How to create a sound security certification scheme - a European experience

European Policy background

In September 2012, the European Commission (EC) published a policy document that defines the short-term cloud computing strategy for the EEA: “European strategy for Cloud computing – unleashing the power of cloud computing in Europe[1]”.
This document has two main goals:

- Making Europe cloud-friendly and cloud-active.
- Connecting digital agenda initiatives.

The planned strategy contains three key actions that EC policy makers have identified to support the uptake of cloud computing in Europe:

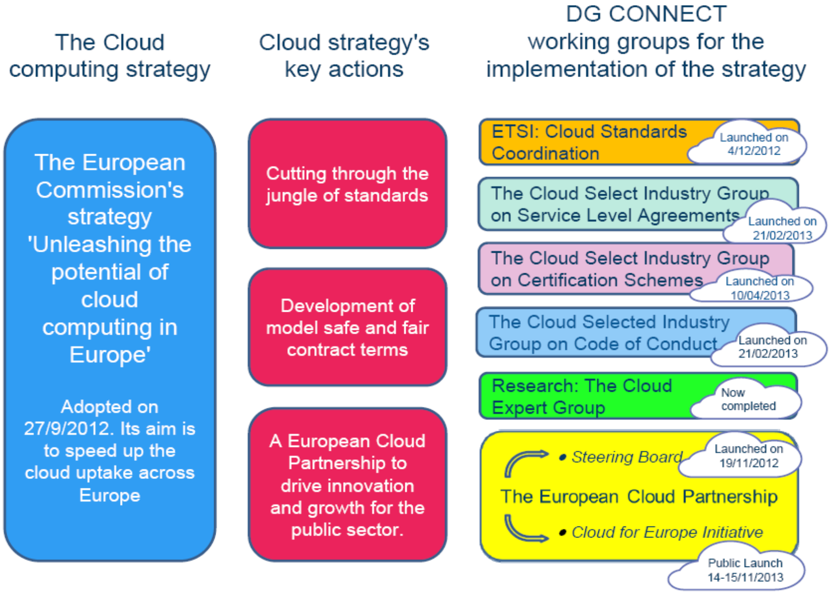
I. “Cutting through the jungle of standards”.

II. Safe and fair contract terms.

III. A European Cloud Partnership.

The figure below provides a summary of the activities related to the implementation of the European Cloud.

Figure 1 - Implementing the European Cloud


The Cloud computing strategy
Cloud strategy's key actions
DG CONNECT working groups for the implementation of the strategy
The European Commission's strategy 'Unleashing the potential of cloud computing in Europe'
Adopted on 27/9/2012. Its aim is to speed up the cloud uptake across Europe
Cutting through the jungle of standards
Development of model safe and fair contract terms
A European Cloud Partnership to drive innovation and growth for the public sector.
ETSI: Cloud Standards Coordination
Launched on 4/12/2012
The Cloud Select Industry Group on Service Level Agreements
Launched on 21/02/2013
The Cloud Select Industry Group on Certification Schemes
Launched on 10/04/2013
The Cloud Selected Industry Group on Code of Conduct
Launched on 21/02/2013
Research: The Cloud Expert Group
Now completed
• Steering Board
Launched on 19/11/2012
The European Cloud Partnership
• Cloud for Europe Initiative
Public Launch 14-15/11/2013

[1] https://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy

For the implementation of key actions 1 and 2, the EC has created the so-called Select Industry Group (SIG) with the goal of bringing together subject matter experts from Industry and not-for-profit organizations to work on **Service Level Agreements**; **Certification Schemes**; **Code of Conduct for Privacy**.

Foundational objectives from the European Commission

The EC cloud computing strategy states "*there is a need for a chain of confidence-building steps to create trust in cloud solutions. This chain starts with the identification of an appropriate set of standards that can be certified in order to allow public and private procurers to be confident that they have met their compliance obligations and that they are getting an appropriate solution to meet their needs when adopting cloud services. These standards and certificates in turn can be referenced in terms and conditions so that providers and users feel confident that the contract is fair*".

"*In addition, take-up amongst public procurers of trusted cloud solutions could encourage SMEs to adopt as well*".

In April 2013, the EC launched the SIG Certification with the aim of supporting the identification of certification(s) schemes(s) "appropriate" for the EEA market:

- Identify objectives, principle and requirements for security and privacy certification schemes.
- List available schemes.

