



Council of the European Union  
General Secretariat

---

---

**Interinstitutional files:  
2017/0225 (COD)**

---

---

**Brussels, 04 May 2018**

**WK 5413/2018 INIT**

**LIMITE**

**CYBER  
TELECOM  
CODEC  
COPEN  
COPS  
COSI  
CSC  
CSCI  
IND  
JAI  
JAIEX  
POLMIL  
RELEX**

### WORKING PAPER

*This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.*

### **WORKING DOCUMENT**

From:	Netherlands delegation
To:	Horizontal Working Party on Cyber issues
Subject:	Proposal for a 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") - Comments from the Netherlands delegation on recitals 55c, 56b, 56d, 58b and 59, Article 2 and Titles III and IV

Delegations will find in Annex the comments of the Netherlands delegation on recitals 55c, 56b, 56d, 58b and 59, Article 2 and Titles III and IV of the above mentioned proposal.

---

WK 5413/2018 INIT

**LIMITE**

**EN**

## ANNEX

**(55c) The choice, by the users of certificates, of the appropriate level of certification and associated security requirements shall be based on a risk analysis on the use of the product, the service or the process. The level of assurance should be commensurate with the level of the risk.**

*Explanation: this new recital explains that the choice for a certain assurance level is based on a risk analysis.*

**(56b) A European cybersecurity certification scheme may specify several evaluations levels depending on the ~~strength~~rigour of the evaluation methodology used which should correspond to one of the assurance levels and should be associated with an appropriate combination of assurance components. For assurance level basic, the evaluation should be guided at least by the following assurance components: the evaluation should at least include a review of the technical documentations of the ICT product or service by the conformity assessment body. Where the certification includes ICT processes, subject to the technical review should also be the process used to design, develop and maintain an ICT product or service. In cases where a European cybersecurity certification scheme provides for a conformity self-assessment, it should be sufficient if the manufacturer or provider has carried out a self-assessment on the compliance of the ICT process, products or services with the certification scheme. For assurance level substantial, the evaluation should in addition to assurance level basic be guided at least by the verification of the conformity of security functionalities of the ICT product or service to its technical documentation. For assurance level high the evaluation should in addition to assurance level substantial be guided at least by an efficiency testing which assesses the resistance of the security functionalities of ICT product or service against those who perform elaborate cyber attacks having significant ~~to unlimited~~ skills and resources.**

*Explanation: Strength is replaced by rigour and unlimited is deleted and skills is added because this is better wording.*

(56d) ENISA should maintain a website providing information on, and publicity of, European cybersecurity certification schemes which should include, amongst others, the requests for the preparation of a candidate European cybersecurity certification scheme as well as the feedback received in the consultation process carried out by ENISA in the preparation phase. Such website should also provide information about certificates and EU ~~declarations of conformity~~ **statements of self assessment** issued under this Regulation.

*Explanation: the name 'declaration of conformity' is already used in the field of full harmonised legislation for the marketing of products. Therefore a different term should be used in this framework. This should be amended in the whole text.*

**(58b) In the process of certification the evaluation is usually done by laboratories which may be a separate entity from the body issuing the certificate at the end of the process. If the issuing of certificates is only allowed by a public body, the national cybersecurity certification authority or a body under its direct responsibility, the evaluation can still be done by private laboratories.**

*Explanation: this new recital clarifies that even if the certificate is issued by a public body the evaluation itself may be done by a private evaluation lab.*

- (59) It is necessary to require all Member States to designate one cybersecurity certification ~~supervisory~~ authority to supervise compliance with obligations arising from this Regulation. The authority should in particular monitor and enforce the obligations of the manufacturer or provider of ICT products and services established in their respective territories relating to the EU ~~declarations of conformity~~ statements of self assessment, assist the national accreditation bodies in the monitoring and supervision of activities of conformity assessment bodies by providing them with expertise and relevant information, authorise conformity assessment bodies to carry out its tasks when they meet additional requirements set out in a scheme and monitor relevant developments in the field of cybersecurity certification ~~of conformity assessment bodies and of certificates issued by conformity assessment bodies established in their territory with the requirements of this Regulation and of the relevant cybersecurity certification schemes~~. National cybersecurity certification ~~supervisory~~ authorities should handle complaints lodged by natural or legal persons in relation to certificates issued by them ~~conformity assessment bodies established in their territories~~, investigate to the extent appropriate the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable time period. Moreover, they should cooperate with other national cybersecurity certification ~~supervisory~~ authorities or other public authority, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific cybersecurity schemes.

