



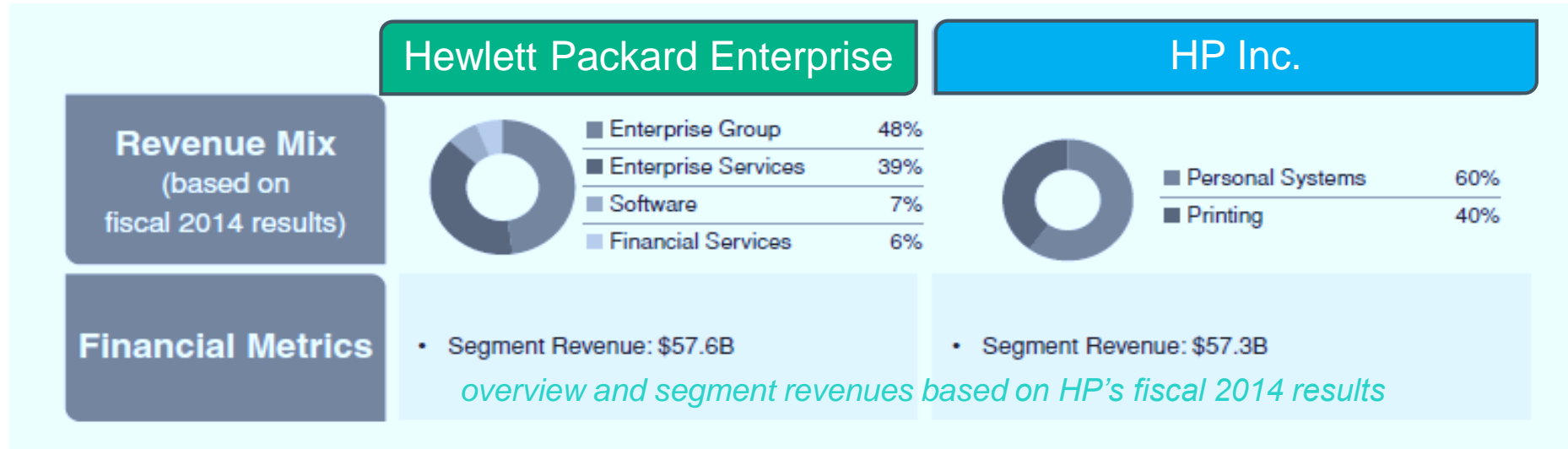
**Hewlett Packard
Enterprise**

Accountability in the Cloud

Dr. Siani Pearson
Principal Research Scientist
Hewlett Packard Labs EMEA

ITU Kaleidoscope – December 10th, 2015

Hewlett-Packard Corporation split



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



Hewlett Packard Enterprise:

- Enterprise technology infrastructure, Software, Services and Financing businesses,



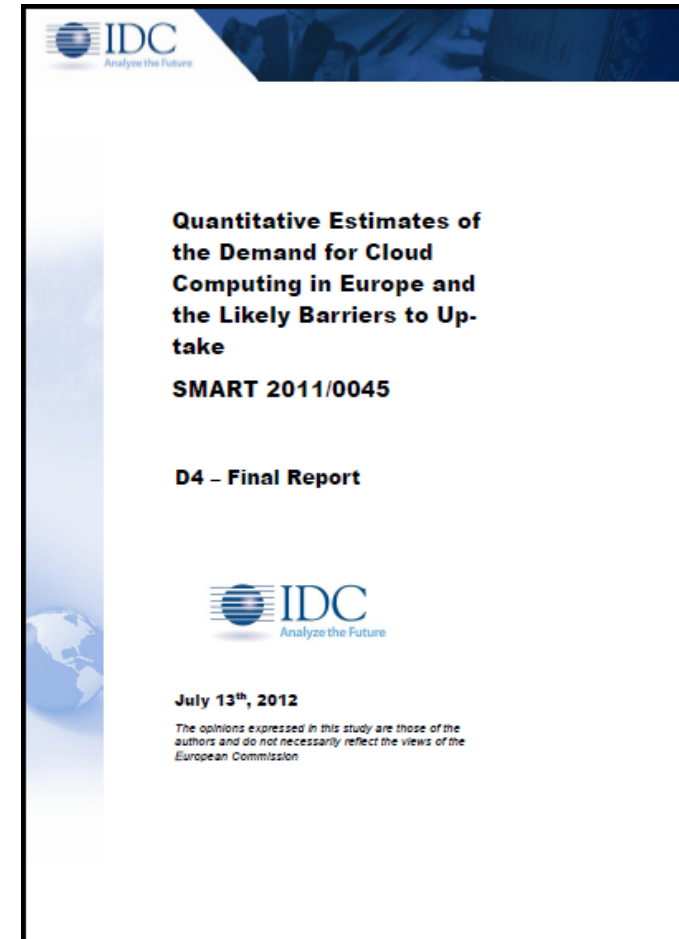
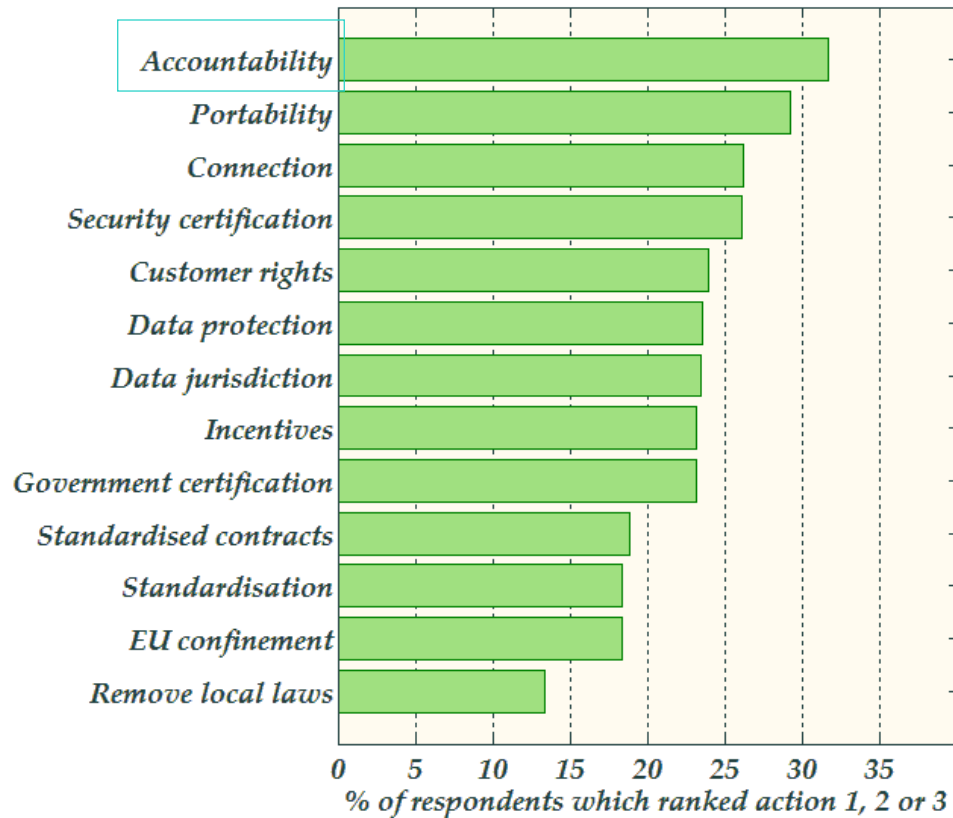
HP Inc:

- 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.



