Supporting the deployment of the EU Cybersecurity Certification Framework

A validation workshop has been delivered by the European Union Agency for Cybersecurity to debate with stakeholders on activities in support of the deployment of the EU cybersecurity certification framework.

Published on December 10, 2019



Dr. Andreas Mitrakas, ENISA

Tagged with

* [Cybersecurity](https://www.enisa.europa.eu/search?Subject%3Alist=Cybersecurity)
* [ENISA](https://www.enisa.europa.eu/search?Subject%3Alist=ENISA)
* [Certification](https://www.enisa.europa.eu/search?Subject%3Alist=Certification)

Pursuant to the EU Cybersecurity Act that entered into force on 27th June 2019, ENISA supports and promotes the development and implementation of Union policy on cybersecurity certification of ICT products, services and processes.

This validation workshop on “**Supporting the deployment of the EU Cybersecurity Certification Framework**” aimed to present the efforts that ENISA has undertaken since the entry into force of the Act and throughout 2019. Presentations included analysis and recommendations as well as input on the response to Commission requests notably on a Common Criteria scheme.

The debate on the various deliverables called for engaging discussions with an expert audience on such areas as, handling of vulnerabilities; maintenance of a scheme in Common Criteria; content of a cybersecurity certification scheme; aspects of deployment of a scheme and market buy-in; aspects related to standardisation and the need to align planning certification schemes with the evolution of standards.

Responding to Commission requests, ENISA is currently carrying out work on two different cybersecurity certification schemes, related to Common Criteria and Cloud services.

The objective of this workshop in terms of validating deliverables with stakeholders was met and it demonstrated in practical terms the engagement of the Agency in terms of accountability and stakeholders’ involvement in the production of its output. This is an area to be monitored further.