Trilateral Research & Consulting

European Commission

Cloud-Select Industry Group Meeting

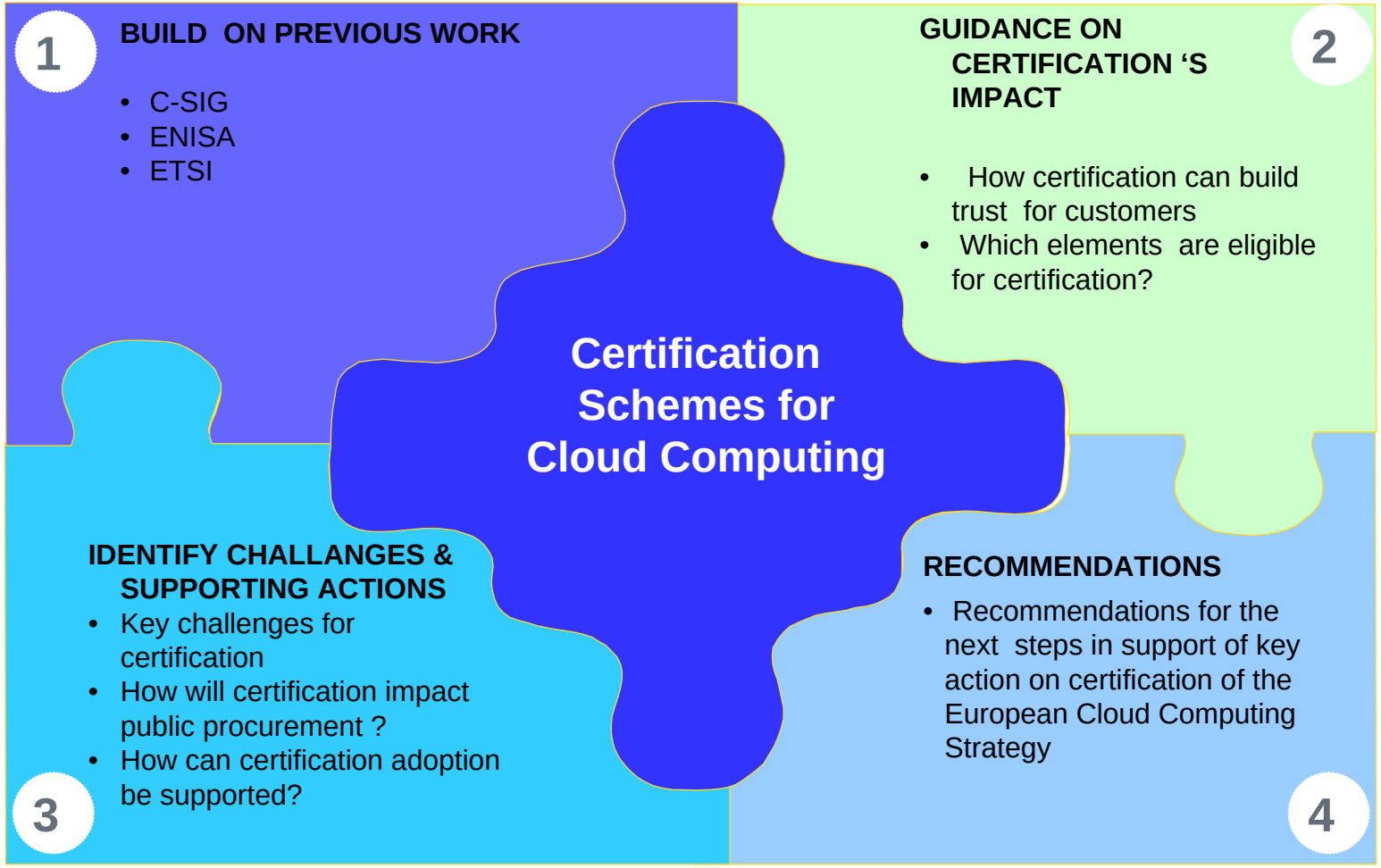
CERTIFICATION SCHEMES FOR CLOUD COMPUTING ?

Monica, Lagazio, Trilateral Research & Consulting

DG CONNECT

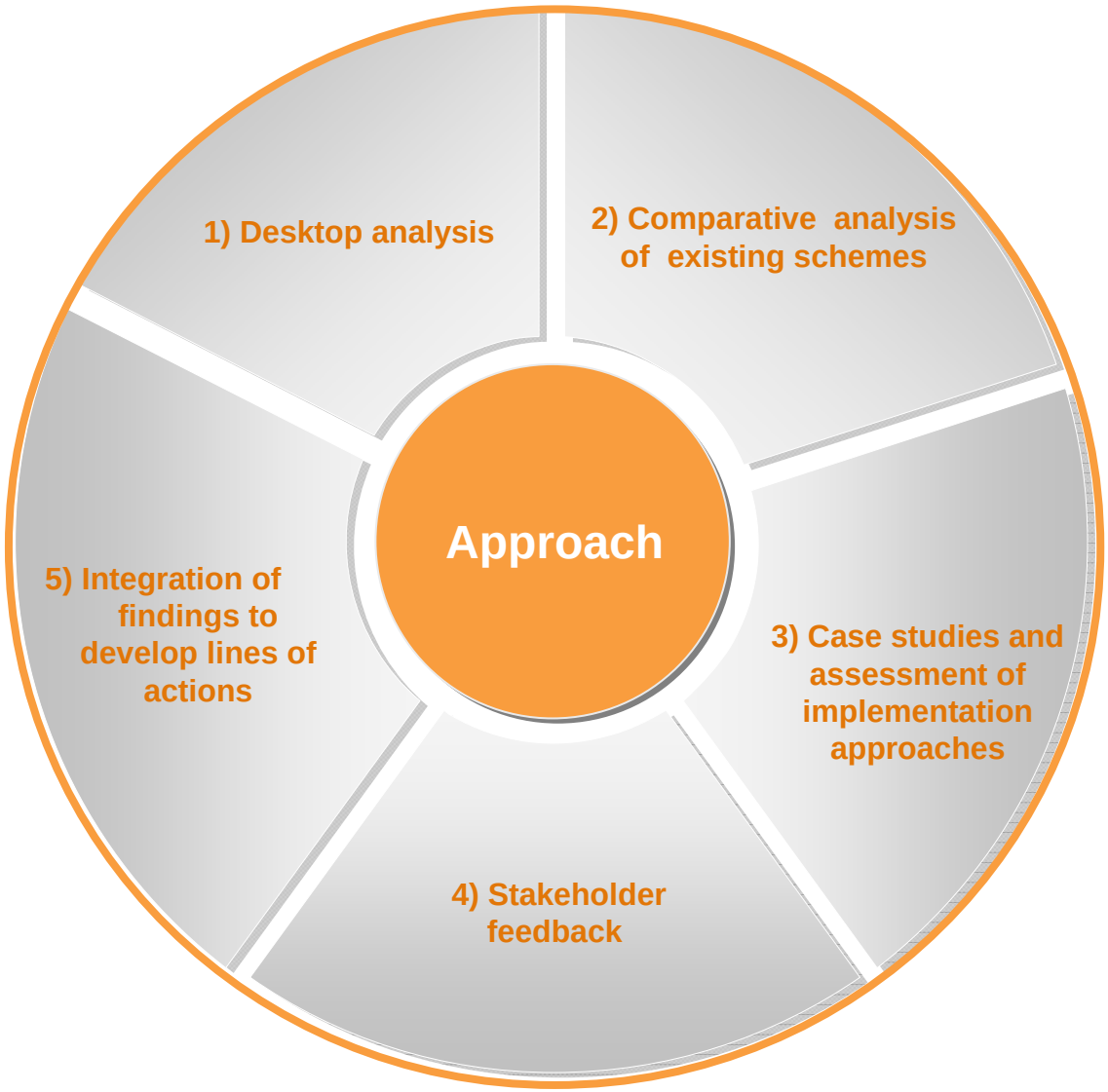
May 19, 2014

The objective of the study is to analyse existing cloud relevant certification schemes, identify benefits and challenges, and formulate recommendations for the next steps of the Commission for its action on certification as part of the Cloud Strategy



We have used a combination of methods to arrive to the key findings of the study and develop the recommendations

1) **Desktop analysis:** existing material and insights by C-SIG, ENISA, ETSI, IDC, EU policy papers, EuroCIO analyses
2) **Comparative analysis of existing schemes:** 24 schemes based on the list compiled by C-SIG and added a few additional schemes to cover more recent developments
3) **Case studies:** 7 non-cloud case studies (in information security, product, environment, finance and entertainment) and 3 implementation approaches (self-regulation, co-regulation, statutory regulation)
4) **Stakeholder feedback:** workshop in Amsterdam, April 2014 and further comments
5) **Integration of findings:** recommendations developed based on all the key findings



