, communicate the customer profile with a notification

As reflected in these functionalities, the Wearable Co devices will utilise with a cloud service provider, who will present his information to the customers in a fully customised way. From the Wearables perspective, the selected cloud provider, which is now called CardioMon, could implement the following functionalities, which are provided in the form of SaaS:

- Analyse the customer profile and provide feedback in a customisable format defined by the customer
- Provide the thresholds for the typical values of the human body metrics per age group and location, including climate and altitude factors.
- Trigger notifications whenever the customers' metrics exceed defined thresholds.
- Offer visualisations of customers' data on maps, which are provided indirectly by Map-on-Web.

Each of the actors implemented in the demonstrator will be participating as one or more of the roles of Data Controller, Data Processor, Cloud Customer, Cloud Providers etc. Each will implement the A4Cloud Tools and architecture and operate the lifecycle for accountability to ensure that appropriate controls and processes for the protection of data are in place and that they are accountable for their use and management of data.

The Wearable Co customers subscribe to the CardioMon to gain access to the respective functionalities. Upon registration, a customer profile is created, which is used by the service to continuously provide the customers with visualisations of their data, according to the analysis of their daily body measures. The customers can interact with the service and consume the suggested programs, but also to request an analysis of their long term status, based on historical records.

Due to the nature of the Wearables use case and the use of the cloud environment to serve the business needs of the Wearables Service, all the required personal data will be managed and processed outside the control of the data subjects and the data controller, which are the customers and the services providers. Thus, the data handling procedures adopted by the different providers are subject to the control of the local Data Protection Authority (DPA), which is responsible to define the data protection compliance rules, as they arise from the established legal framework.

Figure 32 displays an overview over the Wearable use case, summarises the roles involved and shows how the supply service chain is built in order to facilitate the wearables scenario for the relevant customers.

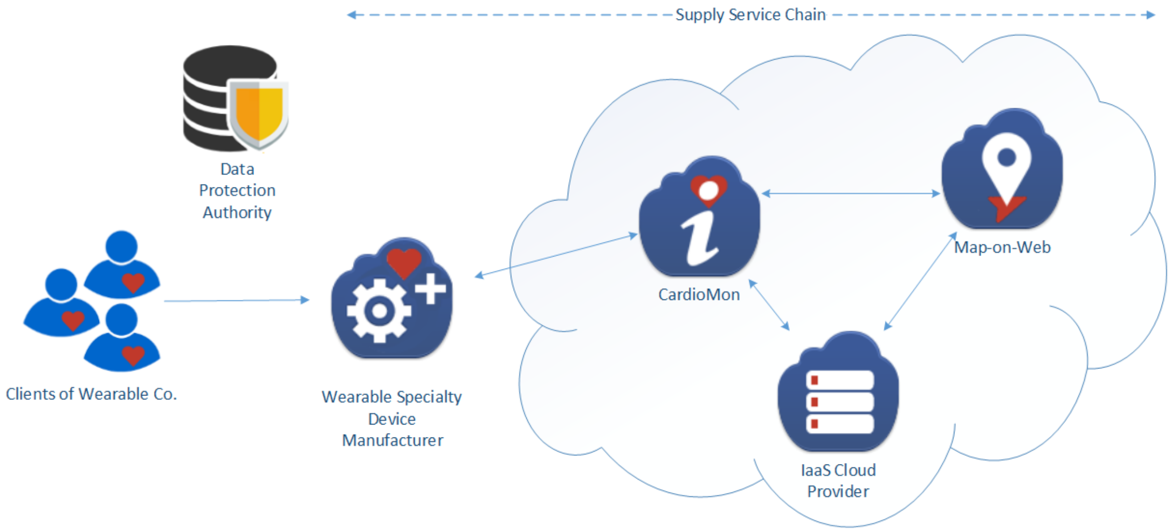


Figure 32: The Wearables service use case

It may become necessary in order to demonstrate the results of the project to enhance the Wearable scenario with additional SaaS providers. One such SaaS provider might be a research institution that can provide analysis of the data in support of horizontal health studies or public policy using anonymised data. Thus the actors such as CardioMon or Map-On-Web may expand the chain of collaborating cloud service providers and must ensure that those it uses meet the data protection and accountability requirements. This will be considered if necessary for demonstration purposed.

10.4 Analysing the Wearables Use Case from an Accountability Perspective

The wearables use case involves the distribution of personal data along a cloud service supply chain. The actors involved in it have to respect the data they process, according to the preferences of the data subjects that own these data and the legal terms that control the provisions of the data handling and sharing practices.

