Privacy and Accountability in the Cloud – Session 2

Siani Pearson, Security and Cloud Lab, HP Labs Bristol

September 2014

Content

Session 2: Impact on Data Protection of Technological and Business Trends

- **Cloud Computing**
  - Definitions
  - Data protection risks
  - Data protection in the cloud
- **Accountability in the Cloud**

EXERCISE: implications of adopting more open practices

Cloud Computing

A very significant shift in the IT landscape

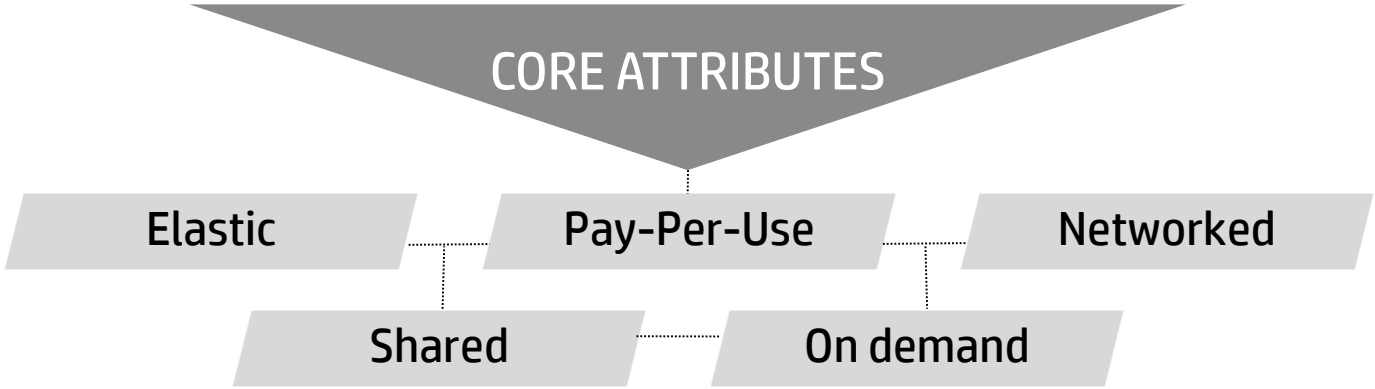
Of the same magnitude as from mainframe to client-server, to PC, to www, to web2.0 and to mobile!

"The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of these announcements. The computer industry is the only industry that is more fashion-driven than women's fashion. Maybe I'm an idiot, but I have no idea what anyone is talking about. What is it? It's complete gibberish. It's insane. When is this idiocy going to stop?"

Larry Ellison, CEO Oracle, September 2008

Cloud definition

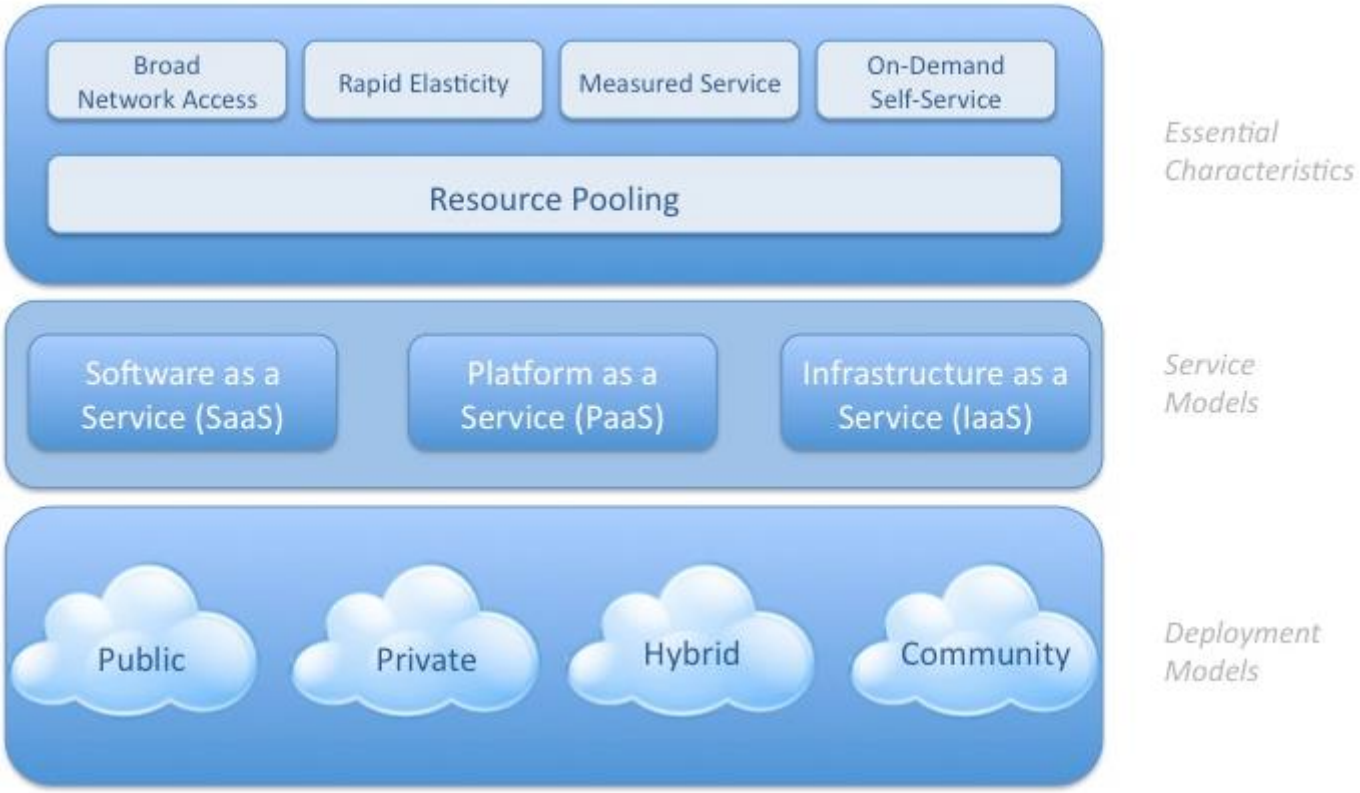
Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction



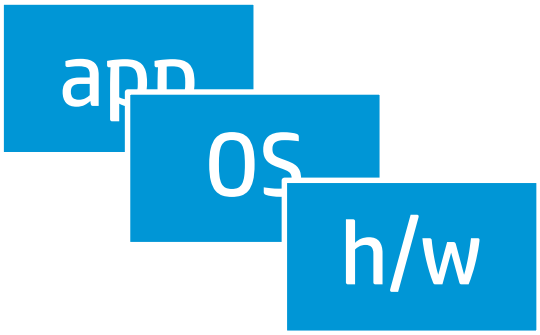
Mell, P. and Grance, T. (2009) A NIST Definition of Cloud Computing, National Institute of Standards and Technology, NIST SP 800-145, http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

Cloud computing

NIST Visual Model of Cloud Computing Definition



Service models



Transformational for all actors in the ICT value chain

- **SaaS: consumers use CSPs' applications running on a cloud infrastructure – a huge choice of apps with no IT department in the way!**
- **PaaS: consumers deploy (onto a cloud infrastructure run by a CSP) applications that have been created using programming languages and tools supported by that provider – innovative eco-systems – micro to macro scale!**
- **IaaS: consumers deploy and run software, with a CSP controlling the underlying cloud infrastructure - Capex to Opex, $$$ not required!**

Cloud deployment models

Private: a cloud infrastructure operated solely for an organisation, accessible only within a private network

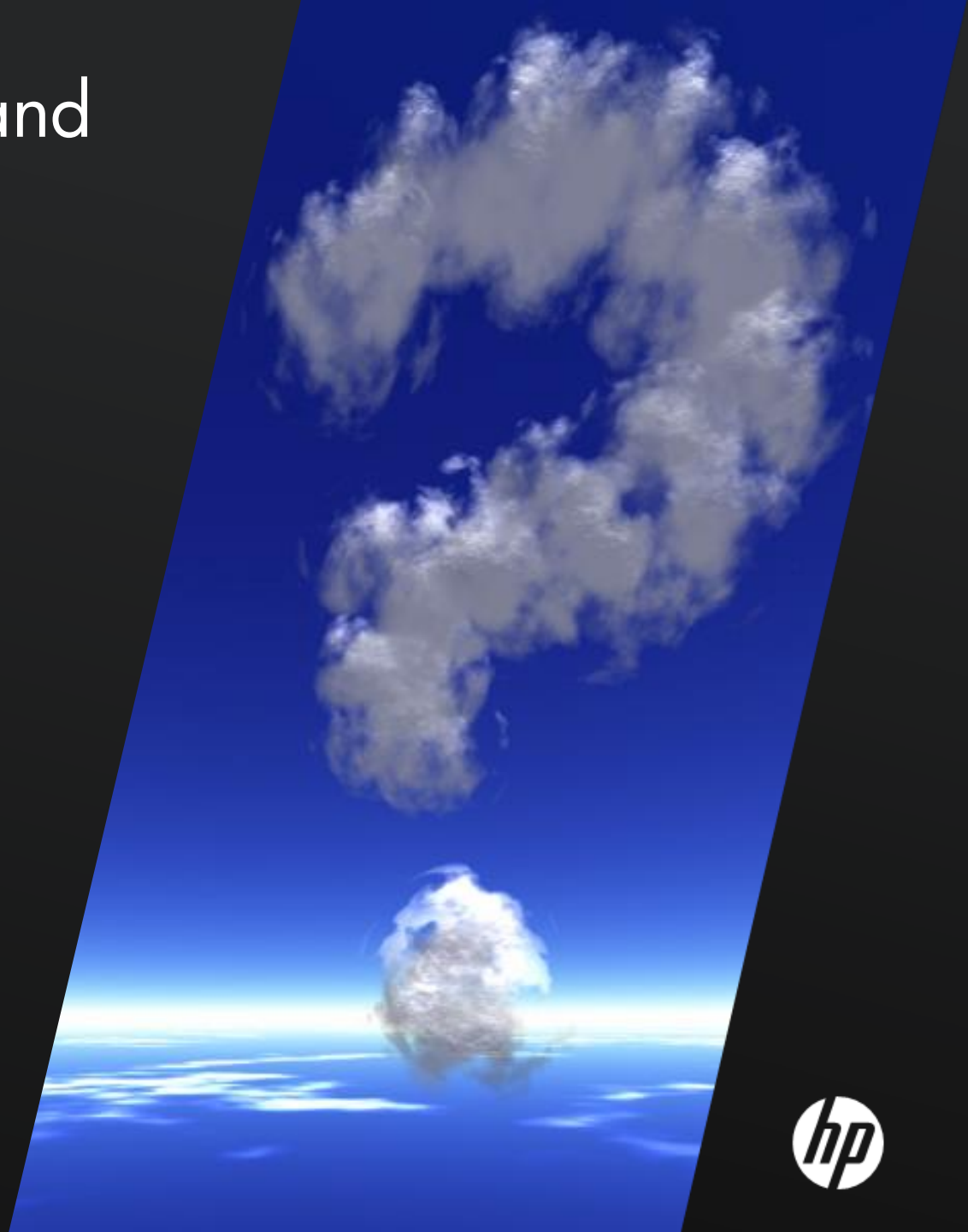
Virtual private: a private cloud existing within a shared or public cloud

