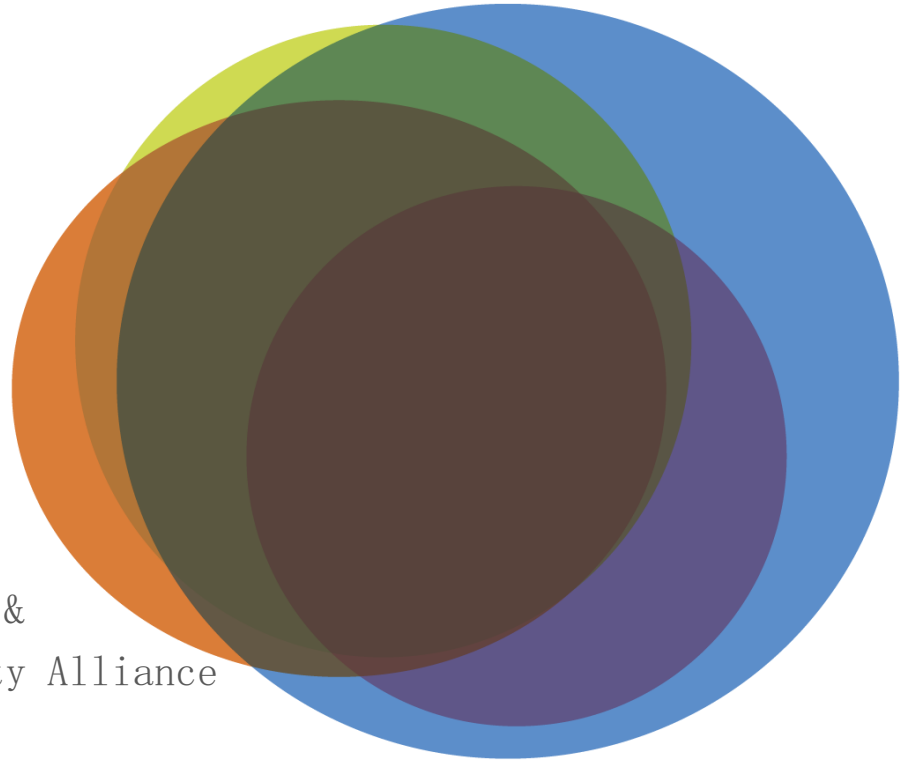
Privacy Compliance and Security SLA: CSA addressing the challenges



Daniele Catteddu, Managing Director EMEA &
OCF-STAR Program Director - Cloud Security Alliance

Arthur van der Wees, Managing Director international law firm Arthur's Legal

Dr. Paolo Balboni, Chair - CSA Privacy Level Agreement Working Group; Founding Partner - ICT LEGAL CONSULTING; Scientific Director - European Privacy Association

ABOUT THE CLOUD SECURITY ALLIANCE

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

- Global, not-for-profit organization
- Over 65,000 individual members, more than 200 corporate members, and 65 chapters
- Building best practices and a trusted cloud ecosystem
  - Agile philosophy, rapid development of applied research
  - GRC: Balance compliance with risk management
  - Reference models: build using existing standards
  - Identity: a key foundation of a functioning cloud economy
  - Champion interoperability
  - Enable innovation
  - Advocacy of prudent public policy

ABOUT THE CLOUD SECURITY ALLIANCE

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

- RESEARCH
  - https://cloudsecurityalliance.org/research/
- ADVISE GOVERNMENTS AND PRIVATE COMPANIES
- EDUCATION - PROFESSIONAL CERTIFICATION - TRAINING
  - https://cloudsecurityalliance.org/education/
- PROVIDER CERTIFICATION
  - https://cloudsecurityalliance.org/star/
- STANDARDS
  - https://cloudsecurityalliance.org/isc/
- Events
  - https://cloudsecurityalliance.org/events/

Cloud Procurement Barriers

PICSE: Cloud service procurement

The overarching objective of PICSE is to set up a **European Procurers ' Platform** capable of raising the level of understanding of the issues surrounding procurement of cloud services

PICSE stakeholders

- Procurement specialists
- Public Research Organisations
- Funding agencies, national research agencies & councils
- SMEs & private sector
- Policy Makers
- Cloud Service Providers
- Associations of local government & procurers
- Public sector Decision Makers
- General Public

About PICSE

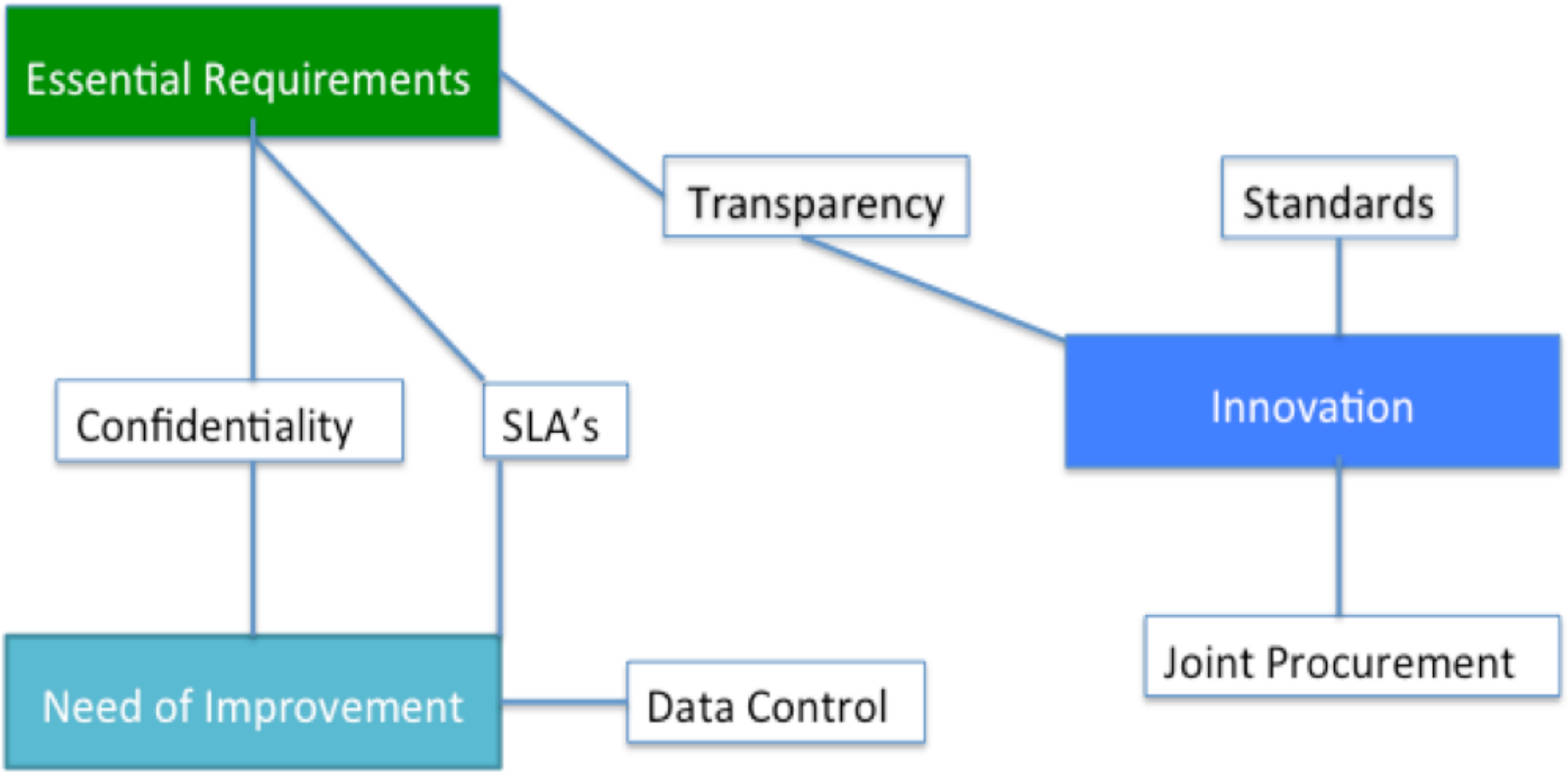
- H2020 Coordination and Support Action
- Total budget: 500 K€
- Duration: 18 months
- Start date: 1 Oct. 2014
- Partners:

