Towards a Conceptual Framework for Accountability
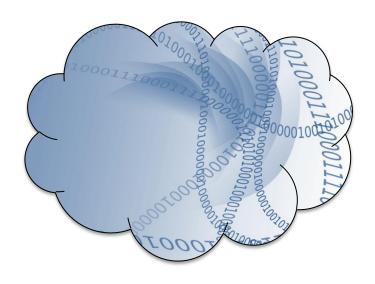
Siani Pearson, HP
TAFC Workshop, Malaga, June 2013

www.a4cloud.eu

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'.

A4Cloud project partners

CLOUD ACCOUNTABILITY PROJECT

Industry Partners

Cloud Community & Standardisation

SAP

ATC — ATHENS TECHNOLOGY CENTER

CSA cloud security alliance SM

Coordinated by:

hp

Research Institutes

ECOLE DES MINES DE NANTES

EURECOM Sophia Antipolis

Queen Mary University of London

HOCHSCHULE FURTWANGEN UNIVERSITY HFU

SINTEF

TILBURG UNIVERSITY

KARLSTADS UNIVERSITET

University of Stavanger

UNIVERSIDAD DE MÁLAGA

R&D in technical, legal and socio-economic aspects of accountability in the cloud

Our Definition of Accountability

Conceptual Definition of Accountability

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

*Concerned about **governance:** processes which devise ways of achieving 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*

Accountability for Data in the Cloud

> **Contextualising accountability for _data governance_ in _cloud ecosystems_**

Definition of Accountability

> **Personal and/or confidential data**

- _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._

> **Ethical aspects of accountability**

> **Deploying mechanisms and tools**
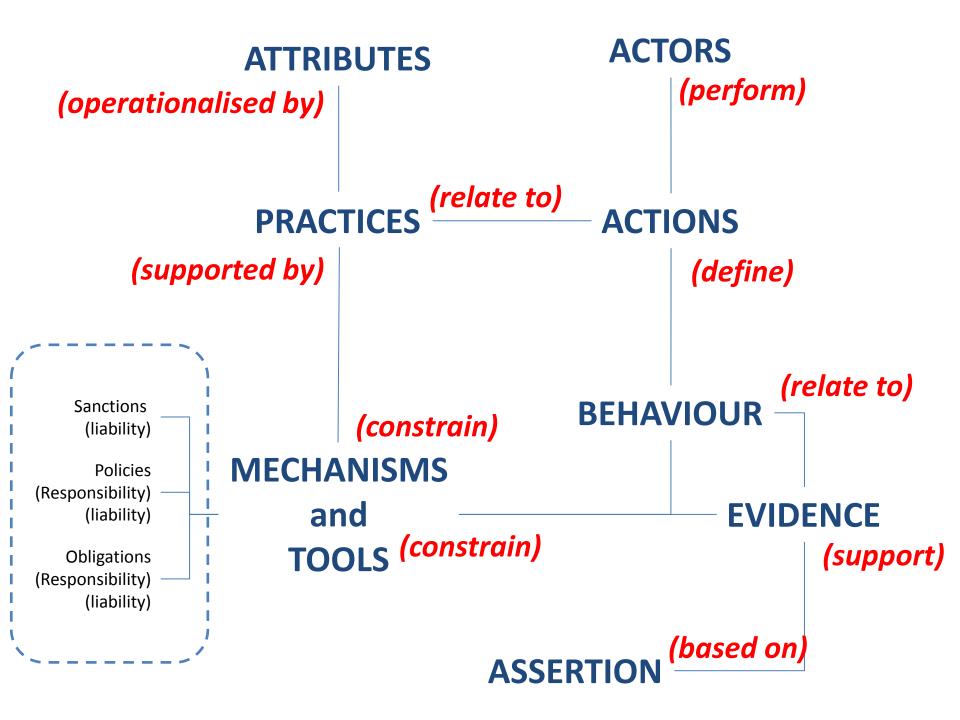
Our Model of Accountability

Accountability Model

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
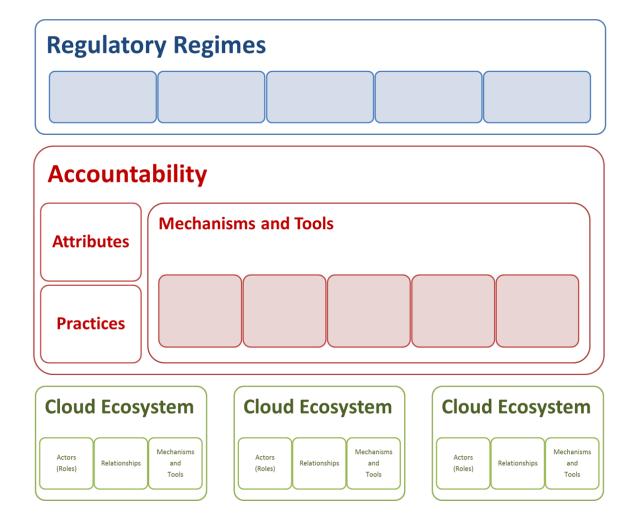
- Enable accountability practices

Accountability

Attributes

Practices

Tools

Accountability Context

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

Oversight

| Identify Risks and Opportunities ➡ | Integrated Governance |

Contextual Approach

Commitment	Implementation	Validation
• Solid policies aligned to external criteria • Management commitment • Full transparency	• Mechanisms to ensure policies and commitments are put into effect with employees	• 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

Accountability Attributes

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).

