On October 6, 2014, HP Company announced it will separate into two independent publicly-traded companies:

**Hewlett Packard Enterprise:**
- Enterprise technology infrastructure, Software, Services and Financing businesses,

**HP Inc:**
- Printing and Personal systems businesses,

*Split has been finalized November 1st, 2015*
Business Users’ Ranking of Key Actions to Improve Cloud Adoption

– Accountability is a clear supporter of growth in the cloud marketplace
Agenda

- The Concept of Accountability
- Accountability Relationships in Cloud Ecosystems
- From Concept to Practice: A4 Cloud project
The Principle of Accountability

Accountability consists of:
• Defining and accepting responsibility
• Ensuring implementation of appropriate actions
• Explaining and justifying actions
• Remediating failure

Article 29 WP 173, Opinion 3/2010 on the principle of accountability:

➢ Data protection must move from ‘theory to practice’.

(i) need for a controller to take appropriate and effective measures to implement data protection principles;

(ii) need to demonstrate upon request that appropriate and effective measures have been taken. Thus, the controller shall provide evidence of (i) above.
Data Controller (DC)
- An entity (whether a natural or legal person, public authority, agency or other body) which alone, jointly or in common with others determines the purposes for which and the manner in which any item of personal data is processed.

Data Processor (DP)
- An entity (whether a natural or legal person, public authority, agency or any other body) which processes personal data on behalf and upon instructions of the Data Controller.

Data Subject
- An identified or identifiable individual to whom personal data relates, whether such identification is direct or indirect (for example, by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity).

Data Protection Authority (DPA)
- The entity responsible in each EU country for the enforcement and monitoring of compliance with data protection legislation.
OECD Privacy Principles form the Basis for most Data Protection and Privacy Laws

<table>
<thead>
<tr>
<th>Collection limitation</th>
<th>Data quality</th>
<th>Purpose specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use limitation</td>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>Openness</td>
<td>Individual participation</td>
<td>Accountability</td>
</tr>
</tbody>
</table>

OECD - Organization for Economic Cooperation and Development
Businesses operate under many obligations and expectations:
- Societal
- Regulatory
- Contractual

Implement appropriate measures to meet obligations and manage risks
- Privacy by design
- Security
- ...

Demonstrate how obligations are met and risks managed
- A central part of accountability
- Increases trust
Accountability Relationships
Who is accountable for what to whom?
Notions of Accountability

**Accountability as a virtue**
- Set of standards for the evaluation of behaviour of public actors

**Accountability as a mechanism**
- Institutional relation in which an actor can be held to account by a forum

Steering accountable behaviour *ex ante*

Giving account *ex post facto*
Accountability Relationships

**Accountor** is accountable to **Accountee** for:

- **Norms**
  - Obligations & permissions that define data practices
    - Can be expressed in policies
    - Derived from law, contracts and ethics

- **Behavior**
  - The actual data processing behavior of an organization

- **Compliance**
  - Entails comparison of organization’s actual behavior with the norms

Copyright Hewlett Packard Enterprise 2015 - Confidential
Example

Accountability through cloud service supply chains to cloud customer, and to governance

DC accountable for applicable data protection measures

DP accountable for cooperation with DC to:
- Respect data subjects’ rights
- Assist DC in providing security measures
- Act only on DC’s behalf

DC : Data Controller
DP: Data Processor
From concept to practice:

A4Cloud project
Cloud Accountability Project

Framework 7 Integrated Project
A4Cloud “Accountability for Cloud and Other Future Internet Services”

Duration: 42 Months (Oct ‘12 to Mar ’16)
13 Partners - Coordinator & Scientific Lead Hewlett Packard Enterprise (HPE)

Industry

Hewlett Packard Enterprise

Community

Ecole des Mines de Nantes
Eurecom
Queen Mary University of London
HFU
SINTEF
Tilburg University

Research

University of Stavanger
University of Malaga

Copyright Hewlett Packard Enterprise 2015 - Confidential
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

**Conceptual Model of Accountability**

- **Accountability**
  - **abstract**
  - **With what?**
  - **How?**
  - **What?**

- **conceptual**
- **organisational**
- **operational**

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

Defining Accountability

Accountability
Attributes
Practices
Mechanisms

State of accepting allocated responsibilities (including usage and onward transfer of data to and from third parties), explaining and demonstrating compliance to stakeholders and remediying any failure to act properly.