*Explanation: the addition in this recital is to clarify how the NCCA should assist the national accreditation body.*

## Article 2

### Definitions

**(16b) “assurance level” means a ground for confidence that an ICT process, product or service meets the security requirements of a specific European cybersecurity certification scheme and states at what level it has been evaluated; the assurance level does not measure the security of an ICT process, product or service themselves.**

*Explanation: we support the definition of assurance level as presented during the HWG of 26/27 April.*

## Article 43

### European cybersecurity certification framework schemes

- 1. The European cybersecurity certification framework is established in order to increase the level of security within the digital European Union. It sets governance that enables a harmonised approach at EU level of European cybersecurity certification schemes, in view of creating a digital single market for ICT processes, products and services.**
- 2. The European cybersecurity certification framework defines a mechanism to establish a European cybersecurity certification scheme shall and to attest that the ICT processes, products and services that have been certified-evaluated in accordance with such scheme comply with specified security requirements as regards their ability to resist at a given level of assurance, actions that aim to compromise with the aim to protect the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, processes, and services and systems throughout their life cycle.**

*Explanation: schemes should be in plural in para 1.*

Article 44

*Preparation and adoption of a European cybersecurity certification scheme*

1. Following a request from the Commission or the Group, ENISA shall prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation.

1a. Following a request from **The preparation of a candidate European cybersecurity certification scheme may be proposed** n, ENISA shall prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this **to the European Cybersecurity Certification Group (the 'Group') established under Article 53 by Member States or interested stakeholder organisations an industry representative body** the European Cybersecurity Certification Group (the 'Group') established under Article 53 may propose the preparation of a candidate European cybersecurity certification scheme to the Commission **The Group** shall assess ~~e~~ such proposals ~~referred to in paragraph 1 of this Article~~ against criteria defined by the Group by means of guidelines in accordance with Article 53(3)(ca) and may request ENISA to prepare a candidate European cybersecurity certification scheme.

2. When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult all relevant stakeholders **by transparent consultation processes** and closely cooperate with the Group. The Group shall provide ENISA with the assistance and expert advice ~~required by ENISA~~ in relation to the preparation of the candidate scheme **and adopt an opinion on the candidate scheme before its submission to the Commission; including by providing opinions** where necessary. ENISA shall ensure that the candidate schemes **are consistent with** ~~meets the requirements of~~ the applicable harmonised standard used for accreditation of the conformity assessment body.
3. ENISA shall **take utmost account of the opinion of the Group before transmitting** ~~transmit~~ the candidate European cybersecurity certification scheme prepared in accordance with paragraph 2 of this Article to the Commission ~~along with the remarks or reservations made by the Group members~~.

4. The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in accordance with Article 55(2), providing for European cybersecurity certification schemes for ICT **processes**, products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation.

*Explanation: we support the revised version of article 44 as proposed during the HWG of 26/27 april.*

#### *Article 44a*

##### *Maintenance of a European cybersecurity certification scheme*

1. The Agency shall maintain a dedicated website providing information on, and publicity of, European cybersecurity certification schemes, certificates and EU **declarations of conformity statements of self assessment** issued pursuant to Article 47b.
2. The Agency, in close cooperation with the Group, shall at least every 5 years review the adopted European cybersecurity certification schemes taking into account feedback received from interested parties. If considered necessary **by the commission or the Group**, the Agency may start the process of developing a revised candidate scheme **in accordance with Article 44(2) and (3)**.
- ~~3. The Agency, in close cooperation with the Group, shall have governance mechanism for updates, amendments and coordination for any particular certification scheme.~~

*Explanation: the name 'declaration of conformity' is already used in the field of full harmonised legislation for the marketing of products. Therefore a different term should be used in this framework. This should be amended in the whole text.*

*In para 2 it should be clarified that either the Commission or the group may decide that review of a scheme is necessary.*

**Commented [A1]:** A recital to clarify what exactly will need to be published is useful. Is the idea that all individual certificates and declarations will be published on the website?