CERN

CSA cloud security alliance®

Trust-IT Services Ltd
Communicating ICT to markets

Cloud Procurement: needs and requirements



Cloud Procurement: Challenges

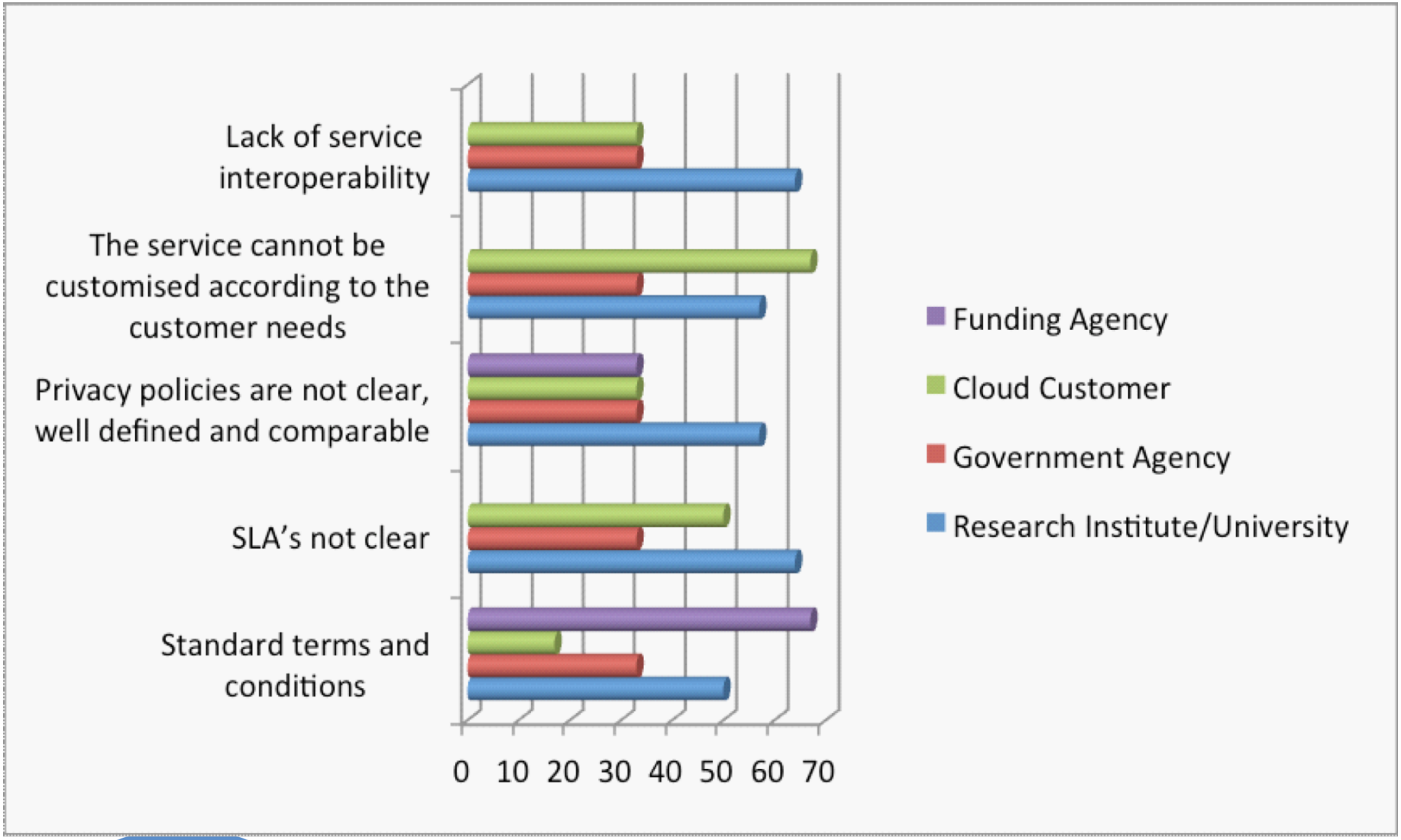


Figure 4: Barriers in different communities

Cloud Procurement: Barriers

Place	Barriers
# 1	Lack of customisation (42%)
# 2	Unclear privacy policies (40%)
# 3	Lack of service interoperability (37%)
# 4	Lack of confidentiality assurance in IPR management (33%)
# 5	Immature services (26%)
# 5	Stringent legal and regulatory requirements (26%)

Table 7: Top 5 barriers related to risks of cloud computing

Cloud Procurement: What to improve?

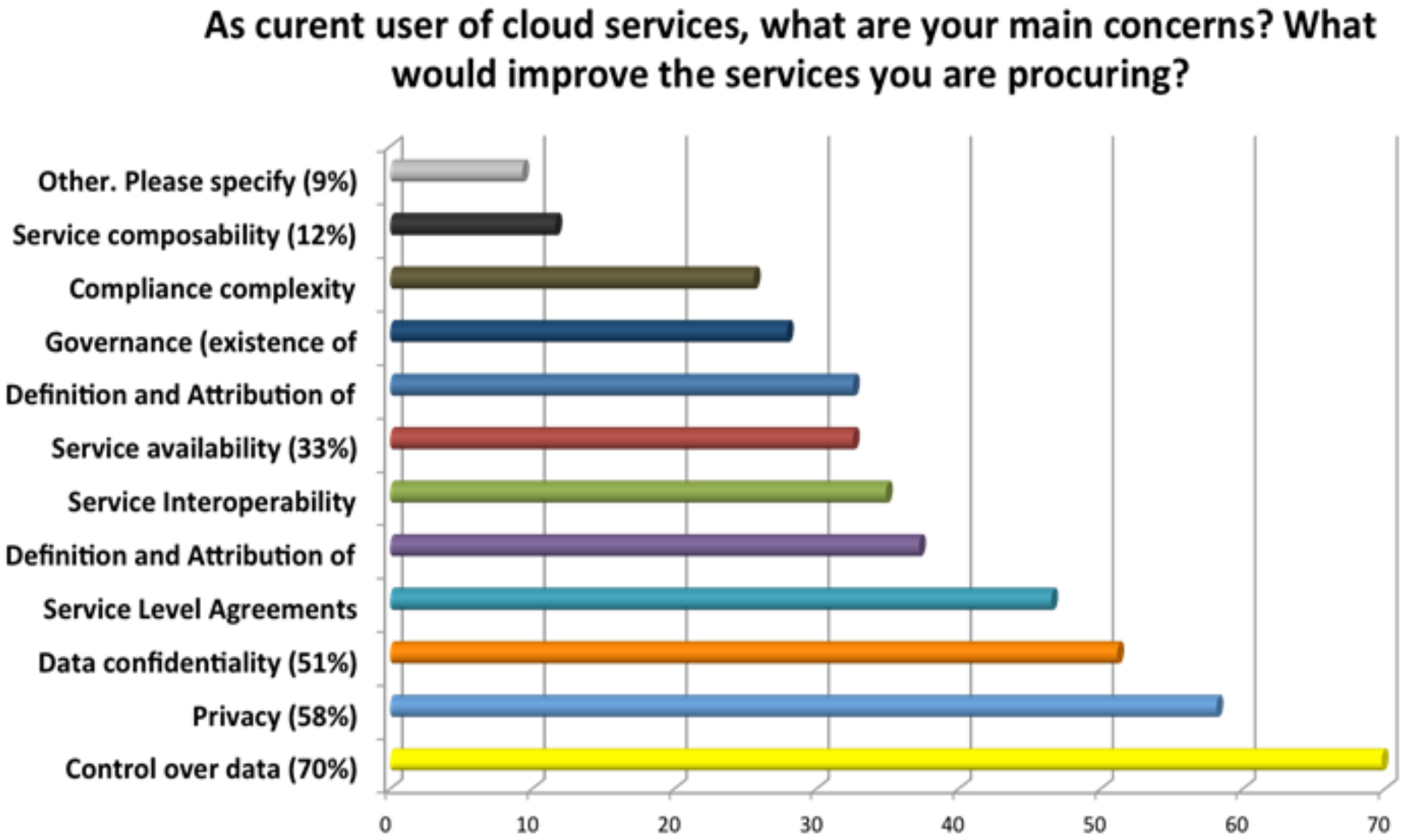


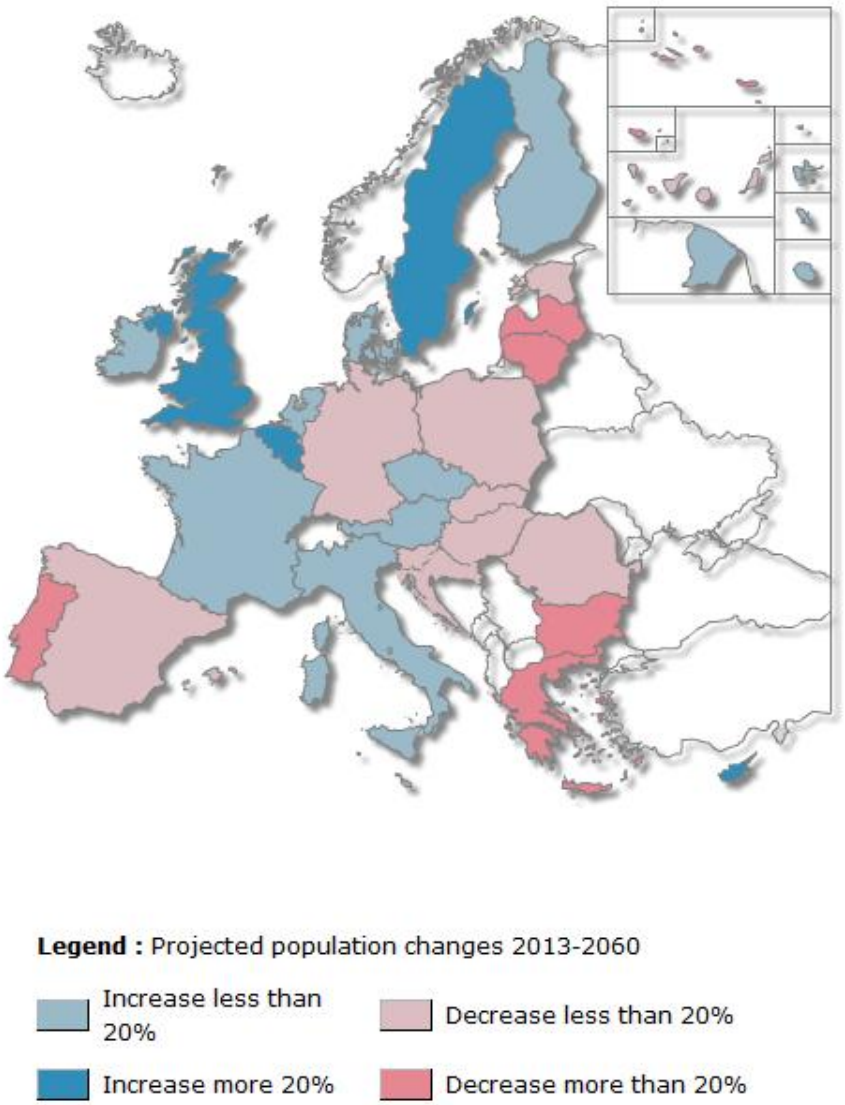
Figure 5: Main concerns in procuring Cloud services

Cloud SLA

Cloud SLAs, SLA Life Cycle & SLA Ready

Arthur van der Wees, Managing Director international law firm Arthur's Legal

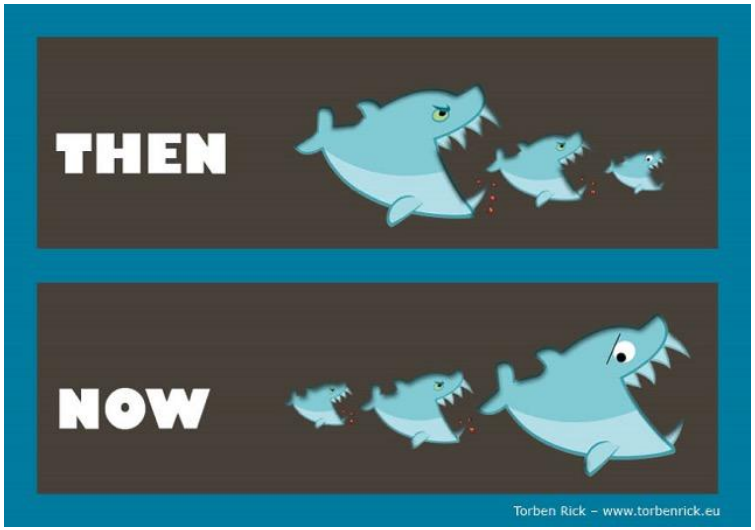
Massive Productivity Growth Necessary: technology is key



government to boosting productivity.