10.4.1 Introducing the Business Concepts

The establishment of the different (cloud) service providers is performed in various time scales. Although a different order may happen and is still valid for our case, we consider the following time schedule:

- In 2012, the IaaS Cloud Provider starts operating as an independent data storage big vendor, which has been deployed in order to host data from various cloud service and Web application providers. The topology of the physical infrastructure involves the physical distribution of the data in many geographical locations, spread around areas governed by different regulatory frameworks. In this use case we assume that the IaaS cloud provider can allocate storage resources in Europe and Africa.
- At a specific period of time in 2013, CardioMon starts its business as a SaaS SME provider in an in-house private cloud. This provider offers algorithms that analyse the profiles of customers and provide them with visualisations, analysis and notifications regarding their health status. In order to accomplish the planned tasks, CardioMon has already come to an agreement with the Map-on-Web SaaS to collaborate in terms of providing the maps overlaid with annotated itineraries based on annotated GPX traces. These images are incorporated by reference in the CardioMon platform. The service provider stores the data which is associated with the itinerary in-house. This agreement has been enforced upon the initiation of CardioMon's business operations.
- Since the first months CardioMon's operation, the need for larger data storage facilities becomes apparent. However, the size of the provider cannot afford for an extension of the private cloud and a strategic decision is made that all the storage facilities are outsourced to a public cloud, reflecting the requirement for collaborating with a trusted IaaS cloud provider. Due to the fact that this service provider handles data classified as sensitive, an accountability based approach is needed, so that the most appropriate IaaS provider is selected to process and host such data. The approach initiates with an analysis of the impact assessment on the involved data from the operation of this SaaS, the

involved risks and the potential mitigation actions, as well as the agreement that should be established between CardioMon and the selected IaaS provider in the form of accountability policy. Such policy should also consider for clarifying the responsibilities for remediation actions among the two parties if a security and/or privacy violation occurs.

- Close to the end of 2013, the Wearables Service, offered by an SME, is about to start in Brussels. The facilitator of the service needs to examine all the legal terms and conditions that govern the operation of such a business to be compliant to the local legal framework and design their policy in a way that the appropriate accountability mechanisms are in place. On top of that, the Wearables Service SME operator needs to discover the most affordable and trusted mapping service to enhance the portfolio of the provided functionalities to their customers (we assume that the same IaaS provider as the one chosen by the mapping service, is selected by this service). The choice needs to consider a lot of parameters, while the operation of the Wearables Service has to reflect the user needs and the limitation of the legal framework. After following the accountability framework and enforce the A4Cloud tools the Wearables Service is gone live.
- In 2014 the Wearables customers start using the Wearables Service. The Web application behaves as expected by the time that an abnormal incident drives the exposure of the service to risks and a relevant policy violation is notified.

We now analyse the above mentioned schedule in more detail. In order to do so, we first identify the cloud computing and data protection roles (see Section 4) for all the actors involved in the wellbeing use case. This is depicted in Table 10.

Table 10: Allocation of roles for the actors in the Wearables use case

Use Case Actor	Cloud Computing Role	Data Protection Role
Wearables customer	Individual Cloud Subject	Data Subject
Wearable Co	Organisation Cloud Customer	Data Controller
CardioMon SaaS	Cloud Provider	Data Processor
Map-on-Web SaaS	Cloud Provider	Data Processor
IaaS Cloud Provider	Cloud Provider	Data Processor
Data Protection Authority	Cloud Supervisory Authority	Supervisory Authority

All these actors (expect from the Wearables customers) have to be accountable with respect to the data they collect and process from the data subjects and they must demonstrate their compliance to the established regulations and organisational policies and the relevant mechanisms to support accountability when operating their businesses. For demonstrating the capability of the A4Cloud tools and the accountability framework to support this wellbeing use case, we instantiate the above time schedule and present the accountability related actions that each organisation actor (thus except the Wearables customers) should undertake to showcase that they are accountable. This instantiation shows how the different actors (from the perspective of their allocated role, as shown in Table 10) adopt the functional elements of the accountability framework, which was presented in Section 2.

10.4.2 Developing the Wearables Use Case

The IaaS Cloud Provider plan their business by examining the type of data they want to enable their customers to store in their cloud infrastructure, in order to analyse the legal requirements that they should implement in their data access services of the cloud infrastructure, through the relevant privacy and security mechanisms (e.g., authentication, authorisation, access control, anonymisation, etc.). With reference to the legal obligations presented in Section 5 of this deliverable, the appointed security representative of the IaaS cloud provider shall decide and accept the responsibility of compliance with the obligations defined for data processors and cloud providers, which are related to personal data management (including data storage and processing). These obligations may refer to the current status of their operating business or any extension to it as part of the business strategy of the IaaS cloud provider (for example the collaboration with third party cloud storage providers).

Table 11: The legal and normative obligations of the IaaS Cloud Provider

Obligation reference	Description of the obligations for the IaaS Cloud Provider
From Legal Perspective	
O17: informing about the use of sub-processors	The IaaS cloud provider is accountable to all of its customers that provide personal data for informing about the use of sub-providers to process these data
O19: evidence of data processing	The IaaS cloud provider is accountable to all of its customers for, upon request, providing evidence on their data processing practices
O20: evidence of data deletion	The IaaS cloud provider is accountable to all of its customers for, upon request, providing evidence on the correct and timely deletion of personal data
From Normative Perspective	
Obligation: privacy-by-default	By default, the IaaS cloud provider implements the strongest privacy settings as the default ones, when receiving personal data for storage
Obligation: monitoring of data practices	The IaaS cloud provider should monitor their actual data practices and keep records of the monitoring and its results
Obligation: compliance with privacy policies	The IaaS cloud provider should be able to demonstrate to any customer compliance with their policies in a timely fashion “reactively” and where possible “proactively”.
Obligation: informing about policy violations	The IaaS cloud provider should be able to inform their customers about any policy violations that are related to any personal data processed within their range of authority
Obligation: remediation in case of damages	The IaaS cloud provider should be able to provide remediation to their customers in the case of damages caused to data subjects due to processing of personal data

By being aware of these obligations and accepting the responsibility for carrying them out, the IaaS cloud provider must proceed to the following accountability-related general steps in order to start their business:

- Identify the risks from processing data in their infrastructure and run a risk analysis on the potential threats and decide on the respective mitigation plans
- Determine the security and privacy mechanisms to be implemented and enforced
- Offer the appropriate tools that enable monitoring the infrastructure and, more specifically, provide logs with respect to data access, data management and data transfer actions.

