www.cloudwatchhub.eu

D4.1 – Cloud certification guidelines and recommendations

Revised Version

A European Cloud observatory supporting cloud policies, standards profiles & services

www.cloudwatchhub.eu | info@cloudwatchhub.eu | @CloudWatchHub

Security and privacy certifications and attestations have been identified as one of most effective and efficient means to increase the level of trust in cloud service and stimulate their adoption. Based on this on assumption a number of efforts have been started in Europe at policy level mainly leaded by the European Commission (EC), ENISA and ETSI. CloudWATCH itself is part of this effort.

Building on the ETSI and on the EC SIG Certification works, CloudWATCH wants to provide through this report a guidance to cloud service customers, cloud service providers and policy makers in their evaluation of suitable security and privacy certification schemes for cloud services.

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

CloudWATCH Mission

The CloudWATCH mission is to accelerate the adoption of cloud computing across European private and public organisations. CloudWATCH offers independent, practical tips on why, when and how to move to the cloud, showcasing success stories that demonstrate real world benefits of cloud computing. CloudWATCH fosters interoperable services and solutions to broaden choice for consumers. CloudWATCH provides tips on legal and contractual issues. CloudWATCH offers insights on real issues like security, trust and data protection. CloudWATCH is driving focused work on common standards profiles with practical guidance on relevant standards and certification Schemes for trusted cloud services across the European Union.

The CloudWATCH partnership brings together experts on cloud computing; certification schemes; security; interoperability; standards implementation and roadmapping as well as legal professionals. The partners have a collective network spanning 24 European member states and 4 associate countries. This network includes: 80 corporate members representing 10,000 companies that employ 2 million citizens and generate 1 trillion in revenue; 100s of partnerships with SMEs and 60 global chapters pushing for standardisation, and a scientific user base of over 22,000.

Disclaimer

CloudWATCH (A European Cloud Observatory supporting cloud policies, standard profiles and services) is funded by the European Commission's Unit on Software and Services, Cloud Computing within DG Connect under the 7th Framework Programme.

The information, views and tips set out in this publication are those of the CloudWATCH Consortium and its pool of international experts and cannot be considered to reflect the views of the European Commission.

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

Document information Summary

Document title:	Cloud certification guidelines and recommendations
Main Author(s):	Daniele Catteddu, Cloud Security Alliance
Contributing author(s):	Marina Bregu, Cloud Security Alliance Jesus Luna, Cloud Security Alliance Konstantinos Mantzoukas, Cloud Security Alliance Alain Pennetrat, Cloud Security Alliance
Reviewer(s):	Michel Drescher, EGI.eu
Editor(s):	Stephanie Parker, Trust-IT Services
Target audiences:	Policy makers, ranging from European Commission to member state levels. Public procurers in European, National and Regional/local institutions and agencies. Procurers of cloud services both in SMEs (small and medium enterprises) and large corporations. Compliance managers of cloud service customers. Compliance managers of cloud service providers.
Keywords:	Certification, Recommendation, Trust Transparency, Assurance, Flexibility, Compliance Cost efficiency, European Commission
Deliverable nature:	Report
Dissemination level: (Confidentiality)	Public
Contractual delivery date:	1 December 2013
Actual delivery date:	31 December 2013
Revised version following Year 1 review	30 January 2015
Reference to related publications	See footnotes and Annex 3

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

Executive Summary

Security and privacy certifications and attestations have been identified as one of most effective and efficient means to increase the level of trust in cloud services and stimulate their adoption. Based on this on assumption a number of efforts have begun in Europe at policy level mainly led by the European Commission (EC), in collaboration with ENISA and the Clouds Standards Coordination CSC ETSI effort. These efforts have aroused much interest in European solutions for cloud standards and software industry development beyond the European Union.

Trust and confidence in cloud computing

The ETSI Cloud Standard Coordination report (December 2013)[1], where several CloudWATCH partners have played an active role, concludes:

> "*One of the main challenges, when it comes to cloud computing, consists of building trust and confidence in cloud computing services. The variety of existing standards, with a varying degree of maturity, as well as the lack of clarity around the suitability of currently available certification schemes, are not really helpful in these trust building efforts. Concerns are being voiced about compliance issues as well as the effectiveness and efficiency of traditional security governance and protection mechanisms applied to the cloud computing" and ".Our analysis has shown that cloud computing governance and assurance standards specifically developed for and aimed at the cloud already exist (e.g., cloud controls framework, security cloud architectures, continuous monitoring of cloud service provider's) and some of them are considered as sufficiently mature to be adopted*."

How CloudWATCH is making a contribution

CloudWATCH is making an active contribution to European efforts through its focus on standards and certification, driving interoperability as key to ensuring broader choice and fairer competition. Building on the ETSI and on the EC SIG Certification works, this CloudWATCH report is aimed at providing guidance for **cloud service customers**, especially public administrations and **small and medium companies**, **cloud service providers** and **policy makers** in their evaluation of possible options for "certifying" the level of security and privacy of cloud services.

The findings of this interim report will be further elaborated in a final report on Certification and Recommendation Guidelines, which will be published in June 2014.

[1] http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF.

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

Main findings of the CloudWATCH analysis

Transparency

A suitable certification scheme should support transparency to the highest degree. Providing visibility into the security and privacy capabilities of a cloud services gives opportunities to all the actors in the cloud computing market to:

- Make more informed and risk based decisions when selecting/assessing a service
- Transform security and privacy capabilities in market differentiator
- Avoid unnecessary regulatory intervention
- Increase the level of trust in the cloud market

Scalability, Flexibility and Cost Efficiency

Moreover certification schemes should be **scalable**, **flexible** and **cost efficient** in order to be able to accommodate the needs of:

- Organizations of different sizes (SMEs, large corporations etc.), operating at the various layers of the cloud stack (SaaS, PaaS, IaaS, XaaS) and in different sectors (e.g. healthcare, finance, public administration, not or less regulated business sectors)
- Organizations with varying assurance requirements.

Our analysis shows that most of the certification schemes considered have some promising transparency features. However, in most cases the level of visibility and information available about the certification process, and audit results are not yet sufficient, and more should be done.

We also noted that most of the certification schemes considered appear to provide the necessary level of scalability, some seem to be cost efficient, but only a few clearly provide the necessary level of flexibility. This lack of flexibility could represent a potential problem since it might prevent, in some cases, the technical frameworks underlying the schemes from being able to evolve at same pace of the cloud market, therefore failing to satisfy changing requirements. Moreover only a few certification schemes are able to address the needs of organizations with varying level of assurance (e.g. very few schemes are based on a maturity /capability model, and very few include a self-certification option).

CloudWATCH Recommendations

Based on these findings and our associated conclusions, CloudWATCH makes the following recommendations.

Supporting Transparency

We recommend cloud customers, especially public administrations, to adopt a cloud selection process that favours certifications/attestations that clearly support transparency. It is of particular importance for a procurement officer to have a clear visibility on the details of technical standard(s) on which the certification assessment is based. Knowing which

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

technical controls are included in a standard is the only way to understand if that technical framework, and the certification scheme it is based on, is suitable to satisfy the technical requirements and compliance needs of a certain organization. Furthermore, importance should be given to the quality of the assessment/audit. This recommendation is mainly addressed to public sector procurement offices, since they have the necessary negotiation power to demand specific features and services.

Appropriate level of detail on information security approaches

We also recommend that Cloud Providers introduce more transparency in their information security approaches. While we do not suggest an approach based on full disclosure, as we do appreciate that in some cases this is not possible given the confidentiality of some information included in the assessment report, Cloud Providers should nevertheless be willing to provide as much details as possible about the results of their certification assessment reports.

Soft law supporting transparency

Further, we recommend that policy makers work on **soft-law** to foster transparency by supporting certification schemes that enable transparency. Transparency is a fundamental attribute of accountability and essential trust-enabling component, and the adoption of soft-law supporting transparency could prevent the need of binding regulatory intervention that might not be the most appropriate measure in a market, which is still underdevelopment and in continuous transformation.

Assurance Certification schemes should provide scalability, flexibility & cost efficiency. We recommend policy makers to endorse/demand for certification schemes that are able to provide scalability, flexibility and cost efficiency and to match the different assurance levels requested by regulatory authorities and customers of any kind (pubic administration, micro, small medium companies and enterprise). There is a clear trade-off between the levels of rigour and the cost of certification (obviously self-certification is less expensive than a certification based on third party assessment). To make market more efficient each actor should be given the possibility to select the most cost effective solution to satisfy its assurance needs.

Address how the FP7 funded projects: A4Cloud, CIRRUS, CUMULUS, SPECS & The STAR certification Training could in the future, or have already addressed some of these recommendations.

Table of Contents

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

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

Tables

Figures

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

1. Context and Scope

1.1 Overview

One of the main objectives of the CloudWATCH project is to accelerate and increase the adoption of cloud computing across the public and private sectors in Europe and strengthen collaborative, international dialogue on key aspects of cloud computing such as interoperability, portability, security and privacy. One of actions associated with this high level objective is to "raise awareness of and promote education about Certification Schemes for cloud services certification", by e.g. providing guidance on how to apply the certification principles (as defined by the SIG Certification) in practice.

This revised version of D4.1 responds to Year one review recommendations to make it *fully clear which criteria have been used to pull together the list of those standards considered relevant, this should be made explicit in the report. Also the reason why only the operational standards have been taken into account for the mapping exercise, needs to be addressed.*
These are addressed in section 1.5 while section 5 looks at next steps for D4.1 including a revised version of the deliverable to be released in early 2015.

CloudWATCH is looking into the topics of standards and certification in order to understand if and how certification can increase the level of trust in the cloud computing business model. Specifically, CloudWATCH is leading activities on certification and testing standard compliance with the aim of providing sound recommendations based on real-life cases and clear explanations on protection from risks.

In Europe, a relevant effort is being taken by the EC includes in the "European Cloud Strategy"[2], which explicitly acknowledges the need of adopting voluntary certification schemes. Such schemes can be used as a measure to increase the level of trust in cloud services.

A similar approach has been taken by other policy makers outside Europe, for instance in the USA, Singapore, Japan, Thailand, Hong Kong and China.

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

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

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

- Suitability of existing security certification 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

In this report we describe in detail the most relevant aspects of this on-going debate. Furthermore, we provide a set of recommendations, the relevance of which is going to be monitored and assessed over the next 12 months of CloudWATCH. The final version of this report ("Cloud certification guidelines and recommendations") will be published in February 2015 and will include a more elaborate and validated set of the initial recommendations.

1.2 Structure of the report

This deliverable is organized in the following manner:

This **Chapter 1** includes target audience, scope, objectives, methodology and approach that was taken to create this deliverable. This chapter also presents our relevant information sources.
Chapter 2 presents the principles, objectives and requirements that are the basis for selecting the appropriate cloud certification schemes.
Chapter 3 discusses and summarizes relevant cloud certification schemes, applying the methodology proposed in Chapter 1. It also provides an easy to digest mapping of certification schemes to the defined objectives and principles.
Chapter 4 presents our main conclusions and overall recommendations respectively.

1.3 Acronyms

The table below provides a list of the main acronyms used in this report.

