Information and technology law course

LECTURE 7 – 16 OCTOBER 2024

FEDERICA CASAROSA – 2024/2025

Not something related to applications at member state level. EU cybersec. act, we have 2 diff. perspectives: the reg. vs 2019 (NIS, 2016/2018 implement.; but there was a realization that ENISA was starting to finish up the mandate). So in the NIS ENISA was portrayed as an helper. We have to keep it! And the another aspect: who sets the standard? Take NIS: trying to create harmonised level at EU states. So we have the possibility to increase the general level at member state. And this for specific OES. What if I have an Estonian manufacturer that wants to get in IT market and is not OES? For supermarkets for example you have a certification of prod. according to specific standards. Why don't we do the same for cybersec standards developed according to the EU procedure? So I can go to all the markets and consumers know that the same product has the same level of sec. So strategy: getting the product to a equal level of control based on standards.

EU cybersecurity act

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ L 151, 7.6.2019.

the Act is a combination of three factors.

- The first is the ambition to achieve a leading role in the global cybersecurity market.
- The second is the necessity to bridge the normative gaps created by the recent cyberattacks, whereby the law-maker realised that the current framework is unable to quickly respond to such threats.
- The third is the political opportunity to react to an emerging debate on the security of our information systems and networks and the geopolitical direction that the Union wants to take.

ENISA

Erwin was born in 2004, with 5 years mandates and in 2019 made permanent.

Strenghtening the role of ENISA

Article 3 Mandate

1. ENISA shall carry out the tasks assigned to it under this Regulation for the purpose of achieving a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. ENISA shall act as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other relevant Union stakeholders. (1)

ENISA shall contribute to reducing the fragmentation of the internal market by carrying out the tasks assigned to it under this Regulation.

2. ENISA shall carry out the tasks assigned to it by Union legal acts that set out measures for approximating Member State laws, regulations and administrative provisions which are related to cybersecurity.

3. When carrying out its tasks, ENISA shall act independently (3) while avoiding the duplication of Member State activities and taking into consideration existing Member State expertise.

4. ENISA shall develop its own resources, including technical and human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation.

Here clarification of what ENISA does.

(1) Nothing about being a legislator. We do not set rules. It only supports member states. Can provide but not enforce! Member states will have the last word. They have a say, whenever there's an issue because they have experts.

(2) There can be collaboration with ENISA.

(3) The fact that I won't have binding power is good because there are not political influences, so it's a double edged sword.

ENISA – objectives

- Empowering Communities
- Cybersecurity Policy
- Operational Cooperation
- Capacity Building
- Trusted Solutions
- Foresight
- Knowledge

Certification schemes

Issue was: we have several products on the market. As a consumer, how do I choose? How do I know that they are secure, for example? We will make it easier for the customer to signal a good security product? A SOYO will never understand, so it is easy to signal with a label! So you have info that the standard is applied correctly and updated.
Problem: for cybersec, if I have a cybersec label it doesn't mean I am safe from risks. So a label only gives a certain level of security but not 0 risks.

Certification systems

Rec 69 Cybersecurity Act

- Therefore, it is necessary to adopt a common approach and to establish a **European cybersecurity certification framework that lays down the main horizontal requirements for European cybersecurity certification schemes to be developed and allows European cybersecurity certificates and EU statements of conformity for ICT products, ICT services or ICT processes to be recognised and used in all Member States**. In doing so, it is essential to build on existing national and international schemes, as well as on mutual recognition systems, in particular SOG-IS, and to make possible a smooth transition from the existing schemes under such systems to schemes under the new European cybersecurity certification framework. The European cybersecurity certification framework should have a twofold purpose. First, it should help increase trust in ICT products, ICT services and ICT processes that have been certified under European cybersecurity certification schemes. Second, it should help avoid the multiplication of conflicting or overlapping national cybersecurity certification schemes and thus reduce costs for undertakings operating in the digital single market. The European cybersecurity certification schemes should be non-discriminatory and based on European or international standards, unless those standards are ineffective or inappropriate to fulfil the Union's legitimate objectives in that regard.