Key Data Protection Terminology

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)

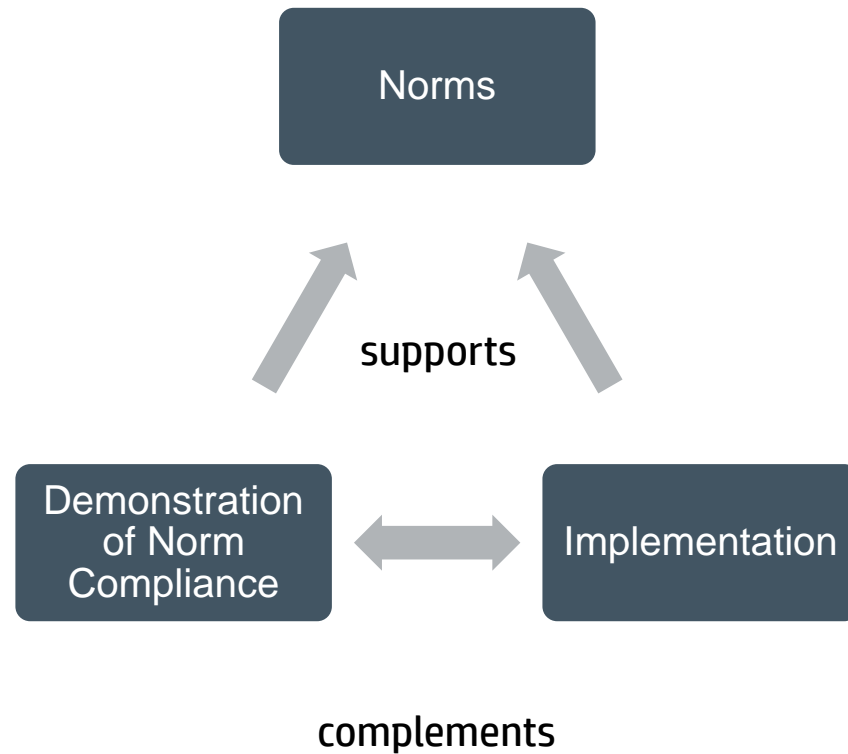
- The entity responsible in each EU country for the enforcement and monitoring of compliance with data protection legislation

OECD Privacy Principles form the Basis for most Data Protection and Privacy Laws

Collection limitation	Data quality	Purpose specification
Use limitation		Security
Openness	Individual participation	Accountability

OECD - Organization for Economic Cooperation and Development

Context



- 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

Steering accountable
behaviour *ex ante*

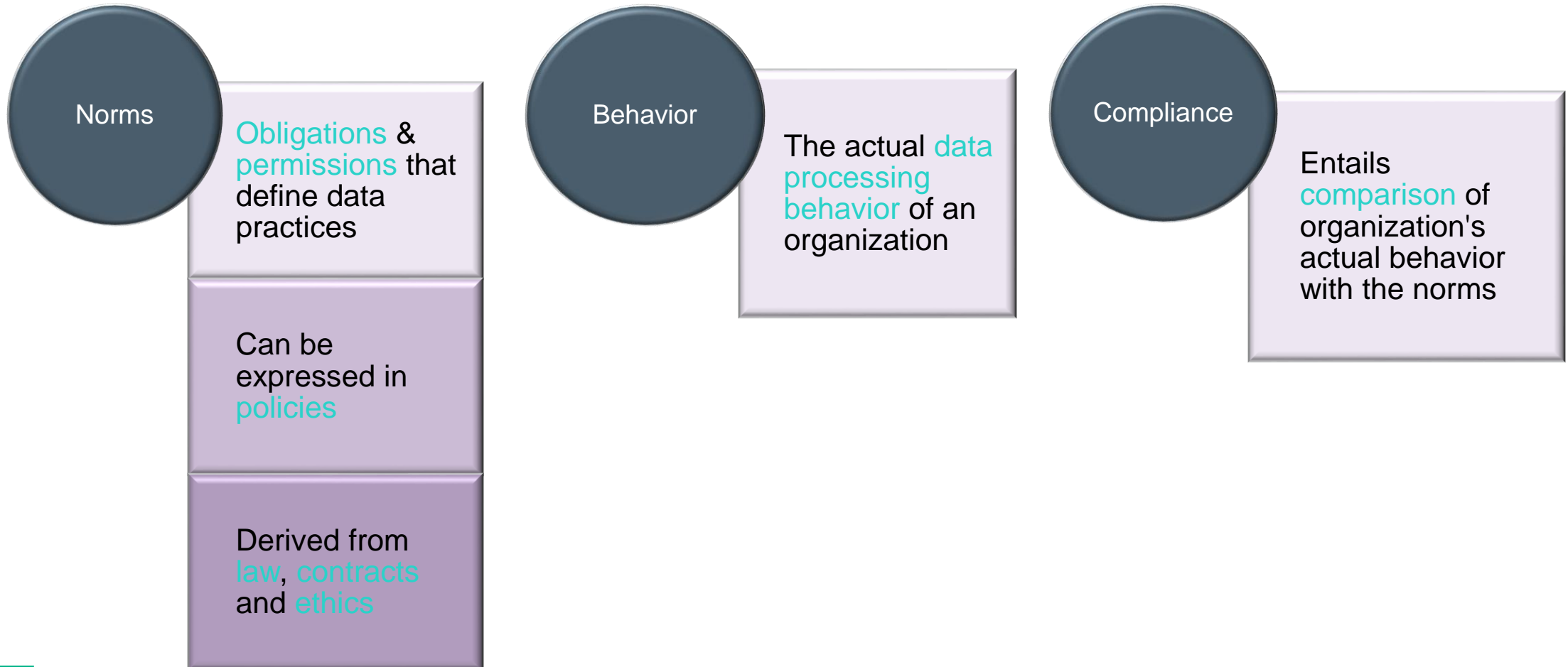
Accountability as a mechanism

- Institutional relation in which an actor can be held to account by a forum

Giving account *ex post facto*

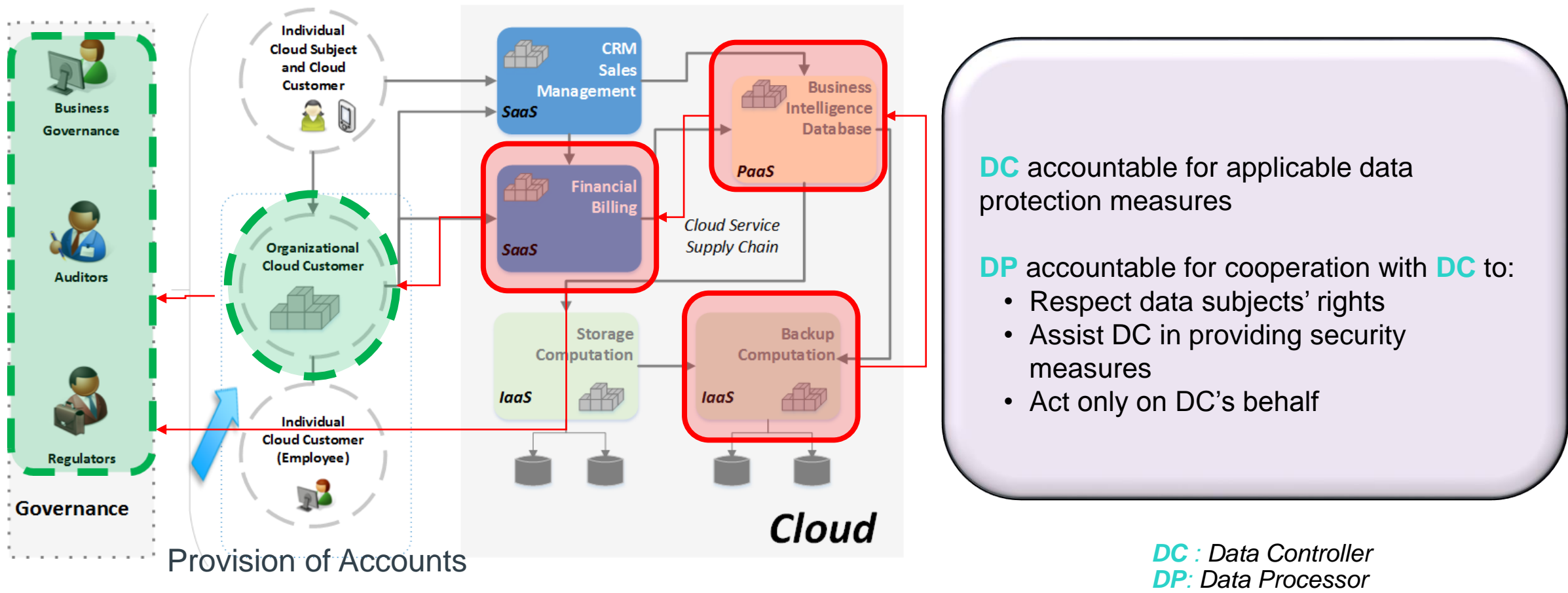
Accountability Relationships

Accountor is accountable to *Accountee* for:



Example

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



From concept to practice:

A4Cloud project



CLOUD
ACCOUNTABILITY
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



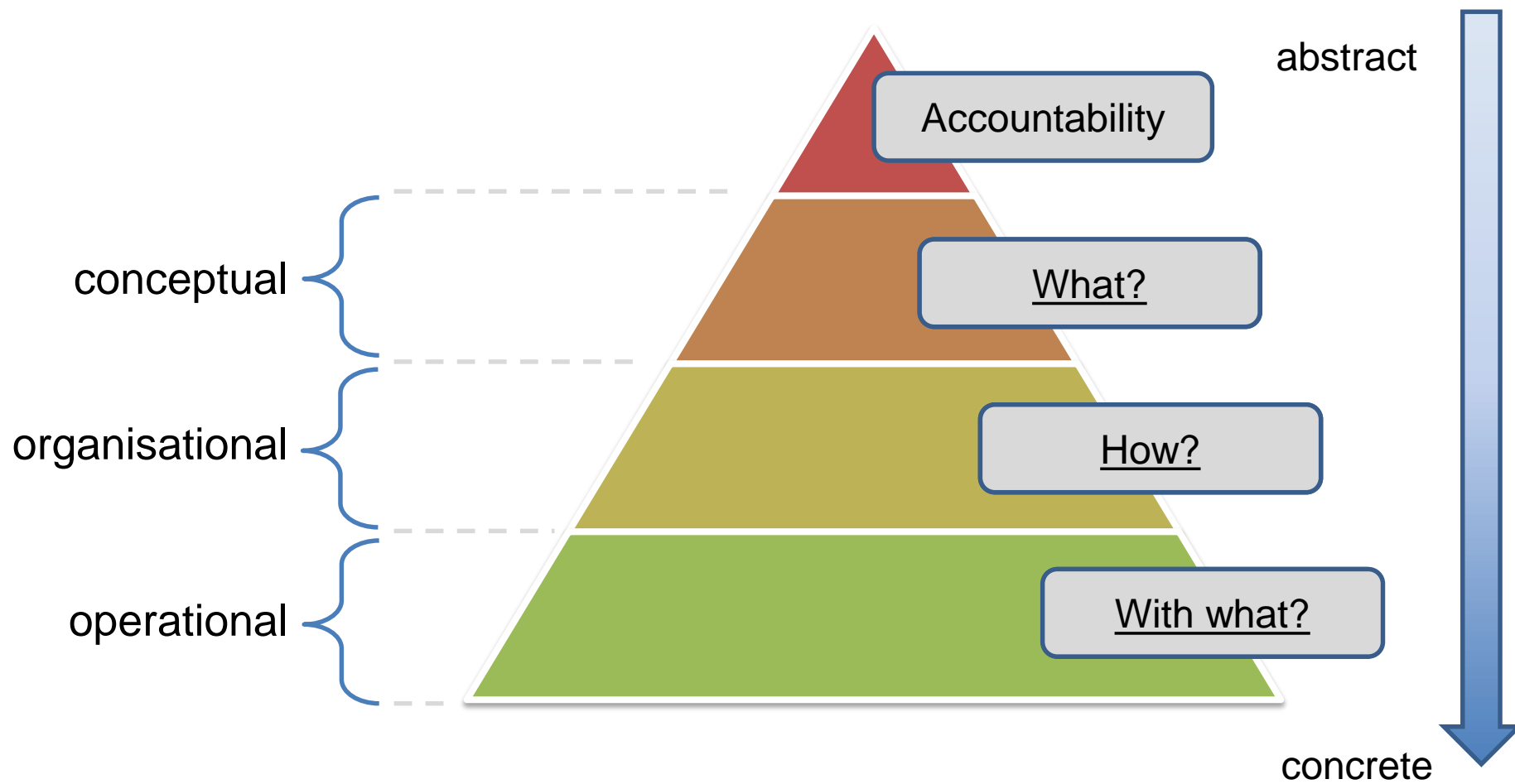
Community



Research

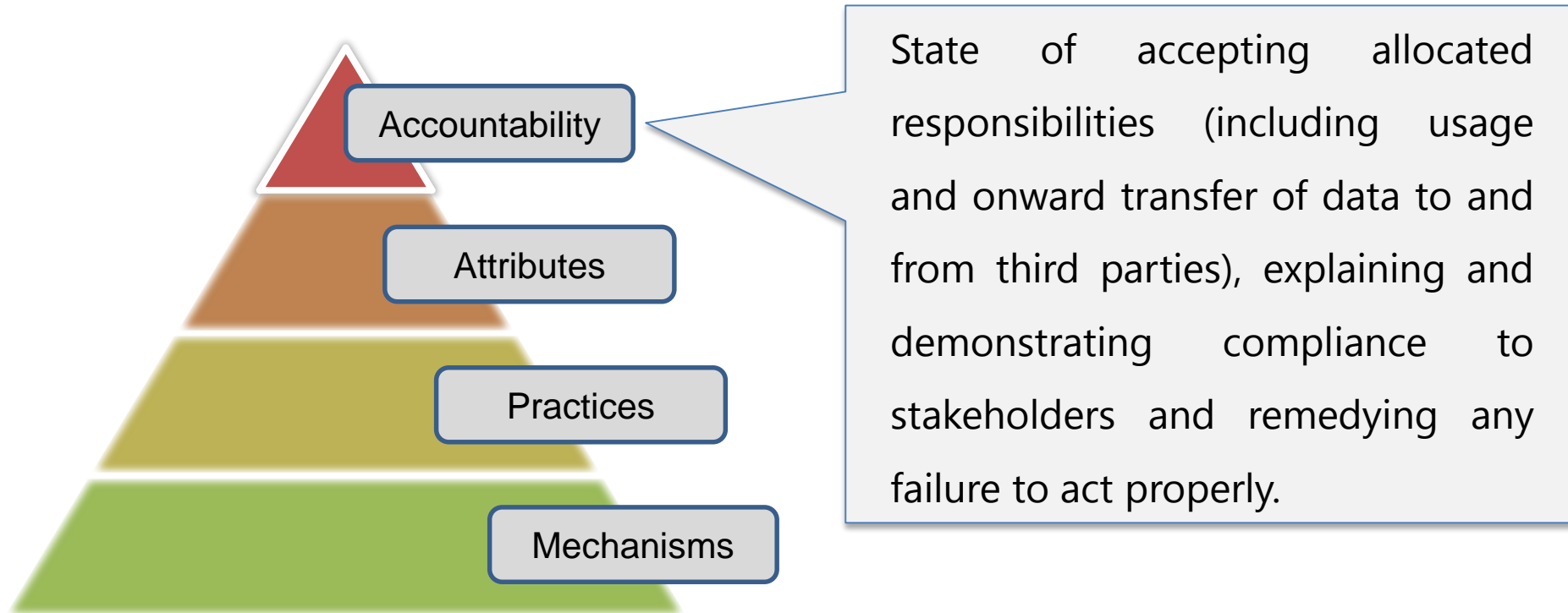


Conceptual Model of Accountability