Key findings on existing schemes: Security is the most common focus for the cloud computing relevant certification schemes analysed (with general certification schemes covering several aspects of cloud computing security)

Certification schemes by focus and function

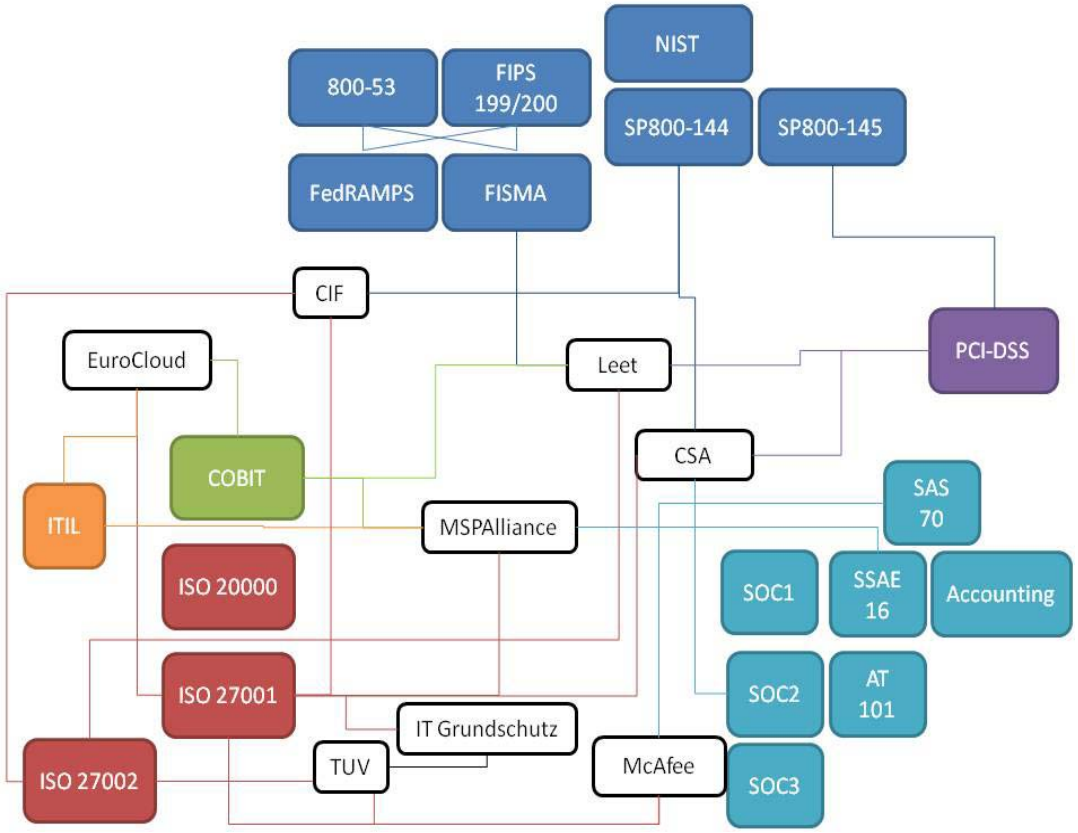
Focus /Function	General	Privacy Data Protection	Inter-operability	Security	Service Management	Reliability /access
Standard			OCCI	ISO/IEC 27001/2, PCI-DSS, CSA CCM	ISO/IEC 20000	
Code of Practice	NZ Code of Practice	NZ Code of Practice*	NZ Code of Practice*		NZ Code of Practice*	NZ Code of Practice*
Self-certification	CIF			CSA STAR self assessment*	NIST SP800-144	
Register	CSA STAR Register	CSA Star*	CSA Star*	CSA STAR Register		
Seals	TRUSTe, Confianza	EuroPriSe, ESRB		Comodo, Leet, TRUSTe, Confianza, EuroPriSe*		
Audit	EuroCloud	MSPAlliance	MSPalliance EuroCloud*	CSA STAR Certification*, CSA STAR Attestation* ISO/IEC 27001/2, FedRAMP, FISMA	MSPAlliance, SOC 1-2-3, ISO/IEC 20000	TUV Trusted Site
Certification-as-a-Service			MSPalliance*	McAfee Cloud Secure		

Key features

- International
- Private sector
- Multiple trust models, but audit dominant method
- No general cloud standards as such much more general focused
- Security relatively well covered
- Focus upon enterprise rather than individual customer
- Not aligned with GDPR but some schemes could adapt to it.

