



Council of the
European Union

Brussels, 19 December 2018
(OR. en)

Interinstitutional File:
2017/0225(COD)

15545/18
ADD 1

LIMITE

CYBER 325
TELECOM 479
COPEN 447
CODEC 2338
COPS 484
COSI 322
CSC 378
CSCI 176
IND 406
JAI 1298
JAIEX 171
POLMIL 230
RELEX 1094

NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee (Part 1)
Subject:	Proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") - Analysis of the final compromise text with a view to agreement

Delegations will find attached an Annex to the Cyber Security Act.

REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES

Conformity assessment bodies that wish to be accredited shall meet the following requirements:

1. A conformity assessment body shall be established under national law and have legal personality.
2. A conformity assessment body shall be a third-party body independent of the organisation or the ICT products or services it assesses.
3. A body belonging to a business association or professional federation representing undertakings involved in the design, manufacturing, provision, assembly, use or maintenance of ICT products or services which it assesses, may, on condition that its independence and the absence of any conflict of interest are demonstrated, be considered a conformity assessment body.
4. A conformity assessment body, its top-level management and the personnel responsible for carrying out the conformity assessment tasks shall neither be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product or service which is assessed, nor shall it be the authorised representative of any of those parties. This shall not preclude the use of assessed products that are necessary for the operations of the conformity assessment body or the use of such products for personal purposes.
5. A conformity assessment body, its top-level management and the personnel responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, manufacture or construction, the marketing, installation, use or maintenance of those ICT products or services, or represent the parties engaged in those activities. They shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall apply, in particular, to consultancy services.

5a. If a conformity assessment body is owned or operated by a public entity or institution, independence and absence of any conflict of interest shall be ensured and documented between, on the one hand, the certification supervisory authority and, on the other hand, the conformity assessment body.

6. Conformity assessment bodies shall ensure that the activities of their subsidiaries or subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.

7. Conformity assessment bodies and their personnel shall carry out the conformity assessment activities with the highest degree of professional integrity and the requisite technical competence in the specific field and shall be free from all pressures and inducements, including of a financial nature, which might influence their judgement or the results of their conformity assessment activities, especially as regards persons or groups of persons with an interest in the results of those activities.

8. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility. Any subcontracting or consultation of external personnel shall be properly documented, shall not involve any intermediaries and shall be subject to a written agreement covering, among other things, confidentiality and conflicts of interest. The conformity assessment body in question shall take full responsibility for the tasks performed.

9. At all times and for each conformity assessment procedure and each kind, category or sub-category of ICT products or services, a conformity assessment body shall have at its disposal the necessary:

(a) personnel with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;

(b) descriptions of procedures in accordance with which conformity assessment is carried out, ensuring the transparency of those procedures and the possibility of reproducing them. It shall have in place appropriate policies and procedures that distinguish between tasks that it carries out as a notified body and other activities;

(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the ICT product or service technology in question and the mass or serial nature of the production process.

10. A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner, and shall have access to all necessary equipment and facilities.

11. The personnel responsible for carrying out conformity assessment activities shall have the following:

(a) sound technical and vocational training covering all the conformity assessment activities;

(b) satisfactory knowledge of the requirements of the assessments they carry out and adequate authority to carry out those assessments;

(c) appropriate knowledge and understanding of the applicable requirements and testing standards;

(d) the ability to draw up certificates, records and reports demonstrating that assessments have been carried out.

12. The impartiality of the conformity assessment bodies, of their top-level management and of the assessment personnel and subcontractors shall be guaranteed.

13. The remuneration of the top-level management and of the assessment personnel of a conformity assessment body shall not depend on the number of assessments carried out or on the results of those assessments.

14. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the State in accordance with national law, or the Member State itself is directly responsible for the conformity assessment.

15. The conformity assessment body and its personnel, committees, subsidiaries, subcontractors, and any associated body or personnel of external bodies of a conformity assessment body shall maintain confidentiality and observe professional secrecy with regard to all information obtained in carrying out their tasks under this Regulation or pursuant to any provision of national law giving effect to it, except where disclosure is required by Union or Member State law to which such persons are subject except in relation to the competent authorities of the Member States in which its activities are carried out. Proprietary rights shall be protected. The conformity assessment body shall have documented procedures in place in respect of the requirements of this Section 15.

15a. With the exception of Section 15, the requirements of this Annex in no way preclude exchanges of technical information and regulatory guidance between a conformity assessment body and a person applying, or considering whether to apply, for certification.

15b. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, taking into account the interests of small and medium-sized enterprises as defined in Recommendation 2003/361/EC in relation to fees.

16. Conformity assessment bodies shall meet the requirements of the relevant standard that is harmonised under Regulation (EC) 765/2008 for the accreditation of conformity assessment bodies performing certification of processes, products or services.

17. Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of the relevant standard that is harmonised under Regulation (EC) 765/2008 for the accreditation of laboratories performing testing.