Acronym	Meaning
AICPA	American Institute of Certified Public Accountants (CPAs),
ANAB	ANSI-ASQ National Accreditation Board
ATO	Authority to Operate
BCP/DR	Business Continuity Planning/Disaster Recovery
BSI	British Standards Institution
CAIQ	Consensus Assessments Initiative Questionnaire

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

CCM	Cloud Global Matrix
CGMA	Chartered Global Management Accountant
CIRRUS	Certification, Internationalisation and Standardization in Cloud Security
CPA	Certified Public Accountant
CRM	Certified Public Accountant Customer relation management systems
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
CTP	Cloud Trust Protocol
DHS	Department of Homeland Security
DOD	U.S. Department of Defense
ECP	European Cloud Partnership
ECSA	EuroCloud Star Audit
EDA	European Defense Agency
EEA	European Economic Area
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
GAPP	Generally Accepted Privacy Principles
GRC	Governance, Risk and Compliance
GSA	U.S. General Service Administration
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as a Service
IAM	Identity and Access Management

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

IDA	Infocomm Development Authority of Singapore

1.4 Target Audiences

This report addresses the following groups of stakeholders:

- Policy makers, ranging from European Commission to member state levels.
- Public procurers in European, National and Regional/local institutions and agencies.
- Procurers of cloud services both in SMEs (small and medium enterprises) and large corporations.
- Compliance managers of cloud service customers.
- Compliance managers of cloud service providers.

Although this report is written from a European perspective, the issues and challenges in the field of security and privacy certification for cloud computing services are not confined to Europe. This report can therefore also be relevant for countries outside the European Economic Area (EEA). Further, CloudWATCH offers a comprehensive vision, and aims to pave the way for globalized approaches to cloud computing certification.

1.5 Scope

This report focuses on security governance certification schemes and privacy certification schemes for cloud services. More specifically this report covers:

- Security governance and privacy certification schemes for cloud computing in the EEA.
- Security governance certification schemes for cloud computing outside the EEA.
- Standards used as base for security governance certification schemes.

It should be noted that the analysis of the available certification schemes is by no means exhaustive or complete. Our approach considers only those schemes that are the most relevant in this area. Beside the relevant certification for the EU market we also wanted to include in the analysis information related to the approaches taken in Countries outside the European Union.

1.5.1 Criteria for determining relevant schemes for analysis

The criteria we have used to determine the relevance of a scheme in the context of our analysis were the following:

1. The scheme and/or the underlying technical standard are included in the ETSI's document: Cloud Standard Coordination Final Report[3]

[3] http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF

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

2. The scheme is included in the ENISA Cloud Certification Scheme List (update October 2013)[4] or it is used as National accreditation scheme for cloud services in a Country or is widely accepted as security accreditation scheme
3. The scheme is operational and has to have a minimum level of market consideration
4. The scheme is cloud specific or at least cloud relevant certification scheme

We have defined an initial pool of certification scheme candidates to be considered in the analysis and assigned them a score based on the above-mentioned criteria.

The pool of schemes was based on the ENISA Cloud Certification Scheme List (CCSL), updated at October 2013 (which included the following schemes: 1) Certified Cloud Service - TÜV Rheinland, 2) CSA Star Program – Open Certification Framework, 3) EuroCloud Star Audit, 4) ISO27001, 5) Security Rating Guide – Leet Security. To this list we added: SOC1-2-3 since they are widely accepted in Industry; Fedramp and Multi-Tier Cloud Security (MTCS) as they are mandatory schemes for certain categories of service in USA and Singapore; and EuroPrise as it is considered as one of the few widely accepted schemes for privacy requirement certification.

Each scheme was given 1 point for each requirement that it met. The schemes that scored at least 3 points were considered in the study. Schemes scoring 2 points were considered as candidates for inclusion in the final version of the report. Schemes scoring less than 2 points were considered as irrelevant to the context of this study.

The cloud certification schemes selected wereanalysed and used as input to elaborate the recommendations presented at the end of this document.
For the sake of clarity, input from the following groups and research informed the decision on what is most relevant and what is outside the scope of this report:

- The EC Selected Industry Group. [5]
- Relevant institutions outside EEA (e.g. NIST, GSA, AICPA, EDA, etc.).
- Standards Development Organizations (SDO).
- Publicly available market research.

1.6 Objectives

The four main objectives of this report are to:

I. Identify principles and requirements for certification schemes suitable for satisfying the EEA's security and privacy requirements.
II. Provide guidance to cloud customers (both in the private and public sectors) with the aim of accelerating the adoption of cloud computing services (especially for SMEs and Public Sector) by clarifying the value and meaning of a cloud certification with

[4] https://resilience.enisa.europa.eu/cloud-computing-certification

[5] http://ec.europa.eu/digital-agenda/en/news/cloud-select-industry-group-research-priorities-competitive-cloud-computing-industry-europe.

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

respect to the capabilities required to address and satisfy security and privacy compliance requirements.

III. Provide guidance to Cloud Service Provider (CSP) on how to select the most appropriate cloud certification for their business needs.

IV. Provide recommendations to CSPs, customers and policy makers with regards to the selection of cloud certifications based on the principles and requirements identified by CloudWATCH (see § 2.5. and 2.6)

1.7 Methodology & Approach

The following approach was followed to produce this report:

- Identifying principles, objectives and requirements for security and privacy certification schemes suitable for the cloud market.
- Stocktaking of the existing certification schemes.
- Analysis of the collected schemes based on the previously identified principles, objectives and requirements (stage 1 above).
- Drawing conclusions and recommendations based on the analysis.

This report has been created based on the input collected from various sources, consolidated and analysed by subject matter experts in the CloudWATCH consortium. Specifically, input for this deliverable has been were collected from the following sources:

- EC Selected Industry Group survey on cloud certifications: this survey was prepared by Cloud Security Alliance and ENISA in the context of the work of the SIG Certification and distributed to the members of this group (the complete results of the survey can be found in Annex 2)
- Certification & testing standard compliance Workshop, EGI Technical Forum, 17 September 2013, Madrid[6].
- NIST[7] (National Institute of Standards and Technology) and FedRAMP[8] web sites.
- Cloud Security Alliance[9] web site
- Cloud Security Alliance International Standardization Council[10]
- AICPA[11] web site
- EuroSeal[12] web site
- EuroCloud[13] web site

[6] https://indico.egi.eu/indico/sessionDisplay.py?sessionId=48&confId=1417#20130918.
[7] http://www.nist.gov/index.html.
[8] http://www.fedramp.com/.
[9] https://cloudsecurityalliance.org/.
[10] https://cloudsecurityalliance.org/isc/.
[11] http://www.aicpa.org/Pages/default.aspx.
[12] https://www.european-privacy-seal.eu/.
[13] http://www.eurocloud.org/.

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

- Interviews and contributions from: FedRAMP/GSA, NIST, AICPA, EDA[14], British Standards Institution[15], Cloud Security Alliance, EuroCloud.

[14] http://www.eda.europa.eu.
[15] http://www.bsigroup.com.

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

2. Drivers for the definition and selection of certification schemes

In this chapter we describe the set of principles, objectives and requirements that should drive the definition and selection of cloud security and privacy certification schemes.

2.1 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" [2].

This document has two main goals:

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

The planned strategy [2] contains three key actions that EC policy makers have identified to support the uptake of cloud computing in Europe:

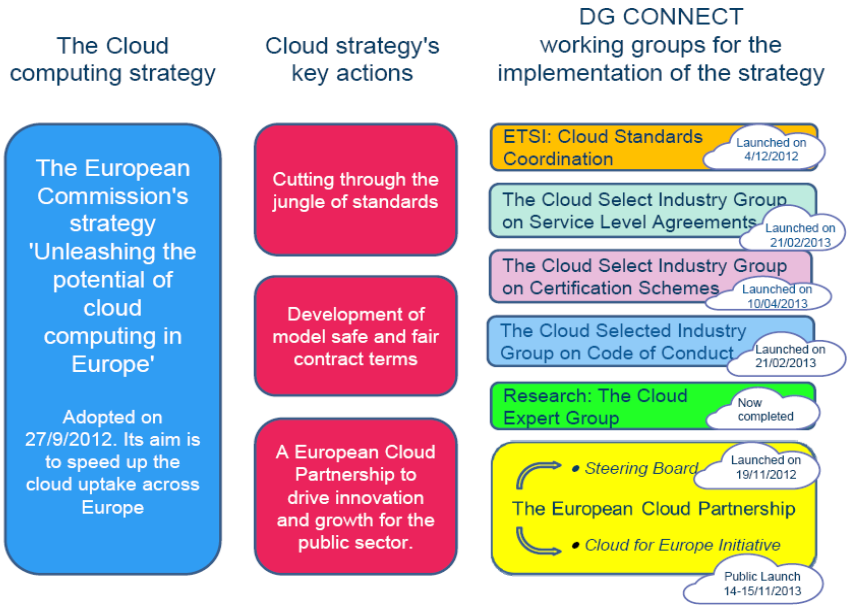
I. "Cutting through the jungle of standards".

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



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

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**.

2.2 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 [1]:

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 [1] 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.

2.3 Prioritizing the EC foundational objectives

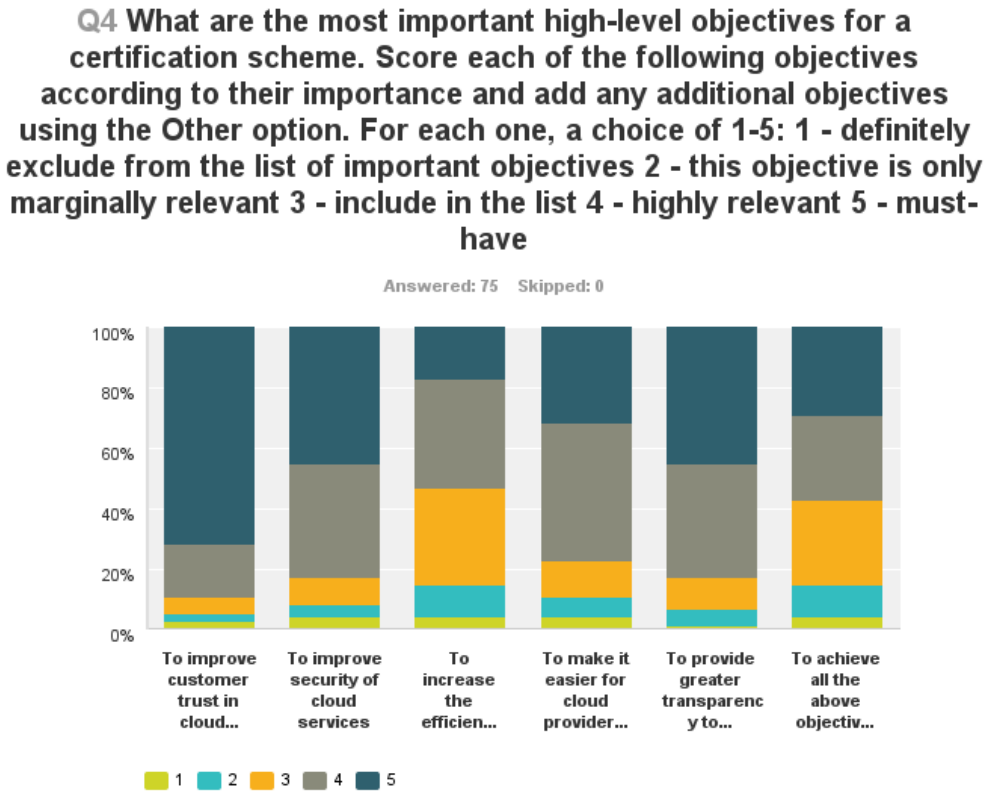
The results of the SIG Certification survey highlighted that the members of the SIG consider that the top three objectives are:

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

- 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.
- 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



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

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

	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

2.4 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.