Faced with rapidly ageing populations and slowing employment growth, mature economies need to boost productivity sharply if they are to escape stagnating living standards. To compensate fully for slower employment growth over the coming 50 years, productivity growth would need to be 80 per cent faster than over the past half-century, according to calculations from McKinsey, the consultancy.

Financial Times (26 May 2015)



Risks, Comfort, Trust in & Rewards of the Cloud

✓ Cloud Services Challenges:

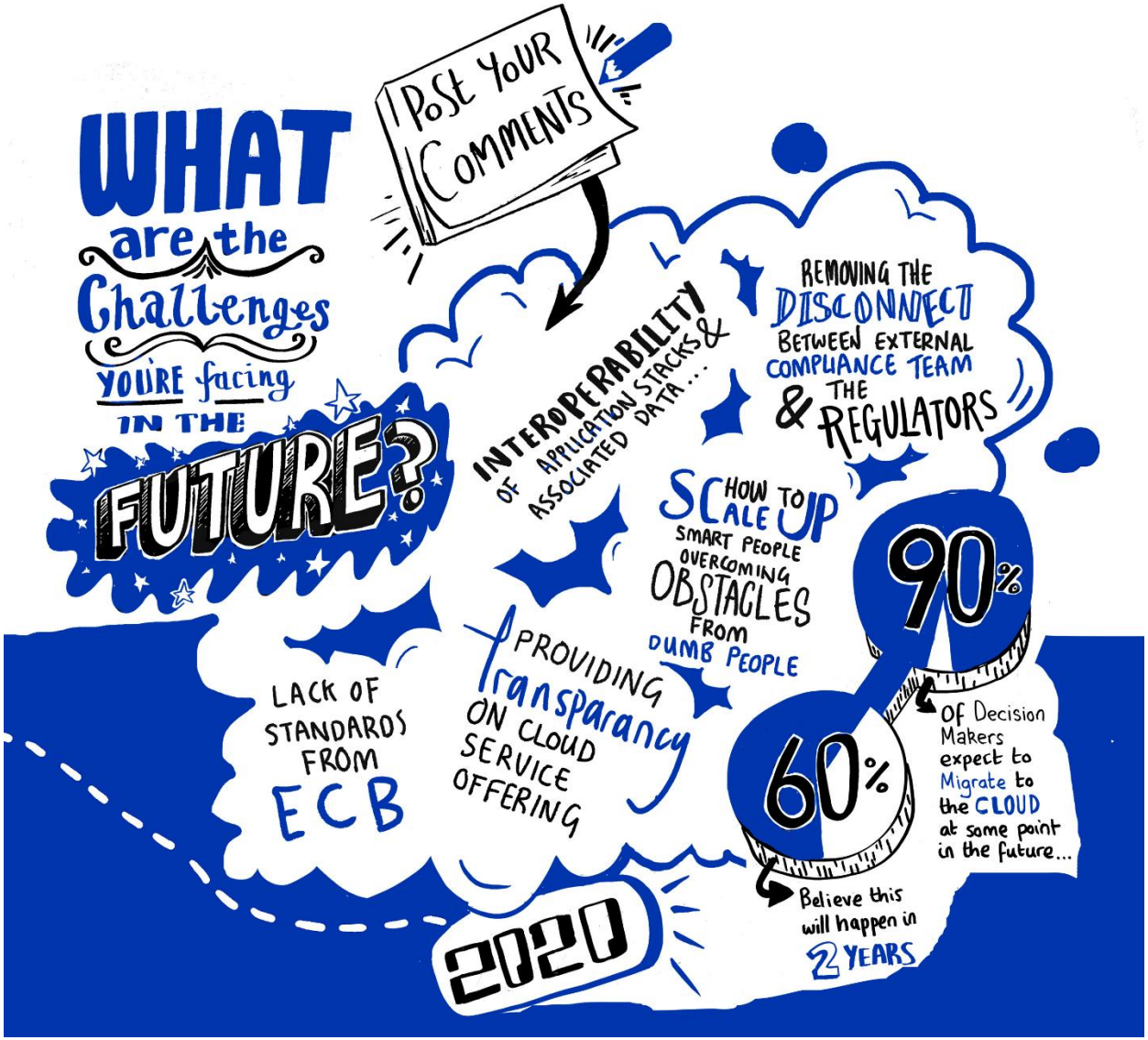
For the 80% not yet using cloud services, **insufficient knowledge** is the main blocking factors (42%).

For the 20% using cloud services, the risk of a **security breach** is the main limiting factor (39%).

Eurostat (EC)

✓ Cybersecurity & Data Protection: Threat or Strength?

Microsoft Azure (ISO 27018)


WHAT are the Challenges YOU'RE facing IN THE FUTURE?
POST YOUR COMMENTS
INTEROPERABILITY OF APPLICATION STACKS & ASSOCIATED DATA...
REMOVING THE DISCONNECT BETWEEN EXTERNAL COMPLIANCE TEAM & THE REGULATORS
SCALE UP HOW TO SMART PEOPLE OVERCOMING OBSTACLES FROM DUMB PEOPLE
LACK OF STANDARDS FROM ECB
PROVIDING Transparancy ON CLOUD SERVICE OFFERING
90% Of Decision Makers expect to Migrate to the CLOUD at some point in the future...
60% Believe this will happen in 2 YEARS
2020

Cloud Computing, SLAs & European Commission

European Commission Priority: Digital Single Market

C-SIG Drafting Group DG CNECT: Select expert group (CSA, IBM, Microsoft, Telecom Italia and Arthur's Legal): EC Cloud SLA Standardisation Guidelines, ISO and other standardisation.

SLA Ready: This 2015/2016 project and its consortium partners help out contributing to a common understanding as well as more standardisation and transparency of cloud SLAs, so companies can make an informed decision what to use and what to expect and trust. @SLAReady

SLA-Ready
Making Cloud SLAs readily usable in the EU private sector

TECHNISCHE UNIVERSITÄT DARMSTADT

Arthur's Legal

cloud security alliance®

Trust-IT Services Ltd
Communicating ICT to markets

NUMERGY
PRODUCTEUR D'ÉNERGIE NUMÉRIQUE

THE FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION
HORIZON 2020

This project has received funding from the EU Framework Programme for Research and innovation H2020 under grant agreement No 644077

Project type: Coordination & Support Action

24 Months:
1 January 2015 - 31 December 2016


01
I'm an SME interested in the cloud but the contract terminology is too confusing
02
I'm confused about how to get the best deal for my cloud contract
03
I'm not sure which cloud delivery options are right for my specific needs
04
I'm worried about uptime and performance on the cloud

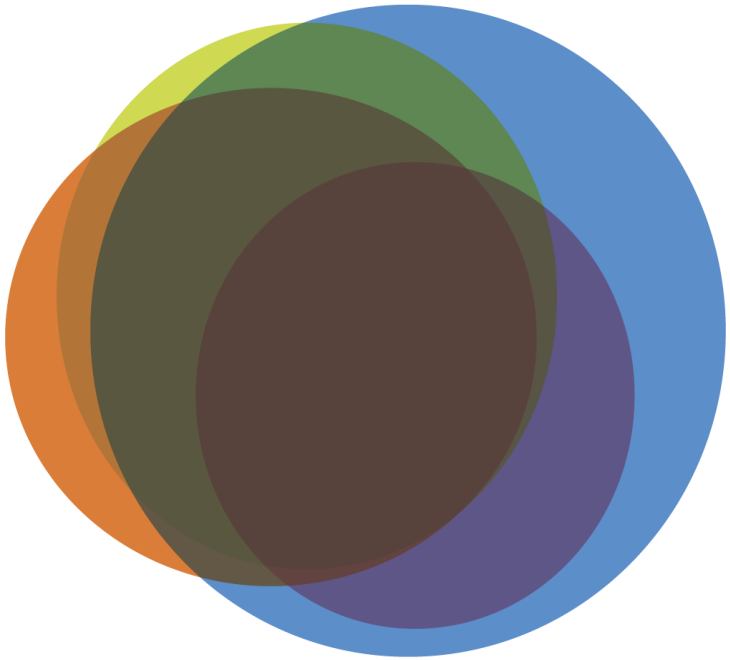
SLA - Ready

Making Cloud SLAs readily usable in the EU private sector

MISSION SLA READY

- **Making Cloud SLAs readily usable in the private sector**
- **Increase the uptake** of cloud computing by making it **easier for SMEs to understand SLAs**
- Improve **transparency** in SLAs for SaaS & IaaS
- Increase the amount of **standardised terms** and **metrics** in SLAs
- **Bridge the disconnect** between supply and demand through common vocabularies
- Provide user-friendly decision making **tools and services**
- Helping out companies to make an **informed decision** about what cloud services to use, and what to expect and trust.