Article 45

**Security objectives of European cybersecurity certification schemes**

A European cybersecurity certification scheme shall be so designed ~~as to take into account~~ achieve, as applicable, **at least** the following security objectives:

- (a) protect data stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access or disclosure **during the entire process, product or service lifecycle**;
- (b) protect data stored, transmitted or otherwise processed against accidental or unauthorised destruction, ~~accidental~~ loss or alteration **or lack of availability during the entire process, product or service lifecycle**;
- (c) ~~ensure that~~ authorised persons, programmes or machines can access exclusively the data, services or functions to which their access rights refer;
- (d) record which data, functions or services have been ~~communicated~~ **accessed, used or otherwise processed**, at what times and by whom;
- (e) ~~ensure that~~ it is possible to check which data, services or functions have been accessed, ~~or~~ used **or otherwise processed**, at what times and by whom;
- (f) restore the availability and access to data, services and functions in a timely manner in the event of physical or technical incident;
- (g) ~~ensure that~~ ICT processes, products and services are provided with up to date software **and hardware** that **does do** not contain ~~known publically~~ **available known** vulnerabilities, and are provided mechanisms for secure ~~software~~ updates;
- (ga) ~~that~~ ICT processes, **products** and services are developed and operated **and products are manufactured** according to the security requirements stated in the particular scheme.

*Explanation: In (g) 'available' should be replaced by 'known'. The use of the word 'operated' does not work well in combination with product assessment as it suggests to address how a user operates a product. Suggested wording for products is 'manufactured'.*



Article 46

*Assurance levels of European cybersecurity certification schemes*

1. A European cybersecurity certification scheme may specify one or more of the following assurance levels: basic, substantial and/or high, for ICT **processes**, products and services issued under that scheme.
2. The assurance levels basic, substantial and high shall ~~meet the following criteria~~ respectively: **refer to a certificate or the assurance level basic shall refer to an EU declaration of conformity statement of self assessment** issued in the context of a European cybersecurity certification scheme, which provides a corresponding degree of confidence (basic, substantial and/or high) in the claimed ~~or asserted~~ cybersecurity qualities of an ICT process, product or service, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of, or to prevent cybersecurity incidents **as follows:**
  - (a) **a European cybersecurity certificate or EU declaration of conformity statement of self assessment that refers to** assurance level “basic” **provides a basic shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a limited** degree of confidence in the claimed ~~or asserted~~ cybersecurity qualities of an ICT **process, product or service, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of cybersecurity and in particular a confidence that the known basic risks for cyber incidents can be prevented;**
  - (b) **a European cybersecurity certificate that refers to** assurance level “substantial” **shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which** provides a substantial degree of confidence in the claimed ~~or asserted~~ cybersecurity qualities of an ICT **process, product or service, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of cybersecurity and in particular a confidence that the known risks of cyber incidents can be prevented and there is also ability to resist cyber attacks carried out by actors with limited resources;**

- (c) a European cybersecurity certificate that refers to assurance level “high” shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a **higher-high** degree of confidence in the claimed ~~or asserted~~ cybersecurity qualities of an ICT process, product or service ~~than certificates with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent cybersecurity and in particular a confidence that cyber incidents can be prevented but there is also ability to resist state-of-the-art cyber attacks carried out by actors with significant or unlimited skills and resources.~~

- 2a. A European cybersecurity certification scheme may specify ~~additional~~ several evaluation levels depending on the **strength/rigour** of the evaluation methodology. Each one of the evaluation levels shall correspond to one of the assurance levels and be defined by an appropriate combination of assurance components.

**a) For assurance level “basic,” the evaluation should be guided at least by the following assurance components:**

**- the technical review by a conformity assessment body of the technical documentation of the ICT product or service, or**

**- a self-assessment by the provider, developer or manufacturer of the ICT product or service demonstrating compliance with the requirements of the scheme.**

**b) For assurance level “substantial,” the evaluation should in addition to assurance level basic be guided at least by the verification of the conformity of security functionalities of the product or service to its technical documentation;**

**c) For assurance level “high,” the evaluation should in addition to assurance level substantial be guided at least by an efficiency testing which assesses the resistance of the security functionalities against those who perform elaborate cyber attacks having significant skills and resources.**