Public: a widely accessible cloud infrastructure

Shared: a cloud that is open to use by selected organisations

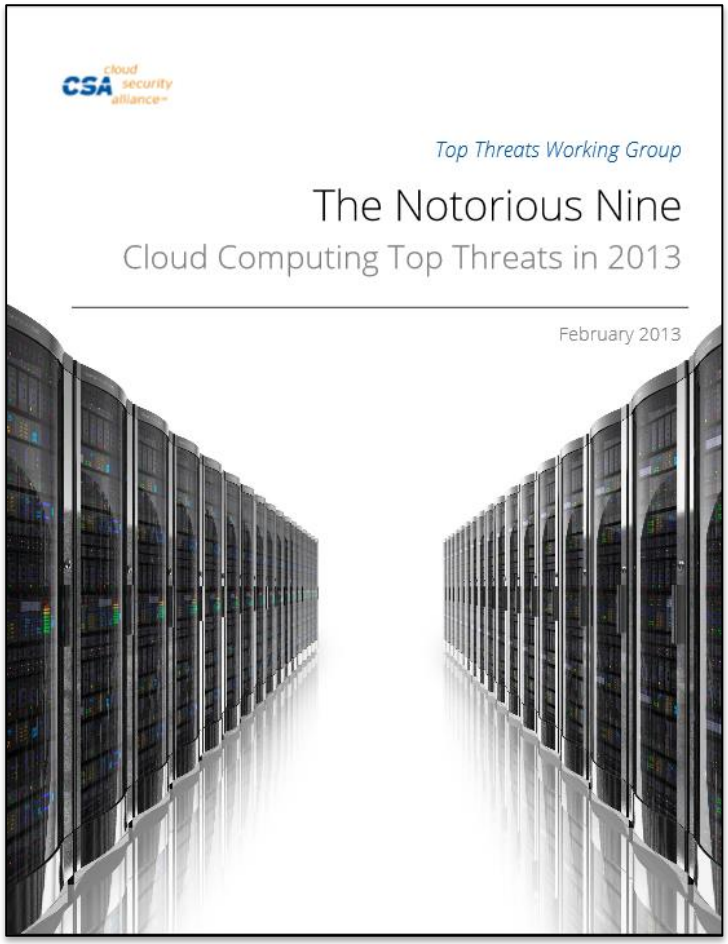
Hybrid: a composition of two or more clouds that remain separate but between which there can be data and application portability

Fear, Uncertainty and Doubt



Technological challenges

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues



Evolving risk perception – CSA top threats

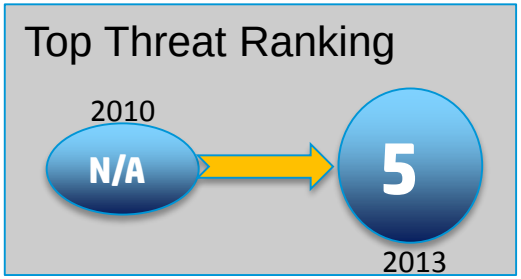
Data breaches

Data loss

Account or Service Hijacking

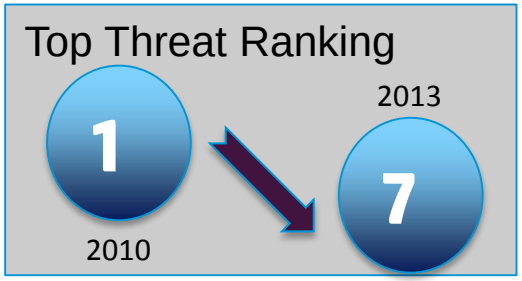
Insecure Interfaces and API

Denial of service



Malicious Insiders

Abuse of Cloud Services



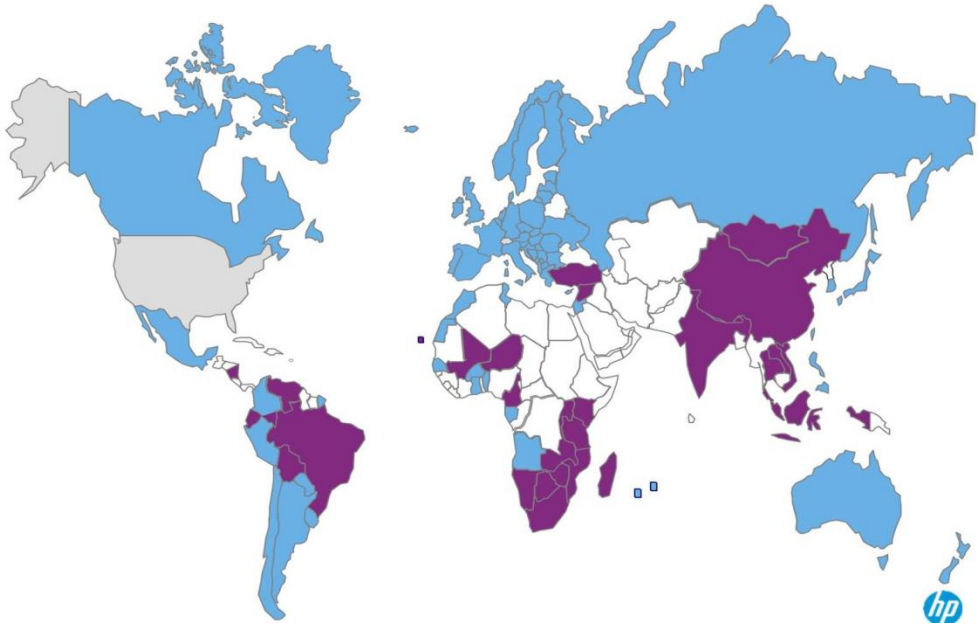
Insufficient Due Diligence

Shared technology vulnerabilities

Regulatory challenges

Uncertainty in all regions and in all business sectors:

- Globalisation and new technologies straining traditional frameworks
- Laws are critical but often lagging behind new technologies
- Emphasis on geography-specific criteria
- Agreement on fundamental principles, but different implementations
- Lack of interoperability between regional legal approaches



National privacy or data protection law in place
Other significant privacy laws in place
Emerging privacy or data protection laws

Cloud can magnify existing issues:

- Transborder data flow restrictions
- Liability questions
- Difficult to know geographic location and which specific servers or storage devices will be used
- Proper data handling and deletion during load-balancing, device reuse, etc.

Societal challenges

- New, innovative business models not obvious or understandable by Data Subjects
- Social norms may be changing **but protection has to stay**
- Traditional "**Consent & Control**" approach may be not sufficient
- **Fear, Uncertainty & Doubt** are shaping perceptions
- Excessive reactivity under scandals pressure drives "impulsive" laws
- Risk of slowing down acceptance or killing new technologies

Trust becomes a key requirement

Data protection in the Cloud

Cloud Computing, Data & Trust

Data moves to the cloud
Reduced transparency
Less control
Concerns over security, integrity, privacy
New risks and vulnerabilities

⇒Firms reluctant to let data flow outside the firms' boundaries into the cloud
⇒Individuals have concerns over privacy, lack of control

Data Protection Risks of Cloud Computing (1)

Opinion 05/2012 on Cloud Computing, Article 29 WP

Lack of control	Cause
Lack of availability	Vendor lock-in
Lack of integrity	Sharing of resources
Lack of confidentiality	Law enforcement requests made directly to a CSP, or without valid EU legal basis
Lack of intervenability	Complexity and dynamics of outsourcing chain
Lack of data subjects' rights	Lack of tools for access, deletion and correction of data
Lack of isolation	Cloud administrators with privileged access rights might link information from different clients

Data Protection Risks of Cloud Computing (2)

Opinion 05/2012 on Cloud Computing, Article 29 WP

Lack of transparency	Cause
Lack of appropriate action by DC or by DS	Insufficient knowledge about potential threats and risks
Lack of knowledge by DC about chain processing	Increased risk involving multiple processors and subcontractors
Lack of knowledge about law applicable to data protection disputes	Personal data processed in different geographic locations within EEA
Lack of knowledge about inadequate levels of data protection or illegality of transfers	Personal data transferred outside EEA without appropriate measures

Cloud features	Key related issues
Multi-tenancy	• Data of co-tenants may be revealed in investigations • Isolation failure • Proper deletion of data and virtual storage devices
Elasticity	• Multiplies attack surfaces • De-anonymisation facilitated
Abstraction	• Cannot rely upon physical security controls
Automation	• Ensuring appropriate data protection when data flows are dynamic • Decrease in human involvement in data protection
Data duplication	• Detecting and determining who is at fault if privacy breaches occur • Difficulty in knowing geographic location and which specific servers or storage devices will be used
Easy data access from multiple locations	• Data access from remote geographic locations subject to different legislative regimes, and transborder data flow compliance issues • Potential for risky usage by employees without due consideration
Subprocessing	• Potential complexity of cloud service delivery chains, both horizontally and vertically • Lack of transparency or compliance by subprocessors • Unauthorized data access from employees of CSPs • Risks to confidentiality from subpoenas or access by foreign governments • Overlapping responsibilities in data management • Unauthorized secondary usage and profiling • Vendor demise

International Data Transfers

Under EU l

CLOUD Major issue

Article 25 Derogations

- EU Commission Findings of **Adequacy** – Argentina, Canada, Israel, Switzerland
- **Safe Harbour** Certified companies
- Data Subject specific **consent**
- **EU Model Contracts** – regulatory approvals
- **Binding Corporate Rules** *(BCR-C done – BCR-P in progress)*
  - Set of rules adopted by a company to provide a legally binding protection for personal data transferred and processed within a global group of companies.
  - Regulatory notification & approval still required in most countries.
  - Applies to data for which HP is a data controller (past, current and prospective employee data, customer data, business contact data).

Cloud Questions

Do we have all the answers?

Cloud users and providers' 'legal & moral' obligation of ensuring privacy and thereby demonstrating the trustworthy nature of their service

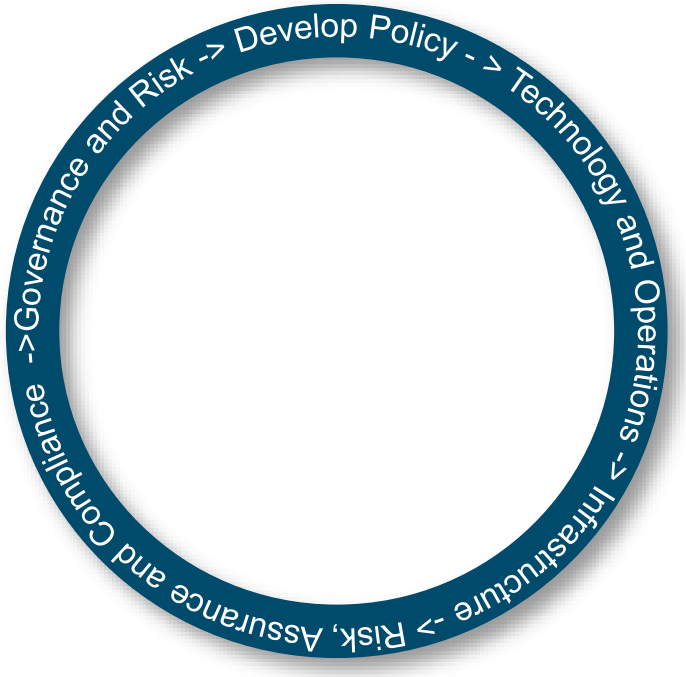
Is data safe across the cloud?	Is it handled based on users' expectations?	Is data handling compliant with laws and regulations?
Is data under control along its complete lifecycle?	Is appropriate data use & obligations ensured along the processing chain?	Are there standards or general practices in place for operating in the Cloud?

Security in the Cloud

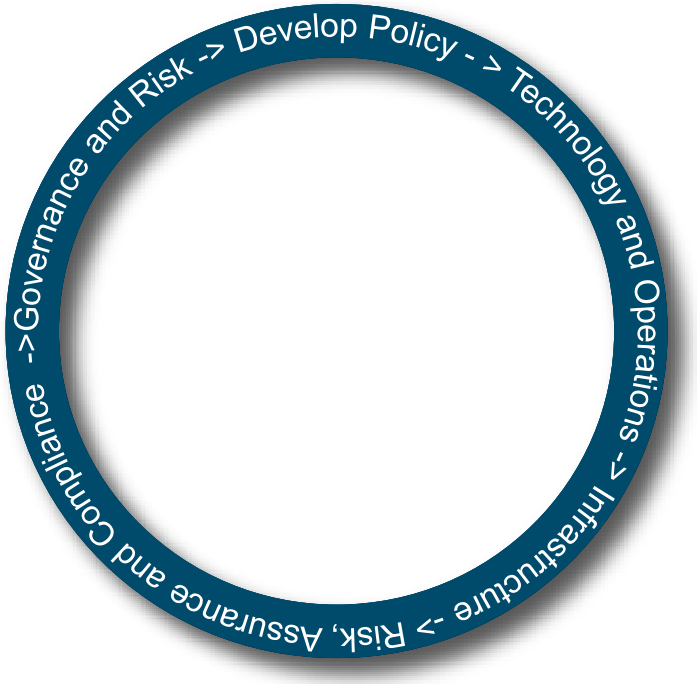
What do we mean by “cloud security”?