'Contributing to common understanding, more standardization and transparency'

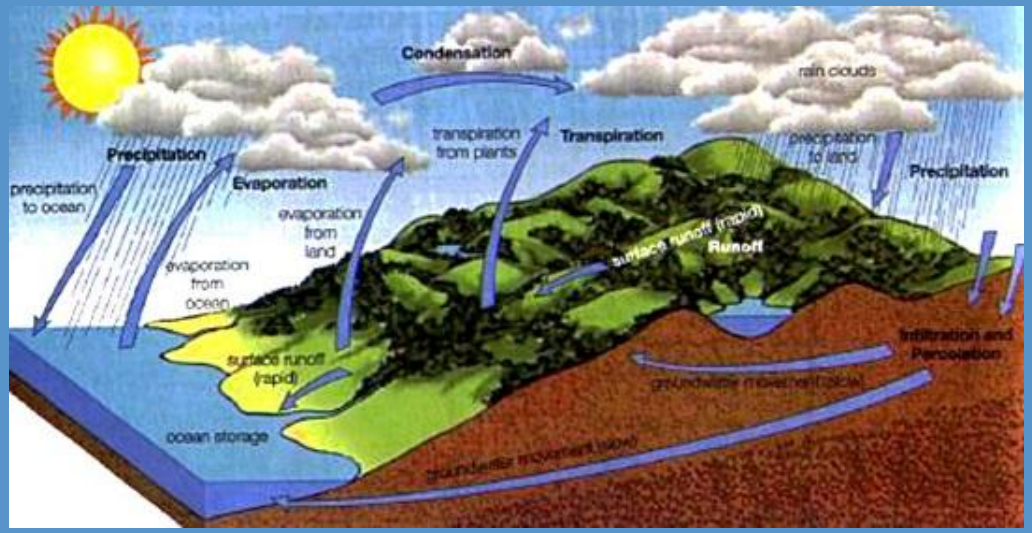


- ✓ EC Cloud SLA Standardisation Guidelines:
- ✓ 4 Main categories Service Level Objectives (SLOs):
  - ✓ Performance
  - ✓ Security
  - ✓ Data Management
  - ✓ Personal Data Protection
- ✓ SLA Life Cycle: Assess, Select, SLA, Execute, Monitor, Update & Terminate
- ✓ Data Life Cycle: Create/derive, Store, Use/Process, Share, Archive, Destroy

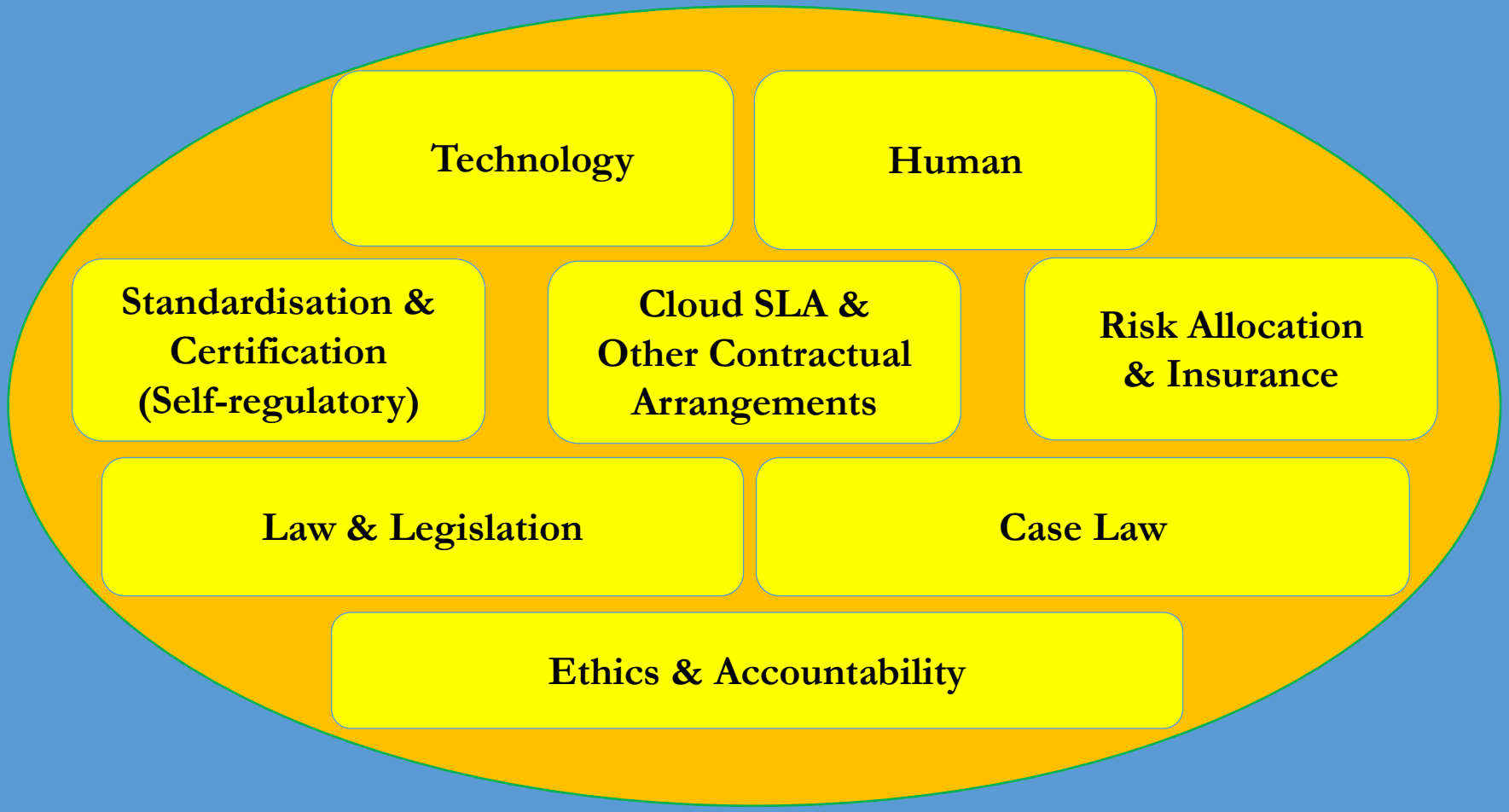
Cloud Service Level Ecosystem

#Cloud #Trust #Strategy #Performance #Security #Data #Data Protection #SLAReady

SLAs are an important but yet only one particle in the Cloud Service Level Ecosystem:



Cloud Service Level Ecosystem



EC Security Service Objectives
Chapter 4 EC SLA Standardisation Guidelines

4.1. Service Reliability
4.2. Authentication & Authorization
4.3. Cryptography
4.4. Security Incident management and reporting
4.5. Logging and Monitoring
4.6. Auditing and security verification
4.7. Vulnerability Management
4.8. Governance
4.8.1. Service changes

Human Factor
Technology
Cloud SLA & Other agreements
Risk Allocation & Insurance
Standardisation & Certification
Law, Legislation & Case law
Ethics & Accountability

The Network and Information Security Directive

Objectives

- Improvement of national security capabilities
- Improvement of national, public & private cooperation
- Adoption of Risk Management Practices in critical sectors
- Reporting of major incidents to the national authorities

Benefits

- More trust in web & e-services for citizens/consumers
- More reliable digital networks/infrastructure for Governments & Businesses
- More reliable services, more equal & stable conditions for the EU economy

Want to take part?

Shape EU Cybersecurity practices on the NIS Platform

@EU_TrustSec

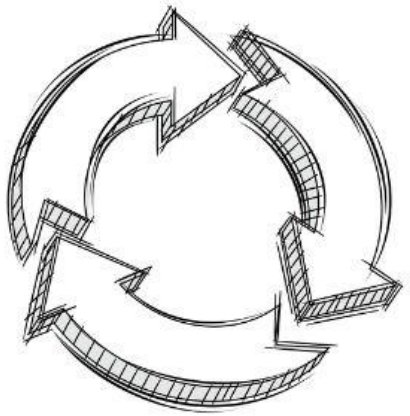
#NIS

More about NIS

Cloud SLA Legal Life Cycle

When zooming in at one (1) SLA from a legal, negotiation and contract management perspective, the life cycle of a SLA can be split in seven (7) headline legal life cycle phases:

1. **Assessment**
2. **Preparation**
3. **Negotiation & Contracting**
4. **Execution & Operation**
5. **Updates & Amendments**
6. **Escalation, and;**
7. **Termination & Consequences of Termination**



State of Practice vs State of Art

- **Current maturity level of Cloud SLAs of CSPs:**

1. Difficult to find, difficult to read & assess: Lot's of push-back at CSPs

2. Performance: Availability, Uptime & Measurements

3. Incident Management: Response time per prioritised incident

4. Carve-outs & other exclusions: 'Planned' Maintenance, Force Majeure, customer, third parties

5. Less than 10% coverage out of the EC SLA Standardisation Guidelines

6. Difficult to monitor, manage & enforce: status.aws.amazon.com (real-time system status & status history (35 days)), trust.salesforce.com (real-time system status & planned maintenance), www.cloudharmony.com/directory (real-time system status & status history (up to 1 year))

Customer is king?