Conceptual attributes of accountability as used across different **multidisciplinary domains**

Accountability Attributes

Assurance · Responsibility · Transparency · Obligations · Verifiability · Liability · Observability · Sanctions · Remediation

Conceptual basis for our definitions, and related taxonomic analysis

Defined in the project glossary

A4Cloud Glossary

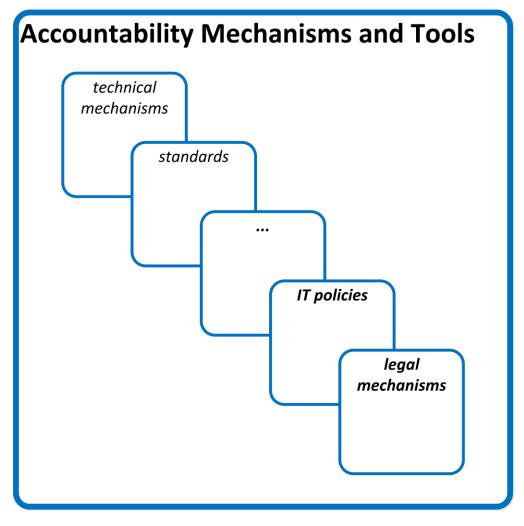| Accountability	Cloud Computing	Information Security	Industry or Research Domain-specific Terminology

ACCOUNTABILITY

TRANSPARENCY

VERIFIABILITY

ATTRIBUTABILITY

Actor A

Actor B

CLOUD

OBSERVABILITY

RESPONSIBILITY
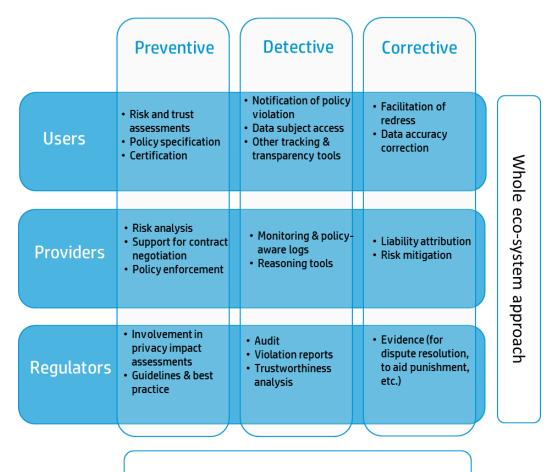
(legal implication)

LIABILITY

Accountability Framework

CLOUD ACCOUNTABILITY PROJECT

	Preventive	**Detective**	**Corrective**
Users	• Risk and trust assessments • Policy specification • Certification	• Notification of policy violation • Data subject access • Other tracking & transparency tools	• Facilitation of redress • Data accuracy correction
Providers	• Risk analysis • Support for contract negotiation • Policy enforcement	• Monitoring & policy-aware logs • Reasoning tools	• Liability attribution • Risk mitigation
Regulators	• Involvement in privacy impact assessments • Guidelines & best practice	• Audit • Violation reports • Trustworthiness analysis	• Evidence (for dispute resolution, to aid punishment, etc.)

Whole eco-system approach

Inter-disciplinary co-design

Accountability Approach

CLOUD
ACCOUNTABILITY
PROJECT

Individual service users

Business governance

Auditors

Regulators

Governance

Primary service provider (PSP)

Accountable service ecosystem

Trusted tools & services supporting accountability

Cloud service supply chain

CSP1

CSP2

CSP3

CSP4

Accountability

Appropriate views of data

SEVENTH FRAMEWORK PROGRAMME

Introduced 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

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

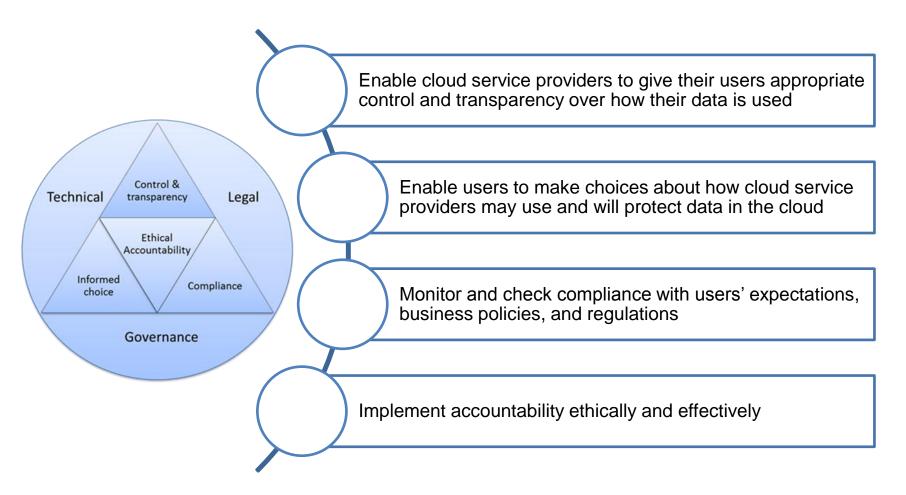https://cloudsecurityalliance.org/events/csa-emea-congress-2013/

CLOUD ACCOUNTABILITY PROJECT

Questions?

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

A4Cloud Deliverables

CLOUD ACCOUNTABILITY PROJECT

Control and Transparency

- Policy Configuration and Enforcement System
- Accountability Validation Tool

Choice

- Risk Assessment Tool
- Contract Support Tool

Compliance

- Evidence Collection System
- Remediation Tool
- Policy Monitoring Tool

Accountability Framework

- Recommendations and guidelines
- Reference architecture
- Models of data governance
- Interoperable policy languages
- Accountability metrics
- Ethical accountability

The Cloud Accountability Project