1. **Security for the cloud?** → Securely use cloud (consumers)
2. **Security from the cloud?** → Security-as-a-Service
3. **Security in the cloud?** → Embedded security (providers)
4. **Security across clouds?** → Hybrid models, interoperability

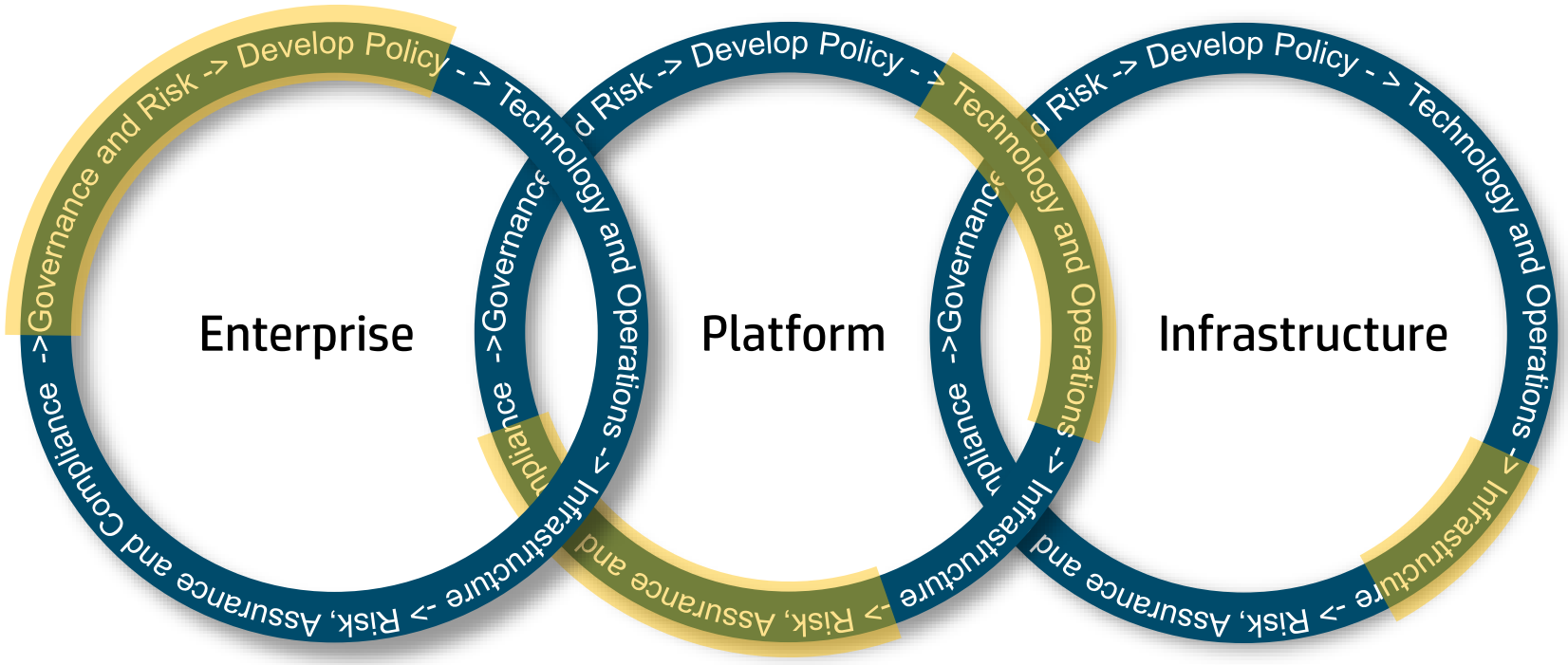
Enterprise security lifecycle



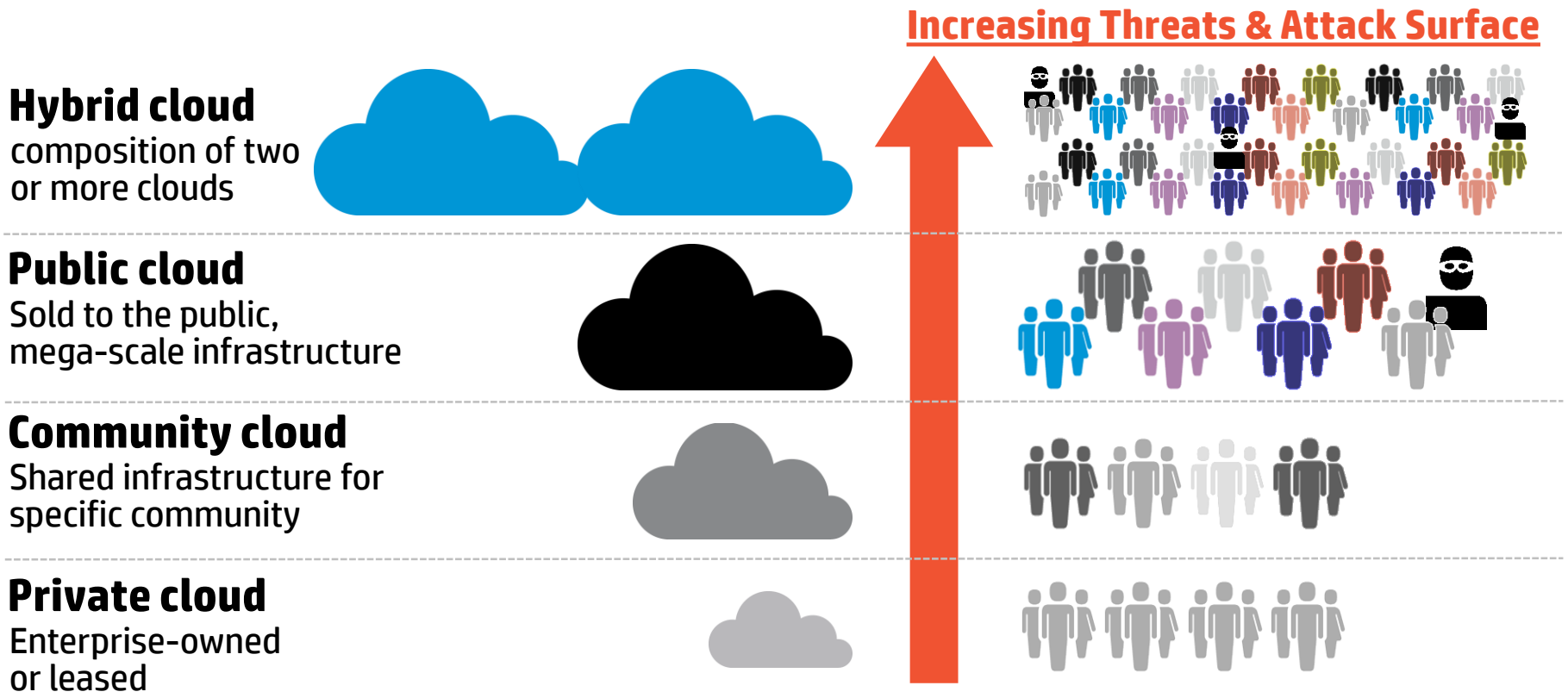
Enterprise security lifecycle



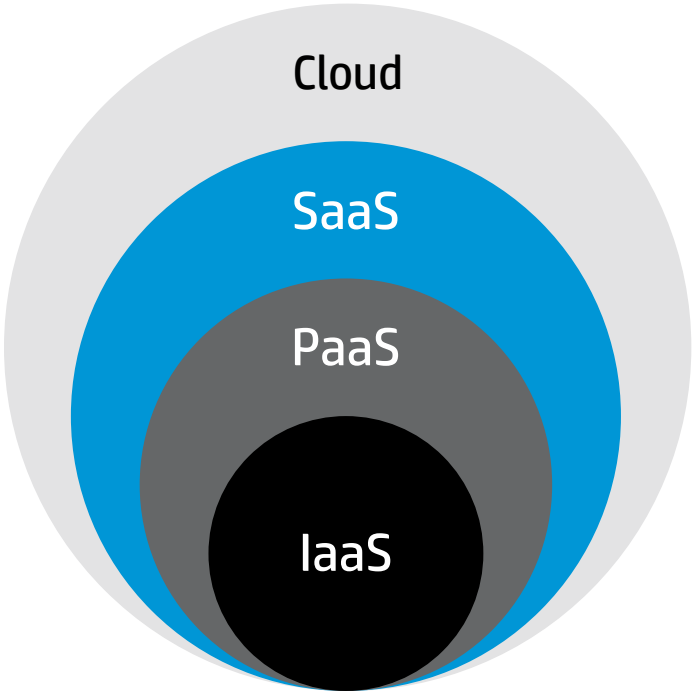
Cloud: transparency and accountability



Cloud models require different security solutions…



...and different roles & responsibilities for security

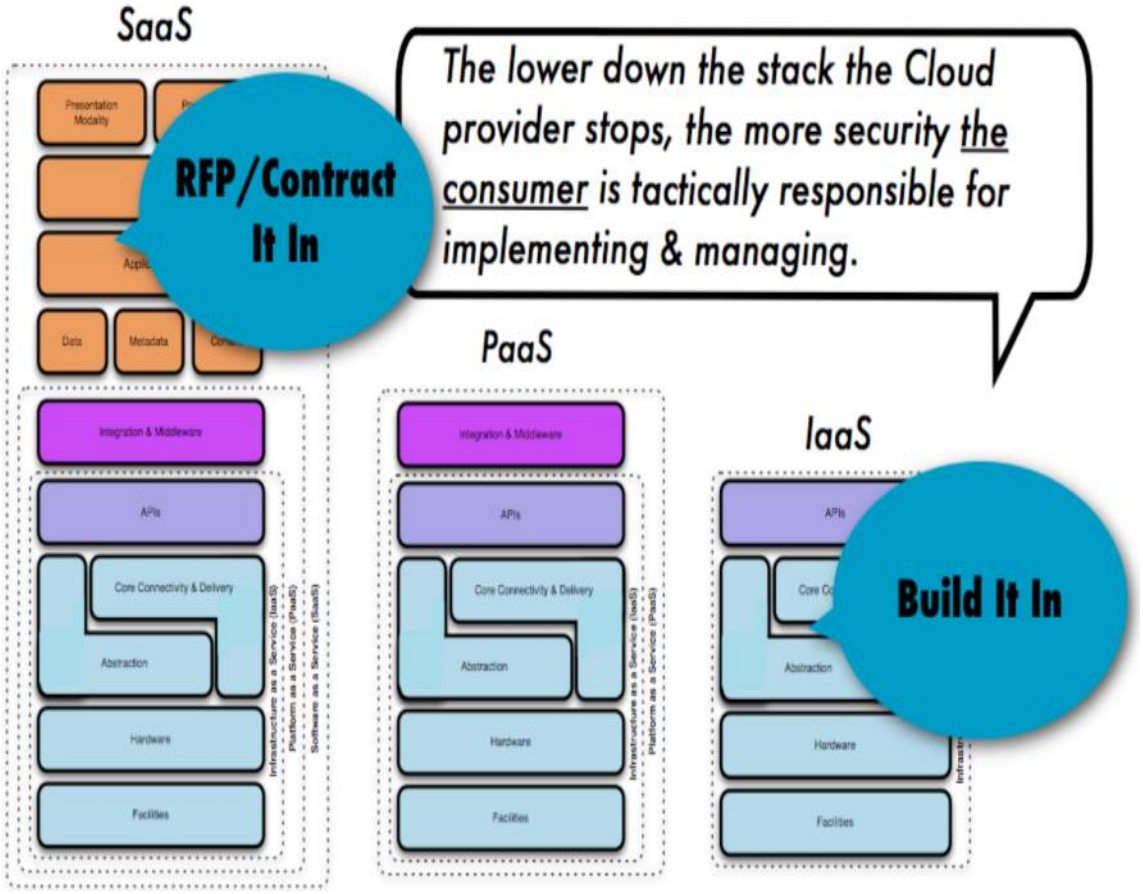


SaaS: Software as a Service, generally provides application, data and infrastructure security, with varying degrees of compliance

PaaS: Platform as a Service, may provide some additional security functions for IDM and secure application development – security falls to app developer and customer IT operations

IaaS: Infrastructure as a Service – providers generally offer basic network & infrastructure security, firewalls, some tools – but customer is generally responsible for implementation, operations, monitoring