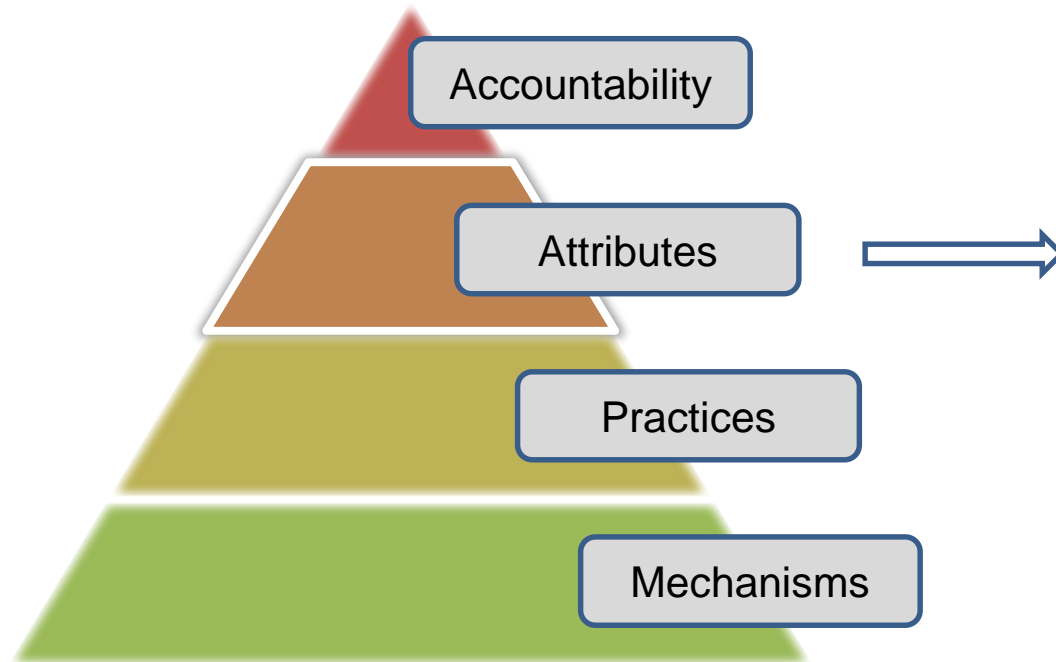
Defining Accountability



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



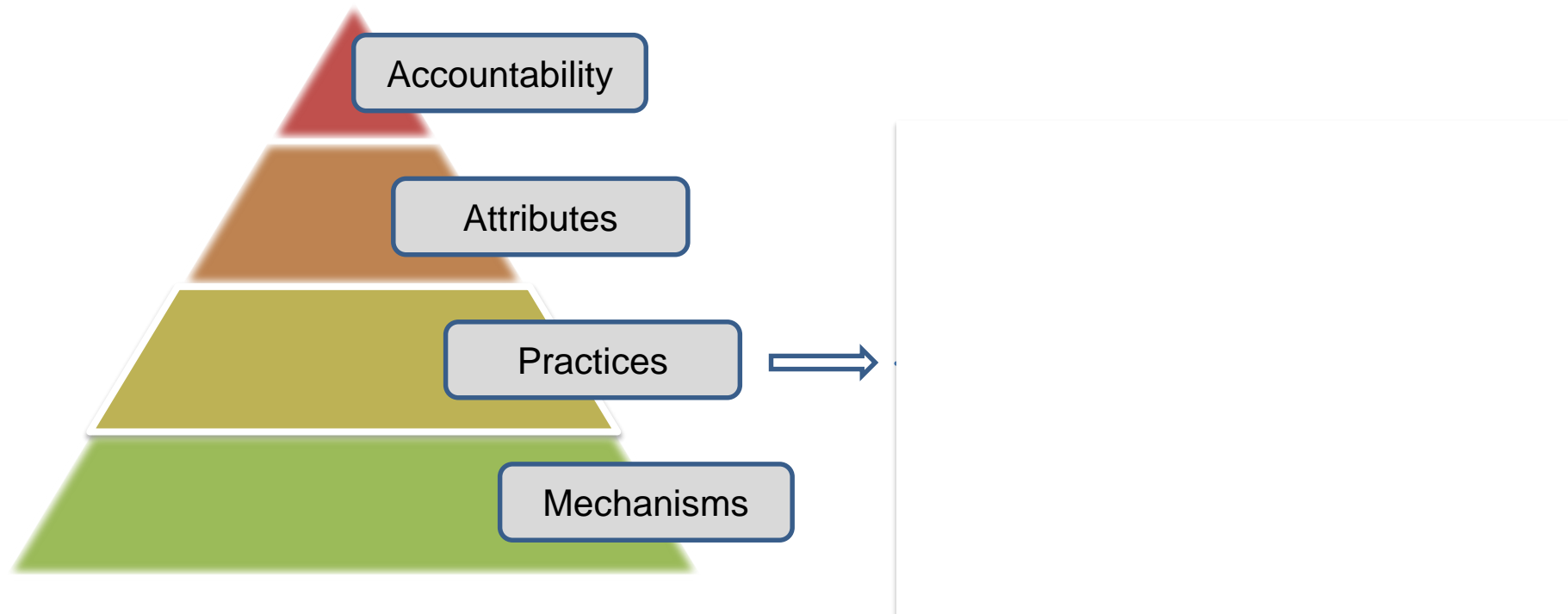
Accountability Attributes



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



Accountability Practices





How can Organisations be Accountable?