The obligations are summarized in Table 11.

In turn, CardioMon needs to start their online business as a SaaS by identifying the legal and normative obligations that should be implemented as part of their everyday activities, in order to protect personal data received from associated organisations for analysis. These obligations are depicted in Table 12.

Table 12: The legal and normative obligations of CardioMon

Obligation Reference	Description of the Obligations for CardioMon
From Legal Perspective	
O17: informing about the use of sub-processors	CardioMon is accountable to any collaborating party for informing about the use of the IaaS Cloud Provider to process personal data
O19: evidence of data processing	CardioMon is accountable to any collaborating party for, upon request, providing evidence on their data processing practices

Obligation Reference	Description of the Obligations for CardioMon
O20: evidence of data deletion	CardioMon is accountable to any collaborating party for, upon request, providing evidence on the correct and timely deletion of personal data
From Normative Perspective	
Obligation: personal data minimization	CardioMon must be designed in order to minimise the amount of personal data needed to provide consultancy on their clients' health status
Obligation: privacy-by-default	By default, CardioMon implements the strongest privacy settings as the default ones, when receiving personal data for processing
Obligation: specifying user preferences	CardioMon should offer their customers services that allow the users to specify privacy preferences, for example with respect to how their data are used by the Map-on-Web SaaS
Obligation: monitoring of data practices	CardioMon should monitor their actual data practices and keep records of the monitoring and its results
Obligation: compliance with privacy policies	CardioMon should be able to demonstrate to any customer compliance with their policies in a timely fashion “reactively” and where possible “proactively”
Obligation: compliance with user preferences	CardioMon should be able to provide evidences to their customers that personal data is processed in accordance to their preferences
Obligation: informing about policy violations	CardioMon should be able to inform their customers about any policy violations that are related to any personal data processed within their range of authority
Obligation: informing about privacy preferences violations	CardioMon should inform their customers and their users about any violations of their privacy preferences
Obligation: remediation in case of damages	CardioMon should be able to provide remediation to their customers in the case of damages caused to data subjects due to processing of personal data

By being aware of these obligations and accepting the responsibility for carrying them out, CardioMon must proceed to the following accountability general steps in order to start their business:

- Identify the risks from processing data and run a risk analysis on the potential threats and decide on the respective mitigation plans
- Determine the security and privacy mechanisms to be implemented and enforced
- Offer the appropriate tools that enable monitoring the exchange of data with other parties (such as the Map-on-Web SaaS) and provide logs with respect to data access, data management and data transfer actions.

Moving to Wearable Co, this actor is both a cloud customer, which needs to identify the appropriate cloud providers to collaborate with, and data controller, who decides which are the necessary personal data that should be collected from the end users, so that the respective functionalities for a wellbeing scenario are being served. Since the Wearable Co is an SME, the appointed legal representative of the organisation needs to follow the accountability lifecycle and verify that Wearable Co is an accountable organisation.

In that respect, Wearable Co needs to comply with the established regulations and, thus, examine the constraints imposed by the local legal framework. Thus, before starting building the application, the business service has to determine which personal data will be collected from the customers and how they will be handled both on the Wearables Service side and the other external services that will be added in the supply chain to improve the quality of the application results and the experience of the end customers. The combination of the application data classification and the imposed regulatory rules can potentially drive the specification and/or refinement of the organisational level policy of the business service, with respect to the way that the Wearables Service should operate.

Wearable Co needs to collaborate with cloud providers for two main reasons. First, a cloud infrastructure provider needs to be selected to host the personal data collected by the Wearables Service and the analysis performed by the service to produce the daily wellbeing program. Second, the Wearables Service needs to consume the results of a mapping service, which provides added value to the produced Wearables Service programs and instantiates them, based on the status of the customers, as determined by CardioMon. The selection of the two providers strongly depends on the accountability requirements that the Wearables Service should satisfy, in terms of both the expected quality of the application itself and the legal restrictions applied by the local regulatory framework (in Brussels). These requirements are drawn in the form of legal and normative obligations that should be accepted by the Wearable Co and they are depicted in Table 13.

