Governance for CCSL and CCSM

Authors

Marnix Dekker, Dimitra Liveri, European Union Network and Information Security Agency (ENISA)

Contact

For enquiries about this document use: cloud.security@enisa.europa.eu

1 Background

The EU's cloud strategy, published in 2012, contains several key actions. Key action 1 called "Cutting through the Jungle of Standards" addresses, among other things cloud standards and cloud certification schemes. Specifically about certification it says the EC will:

"Work with the support of ENISA and other relevant bodies to assist the development of EU-wide voluntary certification schemes in the area of cloud computing (including as regards data protection) and establish a list of such schemes by 2014."

The EC set up a Cloud Select Industry Group (C-SIG) of experts from industry, industry associations and other interested stakeholders to discuss and agree on which steps to take in this direction. The C-SIG working group on Certification Schemes focuses on security certification schemes. The C-SIG working groups are open for participation to all interested stakeholders that are willing to contribute to the work.

At the end of 2013 ENISA, in collaboration and agreement with the EC and the members of the C-SIG working group on certification, published a short paper about certification in the cloud strategy. That paper provides a problem analysis and it motivates the development of **two tools** for existing and potential cloud computing customers in Europe[1]:

- **CCSL - Cloud Certification Schemes List**: CCSL is a list of (existing) certification schemes, relevant for cloud computing customers. CCSL provide potential customers with an overview of objective characteristics per scheme, to help them understand how the scheme works and if it is appropriate for their setting. CCSL was already implemented as an online tool and published in spring 2014. CCSL is being improved continuously and updated by ENISA and stakeholders from industry and public sector.

[1] Note that both tools are focused on customers but they may also be useful for providers.

- **CCSM - Cloud Certification Schemes Metaframework**: CCSM is a metaframework of existing certification schemes, which maps detailed security requirements used in the public sector to security objectives in existing cloud certification schemes. The goal of CCSM is to provide more transparency and help customers in the public sector with their procurement of cloud computing services.

This document describes how these two tools (CCSL and CCSM) are maintained and governed, and it details for example the type of maintenance ENISA carries out, how new schemes get listed, the role of the members of the C-SIG working group on certification, etc. This governance document is **publicly available**.

2 Technical implementation CCSL and CCSM

ENISA has built web applications implementing CCSL and CCSM. The tools can be found at: https://resilience.enisa.europa.eu/cloud-computing-certification/ Technically the two tools are extensions of Plone, an open source CMS.

2.1 Roles and access rights for CCSL and CCSM

CCSL has been developed by ENISA in collaboration with the C-SIG working group on certification. The fields of CCSL have been reviewed by the C-SIG certification working group at the end of 2013 and they can be found in ENISA's short paper about certification in the cloud strategy. There are three different types of users:

- The public (typically SME or government customers and also providers of cloud services),
- Authorized users (members of C-SIG working group on certification), and
- Administrators (ENISA staff).

The public can:

- View the details about different existing certification schemes.
- View the mapping from existing certification schemes to CCSM
- Comment and give feedback about CCSL or CCSM.

Authorized users can also:

- View the working copies of schemes and the copies which are pending approval.
- See the changes between working copies and approved copies of certification schemes.
- Create and edit working copies.
- Map the security objectives in a scheme to the CCSM security objectives
- Submit working copies for approval.

Administrators can in addition:

- Approve working copies which are pending approval.
- Add, edit and delete CCSM security objectives.

2.2 User manual and documentation on CCSL and CCSM

For authorized users there is a manual at: https://resilience.enisa.europa.eu/cloud-computing-certification/ENISACertificationToolManualv3.0.pdf

Authorized users can propose changes via the tracker at https://resilience.enisa.europa.eu/cloud-computing-certification/c-sig-certification-issue-tracker ENISA will also keep track of changes and updates in the tracker.

Please address any issues, bugs, questions to cloud.security@enisa.europa.eu

3 Maintenance and update processes

3.1 Guiding principles

The C-SIG working group on certification derived a set of guiding principles for the listing of certification schemes. Quoting from the output of the C-SIG working group on certification:

"Certification schemes for cloud providers should:

1. *be **customer-centric**, i.e. address real user concerns especially liability and risk in the cloud.*
2. *be **industry-driven and voluntary**, i.e. no mandatory schemes should be imposed.*
3. *have a governance structure with a **separation of duties,** i.e. standard setting, accreditation and execution organizations is carried out by separate organizations**.***
4. *provide for the possibility of **self-attestation.***
5. *be **technology neutral** – i.e. it should be appropriate for all vendors, products, technologies, and business models (closed source, open source, et cetera).*
6. *be **lean and affordable**, i.e. it should be appropriate also for small cloud providers (SMEs).*
7. *be based as much as possible on **global standards** to avoid duplications and ensure **global** compatibility of cloud services."*

3.2 Criteria new schemes

New schemes may be proposed by customers, providers or members of the C-SIG working group on certification. The person is called '**sponsor**'. When this happens ENISA opens a new issue in the issue tracker, stores the request from the sponsor, collects the relevant documentation about the scheme, and checks two criteria:

- **Practical relevance?** ENISA assesses if the new scheme is practically relevant for cloud computing customers. How is this assessed? ENISA checks that ***at least one cloud computing service / cloud service provider*** has been certified (or, in the case of self-assessment, has performed and published a self-assessment).
- **Alignment with C-SIG working group on certification principles?** ENISA assesses if and how the new scheme follows the 7 principles derived by the C-SIG working group on certification (see above). How is this assessed? An ENISA expert reads the documentation about the certification scheme and determines that the scheme is sufficiently ***aligned with the 7 principles***.