We want national standards but we do not want those standard to mean something different in different states. As a manufactor, I don't want to have limits to sell my product, so if I want to market an Italian product in Iceland that has a different certification scheme it will hurt my sales, I should see if I comply with the Iceland standards etc...
So we have the possibility:

(4) 'operator of essential services' means an operator of essential services as defined in point (4) of Article 4 of Directive (EU) 2016/1148;

(5) 'digital service provider' means a digital service provider as defined in point (6) of Article 4 of Directive (EU) 2016/1148;

(6) 'incident' means an incident as defined in point (7) of Article 4 of Directive (EU) 2016/1148;

(7) 'incident handling' means incident handling as defined in point (8) of Article 4 of Directive (EU) 2016/1148;

(8) 'cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;

(9) 'European cybersecurity certification scheme' means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes; (1)

(10) 'national cybersecurity certification scheme' means a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services and ICT processes falling under the scope of the specific scheme;

(11) 'European cybersecurity certificate' means a document issued by a relevant body, attesting that a given ICT product, ICT service or ICT process has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme;

(12) 'ICT product' means an element or a group of elements of a network or information system;

(13) 'ICT service' means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems;

(14) 'ICT process' means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service;

(15) 'accreditation' means accreditation as defined in point (10) of Article 2 of Regulation (EC) No 765/2008;

(16) 'national accreditation body' means a national accreditation body as defined in point (11) of Article 2 of Regulation (EC) No

16:12
16/10/2024

(1) It's like a list of tasks defined or done to have a prod, service or processes up to the standard.

(2) In the national, there's the national authorities certs too! We accept them existence at the moment. The idea, though, is that we shouldn't need the national one if we have the EU one. They should naturally fade.
At the point where universal cert appears, there will be a period of shift.
The harmonization is more important here, because both would create confusion like understanding the best one etc.

