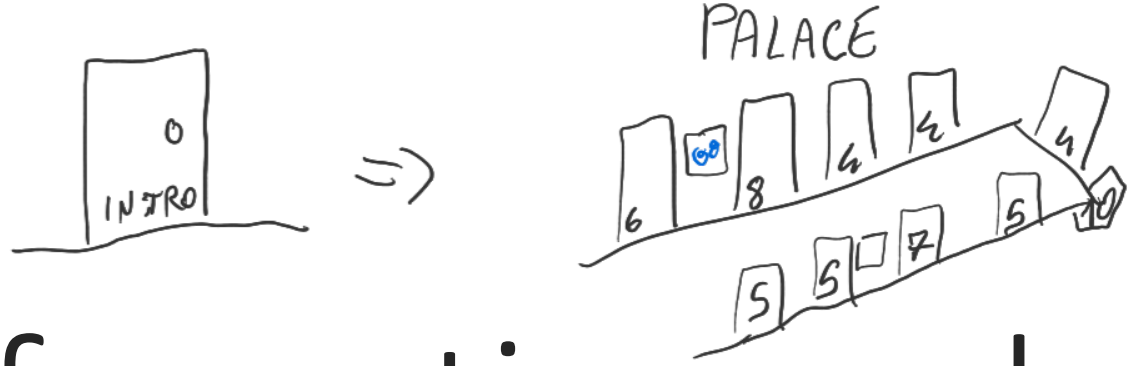


Information and technology law course

LECTURE 4 – 5 / 3 – 7 OCTOBER 2023

FEDERICA CASAROSA – 2024/2025

First one to address NIF security system. But it has to be updated very soon! That's why we have NIS 2.

This is a directive: require implementation at National Level. Translate it into the national legal system, adapt them to the legal system. They are general and need to implement them.

NIS Directive

Allows some time for the implem. (usually 18 month). Until 2018 (June 2016) we didn't have anything. But the impl. is still valid. Same procedure applies*

EU Directive 2016/1148 concerning measures for a high level of common security of network and information systems across the Union (1)

Art. 1(1) (3)

- "This Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market".

* for the NIS 2

2016 (June) | 2022 | NOW

NIS | NIS 2 | October 2024 ⇒ implementation 2024

Adoption dates

2018

National

NIS

(You have to have it by 18 months)

here we had 4 DPCM implementing all the parts of the NIS. Now we will have other interventions that will apply the changes of NIS 2.

NIS is a general framework. Member states will have to be more detailed. NIS and NIS 2 represent 2 different contexts.

Why directive in this case? There was increased cyberattacks and then cyberthreats and attacks occurred (WNCRY). There was the need to react at a national level. But for member states there were different levels of protection. If we are all connected and there is a vulnerable node that's an entrance. So we wanted a high level of common security (1)

If we have several countries with different levels of security, in the best case we want very high level of security. But for countries that do not have a very high level getting there in 18 months is not possible. So we just want a quite good upper level of security.

"If something happens to Estonia, the type of approach to the cyberattack will be the same as the Spain one. This gives a faster response time.

Article 114 of the TFEU, speaks about internal market. The reliability and functioning of business is essential in particular to the functioning of the internal market.
NOT ADDRESSING NATIONAL DEFENSE but the COMPANIES so MARKETS FLOURISH.
As EU I want to solve the fragmentation.
"Such incidents can impede the pursuit of economic activities, damage the economy of the Union".
The 3 first recitals set the scene for the market.
(4) The existing capabilities are not sufficient at Memb. State level, because of very different levels of preparedness and there's fragmentation. => Unequal level of protection in businesses.
I can provide work in the direction of the market, but the M.S. are not able to establish a common ground. I therefore intervene.

Art. 1: Purpose (3): we want harmonized system. Obj: internal market.
- Lays down obligations for member states to adopt a national strategy on the security of net. and IS.
- Create a Cooperative Group to support info sharing.
- Create a CSIRTs Network. Each MS will have their own CSIRT, participating in a Network,
- Security and notification requirements for operators of essential services (↳ connected to int.) and for digital service providers. (They have to adopt measures in order to prevent breaches and notify requir. => if a breach happens they have to report to CSIRT).
- Obligations to designate national competent authorities, single points of contact and CSIRT with tasks related to security of net and info system.

- Companies will need to have point of reference for cybersecurity.
- Revolutionary system for countries which had nothing.
- Lexes specialis (general legislation that applies to everywhere) ↶ Lex Generalis
  ↳ Law dedicated to a sector
  ↳ sector specific

If there are other legal acts by the EU, those provisions of that sector specific Union legal act shall apply (provided that such requirements are at least equivalent in effect to the obligations laid down in this Directive). [This only refers to Union legal acts]
THIS IS FOR SETTING FRAMEWORK.

NIS directive

Lex specialis principle

Art 1 (7)

Where a sector-specific Union legal act requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents, provided that such requirements are at least equivalent in effect to the obligations laid down in this Directive, those provisions of that sector-specific Union legal act shall apply.

Objectives

(5) The existing capabilities are not sufficient to ensure a high level of security of network and information systems within the Union. Member States have very different levels of preparedness, which has led to fragmented approaches across the Union. This results in an unequal level of protection of consumers and businesses and undermines the overall level of security of network and information systems within the Union. Lack of common requirements on operators of essential services and digital service providers in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level. Universities and research centres have a decisive role to play in spurring research, development and innovation in those areas.

Source:

Analysis of the cybersecurity ecosystem in the European Union

Zsolt Bederna · Zoltan Rajnai

Int. Cybersecur. Law Rev. (2022) 3:35–49

Cybersecurity ecosystem

If something happens to the banking provider can have effects on other nodes.

It's important that the connection among the states are crowded.

We wanted to make all these actors secure. Objective: acknowledge this system but make a step forward to make the system secure.

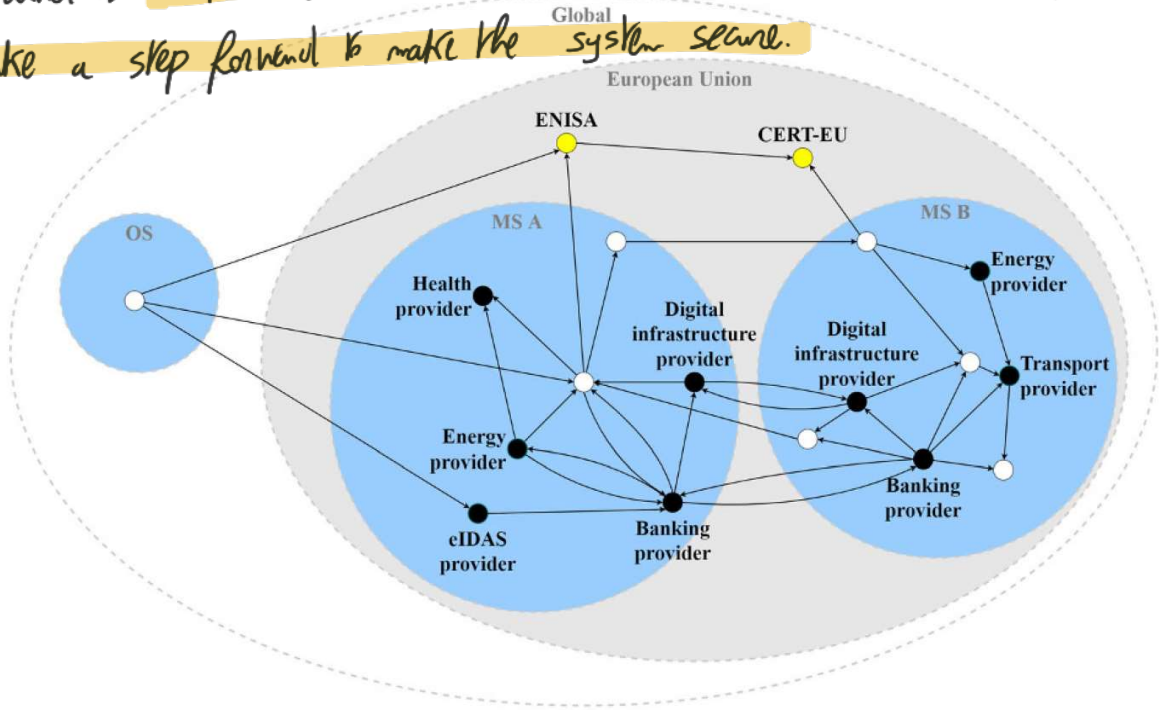


Fig. 2 Conceptualising a subset of stakeholders with hypothetical dependencies (source: own edit)

Objectives of NIS directive

(1) on the Union-level to create a Cooperation Group to support and facilitate strategic cooperation and information exchange among the Member States and to create the computer security incident response teams network (CSIRTs network) promoting operational cooperation;

(2) for Member States to adopt a national strategy and to designate the national competent authorities and at least one competent CSIRT for the essential services; and

(3) for operators of essential services (OESs) and for digital service providers (DSPs) to comply with the established security-related requirements.

National frameworks

Article 7 National strategy on the security of network and information systems

1. Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering at least the sectors referred to in Annex II and the services referred to in Annex III. The national strategy on the security of network and information systems shall address, in particular, the following issues:

(a) the objectives and priorities of the national strategy on the security of network and information systems;

(b) a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors;

(c) the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors;

(d) an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems;

(1) (e) an indication of the research and development plans relating to the national strategy on the security of network and information systems;

(2) (f) a risk assessment plan to identify risks;

(5) (g) a list of the various actors involved in the implementation of the national strategy on the security of network and information systems.

(6) 2. Member States may request the assistance of ENISA in developing national strategies on the security of network and information systems.

Article 7:

We need a cybersec. Strategy for MS.

- Not just giving you the title: she'll give a structure to comply with:
  - The objectives and priorities of the nat. strategy on the security of net. and IS.
  - A governance framework to achieve objectives and priorities of the national strategy, including roles and responsibilities of the government bodies and other relevant actors: you have to put the CSIRT and new organs into the government. They should have direct links to the ministry. We have to create a government framework.
- (3) The identification of measures relating to preparedness, response and recovery including cooperation between public and private sectors. I have to find the measures for all of that and interpret them. Identifying in detail the part of the measures.
- Indication of education, awareness-raising and training programmes relating to the national strategy on the security of net. and IS. Citizens and employee need to know! Not just experts.

(1) To achieve evolution and learning to have something more.

(2) I have to know what would be the problems that might arise (3) connection. (2) is the first step, (3) is the reaction. Risk assessment of my country (ex. essential workers) and then that.

(5)

(6) Since it is difficult and have problems ask Enisa to get help.

Member states shall communicate their strategy to the EU.

Article 8: Actors that will be the experts:

- each member state shall designate

Article 8

National competent authorities and single point of contact

1. Each Member State shall designate one or more national competent authorities on the security of network and information systems ('competent authority'), covering at least the sectors referred to in Annex II and the services referred to in Annex III. Member States may assign this role to an existing authority or authorities.