Table 13: The legal and normative obligations of Wearable Co

Obligation Reference	Description of the Obligations for Wearable Co
From a Legal Perspective	
O1: informing about processing	Wearable Co is accountable to their customers for informing that their personal data are being collected and processed
O2: informing about purpose	Wearable Co is accountable to their customers for informing about the purpose of collecting and processing their personal data
O3: informing about recipients	Wearable Co is accountable to their customers for informing about the recipients of their personal data
O4: informing about rights	Wearable Co is accountable to their customers for informing about the existence of their rights to access and rectify the collected personal data
O5: data collection purposes	Wearable Co is accountable to their customers for collecting personal data only for specific, explicit and legitimate purposes. Moreover, the Wearable Co is accountable to their customers for processing their personal data only for the stated purposes.
O6: the right to access, correct and delete personal data	Wearable Co is accountable to their customers for making it possible for them to access, collect and rectify their personal data
O7: data storage period	Wearable Co is accountable to their customers for keeping their personal data in a form which permits identification for no longer than necessary
O8: security and privacy measures	Wearable Co is accountable to their customers for the security and privacy of the personal data they collect
O9: rules for data processing by provider	Wearable Co is accountable to their customers for how the cloud service providers that they engage process the customers' personal data.
O10: rules for data processing by sub-provider	Wearable Co is accountable to their customers for how any sub-provider to the cloud service provider they engage process the customers' personal data
O11: provider safeguards	Wearable Co is accountable to their customers for choosing cloud providers that can provide sufficient safeguards concerning technical security and organisational measures
O12: sub-provider safeguards	Wearable Co is accountable to their customers for ensuring that all sub-providers involved in the service delivery chain provide sufficient safeguards to protect the personal data that they process
O13: informed consent to processing	Wearable Co is accountable to their customers for obtaining informed consent before collecting their personal data
O14: explicit consent to processing	Wearable Co is accountable to their customers for obtaining their explicit consent before collecting any sensitive personal data
O16: informing DPAs	Wearable Co is accountable to the Data Protection Authority to inform that they collect personal data
O18: security breach notification	Wearable Co is accountable to their customers for notifying them of security incidents that are related to their personal data
O21: data location	Wearable Co is accountable to their customers for informing them about the location of the processing of their personal data
From a Normative Perspective	

Obligation Reference	Description of the Obligations for Wearable Co
Obligation: informing about personal data processing	Wearable Co should inform the selected cloud provider(s) that they will use their services to process personal data

Having these obligations in place, Wearable Co needs advice on how they can select the appropriate cloud providers to collaborate with. The selection is based on both functional and security and privacy characteristics provided by the cloud providers. In this sense, the development of the Wearables Service from an accountability perspective evolves as follows:

- Wearable Co reviews the list of obligations as shown in Table 13 and analyses the security and privacy requirements that should be implemented.
- It performs a survey of the available cloud infrastructure providers and compares their offerings to decide on whom to collaborate with, based on the security and privacy measures that should be safeguarded by the Wearables Service. The IaaS cloud provider is selected. Thus, in Table 13 and the obligations, any reference to cloud providers involves the IaaS cloud provider.
- It performs a survey of the available advisory cloud providers and compares their offerings to decide on whom to collaborate with, based on the security and privacy measures that should be safeguarded by the Wearables Service. The CardioMon SaaS (along with the Map-on-Web SaaS, as a third party) is selected. Thus, in Table 13 and the obligations, any reference to cloud providers involves the CardioMon SaaS.
- Based on the selected candidate cloud provides, Wearable Co performs an impact assessment analysis to identify the risks and determine on the appropriate mitigation plans that should be implemented to ensure compliance with the obligations and the internal policies. This involves the analysis of risk and trust models.
- It comes to an agreement with the cloud providers and requests a demonstration of compliance to their obligations, as cloud providers, handling personal data.
- It, then, compiles the set of obligations and the associated security and privacy requirements to accountability policies that should be enforced upon starting the Wearables Service operation.
- It ensures that the appropriate security and privacy mechanisms, as a result of the impact assessment analysis, are being implemented.
- It ensures that the accountability mechanisms are being integrated into the development of the business service operation and that it is able to demonstrate compliance to the accepted responsibilities and accountability policies.
- It verifies that the accountability mechanisms are correctly implemented.
- The Wearables Service is up and running.

At this point, the Wearables Service is ready to be accessed by the customers.

10.5 Summary

This section has presented the Wearables use case; a new scenario that has been synthesised in order to capture the most interesting features from the three existing business use cases, and that will allow the A4Cloud project to demonstrate all the tools that are being developed without having to implement an complex architecture. The Wearables use case will be further developed in the context of WP:D-7 (instantiation).

11 Conclusions

This deliverable is the final description of the three different A4Cloud business use cases; health care services in the cloud, the cloud-based ERP service and the Rights and relevant obligations in a multi-tenant cloud scenario. As have been shown, the three business use cases are quite different and they complement each other well.

One of the objectives of work package WP:B-3 has been to define the business use cases in terms of the project's conceptual framework. In this deliverable we have worked towards this objective by clarifying the roles of the different actors involved, both in terms of the accountability roles defined by the A4Cloud project as well as in the data protection roles that can be derived from current European data protection legislation. The business use cases have also been analysed in terms of which accountability obligations that apply; i.e. who is responsible to whom and for what, seen from a regulatory, contractual and normative perspective (Section 5). This deliverable also provides an interoperability analysis of the business use cases (Section 6). The latter section concludes by outlining a number of interoperability requirements derived from the regulatory, business, semantic and technical perspectives.