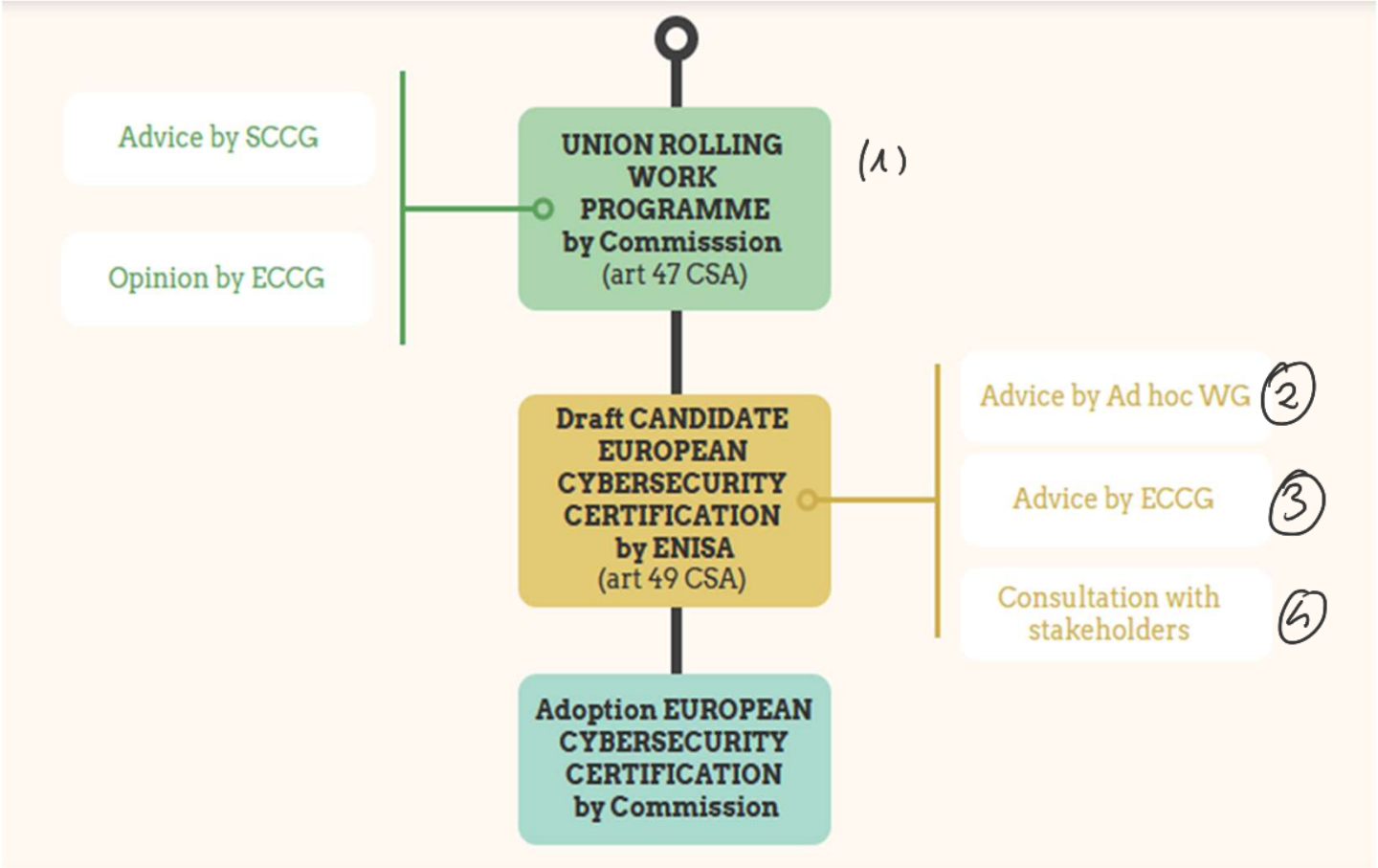
Certification schemes - definition

Art 2

(9) ‘European cybersecurity certification scheme’ means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes;

(10) ‘national cybersecurity certification scheme’ means a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services and ICT processes falling under the scope of the specific scheme;

Certification schemes – procedure



Procedure: the hard work was for ENISA. A procedure that requires an invited knowgen. So ENISA can't choose by themselves. The commission sets the URP.(1) They choose then the important fields on which we need the certificate. ENISA will do the work to draft the document. It is not a closed doors procedure and not just the experts talking. ENISA will create an (2) group, so there there will be for example manufacturers of those kind of tech, representative of MS with similar certs, producers of small parts or of the network on which the system to be standardised is based. So the STAKEHOLDERS.

(3) Euro Cybersec Coop Group that gives advice

(4) And as soon as we have the first draft we have a consultation with them stakeholders. We then have a final revision that can take time: the ball is back to the commission, that will adopt the scheme that'll be available.

Then we have the 2nd part of the life of the cert. scheme.

Certification schemes – procedure

Art 47 The Union rolling work programme for European cybersecurity certification

- 3. Inclusion of specific ICT products, ICT services and ICT processes or categories thereof in the Union rolling work programme shall be justified **on the basis of one or more of the following grounds**:
  - (a) the availability and the development of national cybersecurity certification schemes covering a specific category of ICT products, ICT services or ICT processes and, in particular, as regards the risk of fragmentation;
  - (b) relevant Union or Member State law or policy;
  - (c) market demand;
  - (d) developments in the cyber threat landscape;
  - (e) request for the preparation of a specific candidate scheme by the ECCG.
- 4. The Commission shall take due account of the opinions issued by the ECCG and the Stakeholder Certification Group on the draft Union rolling work programme.

Certification schemes – procedure

Article 51 Security objectives of European cybersecurity certification schemes

A European cybersecurity certification scheme shall be designed to achieve, as applicable, at least the following security objectives:

- (a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;
- (b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;
- (c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;
- (d) to identify and document known dependencies and vulnerabilities;
- (e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
- (f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
- (g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;
- (h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;
- (i) that ICT products, ICT services and ICT processes are secure by default and by design;
- j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

You'll need someone that checks with the compliance.

(2) Basically ensure CIA of data and network is safeguarded. When I publish the cert the idea is that it should increase the level of security.