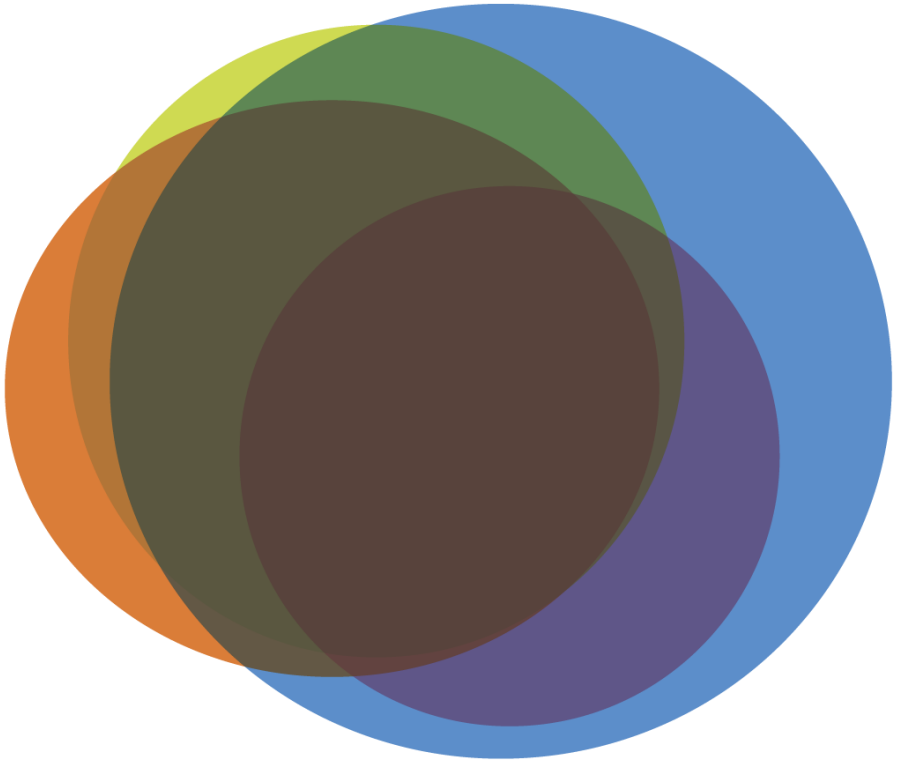
Qualitative vs quantitative Service Levels?

It is a Service! For a customer/user it may be quite different from traditional IT & utilities.

Quality of Living, Mercer: **Vienna (1), Zurich (2), Amsterdam (11), London (40)**

Measuring 36 metrics: Security, International connectivity, Public logistics, Quality of architecture and design, Tolerance, Mobility, Business conditions, Pro-active developments, Environmental responsibility, Medical and other care.

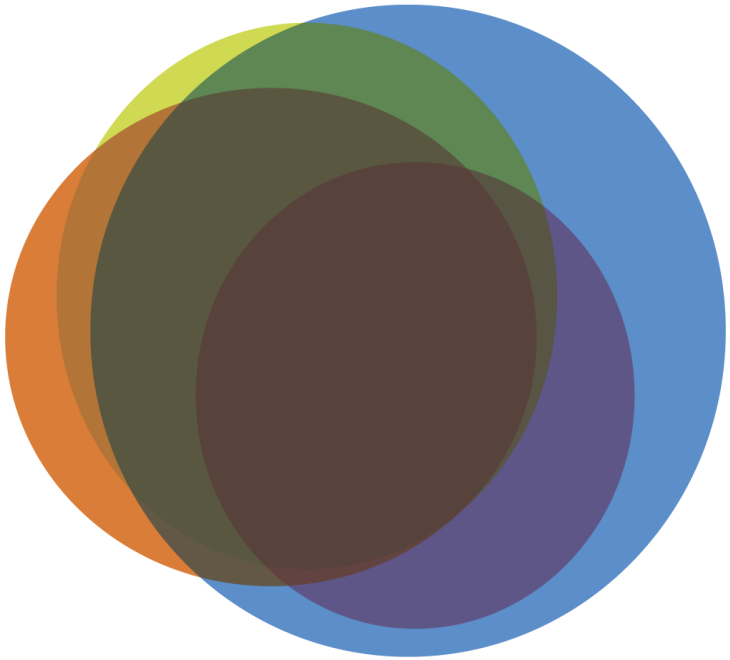
Experience Level Agreement (xLA): it's a feeling! Experience, Perception & Feel versus Facts, Standards & (Post-)commodity



Building block thinking, multi-flavoured, new USPs, upsell potential

#SLA per vertical #SLA per use #SLA for a day # Build your SLA

PRIVACY LEVEL AGREEMENT

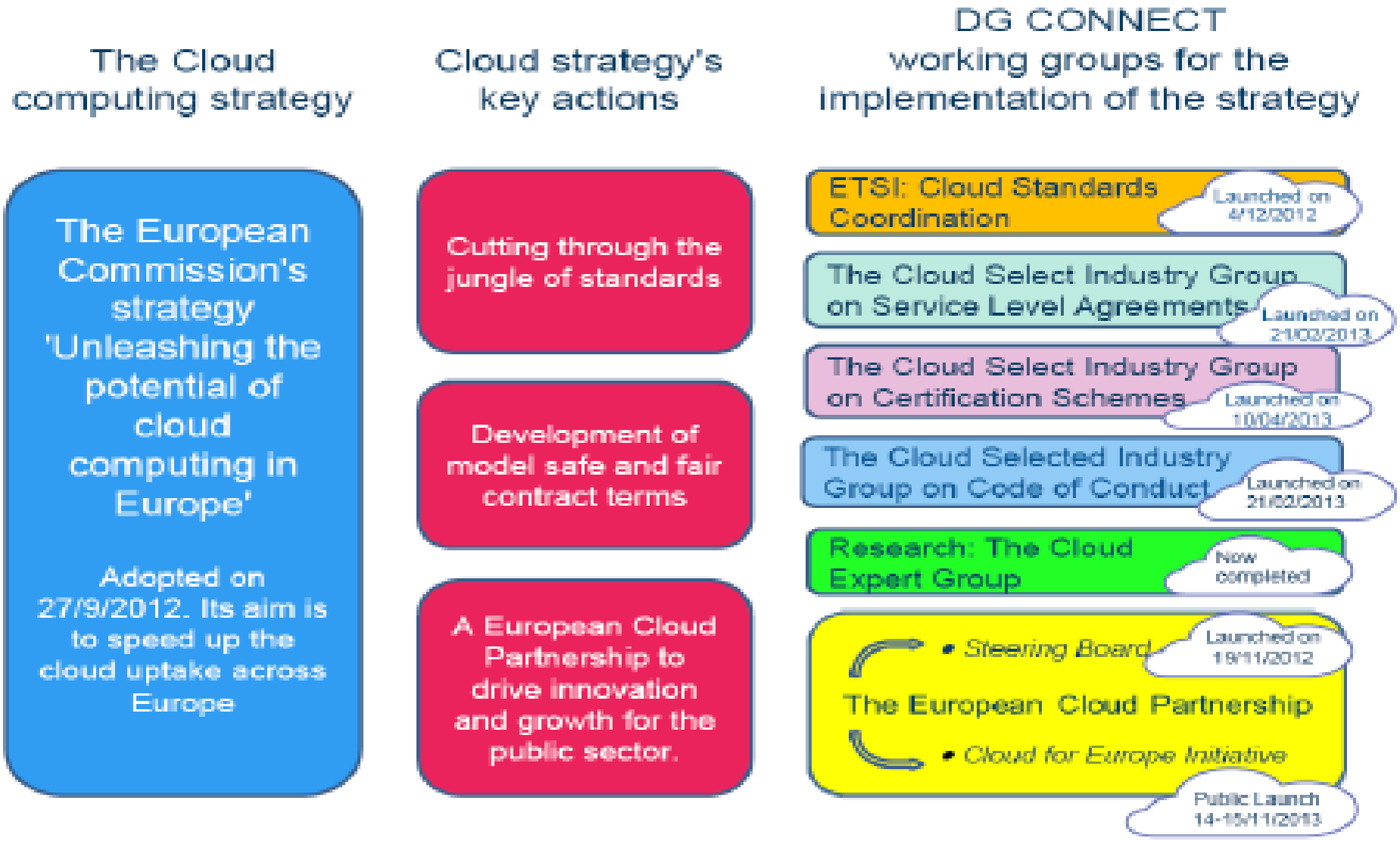


EU Privacy Compliance

CSA PRIVACY LEVEL AGREEMENT and EC CODE of CONDUCT

EC C-SIG
Privacy Code of Conduct

EU Cloud Strategy



Privacy CoC: Purpose and Scope

- The Code is a voluntary instrument, allowing a CSP to evaluate and demonstrate its adherence to the Code's requirements.
- The purpose of this Code is to instil trust and confidence among cloud customers that:
  - the personal data to be processed under the CSP Service Agreement (the customer's personal data) are processed with an appropriate level of data protection;
  - an adhering CSP has met the applicable requirements as set out in this Code related to the processing of personal data, in accordance with the EU Data Protection Directive and its national transpositions.
- The Code applies mainly to Data Processors

Conditions of adherence

- (i) self-evaluation and self-declaration of compliance, or
- (ii) by relying on third-party certification.
- Any CSP may sign up to the Code, irrespective of where personal data is stored and processed. CSPs that have demonstrated their adherence to the Code in accordance with its governance processes may use the Code's relevant compliance marks.

Data Protection Requirements

- Contractual specification of the terms and conditions of the CSP's services
- Processing Personal Data lawfully
- Transfer of the customer's personal data within the CSP's Group
- Transfer of the customer's personal data to a subcontractor
- Right to audit
- Liability
- Cooperation with the customer
- Data Subject complaint handling
- Data Protection Authority request handling
- Confidentiality obligations
- Law enforcement/governmental requests
- Data breach
- Termination of the Services Agreement

Security Requirements

- Availability
- Integrity
- Confidentiality
- Transparency
- Isolation
- Accountability

Status

- CoC was sent to Art29 WP on January 2015 for their review and potential endorsement
- Final (?) feedback expected very soon

PRIVACY LEVEL AGREEMENT

Privacy Level Agreement - PLA V2

EU Compliance Tool

CSA Privacy Level Agreement (PLA [V1])

- Goal:
  - Encourage uniform, consistent and streamlined practices for CSPs in handling personal data
  - Facilitate complete and more relevant disclosures
- Scope & methodology
  - Follows EU Data Protection Directive 95/46/EC principles and EU Commission Proposal for General Data Protection Regulation
  - Addresses WP29 Opinion 5/2012 on Cloud Computing European Data Protection Authorities' guidelines on cloud contracts and use of cloud computing services

DPA's opinions on PLA?

I think [the PLA Outline] is a very helpful document, both for potential customers of CSPs and for CSPs themselves.

By following closely the WP29 Opinion it ensures that both parties understand the obligations under EU law - probably the strictest requirements they will have to comply with.