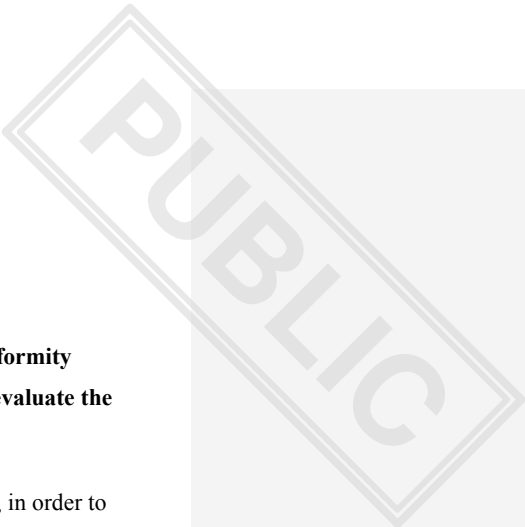
*Explanation: in para 2 it should be clear that the self assessment is only possible for assurance level basic. The addition in 2a is done to make the relation between evaluation methodology and the assurance level clear in the article as well. This is in line with recital 56b. Strength is replaced by rigour and unlimited is deleted and skills is added because this is better wording.*

#### Article 47

##### ***Elements of European cybersecurity certification schemes***

1. A European cybersecurity certification scheme shall include **at least** the following elements:
    - (a) subject-matter and scope of the certification **scheme**, including the type or categories of ICT **processes**, products and services covered **as well as an elaboration of how the certification scheme suits the needs of the expected target groups**;
    - (b) ~~detailed specification of the cybersecurity requirements against which the specific ICT products and services are evaluated, for example by~~ **in the following order of preference**:
      - reference to ~~Union or~~ international, **European, national** standards or ~~where standards are not available~~;
      - **reference to** technical specifications **that meet the requirements of annex II of regulation 1025/2012, or where not available**;
      - **reference to other technical specifications, or where not available**;
      - **other requirements defined in the scheme**
- that are to be** followed in the evaluation;

*Explanation: there should be certain flexibility and as well a hierarchy in the selection of documents which are referenced in the scheme and as a last resort it should as well be possible to define requirements in the scheme itself.*

- 
- (c) where applicable, one or more assurance levels;
- (ca) **where applicable, specific or additional requirements applicable to conformity assessment bodies in order to guarantee their technical competence to evaluate the cybersecurity requirements;**
- (d) specific evaluation criteria and methods used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 45, and that specific cybersecurity requirements referred to in point (b) are achieved;
- (e) **where applicable**, information to be supplied **or otherwise be made available** to the conformity assessment bodies by an applicant which is necessary for certification;
- (f) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;
- (g) ~~where surveillance is part of the scheme, the~~ rules for monitoring compliance with the requirements of the certificates **or the EU declaration of conformity**, including mechanisms to demonstrate the continued compliance with the specified cybersecurity requirements;
- (h) **where applicable**, conditions for granting and renewing a certificate, as well as maintaining, continuing, ~~renewing,~~ extending and reducing the scope of certification;
- (i) rules concerning the consequences of non-conformity of certified **or self-assessed** ICT products and services with the ~~certification~~ requirements **of the scheme**;
- (j) rules concerning how previously undetected cybersecurity vulnerabilities in ICT **processes**, products and services are to be reported and dealt with;
- (k) **where applicable**, rules concerning the retention of records by conformity assessment bodies;
- (l) identification of national **or international** cybersecurity certification schemes covering the same type or categories of ICT **processes**, products and services, **security requirements and evaluation criteria and methods**;

- (m) the content of the issued certificate **or the EU declaration of conformity**;
  - (ma) maximum period of validity of certificates, if applicable;
  - (mb) disclosure policy for granted, amended and withdrawn certificates;
  - (mc) conditions for the mutual recognition of certification schemes with third countries;
  - (md) where applicable, rules concerning a peer review mechanism for the bodies issuing European cybersecurity certificates for high assurance levels pursuant to Article 48(4a) and (4b).**
2. The specified requirements of the scheme shall not contradict any applicable legal requirements, in particular requirements emanating from harmonised Union legislation.
  3. Where a specific Union act so provides, certification **or the EU declaration of conformity** under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that act.
  4. In the absence of harmonised Union legislation, Member State law may also provide that a European cybersecurity certification scheme may be used for establishing the presumption of conformity with legal requirements.