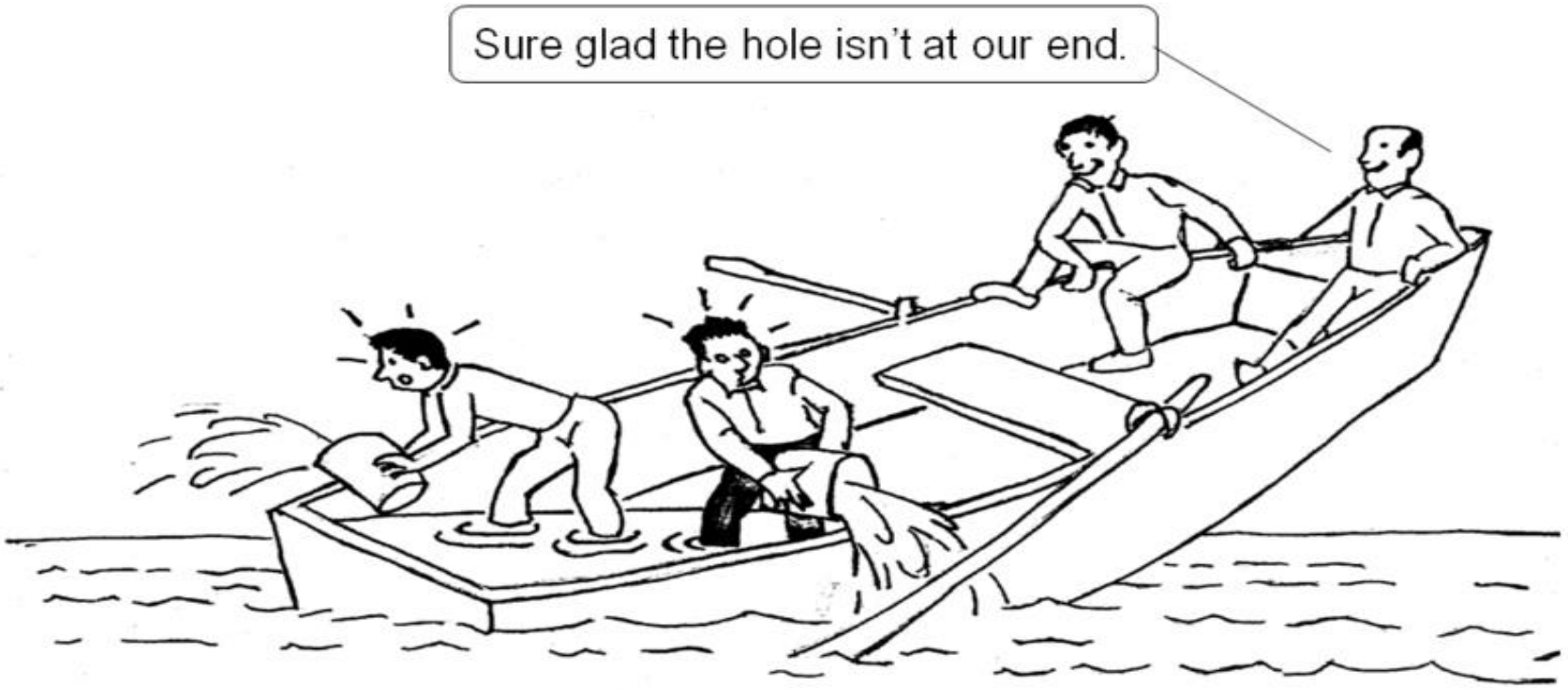
Cloud Security Responsibilities



[CSA, Security guidance for critical areas of focus in cloud computing V3.0, 2011]

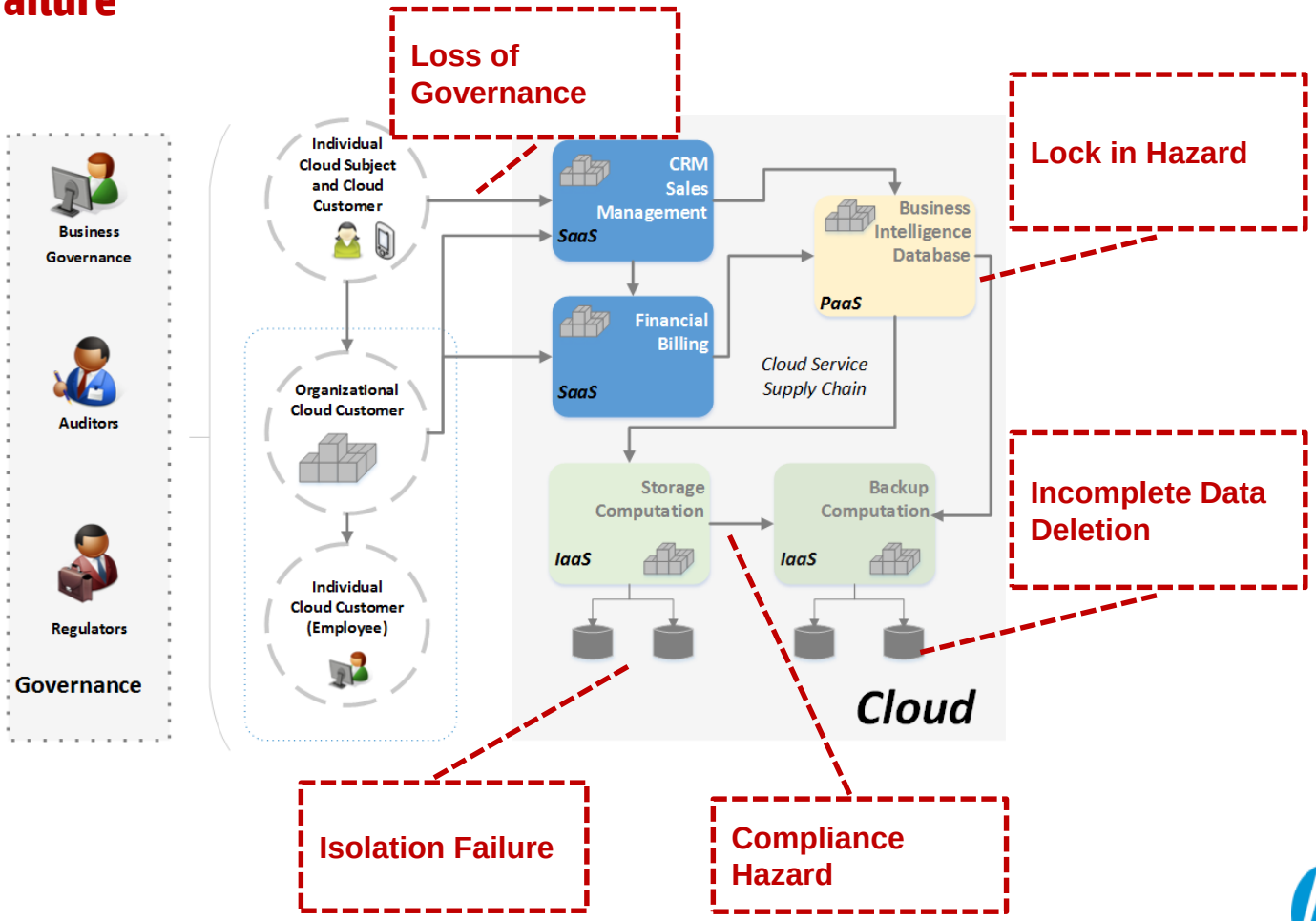
There's a hole in your side of the boat !!!

Security is EVERYONE's job



Cloud Ecosystem Challenges

Ramifications of failure



ENISA Cloud Computing Risks

Risk Category	Risk name
Policy & Organizational	P1. Lock-in P2. Loss of governance ★ P3. Compliance challenges ★ P4. Loss of business reputation due to co-tenant activities P5. Cloud service termination or failure P6. Cloud provider acquisition P7. Supply chain failure

★ Classified as highest risk category

Technical	T1. Resource exhaustion (under or over provisioning) T2. Isolation failure ★ T3. Cloud provider malicious insider - abuse of high privilege roles ★ T4. Management interface compromise (manipulation, availability of infrastructure) ★ T5. Intercepting data in transit T6. Data leakage on up/download, intra-cloud T7. Insecure or ineffective deletion of data ★ T8. Distributed denial of service (DDoS) T9. Economic denial of service (EDOS) T10. Loss of encryption keys T11. Undertaking malicious probes or scans T12. Compromise service engine T13. Conflicts between customer hardening procedures and cloud environment
Legal	L1. Subpoena and e-discovery L2. Risk from changes of jurisdiction ★ L3. Data protection risks L4. Licensing risks

Not Specific to the Cloud	N1. Network breaks N2. Network management (ie, network congestion / mis-connection / non-optimal use) ★ N3. Modifying network traffic N4. Privilege escalation N5. Social engineering attacks (ie, impersonation) N6. Loss or compromise of operational logs N7. Loss or compromise of security logs (manipulation of forensic investigation) N8. Backups lost, stolen N9. Unauthorized access to premises (including physical access to machines and other facilities) N10. Theft of computer equipment N11. Natural disasters

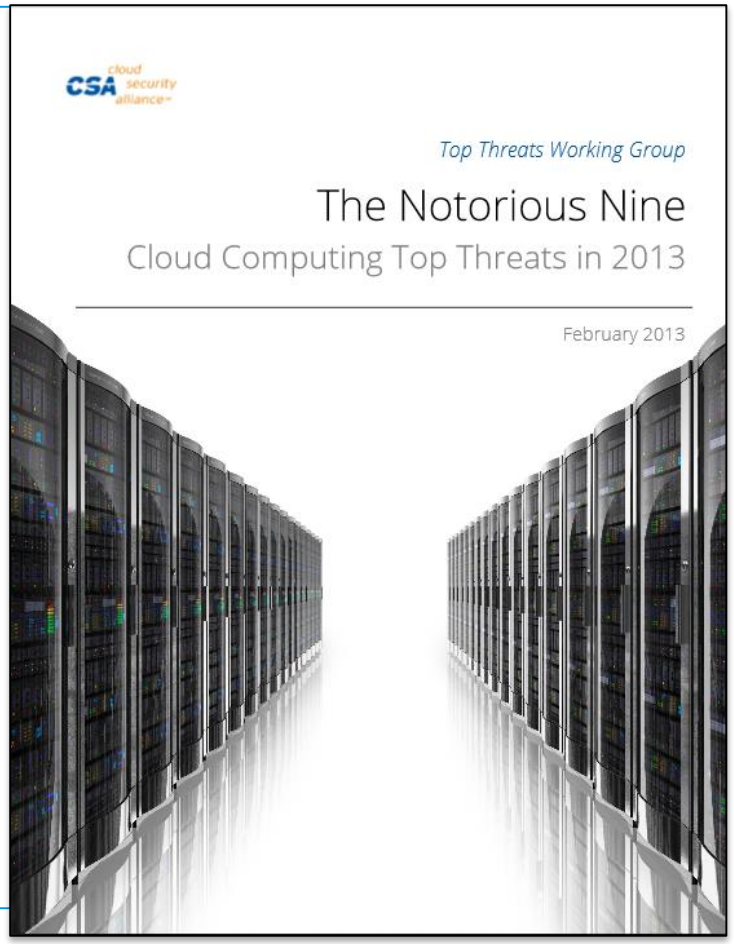
ENISA: Cloud Vulnerabilities

Cloud Specific Vulnerabilities
V1. Authentication Authorization Accounting (AAA) vulnerabilities
V2. User provisioning vulnerabilities
V3. User de-provisioning vulnerabilities
V4. Remote access to management interface
V5. Hypervisor vulnerabilities
V6. Lack of resource isolation
V7. Lack of reputational isolation
V8. Communication encryption vulnerabilities
V9. Lack of or weak encryption of archives and data in transit
V10. Impossibility of processing data in encrypted form
V11. Poor key management procedures
V12. Key generation: low entropy for random number generation
V13. Lack of standard technologies and solutions
V14. No source escrow agreement
V15. Inaccurate modelling of resource
V16. No control on vulnerability assessment process
V17. Possibility that internal (cloud) network probing will occur
V18. Possibility that co-residence checks will be performed
V19. Lack of forensic readiness
V20. Sensitive media sanitization
V21. Synchronizing responsibilities or contractual obligations external to cloud
V22. Cross-cloud applications creating hidden dependency
V23. SLA clauses with conflicting promises *to* different stakeholders
V24. SLA clauses containing excessive business risk
V25. Audit or certification not available to customers
V26. Certification schemes not adapted to cloud infrastructures
V27. Inadequate resource provisioning and investments in infrastructure
V28. No policies for resource capping
V29. Storage of data in multiple jurisdictions and lack of transparency about this
V30. Lack of information on jurisdictions
V31. Lack of completeness and transparency in terms of use
Vulnerabilities not Specific to the Cloud
V32. Lack of security awareness
V33. Lack of vetting processes
V34. Unclear roles and responsibilities
V35. Poor enforcement of role definitions
V36. Need-to-know principle not applied
V37. Inadequate physical security procedures
V38. Misconfiguration
V39. System or OS vulnerabilities
V40. Untrusted software
V41. Lack of, or a poor and untested, business continuity and disaster recovery plan
V42. Lack of, or incomplete or inaccurate, asset inventory
V43. Lack of, or poor or inadequate, asset classification
V44. Unclear asset ownership
V45. Poor identification of project requirements
V46. Poor provider selection
V47. Lack of supplier redundancy
V48. Application vulnerabilities or poor patch management
V49. Resource consumption vulnerabilities
V50. Breach of nda by provider
V51. Liability from data loss (cp)
V52. Lack of policy or poor procedures for logs collection and retention
V53. Inadequate or misconfigured filtering resources