Hopefully it will be accepted by CSPs that, if they want to be viewed as acceptable service providers - especially by EU-based organisations - they are going to have to be able to answer successfully the questionnaire that is annexed to the document.

Billy Hawkes,
Irish Data Protection Commissioner

Transparency and information are key to build trust in the cloud ecosystem.

This is why the CNIL has actively contributed to the elaboration of the PLA-outline.

As it gets gradually adopted by CSPs, it will become an important building block for constructing a modern ethical and privacy-preserving framework, adequate to the challenges that face all stakeholders in the digital world.

Isabelle Falque-Pierrotin,
President of the CNIL

CSA Privacy Level Agreement (PLA [V2])

- EU compliance tool

Goal:

- Provide CSPs a tool to achieve EU-wide data protection compliance
- Provide cloud customer with a tool to evaluate CSP EU-wide data protection compliance

Scope & Methodology

- Deals with the 'B2B' scenario
- Follows EU current Data Protection Law
- Strongly based on WP29 Opinion 5/2012 on Cloud Computing, written in the light of ISO/IEC 27018, the "Cloud Service Level Agreement Standardisation Guidelines", the work developed by the Cloud Select Industry Group on Code of Conduct, & the Cloud Accountability Project
- Considers differences between CSP-controller and CSP-processor

Privacy Level Agreement V2

1. Identity of the CSP (and of representative in the EU as applicable), its role, and the contact information for the data protection inquiries

1. Ways in which the data will be processed

- Personal data location
- Subcontractors
- Installation of software on cloud customer's system

Privacy Level Agreement V2

3. Data transfer

identify on which legal ground: e.g., EU Commission adequacy decision, model contracts, Safe Harbor, Binding Corporate Rules (BCR)

4. Data security measures

- Availability
- Integrity
- Confidentiality
- Transparency
- Isolation (purpose limitation)
- Intervenability

Privacy Level Agreement V2

5. Monitoring

6. Personal Data breach notification

7. Data portability, migration, and transfer back assistance

Privacy Level Agreement V2

8. Data retention, restitution, and deletion

Data retention policy / Data retention for compliance with legal requirements

Data restitution or deletion

9. Accountability

10. Cooperation

9. Legally required disclosure

PLA V2 Table (Annex 1)

	A	B	AD	AE	AF	AG
1			Mandatory under "EU Data Protection Law"	Mandatory under only some of the EU Member State laws		
2					CSP is Data Controller	CSP is Data Processor
3	1. IDENTITY OF THE CSP (AND OF REPRESENTATIVE IN THE EU AS APPLICABLE), ITS ROLE, AND THE CONTACT INFORMATION FOR THE DATA PROTECTION INQUIRIES	*Specify:*				
4		*- CSP name, address, and place of establishment;*	Yes		Applicable	Applicable
5		*- Its local representative(s) (e.g. a local representative in the EU);*	Yes		Applicable	Not Applicable
6		*- Its data protection role in the relevant processing (i.e., controller, joint-controller, processor, or subprocessor);*	Yes		Applicable	Applicable
7		*- Contact details which the customer can use to submit personal data protection related inquiries.*	Yes		Applicable	Applicable
8		*- Contact details of the Data Protection Officer or, if there is no DPO, the contact details of the individual in charge of privacy matters to whom the customer may address requests.*		Yes	Applicable	Applicable
9		*- Contact details of the Information Security Officer, if there is no ISO, the contact details of the individual in charge of security matters to whom the customer may address requests.*		Yes	Applicable	Applicable
10						
	2. WAYS IN WHICH THE DATA WILL BE PROCESSED.	*If the CSP is a controller, provide details on (i) the purposes of the processing for which the data are intended and the necessary legal basis to carry out such processing as per Article 7 Directive 95/46/EC; (ii) any further information such as:* *- the recipients or categories of recipients of the data,* *- the obligatory or voluntary nature of providing the requested data,* *- the existence of the right of access to and the right to rectify the data concerning the data subject* *in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject (Art. 10 Directive 95/46/EC). Distinguish activities*				

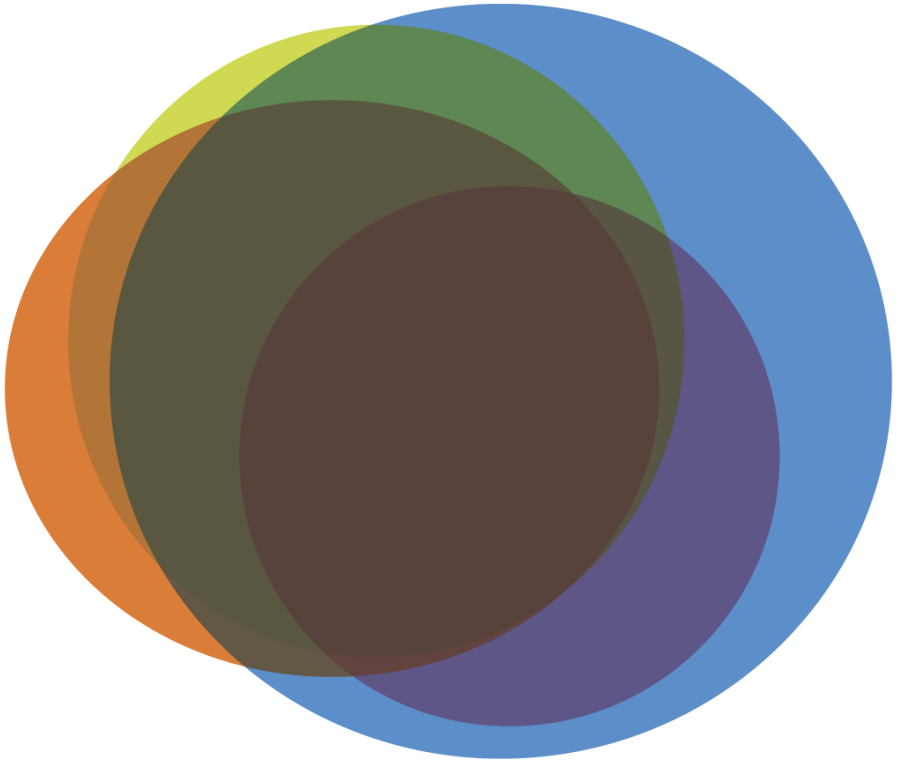
NEXT STEP

PLA [V3] → global version

CLOUD CONTROL MATRIX (CCM)

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE (CAIQ)

WHAT IS THE CCM?



- First ever baseline control framework specifically designed for Cloud supply chain risk management:
  - Delineates control ownership (Provider, Customer)
  - An anchor for security and compliance posture measurement
  - Provides a framework of 16 control domains
  - Controls map to global regulations and security standards
- Industry Driven Effort: 120+ Peer Review Participants
- Participants: AICPA, Microsoft, McKesson, ISACA, Oracle
- Backbone of the Open Certification Framework and STAR

CCM V3.0.1 – 16 CONTROL AREAS

- AIS Application & Interface Security
- AAC Audit Assurance & Compliance
- BCR Business Continuity Mgmt & Op Resilience
- CCC Change Control & Configuration Managemen
- DSI Data Security & Information Lifecycle Mgmt
- DSC Datacenter Security
- EKM Encryption & Key Management
- GRM Governance & Risk Management
- HRS Human Resources Security
- IAM Identity & Access Management
- IVS Infrastructure & Virtualization
- IPY Interoperability & Portability
- MOS Mobile Security
- SEF Sec. Incident Mgmt, E-Disc & Cloud Forensics
- STA Supply Chain Mgmt, Transparency & Accountability
- TVM Threat & Vulnerability Management

136 CONTROLS
Cloud Controls Matrix v3.0

//

133 CONTROLS
Cloud Controls Matrix v3.0.1

CCM v3.0.1

Current Version: Released July 10, 2014

- Builds upon the 5 new domains introduced in v3.0
  - Mobile Security
  - Supply Chain Management
  - Transparency & Accountability; Interoperability & Portability
  - Encryption & Key Management

- Continued improvements in controls including:
  - Language and auditability
  - Reduction of overlapping controls
  - Removed Customer and Provider references within the language

CCM v3.0.1

- New and Updated Mappings including:
  - AICPA 2014 TSC
  - ISO/IEC 27001-2013
  - PCI DSS v3.0
  - NIST SP800-53 R3 App J
  - ENISA IAF
  - 95/46/EC - European Union Data Protection Directive
  - HIPAA / HITECH Act
  - COBIT 5.0
  - Canada PIPEDA
  - COPPA
  - ODCA UM: PA R2.0

CAIQ v3.0.1

Current Version: Released July 10, 2014

- Companion to CSA CCM v3.0.1 and aligned to CSA's Guidance
- Questions mapped to the compliance requirements in CCM v3.0.1
- Helps organizations build assessment processes for cloud providers
- Helps cloud providers assess their own security posture
- Improved cohesion between CCM and CAIQ in v3.0.1
- Questions updated to facilitate STAR measurement

ALIGNMENT CCM & CAIQ

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?
		BCR-07.2		If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?
		BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?
		BCR-07.4		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?
		BCR-07.5		Does your cloud solution include software/provider independent restore and recovery capabilities?

