Accountability for Cloud and other Future Internet Services

The A4Cloud project

Who we are

Cloud Accountability Project

Industry Partners

Cloud Community & Standardisation

SAP

ATC — Athens Technology Center

CSA cloud security alliance℠

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

uma UNIVERSIDAD DE MÁLAGA

R&D in technical, legal and socio-economic aspects of Accountability

Collaborative Project under Call 8 of the 7th Framework Programme of the European Commission
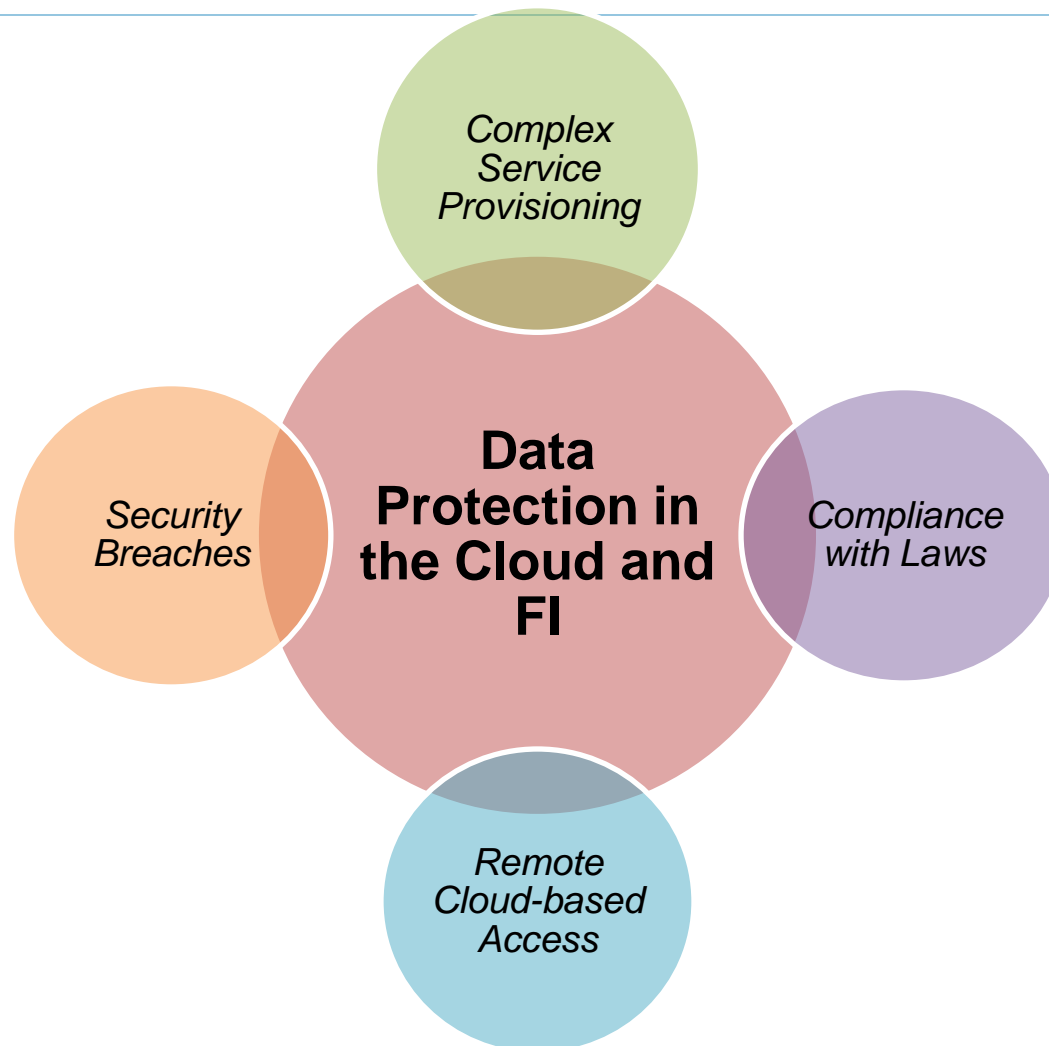
- DG.CONNECT – Unit H4: Trust & Security

Project Start Date: 1st October, 2012

Project Duration: 42 months

Stay tuned - www.a4cloud.eu

CLOUD
ACCOUNTABILITY
PROJECT

Complex Service Provisioning

Security Breaches

Data Protection in the Cloud and FI

Compliance with Laws

Remote Cloud-based Access

Increase trust and assurance

Allow more dynamism

Decrease regulatory complexity

Provide effective data governance and control in cloud-based IT

Accountability-based approaches for trust and security

Accountability consists of explaining one's actions, justifying those actions and remedying any failure to act properly