Key findings on existing schemes: There are six main standards families that are related to certification schemes

Certification schemes and standards families



Key features

- A core set of standards families
  - › Integrative certification schemes blend these
  - › High level of interconnection among the cloud computing certification schemes analysed
  - › Many draw on the similar base standards and refer to each other
- Certification available at a number of levels (products, services, CSPs, service organisations, organisations)

Key findings: Certification could lead to more trusted cloud services overall, however the implication for implementing certification varies based on which element of cloud services is certified

Legal jurisdiction and location	Security and performance	Privacy and confidentiality	Service level agreement	Interoperability and portability	Governance, and supply chain
Impact ▪ Increase trust by supporting good will ▪ Beside certification other mechanism needed (e.g., model contract and SLA) ▪ It requires international co-operation	**Impact** ▪ Increase trust by increased transparency and flexibility ▪ Increase adaptability and flexibility	**Impact** ▪ Contribute to build trusted cloud services by supporting customers' obligations ▪ Low cost of due-diligence	**Impact** ▪ Build trusted paths for cloud services via increased transparency and accountability, and risk transfer	**Impact** ▪ Increase trust by increased transparency and flexibility	**Impact** ▪ Increase trust by increased transparency
Implementation ***Full-approach*** ▪ Significant resources and knowledge from the certification providers, and CAs ▪ Less flexible cloud services and high investment for CSPs ▪ Need to develop international framework and governance ***Light touch*** ▪ Less onerous for certification providers, CAs and CSPs	**Implementation** ▪ Relatively easy to improve existing schemes (low impact on certification providers and CSPs) ▪ Some light monitoring within a self-regulatory context (low impact)	**Implementation** ▪ Audit-based schemes use to audit for privacy (low impact) ▪ Some initial efforts to support privacy requirements for CSPs ▪ Some light monitoring within a self-regulatory context (low impact)	**Implementation** ▪ High financial , resources and organisational efforts from certification providers ▪ High efforts for CAs (new CAs to provide insurance) ▪ Moderate efforts from EU and MS to support the development of balanced standards for SLA	**Implementation** ▪ Some elements in existing schemes (low investment from certification providers) ▪ Moderate to high investment from cloud providers ▪ Low to moderate efforts from CAs, EU and MS to support the development and implementation of standards	**Implementation** ▪ Relatively easier to widen existing schemes (low impact) ▪ Sophisticated CSPs will easily adapt and endorse new requirements ▪ Some light monitoring within a self-regulatory context (low impact)

Key findings: Our overall analysis indicates that several elements of cloud services could be considered for certification

Element of Cloud Services	Level of customer demand	Impact of certification on trust	Feasibility for certification	Could this element be considered for certification?
Legal jurisdiction and location	Very high	Moderate	Low	Partially Other mechanisms may be more effective
Security and performance	Very high	High	High	Yes
Privacy and confidentiality	Very high	High	High	Yes
Service Level Agreement (SLA) including accountability and liability of providers	High	High	Moderate	Yes
Interoperability and portability	High	High	Moderate	Yes
Governance, and service and supply chain management	Moderate	High	High	Yes

Key findings: Existing cloud schemes face some trust challenges, applicable, with different degrees, to different elements of cloud services

Specific Trust Challenges	
Challenges	**Relevance**
▪ Lack of clear guidance for compliance with relevant legislation and industry regulation	▪ Privacy and confidentiality
▪ Lack of clear alignment with customer requirements and application domains	▪ All elements
▪ Lack of clear accountability, risk transfer mechanisms and transparency	▪ All elements
▪ Lack of clear, third-party oversight process	▪ All elements
▪ Lack of clear adaptive mechanisms	▪ All elements
▪ Lack of recognition and user awareness	▪ All elements
▪ Lack of enforcement power	▪ All elements
▪ Lack of further harmonisation and common domain standards	▪ Privacy and confidentiality, interoperability and portability, legal jurisdiction, SLA and governance
▪ Lack of clear added value for participants	▪ Privacy and confidentiality, interoperability and portability, legal jurisdiction, SLA and governance
▪ Lack of perceived independence	▪ All elements

Key findings : The public sector has an important role to play in cloud adoption. Some initiatives are driving cloud adoption at the procurement stage, often supported by certification

European Context

- **The European cloud strategy recognises the importance of the public sector in "shaping the cloud computing market" (i.e., the public sector is the EU's largest buyer of IT)**

- **European Cloud Partnership (ECP)**
  - *Context*: Bring together industry and public sector to support clod adoption
  - *Focus*: Work on common procurement requirements for the public sector
  - *Certification*: Views voluntary cloud certification schemes as a means to facilitate cloud adoption in the public sector and support cloud certification schemes in Europe and their recognition by public authorities. Trusted Cloud Europe (TCE) recognizes cloud certification as a best practice.