Cloud Failures

1. Data Breaches 43 (joint)
2. Data Loss
3. Account Hijacking 3
4. Insecure APIs 53
5. Denial of Service
6. Malicious Insiders 3
7. Abuse of Cloud Services 12
8. Insufficient Due Diligence
9. Shared Technology Issues 5

Analysis of 172 cloud incidents 2008-2012, IEEE Spectrum, December 2012, p84



Protecting information in the cloud

Cloud security: guidance for critical areas

Architecture

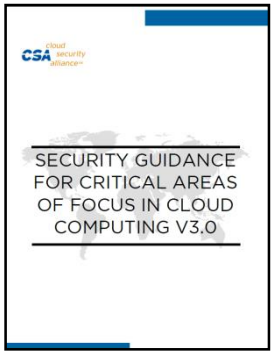
1. Cloud computing architectural framework

Governance

2. Governance and enterprise risk management
3. Legal issues: contracts and electronic discovery
4. Compliance and audit management
5. Information management and data security
6. Interoperability and portability

Operations

7. Traditional security, business continuity, and disaster recovery
8. Data center operations
9. Incident response
10. Application security
11. Encryption and key management
12. Identity, entitlement, and access management
13. Virtualization



http://cloudsecurityalliance.org/

CCM

CCSK™
Certificate of
Cloud Security Knowledge

https://ccsk.cloudsecurityalliance.org/

CSA Security Guidance
Cloud Solutions Risk Assessment

Adopt a risk based approach to moving to the cloud:

1. Identify the asset for the cloud deployment

2. Evaluate the asset

How would we be harmed if …

3. Map the asset to potential cloud deployment models

4. Evaluate potential cloud service models and providers

Focus will be on the degree of control you have to implement risk mitigations in the different SPI tiers

5. Sketch the potential data flow

6. Conclusions

Use cloud only for non-private data

Pretty good solution

Much of the data you process isn't subject to data handling regulations or confidentiality

Some applications don't ever need to use personal or confidential data

Drawbacks:

- Don't get the benefits of cloud computing for private data
- Have to separate private from non-private data

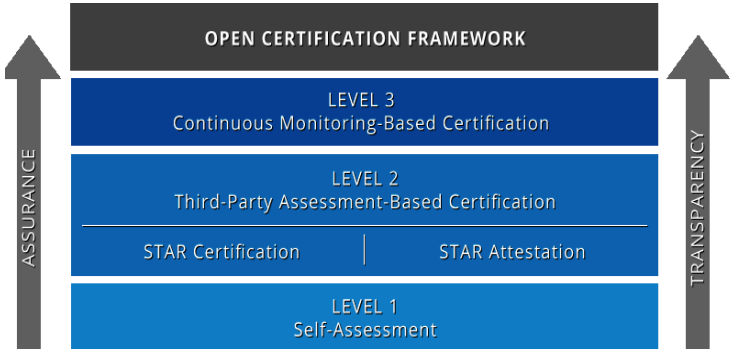
Leave privacy protection to your service provider

SAS-70 Type II/SOC-2, ISO,...

CSA Open Certification Framework

Do this for account data anyway

Security need not suffer



Drawbacks:

- Depends on CSP
- Need to agree roles and responsibilities
- Standard SaaS business models involve repurposing of customer data
- Cloud computing Terms of Service typically offer **no** compensation if your data is stolen or misused

Trusted computing

Uses tamper-resistant hardware storing ID, and machine-readable privacy policies

Data is encrypted twice

- Outer layer can only be decrypted by trusted hardware
- Inner layer can only be decrypted by software that has been checked by an organization you trust to meet a privacy policy you specify

http://www.trustedcomputinggroup.org

Drawback:

- All the organizations which handle your data have to be part of the system
- Limits choice of service providers
- Potential bottleneck

Encryption for cloud storage

Encrypt your data before it's sent to the cloud

Using a key that you don't tell your service provider

- Don't just encrypt it in transit!

"Searchable encryption" lets you search encrypted data in the cloud

- "Cryptographic Cloud Storage", S Kamara & K Lauter, Microsoft Research

Drawback:

- The encrypted data usually can't be processed
- Severely limits the applications possible
- Searchable storage can be unacceptably slow
- Potential key management overhead

Just-in-time decryption

Store data in the cloud encrypted

To process/query it, pass your key to the cloud just in time, re-encrypt straight afterwards

- Mark Cusack, RainStor, “Information Preservation: Structured Data Archiving: Key Issues” http://www.slideshare.net/cpurrington/mark-cusack-cloud-camp4-london-2

Drawback:

- Time window when your data is vulnerable
- Data might be cached, stored in clear or otherwise accessed as a result

Processing encrypted data

Fully homomorphic encryption

- Beautiful theoretical result by Craig Gentry of IBM Research
- General way of calculating any function on encrypted data in the cloud

Multi-party computation

- Could enable CSP and user to cooperate to calculate a function depending on data known to the user and data known to the CSP
- Requires several rounds of interaction

Drawback:

- Not (yet?) practical, unfortunately
- Require cloud providers to rewrite their apps

Obfuscation

Idea

- Obfuscate data before sending it to the cloud for processing
- Using a key you don't tell your service provider
- De-obfuscate result of processing to get right answer
- "A privacy manager for cloud computing", Miranda Mowbray, Siani Pearson & Yun Shen, http://www.hpl.hp.com/techreports/2009/HPL-2009-156.html

Examples

- Automatically replace customer IDs by pseudonyms (TC3 Health)
- Multiply SQL database columns by secret factors, and permute (90% of features of Saleforce.com's sales and marketing suite)

Drawbacks:

- Gives weaker security than encryption
- Application-specific, and not suitable for all applications

Original image by Brian Snelson (exfordy onFlickr) http://www.flickr.com/photos/exfordy/128576390/

Virtual private cloud

Reserved space in a public cloud isolated from other customers

- May be a physical machine in the cloud reserved for you
- Or may use firewalls and encryption for isolation

Protects against attacks by co-located customers

Drawbacks:

- Doesn't in itself protect against other attacks
- Not always clear what is involved

Private cloud

Automated virtualization within your corporate firewall

More privacy, yes.

For some data and applications you have to use private rather than public clouds

Drawbacks:

- Less flexible
- Less scalable
- Can't use economies of scale of very large data centres
- … or of security
- Maintaining, patching and upgrading servers is **your** problem

Cartoon by Geek&Poke http://geekandpoke.typepad.com/geekandpoke/2009/10/the-history-of-the-cloud-part-1.html

Hybrid cloud

Can use a private cloud for certain tasks while a public cloud is used for other less privacy-sensitive tasks

e.g. use a private cloud for mission critical applications, a virtual private cloud for high availability applications, and a public cloud for test and development or productivity applications

Hybrid interoperability allows movement of workloads

Allows contextually tailored solutions and flexibility, driven by customer needs

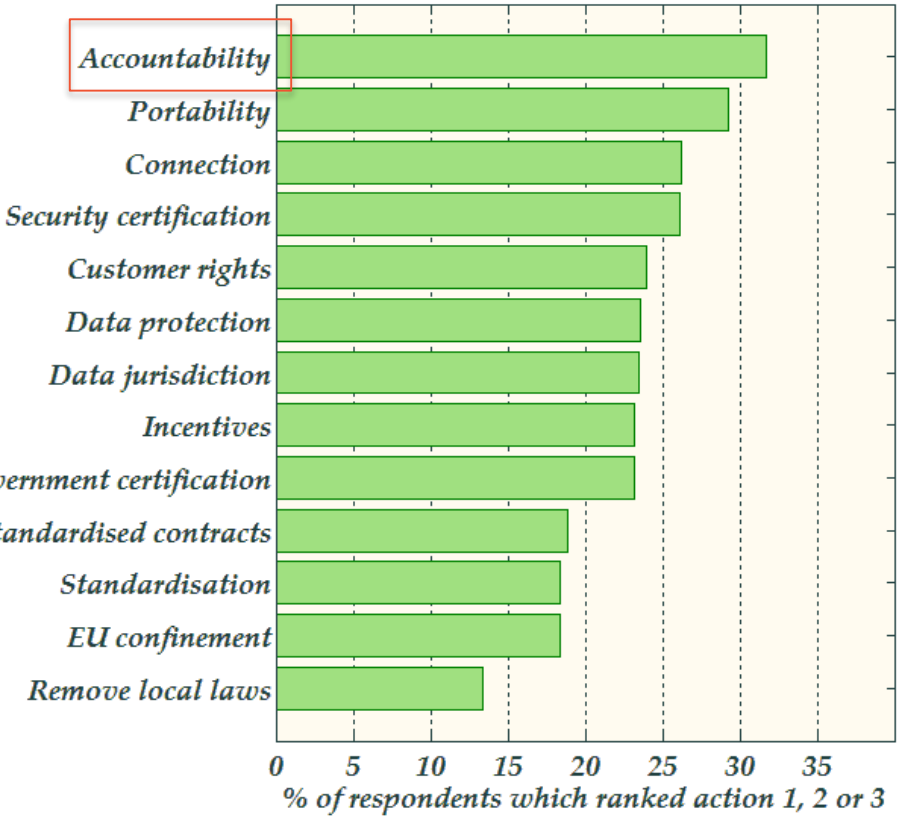
Drawbacks:

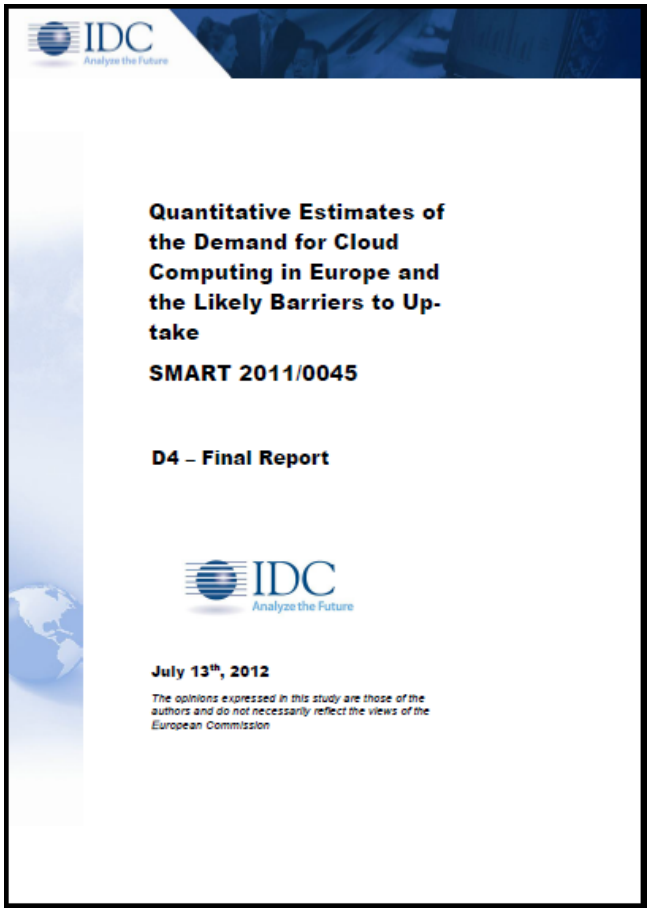
- Need to determine service delivery model for each application/workload
- Shortcomings of individual models still present