Accountability concerns data stewardship regimes in which organizations that are entrusted with personal and confidential data are responsible and liable 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).
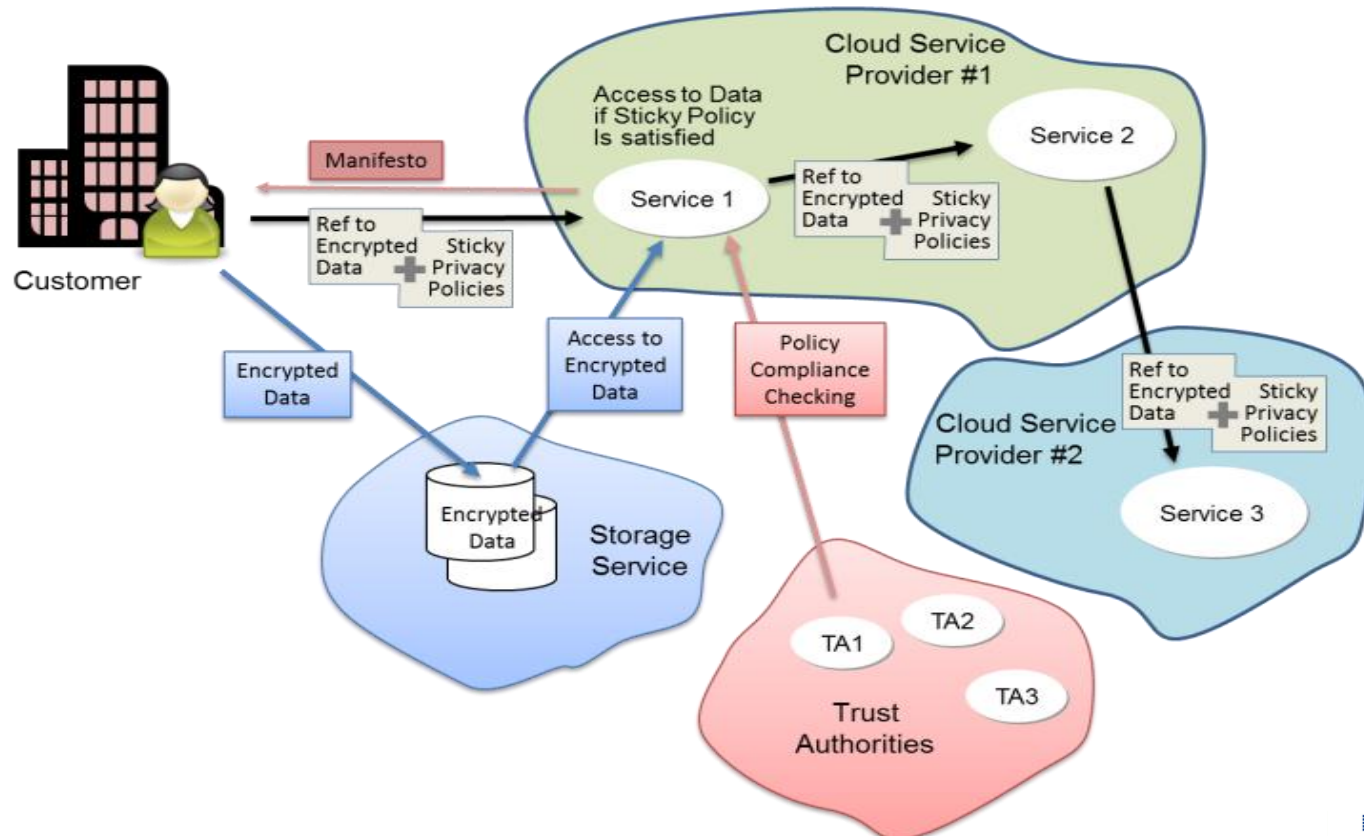
Inter-disciplinary approach for co-designing Accountability
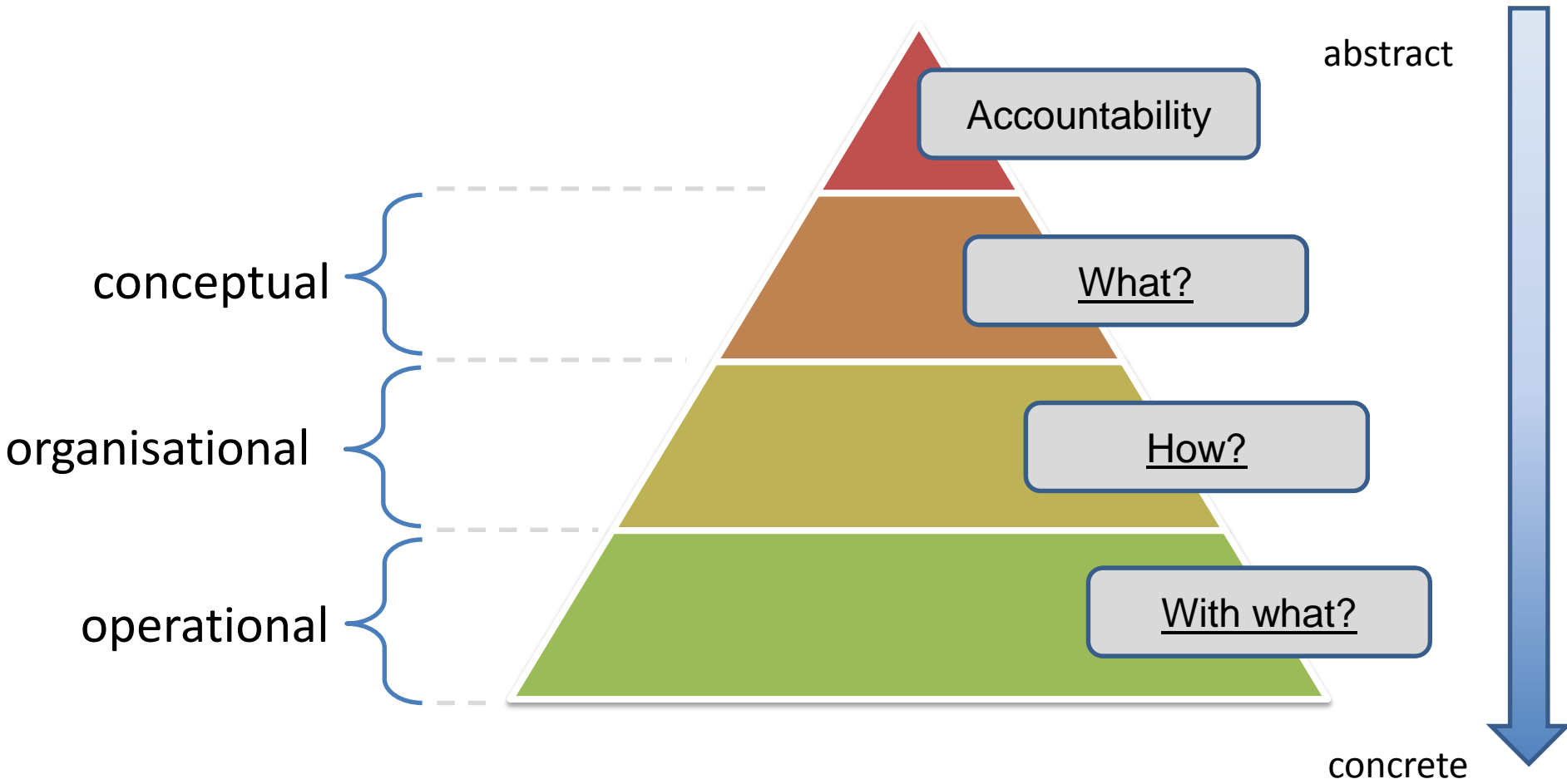
The example of sticky policies