#### Article 47a

##### Conformity self-assessment

- 1.** A European cybersecurity certification scheme may allow for carrying out a conformity assessment under the sole responsibility of the manufacturer or provider of ICT products and services. Such conformity assessment shall be applicable only to ICT products and services **of low risk and complexity** corresponding to assurance level basic.

- 1a. If the scheme for the same products and services allows for both certification and conformity self assessment the scheme shall provide for clear and understandable means to differentiate between products and services that are assessed under the responsibility of the manufacturer or provider and products and services that are certified.**

Article 47b

EU declaration of conformity

21. The manufacturer, importer or provider of ICT products and services may issue an EU declaration of conformity attestation of self assessment stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By drawing up such a declaration attestation, the manufacturer or provider of ICT products and services shall assume responsibility for the compliance of the ICT product or service with the requirements set out in the scheme.
32. The manufacturer, importer or provider of ICT products and services shall keep the EU declaration of conformity attestation of self assessment and technical documentation of all relevant information relating to the conformity of the ICT products or services with a scheme at the disposal of the national cybersecurity certification supervisory authority referred to in Article 50(1) for 10 years. A copy of the EU declaration of conformity attestation of self assessment shall be submitted to the national cybersecurity certification supervisory authority and to ENISA.
43. The issuing of EU declaration of conformity attestation of self assessment is voluntary unless otherwise specified pursuant article 48a, or otherwise in the Union law or in Member States law.
5. The EU declaration of conformity issued pursuant to this Article shall be recognised in all Member States.

*Explanation: the new para 1a makes sure that for the end-user there is a clear distinction between self assessment and certification. The importer is added for the cases where the manufacturer is based outside the EU. In para 3 the submission of the attestation to the NCCA is deleted because it is not clear to which NCCA it should be submitted. The submission to ENISA should be enough if ENISA makes sure that the attestations can be seen by the NCCAs. In para 4 is a reference to a new article 48b inserted to create a legal base for obligatory self assessment.*

Article 48

**Cybersecurity certification**

1. ICT **processes**, products and services that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 44 shall be presumed to be compliant with the requirements of such scheme.
2. The certification shall be voluntary, unless otherwise specified pursuant article 48a, or otherwise in Union law or in Member States law.
3. A European cybersecurity certificate pursuant to this Article referring to assurance level basic or substantial shall be issued by the conformity assessment bodies referred to in Article 51 on the basis of criteria included in the European cybersecurity certification scheme, adopted pursuant to Article 44.
4. By ~~the~~ way of derogation from paragraph 3, in duly justified cases a particular European cybersecurity **certification** scheme may provide that a European cybersecurity certificate resulting from that scheme can only be issued by a public body. Such public body shall be one of the following:
  - (a) a national cybersecurity certification ~~supervisory~~ authority referred to in Article 50(1);
  - (b) a public body that is accredited as conformity assessment body pursuant to Article 51(1) ~~or~~
  - ~~(c) a body established under laws, statutory instruments, or other official administrative procedures of a Member State concerned and meeting the requirements for bodies certifying products, processes and services further to ISO/IEC 17065:2012.~~
- 4a.** In cases where a European cybersecurity certification scheme pursuant to Article 44 requires an assurance level high, the certificate can only be issued by a national cybersecurity certification ~~supervisory~~ authority referred to in Article 50(1).

- 4b. By the way of derogation from paragraph 4a, in duly justified cases a particular European cybersecurity certification scheme may provide that a European cybersecurity certificate for assurance level high resulting from that scheme may be issued by a conformity assessment body referred to in Article 51:**
- (a) upon prior approval by a national cybersecurity certification authority for each individual certificate issued by a conformity assessment body; or**
- (b) upon prior general delegation of this task to a conformity assessment body by the national cybersecurity certification authority.**
5. The natural or legal person which submits its ICT **processes**, products or services to the certification mechanism shall ~~provide~~ **make available to** the conformity assessment body referred to in Article 51 ~~with~~ all information necessary to conduct the certification procedure.
- 5a. The holder of a certificate shall inform the body issuing the certificate about any later detected flaws or irregularities concerning the security of the certified ICT process, product or service that may affect being subject to the certificate. The body shall forward this information without undue delay to the national cybersecurity certification authority in cases where these flaws or irregularities might lead to suspension or withdrawal of the certificate.**
6. Certificates shall be issued for ~~a maximum period of three years~~ **the period defined by the particular certification scheme** and may be renewed, ~~under the same conditions~~, provided that the relevant requirements continue to be met.
7. A European cybersecurity certificate issued pursuant to this Article shall be recognised in all Member States.