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



Embrace responsibilities

Define policies reflecting contextual norms

Enforce policies

Monitor practices

Correct violations

Demonstrate compliance

1

2

3

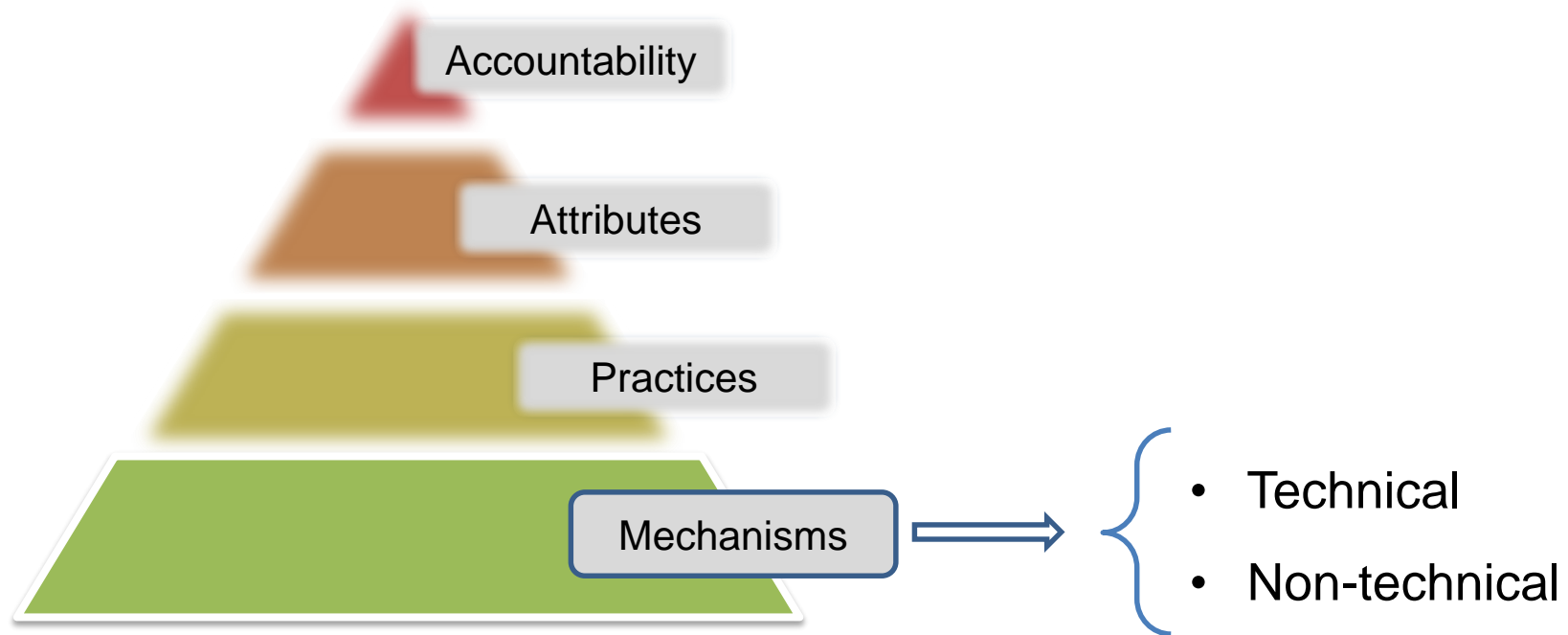
4

5

6