2. The competent authorities shall monitor the application of this Directive at national level.

3. Each Member State shall designate a national single point of contact on the security of network and information systems ('single point of contact'). Member States may assign this role to an existing authority. Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.

4. The single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group referred to in Article 11 and the CSIRTs network referred to in Article 12.

5. Member States shall ensure that the competent authorities and the single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the Cooperation Group.

6. The competent authorities and single point of contact shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities.

7. Each Member State shall notify to the Commission without delay the designation of the competent authority and single point of contact, their tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority and single point of contact. The Commission shall publish the list of designated single points of contacts.

15:32

(S) Don't just put there the authorities. Give them money to work. Otherwise the authority won't work.

Single point of contact should be contacted (the people to contact when in need)

National frameworks

Article 9 Computer security incident response teams (CSIRTs)

1. Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority.

2. Member States shall ensure that the CSIRTs have adequate resources to effectively carry out their tasks as set out in point (2) of Annex I.

Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 12.

3. Member States shall ensure that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level.

4. Member States shall inform the Commission about the remit, as well as the main elements of the incident-handling process, of their CSIRTs.

5. Member States may request the assistance of ENISA in developing national CSIRTs.

The CSIRT should be able to share info securely

ACN is the nat. authority and CSIRT.

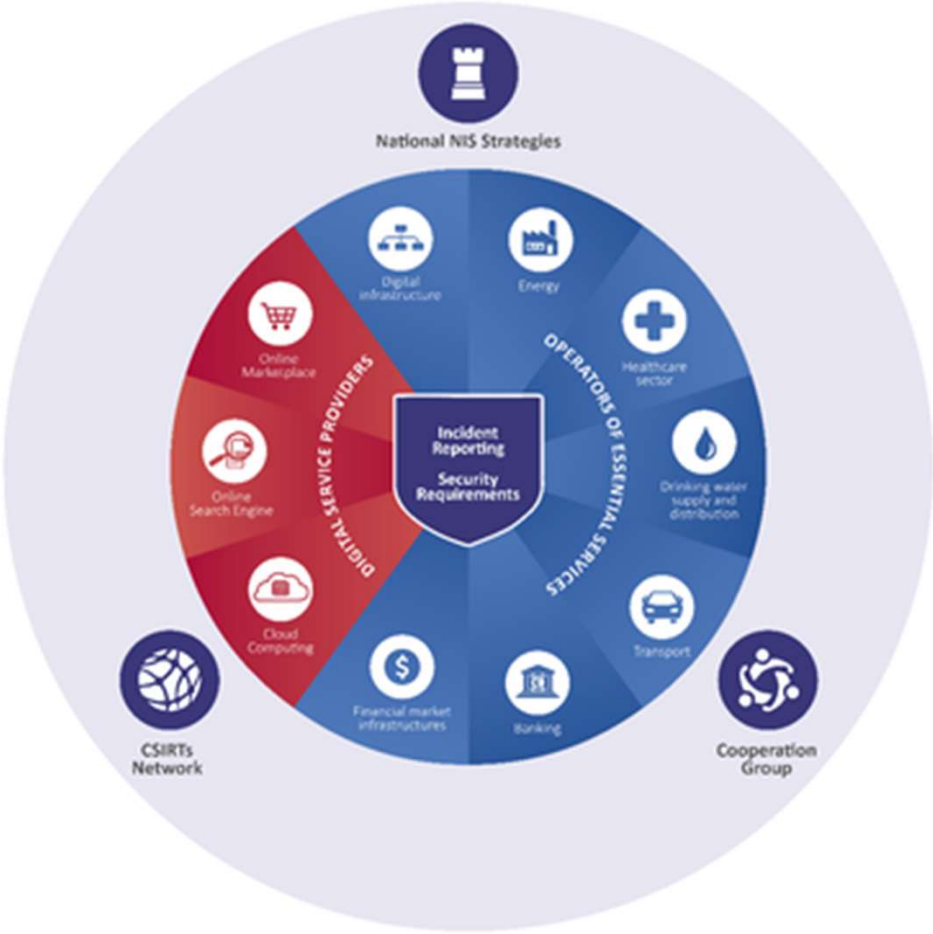
2008 → 2016 → 2022
CI Operators of essential services and digital service providers EE IE (almost same as CE)

Who are them? The ones that provide essential services for member states.

Target

Operators of essential services and

Digital service providers



They should define who they are. In Italy it's state secret. Just list the companies. If they disclose info they are more vulnerable.

Operators of essential services

Article 5 Identification of operators of essential services

1. By 9 November 2018, for each sector and subsector referred to in Annex II, Member States shall identify the operators of essential services with an establishment on their territory.

2. The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows:

- (a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
- (b) the provision of that service depends on network and information systems; and
- (c) an incident would have *significant disruptive effects* on the provision of that service.

... (b) I know what is need to be connected to provide that system. Doesn't matter with who

Where do we need to look at? 2016

Energy (electricity, oil, gas), transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, digital infrastructures.

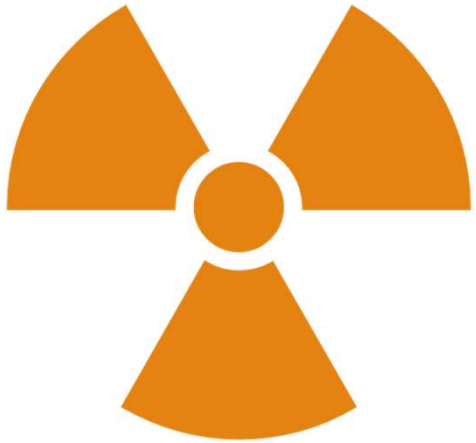
Digital service providers: online marketplace, online search engine, cloud computing service.

The first ones are essential, those are providers, they are a bit less important. They have less requirements.

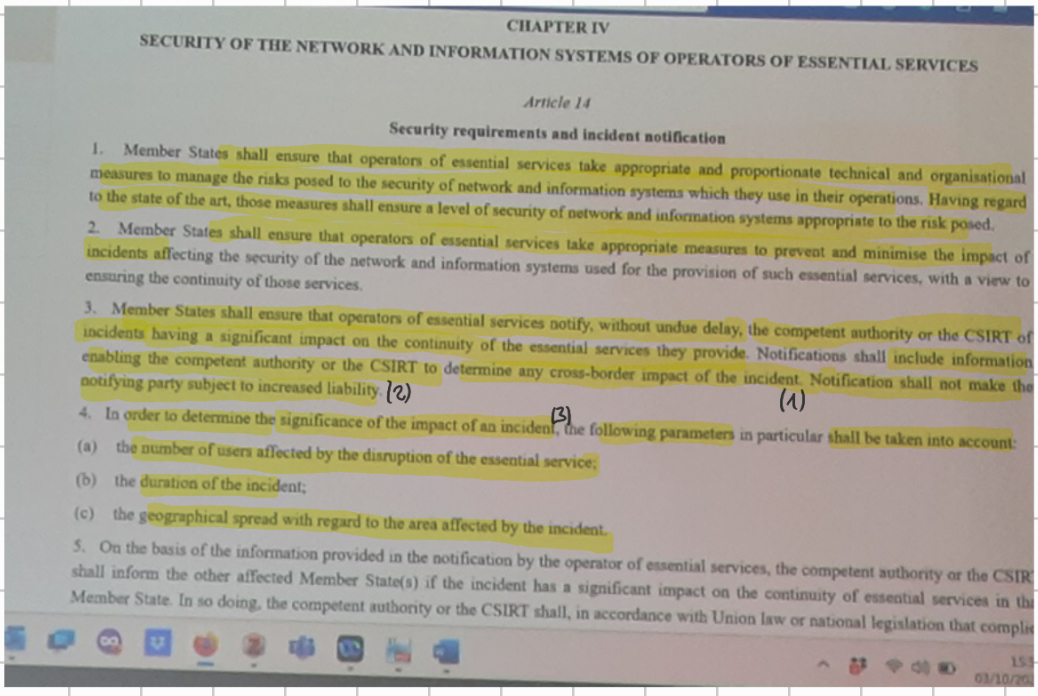
Critical incidents

Article 6 Significant disruptive effect We have the sectors (essential)

1. When determining the significance of a disruptive effect as referred to in point (c) of Article 5(2), Member States shall take into account at least the following cross-sectoral factors:
   - (a)the number of users relying on the service provided by the entity concerned;
   - (b)the dependency of other sectors referred to in Annex II on the service provided by that entity;
   - (c)the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety; how much margin is loose.
   - (d) the market share of that entity;
   - (e) the geographic spread with regard to the area that could be affected by an incident;
   - (f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.



Requirements: Article 14:



CHAPTER IV

SECURITY OF THE NETWORK AND INFORMATION SYSTEMS OF OPERATORS OF ESSENTIAL SERVICES

Article 14

Security requirements and incident notification

1. Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

3. Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability. (2) (1)

4. In order to determine the significance of the impact of an incident, (3) the following parameters in particular shall be taken into account:

(a) the number of users affected by the disruption of the essential service;

(b) the duration of the incident;

(c) the geographical spread with regard to the area affected by the incident.

5. On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in the Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies

(1) We start again with risk assessment in order to set the measures needed. As soon as I have the risk I have the state of the art (acknowledge by the experts community) (state of the art and science ...). As something happens I need to ensure if you are up to date with your measures. Most updated measures = state of the art measures.
=> Risk evaluation, measures looking at the state of the art.