Another objective of work package WP:B-3 has been to analyse the business use cases in the light of progress being made in streams C and D. This deliverable therefore provides an analysis in terms of project tools (Section 7). The analysis demonstrates that most of the actors involved in the business use cases are concerned with accountability functions of the operation phase of their service operation; most importantly with monitoring and notification. The provision of an account is also a very important aspect for most scenarios, especially the validation of the operation, which is concerned with reporting operational aspects.

We have also analysed the business use cases in terms of the accountability governance processes that could be applied in order to help the involved become accountable. The process models in Section 8 demonstrate how the A4Cloud tools will fit into an accountability governance lifecycle. As an example we have instantiated the process models for the healthcare business use case. As can be seen, the processes will involve interactions with A4Cloud tools by, not only data controllers and data processors, but also data subjects and data protection authorities.

The business use cases have played an important role in the requirements phase of the project, and they have been utilized by many other work packages in order to derive requirements, validate their models and theories and demonstrate the different technologies that have been developed. However, ass discussed in Section 10 of this deliverable, we have concluded none of the three existing business use cases can be used on its own to demonstrate all the results of the project; they are either too complex to implement, individually they do not cover the whole space, or (in the case of healthcare) may become entangled with another regulatory domains outside the scope of the work. This deliverable therefore also outlines the Wearables use case, which will be used to create a demonstrator for the complete set of the A4Cloud tools. This new use case will be further analysed, developed and finally implemented under the scope of work package WP:D-7 (instantiation).

12 References

[1] Karin Bernsmed, et.al., "Healthcare Services in the Cloud - Obstacles to Adoption, and a Way Forward". In proceedings of the 9th International Conference on Availability, Reliability and Security (AReS 2014).

[2] Maartje Niezen (Editor), "D:B-4.1 Interim report. The socio-economic landscape of cloud computing", A4Cloud Deliverable, Sep. 2013.

[3] Karin Bernsmed, W. Kuan Hon and Christopher Millard, "Deploying Medical Sensor Networks in the Cloud – Accountability Obligations from a European Perspective". In proceedings of the 7th IEEE International Conference on Cloud Computing (IEEE CLOUD 2014).

[4] Siani Pearson and Massimo Felici (editors), “MSC-2.2 Initial Conceptual Framework,” A4Cloud Milestone Report, Mar. 2013.

[5] Karin Bernsmed (editor), “DB-3.1 Use Case Descriptions”, A4Cloud Deliverable, Jun. 2013.

[6] Theo Koulouris and Fredric Gittler (editors), "MSD-2.2 High-level architecture (Draft)," A4Cloud Milestone Report, Dec. 2013.

[7] Alain Pannetrat (editor), “D:C-3.1 Requirements for cloud interoperability”, A4Cloud Deliverable, Nov. 2013.

[8] F. Liu et al., "NIST Cloud Computing Reference Architecture", NIST Special Publication 500-292, Sep. 2011.

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995.

[10]Siani Pearson and Massimo Felici (editors), “MSC-2.3,” A4Cloud Milestone Report (work in progress).

[11]Massimo Felici (editor), "Glossary of Terms and Definitions", A4Cloud project report, Nov. 2013.

[12]J. Ko et.al., “Wireless Sensor Networks for Healthcare,” *Proc. Ieee*, vol. 98, no. 11, pp. 1947–1960, Nov. 2010.

[13]J. Biswas, et.al., “Processing of wearable sensor data on the cloud - a step towards scaling of continuous monitoring of health and well-being,” 2010, pp. 3860–3863.

[14]C. Millard (editor), "Cloud Computing Law", Oxford: Oxford University Press, 2013.

[15]QMUL and TiU, “Internal Briefing Paper MS: B-5.4 B-5 Contractual and regulatory considerations (WP25),” A4Cloud project report, Jun. 2013.

[16]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), COM (2012) 11 final (25 January 2012).

[17]Martin Gilje Jaatun (editor), "Guiding lights (- The Edinburgh project)", A4Cloud internal report (*work in progress*).

[18]Nils Brede Moe (editor), “D:B-2.1 Stakeholder Workshop 1 Results (Initial Requirements),” A4Cloud Deliverable, Mar. 2013.

[19]Erdal Cayirci (editor), "D:B-2.2 Risk Modelling for Cloud Services Workshop Results", A4Cloud Deliverable, Nov. 2013.

[20]M Felici, T Koulouris, S Pearson Accountability for Data Governance in Cloud Ecosystems, IEEE CloudCom 2013.

[21]Cloud Computing Use Case Discussion Group, “Cloud Computing Use Cases White Paper.” Jul-2010.

[22]P. M. Timothy Grance, The NIST Definition of Cloud Computing. 2011.

[23]“Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing.”

[24]Paul Simmonds, Chris Rezek, and Archiee Reed, “Security Guidance for Critical Areas of Focus in Cloud Computing V3.0,” Cloud Security Alliance, 3.0, 2011.