Certification schemes – governance

Article 58 - National cybersecurity certification authorities

1. **Each Member State shall designate one or more national cybersecurity certification authorities in its territory** or, with the agreement of another Member State, shall designate one or more national cybersecurity certification authorities established in that other Member State to be responsible for the supervisory tasks in the designating Member State. […]

3. Without prejudice to point (a) of Article 56(5) and Article 56(6), each national cybersecurity certification authority shall be **independent of the entities it supervises in its organisation, funding decisions, legal structure and decision-making. […]**

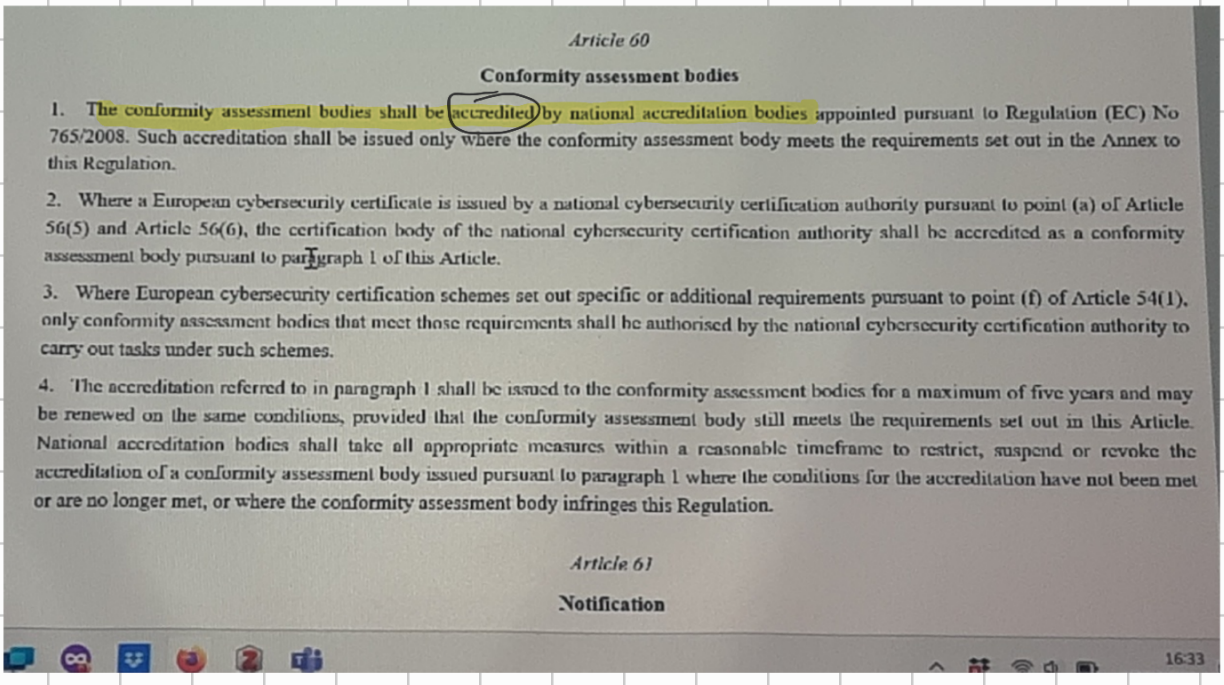
5. Member States shall ensure that national cybersecurity certification authorities have adequate resources to exercise their powers and to carry out their tasks in an effective and efficient manner.

We will need a system to check for the cert. This works for every single MS.

(1) We will have the National Authority (ITALY = ACN).

(2) If I am NA I can't have any contact with those who ask me to grant certs. The independence of each actor is important.

Conf. Assess. BODIES: The NA has the possibility to undertake the CAB: we have a lot of manufacturers and 1 NA!



Article 60

Conformity assessment bodies

1. The conformity assessment bodies shall be accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008. Such accreditation shall be issued only where the conformity assessment body meets the requirements set out in the Annex to this Regulation.

2. Where a European cybersecurity certificate is issued by a national cybersecurity certification authority pursuant to point (a) of Article 56(5) and Article 56(6), the certification body of the national cybersecurity certification authority shall be accredited as a conformity assessment body pursuant to paragraph 1 of this Article.