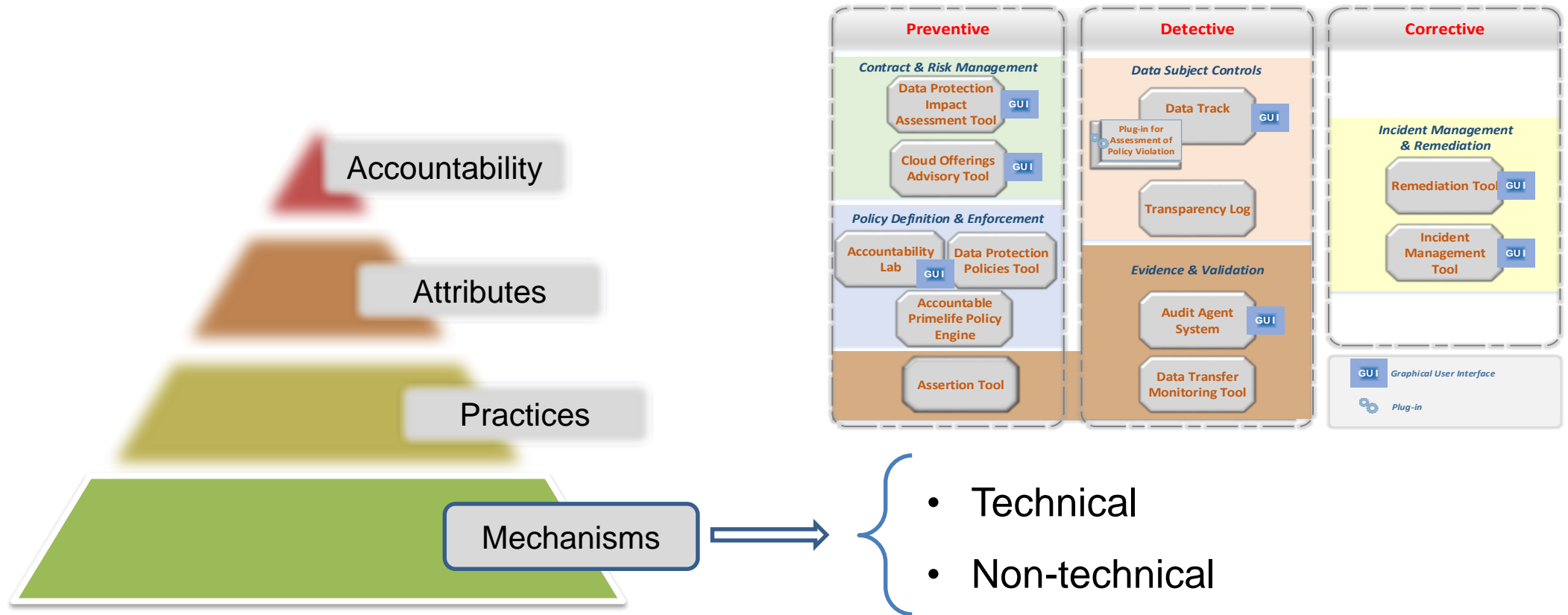


Accountability Mechanisms



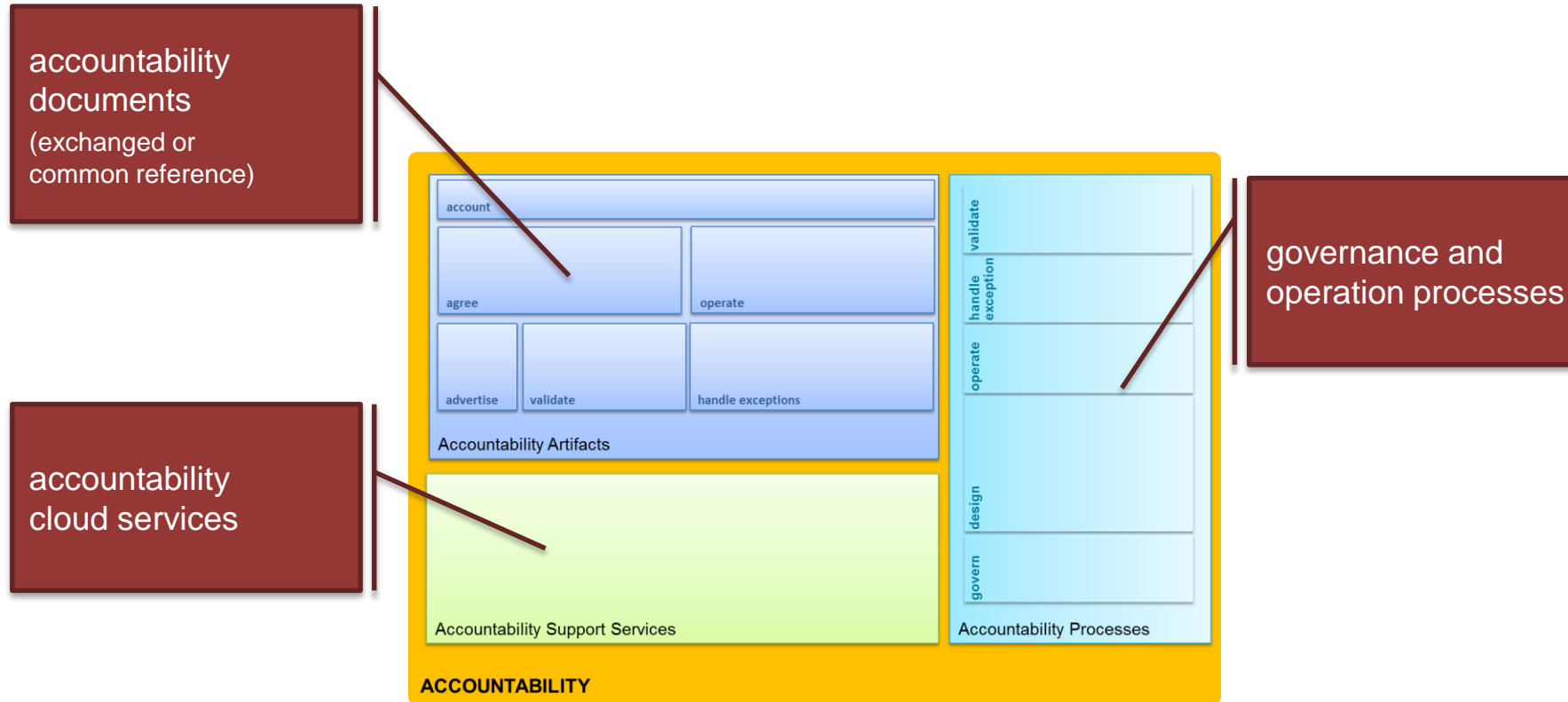


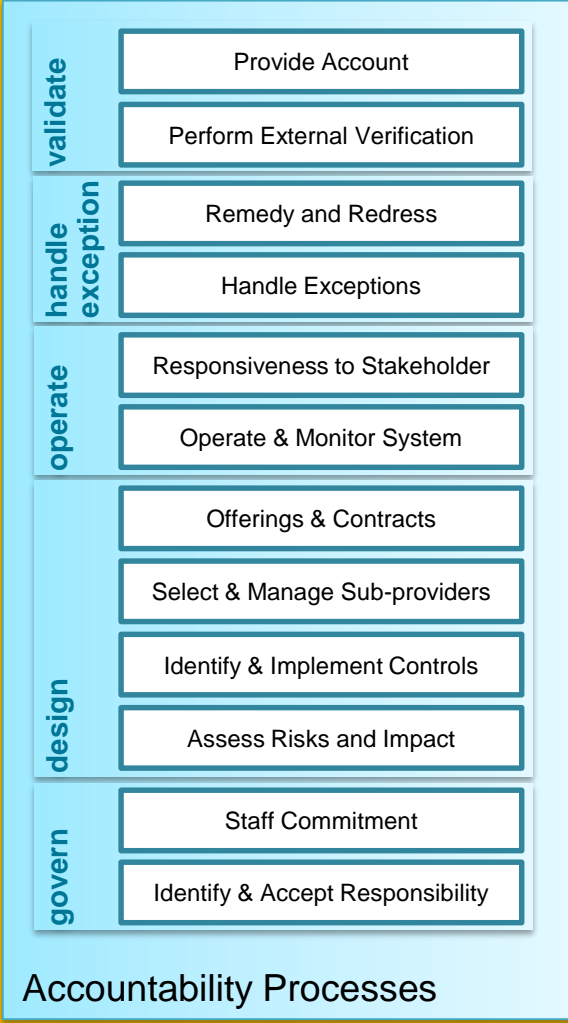
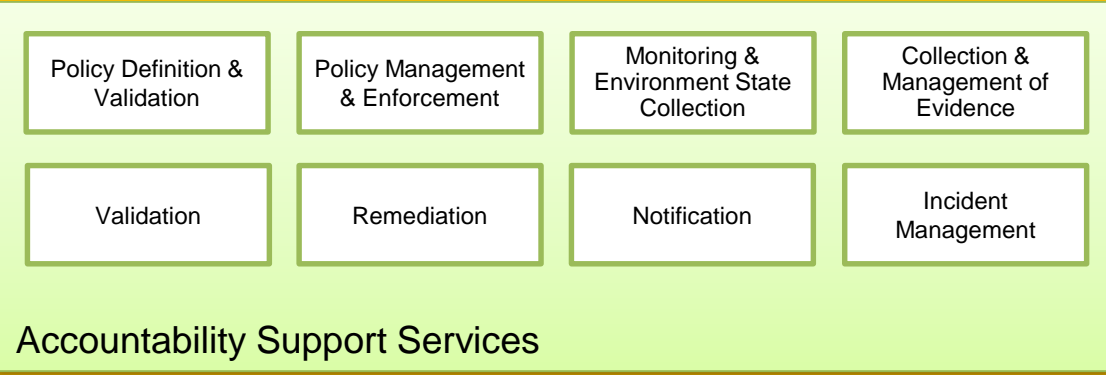
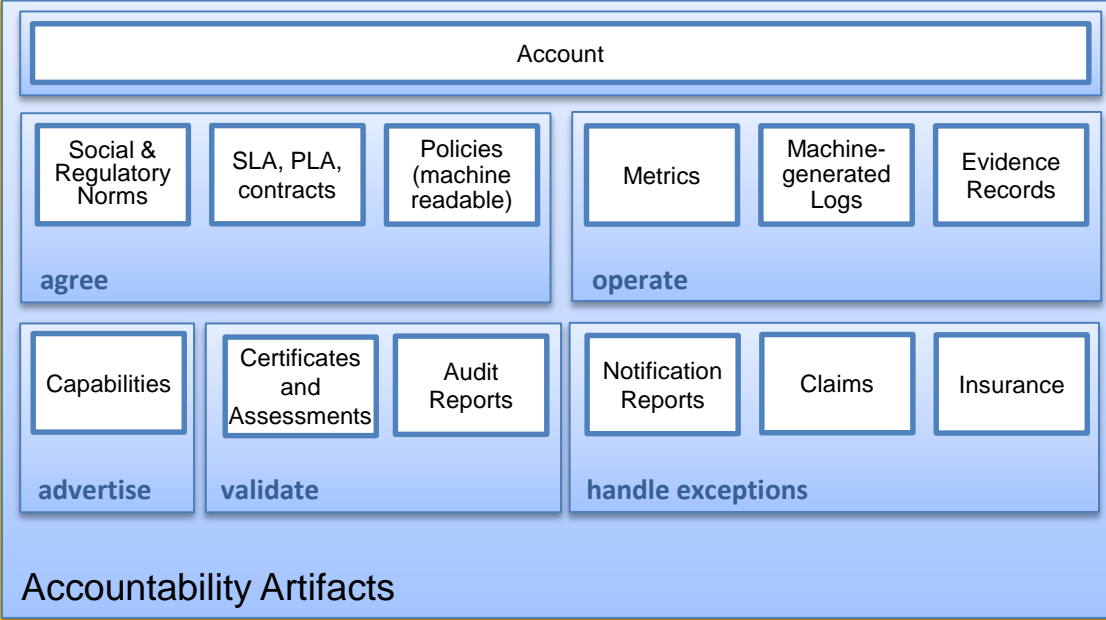
Accountability Mechanisms