- **Cloud 4 Europe (C4E)**
  - *Context*: 42-month research initiative (FP7) , which was officially launched with a conference in Berlin on the 14 November 2013.
  - Focus: Identify public sector pre-commercial procurement requirements and usage scenarios for cloud computing (specifically for public administration)
  - *Certification*: Reflect on the role that cloud certification could play in pre-commercial procurement and the development of trusted cloud services in the public sector across Europe.

- **G-Cloud**
  - *Context*: Support the UK public sector when procuring cloud services by providing a set of cloud services that are common among a broader group of public users
  - *Focus*: Set of procurement frameworks , which allow the whole of the UK public sector to buy cloud-based services through a marketplace called the 'CloudStore
  - *Certification*: Security accreditation is required for all services which will hold data at a specified 'Business Impact Level profile' and above (categorisation of government services based on the sensitivity of data.) Accreditation fis carried out by the Pan Government Accreditation service operating under the authority of the G-cloud Senior Information Risk Owner (SIRO).

Adoption takes

- **Procurement as a key channel for cloud adoption in the public sector**
- **Supportive initiatives for addressing fragmentation and lack of public trust in cloud services**
- **Cloud certification as an effective tool for supporting efficiency in the procurement phase by means of standardised processes and procedures**

Key findings: Drawing from these initial initiatives, future directions to further enhance public sector adoption of cloud in Europe could have certification as an important facilitator

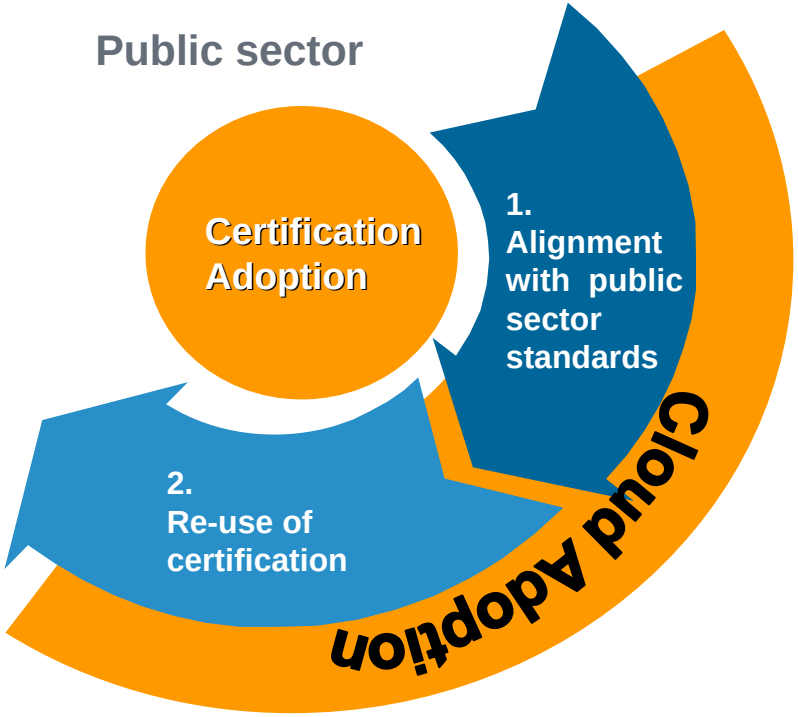
Way Forward :

Further steps in promoting certification could focus on:

1. ***Further development of cloud certification to align to public sector standards/requirements across Europe***
2. ***Further adoption and re-use of cloud certification and/or accreditation by public administrations across Members States based on mutual recognition***

KEY BENEFITS

- **Reduce cost of procurement for public sector and cloud providers**
  - **Speed up and facilitate cloud procurement and due diligence**
- **Create trusted cloud services for public sector across Europe**
- **Promote one single market based on a larger economy of scale**



By integrating the key findings of the analysis, we have identified 7 possible lines of actions:

1 Extend cloud certification

Extend cloud certification to cover additional elements of cloud services

2 Alignment to customers' requirements

Support greater alignment to customers' requirements

3 Establishment of regulatory governance

Establish regulatory governance to support transparency and accountability

4 Regulatory oversight

Regulatory oversight: Accreditation of certifiers by regulators or a newly established industry body