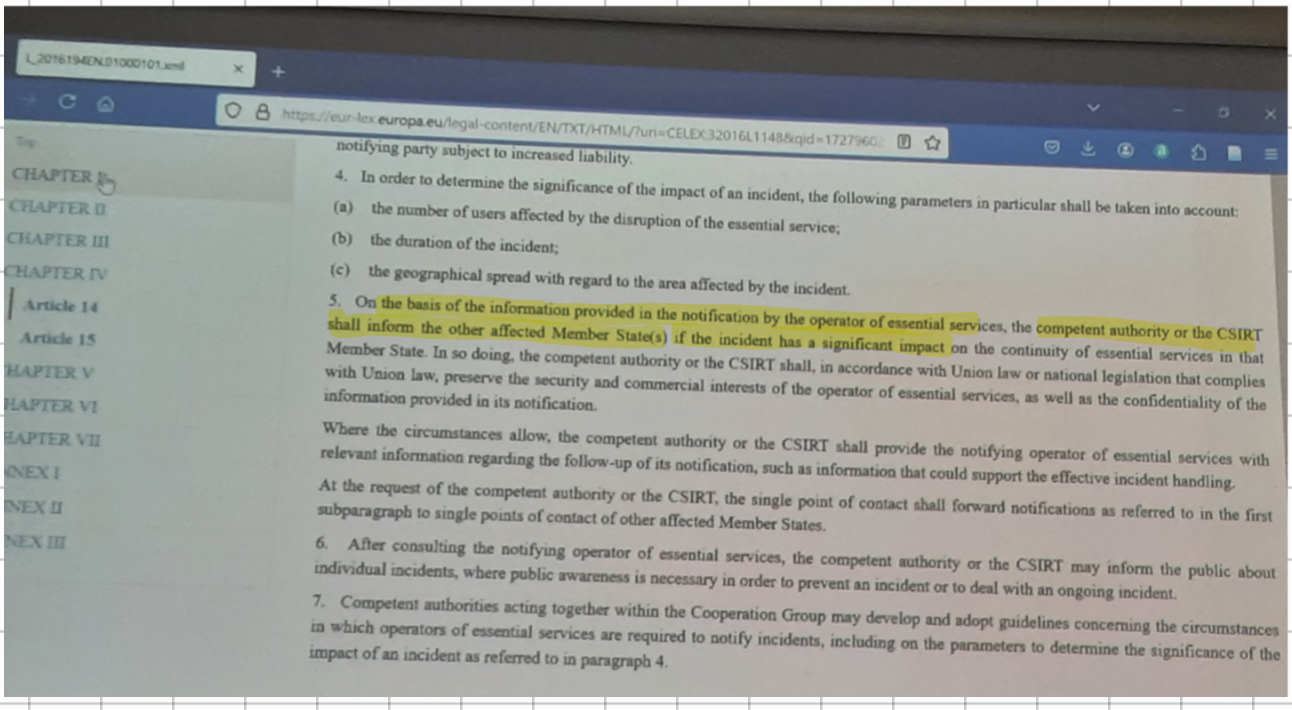
- It's the member state that checks that the operator is taking appropriate measures.

Back to (1), the measures are technical and organizational measures. Article 14 does not tell you what measures. Based on the risks.

(2) Prevention and resilience (minimise the impact: measures to mitigate).

(3) OK, took all the measures but you get attacked. You have to notify. "Undue delay"; how long? In Italy 6-12 hours. Given the notif, CSIRT may have info about similar incidents to provide guidance. A dialogue is opened. (1) The impact could vary! (2) Saying there is a problem will not make me liable. This is not something that will be used against me for liability. Liability is 0 if you were not negligent and did what you had to suggested in (1).

(3) This defines the threshold. Depends on the parameters adopted by the MS.


L_2016194EN.01000101.xml
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&qid=1727960
Top
CHAPTER I
CHAPTER II
CHAPTER III
CHAPTER IV
Article 14
Article 15
HAPTER V
HAPTER VI
HAPTER VII
NEX I
NEX II
NEX III
notifying party subject to increased liability.
4. In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:
(a) the number of users affected by the disruption of the essential service;
(b) the duration of the incident;
(c) the geographical spread with regard to the area affected by the incident.
5. On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification.
Where the circumstances allow, the competent authority or the CSIRT shall provide the notifying operator of essential services with relevant information regarding the follow-up of its notification, such as information that could support the effective incident handling.
At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications as referred to in the first subparagraph to single points of contact of other affected Member States.
6. After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident.
7. Competent authorities acting together within the Cooperation Group may develop and adopt guidelines concerning the circumstances in which operators of essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident as referred to in paragraph 4.

Operators of essential service

Consistency approach in OES identification

- 1. To reduce the risks related to cross-border dependencies:
- 2. To guarantee a level playing field for operators in the internal market:
- 3. To reduce the risk of divergent interpretations of the Directive:
- 4. To develop a comprehensive overview of the level of cyber-resilience across the EU

Security requirements - OSE

Art 14 Security requirements and incident notification

1. Member States shall ensure that operators of essential services *take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations*. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

2. Member States shall ensure that operators of essential services *take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services*, with a view to ensuring the continuity of those services.

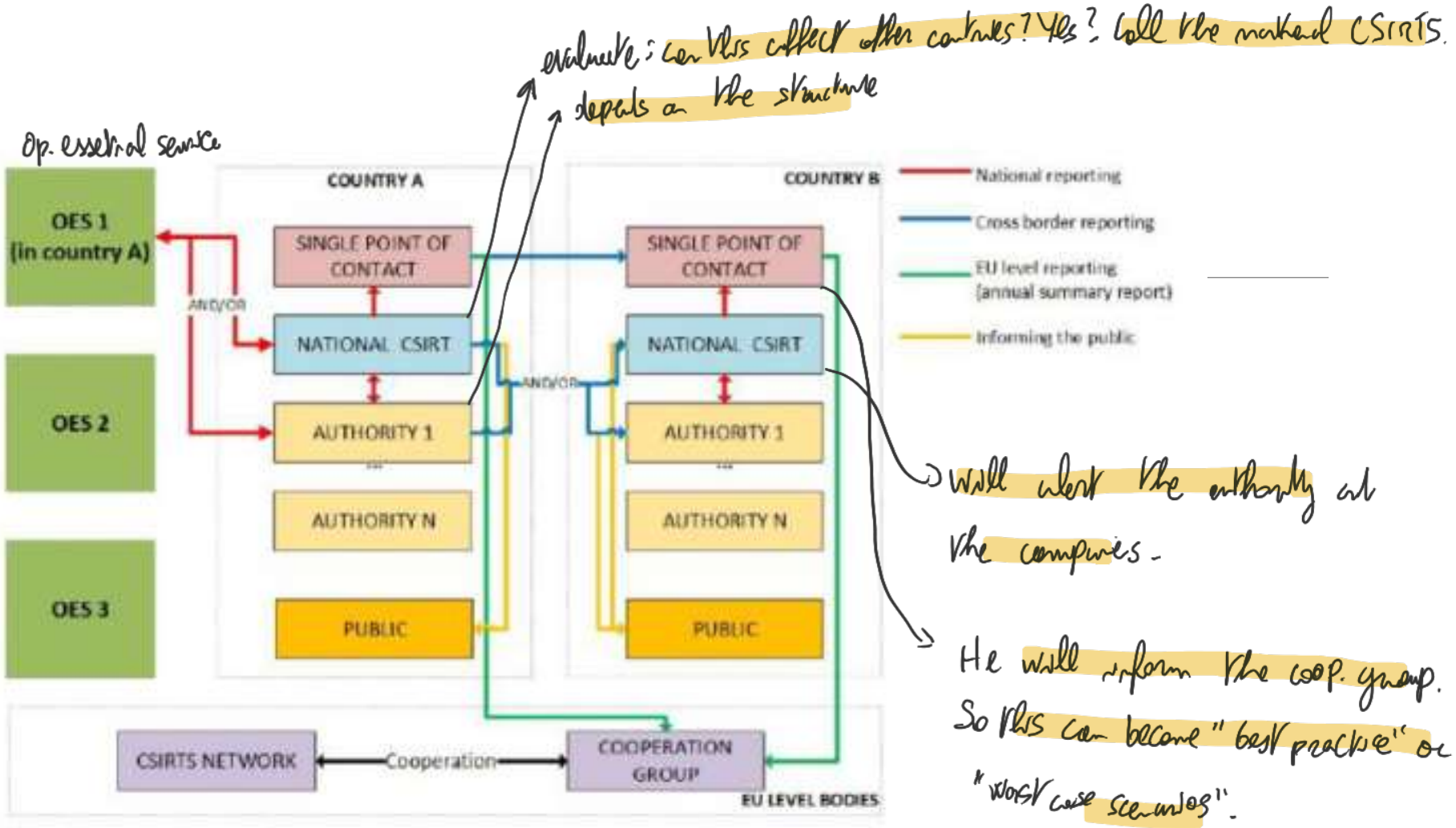
Incident notification – OSE

Art 14 Security requirements and incident notification

3. Member States shall ensure that *operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide*. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

4. In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:

- (a) the number of users affected by the disruption of the essential service;
- (b) the duration of the incident;
- (c) the geographical spread with regard to the area affected by the incident.


Op. essential service
COUNTRY A
COUNTRY B
OES 1 (in country A)
OES 2
OES 3
SINGLE POINT OF CONTACT
NATIONAL CSIRT
AUTHORITY 1
AUTHORITY N
PUBLIC
AND/OR
CSIRTS NETWORK
Cooperation
COOPERATION GROUP
EU LEVEL BODIES
National reporting
Cross border reporting
EU level reporting (annual summary report)
Informing the public
evidence: can this affect other countries? Yes? Call the national CSIRTS.
depends on the structure
will alert the authority of the companies.
He will inform the coop. group. So this can become "best practice" or "worst case scenarios".

Not all of them are reported. A IV can occurr in a deluged time. The company now is vulnerable and actors might be interested of this vulnerability. This info between company and CSIRT should be secure.

Notification to the public

(59) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing. **Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats against possible reputational and commercial damage for the operators of essential services and digital service providers reporting incidents**. In the implementation of the notification obligations, competent authorities and the CSIRTs should pay particular attention to the need to keep information about product vulnerabilities strictly confidential, prior to the release of appropriate security fixes.

Make sure that when I report to the public, I need to make sure that the problem is solved

There's no obligation to notify the public. It's up to the CSIRTs and the authorities.

In some situations knowledge of the attack may cause criminal interest or damage the company reputation.

Digital service providers

(48)

Many businesses in the Union rely on digital service providers for the provision of their services. As some digital services could be an important resource for their users, including operators of essential services, and as such users might not always have alternatives available, this Directive should also apply to providers of such services. The security, continuity and reliability of the type of digital services referred to in this Directive are of the essence for the smooth functioning of many businesses. **A disruption of such a digital service could prevent the provision of other services which rely on it and could thus have an impact on key economic and societal activities in the Union.** Such digital services might therefore be of crucial importance for the smooth functioning of businesses that depend on them and, moreover, for the participation of such businesses in the internal market and cross-border trade across the Union. Those digital service providers that are subject to this Directive are those that are considered to offer digital services on which many businesses in the Union increasingly rely.

imposes some security requirement (similar to article 12)

Security requirements – DSP

Article 16 Security requirements and incident notification

1. Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:

(a) the security of systems and facilities;

(b) incident handling;

(c) business continuity management; (Resilience, mitigation measures)

(d) monitoring, auditing and testing; (how do I control that the measures are upheld

(e) compliance with international standards. Because they are similar

2. Member States shall ensure that digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services.

Security requirements – DSP

* Not significant. It's stronger. If I am taking into account the threshold for notification there's a difference between Digital service Prov and essential ...

Article 16 Security requirements and incident notification

3. Member States shall ensure that digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability.

4. In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account:

(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;

(b) the duration of the incident; Longer

(c) the geographical spread with regard to the area affected by the incident; Wider

(d) the extent of the disruption of the functioning of the service; Bigger

For DSP than ES ↓

(e) the extent of the impact on economic and societal activities.

The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph.

They are so important that I want to have the knowledge of the incident.