The first step undertaken by the SIG Certification was the preparation and launch of a survey between the members of group. The questionnaire, created by ENISA and Cloud Security Alliance, derived from the EC's cloud strategy the following six mains objectives:

I. Improve customer trust in cloud services.

II. Improve security of cloud services.

III. Increase the efficiency of cloud service procurement.

IV. Make it easier for cloud providers and customers to achieve compliance.

V. Provide greater transparency to customers about provider security practices.

VI. Achieve all the above objectives as cost-effectively as possible.

It should be noted that, the objectives, principles and requirements defined by the EC SIG Certification can be also found in other policy documents in other countries and in general can be regarded as common sense goal to increase the level of adoption of cloud computing in Europe.

Prioritizing the EC foundational objectives

The results of the SIG Certification survey highlighted that the members of the SIG consider that the top three objectives are:

- To improve customer trust in cloud services: giving emphasis on trust as a necessary condition for a large scale adoption of cloud services and, indirectly confirming that the lack of trust has been so far the highest barrier to cloud uptake.

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

- To improve the security of cloud services: giving emphasis on the fact security certifications should be a vehicle to provide a competitive advantage to those CSP.
- To provide greater transparency to customers about CSP's security practices: placing emphasis on the fact that cloud certifications should provide enough details on what is effectively certified, based on which security measures, how and by whom.

The figure below shows responses on the most important high-level objectives.

Figure 2 – SIG Certification Survey: high-level objectives

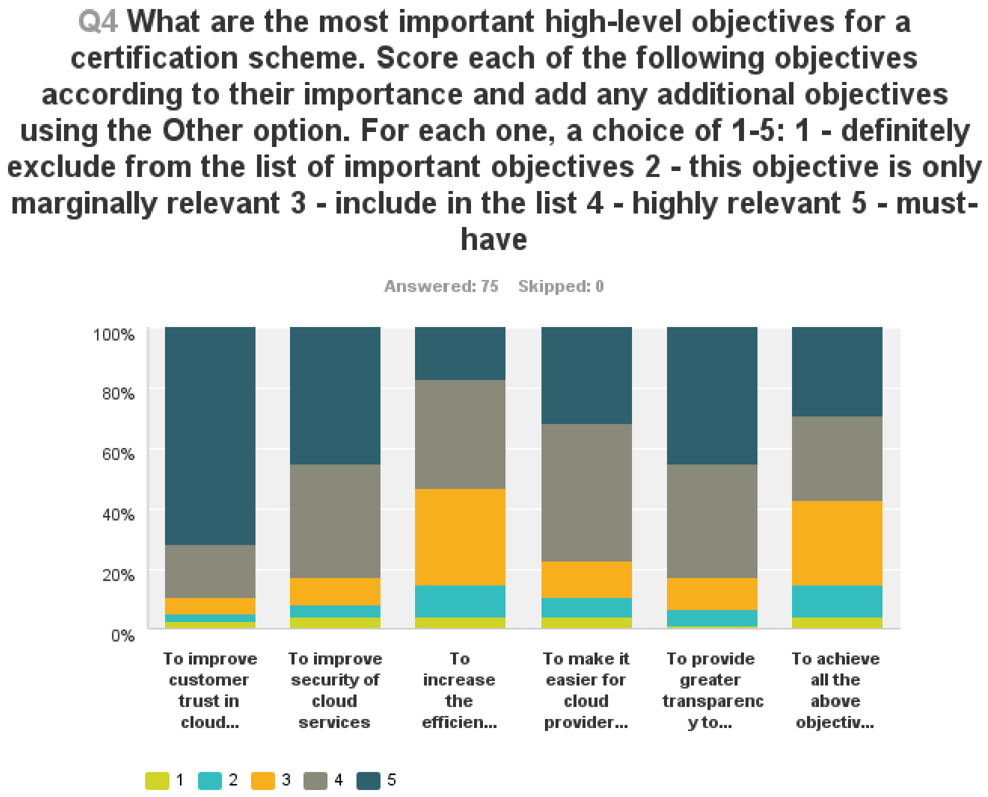
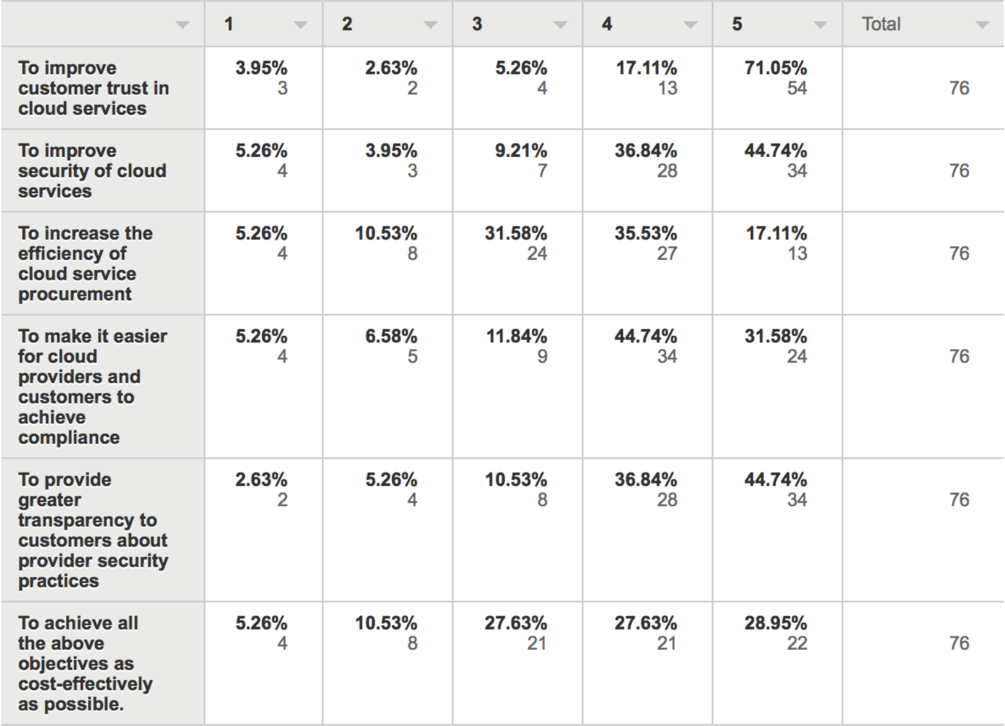