5 Promote standardisation where lacking

Promote and facilitate standardisation in areas where this is presently lacking (e.g., SLA, legal jurisdiction),

6 Development of risk transfer mechanisms

Development of risk-transfer mechanisms for liability and accountability

7 Integration of national accreditations

Integration of national cloud accreditation schemes for public procurement via mutual recognition

Thank you

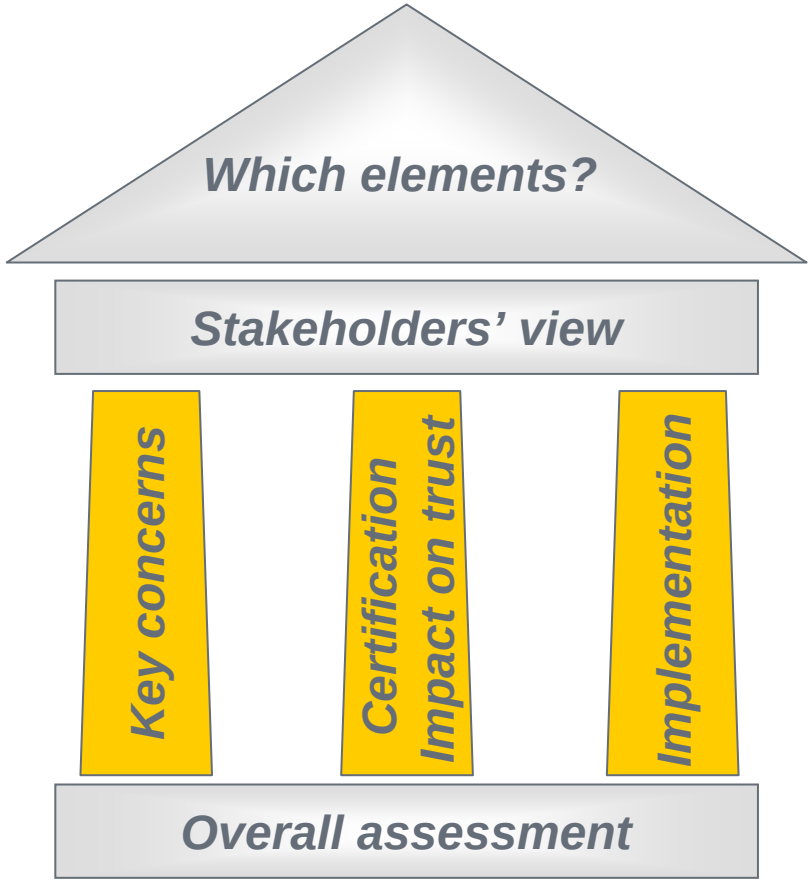
Appendix

Appendix: the 24 analysed schemes

- Cloud Industry Forum Self-Certification scheme
- Cloud Security Alliance Open Certification Frameworkj
- COBIT
- Comodo Secure
- Confianza Online
- ESRB Privacy Certified
- Eurocloud Star Audit SaaS
- EuroPriSe
- FedRAMP
- FISMA
- ISO 20000
- ISO/IEC 27001I
- T-Grundschutz
- McAfee Cloud Secure
- Leet Security Rating
- MSPAlliance Unified Certification Standard
- New Zealand Cloud Computing Code of Practice
- NIST SP800-144
- Open Cloud Computing Interface
- Payment Card Industry Data Security Standard (PCI-DSS)
- SOC 1-2-3
- TRUSTe Cloud Data Privacy Certification Program
- TUV Trusted Site

To identify which elements could be certified we assessed key stakeholders' view with focus on key concerns for adoption, how certification can enhance trust and complexity of implementation

- Key concerns for cloud adoption (based on IDC questionnaire)
- How certification could address key concerns by increasing trust
- Some directions on complexity of implementation (i.e., burdens on certification providers, cloud providers, certification subscribers, EC and MS)



Key findings: By assessing seven non-cloud case studies we have identified general challenges arising from efforts to implement certification schemes in Europe

General Lessons Learned

Short-comings	Key Requirements
▪ Gaps in underlying (technical or regulatory) framework ▪ Lack of adequate support from Member States (and consequent lack of acceptance, technical barriers) ▪ High levels of national variations in implementation and enforcement - difficulty of ensuring consistency ▪ Resistance to and mistrust of scheme (i.e., actual delivery of benefit) ▪ Fraudulent use of marks, logos (counterfeiting) ▪ Administrative burdens ▪ Competition and confusion with other logos ▪ Free riding (i.e., clear responsibility for enforcement) ▪ Over protectionism (i.e., encourage and support acceptance in EU and beyond the EU) ▪ Ambiguity and complexity of legislative requirements	▪ Clear policy goal for the certification scheme ▪ Harmonised rules for implementation of the scheme and use of the mark/logo (e.g., among national authorities and industry) ▪ Additional legal rules to strengthen credibility of scheme and provide support (providing credibility and incentive) ▪ Robust (yet adaptable) certification criteria ▪ Clear and uniform framework of standards and scheme criteria (also clear and unambiguous language) ▪ Key stakeholder confidence and support ▪ Access mechanisms for certifiers and/or authorities to the certified service ▪ Adequate and meaningful monitoring and enforcement (including efficient market surveillance) ▪ Measures for regular review, improve and make innovations to the scheme ▪ Sustainability ▪ Dedicated body or bodies overseeing the scheme's design, implementation and innovation.