Reference Architecture Framework

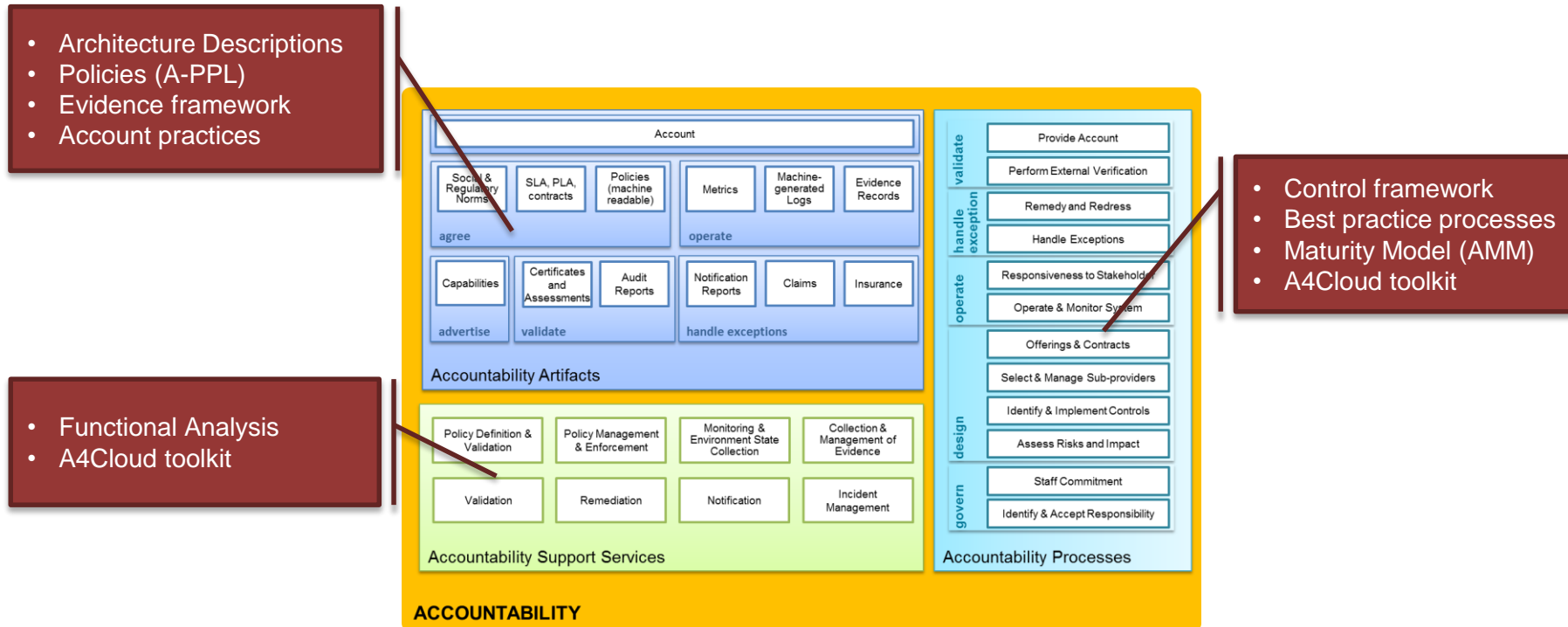




ACCOUNTABILITY

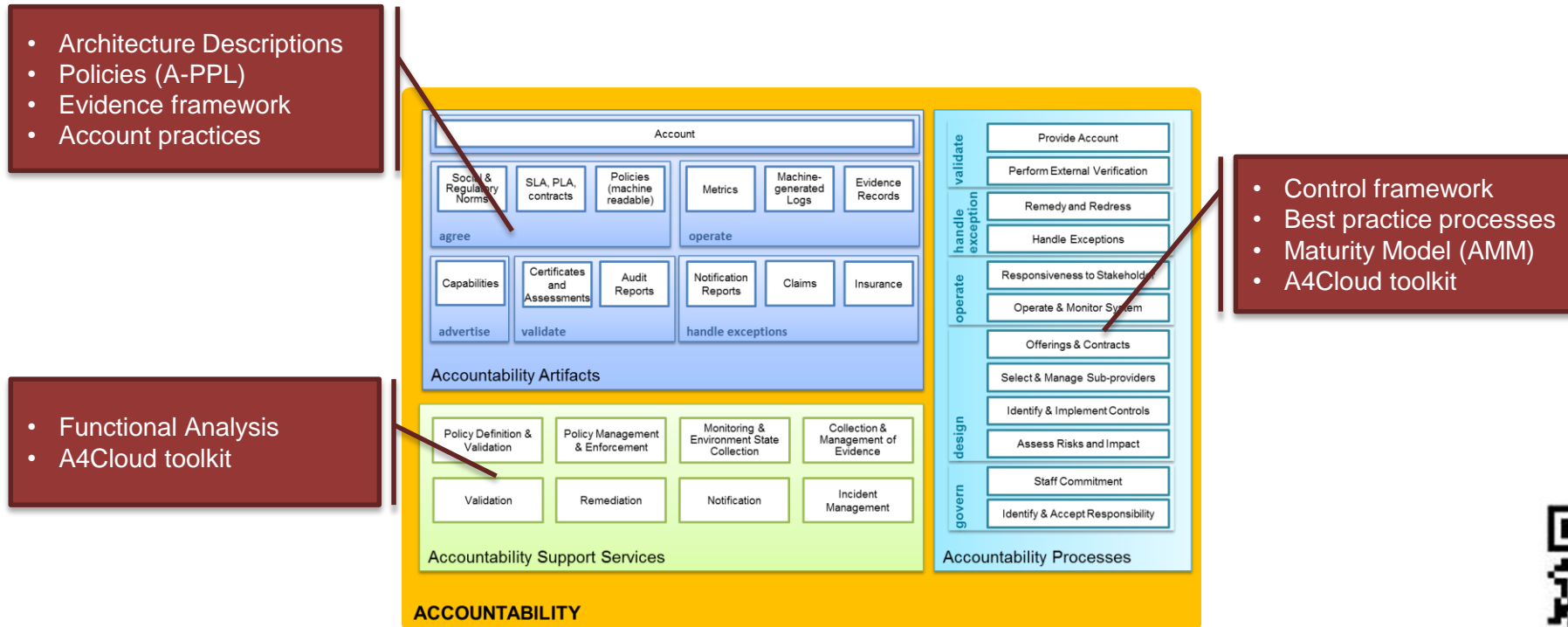


Reference Architecture Details





Reference Architecture Details



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

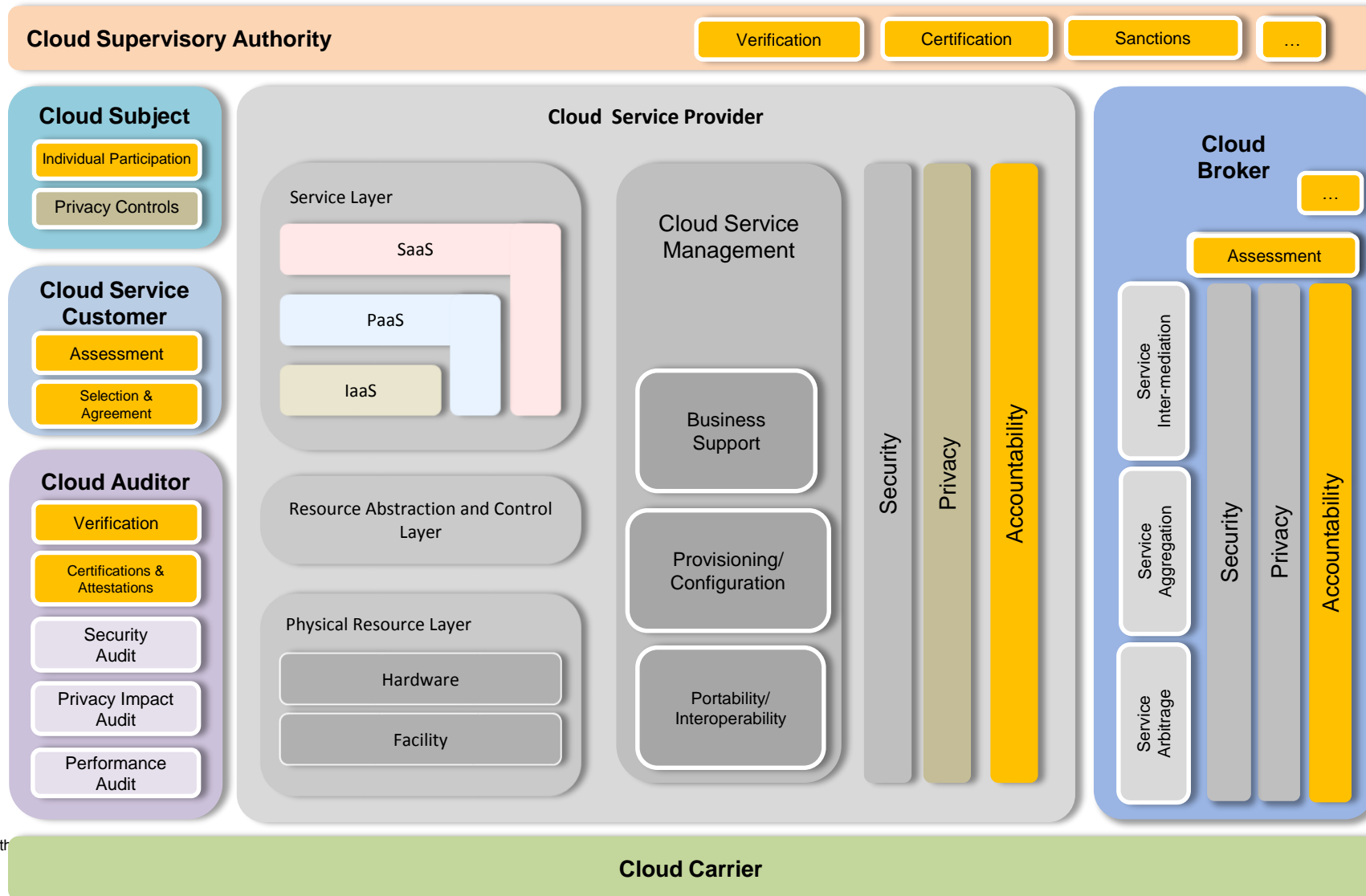
siani.pearson@hpe.com

© 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.





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)**

Accountability Artifacts

Accountability Artifact	Brief description
Capabilities	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.
Social & regulatory norms	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.
SLA, PLA, Contract	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 to binding legal obligations.
Machine-readable policy	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.
Metrics	Measurements of various service-specific objective and subjective performance characteristics over defined periods of time.
Machine-generated logs	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.
Evidence record	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.
Notification report	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.
Claims	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.
Insurance	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.
Assessments and Certificates	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])
Audit report	Document which contains evidence records and related objects (i.e. logs, policies) obtained and compiled using a specific methodology to demonstrate compliance.
Account	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.