Accountability in the Cloud

Business Users' Ranking of Key Actions to Improve Cloud Adoption

Accountability is a clear supporter of growth in the cloud marketplace




IDC
Analyze the Future

Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take

SMART 2011/0045

D4 – Final Report

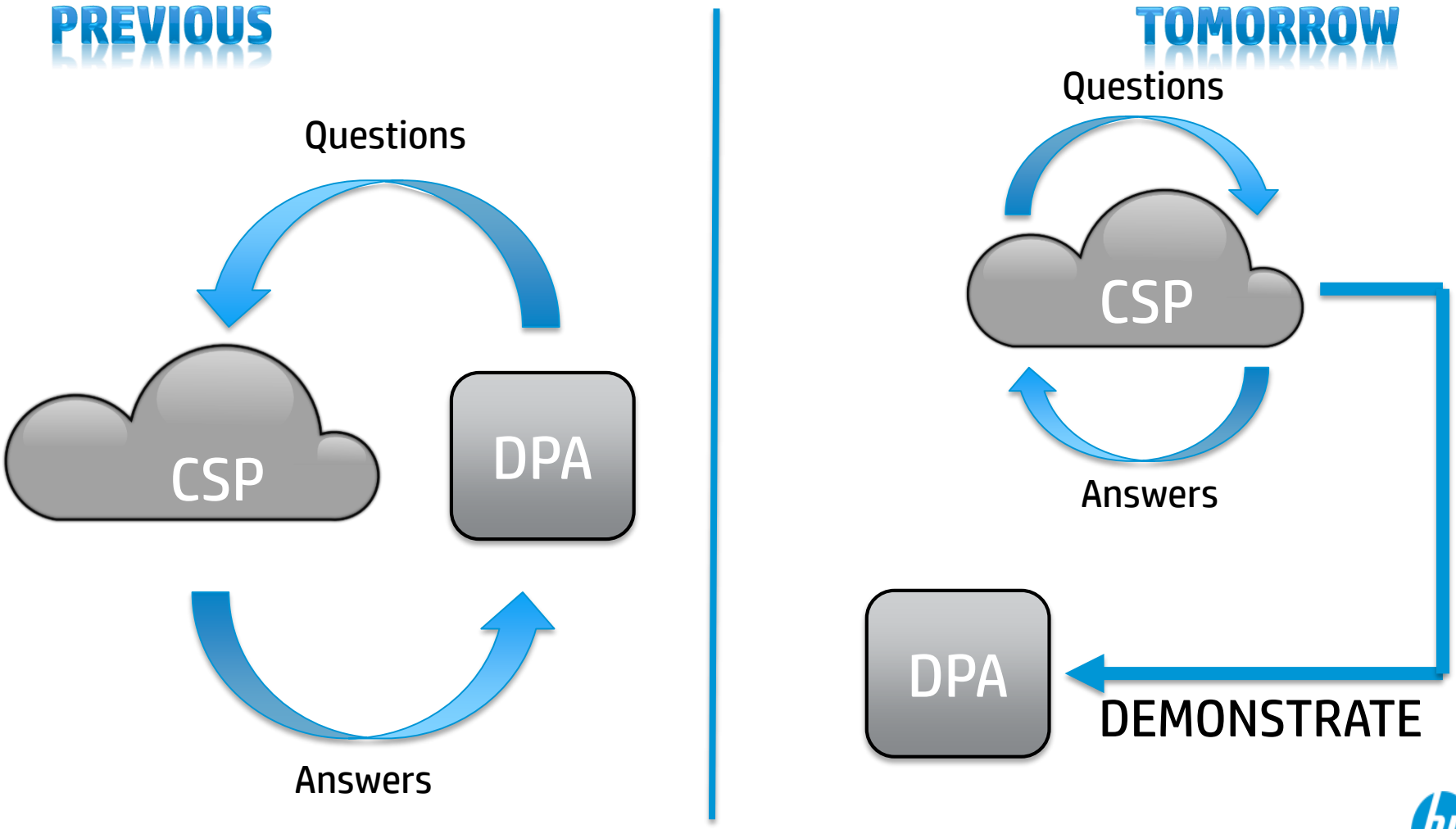
IDC
Analyze the Future

July 13th, 2012

The opinions expressed in this study are those of the authors and do not necessarily reflect the views of the European Commission

Based on data from: IDC, Quantitative Estimates of the Demand of Cloud Computing in Europe, 2012

Moving to an accountability-based approach

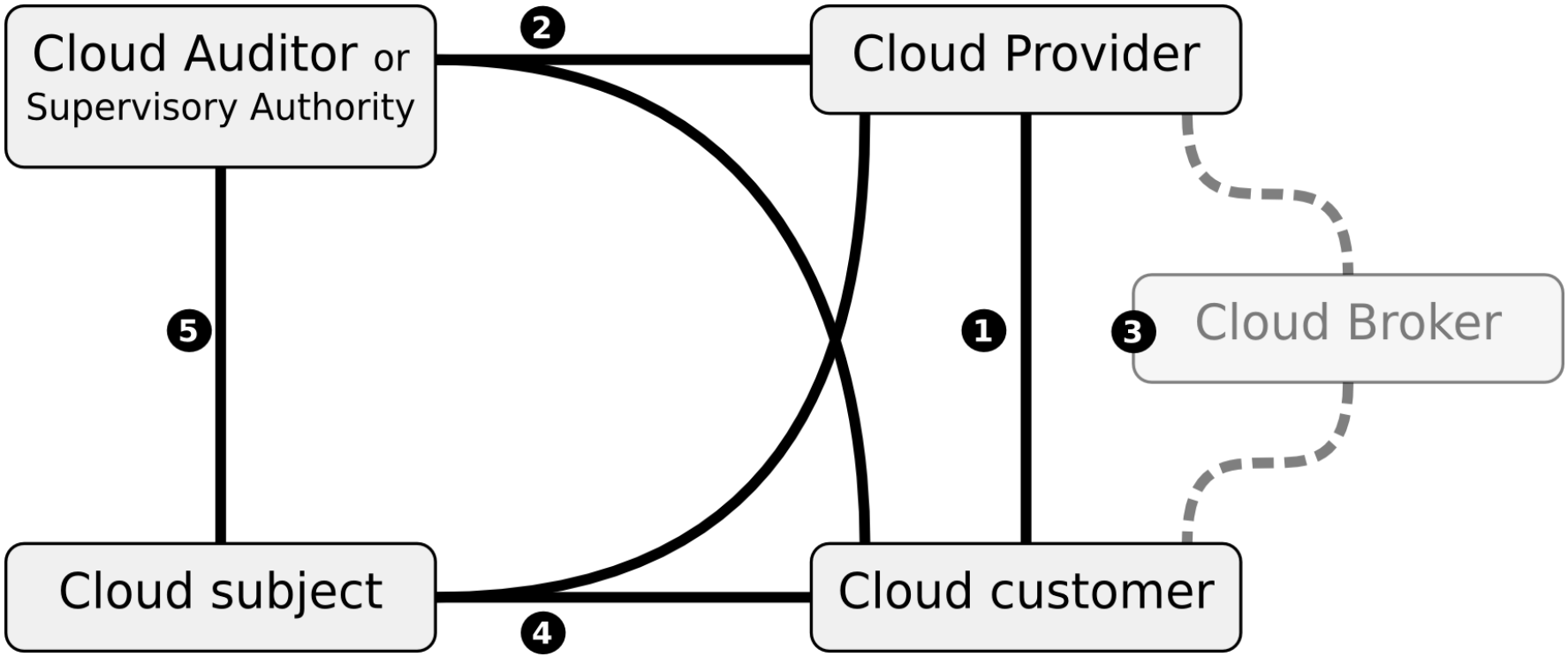


Account in the Cloud

Forms of “accounts”:

- Data Protection Impact Assessment (by DC & DP)
- Notification to the supervisory authorities
- Notification to data subjects
- Contractual compliance verification
- Documentation obtained, created, and maintained by DC & DP
- Certifications and seals
- Audit Reports

Actors of cloud accountability



Key Data Protection Terminology

Data Controller

Data Processor

Data Subject

DPA

Organisational cloud customer is in general considered DC
- regulated by DPA

Cloud service provider nearly always DP
- may need to assume co-controllership responsibilities
- may not know who the users are or what their services are being used for

Joint controllership may be relevant to some cloud providers, who may be considered a joint controller through determining processing 'means'.

Cloud client/controller may not be solely able to determine the purposes and the means of processing because the CSP:

- designs the infrastructure and also, in a measure depending on the cloud model (IaaS, PaaS or Saas), the services
- elaborates standard SLAs with little/no customisation possibility

Actor Roles

Extended NIST cloud roles	Data protection roles
Cloud subject	Data subject
Cloud customer	Data controller or Data processor
Cloud provider	Data processor or Data controller
Cloud carrier	Data processor or Data controller (unlikely) or Not applicable.
Cloud broker	Data processor or Data controller
Cloud auditor	(Not Applicable)
Cloud supervisory authority	Supervisory authority (DPA or NRA)
(Not Applicable)	Third party
(Not Applicable)	Recipient

Cloud Accountability 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)
Funding: €13m total funding (€10m EC funding)
13 Partners - Coordinator & Scientific Lead Hewlett Packard (HP)