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

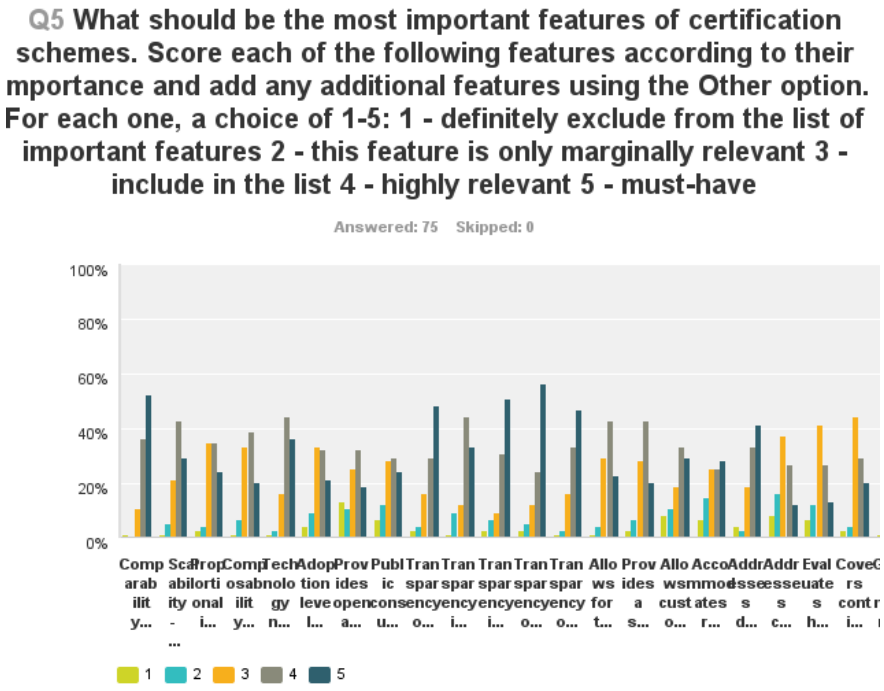
10. Transparency in reporting of audit results including what is not reported (as far as possible within confidentiality constraints).
11. Transparency in the auditor/assessor accreditation process.
12. Transparency of scope: to allow consumer to verify which services, processes or systems are in scope 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

2.5 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

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

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.

2.6 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"[16].
- **Generic vs. Cloud specific schemes**: the most widely recognised information security certification is ISO 27001[17]. 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:

[16] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.
[17] 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[18] 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

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

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

July[19], where it points to a convergent agreement on the need to facilitate interoperability and cooperation. Hence a global approach to certification should be preferred.

[19] 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 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.

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

3. Relevant certification schemes for security and privacy

3.1 ISO/IEC 27001:2013

Name of the programme: ISO/IEC 27001:2013[20] - Information technology – Security techniques – Information security management systems - Requirements

Governing of the standard: ISO – ISO/IEC – JTC 1[21]

Accreditation Body/Bodies: Numerous, including UKAS[22], ANAB[23], JAS-ANZ[24]

Table 1 - ISO/IEC 27001:2013

Scope: Information Security
Cloud-relevance: ISO 27001 covers all areas of information security and is applicable to cloud services.
Type of certifiable organisation: Any - SaaS, PaaS, IaaS
Type of trust models applicable: self-attestation/third-party/benchmark-test: Third party assessment with accreditation programs in place for certifying bodies.
Is the certification proprietary or open: Open
Programme, status (operational, in development): Operational

ISO/IEC 27001 is the international standard for information security management. It outlines how to put in place an independently assessed and certified information security management system. This allows you to more effectively secure all financial and confidential data, so minimizing the likelihood of it being accessed illegally or without permission.

With ISO/IEC 27001 you can demonstrate commitment and compliance to global best practice, proving to customers, suppliers and stakeholders that security is paramount to the way you operate.

The main body of the standard outlines the requirements of a system to manage information security. There is also an Annex A, which contains and extensive list of controls. These

[20] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.
[21] http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/jtc1_home.htm.
[22] http://www.ukas.com.
[23] http://www.anab.org/.
[24] http://www.jas-anz.com.au.

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

controls, along with others as required, are selected by assessing the risks facing the organisation and the applicability of the controls to manage those risks. The combination of the controls and the management system to maintain these controls makes ISO 27001 a highly effective information security standard.

The standard follows the approach common in International management systems standards, making it easy to integrate with other systems and organisation might already have in place. The 7 core elements of the new version of the standard published in 2013 are:

I. Context of the Organization
II. Leadership
III. Planning
IV. Support
V. Operation
VI. Performance Evaluation
VII. Improvement

3.2 SSAE16 – SOC 1-2-3

Name of the programme: Service Organization Control (SOC)[25]

Governing of the standard: AICPA Attestation Standards

Accreditation Body/Bodies: State licensing bodies

Scope: SOC 1: Controls relevant to user entities' internal control over financial reporting SOC2 2: AT Section 101, *Attest Engagements (*AICPA, *Professional Standards)* SOC3: Controls relevant to security, availability, confidentiality, and processing integrity
Cloud-relevance: Not cloud specific. Cloud relevance is provided through the use of Cloud Security Alliance Cloud Control Matrix (See STAR Attestation and the following reference)[26].
Type of certifiable organisation: SaaS, PaaS, IaaS
Type of trust models applicable: Independent 3rd party assurance.
Is the certification proprietary or open: Report is restricted to use of management of the

[25] www.aicpa.org/SOC.
[26] http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/csa-position-paper-on-aicpa-service-organization-control-reports.pdf.

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

service organization and other specified parties. If prospective user entities are intended users of the report, the prospective user entities should have sufficient knowledge and understanding of the nature of services provided by the service organization; how the service organization's system interacts with user entities, subservice organizations, and other parties; internal control and its limitations; complementary user-entity controls and how they interact with related controls at the service organization and subservice organization to meet the applicable trust services criteria; the applicable trust services criteria; and the risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

Programme, status (operational, in development): Operational

For over 20 years, Certified Public Accountants have performed specialized audits of information technology (IT) internal controls at service organizations. During this time, a report by a CPA firm has become the standard for reporting on internal controls at a service organization as required by the U.S. Government, Security and Exchange Commission (SEC), the financial services industry, and standard contract terms with countless service organization users. One of the main reasons for this wide adoption has been that the professional standards that underpin these CPA reports provide customers with a basis for relying on the reports' conclusions. The objective of these service organization reports (SOC) has been to provide the customers of service organizations, and the auditors of those customers, assurance over the effective operation of IT controls designed to address IT risk to information processing. To provide the framework for CPAs to examine controls and to help management understand the related risks, the American Institute of Certified Public Accountants (AICPA) established three Service Organization Control (SOC) reporting options (SOC 1, SOC 2 and SOC 3 reports).

- **SOC 1**

SOC 1 engagements are performed in accordance with Statement on Standards for Attestation Engagements (SSAE) 16, Reporting on Controls at a Service Organization. SOC 1 reports focus solely on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements. Use of a SOC 1 report is restricted to existing user entities (not potential customers). There are two types of SOC 1 reports:

- **Type 1** – A report on management's description of the service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.
- **Type 2** – A report on management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.

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

- **SOC 2**

Recognizing customers' need for assurance extended beyond financial objectives, the AICPA in collaboration with Canadian Institute of Chartered Accountants (CPA Canada) first formulated the Trust Services Principles and Criteria (TSPC) in 2002 to assist in brokering a trust-relationship between the vastly increasing IT service- and data processing industry and its customers. The TSPC provides a framework for a CPA to report on the design and operating effectiveness of Security, Confidentiality, Availability, Privacy and Processing Integrity controls.

SOC 2 engagements use the predefined criteria in the TSPC, as well as the requirements and guidance in AT Section 101, Attest Engagements, of SSAEs (AICPA, Professional Standards, vol. 1). A SOC 2 report is similar to a SOC 1 report. Either a type 1 or type 2 report may be issued. The report provides a description of the service organization's system. For a type 2 report, it also includes a description of the tests performed by the service auditor and the results of those tests. SOC 2 reports specifically address one or more of the following five key system attributes:

- **Security** - The system is protected against unauthorized access (both physical and logical).
- **Availability** - The system is available for operation and use as committed or agreed.
- **Processing integrity** - System processing is complete, accurate, timely and authorized.
- **Confidentiality** - Information designated as confidential is protected as committed or agreed.
- **Privacy** - Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice, and with criteria set forth in Generally Accepted Privacy Principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants.

Additionally, the scope of the SOC 2 report can address other criteria related to HIPAA, e-Prescribing, FISMA and other IT (security) requirements.

Today, with the rise of cloud computing, the demand for reporting by CPA firms on controls related to security, confidentiality, and availability has seen a resurgence and large cloud service providers (CSP) have, or are in the process of, providing their customers with SOC 2 reports to address this demand.

In a position paper released February 2013, the CSA stated that "for most cloud providers, a type 2 SOC 2 attestation examination conducted in accordance with AT section 101 of the AICPA attestation standards is likely to meet the assurance and reporting needs of the majority of users of cloud services, when the criteria for the engagement are supplemented

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

by the criteria in the CSA Cloud Controls Matrix," [3] a framework CSA provides for assessing the overall security risk of a cloud provider.

"The cloud can create great efficiencies for businesses, but it also introduces challenges and complexities for those businesses and their stakeholders who rely on the information's integrity, security, and privacy," said Susan Coffey, CPA, CGMA, the AICPA's senior vice president–Public Practice & Global Alliances, in a news release. "We're delighted that the Cloud Security Alliance has given its stamp of approval to Service Organization Control Reports as a mechanism to meet this reporting challenge."

- **SOC 3**

SOC 3 engagements also use the predefined criteria in the TSPC that are used in SOC 2 engagements. The key difference between a SOC 2 report and a SOC 3 report is that a SOC 2 report, which is generally a restricted-use report, contains a detailed description of the service auditor's tests of controls and results of those tests as well as the service auditor's opinion on the description of the service organization's system. A SOC 3 report is a general-use report that provides only the auditor's report on whether the system achieved the trust services criteria (no description of tests and results or opinion on the description of the system). It also permits the service organization to use the SOC 3 seal on its website.

Table 2 - Overview of SOC Reports

SOC 1 [SM] Reports
Relevant Professional Standards AT Section 801, *Reporting on Controls at a Service Organization (*AICPA, *Professional Standards)*
Intended users of report Management of the service organization, user entities and auditors of user entities' financial statements
SOC 2 SM Reports
Relevant Professional Standards AT Section 101, *Attest Engagements (*AICPA, *Professional Standards)*
Intended users of report Management of the service organization and other specified parties who have sufficient knowledge and understanding of the following: ▪ Management of the service organization and other specified parties who have sufficient knowledge and understanding of the following: ▪ The nature of the services provided by the service organization. ▪ How the service organization's system interacts with user entities, subservice organizations, and other parties. ▪ Internal controls and its limitations. ▪ Complementary user-entity control and how they interact with related control at the service organization to meet the applicable trust services criteria. ▪ The applicable trust services criteria. ▪ The risks that may threaten the achievement of the applicable trust services criteria and how control address those risks.