*Explanation: in para 2 reference to a new article 48a is inserted to create a legal base for obligatory certification. In para 5a it should be clear that the CAB only has to actively inform the NCCA in cases where a certificate might be suspended or withdrawn. Otherwise the NCCAs will receive a lot of irrelevant information. It as well will create an unclear situation on the exact information for the CAB to submit to the NCCA because flaws and irregularities is not well defined.*



**Article 48a (new)****Obligatory certification or self-assessment**

1. The Commission may adopt implementing acts, in accordance with Article 55(2), providing for obligatory certification or self-assessment of products, processes or services according to European cybersecurity certification schemes adopted pursuant to article 44.
2. The implementing act shall clearly specify for which products, processes or services the certification or self-assessment will be obligatory. The scope of products, processes or services for which certification or self-assessment will be obligatory may be smaller than the scope of the European cybersecurity certification scheme.
3. In preparing a draft implementing act the Commission shall:
  - a) carry out an assessment, which at least shall consider the benefits in terms of impact on the level of security within the digital European Union, and costs for businesses and users;
  - b) take into account existing national legislation that Member States consider relevant;
  - c) carry out appropriate consultation with stakeholders;
  - d) set implementing date(s), any staged or transitional measure or periods, taking into account, in particular, possible impacts on SMEs or on specific product groups manufactured primarily by SMEs.

*Explanation: the framework should provide for a legal base to make self assessment or certification obligatory for a specific scope. This creates the possibility to adopt implementing acts for certain groups of products where in relation to the developments of the internet of things the risks as biggest. See our separate paper on this issue for more explanation.*

Article 50

**National cybersecurity certification supervisory authorities**

1. Each Member State shall appoint a national **cybersecurity** certification **supervisory** authority.
2. Each Member State shall inform the Commission of the identity of the authority appointed.
3. **Without prejudice to Article 48(4)(a) and (e),** Each national **cybersecurity** certification **supervisory** authority shall, in its organisation, funding decisions, legal structure and decision-making, be independent of the entities they supervise.
- 3a. Member States shall ensure that the activities of the national cybersecurity certification authority related to the issuance of certificates in accordance with article 48(4)(a) adhere to a strict separation of roles and responsibilities with the supervisory activities in this article and that both activities function independently from each other.**
4. Member States shall ensure that national **cybersecurity** certification **supervisory** authorities have adequate resources to exercise their powers and to carry out, in an effective and efficient manner, the tasks assigned to them.
5. For the effective implementation of the regulation, it is appropriate that these authorities participate in the European Cybersecurity Certification Group established pursuant to Article 53 in an active, effective, efficient and secure manner.
6. National **cybersecurity** certification **supervisory** authorities shall:
  - ~~(a) **monitor and enforce the application of the provisions under this Title at national level and supervise compliance of the certificates that have been issued by conformity assessment bodies established in their respective territories with the requirements set out in this Title and in the corresponding European cybersecurity certification scheme;**~~
  - (a) On a risk based approach perform appropriate checks on certified products, services and processes to verify if processes, products and services which are claimed to be certified according a European cybersecurity certification scheme indeed are certified.**

(a1) Perform system supervision by sample based checks to verify if products, services and processes that are certified indeed meet the requirements of the relevant European cybersecurity scheme.

Explanation: with the deletion of paragraph (a) there are no tasks anymore for the NCCA related to the supervision of certified products, services and processes. Likewise the new paragraph (aa) the NCCA should perform some kind of supervision in the field of certification. The NCCA should on a risk based approach check if products, services and processes that claim to be certified indeed are certified. This cannot be done by CABs. And if there is no supervision there is a risk that vendors might just claim a fake certificate without having a certificate in reality. The NCCA should as well on a sample based manner sometimes check if products, services and processes indeed meet requirements of the certificate. This is important to gather relevant information about the functioning of the certification as a whole.