3. Where European cybersecurity certification schemes set out specific or additional requirements pursuant to point (f) of Article 54(1), only conformity assessment bodies that meet those requirements shall be authorised by the national cybersecurity certification authority to carry out tasks under such schemes.

4. The accreditation referred to in paragraph 1 shall be issued to the conformity assessment bodies for a maximum of five years and may be renewed on the same conditions, provided that the conformity assessment body still meets the requirements set out in this Article. National accreditation bodies shall take all appropriate measures within a reasonable timeframe to restrict, suspend or revoke the accreditation of a conformity assessment body issued pursuant to paragraph 1 where the conditions for the accreditation have not been met or are no longer met, or where the conformity assessment body infringes this Regulation.

Article 61

Notification

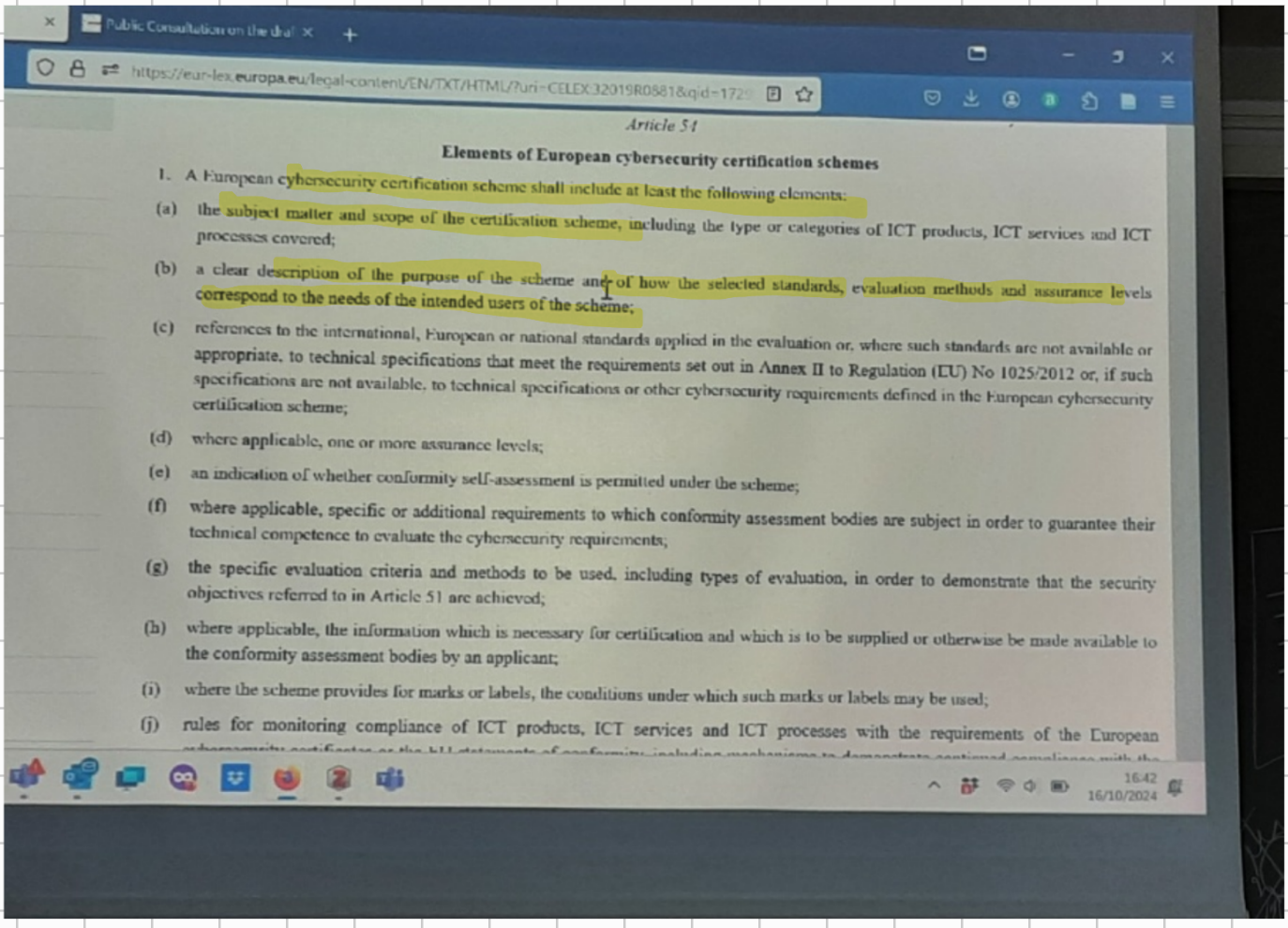
16:33

(1) Conf. assessment bodies will ensure compliance. So the CAB requires tech docs and proof for compliance, then if you have a green light you go to the NA and give you the label. To ensure independence and no corruption, we cannot make people pay for evaluation. The state will supply investments.

But what happens after a couple of years? So let's say I do not comply anymore with the cert? It is possible to have control for compliance in the future too.

Problem: only sanction is suspension or removal of the label. NOTE: the CERT suspension could damage your reputation, sure, but is it enough?

NOTE: it's possible that this structure isn't needed:



Public Consultation on the draf

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&qid=172

Article 51

Elements of European cybersecurity certification schemes

1. A European cybersecurity certification scheme shall include at least the following elements:

(a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services and ICT processes covered;

(b) a clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme;

(c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;

(d) where applicable, one or more assurance levels;

(e) an indication of whether conformity self-assessment is permitted under the scheme;

(f) where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements;

(g) the specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the security objectives referred to in Article 51 are achieved;

(h) where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant;

(i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;

(j) rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European

16:42
16/10/2024