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

SOC 3 [SM] Reports
Relevant Professional Standards: AT Section 101, *Attest Engagements (*AICPA, *Professional Standards)*
Intended users of report: Anyone

3.3 Cloud Security Alliance Open Certification Framework

Name of the programme: Open Certification Framework – STAR

Governing of the standard: Cloud Security Alliance

Accreditation Body/Bodies: Cloud Security Alliance, British Standard Institution (for STAR Certification), AICPA (for STAR Attestation)

Table 3 - CSA STAR

Scope: Security and Privacy

The standard underlying the CSA OCF/STAR Programme Cloud Control Matrix (CCM).

CCM is composed of 98 controls, structured in 13 domains and covers the following areas:

- Compliance - Information System Regulatory Mapping
- Data Governance - Information Leakage
- Facility Security - Secure Area Authorization
- Human Resources - Employment Termination
- Information Security - User Access Restriction / Authorization
- Information Security - Incident Reporting
- Information Security - Source Code Access Restriction
- Risk Management - Business / Policy Change Impacts
- Resiliency - Business Continuity Testing
- Security Architecture - Remote User Multi-Factor Authentication
- Security Architecture - Shared Networks
- Security Architecture - Audit Logging / Intrusion Detection

The CCM is considered as meta framework since is mapped against the most relevant information security controls framework: ISO 27001-2005, NIST SP 800-53, FedRAMP, PCI DSS, Cobit v4.1, AICPA Trust Principles, ENISA Information Assurance Framework and German BSI Cloud Security Catalogue.

Cloud-relevance: Cloud specific

Type of certifiable organisation: SaaS, PaaS, IaaS

Type of trust models applicable:

- Self-Assessment: CSA STAR Self Assessment

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

▪ Third party independent audit: CSA STAR Certification and CSA STAR Attestation ▪ Continuous monitoring based certification: CSA STAR Continuous (not operational yet)
Is the certification proprietary or open: Open
Programme, status (operational, in development): Operational

The following text is based on information received from Cloud Security Alliance:

- The CSA Open Certification Framework can be described as an industry initiative to allow global, accredited, trusted certification of cloud providers.
- The CSA Open Certification Framework is a program for flexible, incremental and multi-layered cloud provider certification according to the Cloud Security Alliance's security guidance and control objectives:
  - Consensus Assessments Initiative Questionnaire (CAIQ).
  - Cloud Controls Matrix (CCM).

The program integrates with popular third-party assessment (ISO27001) and attestation statements (SOC2) developed within the public accounting community to avoid duplication of effort and cost.

The CSA Open Certification Framework is based upon the control objectives and continuous monitoring structure as defined within the CSA GRC (Governance, Risk and Compliance) Stack research projects.

The CSA Open Certification Framework is structured in three tiers in order to address varying assurance requirements and maturity levels of providers and consumers. These range from the CSA STAR Self-assessment to high-assurance specifications that are continuously monitored.

The three levels of the OCF Programme are:

- Level 1 – CSA STAR Self-Assessment
- Level 2 – CSA STAR Certification/Level 2 – CSA STAR Attestation
- Level 3 – CSA STAR Continuous

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

3.3.1 STAR Self-Assessment

CSA STAR Self Assessment is a self-assessment due diligence process based on CSA best practice Consensus Assessments Initiative Questionnaire (CAIQ)[27] and Cloud Controls Matrix (CCM).

The results of the self-assessment are voluntarily published by the CSP on the CSA STAR web site that is freely available and open to all cloud providers.

Cloud providers can submit two different types of reports to indicate their compliance with CSA best practices:

- The Consensus Assessments Initiative Questionnaire (CAIQ), which provides industry-accepted ways to document what security controls exist in IaaS, PaaS, and SaaS offerings. The questionnaire (CAIQ) provides a set of over 140 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider. Providers may opt to submit a completed Consensus Assessments Initiative Questionnaire.
- The Cloud Controls Matrix (CCM), which provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry. Providers may choose to submit a report documenting compliance with Cloud Controls Matrix.

3.3.2 STAR Certification

The CSA STAR Certification[28] is a third party independent assessment of the security of a cloud service provider. A technology-neutral certification that leverages the requirements of the ISO/IEC 27001:2005 management system standard together with the CSA Cloud Control Matrix.

The independent assessment is conducted by certification body (such as the British Standard Institution) accredited CSA. The assessment assigns a 'Management Capability' score to each of the CCM security domains. Each domain is scored on a specific maturity and will be measured against 5 management principles.

The internal report shows organizations how mature their processes are and what areas they need to consider improving on to reach an optimum level of maturity. These levels will be designated as either "No", "Bronze", "Silver" or "Gold" awards. Certified organization will be listed on the CSA STAR Registry as "STAR Certified".

[27] https://cloudsecurityalliance.org/research/cai/.
[28] https://cloudsecurityalliance.org/star/certification/.

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

CSA STAR CERTIFICATION evaluates the efficiency of an organization's ISMS and ensures the scope, processes and objectives are "Fit for Purpose", and helps organizations prioritize areas for improvement and lead them towards business excellence.

It also enables effective comparison across other organizations in the applicable sector and it is focused on the strategic & operational business benefits as well as effective partnership relationships.

CSA STAR Certification enables the auditor to assess a company's performance, on long-term sustainability and risks, in addition to ensuring they are SLA driven, allowing senior management to quantify and measure improvement year on year.

The STAR certification scheme is designed to comply with:

- ISO/IEC 17021:2011, Conformity assessment – Requirements for bodies providing audit and certification of management systems.
- ISO/IEC 27006:2011, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems.
- ISO 19011, Guidelines for auditing management systems.

3.3.3 STAR Attestation

The STAR Attestation[29] is positioned as STAR Certification at Level 2 of the Open Certification Framework and is likewise STAR Certification a third party independent assessment of the security of a cloud service provider.

Star Attestation is based on type 2 SOC attestations supplemented by the criteria in the Cloud Controls Matrix (CCM). This assessment:

- Builds on the key strengths of SOC 2 (AT 101).
- Provides for robust reporting on the service provider's description of its system, and on the service provider's controls, including a description of the service auditor's tests of controls in a format very similar to the now obsolete SAS 70 reporting format, and current SSAE 16 (SOC 1) reporting, thereby facilitating market acceptance.
- Evaluation over a period of time rather than a point in time.
- Recognition with an AICPA Logo.

3.3.4 STAR Continuous

CSA STAR Continuous[30] will be based on a continuous auditing/assessment of relevant security properties.

[29] https://cloudsecurityalliance.org/star/attestation/.

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

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.

3.4 EuroPrise: The European Privacy Seal

Name of the programme: Europrise[31]

Governing of the standard: EuroPrise GMBH, with a board of stakeholders including the German Data Protection of Schleswig-Holstein.

Accreditation Body/Bodies: EuroPrise GMBH accredits independent third party auditors based on an evaluation. Third party independent auditors are accredited by the Europrise Certification Authority. Third party auditors evaluate the product or service and produce an evaluation report. The seal is awarded after report has been validated by the Europrise Certification Authority.

Table 4 - EuroPrise

Scope: Data protection
Cloud-relevance: Not cloud specific (just like ISO 27001) but could be applied to a cloud service, and has already been awarded to a search engine and a behavioural advertising network.
Type of certifiable organisation: Certifies IT products and services. Does not apply to organizations.
Type of trust models applicable: Evaluation by accredited independent third party auditors.
Is the certification proprietary or open: Proprietary
Programme, status (operational, in development): Operational

[30] https://cloudsecurityalliance.org/star/continuous/.
[31] https://www.european-privacy-seal.eu/.

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

EuroPrise is a European certification scheme that certifies compliance of IT products and services with a catalogue of criteria that are based on the European Data Protection directives (95/46/EC and 2002/58/EC) and opinions of Article 29 working party.

The EuroPrise trustmark is awarded after (1) an evaluation by an independent accredited auditor and (2) the validation of the produced evaluation report by the Europrise certification body.

EuroPrise is currently governed by the data protection authority of Schleswig-Holstein (ULD) in Germany. However, starting on January 1st 2014, governance will be handed over to an independent private entity, EuroPrise GMBH, in order to account for the expansion of this trustmark.

3.5 EuroCloud – STAR Audit

Name of the programme: EuroCloud Star Audit (ECSA)[32]. The international platform based on Promis with multiple languages available in Q2/2014

Governing of the standard: EuroCloud

Accreditation Body/Bodies: In preparation

Table 5 - EuroCloud STAR Audit

Scope: Transparency about the Cloud Service Delivery chain and involved subcontractors. Legal compliance according to individual regulations per EU country. Data Security and Data privacy. DC resilience. Business Operations. Reversibility and Interoperability
Cloud-relevance: ECSA is cloud specific quality insurance and certification programme
Type of certifiable organisation: Any SaaS, PaaS, IaaS
Type of trust models applicable: Self-assessment (no certificate, only benchmark) Third party assessment with certification
Is the certification proprietary or open: Open (not yet fully disclosed, planned for Q1/2014)
Programme, status (operational, in development): Operational

[32] http://www.saas-audit.de/en/. For a sample of dissemination in German, see https://www.promis.eu/de/eurocloud-star-audit/.

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

The following text is based on information received from EuroCloud:

The EuroCloud STAR Audit programme is based on:

- Detailed market analysis about the European Cloud Provider setup
- Modular structure of the certification pillars to co-work on Cloud Service certification and allow each involved entity to take care about their areas
- Allow partial certification (e.g. datacentre or SaaS Ready) to provide prepared approval for full Cloud Service certification
- Various publications to train the market with the key requirements
- Strong involvement of IT Lawyers to include country specific legal and compliance requirements.

The EuroCloud Star Audit (ECSA) is scoping solely for the European Market and has established partnerships throughout the EuroCloud network with 22 EuroCloud associations. There is a strong involvement in EU and country specific initiatives especially in the area of data protection form a European and country specific understanding.

The graduation by 3 to 5 Stars for a trusted Cloud Service allows a differentiation according to the market needs and is affordable even for SME CSPs. Beside this the modular structure is prepared to provide core service certification with a minimum of effort for add on Services.

3.6 USA: Federal Risk and Authorization Management Program (FedRAMP)

Name of the programme: Federal Risk and Authorization Management Program (FedRAMP)[33]

Governing of the standard: The FedRAMP Joint Authorization Board (JAB)

Accreditation Body/Bodies: A board composed by NIST and the FedRAMP PMO review and approve qualified 3PAOs (Third Party Assessment Organizations), which are the assessors accredit to perform conformity assessment.

Table 6 - FedRAMP

Scope: Security and privacy
Cloud-relevance: FedRAMP is cloud specific accreditation programme

[33] http://www.gsa.gov/portal/category/102371?utm_source=OCSIT&utm_medium=print-radio&utm_term=fedramp&utm_campaign=shortcuts.

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

Type of certifiable organisation: SaaS, PaaS, IaaS
Type of trust models applicable: Third party assessment
Is the certification proprietary or open: Open
Programme, status (operational, in development): Operational

The following text is based on information received by NIST and by the USA General Service Administration (GSA):

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based services. FedRAMP uses a "do once, use many times" framework that intends to saves costs, time, and staff required to conduct redundant agency security assessments and process monitoring reports.