Figure 3 – Details of the answer to the questionnaire on the prioritization of objectives

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994



	1	2	3	4	5	Total
To improve customer trust in cloud services	3.95% 3	2.63% 2	5.26% 4	17.11% 13	71.05% 54	76
To improve security of cloud services	5.26% 4	3.95% 3	9.21% 7	36.84% 28	44.74% 34	76
To increase the efficiency of cloud service procurement	5.26% 4	10.53% 8	31.58% 24	35.53% 27	17.11% 13	76
To make it easier for cloud providers and customers to achieve compliance	5.26% 4	6.58% 5	11.84% 9	44.74% 34	31.58% 24	76
To provide greater transparency to customers about provider security practices	2.63% 2	5.26% 4	10.53% 8	36.84% 28	44.74% 34	76
To achieve all the above objectives as cost-effectively as possible.	5.26% 4	10.53% 8	27.63% 21	27.63% 21	28.95% 22	76

Principles and requirements identified by the EC SIG

In the context of the same survey, the EC SIG Certification group has identified the following set of twenty-five features for a sound security certification scheme. It must be considered that this set of 25 features is a mix of both principles and requirements:

1. Comparability: results should be repeatable, quantifiable and comparable across different certification targets.
2. Scalability: the scheme can be applied to large and small organizations.
3. Proportionality: evaluation takes into account risk of occurrence of threats for which controls are implemented.
4. Composability/modularity: addresses the issue of composition of cloud services including dependencies and inheritance/reusability of certifications.
5. Technology neutrality: allows innovative or alternative security measures
6. Adoption level (number of providers adopting the certification).
7. Provides open access to detailed security measures.
8. Public consultation on drafts of certification scheme during development.
9. Transparency of the overall auditing process.
10. Transparency in reporting of audit results including what is not reported (as far as possible within confidentiality constraints).
11. Transparency in the auditor/assessor accreditation process.