(cloud couple) ? DSP

What happens if an ES operator is relying on a DSP service? What if the incident occurs on the CCS? Who should notify? In this case, the OES should report. But what do they know? They have to contact the DSP and get info to contact CSIRT

Different approach towards DSP

(49) Digital service providers should ensure a level of security **commensurate with the degree of risk posed to the security of the digital services they provide**, given the importance of their services to the operations of other businesses within the Union. In practice, **the degree of risk for operators of essential services, which are often essential for the maintenance of critical societal and economic activities, is higher than for digital service providers**. Therefore, the security requirements for digital service providers should be lighter. Digital service providers should remain free to take measures they consider appropriate to manage the risks posed to the security of their network and information systems. Because of their cross-border nature, digital service providers should be subject to a more harmonised approach at Union level. Implementing acts should facilitate the specification and implementation of such measures.

NIS evaluation

Broad and abstract - pros and cons

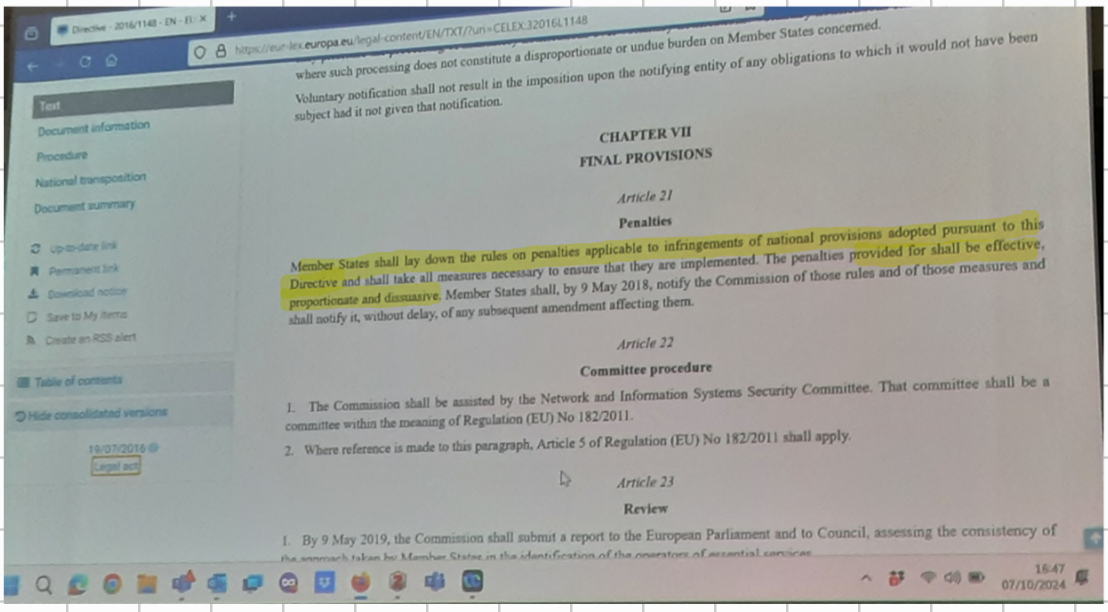
Uniform and continous testing and control is not compulsory

(3) Limited role of law enforcement authorities

In 2020 commission started to evaluate the impact of the directive to see if the MS have implem. it correctly. Main issues: It's good but too broad (several sectors), not so elaborated in terms of measures (remember article 14: organizational and technical measures). The COOPERATION NETWORK was only produced as soft laws. From the legal perspective we needed something more relevant. Having very general provisions was kind of good, because if I was too specific it would have become outdated.

There was also not a check and a continuous control, not something that to be revised. It was not mandatory.

(3) There are no sanctions. In the end:



where such processing does not constitute a disproportionate or undue burden on Member States concerned.

Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification.

CHAPTER VII

FINAL PROVISIONS

Article 21

Penalties

Member States shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by 9 May 2018, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

Article 22

Committee procedure

1. The Commission shall be assisted by the Network and Information Systems Security Committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 23

Review

1. By 9 May 2019, the Commission shall submit a report to the European Parliament and to Council, assessing the consistency of

Penalties were up to the member states; some were stricter and other lighter.
Only guideline: something that goes against who did something wrong (effective), proportionate and dissuasive (for others).

Number of operators of Essential services:

Figure 1: The number of OESs identified differs significantly across the EU

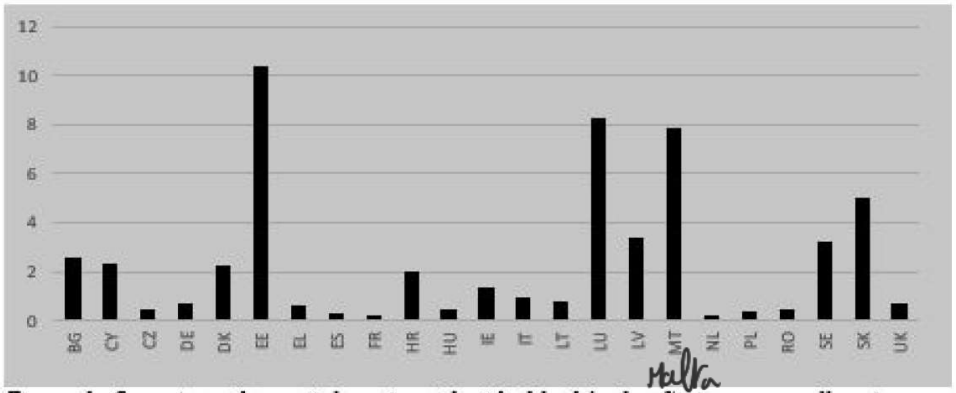


Figure 1: Operators of essential services identified by Member States across all sectors per 100 000 inhabitants[1]

Source: European Commission, 2020.

Proportionate to the number of inhabitants. In some countries there are a lot, in others not so much. We need to have better criteria to find operators of ES.

NIS evaluation

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS 2)

Expanding the scope of the current NIS Directive

New sectors based on their criticality for the economy and society

Eliminate the distinction between operators of essential services and digital service providers

Strengthen security requirements for the companies, by imposing a risk management approach

* So for cybersec. risks, look at NIS 2, for other risks look at 2554.
JMP A

NIS 2 Directive

Article 2

1. This Directive applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union. Article 3(4) of the Annex to that Recommendation shall not apply for the purposes of this Directive.

2. Regardless of their size, this Directive also applies to entities of a type referred to in Annex I or II, where:
   - (a) services are provided by:
     - (i) providers of public electronic communications networks or of publicly available electronic communications services;
     - (ii) trust service providers;
     - (iii) top-level domain name registries and domain name system service providers;
   - (b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;
   - (c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;
   - (d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;
   - (e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;
   - (f) the entity is a public administration entity:
   - (i) of central government as defined by a Member State in accordance with national law; or
   - (ii) at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities.

3. Regardless of their size, this Directive applies to entities identified as critical entities under Directive (EU) 2022/2557.

4. Regardless of their size, this Directive applies to entities providing domain name registration services.

Source: Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations

Thomas Sievers

Int. Cybersecur. Law Rev. (2021) 2:223–231

*Something new! That now has become important

A

Table 1 Comparison of sectors under NIS1 (not in bold) and NIS2 (in bold); sub-sectors in parenthesis. The order of the listed (sub-)sectors corresponds to the one in the NIS2 Annexes

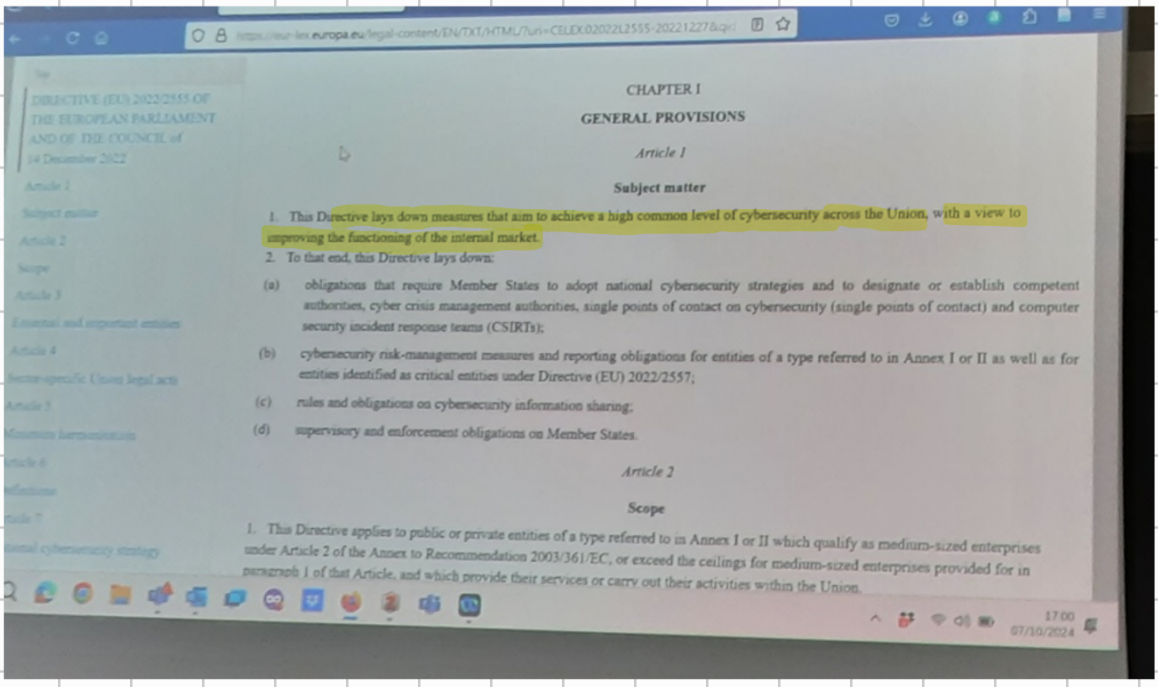
Essential entities	Important entities
– Energy (electricity—now including **production**; **aggregation**; **demand response** and **energy storage**; **electricity markets**—; **district heating**; oil; gas and **hydrogen**)	– **Postal and courier services** – **Waste management** – **Chemicals** (**manufacture**; **production**; **distribution**) – **Food** (**production**; **processing**; **distribution**) – **Manufacturing** (**medical devices**; **computer, electronic and optical products**; **electrical equipment**; **machinery**; **motor vehicles and (semi-)trailers**; **transport equipment**) – Digital providers (online marketplaces; search engines; **social networks**)
– Transport (air; rail; water; road) – Banking – Financial market infrastructures – Health (healthcare; **EU reference labs**; **research and manufacturing of pharmaceuticals and medical devices**) – Drinking water – **Waste water** – Digital infrastructure (IXP; DNS; TLD; cloud; **data centre service providers**; **CDN**; **trust service providers**; **electronic communications**) – **Public administrations** – **Space**	

→ it's here now.

Not included before. New sectors are included that were not there before.

Different Terminology: EE and IE. Remember the Cloud incident: the ES operator was a mediator. Now we don't have this differentiation anymore: obligations for EE and IE are the same. They all have same security and notif requirements. *1

#1



CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

1. This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market.
2. To that end, this Directive lays down:

(a) obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);

(b) cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive (EU) 2022/2557;

(c) rules and obligations on cybersecurity information sharing;

(d) supervisory and enforcement obligations on Member States.