The purpose of FedRAMP is to:

- Ensure that cloud based services have adequate information security.
- Eliminate duplication of effort and reduce risk management costs.
- Enable rapid and cost-effective procurement of information systems/services for Federal agencies.

FedRAMP is the result of close collaboration with cybersecurity and cloud experts from GSA, NIST, DHS[34], DOD[35], NSA[36], OMB[37], the Federal CIO Council[38] and its working groups, as well as private industry.

The FedRAMP assessment process is initiated by agencies or cloud service provider (CSPs) beginning a security authorization using the FedRAMP requirements which are FISMA compliant and based on the NIST 800-53 rev3 and initiating work with the FedRAMP PMO.

CSPs must implement the FedRAMP security requirements on their environment and hire a FedRAMP approved third party assessment organization (3PAO) to perform an independent assessment to audit the cloud system and provide a security assessment package for review.

The FedRAMP Joint Authorization Board (JAB)[39] will review the security assessment package based on a prioritized approach and may grant a provisional authorization. Federal agencies

[34] http://www.dhs.gov.
[35] http://www.defense.gov.
[36] http://www.nsa.gov.
[37] http://www.whitehouse.gov/omb.
[38] https://cio.gov.
[39] http://www.gsa.gov/portal/content/134223.

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

can leverage CSP authorization packages for review when granting an agency Authority to Operate (ATO) saving time and money.

FedRAMP uses a security risk model that can be leveraged among agencies based on a consistent security baseline. FedRAMP provides processes, artefacts and a repository that enables agencies to leverage authorizations with:

- Standardized security requirements and on-going cyber security for selected information system impact levels.
- Conformity assessment program that identifies qualified independent, third-party assessments of security controls implemented by CSPs.
- Standardized contract language to help agencies integrate FedRAMP requirements and best practices into acquisitions.
- Repository of authorization packages for cloud services that can be leveraged government-wide.
- Standardized On going Assessment and Authorization processes for multi-tenant cloud services.

The FedRAMP security authorization process has four distinct areas:

I. **Security Assessment**.

A CSP or an agency may request a provisional Authority to Operate (ATO) granted by the JAB under the FedRAMP security assessment process. The process follows the NIST 800-37 risk management framework as tailored for a shared responsibility environment. The CSP identifies the appropriate baseline; implements appropriate security controls, and documents the implementation. The CSP contracts with an accredited Third Party Assessment Organizations (3PAO) to independently verify and validate their security implementations and their security assessment package. The CSP submits the package to FedRAMP for review. Once documentation and test results are completed, the assessment is measured against the FedRAMP requirements and if the JAB is satisfied that the risks are acceptable, a Provisional Authorization is granted. Agencies can then leverage the JAB Provisional Authorization as the baseline for granting their own ATO.

II. **Leverage the Authority to Operate (ATO).**

The PMO will maintain a repository of FedRAMP Provisional Authorizations and associated security assessment packages for agencies to review. Agencies can use the Provisional Authorizations and security assessment packages as a baseline for granting their own ATO. If necessary, agencies can add additional controls to the baseline to meet their particular security profile.

III. **On-going Assessment and Authorization (Continuous Monitoring).**

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

For systems with a Provisional Authorization, FedRAMP, in conjunction with the DHS, conducts on going assessment and authorization (continuous monitoring) activities. On-going assessment and authorization (continuous monitoring) determines if the set of deployed security controls continue to be effective over time.

IV. PAO Accreditation.

CSPs applying for an ATO must use an accredited 3PAO. A review board, with representation from NIST and the FedRAMP PMO, accredits 3PAOs. The approval process requires applicants to demonstrate their technical capabilities and their independence as an assessor. The approval process follows the conformity assessment approach outlined in ISO/IEC 17020. FedRAMP maintains a list of approved 3PAO from which CSPs can choose.

3.7 Singapore: Multi-Tier Cloud Security (MTCS)

Name of the programme: SS584 - Multi-Tier Cloud Security (MTCS)[40].

Governing of the standard: Cloud Computing Standards Coordinating Task Force appointed by IT Standard Committee (ITSC).[41]

Accreditation Body/Bodies: Five qualifying certification bodies – the British Standard Institute, Certification International Pte Ltd[42], DNV Business Assurance[43], SGS International Certification[44] and TUV SUD PSB Certification[45].

IDA (Infocomm Development Authority of Singapore)[46] will be working to cross-certify the MTCS SS with other international standards or certification schemes – such as the International Standard Organization (ISO) 27001 Information Security Management System (ISMS)[47] and Cloud Security Alliance (CSA) Open Certification Framework (OCF) – to help those CSPs already certified against them to meet SS 584.

Table 7 - Singapore

Scope: Sound risk management and security practices for Cloud Computing, Transparency

[40] https://www.ida.gov.sg/~/media/Files/About%20Us/Newsroom/Media%20Releases/2013/1311_cloudasia/MTCSFactSheet.pdf.
[41] http://www.itsc.org.sg.
[42] http://www.sac-accreditation.gov.sg/cab/acab/pages/cabdetails.aspx?pk=0056-MS-MSBC-01.
[43] http://www.dnvba.com/Global/Pages/default.aspx.
[44] http://www.sgs.com.
[45] http://www.tuv-sud-psb.sg.
[46] http://www.ida.gov.sg.
[47] http://www.bsigroup.com/en-GB/iso-27001-information-security/.

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

and accountability in the cloud
Cloud-relevance: The SS 584 is the world's first cloud security standard that covers multiple tiers and can be applied by Cloud Service Providers (CSPs) to meet differing cloud user needs for data sensitivity and business criticality.
Type of certifiable organisation: Cloud Service Providers (CSPs)
Type of trust models applicable: Third-party certification and a self-disclosure requirement.
Is the certification proprietary or open: Open
Programme, status (operational, in development): Operational

In April 2012, Infocomm Development Authority of Singapore initiated the formation of an industry working group under the purview of the Information Technology Standards Committee (ITSC) to undertake the development of multi-tier cloud security (MTCS) standard. This standard describes the relevant cloud computing security practices and controls for public cloud users, public cloud service providers, auditors and certifiers. Recognising security risk requirements differ from users to users, different control measures are specified for different levels of security requirements in this multi-tier model.

MTCS seeks to address needs such as transparency of cloud users. Transparency is a way to build trust between CSPs & cloud users.

With the new standard, certified CSPs will be able to better spell out the levels of security that they can offer to their users. This is done through third-party certification and a self-disclosure requirement for CSPs covering service-oriented information normally captured in Service Level Agreements. The disclosure covers areas including: Data retention; data sovereignty; data portability; liability; availability; BCP/DR; incident and problem management.

MTCS SS has three different tiers of security, Tier 1 being the base level and Tier 3 being the most stringent.

- **Tier 1** – Designed for non-business critical data and system, with baseline security controls to address security risks and threats in potentially low impact information systems using cloud services (e.g.: Web site hosting public information).
- **Tier 2 –** Designed to address the need of most organizations running business critical data and systems through a set of more stringent security controls to address security risks and threats in potentially moderate impact information systems using cloud services to protect business and personal information (e.g.: Confidential business data, email, CRM – customer relation management systems).

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

- **Tier 3 –** Designed for regulated organizations with specific requirements and more stringent security requirements. Industry specific regulations may be applied in addition to these controls to supplement and address security risks and threats in high impact information systems using cloud services (e.g. highly confidential business data, financial records, medical records).

3.8 China

Name of the programme: Information Security Technology - Security Capability Requirements of Cloud Computing Services[48]; 2. Information Security Technology - Security Guide of Cloud Computing Services[49].

Governing of the standard: China's National Information Security Standards Technical Committee (TC260).

Accreditation Body/Bodies: TC260

Table 8 - China

Scope: Cloud security
Cloud-relevance: Security guides and security requirements for the cloud
Type of certifiable organisation: Cloud computing services
Type of trust models applicable: Third party
Is the certification proprietary or open: Open
Programme, status (operational, in development): In development

The Chinese cloud security national standard is currently under development with the first round of public comments. Developed by TC260, the standardization group in charge of security standards development, there are 2 standards in total:

48 http://www.tc260.org.cn/getIndex.req?action=quary&req=modulenvpromote&id=2366&type=0&moduleId=656&sid=45.

49 http://www.tc260.org.cn/getIndex.req?action=quary&req=modulenvpromote&id=2365&type=0&moduleId=656&sid=45.

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

- Information Security Technology - Security Capability Requirements of Cloud Computing Services.
- Information Security Technology - Security Guide of Cloud Computing Services.

The standard sets guidelines for data retention, data sovereignty, identity management, cloud service provider size and operational experience, and business dealings between cloud service providers and government customers. Initial drafts were completed without formal industry participation, as foreign companies are restricted from becoming voting members of TC260.

3.9 Hong Kong

Name of the programme: Practice Guide for Procuring Cloud Services[50]

Governing of the standard: Office of the Government Chief Information Officer (OGCIO), Government of Hong Kong:

I. Working Group on Cloud Computing Interoperability Standards (WGCCIS).
II. Working Group on Cloud Security and Privacy (WGCSP).
III. Working Group on Provision and Use of Cloud Services (WGPUCS).

Accreditation Body/Bodies: It is not a certification.

Table 9 - Hong Kong

Scope: Security
Cloud-relevance: It refers to all types of service models (SaaS, PaaS, IaaS) and to all deployment models (Public, Hybrid, Private, Community).
Type of certifiable organisation: Mostly intended for small and medium enterprises (SMEs).
Type of trust models applicable: n/a
Is the certification proprietary or open: The documentation is freely available
Programme, status (operational, in development): n/a

The Practice Guide of Procuring Cloud Services is a collection of best practices and guidelines that is aimed mostly at users that are willing to adopt cloud technology. It lists a set of challenges and points of consideration that potential customers of the cloud should keep in

[50] http://www.infocloud.gov.hk/home/10791?lang=en.

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

mind when designing applications that are going to be deployed in the cloud. It is written in natural language and addresses a series of problems that exist in the domain of cloud computing that users need to be aware when shifting their businesses in the cloud in order to get the best out of it without compromising security.

The core aspects that are being examined in Practice Guide of Procuring Cloud Services are the following:

I. Service Cost
II. Service Level Agreements (SLA) & Service Level Objectives (SLO)
III. On Boarding & Off Boarding
IV. Service Operation
V. Security and Privacy Protections
VI. Service Commitments/Warranties
VII. Data Ownership & Location and IP Ownership
VIII. Service Default
IX. Contracting (Terms of Service)

3.10 Australia

Name of the programme: Cloud Computing Security Considerations[51]

Governing of the standard: Australian Government – Department of Defence

Accreditation Body/Bodies: CSOC–Cyber Security Operations Centre

Table 10 - Australia

Scope: Availability of data and business functionality Protecting data from unauthorized access Handling security incidents
Cloud-relevance: It refers to all types of service models (SaaS, PaaS, IaaS) and to all deployment models (Public, Hybrid, Private, Community).
Type of certifiable organisation: Any agency that wishes to migrate to the cloud.

[51] http://www.asd.gov.au/infosec/cloudsecurity.htm.

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

Type of trust models applicable: Self-attestation.
Is the certification proprietary or open: Open
Programme, status (operational, in development): Operational

The Australian Department of Defence issued the Cloud Computing Security Considerations, which explains several cloud related terms such as delivery models, deployment models and service types and benefits.