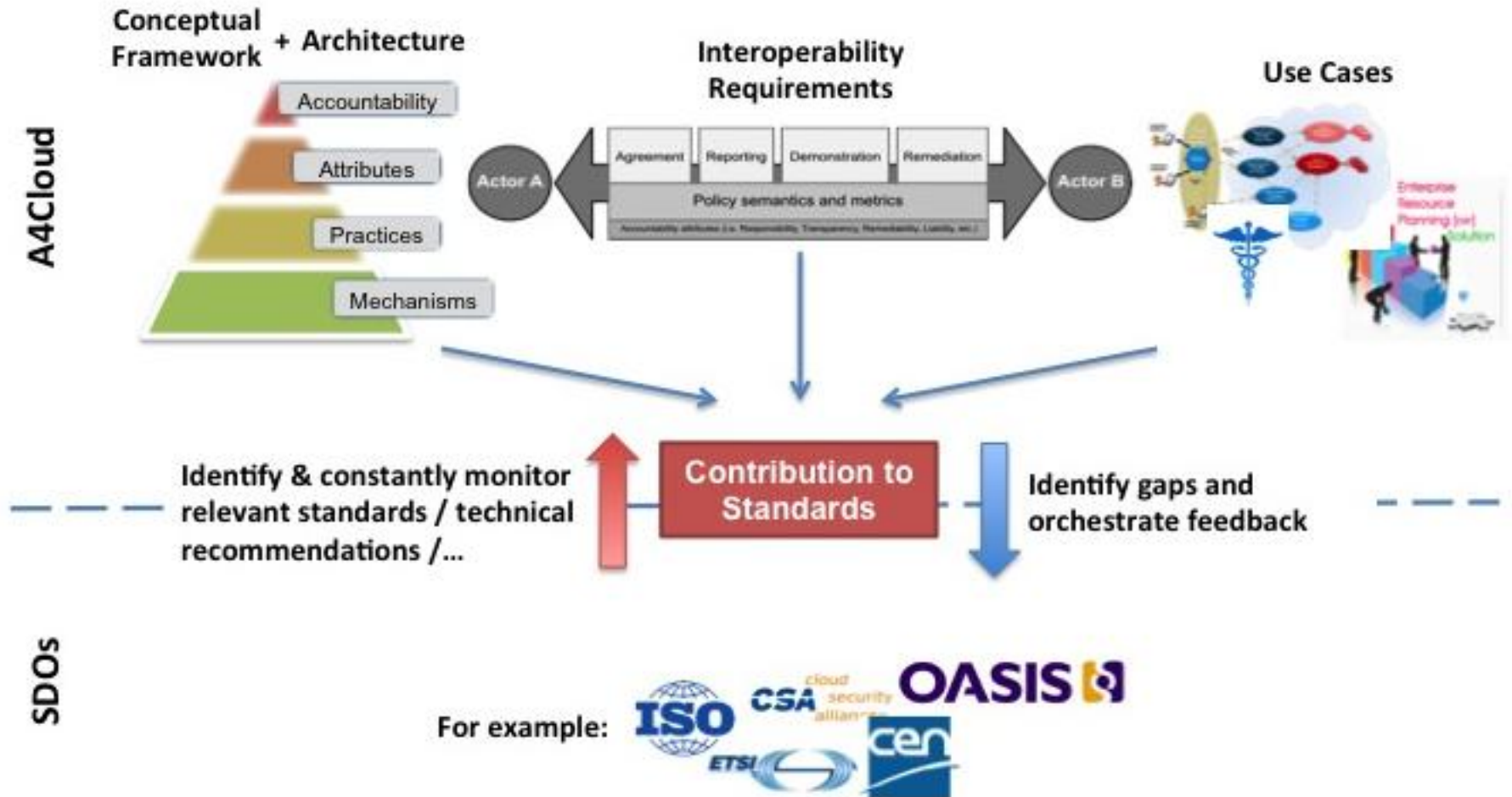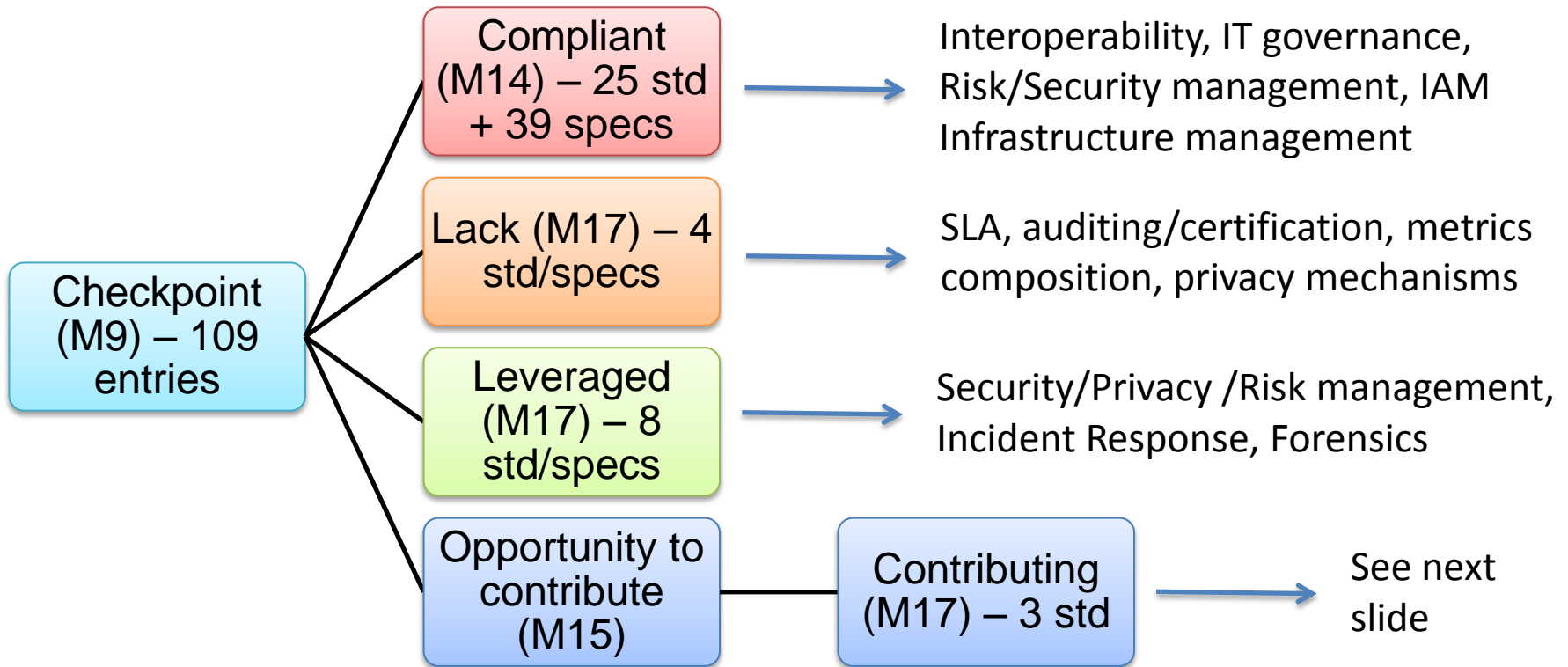| Tool	Purpose
Accountability and Privacy Enforcement Tool	Enable enforcement of policies in ways that can be verified and audited
Audit Agent System	Enables customers of cloud services to perform audits of their cloud infrastructures
Cloud Control Tool (CCT)	The declarative definition of implementation techniques and tools for the addition of new functionalities to existing Cloud applications and infrastructures
Data Protection Impact Assessment Tool	Selecting service providers by assessing the impact of a particular choice before sensitive information is transferred or shared
Data Track	Enabling data subjects to exercise their rights online to access, correct and request removal of their data at data controllers
Data Transfer Control Tool	Accountable data localization and transfer across cloud software, platform and infrastructure services, usually run by data processors
Incident Response Tool	Provides data subject access rights and to file complaints regarding the processing of personal data by the controller and/or an incident
Plug-in for assessment of policy violation	Provide an assessment on the relevance of the violation of policies, so that stakeholders receive information about the most relevant policy violations
Redress Tool	Advises end users and organisations on actions that can be taken in case of violations
Tool for Cloud Contracts	A simple expert system to help with drafting and managing custom contracts
Transparency Log	Transfer of data from CPs to CCs/CAs in a secure and privacy-friendly way