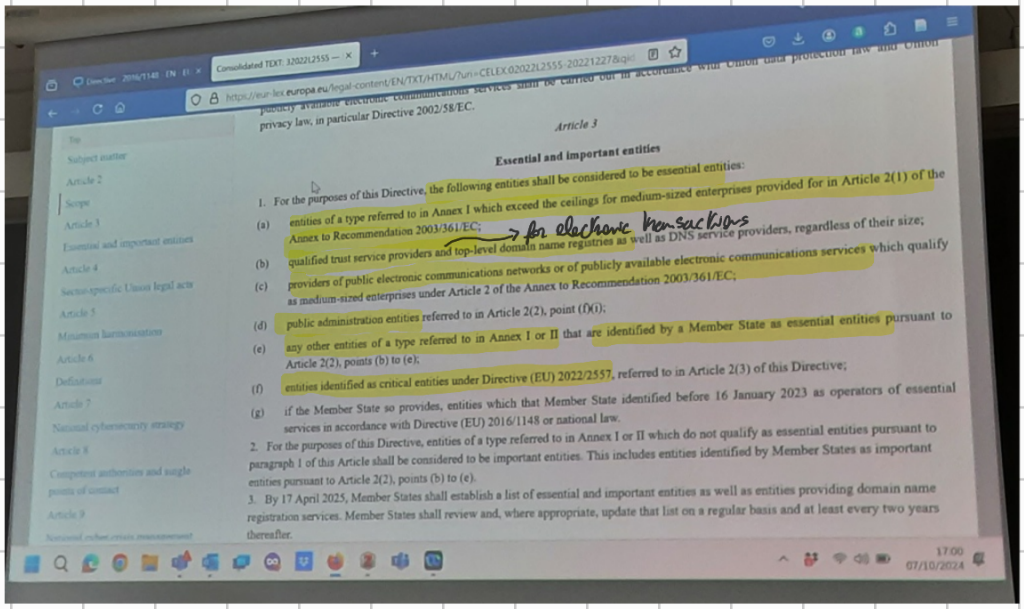
Article 2

Scope

1. This Directive applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union.

Objectives are practically the same.

© Orgs. that offer essential comm. infrastr. and services to the public (telephone lines, cellular networks, ADSL, fibers, mobile data services)



privacy law, in particular Directive 2002/58/EC.

Article 3

Essential and important entities

1. For the purposes of this Directive, the following entities shall be considered to be essential entities:

(a) entities of a type referred to in Annex I which exceed the ceilings for medium-sized enterprises provided for in Article 2(1) of the Annex to Recommendation 2003/361/EC; → for electronic transactions

(b) qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size;

(c) providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC;

(d) public administration entities referred to in Article 2(2), point (f)(i);

(e) any other entities of a type referred to in Annex I or II that are identified by a Member State as essential entities pursuant to Article 2(2), points (b) to (e);

(f) entities identified as critical entities under Directive (EU) 2022/2557, referred to in Article 2(3) of this Directive;

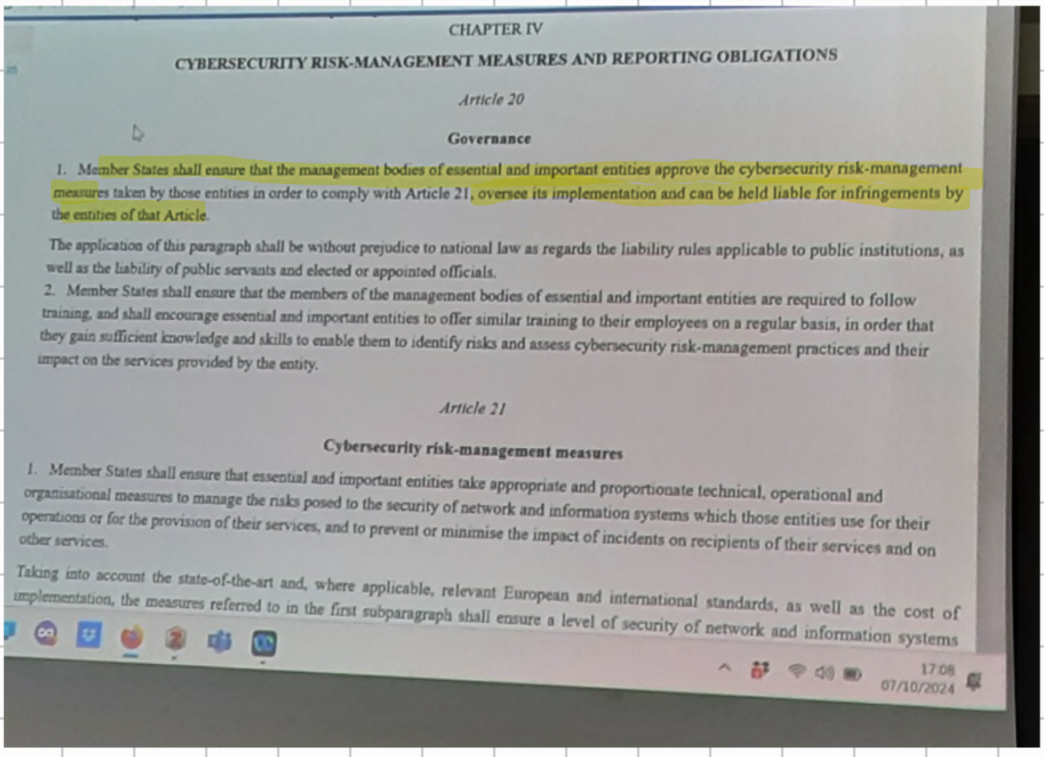
(g) if the Member State so provides, entities which that Member State identified before 16 January 2023 as operators of essential services in accordance with Directive (EU) 2016/1148 or national law.

2. For the purposes of this Directive, entities of a type referred to in Annex I or II which do not qualify as essential entities pursuant to paragraph 1 of this Article shall be considered to be important entities. This includes entities identified by Member States as important entities pursuant to Article 2(2), points (b) to (e).

3. By 17 April 2025, Member States shall establish a list of essential and important entities as well as entities providing domain name registration services. Member States shall review and, where appropriate, update that list on a regular basis and at least every two years thereafter.

(1) Whatever goes over the medium-sized enterprise is an essential entity.
But, not all countries have huge enterprises. This won't always work. We have exceptions:
(e) But the MS can also add essential entities.
(f) directive of resilience. If you are a critical entity there, you are an EE here.
(g) the old ES defined by the NIS 2.
In the NIS, only member states decided, in this case it is not needed. We are enlarging the level of control over companies.

- Nothing changed in terms of competent authorities and national cybersecurity strategy.



CHAPTER IV

CYBERSECURITY RISK-MANAGEMENT MEASURES AND REPORTING OBLIGATIONS

Article 20

Governance

1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.

The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.

2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Article 21

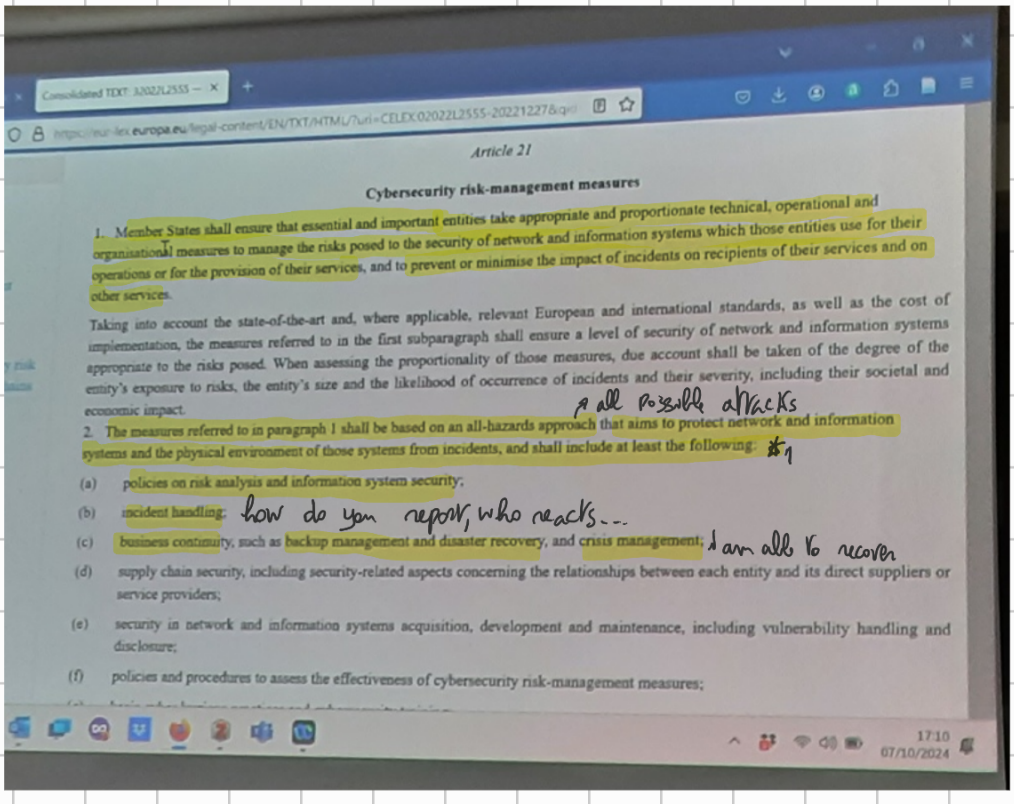
Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems

17:08
07/10/2024

- We have liability: if you are negligent, the CEO will be held responsible. It's not just left without control.



Consolidated TEXT: 32022L2555 — ×

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02022L2555-20221227&qid

Article 21

Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following: *1

(a) policies on risk analysis and information system security;

(b) incident handling; how do you report, who reacts...

