CloudWatch

A European cloud observatory supporting cloud policies, standard profiles & services

Building trust in the cloud

Cloud Certification Recommendations

January 2014

www.cloudwatchhub.eu

CloudWATCH is funded by the European Commission Framework Programme
DG Connect Software & Services, Cloud. Contract No. 610994

SEVENTH FRAMEWORK PROGRAMME

European Commission

Security and Privacy Certifications

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 assumption, a number of efforts have been started in Europe at policy level, mainly led by the European Commission (EC) and their Special Industry Group on Certification, the European Union Agency for Network and Information Security (ENISA) and the European Telecommunications Standards Institute (ETSI), where CloudWATCH plays a role. There is now a growing interest in European solutions for cloud standards and software industry development beyond the European Union. Building on this work CloudWATCH aims to provide guidance to cloud service customers, cloud service providers and policy makers in their evaluation of suitable security and privacy certification schemes for cloud services.

The Challenge Today - Trust and confidence in cloud computing

"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.[...]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."

The ETSI Cloud Standards Coordination Report (November 2013)

Two strategic actions to overcome these challenges relate to better cloud certification schemes and better enforcement of legal obligations. Certification schemes should be based on the available set of security standards. Achieving these goals would enlarge the variety and coverage of services available with the right level of security and offer significant business opportunities to customers.

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.
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. Recommendations are of interest to 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 small and medium enterprises (SMEs) and large corporations; compliance managers of cloud service customers and compliance managers of cloud service providers.

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 into market differentiators
- Avoid unnecessary regulatory intervention
- Increase the level of trust in the cloud market

Scalability, flexibility and cost efficiency

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

- Organisations 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)
- Organisations with varying assurance requirements

Most of the certification schemes analysed have several 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.

Most of the certification schemes considered appear to provide the necessary level of scalability and a number appear to be cost efficient. However, only a few clearly provide the necessary level of flexibility. In some cases this lack of flexibility could represent a potential problem preventing the technical frameworks underlying the schemes from being able to evolve at same pace of the cloud market, and 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

Cloud customers, especially public administrations, require that their cloud service selection involves a process for 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 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 for specific feature and service.

Appropriate level of detail on information security approaches

We also recommend that Cloud Providers introduce more transparency in their information security approaches. They should be willing to provide as much detail 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.

Soft law supporting transparency

Further, we recommend that 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. The adoption of soft-law supporting transparency could prevent the need for binding regulatory intervention which might not be the most appropriate measure in a market that is underdeveloped and in continuous transformation.

Assurance Certification schemes should provide scalability, flexibility & cost efficiency

We recommend policy makers to endorse/demand certification schemes that provide scalability, flexibility and cost efficiency and to match the different assurance levels requested by regulatory authorities and all kinds of customers (pubic administration, micro, SMEs). 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.

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.

Cloud certification recommendations, January 2014

Main author: Daniele Catteddu, Cloud Security Alliance. Contributing authors: Marina Bregu, Jesus Luna, Konstantinos Mantzoukas, Alain Pennetrat, Cloud Security Alliance

Editor: Stephanie Parker, Trust-IT Services Ltd

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.

The CloudWATCH Consortium

Trust-IT Services Ltd
Communicating ICT to markets

CSA cloud security alliance

Fraunhofer FOKUS

EGI

DIGITALEUROPE

Oxford e-Research Centre

University of Oxford