- (aa) monitor and enforce the obligations of the manufacturer or provider of ICT products and services set out in Article 47a(2) and (3) established in their respective territories~~b~~;
- (b) ~~monitor and supervise, in close cooperation with~~ assist the national accreditation bodies in the monitoring and supervision of, ~~the~~ activities of conformity assessment bodies for the purpose of this Regulation, ~~including in relation to the notification of conformity assessment bodies and the related tasks set out in Article 52 of this Regulation. These monitoring and supervisory activities shall not overlap with the activities performed by the national accreditation bodies~~;
- (ba) monitor and supervise the activities of the ~~public body~~ bodies referred to in Article 48(4)~~(c)~~;
- (bb) authorise conformity assessment bodies referred to in Article 51(1~~ba~~) and restrict, suspend or withdraw existing authorisation in cases of non-compliance with the requirements of this Regulation;

- (c) handle complaints lodged by natural or legal persons in relation to certificates issued by ~~conformity assessment bodies or public bodies referred to the national cybersecurity~~ **certification authority in accordance with Article 48(4)(a) and 48(4a) established in their territories**, investigate, to the extent appropriate, the subject matter of the complaint, and inform the complainant of the progress and the outcome of the investigation within a reasonable time period;
- (d) cooperate with other national **cybersecurity** certification ~~supervisory~~ authorities or other public authorities, including by sharing information on possible non-compliance of ICT **processes**, products and services with the requirements of this Regulation or specific European cybersecurity certification schemes;
- (e) monitor relevant developments in the field of cybersecurity certification.
7. Each national **cybersecurity** certification ~~supervisory~~ authority shall have at least the following powers:
- (a) to request conformity assessment bodies, ~~and~~ European cybersecurity certificate holders **and issuers of EU declaration of conformity** to provide any information it requires for the performance of its task;
- (b) to carry out investigations, in the form of audits, of conformity assessment bodies, ~~and~~ European cybersecurity certificates' holders **and issuers of EU declaration of conformity**, for the purpose of verifying compliance with the provisions under Title III;
- (c) to take appropriate measures, in accordance with national law, in order to ensure that conformity assessment bodies, ~~or~~ certificate holders **and issuers of EU declaration of conformity** comply with this Regulation or with a European cybersecurity certification scheme;
- (d) to obtain access to any premises of conformity assessment bodies and European cybersecurity certificates' holders for the purpose of carrying out investigations in accordance with Union or Member State procedural law;

**Commented [A2]:** This change leads to 2 questions:  
-What's the exact difference between this provision and article 53a (1)?  
-What's the reason to not provide for the possibility to lodge complaints against certificates issued by CAB's or public bodies?

- (e) to withdraw, in accordance with national law, certificates **issued by the national cybersecurity certification authority in accordance with Article 48(4)(a)** that are not compliant with this Regulation or a European cybersecurity certification scheme;
  - (f) to impose penalties, as provided for in Article 54, in accordance with national law, and to require the immediate cessation of the breaches of obligations set out in this Regulation.
8. National **cybersecurity** certification ~~supervisory~~ authorities shall cooperate amongst each other and the Commission and, in particular, exchange information, experiences and good practices as regards cybersecurity certification and technical issues concerning cybersecurity of ICT **processes**, products and services.

*Article 51*

***Conformity assessment bodies***

1. The conformity assessment bodies shall be accredited by the national accreditation body named pursuant to Regulation (EC) No 765/2008 only when they meet the requirements set out in the Annex to this Regulation. **The requirements shall be defined in accordance with global accreditation standards and shall ensure that the accreditation bodies operate in open, transparent, and fair manner.**

**1a. In cases where a European cybersecurity certificate is issued by a national cybersecurity certification authority pursuant to Article 48(4)(a), the certification body of the national cybersecurity certification authority shall be accredited as conformity assessment body pursuant to paragraph 1 of this Article.**

**1ba.** ~~Where applicable,~~ the conformity assessment bodies shall be authorised by the national **cybersecurity** certification ~~supervisory~~ authority to carry out its tasks when they meet **the requirements set out in the Annex to this Regulation and if applicable** specific or additional requirements set out in the European certification scheme pursuant to Article 47(1)(ca).