(c) business continuity, such as backup management and disaster recovery, and crisis management; I am able to recover

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

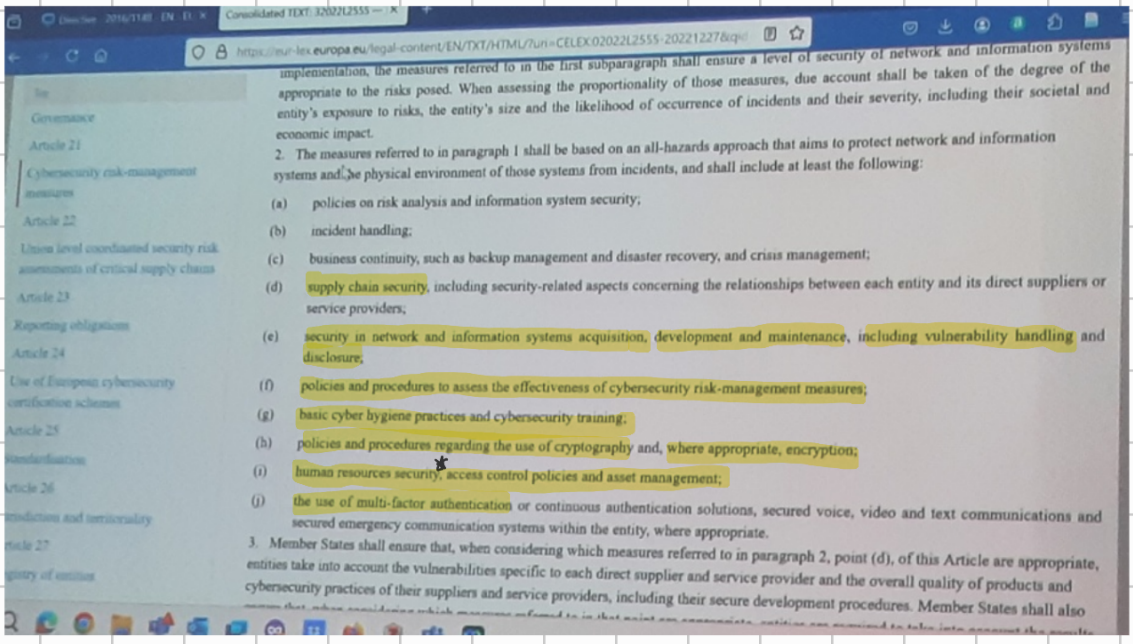
(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

17:10
07/10/2024

all possible attacks

(1) Not what delivered, but we have a list in par. 2.

*1 take at least into account



Governance
Article 21
Cybersecurity risk-management measures
Article 22
Union level coordinated security risk assessments of critical supply chains
Article 23
Reporting obligations
Article 24
Use of European cybersecurity certification schemes
Article 25
Standardisation
Article 26
Jurisdiction and territoriality
Article 27
Registry of entities

implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

3. Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also

(d). If I am above the threshold to be qualified as EE, I need to comply. But those companies have connection with others, which might not be EE/IE. But the requirement for sec falls on the EE/IE. They will have to check to see if those links ensure the same level of security. The other actors will be indirectly imposed to comply with requirements. Can be for example contractually imposed or provide me info of your sec. level or provide a certification for the standard. The supplier will need to invest in security to collaborate with bigger companies.

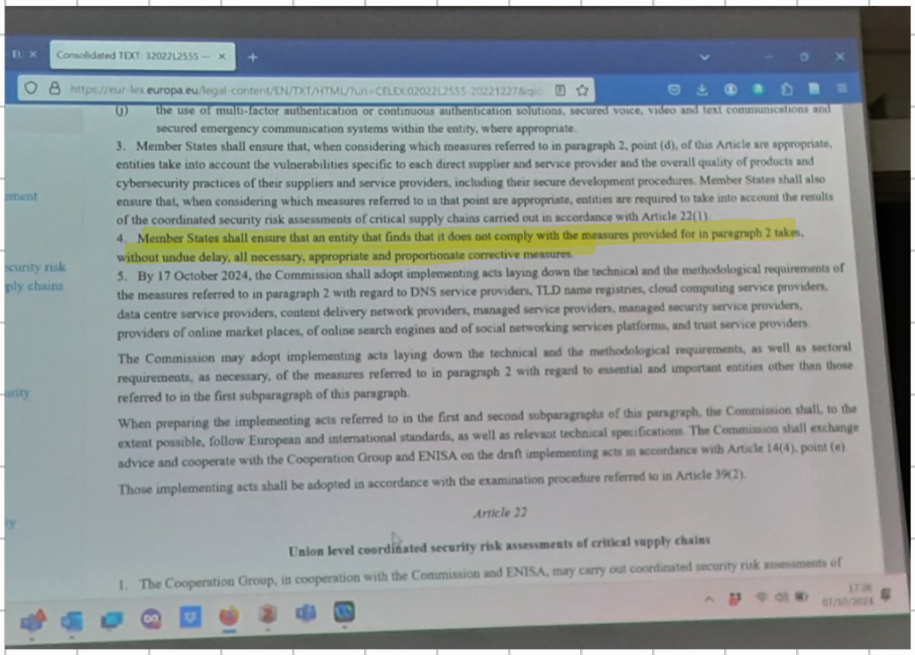
NOTE: in case there is an attack to supply chain that causes troubles to the EE, there is no obligation to report to the CSIRT. But I, company, will want to know of the problem so that in case I can voluntary notify the CSIRT.

(e): I have to check that elements I buy reflect my standard.

(8): Make employees know about cybersecurity.

* Organizational measures.

These are all applicable to EE/IE.



(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

3. Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

4. Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.

5. By 17 October 2024, the Commission shall adopt implementing acts laying down the technical and the methodological requirements of the measures referred to in paragraph 2 with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

The Commission may adopt implementing acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph.

When preparing the implementing acts referred to in the first and second subparagraphs of this paragraph, the Commission shall, to the extent possible, follow European and international standards, as well as relevant technical specifications. The Commission shall exchange advice and cooperate with the Cooperation Group and ENISA on the draft implementing acts in accordance with Article 14(4), point (e).

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

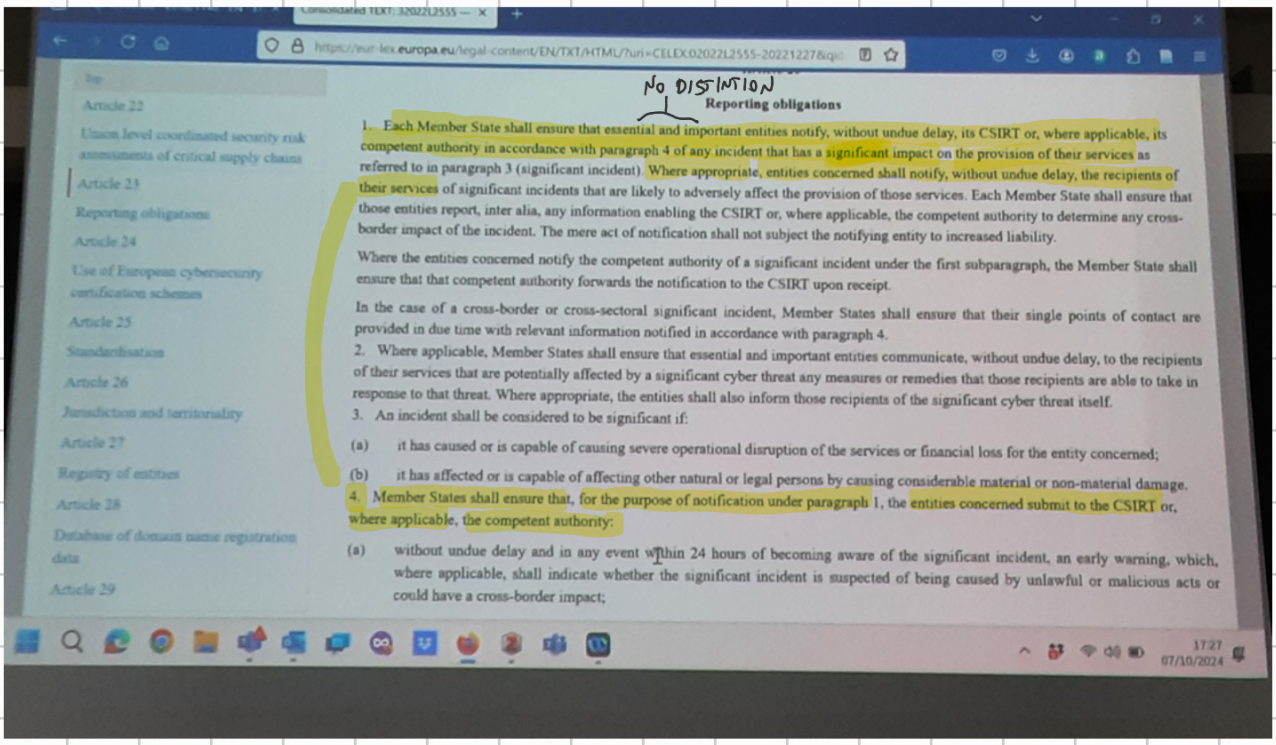
Article 22

Union level coordinated security risk assessments of critical supply chains

1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of

There will be sanctions.

REPORTING looks upon short and medium-long term perspective.



NO DISTINTION

Reporting obligations

1. Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability.

Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that that competent authority forwards the notification to the CSIRT upon receipt.

In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.

2. Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.

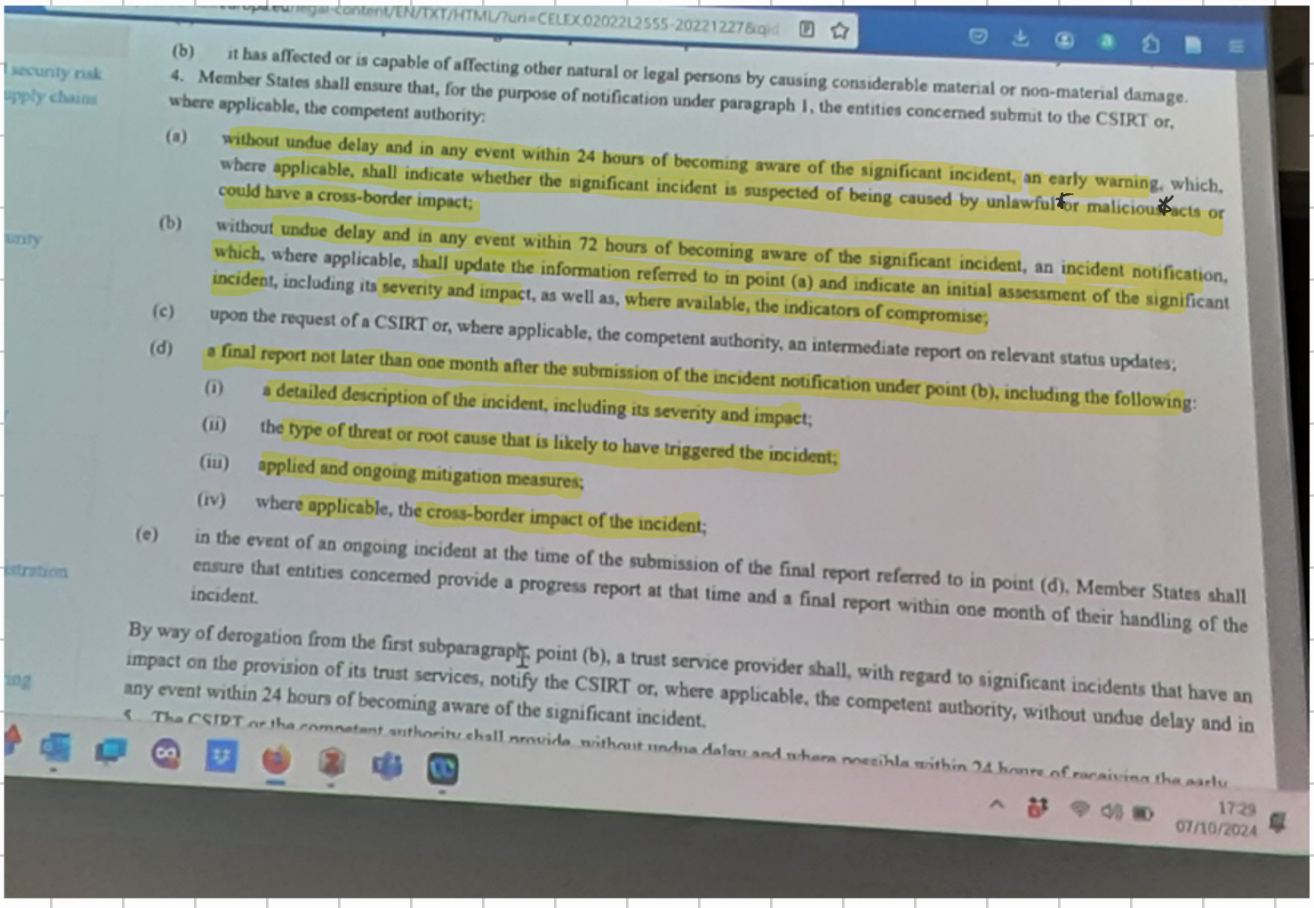
3. An incident shall be considered to be significant if:

(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;

(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:

(a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;



(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:

(a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

(b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;

(c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;

(d) a final report not later than one month after the submission of the incident notification under point (b), including the following:

(i) a detailed description of the incident, including its severity and impact;

(ii) the type of threat or root cause that is likely to have triggered the incident;

(iii) applied and ongoing mitigation measures;

(iv) where applicable, the cross-border impact of the incident;

(e) in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.

By way of derogation from the first subparagraph, point (b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the CSIRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of becoming aware of the significant incident.

5. The CSIRT or the competent authority shall provide, without undue delay and where possible within 24 hours of receiving the early

17:29
07/10/2024

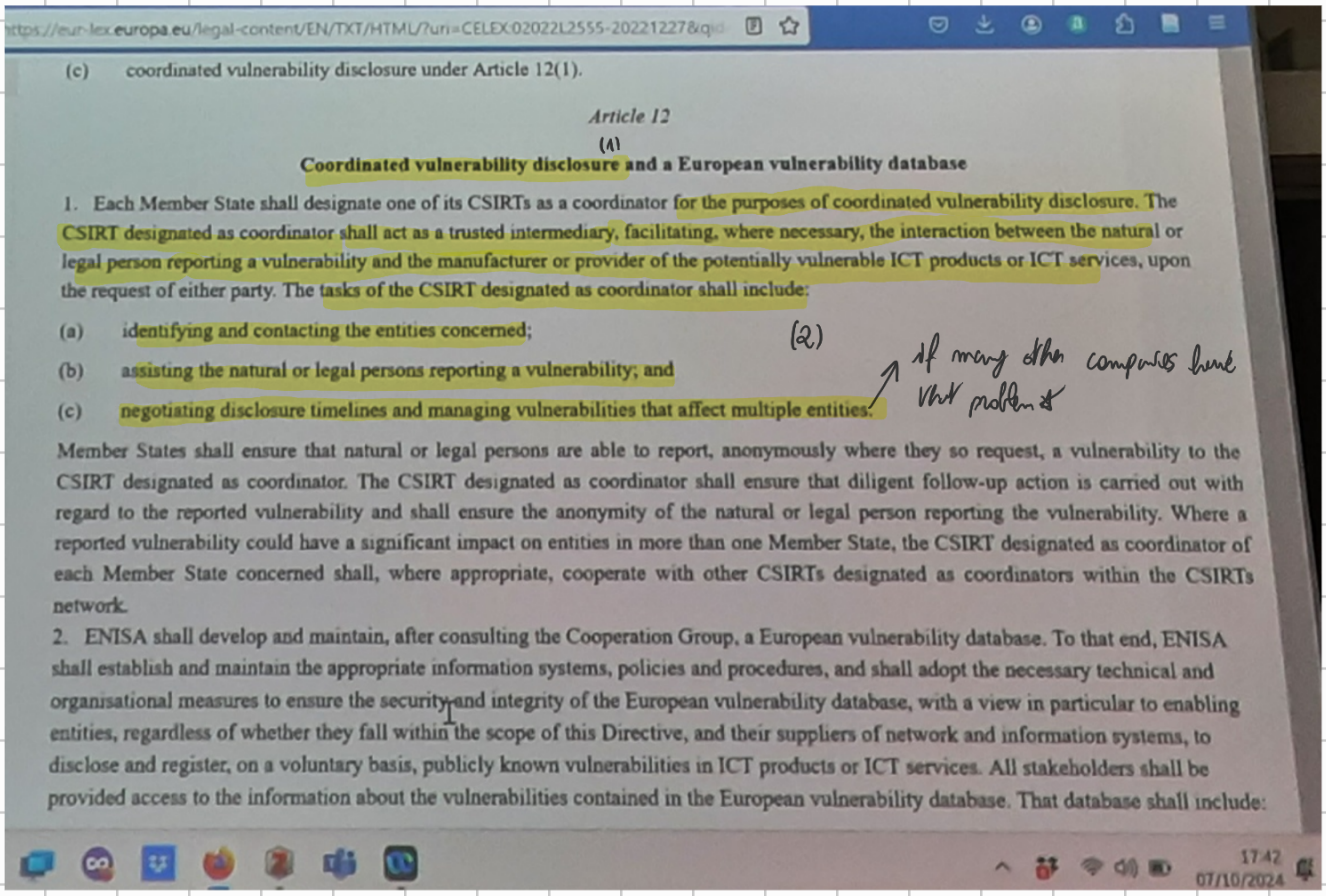
(a): I have a problem but I'm still checking. Just say that within 24 hours I need to notify an early warning. * Someone that is doing this on purpose.

(b): At 72 hours, 2nd notif: take into account what has happened if it is huge.

(d): 72 h + 1 month: final report. You should have tackled the issue in 1 month.

↳ Check the problem origination. What I did, (3), if they worked, if they didn't.

In NIS we stopped at (a), only. The long perspective is to learn from the mistakes: get the measures adopted by other companies. We learn from the incidents. Not just "looking at the emergency situation". Being able to have additional info (d) is getting knowledge for solution of the problem.



https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02022L2555-20221227&qid

(c) coordinated vulnerability disclosure under Article 12(1).

Article 12

(1)

Coordinated vulnerability disclosure and a European vulnerability database

1. Each Member State shall designate one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure. The CSIRT designated as coordinator shall act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party. The tasks of the CSIRT designated as coordinator shall include:

(a) identifying and contacting the entities concerned;

(2)

(b) assisting the natural or legal persons reporting a vulnerability; and

(c) negotiating disclosure timelines and managing vulnerabilities that affect multiple entities.

↑ if many other companies have that problem

Member States shall ensure that natural or legal persons are able to report, anonymously where they so request, a vulnerability to the CSIRT designated as coordinator. The CSIRT designated as coordinator shall ensure that diligent follow-up action is carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability. Where a reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT designated as coordinator of each Member State concerned shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.

2. ENISA shall develop and maintain, after consulting the Cooperation Group, a European vulnerability database. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures, and shall adopt the necessary technical and organisational measures to ensure the security and integrity of the European vulnerability database, with a view in particular to enabling entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, to disclose and register, on a voluntary basis, publicly known vulnerabilities in ICT products or ICT services. All stakeholders shall be provided access to the information about the vulnerabilities contained in the European vulnerability database. That database shall include:

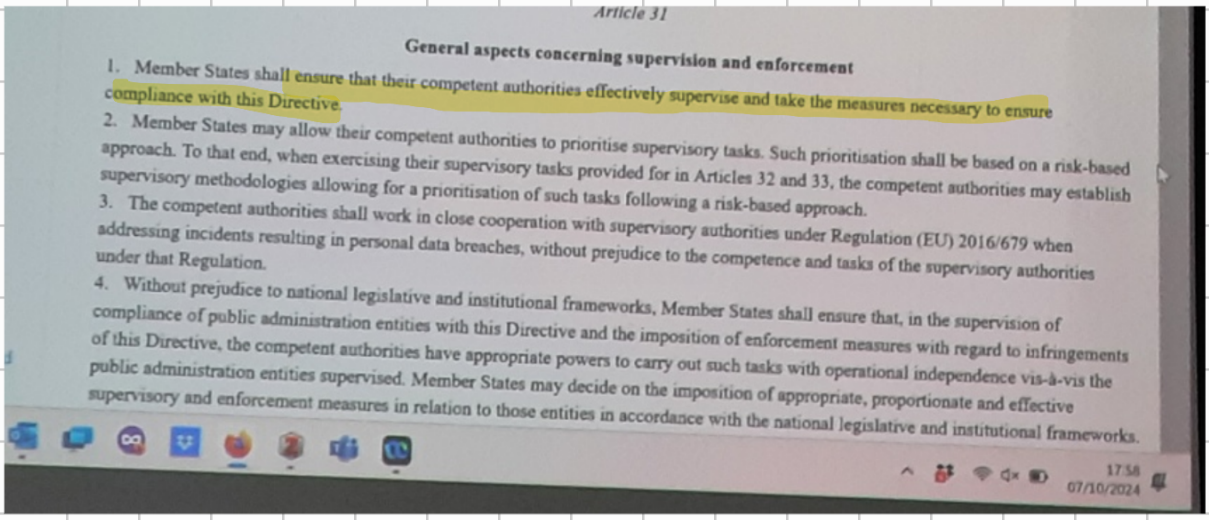
17:42
07/10/2024

(1) Addition of the NIS2: No obligation to inform. NoIFs is only about incidents of significant incidents. Vulnerability: there is a risk that an incident might happen. It's not a problem directly needed to be solved, but the intention of NIS 2 is to ensure prevention. The vulnerability can be there and at 1 point I know it. I am aware of the fact that this should be solved. In the period between detection and solution (mitigation at worst), I know about the problem. I know that I can have an issue and I have to react. But how to disclose? I can't do it in public. I have to handle a high level of secrecy and control. The CSIRT might have knowledge to help me. After solution this can become public knowledge by the CSIRT. Not immediate though; when the company has adapted the patch for the problem (and maybe the suppliers too) we can inform others. This is a way to prevent attacks through voluntary coordination.

(2) You can contact the CSIRT and be screened by being discovered by the vulnerable company. We want people who report to be protected (b).

* We use that to be better and improve.

Someone to check the compliance of the DIR.