Current status: areas being covered

CLOUD ACCOUNTABILITY PROJECT

Checkpoint (M9) – 109 entries

Compliant (M14) – 25 std + 39 specs → Interoperability, IT governance, Risk/Security management, IAM Infrastructure management

Lack (M17) – 4 std/specs → SLA, auditing/certification, metrics composition, privacy mechanisms

Leveraged (M17) – 8 std/specs → Security/Privacy /Risk management, Incident Response, Forensics

Opportunity to contribute (M15) → Contributing (M17) – 3 std → See next slide

CSA Cloud Trust Protocol (CTP)
ODCA Service Orchestration
CSA Open Certification Framework
CSA Cloud Control Matrix (CCM)
CSA CAIQ
ITIL
COBIT
ISO 27001
ISO 27036
oAuth
WSLA
WS-Agreement
CIM suite of standards - e.g. CIM-SPL
CIMI (Cloud Infrastructure Management Interface)
OCCI
OpenID
SAML

OATH (not OAUTH)
ARF
X-ARF (Extensible abuse reporting format)
M-ARF (Messaging abuse reporting format)
CVE
CWE
SCAP
CSA Cloud Trust Protocol (CTP)
SUoM: ODCA Standard Units of measure
ENISA Procure Secure
CloudAudit
PKI standards (X.509, XML Digital Signature, PKCS* etc...)
TLS
PKCS*
SHA2
ECRYPT yearly report
+ Key management standards as above

CLOUD
ACCOUNTABILITY
PROJECT

Thank You.