Controls now directly referenced

Numbering & questions linked to control

FUTURE OF CCM

- Continue to improve controls:
  - Auditability & Measurement
  - Clarity
  - Intent
- Revisit the development cycle
- Evaluate additional candidates for mapping

OPEN CERTIFICATION FRAMEWORK (OCF) / STAR Program

CERTIFICATION CHALLENGES

- Provide a globally relevant certification to reduce duplication of efforts
- Address localized, national-state and regional compliance needs
- Address industry specific requirements
- Address different assurance requirements
- Address "certification staleness" - assure provider is still secure after "point in time" certification
- Do all of the above while recognizing the dynamic and fast-changing world that is cloud

DEBATING AROUND CERTIFICATION FOR CLOUD

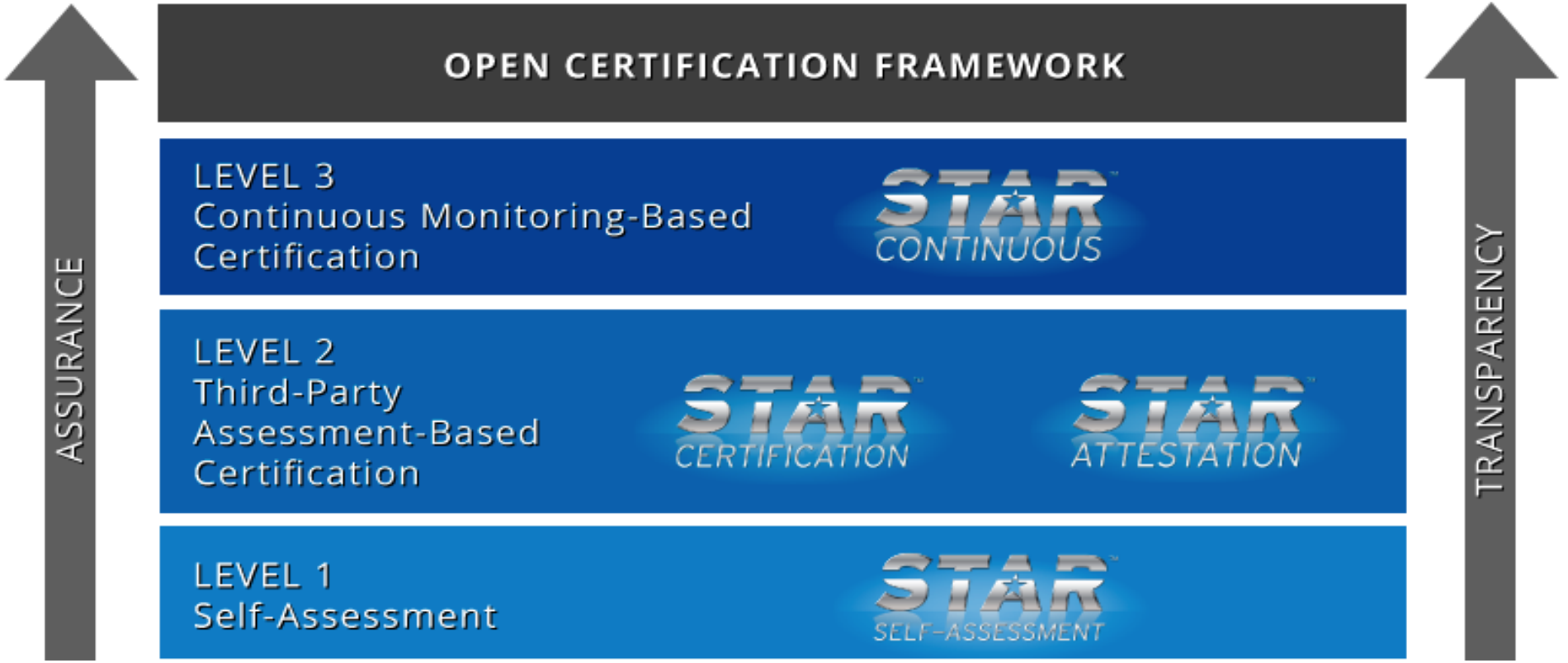
The debate around cloud certification has been based on the following key aspects:

- Suitability of existing security certification/Attestation schemes (e.g. ISO 27001 or SSAE16/SOC1-2-3) for the cloud market vs. the needs to introduce new schemes
- Mandatory vs. voluntary industry driven approaches
- Global vs. Regional/National schemes
- Cost
- Transparency
- Assurance and maturity/capability models

CSA STAR: SECURITY, TRUST & ASSURANCE REGISTRY

- Launched in 2011, the CSA STAR is the first step in **improving transparency and assurance** in the cloud.
- Searchable registry to allow cloud customers to review the security practices of providers, accelerating their due diligence and leading **to higher quality procurement experiences.**
- The STAR is a **publicly accessible** registry that documents the security controls provided by cloud computing offerings
- Helps users to assess the security of cloud providers
- It is based on a multilayered structure defined by **Open Certification Framework Working Group**

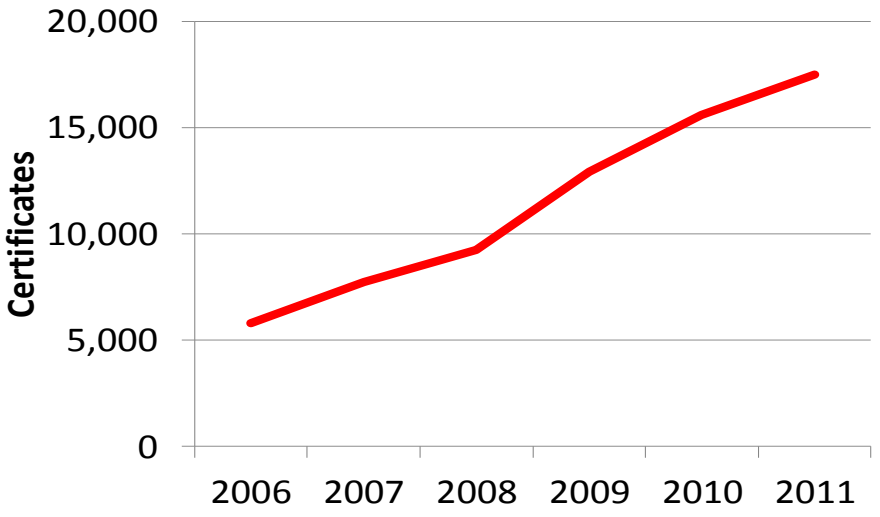
OPEN CERTIFICATION FRAMEWORK



The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.

CSA STAR CERTIFICATION & ISO 27001

- WHY CSA STAR Certification builds on ISO27001?
- Help organizations prioritize areas for improvement and lead them towards business excellence.
- ISO 27001 is the international standard for information security
- Considered as Gold Standard for information security
- There are over 20,000 organisations certified globally in over 120 countries.



ISO 27001 CRITICISMS

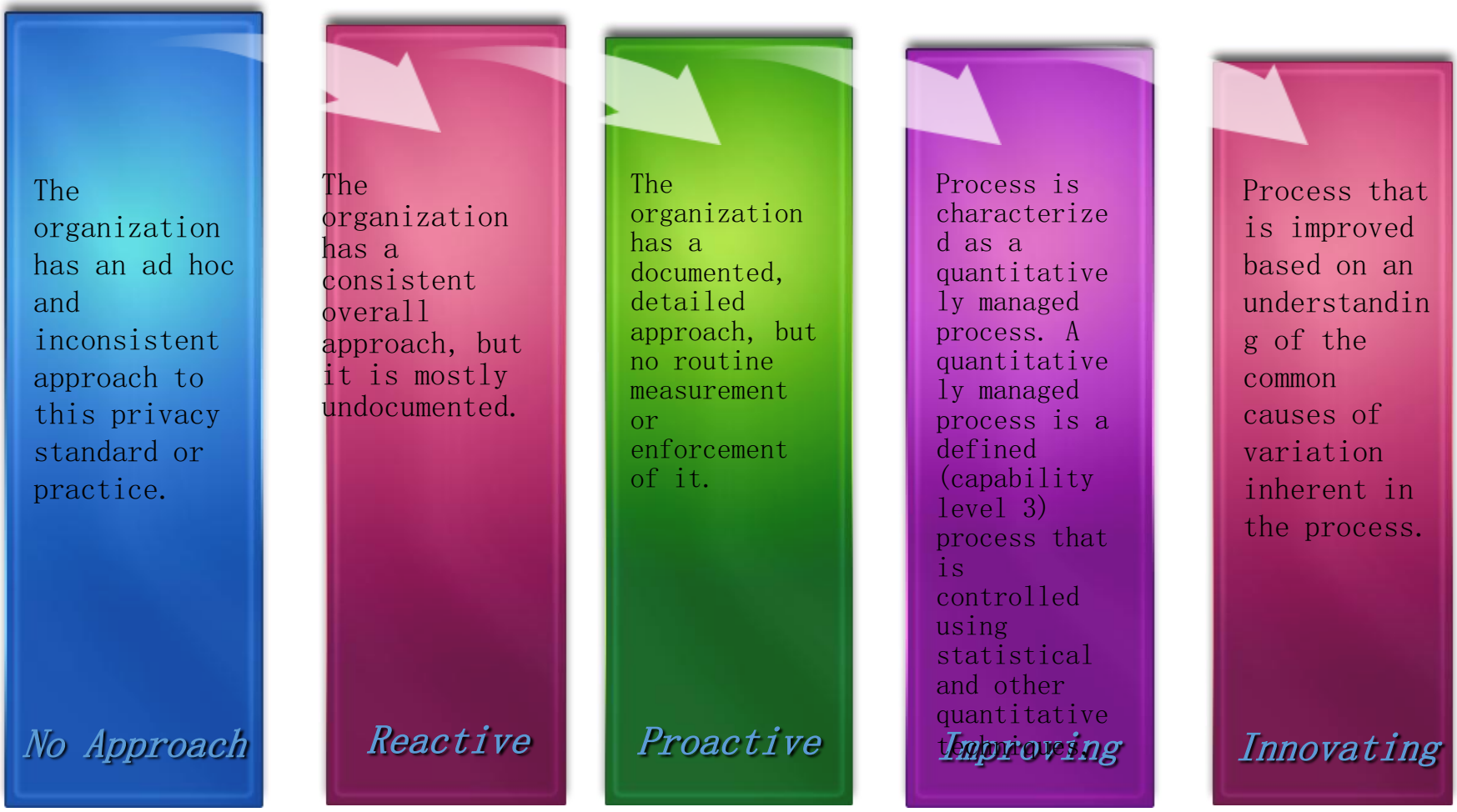
- ISO 27001 is updated every 8 years – the controls become obsolete faster than that
- It is a one size fits all standard but there are some industry specific concerns it does not cover, ie it is not Cloud relevant
- Any standard can become a lowest common denominator
- People can certify any scope they like within their organisation to mislead clients
- It doesn't support transparency

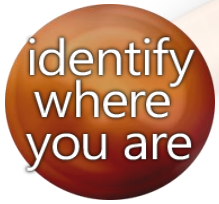
WHAT IS CSA STAR CERTIFICATION?