2. Accreditation shall be issued for a maximum of five years and may be renewed on the same conditions provided that the conformity assessment body meets the requirements set out in this Article. Accreditation bodies shall **take all appropriate measures within a reasonable timeframe to restrict, suspend or** revoke an accreditation of a conformity assessment body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a conformity assessment body infringe this Regulation.

*Explanation: in para 1 the last sentence is superfluous because the requirements in the annex will be part of the regulation anyway. 1b is amended because there should be no difference in CAB that meet additional requirements and other CABs. For the sake of clarity all CABs should be authorised. It is a 3 step process: 1. Accreditation, 2. Authorisation, 3. Notification.*

#### Article 53

##### **European Cybersecurity Certification Group**

1. The European Cybersecurity Certification Group (the 'Group') shall be established.
2. The Group shall be composed of **representatives from the** national **cybersecurity** certification **supervisory** authorities. **The authorities shall be represented by the heads of** **by other high level representatives of national cybersecurity certification supervisory** **authorities.**
3. The Group shall have the following tasks:
  - (a) to advise and assist the Commission in its work to ensure a consistent implementation and application of the present Title, in particular regarding cybersecurity certification policy issues, coordination of policy approaches, and the preparation of European cybersecurity certification schemes;

- (b) to assist, advise and cooperate with ENISA in relation to the preparation of a candidate scheme in accordance with Article 44 of this Regulation;

**(ba) to adopt an opinion on the candidate scheme pursuant to Article 44 of this Regulation;**

- (c) to ~~propose to the Commission that it requests~~ **request** the Agency to prepare a candidate European cybersecurity certification scheme in accordance with Article 44 of this Regulation;

**(ca) to develop and adopt guidelines on criteria for assessment of proposals for the preparation of a candidate scheme submitted to the Commission or the Group pursuant to Article 44(1a);**

- (d) to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes;
- (e) to examine the relevant developments in the field of cybersecurity certification and exchange good practices on cybersecurity certification schemes;
- (f) to facilitate the cooperation between national **cybersecurity** certification ~~supervisory~~ authorities under this Title through **capacity building**, the exchange of information, in particular by establishing methods for the efficient exchange of information relating to all issues concerning cybersecurity certification;

**(fa) to participate in the organisation and provide support to the implementation of the peer review mechanism between the bodies referred to in Article 48(4a) and (4b) in accordance with the rules established in a European cybersecurity certification scheme pursuant to Article 47(1)(md) of this Regulation.**

4. The Commission shall chair the Group **in the capacity of a moderator** and provide the secretariat to it, with the assistance of ENISA as provided for in Article 8(a).

*Explanation: para 2 should be less specific to let the member state decide who exactly to represent them.*

*Article 58*

***Entry into force***

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

1b. This regulation shall apply from [the twentieth day following that of its publication in the Official Journal of the European Union] with the exception of articles 47 paragraph 2-4, 48, 50, 51, 52, 53a en 53b [and allother articles that need (amendment of) national legislation. The exact articles that need to be excluded shall be decided on when the text is stable] which shall apply from [24 months after the date of publication of this Regulation in the Official Journal of the European Union].

1c. by way of derogation of article 53.2 member states that do not have a national cybersecurity certification supervisory authority yet may let them represent by another entity untill latest the date of application.

2. This Regulation shall be binding in its entirety and directly applicable in all Member States.

*Explanation:* for certain articles national legislation is necessary and the appointment and preparation of the NCCA will take time. Therefore certain articles should apply 24 months after the publication of the regulation. The exact articles for which this is the case shall be decided on later when the text is stable. A derogation needs to be in place to make sure the group can start as soon as possible.



## Annex

16. Conformity assessment bodies shall meet the requirements of the relevant standard ~~EN ISO/IEC 17065:2012~~ that is harmonised under regulation 765/2008 for the accreditation of conformity assessment bodies performing certification of services, processes or products.

17. Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of the relevant standard ~~EN ISO/IEC 17025:2005~~ that is harmonised under regulation 765/2008 for the accreditation of laboratories performing testing.

*Explanation: the ISO 17025 is recently reviewed and a 2018 version is adopted. The standards are regularly reviewed. Therefore a more general reference should be chosen to make sure that references will not become outdated. Here you can see that both standards are harmonised under regulation 765/2008: [https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/new-legislative-framework-and-emas\\_en](https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/new-legislative-framework-and-emas_en)*