Line of actions	(1)Extend cloud certification to cover additional elements of cloud services	(2) Greater alignment to customers' requirements, including scalability, flexibility and cost efficiency	(3) Establish regulatory governance to support transparency and accountability	(4) Regulatory oversight: Accreditation of certifiers by regulators or a newly established industry body	(5) Promote and facilitate standardisation in areas where this is presently lacking	(6) Development of risk-transfer mechanisms for liability and accountability	(7) Integration of national cloud accreditation schemes for public procurement via mutual recognition
Objective	-Promote cloud adoption -Respond to customer needs	-Promote cloud adoption -More effective and efficient procurement process (i.e., speed up due diligence) -Development of trusted cloud services	-Promote cloud adoption -Development of trusted cloud services	-Promote cloud adoption -Development of trusted cloud services -Promote harmonisation and single market	-Promote cloud adoption -Respond to customer needs -Promote harmonisation and single market -Development of trusted cloud services	-Promote cloud adoption -Development of trusted cloud services	-Promote cloud adoption -Promote single market -Facilitate and reduce cost of public procurement -Development of trusted cloud services
Addressed challenges	-Lack of clear alignment with customers' requirements and application domains	-Lack of clear alignment with customers' requirements and application domains -Lack of clear guidance for compliance with relevant legislation and industry regulation -Lack of clear added value for participants	-Lack of clear accountability and transparency -Lack of clear guidance for compliance with relevant legislation and industry regulation -Lack of perceived independence	-Lack of clear accountability and transparency -Lack of recognition and user awareness -Lack of clear guidance for compliance with relevant legislation and industry regulation -Lack of further harmonisation and common domain standards -Lack of perceived independence -Lack of enforcement	-Lack of clear alignment with customer requirements and application domains -Lack of further harmonisation and common domain standards	-Lack of clear accountability, risk transfer mechanisms and transparency	-Lack of further harmonisation and common domain standards -Lack of clear added value for participants
Key implementation stockholders	-Scheme providers -European Commission and Member States -Industry organisations & industry players	-Scheme providers -European Commission and Member States -Regulators -Industry organisations & industry players	-Scheme providers -European Commission and Member States -Regulators	-European Commission and Member States -Regulators -Industry organisations & industry players	-Scheme providers -European Commission and Member States -Industry organisations & industry players	-Scheme providers -European Commission and Member States -Regulators -Industry organisations & industry players	-European Commission and Member States -Regulators -National public administration
Impact on stakeholders?	***Scheme providers*** -Play an active and leadership role -Additional resources and expertise ***European Commission & Member States*** -Facilitate and provide guidance -Promoting and supporting initiatives via financial backing and political endorsement ***Industry organisations & industry players*** -Provide leadership and guidance -Provide a channel for collaboration among different stakeholders -Endorsement and backing -Active participation by industry players	***Scheme providers*** -Play an active and leadership role -Additional resources and expertise -Set up internal processes for transparency and flexibility ***European Commission & Member States*** -Facilitate and provide guidance -Promoting and supporting initiatives via financial backing and political endorsement ***Regulators*** -Provide clear guidance -Promoting and supporting initiatives via financial backing and political endorsement -Formal endorsement and benchmarking via a reporting process ***Industry organisations & industry players*** -Provide leadership and guidance -Provide a channel for collaboration among different stakeholders - Formal endorsement and backing - Set up a reporting process requiring some operational investment -Active participation by industry players -Economic gains for industry players (i.e., saving time and money)	***Scheme providers*** -More regulation and less flexibility -Adapt their internal process with implication on resources and operational cost ***European Commission & Member States*** -Facilitate and provide leadership for development of statutory rules and guidance ***Regulators*** -Develop statutory rules and guidance ***Industry organisations & industry players*** -Collaborate in developing rules and guidance (i.e., participation in industry consultations) -Potential increase in certification cost and effort required for certification application -Cloud providers need to adapt their internal process with implication on resources and operational cost -Long term economic gains for industry players (i.e., saving time and money)	***Scheme providers*** -More regulation and less flexibility -Adapt their internal process with implication on resources and cost ***European Commission & Member States*** -Provide leadership on new rules and setting up industry bodies with specific monitoring tasks ***Regulators*** -Increase legislative and monitoring responsibilities with impact on resources and operating cost ***Industry organisations & industry players*** -Set up and run a formal structure with monitoring responsibilities with significant financial and organisational commitment -Initial higher cost for industry players (i.e., levy to support industry bodies with monitoring responsibilities) -Cloud providers need to adapt their internal process with implication on resources and operational cost -Long term economic gains for industry players (i.e., saving time and money)	***Scheme providers*** -Need to play an active and leadership role in the formulation of standards -Need for additional resources and expertise ***European Commission & Member States*** -Facilitate and provide guidance -Set up co-ordination initiatives -Promoting and supporting initiatives via financial backing and political endorsement ***Industry organisations & industry players*** -Play an active and leadership role in the formulation of standards -Provide a channel for collaboration among different stakeholders -Formal endorsement and backing -Active participation by industry players -Cloud providers need to adapt their internal process with implication on resources and operational cost -Economic gains for industry players (i.e., saving time and money)	***Scheme providers*** -Need for additional resources and expertise -Possible extension of financial responsibility to cover insurance or cost of risk transfer mechanisms -Economic gains from selling risk transfers mechanisms ***European Commission & Member States*** -Facilitate and provide guidance -Promoting and supporting initiatives via financial backing and political endorsement ***Regulators*** -Provide guidance -Promoting and supporting initiatives via financial backing and political endorsement -Formal endorsement ***Industry organisations & industry players*** -Play an active and leadership role in the formulation of risk transfer mechanisms -Play an active role in the implementation of risk transfer mechanisms with higher responsibilities and higher financial commitments in order to cover 'liability certification' and cost of risk transfer mechanisms -Initial higher cost for cloud providers -Economics gains for industry players	***European Commission & Member States*** -Facilitate and provide leadership for development of multilateral agreements or a Common Criteria-type scheme ***Regulators (and national public administration)*** -Time and resources to negotiate and set up multilateral agreements or a Common Criteria-type scheme -Resources to operate the scheme at the national level ***Industry organisations & industry players*** -Collaborate in developing the mutual recognition framework (i.e., participation in industry consultations) -Lower cost of public procurement competition for industry operators
Type of implementation	Self-regulation	Self-regulation	Co-regulation	Co-regulation	Self-regulation	Self-regulation	Self-regulation
Risks	-Weak alignment with end-users' requirements -Too much discretion and variation in quality, standards and practices -Accountability and transparency are not fully addressed	-Still discretion and variation in quality, standards and practices -Accountability and transparency are not addressed	-Higher regulatory burden and market cost -Some loss of flexibility and competitive advantage -Proliferation of different regulatory governance frameworks in MS -Low compliance due to lack of enforcement and monitoring	-Higher regulatory burden and market cost -Some loss of flexibility and competitive advantage -Proliferation of different regulatory oversight regimes in the Member State	-Risk of low adoption of standards and/or code of practice -Risk that alignment with customers' requirements is still inadequate -Accountability and transparency are not fully addressed -Proliferation of standards with negative impact on innovation -Higher market barriers for SMEs	-Low adoption -Too expensive for SMEs -Insurance assessment too complex and high administrative burden -Insurance scams	-Lack of political will by Member States -Slow progress and slow implementation due to silo culture in public sector
Relevance for key elements of cloud services	-Additional elements of security (including non functional ones) -Privacy and confidentiality -Governance and supply chain management	All elements	All elements with higher relevance for privacy and confidentiality	All elements	-SLA including accountability and transparency -Interoperability and portability -Legal jurisdiction and location	All elements	All elemnts
Incompatibility with other line of actions	2 and 4	1 and 4	4	3, 1 , 2 and 5	4	None but it requires 3	None

Proprietary and confidential. Do not distribute.