A4Cloud- Accountability in the Cloud

Carmen Fernández Gago
NICS Lab
Universidad de Málaga
Outline

• A4Cloud overview
• A4Cloud solution
• Contribution of UMA
• Standards
• Current state
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Accountability in the Cloud

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.
Accountability is a critical prerequisite for effective governance and control of corporate and private data processed by cloud-based IT services.

But how can cloud (and other) service providers be accountable for how they manage personal, sensitive and confidential information ‘in the cloud’?
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

**Objectives**

**Objective 1:** Develop tools that enable cloud service providers to give their users appropriate control and transparency over how their data is used, confidence that their data is handled according to their expectations and is protected in the cloud, delivering increased levels of accountability to their customers.

**Objective 2:** Create tools that enable cloud end users to make choices about how cloud service providers may use and will protect data in the cloud, and be better informed about the risks, consequences, and implementation of those choices.

**Objective 3:** Develop tools to monitor and check compliance with users’ expectations, business policies and regulations.

**Objective 4:** Develop recommendations and guidelines for how to achieve accountability for the use of data by cloud services, addressing commercial, legal, regulatory and end user concerns and ensuring that technical mechanisms work to support them.
Accountability consists of:

- Defining and accepting responsibility
- Ensuring implementation of appropriate actions
- Explaining and justifying actions
- Remediating failure
An accountable organisation must commit to responsible stewardship of other people’s data. It:

- **defines** what it does,
- **monitors** how it acts,
- **remedies** any discrepancies between the definition of what should occur and what is actually occurring
- **explains** and justifies any action.
Demonstrate Accountability

- Accountability Attributes
  - Conceptual elements of accountability as used across different domains

- Accountability Practices
  - Emergent behaviour characterising accountable organizations

- Accountability Mechanisms
  - Operational processes, non-technical mechanisms and technical tools that support accountability practices

The Objective

- Transparency
- Responsiveness
- Responsibility
- Remediability
- Verifiability
- Effectiveness
- Appropriateness

Defining governance
Ensuring governance
Demonstrating governance
Holding to account

Different mechanisms supporting accountability (Preventive, Detective, Corrective)
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
<table>
<thead>
<tr>
<th>Role</th>
<th>Tool</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SME user &amp; SME user</td>
<td>DPIAT</td>
<td>Assess risks</td>
</tr>
<tr>
<td>Data Subject &amp; SME user</td>
<td>COAT</td>
<td>Advises on who complies more with preferences</td>
</tr>
<tr>
<td>CSP Privacy Officer &amp; Service Spec.</td>
<td>AccLab</td>
<td>Defines policies</td>
</tr>
<tr>
<td>Cloud Customers, Auditor</td>
<td>A-PPL Engine</td>
<td>Enforces policies</td>
</tr>
<tr>
<td>Privacy Officer &amp; Int. Ext. Auditors</td>
<td>Data Transfer Monitor Tool</td>
<td>Identifies policy violations</td>
</tr>
<tr>
<td>Auditor</td>
<td>AAS</td>
<td>Provides Audit Records</td>
</tr>
<tr>
<td>CSP</td>
<td>Assertion Tool</td>
<td>Provides Accountability Assertions</td>
</tr>
<tr>
<td>Data Subject &amp; SME user</td>
<td>Incident reporting, Redress</td>
<td>Informs, fixes, supports compensation</td>
</tr>
<tr>
<td>Data Subject</td>
<td>Data Track</td>
<td>Presents data disclosures</td>
</tr>
<tr>
<td>Transp. Log</td>
<td>Monitor</td>
<td>Monitor</td>
</tr>
</tbody>
</table>

This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Contribution of UMA
A4Cloud and the Role of Metrics in Accountability

- Metrics as a means for demonstrating accountability
  - Metrics contribute to show that the proper mechanisms for privacy, security and information governance are in place.
  - Metrics are used for exposing inside information to end-users.
  - Metrics support reasoning and decision-making.
Eliciting Metrics for Accountability

• How to measure Accountability?

• The nature of the Accountability attributes is very abstract:
  • Transparency, Responsibility, Attributability, Verifiability, Liability, Observability, Remediability

• Two complementary approaches were followed:
  • Top-down approach: Metrics Metamodel
  • Bottom-up approach: Analysis of Control Frameworks
The goal of this metamodel is to serve as a language for describing:

- attributes in terms of entities, evidence and activities

Metrics take two main kinds of inputs: **evidence** and **criteria**.

Appropriate for identifying sub-attributes of the accountability attributes and for identifying the concepts to be measured.

It is not enough when trying to define metrics.
Bottom-up approach

- Eliciting metrics from relevant control frameworks
  - A first step is to identify which controls are relevant for accountability attributes
  - Next, measurable aspects (quantitative/qualitative) are identified
  - Metrics derived this way will be automatically aligned with the principles of accountability, since a quantitative improvement in the measured results will have benefetial effects on the fulfillment of the controls.
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).
Eliciting Metrics for Accountability

Security Incident Management, E-Discovery & Cloud Forensics

Incident Reporting

SEF-03

Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.
Accountability Metrics Catalogue

- A catalogue of 39 metrics organized in three categories
  - Verifiability and Compliance: Demonstrating compliance to good practices and regulations.
  - Transparency, Responsibility and Attributability: Measuring the characteristics about the internal processes that provide Accountability.
  - Remediability and Incident Response: Measuring aspects related to remediation, redress, and incident response. The concept of Accountability goes beyond showing compliance and providing transparency, and must include also response to threats, incidents and failures to comply.
Example: Metric 15. Type of Notice

**Description:** This metric describes the type of privacy notice provided by the collecting organization, depending on how the privacy notice is offered to the data subjects. Ideally, multi-layer notice should be provided so data subjects have the information necessary to make decisions at any point in time.

**Accountability Attributes:** Transparency.

**Associated Evidence:** Privacy Notice

**Formulation and output:**

- Level 1 – Single notice: The organization provides only a single document describing the privacy notice.

- Level 2 – Multi-layer notice: The organization provides different layers of notices. Each layer can present different degrees of information, as long as the union of all the layers is compliant with applicable privacy regulations.

**References:** NIST SP 800-53 R4 (TR-1).
A4Cloud and Standards

- **19806-P1** (vocabulary). Contribution to this standard with the proper vocabulary of A4Cloud.
- **19086-P2** (metrics). We provided feedback for the first version. The second version to be released soon.
- **19086-P3** (requirements). Awaiting for the outcomes of the SC38 meeting.
- We have contributed to the **NIST RATAX** standard on metrics for the cloud
  - Our metrics are being written using their template for metrics
Applications and Future Work

- The project is in the process of integration of the different tools
  - They are being tested at the moment in some application scenarios.
- Application of the metrics for accountability for the development of an **Accountability Maturity Model (AMM)**.
- Still in conversations with standardization bodies to include all the accountability results obtained in them.