Responsibilities may be derived from law, social norms, agreements, organisational values and ethical obligations.
Accountability Attributes

- Transparency
- Responsiveness
- Responsibility
- Remediability
- Verifiability
- Appropriateness
- Effectiveness
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

Accountability Practices

- Define governance
- Ensure implementation
- Explain & justify actions
- Remedy failures

Accountability

Attributes

Practices

Mechanisms
Organisations must demonstrate willingness and capacity to be responsible and answerable for data practices

1. Embrace responsibilities
2. Define policies reflecting contextual norms
3. Enforce policies
4. Monitor practices
5. Correct violations
6. Demonstrate compliance

How can Organisations be Accountable?
Accountability Mechanisms

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

Accountability Mechanisms

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

Accountability Support Services

Policy Definition & Validation
Policy Management & Enforcement
Monitoring & Environment State Collection
Collection & Management of Evidence
Validation
Remediation
Notification
Incident Management

Accountability Artifacts

Social & Regulatory Norms
SLA, PLA, contracts
Policies (machine readable)
Metrics
Machine-generated Logs
Evidence Records
Certificates and Assessments
Audit Reports
Notification Reports
Claims
Insurance

Accountability Processes

Provide Account
Perform External Verification
Remedy and Redress
Handle Exceptions
Responsiveness to Stakeholder
Operate & Monitor System
Offerings & Contracts
Select & Manage Sub-providers
Identify & Implement Controls
Assess Risks and Impact
Staff Commitment
Identify & Accept Responsibility

Staff Commitment
Identify & Implement Controls
Assess Risks and Impact
Staff Commitment
Identify & Accept Responsibility
This project is partly funded from the European Commission’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

Reference Architecture Details

- Architecture Descriptions
- Policies (A-PPL)
- Evidence framework
- Account practices

- Control framework
- Best practice processes
- Maturity Model (AMM)
- A4Cloud toolkit

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

Reference Architecture Details

- Architecture Descriptions
- Policies (A-PPL)
- Evidence framework
- Account practices

- Control framework
- Best practice processes
- Maturity Model (AMM)
- A4Cloud toolkit

www.a4cloud.eu/content/cloud-accountability-reference-architecture
In Conclusion

- Accountability is a hard problem
- Accountability across the Cloud provisioning chain is even harder

- How do you eat an elephant? ... bit by bit!
- Our research segments the accountability problem space into addressable chunks

- It will take time ... but it will happen
- Just as it took time for widespread compliance to ISO 27001
Thank you

Siani Pearson
Principal Research Scientist – Hewlett Packard Labs
siani.pearson@hpe.com
This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

Introducing Accountability into NIST Cloud Architecture
Integrating Accountability into Standards

Selective contributions in the areas of:

- SLAs
- Assessment & Certification
- Risk Management
- Privacy Impact Assessments (PIA)

Contributions to

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

<table>
<thead>
<tr>
<th>Accountability Support Service</th>
<th>Brief description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy definition and validation</strong></td>
<td>Systems that enable and facilitate the definition and configuration of policies and validate that policy terms have been extracted properly from higher-level, human-readable documents such as SLAs, PLAs and contracts.</td>
</tr>
<tr>
<td><strong>Policy management &amp; enforcement</strong></td>
<td>Enforcement covers systems that ensure operations (such as handling of data) are performed exclusively according to defined policies. Management covers systems that support the lifecycle of policies themselves, such as versioning, editing, testing, updating and deleting.</td>
</tr>
<tr>
<td><strong>Monitoring &amp; environment state collection</strong></td>
<td>Systems that monitor, collect and store information on the state and operation of the various systems and components that comprise a particular cloud service.</td>
</tr>
<tr>
<td><strong>Collection &amp; management of evidence</strong></td>
<td>Systems that collect and compile evidence records about the state and operation of designated elements of a cloud service, and manage their full lifecycle according to specific integrity, confidentiality and access control requirements.</td>
</tr>
<tr>
<td><strong>Incident management</strong></td>
<td>A collection of systems tasked with supporting and coordinating the incident management process.</td>
</tr>
<tr>
<td><strong>Notification</strong></td>
<td>Systems that enable the formation, population and transmission of notification reports to authorised parties.</td>
</tr>
<tr>
<td><strong>Remediation</strong></td>
<td>Systems that assist in compiling and communicating remediation options to affected parties.</td>
</tr>
<tr>
<td><strong>Validation</strong></td>
<td>Systems that validate the extent of the ability of the systems (and their configurations) in place to support accountability assertions.</td>
</tr>
</tbody>
</table>
# Accountability Processes

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

1. Accept responsibility
2. Staff commitment
3. Assess risk & impact
4. Identify & implement controls (inc. policies)
5. Select & manage sub-providers
6. Offering & contracts
7. Responsiveness to stakeholders
8. Monitor practices
9. Perform validation
10. Account: Notification
11. Remedy & redress
12a. Account: Demonstrate appropriateness
12b. Handle exceptions
12c. Demonstrate effectiveness

Account: Notification

Responsiveness to stakeholders

Monitor practices
Privacy for organisations

– At the broadest level, privacy is:
  • The right to be let alone

– In the commercial/consumer context:
  • Protection and careful use of the personal data of customers and employees
  • Meeting the expectations of customers about the use of their personal data

– For corporations, privacy is about:
  • The application of laws, policies, standards and processes by which the personal data of individuals is managed
“Privacy encompasses the rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention of personally identifiable information.”

The American Institute of Certified Public Accountants (AICPA)