The document targets users with the aim of increasing their understanding of the fundamentals of the cloud computing paradigm and helps them identify security threats that might have a malicious impact on their applications and data deployed in the cloud. Instead of being a list of security issues that need to be taken into account, they are expressed as a series of questions that need to be answered by the potential user and can help the user understand the risks that he or she might be taking when migrating to the cloud.

This document is also aimed at providing the means for agencies to perform a risk assessment to determine the viability of using cloud-computing services. This assessment is based on a list of thought-provoking questions on the risks associated with adoption of cloud services. The ultimate goal of the guidelines is to facilitate business and IT professionals to make more informed decisions and determine the extent to which cloud meets their strategic business goals while mitigating the risks involved.

3.11 New Zealand

Name of the programme: Cloud Computing Code of Practice[52]

Governing of the standard: Institute of IT Professionals (IITP) New Zealand

Accreditation Body/Bodies: Institute of IT Professionals (IITP) New Zealand

Table 11 - New Zealand

Scope:
Ownership of Information
Security
Data location
Data access and use
Backup and maintenance

[52] https://www.thecloudcode.org/.

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

Geographical Diversity SLA and Support Data Transportability Business Continuity Ownership of Application Customer Engagement Data Breaches Law Enforcement Region Specific Issues
Cloud-relevance: It refers to all types of cloud services and models.
Type of certifiable organisation: Any providers operating in New Zealand and any New Zealand provider that operates outside the country.
Type of trust models applicable: Benchmark-test
Is the certification proprietary or open: Open
Programme, status (operational, in development): Operational

Cloud Code allows providers to expose specific details about the way they treat their clients' data and applications. It gives users the opportunity to have a closer look to the in-house operations that take place within the provider's infrastructure.

Providers that wish to be certified need to disclose a series of information that are related to certain internal operations that are of interest for potential customers. That information is then stored in centralized database where potential users of the providers can consult in order to assess whether the providers can meet their security and operation requirements. This providers a common framework that can help users evaluate the applicability and efficiency of providers for their systems allowing them to know beforehand how their data will be treated.

3.12 Other certifications schemes

Other certifications scheme available for the EEA market or currently under development, but not described in details in this chapter are: TUV Rheinland[53]; ISO 20000 / ITIL[54]; PCI – DSS[55]; LeetSecurity Rating[56]; Cloud Industry Forum / Code of Practice[57].

[53] http://www.tuv.com/en/corporate/business_customers/consulting_and_information_security/strategic_information_security/cloud_security_certification/cloud_security_certification.html.
[54] http://en.wikipedia.org/wiki/ISO/IEC_20000.

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

The main reasons why we did not provide further details about those schemes are:

- The fact that a certain scheme is not cloud security/privacy specific.
- The lack of information.
- The decision taken by other organization (e.g. ETSI[58]) to consider a certain scheme as not developed by a Standard Organization and therefore potentially unsuitable.

The content of the chapter will reviewed based on further input that will be collected by the CloudWATCH project during the period from month 4 to month 18 of project.

During the period the list of certification schemes analysed in this report will ne most likely extended.

[55] https://www.pcisecuritystandards.org/security_standards/.
[56] http://www.leetsecurity.com.
[57] http://www.cloudindustryforum.org/code-of-practice/the-business-case.
[58] http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF.

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

3.13 Mapping schemes with objectives and features

In this chapter we include a mapping between the key objectives and features identified in chapter 3 and the operational certification described in chapter 4. For the purpose of this mapping we only considered certification schemes, which are already operational. The inputs collected are summarized in the tables below.

The approach used in the mapping has been the following:

- Assigning a "**YES**" when from the analysis of the information in presented in chapter 4 is was clear that the scheme provides certain feature / support a certain objective.
- Assigning a "**NO**" when from the analysis of the information in presented in chapter 4 is was clear that the schemes doesn't provide a certain feature / doesn't support a certain objective.
- Assigning a "**PARTIAL**" when from the analysis of the information in presented in chapter 4 it was not clear if the scheme provides the feature/support the objective (e.g. there are not enough evidences).

The table below shows the outcomes of the mapping exercise and provide an imperfect summary of the key objectives identified by the EC SIG Certification that each certification schemes is able to support as well as a summary of the key features characterizing the schemes.

This mapping will be reviewed based on further input that will be collected by the CloudWATCH project during the period from month 4 to month 16 of project.

The new input and possible amendment to this mapping will be incorporated in the final report on Cloud certification guidelines and recommendations.

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

Table 12 - Mapping schemes: objectives

Mapping schemes / objectives						
Certification Scheme	**Improve trust**	**Improve security**	**Efficiency of procurement**	**Compliance**	**Transparency**	**Cost-effective**
ISO 27001	Yes	Yes	Partial	Partial	No	Yes
SOC 1-2-3-	No	Yes	No	Partial	No	Partial
CSA STAR – OCF	Yes	Yes	Yes	Partial	Yes	Yes
EuroPrice	Partial	Partial	Partial	Partial	Partial	Partial
ECSA	Partial	Yes	Yes	Partial	Partial	Partial
USA-FedRAMP	Yes	Yes	Yes	Yes	Yes	No
Singapore-MTCS	Yes	Yes	Yes	Yes	Yes	Yes

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

Table 13 - Mapping schemes: features

Mapping schemes / features							
Certification Scheme	**Transparency**	**Scalability**	**Flexibility**	**Privacy-relevance**	**Comparability**	**Specific**	**Global**
ISO 27001	No	Yes	Partial	Partial	No	No	Yes
SOC 1-2-3-	No	Yes	No	Partial	No	No	Yes
CSA STAR – OCF	Yes	Yes	Yes	Partial	Yes	Yes	Yes
EuroPrice	No	No	No	Yes	No	No	No
ECSA	Partial	Yes	Partial	Partial	Partial	Yes	No
USA-FedRAMP	No	Yes	No	Partial	Yes	Yes	No
Singapore-MTCS	Yes	Yes	Yes	No	Partial	Yes	No

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

4. Recommendations and Conclusions

In this chapter we draw conclusions and provide recommendations based on the analysis of the input collected.

4.1 Conclusion 1 – Transparency

Audience: Cloud Customers - Cloud Providers - Policy makers

A suitable certification scheme should support transparency to the highest degree. Providing visibility into the security and privacy capabilities of a cloud services gives the opportunity for:

- cloud customers (both in the privacy and public sector) to make more informed and risk based decisions when selecting/assessing a service
- cloud providers that offer better security capabilities and that are more privacy-minded to differentiate their service
- policy makers to better understand the functioning of the market and avoid unnecessary regulatory intervention or intervene in a more targeted and focused way in the market requires a regulatory intervention.
- transparency in general as a trust-enabling factor

Most of the certification schemes considered in our analysis have some promising transparency features, but in most cases the level of visibility and information available about the certification process, the process of accreditation of auditors, the underlying standard(s), the audit results and report are not yet sufficient for cloud customer to make informed decision and for cloud provider to make of security and privacy excellent a competitive advantage.

4.2 Recommendation 1 – Transparency

We recommend cloud customers, especially public administrations, to adopt a cloud selection process (e.g. call for proposal, request for proposal, etc.) which favours certifications/attestations that clearly support transparency. It is of particular importance for a procurement officer to have a clear visibility on the details of technical standard(s) on which the certification assessment is based on (i.e. clear understanding of the technical controls and control objectives included in the standard). Knowing which technical controls are included in a standard is the only way to understand if that technical framework, and the certification scheme it is based upon, is suitable to satisfy the technical requirements and compliance needs of a certain organization.

Moreover importance should be given to the quality of the assessment/audit, therefore we recommend cloud customer to look for certification schemes that provide transparency into the certification process as well as the process of accreditation of auditors. A rigorous, consistent and transparent process of auditor accreditation should be seen an essential feature of in a certification scheme, as this will provide a reasonable level of assurance that

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

only qualified and reputable auditors are allowed to issue certificate and that the results of a certification assessment are consistent and comparable.
This recommendation is mainly addressed to public sector procurement offices, since they have the necessary negotiation power to demand for specific features and services.

We also recommend Cloud Providers to introduce more transparency in their information security approaches. They should be willing to provide as much details as possible about the results of their certification assessment reports. We do not suggest an approach based on full disclosure, as we do appreciate that in some cases this is not possible given the confidentiality of some information included in the assessment report, but we do recommend to providers not to hide information that is relevant to regulatory authorities and customer behind unreasonable confidentiality claims.

We recommend policy makers to work on soft-law to foster transparency by supporting certification schemes that enable transparency. We have already mentioned in our conclusion that transparency is a fundamental attribute of accountability and essential trust-enabling component. As such the adoption of soft-law supporting transparency could eliminate the need for more strict binding regulatory intervention, which might not be the most appropriate measure in a market that is still immature and in continuous transformation.

4.3 Conclusion 2 – Scalability, Flexibility, Cost efficiency

Audience: Cloud Customers - Cloud Providers - (Policy makers)

Certification scheme should be scalable, flexible and cost efficient in order to be able to accommodate the needs of:

- Organizations operating in highly regulated sectors (e.g. healthcare, finance, public administration), as well as organisation operating in less or non-regulated business sectors,
- Organization of all sizes (small and medium companies as well as big corporation), operating at various layers of the cloud stack (SaaS, PaaS, IaaS, XaaS) and with different budgets for information security, auditing and compliance programmes.
- Organization with varying assurance requirements, going from those companies operating in critical sectors (e.g. critical information infrastructure) and therefore demanding high level of assurance (e.g. certification based on accredited third party independent assessment or continuous monitoring based certification/attestation) to those organisations operating in non-critical business areas and therefore satiable with a self-certification.
- Flexibility should be also understood as the capability of the technical standard underlying a certification scheme to accommodate changes in the legal and regulatory framework and as well as advancement and changes in the technology landscape.

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

Most of the certification schemes considered in our analysis appear to provide the necessary level of scalability, some seem to be cost efficient, but only a few clearly provide the necessary level of flexibility. This lack of flexibility could represent a potential problem since it might prevent, in some cases, the technical framework underlying the schemes from being able to change at the same pace as the cloud market, therefore failing to satisfy changing requirements.

Moreover it appears that only a few certification schemes are able to address the needs of organizations with varying levels of assurance (e.g. very few schemes are based on a maturity /capability model, and very few include the self-certification option).

4.4 Recommendation 2 – Assurance

Audience: Policy makers - Cloud Customers

We recommend policy makers to endorse/demand for certification schemes that are able to provide scalability, flexibility and cost efficiency and to match the different assurance levels requested by regulatory authorities and customers of any kind (pubic administration, micro, small medium companies and enterprise). There is a clear trade-off between the levels of rigour and the cost of certification (obviously self-certification is less expensive than a certification based on third party assessment). As such, to make the market more efficient each actor should be given the possibility to select the most cost effective solution to satisfy its assurance needs.

We address a similar recommendation to cloud customer, who should be asking providers for certifications that match their assurance requirements.

IMPORTANT NOTE: The conclusion and recommendation might be reviewed based on further input that will be collected by the CloudWATCH project during the period from January to June 2014,and beyond that, if necessary.

Although we do not expect any major change in the key elements of our findings and recommendations, new developments in the cloud market as well as upcoming evolutions in the legal framework may lead us to formulate further recommendations in the future.