[25]Policy Representation Framework. Monir Azraoui, Karin Bernsmed, Ronan-Alexandre Cherrueau, Rémi Douence, Kaoutar Elkhiyaoui, Alexandr Garaga, Hervé Grall, Refik Molva, Melek Önen, Jean-Claude Royer, Anderson Santana de Oliveira, Mohamed Sellami, Jakub Sendor and Mario Südholt. Accountability for Cloud and Future Internet Services - A4Cloud Project, D34.1, December 2013.

[26]Enforcement Tools, Service Specification and Architectural Design. Anderson Santana de Oliveira, Alexander Garaga, Kateline Jenatton, Jakub Sendor, Monir Azraoui, Kaoutar Elkhiyaoui, Melek Önen, Walid Benghabrit, Jean-Claude Royer, Mohamed Sellami and Nick Papanikolaou. Accountability for Cloud and Future Internet Services - A4Cloud Project, D43.1, November 2013.

[27]A Cloud Accountability Obligations Representation Framework. Walid Benghabrit, Hervé Grall, Jean-Claude Royer, Mohamed Sellami, Melek Önen, Anderson Santana De Oliveira and Karin Bernsmed. CLOSER 2014, IEEE Computer Society.

[28]Abstract Accountability Language. Walid Benghabrit, Hervé Grall, Jean-Claude Royer, Mohamed Sellami, Karin Bernsmed and Anderson Santana De Oliveira. IFIPTM - 8th IFIP WG 11.11 International Conference on Trust Management, short paper, July 2014.

[29]Accountability for Abstract Component Design. Walid Benghabrit, Hervé Grall, Jean-Claude Royer and Mohamed Sellami. EUROMICRO SEAA 2014, IEEE Computer Society, to appear.

[30]A Brief Introduction to XACML. OASIS Standard. https://www.oasis-open.org/committees/download.php/2713/l, 2003.

[31]S4p: A generic language for specifying privacy preferences and policies. Moritz Y Becker, Alexander Malkis, and Laurent Bussard. Microsoft Research, 2010.

[32]A formal privacy management framework. Daniel Le Métayer. Formal Aspects in Security and Trust, pages 1-15, 2009.

[33]BPMN 2.0. Introduction to the Standard for Business Process Modeling. Thomas Allweyer. ISBN-13: 978-3839149850

[34]Claudio A. Ardagna, Laurent Bussard, Sabrina De Capitani Di Vimercati, Gregory Neven, Stefano Paraboschi, Eros Pedrini, Stefan Preiss, Dave Raggett, Pierangela Samarati, Slim Trabelsi, and Mario Verdicchio. Primelife policy language. http://www.w3.org/2009/policy-ws/papers/Trabelisi.pdf, 2009.

[35]D:C-6.2 Prototype for the data protection impact assessment tool. Anderson Santana de Oliveira, Alexander Garaga, Erdal Cayirci, Dimitra Stefanatou, Ronald Leenes, Lorenzo Della Corte, Rehab Alnemr, Massimo Felici, Siani Pearson, Asma Vranaki. Accountability for Cloud and Future Internet Services - A4Cloud Project, D36.2, September 2014.

[36]ENISA, “Cloud Computing; Benefits, Risks and Recommendations for Information Security,” 2009 Edition, http://www.enisa.europe.eu, June 2014.

[37]CSA, “Consensus Assessment Initiative Questionnaire,” https://cloudsecurityalliance.org/research/cai/, June 2014.

[38]Cayirci, E. Garaga A. Oliveira, A.S. Roudier, Y. (2014), Cloud Adoption Risk Assessment Model”, 2014 International Workshop on Advances in Cloud Computing Legislation, Accountability, Security and Privacy (CLASP) (accepted).

[39]CNIL, “Methodology for Privacy Risk Management: How to Implement the Data Protection Act,” 2012 Edition, http://www.cnil.fr/english/publications/guidelines/, June 2014.

Appendix A: Process Modelling Principles

In this section we describe the modelling principles that we have followed when creating the BPMN models[34].

Principle 1: A unified business process understanding
All BPMN models

- Should be based on one or more to-be scenarios in DB3.1, i.e. it should reflect the need(s) of one of the personas described in this deliverable.
- Must clearly indicate what data is being processed and what A4Cloud tools are involved.
- Must include a clear beginning and a clear end.
- Must be based on a reusable set of activities

Principle 2: A minimal subset of BPMN elements
All BPMN models should be based on a minimal subset of the BPMN elements that are defined in [33].

Principle 3: Strict naming conventions

- All *participants* should be described by their persona's name, followed by brackets that indicate their roles in the cloud ecosystem and the data protection setting, e.g. "Kim [cloud subject; data subject]" and "Peter [cloud provider; data controller]".
- All *activities* should be described by a strong verb and a noun, e.g., "Input Requirements" and "Evaluate Service Offers".
- All *events* should be described by a noun, e.g. "List of cloud service offers" and "Incident".
- All *data* should be described by a noun, e.g. "Contract with hospital".
- All *pools* should describe the name of the process, followed by a reference to a persona and one or more scenarios in DB3.1, e.g. "Incident management (Michael, Scenario 3.1.3)".
- All *swim-lanes* should describe either the process performed by a persona or a parallel process involving one or more of the A4Cloud tools.
- All gateways should be unnamed (since they do not perform any work)
- All sequence flows should be named only after a data-based gateway, giving a condition on which it is activated, e.g. "Legal advice needed".