If the scheme is of practical relevance and is sufficiently aligned with the 7 principles, then ENISA opens a new issue in the issue tracker and sends an email to the members of C-SIG working group on certification. The email explains that a new cloud computing scheme has been proposed, and why ENISA believes the criteria are met. ENISA will provide the sponsor with submission form (template in Annex A).

In the email ENISA provides a link to the relevant issue in the issue tracker, allowing members of C-SIG working group on certification **two weeks** to discuss and evaluate, using the issue tracker. ENISA will provide an assessment report filled in with the details to be evaluated (template Annex B).

After two weeks ENISA will respond by email to the sponsor and the members of C–SIG working group on certification, capturing the consensus of the group about the proposed scheme.

After that ENISA will start work with the sponsor to include the scheme (see below 'Adding a new scheme').

If the scheme is not relevant or not sufficiently aligned with the principles, then ENISA sends an email to the members of C-SIG working group on certification, subject 'Rejected proposal new CCSL scheme'. The email explains why the scheme is not relevant or not sufficiently aligned with the 7 principles then ENISA will send an email to the members of the C-SIG working group on certification, explaining why it believes the criteria are not met. Members of C-SIG working group on certification have 2 weeks to provide comments. After two weeks ENISA informs the sponsor and closes the issue.

3.3 Adding a new scheme

ENISA depends on industry experts to propose new schemes and collect the necessary information and mapping in CCSL and CCSM. Below we refer to them as scheme *sponsors*.

ENISA will provide a sponsor with accounts to add a new scheme to CCSL and to fill in the required information. Each scheme in CCSL has one or more sponsors.

Sponsors agree to work with ENISA to fill in all the required fields, that includes all fields in parts 1 to 5 of CCSL as well as the mapping from the objectives in CCSL part 5 to the objectives in CCSM.

ENISA validates the correctness and completeness of the information according to 6 quality principles to check the information provided:

- **Brief:** Short text is easier to read and understand. We also want to avoid duplicating existing websites and literature.
- **Completeness:** The information should be complete and not leave important aspects unaddressed.
- **Relevance and on-topic:** The information should be relevant and on-topic.
- **Factual: The information should be** factual to maintain objectivity of the information in CCSL. Marketing text is avoided.
- **Accurate:** Information should be accurate/correct.
  To the present: Information should cover only what is valid present moment. Promises, projections or announcements about future publications or ideas are avoided.

If a sponsor is a third party, and not the owner of a scheme, then ENISA will ensure that the information provided by the sponsor is cross-checked with the owner or governing organization of the scheme.

If all the information is provided the scheme will be approved and ENISA will close the issue.

3.4 Changing or deleting schemes

ENISA and members of C-SIG working group on certification can make small changes and corrections to all listed schemes, using the webapplication. All changes are logged and visible to all member of the C-SIG working group on certification.

ENISA and members of C-SIG working group on certification may propose deletion of a scheme.

In case of major changes or deletion ENISA may inform the members of C-SIG working group on certification by email and document it in the issue tracker.

3.5 Changing the structure of CCSL or CCSM

ENISA and members of C-SIG working group on certification can propose changes to the structure of CCSL and the security objectives in CCSM.

ENISA will make these changes only when there is consensus amongst members of the C-SIG working group on certification.

In case of changes to the structure of CCSL or CCSM, ENISA will notify the members of the C- SIG working group on certification, and give scheme sponsors sufficient time to update.

Annex A: Cloud Certification Scheme List: Submission Report (template)

Certification Scheme name:

Governing Organisation name:

Website:

Please explain below how your certification scheme meets the C-SIG principles

Principles	Evidence of compliance
Scheme is customer-centric. *i.e. addresses real user concerns especially liability and risk in the cloud*	
Scheme is industry-driven and voluntary. *i.e. no mandatory schemes should be imposed*	
Scheme has a governance structure with a separation of duties. *i.e. standard setting, accreditation and execution organizations is carried out by separate organizations*	
Scheme provides the possibility of self-attestation.	
Scheme is technology neutral. *i.e. it should be appropriate for all vendors, products, technologies, and business models (closed source, open source, et cetera)*	
Scheme is lean and affordable. *i.e. it should be appropriate also for small cloud providers (SMEs)*	
Scheme is based on global standards to avoid duplications and ensure global compatibility of cloud services.	

Current adoption of the certification framework (please provide information on the status and number of providers certified):

Annex B: Cloud Certification Scheme List: Assessment Report

Certification Scheme name:

Governing Organisation name:

Website:

Objectives	Proof	Comments
Scheme is customer-centric. *i.e. addresses real user concerns especially liability and risk in the cloud*		
Scheme is industry-driven and voluntary. *i.e. no mandatory schemes should be imposed*		
Scheme has a governance structure with a separation of duties. *i.e. standard setting, accreditation and execution organizations is carried out by separate organizations*		
Scheme provides the possibility of self-attestation.		
Scheme is technology neutral. *i.e. it should be appropriate for all vendors, products, technologies, and business models (closed source, open source, et cetera)*		
Scheme is lean and affordable. *i.e. it should be appropriate also for small cloud providers (SMEs)*		
Scheme is based on global standards to avoid duplications and ensure global compatibility of cloud services.		

Summary result: