CloudWatch

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

Building trust in the cloud through transparent, flexible and detailed cloud certifications

Cloud Certification Recommendations

March 2015

www.cloudwatchhub.eu

CloudWATCH is funded by the European Commission
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 services and stimulate their adoption. Based on this a number of efforts have begun in Europe at policy level mainly led by the European Commission (EC), in collaboration with the European Union Agency for Network and Information Security (ENISA) and the Clouds Standards Coordination (CSC) European Telecommunications Standards Institute (ETSI). These efforts have aroused much interest in European solutions for cloud standards and software industry development beyond the European Union.

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

The CloudWATCH project 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 work by ETSI and the EC's Cloud Select Industry Group , CloudWATCH aims to provide 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.

Main findings of the CloudWATCH analysis

Over the last 15 months, the CloudWATCH consortium has analysed currently available cloud security cetifications schemes with the following findings:

- » The majority 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.
- » While most certification schemes considered appear to provide the necessary level of scalability and some seem to be cost efficient, although 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 underlying technical frameworks from being able to evolve at same pace of the cloud market, therefore failing to satisfy changing requirements.
- » Only a few certification schemes are able to address the needs of organisations with varying level of assurance. For example, 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.

Add transperency requirements in the procurement process

We recommend that cloud customers, especially public administrations, adopt a cloud selection process that favours certifications/attestations which clearly support transparency. It is particularly important that the details of technical standard(s) on which the certification assessment is based is clear to procurement officers. 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 organisation. 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.

Introduce appropriate level of detail on information security approaches

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

Soft law supporting transparency

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. The adoption of soft-law supporting transparency could prevent the need binding regulatory intervention that might not be the most appropriate measure in a market which is still under development and in continuous transformation.

Increase trust through clearly defined SLAs

We recommend cloud providers and customers to clearly define the scope, requirements and monitoring parameters of the SLA based on their compliance needs. These may significantly differ from customer to customer. Policies and procedures should be implemented to ensure the consistent review of SLAs between providers and customers across the relevant supply chain.

Certification schemes should provide scalability, flexibility & cost efficiency

Finally, we recommend that policy makers endorse/demand 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 the 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, March 2015

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