Principle 4: Simple business process diagrams
All BPMN models should ideally consists of at most 10 activities

Principle 5: Appropriate abstractions
All BPMN models should have an appropriate level of abstraction: avoid including unnecessary details, e.g. the inner workings of the A4Cloud tools.

Principle 6: Verification
All BPMN models should be reviewed by appropriate stakeholders (preferably the tool owners).

[34] Inspired by http://www.slideshare.net/Dariusilingas/bpm-europe2013-efficientuseofbpmnpublish

Appendix B: Tool Analysis of the Business Use Cases

In this section, we present the analysis tables, which were used to map the to-be scenarios of BUC1, 2 and 3 described in D:B-3.1 [5] to the A4Cloud tools, as well as to the accountability functions, which play a central role in the scenarios.

B.1 Scenario / Tool Mapping for Business Use Case 1

Functional Areas	Tool	Cloud Subject	Cloud Customer	Cloud Provider	Superv. Authority
Contract & Risk Management	Cloud Offerings Advisory Tool			- 4.1.4a (identify controls)	
	Data Protection Impact Assessment Tool		- 3.1.2a (accept responsibility, identify controls)		
Policy Definition & Enforcement	Data Transfer Monitoring Tool		- 3.1.1b (provision of account, monitoring system) - 3.1.1c (provision of account, monitoring system)	- 5.1.1a (provision of account, monitoring system, external verification)	
	AccLab	- 1.1.1a (provision of account) - 1.1.2a (provision of account) - 1.1.2b (provision of account) - 2.1.1b (provision of account)	- 3.1.1a (identify controls, implement measures)		
	A-PPL Engine	- 1.1.2c (-) - 1.1.3a (provision of account, monitoring system)	- 3.1.1a (identify controls, implement measures) - 3.1.1b (provision of account, monitoring system) - 3.1.3a (monitoring system, notification)		
Evidence & Validation	Audit Agent System		- 3.1.1c (provision of account, monitoring system) - 3.1.1d (provision of account, monitoring system) - 3.1.1e (provision of account, monitoring system, notification) - 3.1.3a (monitoring system, notification)	- 4.1.3a (provision of account, monitoring system, external verification) - 5.1.1a (provision of account, monitoring system, external verification) - 5.1.1b (-)	- 6.1.1a (provision of account, monitoring system, external verification)
	Assertion Tool	Meta tool for checking correctness of A4Cloud tools.			
Data Subject Controls	Data Subject Access Request Tool	Insufficient information on tools, as of time of writing.			
	Data Track (& Plugin for Policy Violation)	- 1.1.1b (monitoring system) - 1.1.1c (provision of account, monitoring system, notification, remediation and redress) - 1.1.2c (-) - 1.1.3a (provision of account, monitoring system)			

Incident Response & Remediation	Transparency Log	- 1.1.3a (provision of account, monitoring system)	- 3.1.3a (monitoring system, notification)		
	Remediation & Redress Tool		- 3.1.3b (notification, remediate and redress)		- 6.1.1b (remediate and redress)
	Incident Response Tool		- 3.1.3a (monitoring system, notification) - 3.1.3b (notification, remediate and redress)		

B.2 Scenario / Tool Mapping for Business Use Case 2

Functional Areas	Tool	Cloud Subject	Cloud Customer	Cloud Provider	Superv. Authority
Contract & Risk Management	Cloud Offerings Advisory Tool		- 8.1.1b (identify controls)		
	Data Protection Impact Assessment Tool		- 8.1.1b (identify controls)	- 10.1.1a (identify controls)	
Policy Definition & Enforcement	Data Transfer Monitoring Tool			- 9.1.1a (provision of account, monitoring system)	
	AccLab	- 7.1.1a (provision of an account, monitoring system, external verification)		- 9.1.1a (provision of account, monitoring system)	
	A-PPL Engine			- 9.1.1a (provision of account, monitoring system)	
Evidence & Validation	Audit Agent System	- 7.1.1b (provision of account, monitoring system, external verification)	- 8.1.1a (monitoring system)		- 12.1.1a (external verification)
	Assertion Tool	Meta tool for checking correctness of A4Cloud tools.			
Data Subject Controls	Data Subject Access Request Tool	Insufficient information on tools, as of time of writing.			
	Data Track (& Plugin for Policy Violation)	- 7.1.1a (provision of an account, monitoring system, external verification)			
	Transparency Log	- 7.1.1b (provision of account, monitoring system, external verification)		- 11.1.1a (notification)	
Incident Response & Remediation	Remediation & Redress Tool				
	Incident Response Tool			- 11.1.1a (notification)	

B.3 Scenario / Tool Mapping for Business Use Case 3

Functional Areas	Tool	Cloud Subject	Organizational Cloud Customer	Cloud Provider	Superv. Authority