Industry

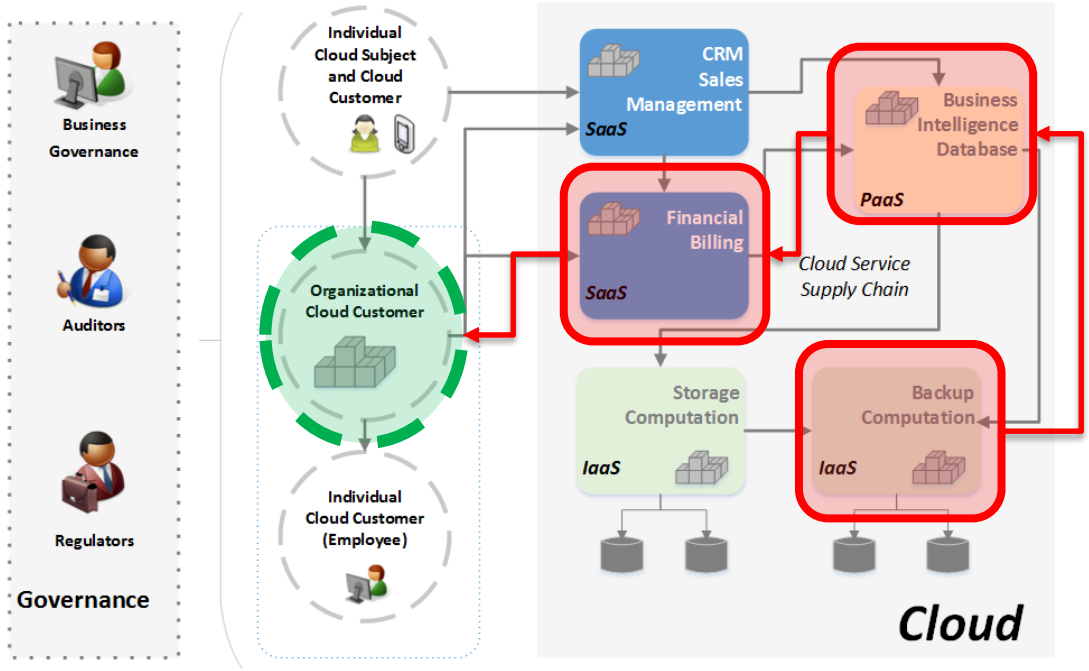
Community

Research

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

Accountability Relationships

Accountability through cloud service supply chains to cloud customer



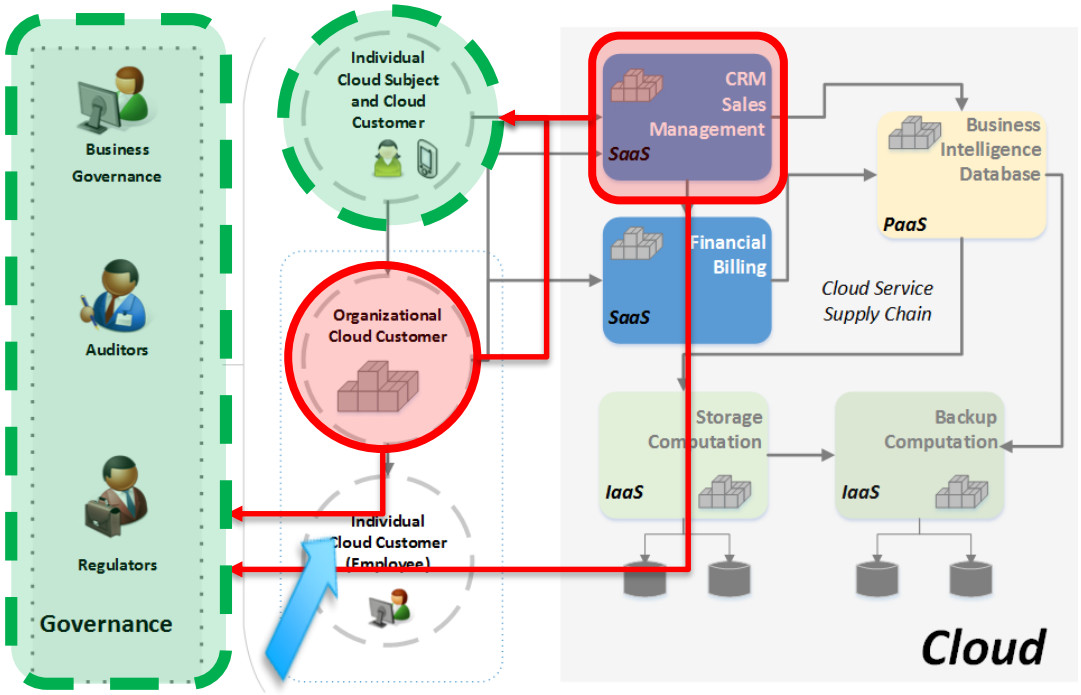
DC accountable for applicable data protection measures

DP accountable for cooperation with DC to:

- meet data subjects' rights
- assist DC in providing security measures
- act only on DC's behalf

Accountability Relationships

Cloud providers & customers accountable to cloud subjects, cloud supervisory authority and society

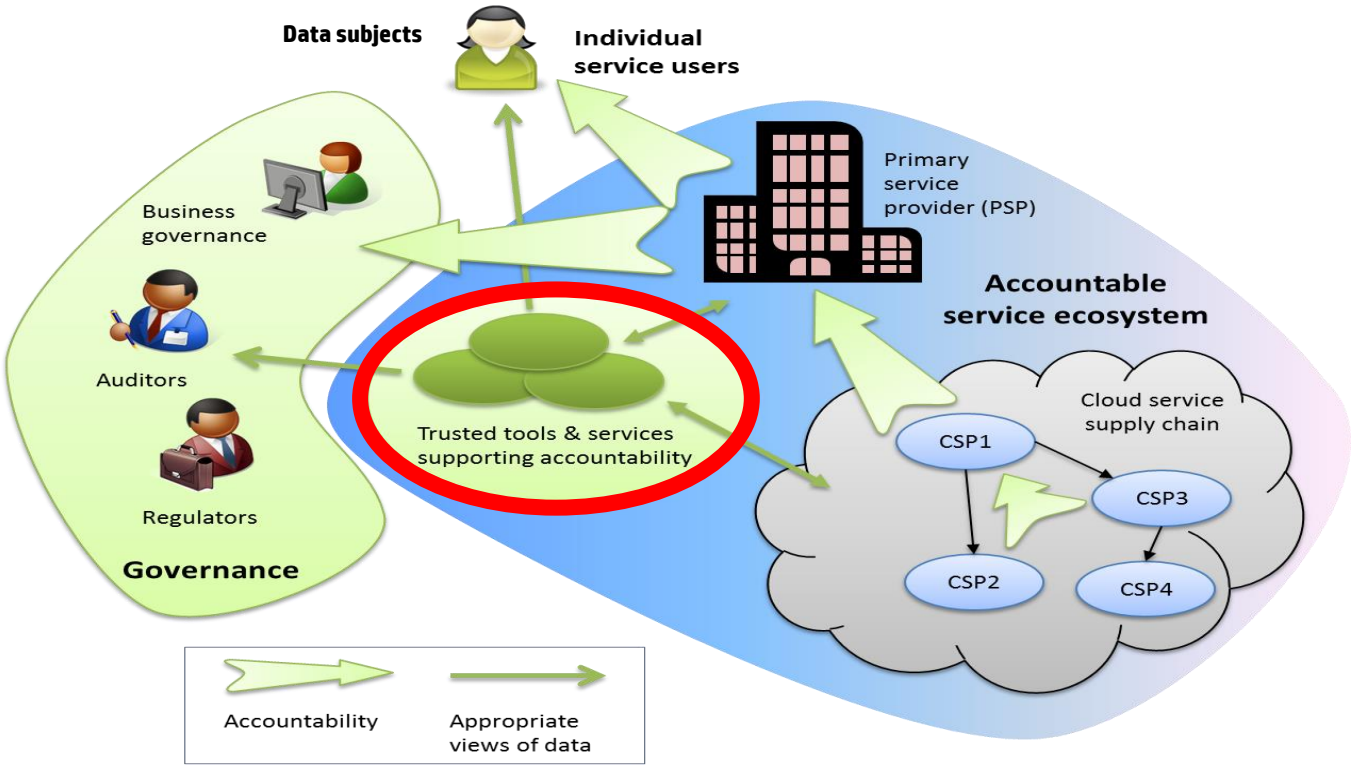


Provision of Account

- All actors ultimately accountable to cloud subject
- Governance holds to account
  - especially concerned with non-functional aspects

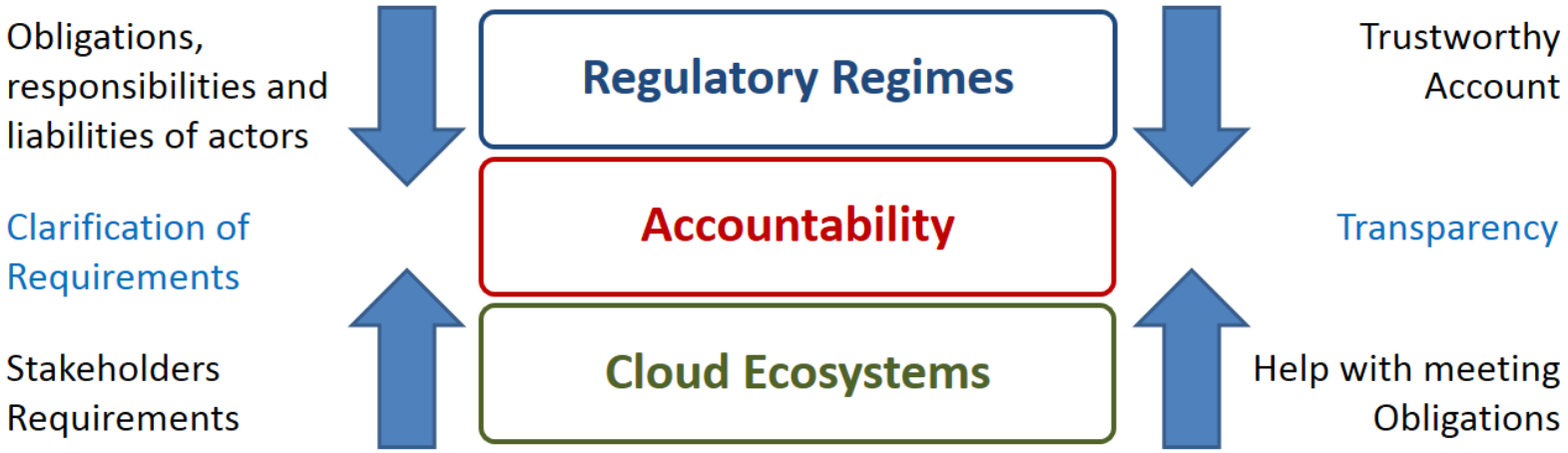
CLOUD ACCOUNTABILITY PROJECT

Accountability Approach



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

Accountability Context



CLOUD ACCOUNTABILITY PROJECT

Accountability-based Approach in the Cloud

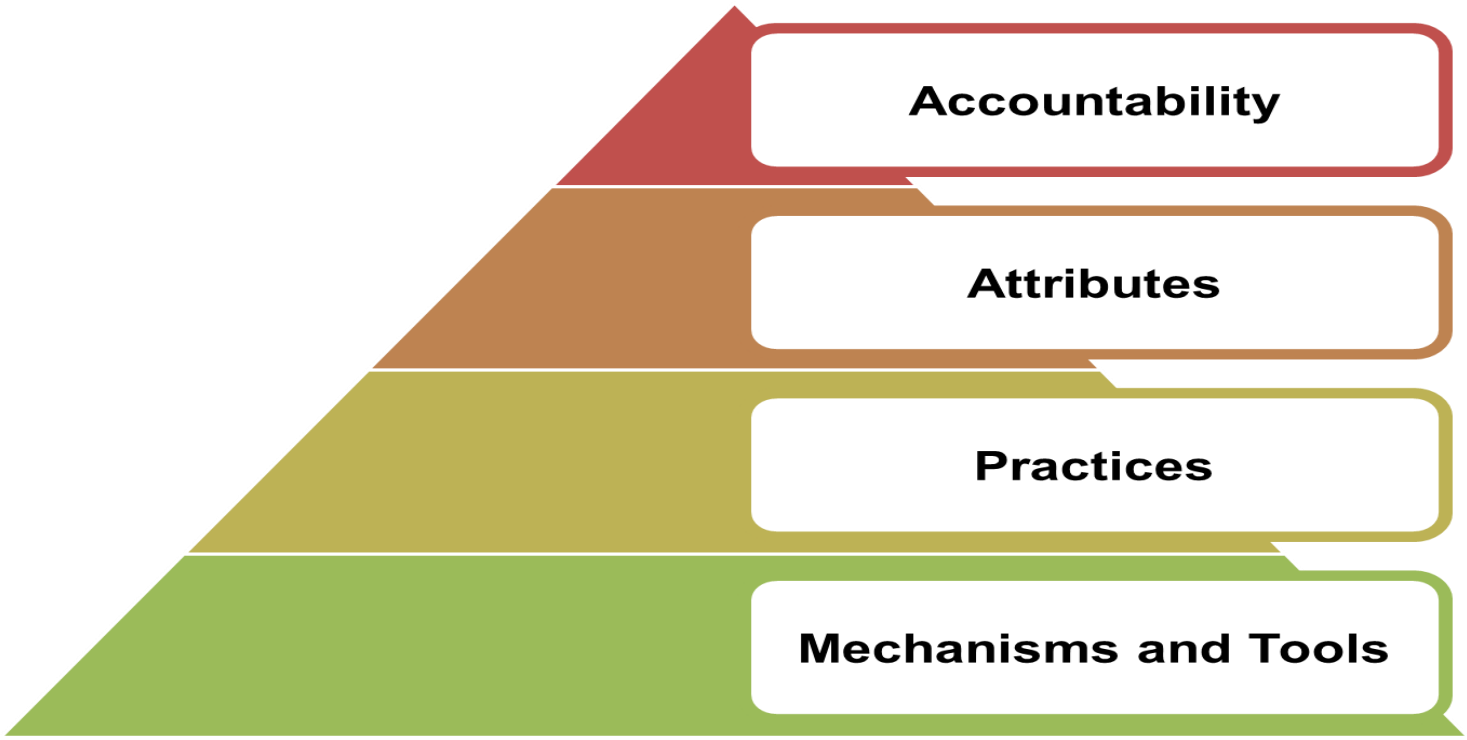
We take a 'strong accountability' approach

In particular, via:

- Being precise about what accountability means
- Joining technical measures to enhance the integrity and authenticity of logs with enhanced reasoning about how these logs show whether or not data protection obligations have been fulfilled (trusted logs + analysis)
- Including verification by independent, trusted entities and certification based on such verification
- Moving beyond accountability of procedures, to accountability of practice

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

Accountability Model



CLOUD ACCOUNTABILITY PROJECT

Defining Accountability for Data in the Cloud

Contextualizing accountability for data governance in cloud ecosystems

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, storing, sharing, deleting and otherwise using the data according to contractual and legal requirements from the time it is collected until when the data are 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