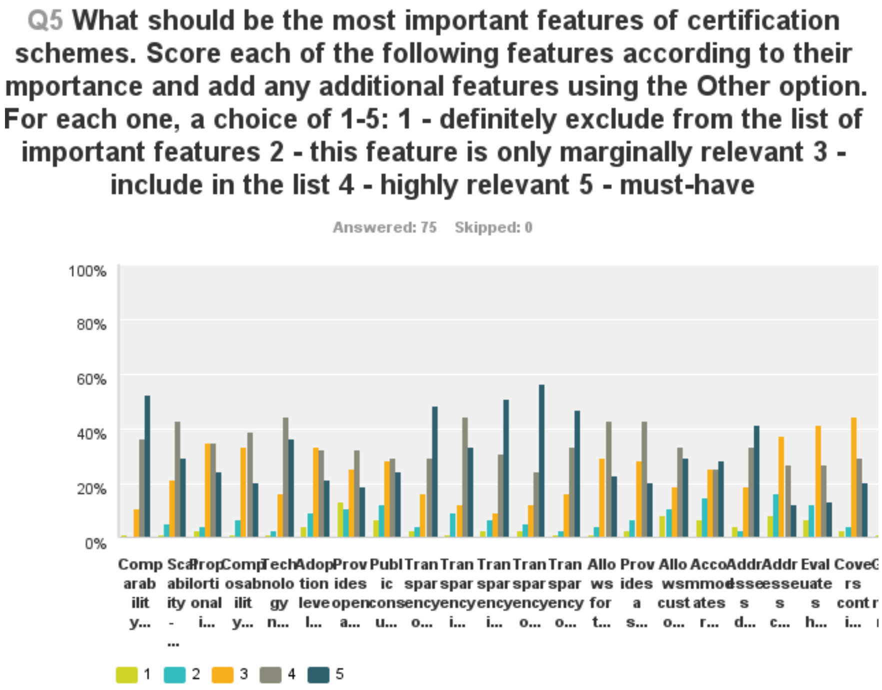
12. Transparency of scope: to allow consumer to verify which services, processes or systems are in scope of certification and which controls have been audited.
13. Transparency of validity or timing (how long is the certification valid for, when did the certification take place).
14. Allows for transparency on good practice against customer requirements.
15. Provides a scale of maturity in security measures.
16. Allows customers and providers to select the trust model that best suits their requirements, e.g. self- assessment, third party assessment, internal audit etc.
17. Accommodates requirements of specific business sectors (e.g. banking and Finance, eHealth, Public Administration, etc.).
18. Addresses data protection compliance including data transfers across border.
19. Addresses capacity management and elasticity controls.
20. Evaluates historical performance against SLA commitments.
21. Covers continuous monitoring: it goes beyond point-in-time assessment by taking into account historical performance and monitoring controls in place.
22. Global/international reach/recognition.
23. Recognition of the certification scheme or standard by accreditation bodies (regional/ national/ sector).
24. Accountable and ethical governance of the certification scheme e.g. fair representation in governance board.
25. Ability for customer organization to rely on results.

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

Prioritizing EC SIG principles and requirements

The figure below present the results to Question 5 of the SIG Certification survey.

Figure 4 – SIG Certification Survey: relevant features



The results of the survey, reported above, can be summarised by the following principles and requirements:

- **Transparency**: the certification schemes should offer full visibility on (1) the way it is structured; (2) the underlying standard(s) on which it is based, (3) how the assessment/audit is conducted, (4) how the auditors are qualified and accredited, (5) the scope of the certification and finally, (6) on the controls against which the assessment is conducted.
- **Scalability**: the certification scheme should be able to scale depending on the needs/size of the CSP (ranging from a big enterprises to small businesses) and, any kind of service model (IaaS, PaaS, SaaS).
- **Flexibility**: the certification schemes should provide a sufficient degree of flexibility in order to:
  - Address sector specific requirements.
  - Provide alternative means to satisfy a certain requirement and reach a control objective. In other words, the security framework on which the

certification is based should foresee the concept of compensating controls and avoid being unnecessarily prescriptive.

- Satisfy varying assurance requirements. In other words, means that certification schemes should foresee different types of assessments/audits including self-assessment, third party assessment, and other more sophisticate types of assessments and audits (e.g., based on continuous collection of evidences, continuous monitoring or trusted computing based certification).

- **Privacy-relevant**: the certification schemes should contain controls able to satisfy data protection compliance requirements
- **Comparability**: results should be repeatable, quantifiable and comparable across different certification targets.