Contract & Risk Management	Cloud Offerings Advisory Tool			- 15.1.1a (provision of account, external verification) - 15.1.1b (accept responsibility, identify controls) - 15.1.1e (accept responsibility, identify controls)	16,17
	Data Protection Impact Assessment Tool			- 15.1.1b (accept responsibility, identify controls) - 15.1.1e (accept responsibility, identify controls)	
Policy Definition & Enforcement	Data Transfer Monitoring Tool		- 14.1.1a (monitoring system, external verification) - 14.1.1c (provision of account, monitoring system, external verification)		- 16.1.1a (provision of account, monitoring system, external verification, notification) - 16.1.1b (external verification) - 17.1.1a (external verification, notification)
	AccLab	- 13.1.1b (provision of account)	- 14.1.1b (provision of account)	- 15.1.1c (implement measures)	- 19.1.1a (implement measures)
	A-PPL Engine	- 13.1.1c (provision of account, monitoring system, notification) - 13.1.1d (provision of account, notification, remediation) - 13.1.1e (provision of account) - 13.1.1g (provision of account, monitoring system, external verification, notification, remediation)	- 14.1.1d (notification) - 14.1.1e (provision of account, notification)	- 15.1.1c (implement measures)	- 19.1.1a (implement measures)
Evidence & Validation	Audit Agent System		- 14.1.1a (monitoring system, external verification) - 14.1.1c (provision of account, monitoring system, external verification)	- 15.1.1d (provision of account, monitoring system, notification)	- 16.1.1a (provision of account, monitoring system, external verification, notification) - 16.1.1b (external verification) - 17.1.1a (external

					verification, notification) - 18.1.1b (monitoring system, external verification) - 20.1.1a (monitoring system, external verification)
	Assertion Tool	Meta tool for checking correctness of A4Cloud tools.			
Data Subject Controls	Data Subject Access Request Tool	Insufficient information on tools, as of time of writing.			
	Data Track (& Plugin for Policy Violation)	- 13.1.1c (provision of account, monitoring system, notification) - 13.1.1d (provision of account, notification, remediation) - 13.1.1e (provision of account) - 13.1.1g (provision of account, monitoring system, external verification, notification) - 18.1.1a (provision of account, monitoring system, notification)			
	Transparency Log	- 13.1.1c (provision of account, monitoring system, notification) - 13.1.1d (provision of account, notification, remediation) - 13.1.1e (provision of account) - 13.1.1g (provision of account, monitoring system, external verification, notification, remediation)	- 14.1.1d (notification)	- 15.1.1d (provision of account, monitoring system, notification)	
Incident Response & Remediation	Remediation & Redress Tool	- 13.1.1f (remediation and redress)			- 18.1.1b (monitoring system, external verification)
	Incident Response Tool	- 13.1.1g (provision of account, monitoring system, external verification, notification, remediation)	- 14.1.1d (notification)	- 15.1.1d (provision of account, monitoring system, notification)	

Appendix C: Cloud Security Risk Assessment Input

C.1 ENISA's List of Risk Scenarios and Their Categories

Risk Category	Risk name
Policy & Organizational	P1.Lock-in P2.Loss of governance P3.Compliance challenges P4.Loss of business reputation due to co-tenant activities P5.Cloud service termination or failure P6.Cloud provider acquisition P7.Supply chain failure
Technical	T1. Resource exhaustion (under or over provisioning) T2. Isolation failure T3. Cloud provider malicious insider - abuse of high privilege roles T4. Management interface compromise (manipulation, availability of infrastructure) T5. Intercepting data in transit T6. Data leakage on up/download, intra-cloud T7. Insecure or ineffective deletion of data T8. Distributed denial of service (DDoS) T9. Economic denial of service (EDOS) T10. Loss of encryption keys T11. Undertaking malicious probes or scans T12. Compromise service engine T13. Conflicts between customer hardening procedures and cloud environment
Legal	L1. Subpoena and e-discovery L2. Risk from changes of jurisdiction L3. Data protection risks L4. Licensing risks
Not Specific to the Cloud	N1. Network breaks N2. Network management (i.e., network congestion / disconnection / non-optimal use) N3. Modifying network traffic N4. Privilege escalation N5. Social engineering attacks (i.e., impersonation) N6. Loss or compromise of operational logs N7. Loss or compromise of security logs (manipulation of forensic investigation) N8. Backups lost, stolen N9. Unauthorized access to premises (including physical access to machines and other facilities) N10. Theft of computer equipment N11. Natural disasters

C.2 Vulnerability Indices for the BUC2 SaaS

Risk	Vulnerability Index
R-01	0.405934883
R-02	0.405385514
R-03	0.444698566
R-04	0.202830272
R-05	0.335959243
R-06	0.473684211
R-07	0.442677307
R-08	0.3777523
R-09	0.224310776
R-10	0.297268443

R-11	0.194050832
R-12	0.259796938
R-13	0.289997179
R-14	0.369565217
R-15	0.245797721
R-16	0.238656215
R-17	0.278763441
R-18	0.256531532
R-19	0.182816836
R-20	0.405595886
R-21	0.356579984
R-22	0.444444444
R-23	0.444444444
R-24	0.473684211
R-25	0.219774235
R-26	0.219774235
R-27	0.211996849
R-28	0.235588738
R-29	0.222943394
R-30	0.240628942
R-31	0.240628942
R-32	0.171073581
R-33	0.173469388
R-34	0.173469388
R-35	0.244186047