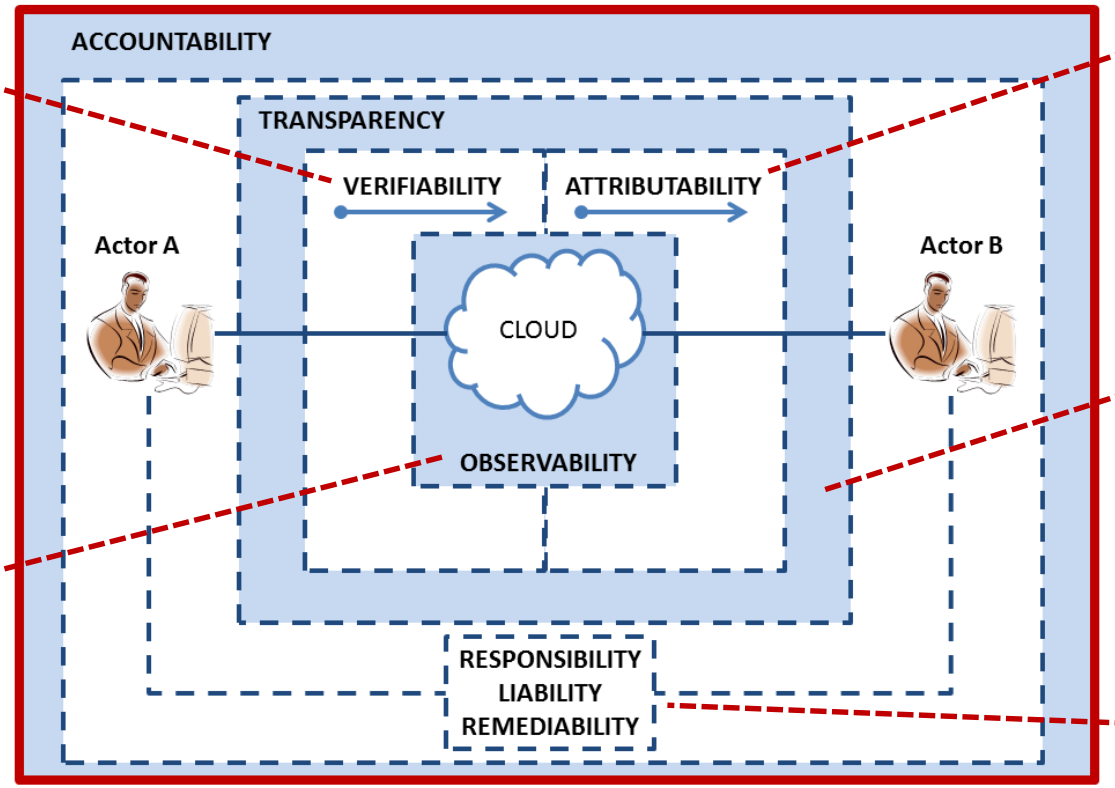
This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).

CLOUD ACCOUNTABILITY PROJECT

Accountability Attributes

Assess compliance

Analyse cloud behaviour



Identify causes

Support openness

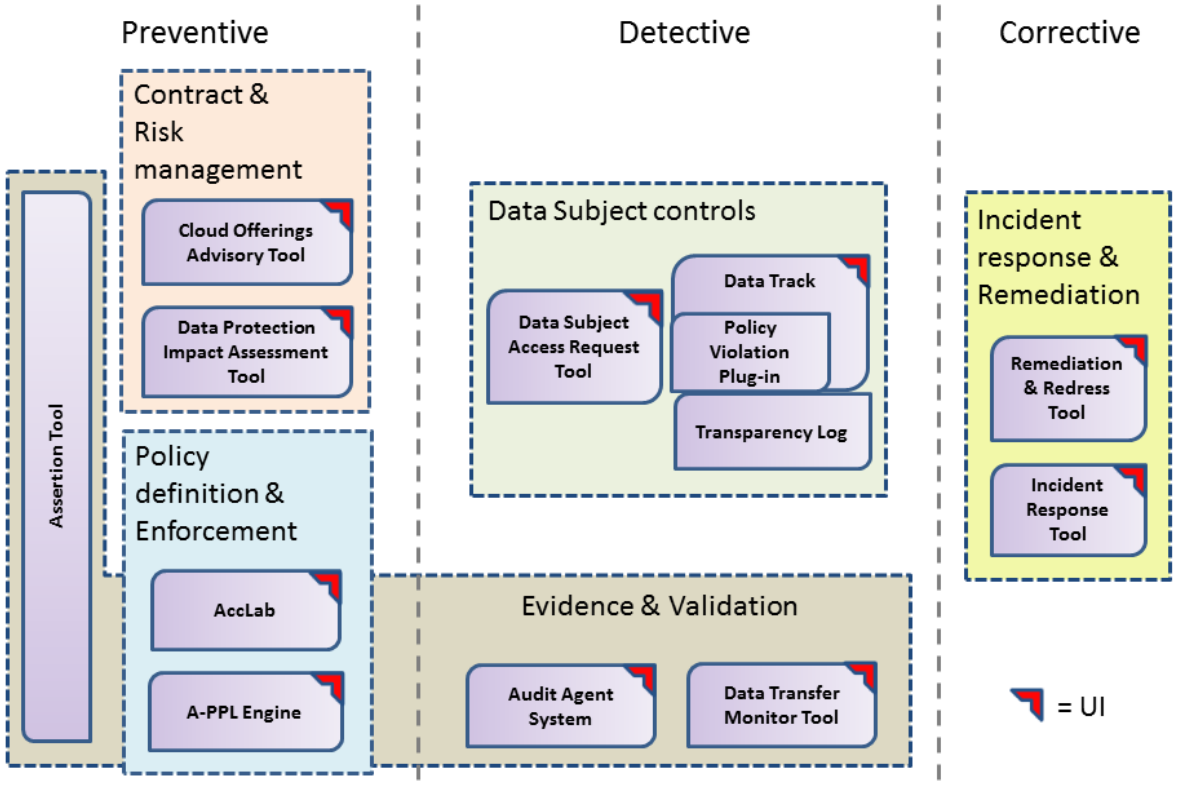
Provide Assurance

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

Practice	Function	Mechanisms
Define governance	Policy definition	• Clear definition of responsibilities within policies • Enhancement of policies to include ethical aspects reflecting social values • Machine readable policies
Ensure implementation	Policy implementation	• Automated policy enforcement
	Risk assessment	• Data protection impact assessment
Explain & justify actions	Transparency	• Tool to support contractual transparency • Tool to support data subject access and correction
	Evidence for verifiability (e.g. within provision of accounts or for certification)	• Automated monitoring and collection of evidence tools • Assurance about accountability tools deployed
	Detection of policy violation	• Assessment of satisfaction or violation of obligations
Remedy failure	Remediation	• Remediation tool • Attribution of failure
	Exception notification	• Incident response tool

CLOUD ACCOUNTABILITY PROJECT

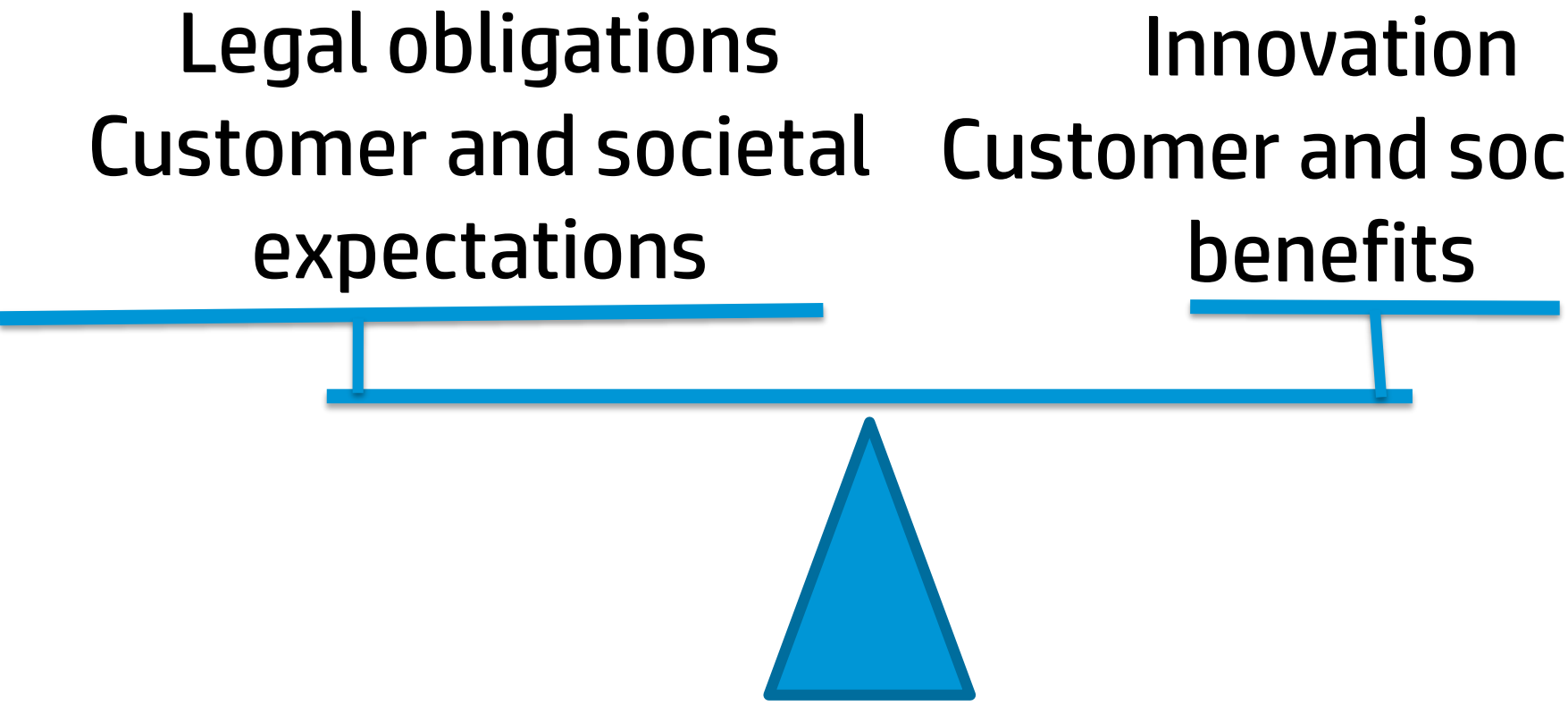
A4Cloud Toolkit



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

Impact of technological and business trends

Trust Challenge



Implications of adopting more open practices – security and privacy risks and design suggestions

Exercise 3

Groups of about 7 people reporting back

Some suggestions to consider

1. A Day made of Glass: http://www.youtube.com/watch?v=6Cf7IL_eZ38

2. Google Glasses: http://ed.ted.com/lessons/rapid-prototyping-google-glass-tom-chi

and

http://www.youtube.com/watch?v=0HS161sdheI

3. Self Driving Cars: http://www.youtube.com/watch?v=7_STMOonchg

4. Internet of Things: http://www.youtube.com/watch?v=Cpbbrpgwu2I

5. Personalised health services, e.g. *www.umotif.com*, *Care.data*

…

Further Reading

1. Cloud Security Alliance (CSA) (2011) Security Guidance for Critical Areas of Focus in Cloud Computing. V3, English language version.
2. Catteddu D, Hogben G (eds.) (2009) Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA Report.
3. European Parliament (2012) Fighting Cyber Crime and Protecting Privacy in the Cloud. Directorate-General for Internal Policies.
4. Gellman R (2009) Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. World Privacy Forum.
5. Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly.
6. Pearson S (2011) Toward Accountability in the Cloud. IEEE Internet Computing, IEEE Computer Society, July/August, 15(4):64-69.
7. Pearson S (2012) Privacy, Security and Trust in Cloud Computing. In: Pearson, S., Yee, G. (eds.), Privacy and Security for Cloud Computing, Computer Communications and Networks, 3-42. Springer.
8. White House (2014) Big Data: Seizing Opportunities, Preserving Values.

Thank you

Siani Pearson, Principal Researcher, HP Labs
Email: siani.pearson@hp.com
Tel: +44 (0) 117 316 2558