Other relevant elements to consider

Other relevant aspects to be considered in the on-going debate on security certifications schemes for cloud computing such as:

- **Voluntary vs. Mandatory approach**: a majority of cloud stakeholders seem to converge around the idea that a voluntary certification approach should be preferred instead of a mandatory one. The voluntary approach is also preferred by EC. Take for example the European Cloud Strategy, which indicates the need of "development of EU-wide voluntary certification schemes in the area of cloud computing […]". A similar statement can be found in the Art 29 WP "Opinion 05/2012 on Cloud Computing"[2].
- **Generic vs. Cloud specific schemes**: the most widely recognised information security certification is ISO 27001[3]. There are over 17,500 organizations certified globally in over 120 countries. It is a management systems standard, outlining the processes and procedures an organization must have in place to manage Information Security issues in core areas of business. The British Standard Institution (BSI), market leader in the ISO27001 certification, considers it as the gold standard for information security, but argues that ISO 27001 is a general purpose certification that has some limitations when it comes to the certification of cloud computing services. During the CloudWATCH "Certification & testing standard compliance" workshop, at the EGI Technical Forum (17 September 2013, Madrid), Tom Nicholls (Global Commercial Manager Systems Certification at the British Standard Institution) identified the following gaps and limitation in the ISO 27001:

[2] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[3] http://www.iso27001security.com/html/27001.html.

CloudWATCH is funded by the EC FP7 - DG Connect Software & Services, Cloud. Contract No. 610994

- **Out of date**: the recommended list of security control objectives in ISO 27001 (Annex A) is updated every 8 years, which means that the controls soon become obsolete.
- **It is a "one-size-fits-all"** that does not cover some industry specific concerns. Control objectives and controls listed in Annex A of ISO27001 are not exhaustive. Furthermore, specified controls are not fit for the purpose for cloud computing services.
- **Lack of transparency**: ISO27001 does not encourage transparency, since in most of the cases organizations that obtain a certification are not publishing information about the scope of it (which service, department, areas of the organisation are ISO certified?) and neither about the statement of applicability (which controls the company has been audited against?).

These limitations, identified by BSI (and previously by Cloud Security Alliance), are also the reasons why ISO/IEC SC27 is working on new standards to better satisfy the needs of the cloud computing market. In particular ISO is working on the following new international standards:

- ISO 27009 Information technology – Security techniques – The use and application of ISO/IEC 27001 for sector/service specific third party accredited certifications.
- ISO 27017_ Information technology – Security techniques – Code of practice for information security controls for cloud computing services based on ISO/IEC 27002.
- ISO 27018_ Information technology – Security techniques – Code of practice for data protection controls for public cloud computing services.

Based on (1) the previously mentioned input; (2) the input provided by the members of the SIC Certification group and (3) on the fact that a number of countries have already developed (e.g., USA, Singapore) or are developing cloud security certifications (e.g., Hong Kong, Australia, Germany, etc.), we can conclude that new certification schemes should satisfy the cloud market's needs of trust.

- **Global vs. National**: in recent months there's been an intense debate in Europe around the need of having National vs. European vs. Global certification schemes. There is no common view across the various actors in the market and different stakeholders. For example, some policy makers are in favour of national schemes, while others would prefer a more global approach. Most cloud providers are in favour of global schemes to avoid duplication of efforts and costs, etc.

A recent panel discussion took place during the launch of the Cloud for Europe[4] project on 14 November 2013 and is also on the agenda of the European Cloud Partnership Steering Board (ECP-SB). The recommendations of ECP-SP (see report of the meeting of the 4th of July[5], where it points to a convergent

[4] http://www.cloudforeurope.eu.

[5] http://ec.europa.eu/digital-agenda/en/european-cloud-partnership. The Board highlighted the importance of technical solutions (including encryption) to support security: the goal is ensuring security, not keeping data within the borders of states (as currently valid laws require). President Ilves

agreement on the need to facilitate interoperability and cooperation. Hence a global approach to certification should be preferred.
port portability.

noted that Estonia and Finland intend to work together to build mutually interoperable e-service systems. This might eventually allow both countries to move backups of data to data centres established outside of their borders to support redundancy – but to achieve that, we will need to deal with the legal aspects of data storage abroad.