Accountability Support Services

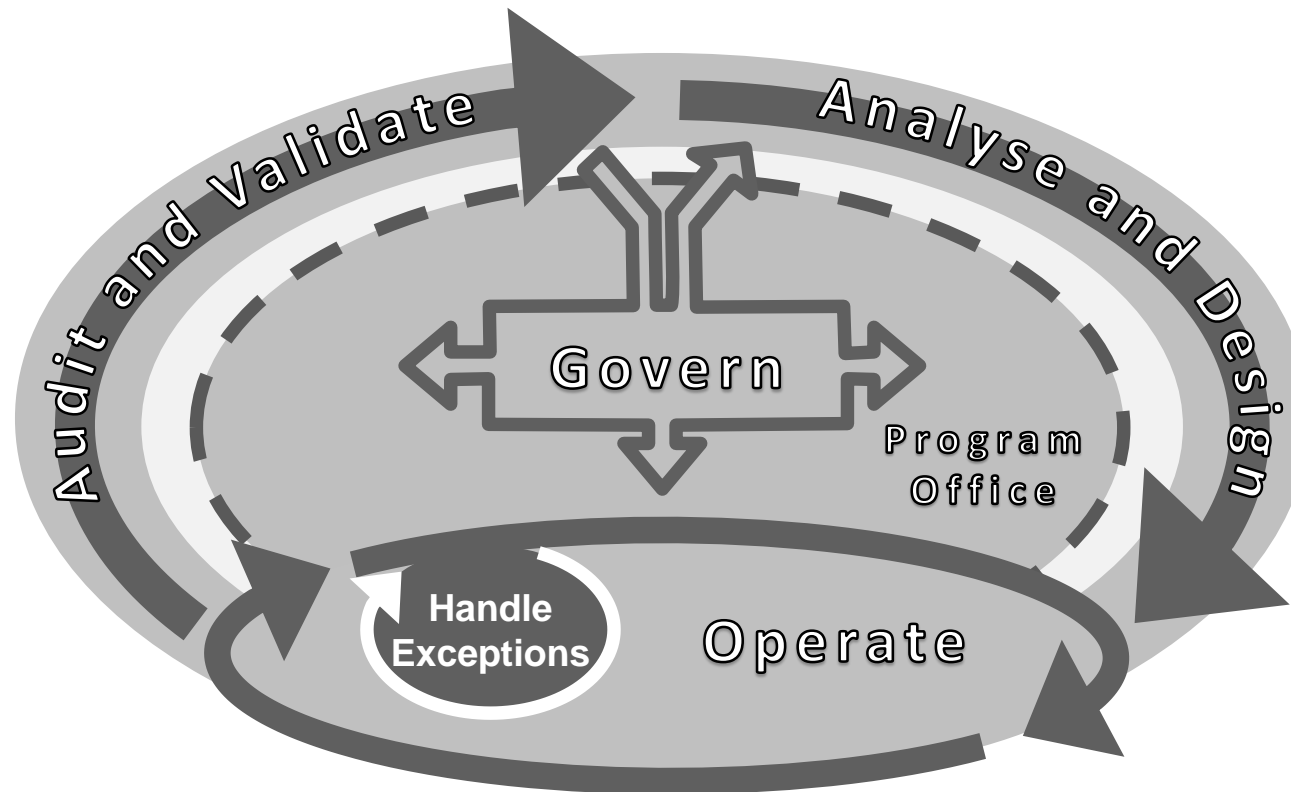
Accountability Support Service	Brief description
Policy definition and validation	Systems that enable and facilitate the definition and configuration of policies and validate that policy terms have been extracted properly from higher-level, human-readable documents such as SLAs, PLAs and contracts.
Policy management & enforcement	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.
Monitoring & environment state collection	Systems that monitor, collect and store information on the state and operation of the various systems and components that comprise a particular cloud service.
Collection & management of evidence	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.
Incident management	A collection of systems tasked with supporting and coordinating the incident management process.
Notification	Systems that enable the formation, population and transmission of notification reports to authorised parties.
Remediation	Systems that assist in compiling and communicating remediation options to affected parties.
Validation	Systems that validate the extent of the ability of the systems (and their configurations) in place to support accountability assertions.

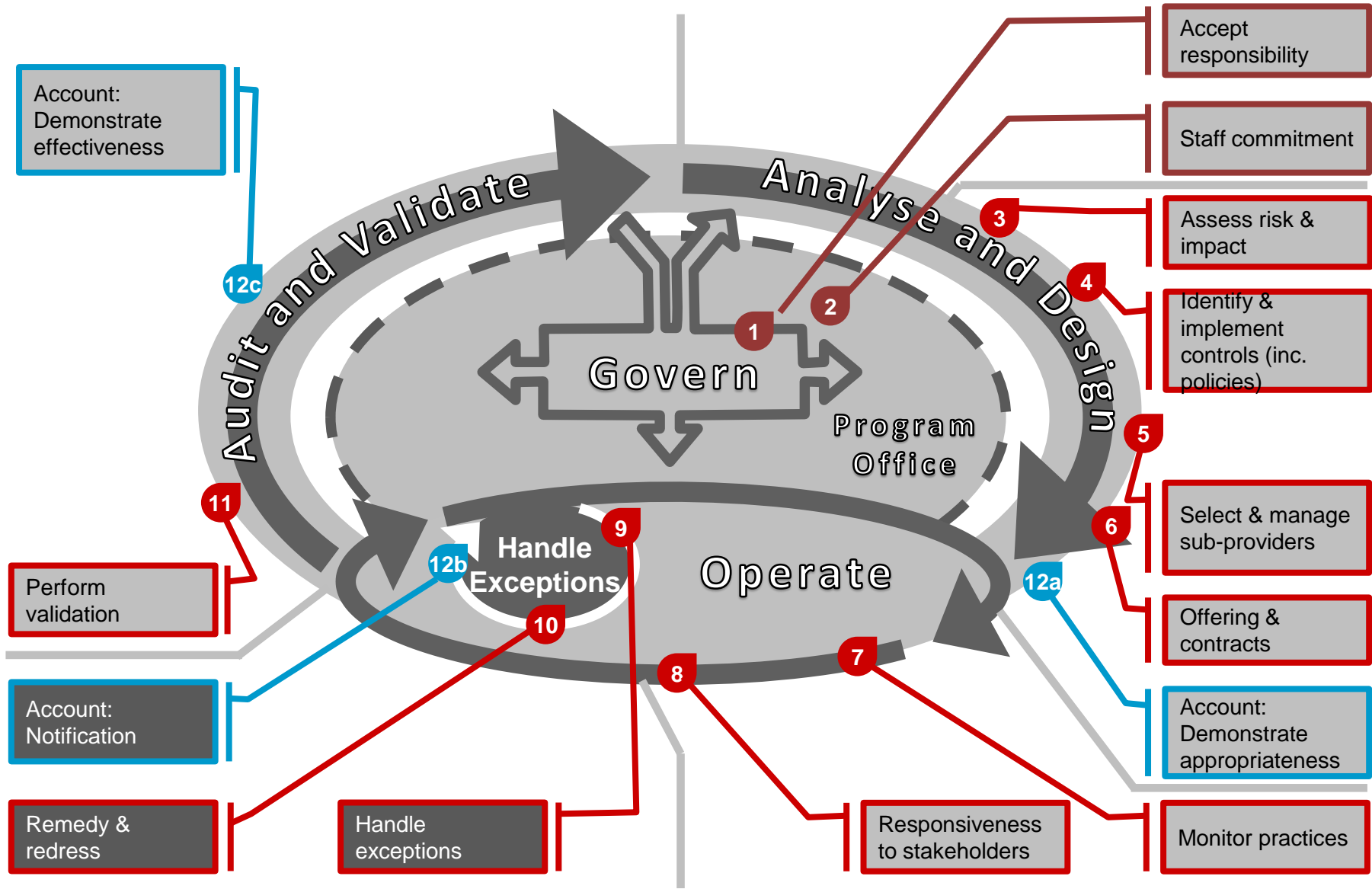
Accountability Processes

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



Accountability Lifecycle





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)