- The CSA STAR Certification is a **rigorous third-party independent assessment** of the security of a cloud service provider.
- **Technology-neutral** certification leverages the requirements of the **ISO/IEC 27001:2013** & the **CSA CCM**
- Integrates ISO/IEC 27001:2013 with the CSA CCM as **additional or compensating controls.**
- **Measures the capability levels** of the cloud service.
- Evaluates the efficiency of an organization's ISMS and ensures the scope, processes and objectives are **"Fit for Purpose."**
- Based upon the **Plan, Do, Check, Act** (PDCA) approach
- Enables the auditor to assess a company's performance, **on long-term sustainability and risks**, in addition to ensuring they are **SLA driven.**

HOW DO YOU GET THERE?

OPTIMIZATION MODEL





HOW TO TAKE THE JOURNEY

No Approach

The organization has an ad hoc and inconsistent approach to this privacy standard or practice.

Reactive

The organization has a consistent overall approach, but it is mostly undocumented.

Proactive

The organization has a documented, detailed approach, but no routine measurement or enforcement of it.

Improving

Process is characterized as a quantitatively managed process. A quantitatively managed process is a defined (capability level 3) process that is controlled using statistical and other quantitative techniques.

Innovating

Process that is improved based on an understanding of the common causes of variation inherent in the process.

MANAGEMENT CAPABILITY / MATURITY: SCORES

- When an Organization is audited a Management Capability Score will be assigned to each of the control areas in the CCM.
- This will indicate the capability of the management in this area to ensure the control is operating effectively.
- The management capability of the controls will be scored on a scale of 1-15. These scores have been divided into 5 different categories that describe the type of approach characteristic of each group of scores.

Score	Descriptor
1-3	No Formal Approach
4-6	Reactive Approach
7-9	Proactive Approach
10-12	Improvement Based Approach
13-15	Optimising Approach

APPROVING ASSESSORS

- They must demonstrate knowledge of the Cloud Sector
  - Either through verifiable industry experience - this can include though assessing organizations
  - Or through completing CCSK certification or equivalent
- They must be a qualified auditor working a ISO 27006 accredited CB
  - Evidence of conducting ISO 27001 assessments for a certification body accredited by an IAF member to ISO 27006 or their qualifications as an auditor for that organization.
- They must complete the CSA approved course qualifying them to audit the CCM for STAR Certification

ACCREDITED CERTIFICATION BODIES

WHO IS USING CSA STAR?

- Currently 135 Cloud Service Providers Word Wide have decided to be part of the STAR Program!
- That includes companies with either STAR Self Assessment (102) or STAR Certification (30) or STAR Attestation (3)
- Several other in the process of completing their auditing processes

How about Governments & EU Institutions?

Are they requesting CSA

EC and EU Parliament

- The Directorate-General for Informatics (DIGIT) in a tender that aims to secure about 2500 VM & 2500 Terabytes of storage for a number of EU Institutions (75% of the volume will be reserved for the European Parliament, Council and other EU) requests the candidate tenders to make use of the CSA STAR program to show compliance with security requirements established by the European Security Agency (ENISA).

https://etendering.ted.europa.eu/document/document-file-download.html?docFileId=7469

Please check out Annex 2 Security Requirements.

EC and EU Parliament

- The EC is just the last (and surely not the least) that recognises the values of our certification and assurance program, prior to them other Governments (e.g. UK, Spain, Taiwan, Singapore, Canada, etc.) has made direct reference to STAR and CCM.

UK G-Cloud example

CESG

See more information about this Guidance

Guidance

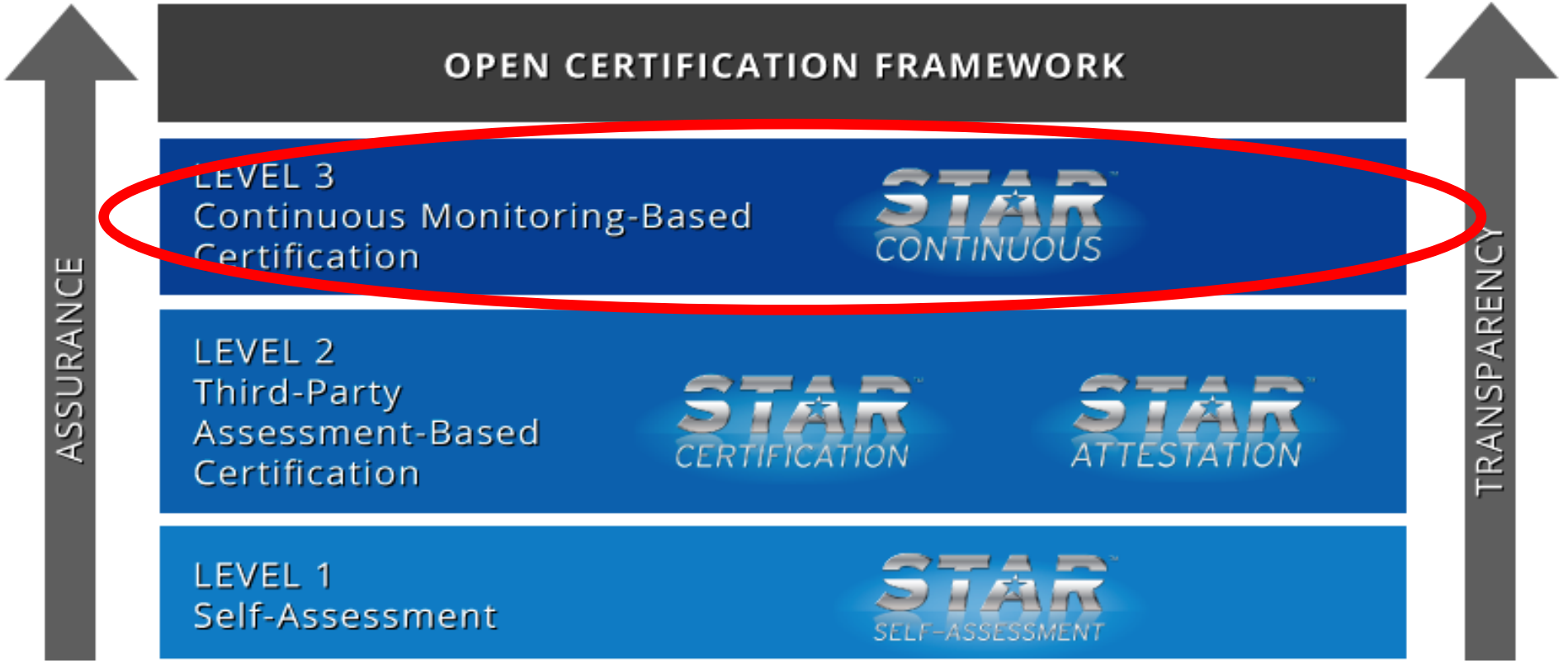
Implementing the Cloud Security Principles

Published 23 April 2014

Table 1: Common approaches to implementing objectives

Standard	Guidance on certification
ISO/IEC 27001:2005 or ISO/IEC 27001:2013	It is possible to be certified as compliant with ISO/IEC 27001:2005 or ISO/IEC 27001:2013. Since the scope of the certification can be specified by the organisation being certified, when using this mechanism to demonstrate implementation of one of more Cloud Security Principles it is recommended that the scope be verified as covering the right aspects. The individual performing this review should have the qualifications referenced in Table 1. ISO/IEC 27001 certification will not verify that the controls implemented by the service provider are effective. When relying on ISO/IEC 27001 certification, consumers should note that the United Kingdom Accreditation Service (UKAS) is the only national accreditation body recognised by government to assess organisations that provide certification services. ISO/IEC 27001 audits performed by bodies not recognised by UKAS may reduce the confidence that consumers can place in their quality.
Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v3.0	CSA CCM v3.0 compliance is achieved through CSA's STAR scheme. Consumers are advised that the first level of STAR is 'self-assessment' - service providers referencing STAR at this level should be considered to fall into the 'Service provider assertion' category above. The remaining levels of STAR ('certification', 'attestation' or 'continuous') should be considered to fall in the 'Independent validation of assertions' category. As with ISO/IEC 27001:2005 or ISO/IEC 27001:2013 it is recommended that a qualified individual verify the scope and implementation of controls to ensure they support implementation of the Cloud Security Principles claimed. The individual performing this review should have the qualifications referenced in Table 1.

OPEN CERTIFICATION FRAMEWORK



The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.

OCF Level 3

CSA STAR CONTINUOUS

- CSA STAR Continuous will be based on a continuous auditing/assessment of relevant security properties.
- It will built on the following CSA best practices/standards:
  - Cloud Control Matrix (CCM)
  - Cloud Trust Protocol (CTP)
  - CloudAudit (A6)
- CSA STAR Continuous is currently under development and the target date of delivery is 2015.

THANK YOU!

CONTACT US

Daniele Catteddu; Managing Director EMEA, Cloud Security Alliance

Twitter: @DanieleCatteddu

@CloudSA

dcatteddu@cloudsecurityalliance.org

star-help@cloudsecurityalliance.org

https://cloudsecurityalliance.org/star/

http://picse.eu

http://specs-project.eu/

CONTACT US

Please check:

www.arthurslegal.com

www.zappliedplatform.com

www.sla-ready.eu

Follow us:

@Arthurslegal

@Zapplied

@SLAReady

Arthur's Legal
Challenge the status quo

CONTACT US

Dr. Paolo Balboni,
paolo.balboni@ictlegalconsulting.com
Chair - CSA Privacy Level Agreement Working Group;
Founding Partner - ICT LEGAL CONSULTING;
Scientific Director - European Privacy Association

InfoSecurity Europe 2015
Olympia, United Kingdom
4 June 2015

Follow @balbonipaolo