Towards a Conceptual Framework for Accountability

Siani Pearson, HP
TAFC Workshop, Malaga, June 2013

This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
A4Cloud focuses on **accountability** as a critical prerequisite for effective governance and control of corporate and private data processed by cloud-based IT services.

The project aims to assist holding cloud (and other) service providers accountable for how they manage **personal, sensitive and confidential information** ‘in the cloud’.

www.a4cloud.eu
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Our Definition of Accountability
Defining Accountability

Conceptual Definition of Accountability

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

- Responsible and proactive (explaining, justifying, remedying) delivery of actions

- Compliance with respect to internal and external criteria defined by stakeholders

Applicable across different domains and capturing a shared multidisciplinary understanding within the project

Concerned about governance: processes which devise ways of achieving accountability

This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Accountability for Data in the Cloud

Definition of Accountability

• Accountability for an organisation consists of accepting responsibility for the stewardship of personal and/or confidential data with which it is entrusted in a cloud environment, 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).

• It involves committing to legal and ethical obligations, policies, procedures and mechanisms, explaining and demonstrating ethical implementation to internal and external stakeholders and remedying any failure to act properly.

Contextualising accountability for data governance in cloud ecosystems

Personal and/or confidential data

Ethical aspects of accountability

Deploying mechanisms and tools
Our Model of Accountability
From accountability to being accountable

- Operationalise the accountability definitions
- Capture different abstraction levels of accountability
- Identify attributes contributing towards accountability
- Characterize accountable organisations
- Identify elements of accountability practices
- Enable accountability practices
Accountability

Attributes

Practices

Tools
ACTORS  ACTIONS

ATTRIBUTES  PRACTICES  ACTIONS

ANALYSIS  MECHANISMS

SUPPORT  TOOLS

EVIDENCE  ASSERTION
Accountability Context

Regulatory Regimes

Accountability

Attributes

Mechanisms and Tools

Practices

Cloud Ecosystem

Actors (Roles)

Relationships

Mechanisms and Tools

Cloud Ecosystem

Actors (Roles)

Relationships

Mechanisms and Tools

Cloud Ecosystem

Actors (Roles)

Relationships

Mechanisms and Tools

This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Accountability Practices

*Defining central behaviour of an organisation adopting an accountability-based approach*

**Defining governance** to responsibly comply with internal and external criteria, particularly relating to treatment of personal data and confidential data

**Ensuring implementation of appropriate actions** (including procedural mechanisms to ensure these policies get rolled out) which might include some technology in the form of decision support systems and risk assessment

**Explaining and justifying those actions** - demonstrating regulatory compliance, that stakeholders’ expectations have been met and that organizational policies have been followed

**Remedying any failure to act properly**
Accountability Practices

Organisational accountability

Accountability practices – What organisations must do to be accountable

Identify Risks and Opportunities → Integrated Governance

Commitment
- Solid policies aligned to external criteria
- Management commitment
- Full transparency

Implementation
- Mechanisms to ensure policies and commitments are put into effect with employees

Validation
- Monitoring and assurance programs that validate both coverage and effectiveness of implementation

Demonstration
- DEMONSTRATE capacity to internal stakeholders
- DEMONSTRATE capacity to external stakeholders
- DEMONSTRATE capacity to individual data subjects

This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Responsibility: The state of being assigned to take action to ensure conformity to a particular set of policies or rules.

Transparency: The property of an accountable system that it is capable of “giving account” of, or providing visibility of, how it conforms to its governing rules and commitments.

Liability: The state of being liable (legally responsible).

Remediation: The act or process of correcting a fault or deficiency.

Verifiability: A property of an object, process or system that its behaviour can be verified against a set of requirements.

Observability: A property of an object, process or system which describes how well the internal actions of the system can be described by observing the external outputs of the system.

Attributability: A property of an observation that discloses or can be assigned to actions of a particular actor (or system element).
ACCOUNTABILITY

TRANSPARENCY

VERIFIABILITY

ATTRIBUTABILITY

OBSERVABILITY

RESPONSIBILITY

(legal implication)

LIABILITY

Actor A

Actor B

CLOUD
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

Accountability Mechanisms and Tools

Diverse accountability mechanisms and tools that support accountability practices, that is, accountability practices use them.
CLOUD ACCOUNTABILITY PROJECT

Accountability Framework

Preventive
- Risk and trust assessments
- Policy specification
- Certification

Detective
- Notification of policy violation
- Data subject access
- Other tracking & transparency tools

Corrective
- Facilitation of redress
- Data accuracy correction

Users
- Risk analysis
- Support for contract negotiation
- Policy enforcement

Providers
- Monitoring & policy-aware logs
- Reasoning tools

Regulators
- Involvement in privacy impact assessments
- Guidelines & best practice

Whole eco-system approach

Inter-disciplinary co-design

This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Introduction of A4Cloud project

- Highlighted its relevance for global business & cloud computing

Defined accountability

- Clarified focus and scope and introduced accountability model

Introduced accountability framework

- Overall approach

For further details, see pre-proceedings paper
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

IEEE CloudCom 2013
5th IEEE International Conference on Cloud Computing Technology and Science
December 2-5, Bristol, UK
2013.cloudcom.org
Hosted by HP and the University of the West of England
Cloud Accountability Project Workshop:
risk workshop for those actively involved in cloud business

Cloud Security Alliance EMEA Congress
24-26 September
Edinburgh, Scotland

http://www.a4cloud.eu/a4cloud_risk_workshop

https://cloudsecurityalliance.org/events/csa-emea-congress-2013/
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

**A4Cloud Objectives**

- **Enable cloud service providers to give their users appropriate control and transparency over how their data is used.**
- **Enable users to make choices about how cloud service providers may use and will protect data in the cloud.**
- **Monitor and check compliance with users’ expectations, business policies, and regulations.**
- **Implement accountability ethically and effectively.**
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).