5. Next steps

This current version of the report will be updated during period from M4 to M18.
The objective of the revision of this initial version will be to:

- Analysing the change in the cloud certification landscape 12 month after the issuing of the version 1 of the report
- Validate the initial recommendations included in V.1
- Collect input to define a final set of recommendation from the CloudWatch project in the area of security and privacy certification for cloud computing.

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

The necessary input to review the current version of D4.1. will be collected though the participation of the Cloud Watch consortium members into relevant fora (EC C-SIG, ENISA expert groups, etc), the feedback from the dissemination and educational events organised in the context of the CloudWatchHUB (e.g. webinar), the results of a new survey to be launched in November 2014 (see Annex 3).

The final version of D4.1 - Cloud certification guidelines and recommendations will be delivered in February 2015, at M18 of the CloudWatch project and will be part of the CloudWatchHUB awareness campaign for cloud adoption.

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

Annex 1 – SIG Certification Survey

In March 2013, the EC on Cloud Certification Selected Industry Group (SIG Certification) prepared and launched a survey with the objectives of identifying most relevant high objectives and features for a cloud certification scheme for security governance.

The survey was prepared by Cloud Security Alliance and ENISA and reviewed by the other members of the SIG Certification[59].

We report below the short questionnaire, which also collected the respondent's **name**, **organization** and **sector**.

The certification SIG will produce a list of information security certification schemes which are fit-for-purpose to certify cloud computing services. As a first step, we are collecting views from SIG members on high level objectives and important features a certification scheme should have for inclusion in this list, as well as an initial list of candidates for inclusion in the list. Please complete the following. NB we have suggested some possible answers for the first two questions to avoid duplication of effort.

What are the most important high-level objectives for a certification scheme. Check below if you agree/disagree with any of the following and add any additional principles/clarifications.

For each one, a choice of 1-5

1. *definitely exclude from the list of important objectives*
2. *this objective is only marginally relevant*
3. *include in the list*
4. *highly relevant*
5. *must-have*

1. *To improve customer trust in cloud services*	
2. *To improve security of cloud services*	
3. *To increase the efficiency of cloud service procurement*	
4. *To make it easier for cloud providers and customers to achieve compliance*	
5. *To provide greater transparency to customers about provider security practices*	

[59] https://www.surveymonkey.com/s/MM8DXG2.

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

6. *To achieve all the above objectives as cost-effectively as possible.*	
7. *Other - add your own objective. Free text and relevance score 1-5*	

2. What are the most important features of certification schemes and their underlying standards. Check below if you agree/disagree with any of the following and add any additional criteria/clarifications.

For each one, a choice of 1-5

1. *definitely exclude from the list of important features*
2. *this feature is only marginally relevant*
3. *include in the list*
4. *highly relevant*
5. *must-have*

1. *Comparability – results should be repeatable, quantifiable and comparable across different certification targets.*	
2. *Scalability - the scheme can be applied to large and small organisations.*	
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 (crocodiles rather than security guards e.g.).*	
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.*	

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

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 allows consumer to tell 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 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*	
26. *Other - add your own – free text and relevance score (1-5)*	

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

3. *Please provide us with cloud-relevant certification programmes. Fill in an as many of the fields as possible but if you are short on time, even a name and URL is enough.*

Schemes Description	
Name of programme:	
URL:	
Governing body of standard:	
Accreditation body(ies):	
Scope: E.g. data protection	
Cloud-relevance:	
Type of certifiable organisation:	
Type of trust models applicable: self-attestation/third-party/benchmark-test:	
Description - please add information on e.g. the certification, accreditation and certification scheme:	
Is the certification proprietary or open:	
Programme, status (operational, in development):	

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

Annex 2 - Report on the CloudWATCH Workshop at EGI TF

Workshop title: Certification & testing standard compliance Workshop,

Venue and data: EGI Technical Forum, 17 September 2013, Madrid

Workshop objectives: The workshop was aimed at defining principles and specifications for the creation of an open schema to certify organisations and services against existing Cloud requirements and technical Cloud profiles. It also aimed to collect valid input to develop "Cloud certification and recommendation guidelines". The workshop was based on existing material, existing cloud specific certification schema, and under development and cloud specific certificaion schemas.

Chair: Daniele Cattedu, Cloud Security Alliance (CSA)

Speakers: Tjabbe Bos, European policy, European Commission; Tom Nicols, British Institute of Standards (BSI), "Certifying information security in the cloud"; Owen Appleton, Emergence Tech, "Initiatives focused on management certification, FedSM"; Daniele Cattedu, CSA, "CSA's Cloud Control Matrix, including its relevance for the activities of BSI".

Main discussion points and conclusions

- The participants agreed that there is a general consensus on the approach adopted by CloudWATCH, specifically the approach adopted by CSA.
- It is important to note the different perspectives and concerns across enterprise, government and research. Security and data are both good examples of these differences, where the research community has different concerns. This finding is also collaborated by the XSEDE Survey Report, which concludes that the willingness to share, especially in trusted environments and partnerships, probably explains why security and data score lower as concerns in the research community.
- Different requirements in public administrations and current local/national regulations in Europe are equally important. Germany is a good example of this with its particularly strict data protection regulations in relation to cloud adoption. Generally, key concerns include data crossing borders, ensuring security is not compromised.

- **EU policy perspectives**

Certification is a key action in the **European Cloud Computing Strategy** (September 2012) and related to defining the extent to which Europe is cloud friendly and cloud active. It is essential that we ensure transparency in the marketplace and guarantee confidentiality in the cloud. A multi-stakeholder dialogue is key to achieving more transparency.

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

These strategic actions are also linked with objectives of the **Digital Agenda for Europe** in terms of **data protection** and **network security**, arriving at a **common legal framework** to facilitate the development of cloud computing. The ultimate goal is to facilitate the development of cloud computing.

Standards are one of the most effective ways of achieving greater clarity around users' needs. Certification means providers using specific standards. This is important because customers need assurance. The work **ETSI** has been tasked to do is aimed at increasing clarity, specifically on what users really need.

Measures need to be easy for users to follow. Certification can offer a good solution even though it cannot give all the answers. There are already some certification schemes, e.g. the Cloud Security Alliance. The **Selected Industry Group** (SIG) certification expert group supports the EC in implementing action 1 of the Europe Cloud Strategy. The SIG-certification agreed that the group will produce a list of security certification requirements and schemes which are fit-for-purpose to certify cloud computing services. The SIG has worked with the EC to provide a list of schemes: some are sector specific, others are country specific but there is also some overlap. How do these schemes overlap?

The SIG has highlighted that it is important that schemes are based on real customer needs; that they need to be flexible and that they are not too costly. However, there is also some friction, e.g. around self-certification, because it is not customer-centric. There are no clear answers yet on this approach to certification.

ENISA has been tasked with making an assessment of certification schemes to ensure a better understanding of the schemes, moving beyond the current classification. This assessment will look at:

- What standards are they building on?
- Are these standards open?
- Are these standards relevant to cloud computing?
- Do they deal with governance?

ENISA is developing a **framework** and has talked to the owners of these schemes. The assessment is expected in late September and will be presented to the SIG in October[60]. One of the aims is to also involve customers to discuss preliminary results, as well as to understand which standards can already be certified.

- **Certifying information security in the cloud**

[60] https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy

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

ISO 27001 is the international standard for information security. It was developed from BS 7799. There are over 17,500 organisations certified globally in over 120 countries. A new version of the standard is due for release (no date given). It is a management systems standard, outlining the processes and procedures an organisation must have in place to manage Information **Security issues** in core areas of business. The standard does not stipulate exactly how the process should operate.

Risk assessment is key to ensure that a certification scheme works effectively (are people sufficiently trained? Are there sufficient resources? What are the real requirements with regards to risk? What checks and processes have been put in place? Is the standard getting to the heart of the problem? What do we need to do to make it appropriate?).

Gaps identified:

- Out of date: The suggested list of risk assessment and controls was written in 2005 (Annex to ISO27001). ISO27001 is updated every 8 years, which means that the controls soon become obsolete.
- Make it more relevant to today's digital marketplace.
- Coverage not broad enough: It is a "one-size-fits-all" that does not cover some industry specific concerns. Control objectives and controls listed in Annex A are not exhaustive.
- What has actually been certified? Any standard can become a lowest common denominator. People can certify any scope they like within their organization.

CSA's Cloud Control Matrix (CCM) will fill specific needs. Hence the BSI has teamed up with CSA to work on common goals. The main motivations are:

- It works with other standards: ISO27001, COBIT[61], NIST SP800-53, FedRamp. PCI[62], BITS[63], GAPP[64], Jericho Forum[65], NERC CIP[66].
- It was written with the intention of being publicly available.
- It will be updated to keep pace with changes.
- It is driving continuous improvements.

While the management system can stay static, the controls can be changed and adapted. Cloud specific controls are currently missing but are a requirement.

---

[61] http://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx.
[62] https://www.pcisecuritystandards.org.
[63] http://www.bits.org.
[64] http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/GENERALLYACCEPTEDPRIVACYPRINCIPLES/Pages/default.aspx.
[65] http://www.opengroup.org/getinvolved/workgroups/jericho.
[66] http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

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

Many standards are in substance guidelines on best practices. What we need is the ability to tick specific points, like Do you have X? Yes/No. A best practice does not allow this.

Should we have different levels of certification? Gold, silver, bronze

Management Capability (Maturity) Scores

- The audit approach is aimed at continual improvement.
- It can allay the risk of standards becoming the lowest common denominator.
- It would help draw attention to the management system and prevent certification becoming the end of the journey.

Maturity models are not new, especially in the IT sector. However, 3rd party auditing of them is less common. BSI and TICKIT Plus[67] has done it, so it could become more widespread.

In summary: ISO27001 is a core system required to manage information security. Cloud controls are focused on areas that are critical to cloud computing. Drive the use of an auditable framework to assess maturity (maturity models). The expected impact of the STAR Certification is to increase security, trust and assurance in cloud services.

- **Lightweight standards and service management in federated clouds**

FedSM[68] aims at improving IT Service Management (ITSM) in federated e-Infrastructures through the introduction of techniques and approaches from commercial ITSM. FITSM is focused on service management. CloudWATCH could consider service management standards, especially the most relevant ones for federated clouds. FitSM is a lightweight federate service management standard that could be considered in this regard. It provides a baseline for service management in a way that is enough to be effective and as a basis for the further development of the ISO 20k standard family.

Federation management issues are:

- Collaboration not hierarchy
- Heterogeneous federation members, vary by:
  - Country
  - Sector
  - Org type (academic, commercial, public sector)
- Lack of cohesive provider management
- Some: lack of ITSM knowledge in general (new providers)
- Others: ITSM varies across federation
- Passive customers

[67] http://www.tickitplus.org.
[68] http://www.fedsm.eu/.

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

- Do not state or require specific service levels

Because providers do things in different ways, there needs to be cohesion around the services provided, e.g. EGI is a service provider and though it has many years' experience in service level agreements, it is not linked to a blueprint that helps develop a service. We therefore need a simple starting point, a common way of talking about service management, making it more realistic and re-working people's roles rather than changing them. FITSM focuses on the core services, following a "bit at a time" approach and creating a baseline for federated services rather than straight to the full system. Guided self-assessments enable the mapping of processes; evaluating the extent to which the criteria is met. IT Service management for clouds is essential for hybrid, multi-provider and federated scenarios.