(2) What are the assurance levels: we do not have B&W, but also Grey. Same tech can be used in different areas and different contexts with different level of risks. You cannot ask SMEs to spend a lot!
We provide the basic vs substantial assurance levels, and medium. Diff. levels based on the type of risks and attacks. Ass. levels also have an impact on the assessment process. The lowest assurance level can also be self assessed. So it's not extremely expensive to invest. So I'll go to the NA and say "I did my work" to get the CERT. You can still get checked by CAB.

Certification schemes – governance

(97) Once a European cybersecurity certification scheme is adopted, **manufacturers or providers of ICT products, ICT services or ICT processes should be able to submit applications for certification** of their ICT products or ICT services to the conformity assessment body of their choice anywhere in the Union. Conformity assessment bodies should be accredited by a national accreditation body if they comply with certain specified requirements set out in this Regulation. Accreditation should be issued for a **maximum of five years and should be renewable on the same conditions** provided that the conformity assessment body still meets the requirements. **National accreditation bodies should restrict, suspend or revoke the accreditation of a conformity assessment body where the conditions for the accreditation have not been met or are no longer met**, or where the conformity assessment body infringes this Regulation.

Certification schemes – conformity assessment

Art 53

1. A European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes. **Conformity self-assessment shall be permitted only in relation to ICT products, ICT services and ICT processes that present a low risk corresponding to assurance level 'basic'.**

2. The manufacturer or provider …may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By issuing such a statement, the manufacturer or provider …shall assume responsibility for the compliance of the ICT product, ICT service or ICT process with the requirements set out in that scheme.

3. T**he manufacturer or provider …shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products or ICT services with the scheme available to the national cybersecurity certification autho**rity referred to in Article 58 for the period provided for in the corresponding European cybersecurity certification scheme. A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.

4. The issuing of an EU statement of conformity is voluntary, unless otherwise specified in Union law or Member State law.

5. EU statements of conformity shall be recognised in all Member States.

SUM UP:

Certification schemes

Centralised system

Granular system

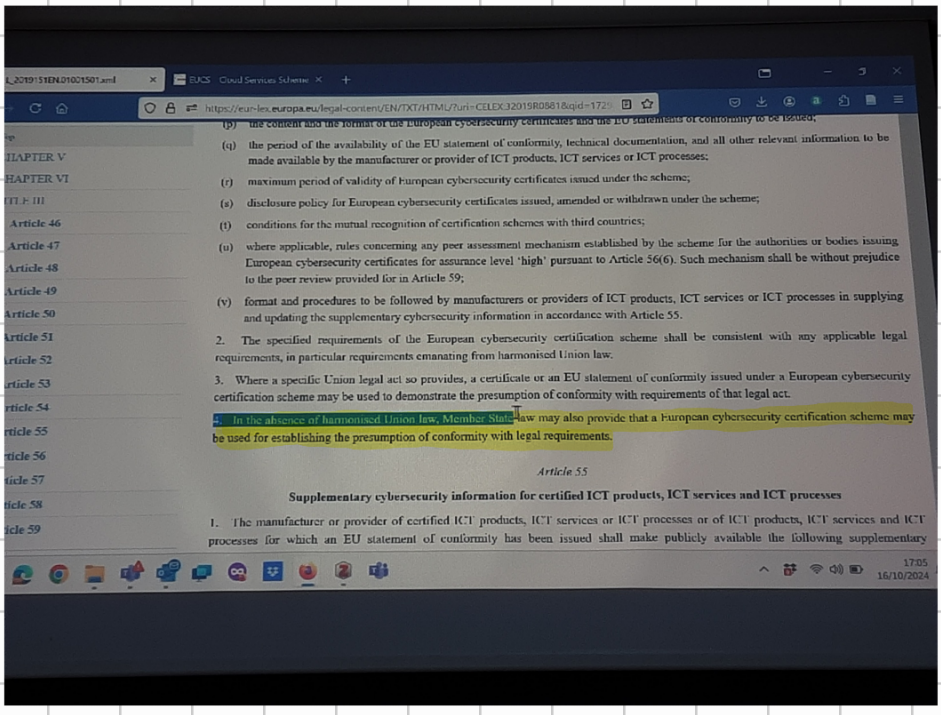
Legal effect ①

makes the balls rolling

We have a centralised struct: who does what? Commission, ENISA does the draft and commission approves the scheme. ASA you have the European Certificate, the others will fade out.

The assurance level is important for the manufactors: a SME cannot immediately get to high level of assurance if we have non critical actors. We might not bother to have a high level, so this allows the cert. to adapt to the need of the entities. This helps both the big guys and the small providers. It also helps the small entities to understand what security means.

(1)



- For instance I have a legislation called Cyber resilience Act. If there's no standard the cert. scheme can become one. For ex. The NIS has set the standard for sec. of OES. If there was a EU scheme for transport security, and ES one already compliant with the standard I don't need to comply with NIS since I already comply with the cert. The EU will tell "You comply if you comply with standards".

Proposal for a revision of the Cybersecurity Act

Matter of including something new?

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services

COM/2023/208 final

Main change

- Inclusion of managed security services (service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident response, penetration testing, security audits and consultancy) also as a subject for certification schemes (1)

We have certs about ICT products, services and procedures.

(1) So the focus was on the internal product and company. In this case we are including managed security services: there are companies that provide pen tests: possibility to have those activities included.

Proposal for a revision of the Cybersecurity Act

51 objective of certs schemes.

'Article 51a Security objectives of European cybersecurity certification schemes for managed security services

A European cybersecurity certification scheme for managed security services shall be designed to achieve, as applicable, at least the following security objectives:

- (a) ensure that the managed security services are provided with the requisite competence, expertise and experience, including that the staff in charge of providing these services has a very high level of technical knowledge and competence in the specific field, sufficient and appropriate experience, and the highest degree of professional integrity;
- (b) ensure that the provider has appropriate internal procedures in place to ensure that the managed security services are provided at a very high level of quality at all times ;
- (c) protect data accessed, stored, transmitted or otherwise processed in relation to the provision of managed security services against accidental or unauthorised access, storage, disclosure, destruction, other processing, or loss or alteration or lack of availability;
- (d) ensure that the availability and access to data, services and functions is restored in a timely manner in the event of a physical or technical incident;
- (e) ensure that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;
- (f) record, and enable to assess, which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
- (g) ensure that the ICT products, ICT services and ICT processes [and the hardware] deployed in the provision of the managed security services are secure by default and by design, do not contain known vulnerabilities and include the latest security updates;';

(1) Not just certifying the object of cec, but also the people who provides you the product.

(2) Whenever I'm providing the services I will be certified.