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

Annex 3 – Second survey – D4.1. final version

Annex 3 includes the set of questions that will be included in the second survey that will be launched under Task 4.3 of the CloudWatch project in November 2015.

This survey has been designed to collect information to be used in the drafting of the V2 of the CloudWatch report: "Cloud certification: guidelines and recommendations".

The survey has a threefold objective:

- Collect data for analysing the change in the cloud certification landscape 12 month after the issuing of the version 1 of the report
- Validate the initial recommendations included in V.1
- Collect input to define a final set of recommendation from the CloudWatch project in the area of security and privacy certification for cloud computing.

QUESTIONNAIRE

1. Are you a:
    a. Cloud customer (current)
    b. Cloud customer (potential)
    c. Cloud provider
    d. Both (please specify)

2. In which business sector do you work:
    a. Private sector (please specify)
    b. Public sector (please specify)
    c. Other (please specify)

3. Based on your experiences, which one of the following can increase the level of trust of the Cloud computing services, making the market more reliable, secure and efficient?

For each one, a choice of 1-5

    1. *definitely not relevant / important*
    2. *only marginally relevant*
    3. *relevant / important*
    4. *highly relevant*
    5. *must-have*

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

1. *Risk assessment: Cloud customer performs risk assessment*	
2. *Risk assessment: the CSP performs risk assessment*	
3. *Clear, complete and comparable SLA*	
4. *CSP internal due diligence results (compliance with standards and regulations)*	
5. Third-party certification/attestation of CSP's	
6. Other (please specify):	

4. Based on your experiences, which of the following are the key criteria to be considered when assessing a Cloud security certification scheme

For each one, a choice of 1-5

1. *definitely exclude from the list of important criteria*
2. *this criteria is only marginally relevant*
3. *include in the list*
4. *highly relevant*
5. *must-have*

1. *Certification process for the certification scheme is transparent*	
2. *Only auditors accredited through a rigorous, consistent and transparent process should be qualified to conduct the assessment issue the certificate*	
3. *The cost (both financial and technical) is affordable for any kind of organization (e.g. the cost depends on the level of assurance provided/requested, the work done and the results obtained in other audit/certification/assessment can be leveraged, etc.)*	
4. The underlying technical standard(s) are publicly available.	
5. The underlying technical standard(s) are open standard(s)	
6. *Certification scheme is able to satisfy technical requirements and compliance needs of an organization*	
7. *Results of a certification assessment are consistent and comparable*	

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

8. *The Governance structure of the certification scheme guarantees independence, transparency and appropriate division of responsibilities*	

5. Based on the answers you have provided to the previous question (Q4), what are your expectations in terms of quality, transparency, assurance and cost? Please provide description of your expectation only for those options that scored 3 to 5 in the previous question.

1. *Certification process for the certification scheme is transparent*	
2. *Only auditors accredited through a rigorous, consistent and transparent process should be qualified to conduct the assessment issue the certificate*	
3. *The cost (both financial and technical) is affordable for any kind of organization (e.g. the cost depends on the level of assurance provided/requested, the work done and the results obtained in other audit/certification/assessment can be leveraged, etc.)*	
4. The underlying technical standard(s) are publicly available.	
5. The underlying technical standard(s) are open standard(s)	
6. *Certification scheme is able to satisfy technical requirements and compliance needs of an organization*	
7. *Results of a certification assessment are consistent and comparable*	
8. *The Governance structure of the certification scheme guarantees independence, transparency and appropriate division of responsibilities*	

6. Do you believe you have a sufficient knowledge about security and privacy certification schemes for clouds?:
    a. YES (I have a clear understanding of the available options)
    b. PARTIAL (I have some knowledge about some schemes, but I would require more details to be able to make an informed decision.
    c. NO (I do not have enough info about available schemes. This is due to lack of time from my side for assessment of the available information about the scheme

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

d. NO (I do not have enough info about available schemes. This is due to the fact that information about the schemes isn't easily available for consultation or completely missing).

7. Are you aware of the following Cloud certification schemes?

For each one, a choice of 1-5

1. *Unknown*
2. *Yes, not interested*
3. *Yes, not applicable*
4. *Yes, considering to use in future*
5. *Yes, already using the scheme*

ISO/IEC 27001	
SOC 1-2-3	
CSA STAR -OCF	
EuroPriSe	
Certified Cloud Service - TÜV Rheinland	
ECSA	
USA-FedRAMP	
Singapore-MTCS	
Other (please specify)	

8. Based on your answers on the previous question (Q7), please specify if you know and have access to (or if the general public can access) the technical standard (the set of technical controls) that is used in the auditing process associated to these certification schemes.

ISO 27001	
SOC 1-2-3	
CSA STAR -OCF	
EuroPriSe	
Certified Cloud Service - TÜV Rheinland	

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

ECSA	
USA-FedRAMP	
Singapore-MTCS	
Other (please specify)	

9. Based on your answers on question 7, please specify if you know and have access to (or if the general public can access) information about the Governance structure (who is the scheme owner, who is governing the underlying technical standard, who is running the auditor accreditation, is the there a separation of duties between who is owning the scheme and the auditors, etc.) of the certification schemes:

ISO 27001	
SOC 1-2-3	
CSA STAR -OCF	
EuroPriSe	
Certified Cloud Service - TÜV Rheinland	
ECSA	
USA-FedRAMP	
Singapore-MTCS	
Other (please specify)	

10. Based on your answers on question 7, please specify if you know and have access to (or if the general public can access) information about the process for certifying/accrediting/training the auditors:

ISO 27001	
SOC 1-2-3	
CSA STAR -OCF	

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

EuroPriSe	
Certified Cloud Service - TÜV Rheinland	
ECSA	
USA-FedRAMP	
Singapore-MTCS	
Other (please specify)	

11. Are certification schemes that you are aware of used to facilitate the procurement processes or requested as requirements in procurement processes?

ISO 27001	YES/NO – Specify
SOC 1-2-3	YES/NO – Specify
CSA STAR -OCF	YES/NO – Specify
EuroPriSe	YES/NO – Specify
Certified Cloud Service - TÜV Rheinland	YES/NO – Specify
ECSA	YES/NO – Specify
USA-FedRAMP	YES/NO – Specify
Singapore-MTCS	YES/NO –

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

	Specify
Other (please specify)	YES/NO – Specify

12. Which are, between the schemes you are aware of, the ones that are sufficiently mature?

ISO 27001	YES/NO – Why?
SOC 1-2-3	YES/NO – Why?
CSA STAR -OCF	YES/NO – Why?
EuroPriSe	YES/NO – Why?
Certified Cloud Service - TÜV Rheinland	YES/NO – Why?
ECSA	YES/NO – Why?
USA-FedRAMP	YES/NO – Why?
Singapore-MTCS	YES/NO – Why?
Other (please specify)	YES/NO – Why?

13. Based on your experiences, are there additional existing gaps, which are not addressed by the Cloud security and privacy certification schemes that you are aware of?
    a. No
    b. Yes (please specify): _____

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

14. In last 12 months, have Cloud certification schemes become better understood by CSP's or by Cloud customers? Do you see an increasing level of adoption in the last 12 months? Please reply: TRUE or FALSE the following:
    a. Both CSP's and Cloud customers are more aware of existing schemes and the level of adoption is increasing : TRUE / FALSE
    b. Both CSP's and Cloud customers a more aware of existing schemes, but the level of adoption is not increasing: TRUE / FALSE
    c. Cloud customers are more aware of existing scheme and are demanding to provider to get certified: TRUE / FALSE
    d. There isn't a sufficient level of awareness in the market: TRUE / FALSE

15. Based on your experiences, what are the most significant trends in the Cloud security and privacy certification landscape?
    Version 1 of the CloudWatch report included a set of recommendations that we would like you to validate.
    F*or each one, a choice of 1-3*
    1. *Strongly agree*
    2. *Partially agree (please clarify*
    3. *I disagree (please clarify)*

    a. **Supporting Transparency (1)**: It is of particular importance for a procurement officer to have a clear visibility on the details of technical standard(s) on which the certification assessment is based. Knowing which technical controls are included in a standard is the only way to understand if that technical framework, and the certification scheme it is based on, is suitable to satisfy the technical requirements and compliance needs of a certain organization.

    b. **Supporting Transparency (2)**: importance should be given to the quality of the assessment/audit. This recommendation is mainly addressed to public sector procurement offices, since they have the necessary negotiation power to demand for specific feature and service.

    c. **Appropriate level of detail on information security approaches:** Cloud Service Providers should introduce more transparency in their information security approaches. They should be willing to provide as much details as possible about the results of their certification assessment reports. We do not suggest an approach based on full disclosure, as we do appreciate that in some cases this is not possible given the confidentiality of some information included in the assessment report.

    d. **Soft law supporting transparency**: policy makers should work on **soft-law** to foster transparency by supporting certification schemes that enable transparency. Transparency is a fundamental attribute of accountability and essential trust-enabling component, and the adoption of soft-law supporting transparency could prevent the need of binding regulatory intervention that it might not be the most appropriate measure in a market,

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

underdevelopment and in continuous transformation.

e. **Assurance Certification schemes should provide scalability, flexibility & cost efficiency**: policy makers should endorse/demand for certification schemes that are able to provide scalability, flexibility and cost efficiency and to match the different assurance levels requested by regulatory authorities and customers of any kind (pubic administration, micro, small medium companies and enterprise). There is a clear trade-off between the levels of rigour and the cost of certification (obviously self-certification is less expensive than a certification based on third party assessment) and to make market more efficient each actor should be given the possibility to select the most cost effective solution to satisfy its assurance needs.

Annex 4 - References

[1] Cloud Select Industry Group: Research Priorities for a Competitive Cloud Computing Industry in Europe.

http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1624 -- Last accessed 15th Dec 2013.

[2] European Commission. (2012). Unleashing the Potential of Cloud Computing in Europe.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF. Last accessed 15th Dec 2013

[3] CSA. (2013). *Cloud Controls Matrix*.

https://cloudsecurityalliance.org/research/ccm/. Last accessed 15th Dec 2013.

Annex 5 - Document Log

DOCUMENT ITERATIONS		
V0.1	Table of content and initial text of chapter 1, 2, 3, and Annex 1 and 2.	Daniele Catteddu, Cloud Security Alliance
V0.2	Added text of chapter 4,5,6	Daniele Catteddu, Cloud Security Alliance
V0.3	Initial review from EGI	Michel Drescher, EGI
V0.4	Comments from EGI incorporated, and added new text in chapter 1, 2, 3.	Daniele Catteddu, Cloud Security Alliance

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

V0.5	Internal review from CSA team	Alain Pennetrat and Jesus Luna, Cloud Security Alliance
V0.6	Work on chapter 3	Marina Bregu and Konstantinos Mantzoukas, Cloud Security Alliance
V0.7	Review from TRUST-IT	Stephanie Parker, Trust-IT
V0.8	Comments from Trust-IT incorporate, added initial version of the chapter 4 included, list of acronyms, reference and executive summary	Daniele Catteddu, Marina Bregu Cloud Security Alliance
V0.9	Final review	Michel Drescher, EGI, Stephanie Parker, Trust-IT
V1.0	Final version	Daniele Catteddu, Cloud Security Alliance

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