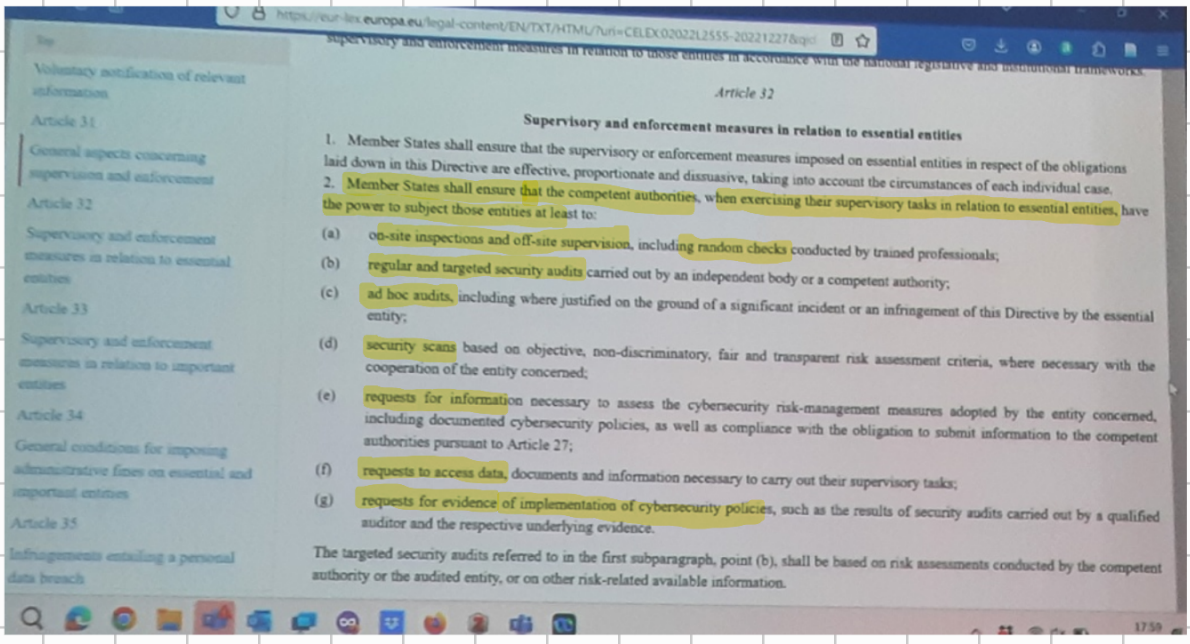
Article 31

General aspects concerning supervision and enforcement

1. Member States shall ensure that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive.
2. Member States may allow their competent authorities to prioritise supervisory tasks. Such prioritisation shall be based on a risk-based approach. To that end, when exercising their supervisory tasks provided for in Articles 32 and 33, the competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.
3. The competent authorities shall work in close cooperation with supervisory authorities under Regulation (EU) 2016/679 when addressing incidents resulting in personal data breaches, without prejudice to the competence and tasks of the supervisory authorities under that Regulation.
4. Without prejudice to national legislative and institutional frameworks, Member States shall ensure that, in the supervision of compliance of public administration entities with this Directive and the imposition of enforcement measures with regard to infringements of this Directive, the competent authorities have appropriate powers to carry out such tasks with operational independence vis-à-vis the public administration entities supervised. Member States may decide on the imposition of appropriate, proportionate and effective supervisory and enforcement measures in relation to those entities in accordance with the national legislative and institutional frameworks.

17:58
07/10/2024

32 for EE, 33 for IE par. 2.



Voluntary notification of relevant information
Article 31
General aspects concerning supervision and enforcement
Article 32
Supervisory and enforcement measures in relation to essential entities
Article 33
Supervisory and enforcement measures in relation to important entities
Article 34
General conditions for imposing administrative fines on essential and important entities
Article 35
Infringements entailing a personal data breach

Article 32

Supervisory and enforcement measures in relation to essential entities

1. Member States shall ensure that the supervisory or enforcement measures imposed on essential entities in respect of the obligations laid down in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.
2. Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to:

(a) on-site inspections and off-site supervision, including random checks conducted by trained professionals;

(b) regular and targeted security audits carried out by an independent body or a competent authority;

(c) ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity;

(d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned;

(e) requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;

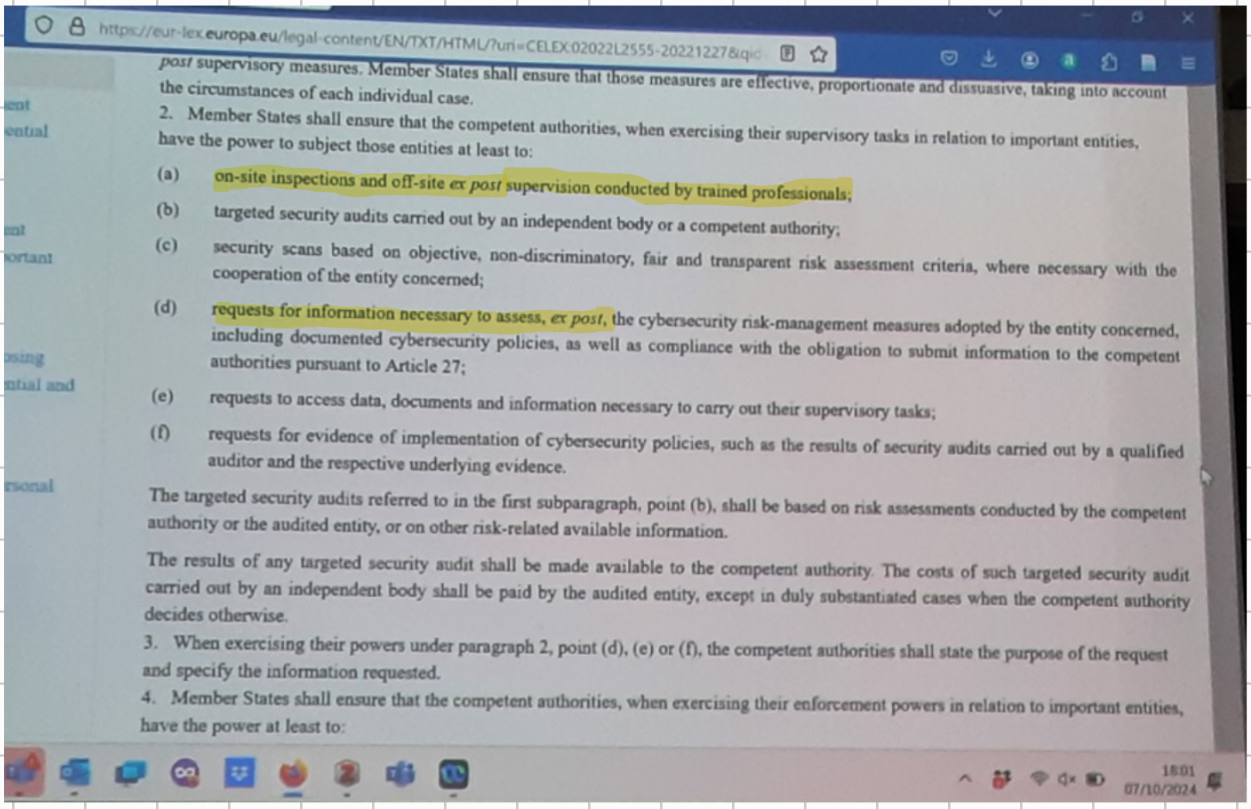
(f) requests to access data, documents and information necessary to carry out their supervisory tasks;

(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.

17:59

(2) Power to do something: they can be random check to ensure that sec. level is always high.



post supervisory measures. Member States shall ensure that those measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to:

(a) on-site inspections and off-site *ex post* supervision conducted by trained professionals;

(b) targeted security audits carried out by an independent body or a competent authority;

(c) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned;

(d) requests for information necessary to assess, *ex post*, the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;

(e) requests to access data, documents and information necessary to carry out their supervisory tasks;

(f) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.

The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.

3. When exercising their powers under paragraph 2, point (d), (e) or (f), the competent authorities shall state the purpose of the request and specify the information requested.

4. Member States shall ensure that the competent authorities, when exercising their enforcement powers in relation to important entities, have the power at least to:

For IE we need a trigger or an incident in order to get the controls. This is the only difference. The supervision authorities need a reason. For them I can check your work only if something happened. The distinction is only important for the fact that regardless of an incident I can check EE.

Security requirements

Article 21 Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

- (a) policies on risk analysis and information system security;
- (b) incident handling;
- (c) business continuity, such as backup management and disaster recovery, and crisis management;
- (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- (g) basic cyber hygiene practices and cybersecurity training;
- (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- (i) human resources security, access control policies and asset management;
- (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Notification of incidents

Article 23

Reporting obligations

1. Each Member State shall ensure that **essential and important entities notify, without undue delay, its CSIRT** or, where applicable, its competent authority in accordance with paragraph 4 **of any incident that has a significant impact on the provision of their services** as referred to in paragraph 3 (significant incident). Where appropriate**, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services**. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. **The mere act of notification shall not subject the notifying entity to increased liability**.

Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that that competent authority forwards the notification to the CSIRT upon receipt.

In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.

2. Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.

Notification of incidents

3. An incident shall be considered to be significant if:
   - (a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
   - (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:
   - (a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
   - (b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;
   - (c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;
   - (d) a final report not later than one month after the submission of the incident notification under point (b), including the following:
     - (i) a detailed description of the incident, including its severity and impact;
     - (ii) the type of threat or root cause that is likely to have triggered the incident;
     - (iii) applied and ongoing mitigation measures;
     - (iv) where applicable, the cross-border impact of the incident;
   - (e) in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.

By way of derogation from the first subparagraph, point (b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the CSIRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of becoming aware of the significant incident.

Supervision – essential entities

Article 32 Supervisory and enforcement measures in relation to essential entities

1. Member States shall ensure that the supervisory or enforcement measures imposed on essential entities in respect of the obligations laid down in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to:

- (a) **on-site inspections and off-site supervision**, including random checks conducted by trained professionals;
- (b) **regular and targeted security audits** carried out by an independent body or a competent authority;
- (c) **ad hoc audits**, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity;
- (d) **security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria**, where necessary with the cooperation of the entity concerned;
- (e) requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;
- (f) **requests to access data, documents and information necessary** to carry out their supervisory tasks;
- (g) **requests for evidence of implementation of cybersecurity policies**, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.

The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.

Supervision – important entities

Article 33 Supervisory and enforcement measures in relation to important entities

1. When provided with evidence, indication or information that an important entity allegedly does not comply with this Directive, in particular Articles 21 and 23 thereof, Member States shall ensure that the competent authorities take action, where necessary, through ex post supervisory measures. Member States shall ensure that those measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to:

- (a) on-site inspections and off-site ex post supervision conducted by trained professionals;
- (b) targeted security audits carried out by an independent body or a competent authority;
- (c) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned;
- (d) requests for information necessary to assess, ex post, the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;
- (e) requests to access data, documents and information necessary to carry out their supervisory tasks;
- (f) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.

The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.

Sanctions

Article 34 General conditions for imposing administrative fines on essential and important entities

1. Member States shall ensure that the administrative fines imposed on essential and important entities pursuant to this Article in respect of infringements of this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

Same. But:

2. Administrative fines shall be imposed in addition to any of the measures referred to in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g).

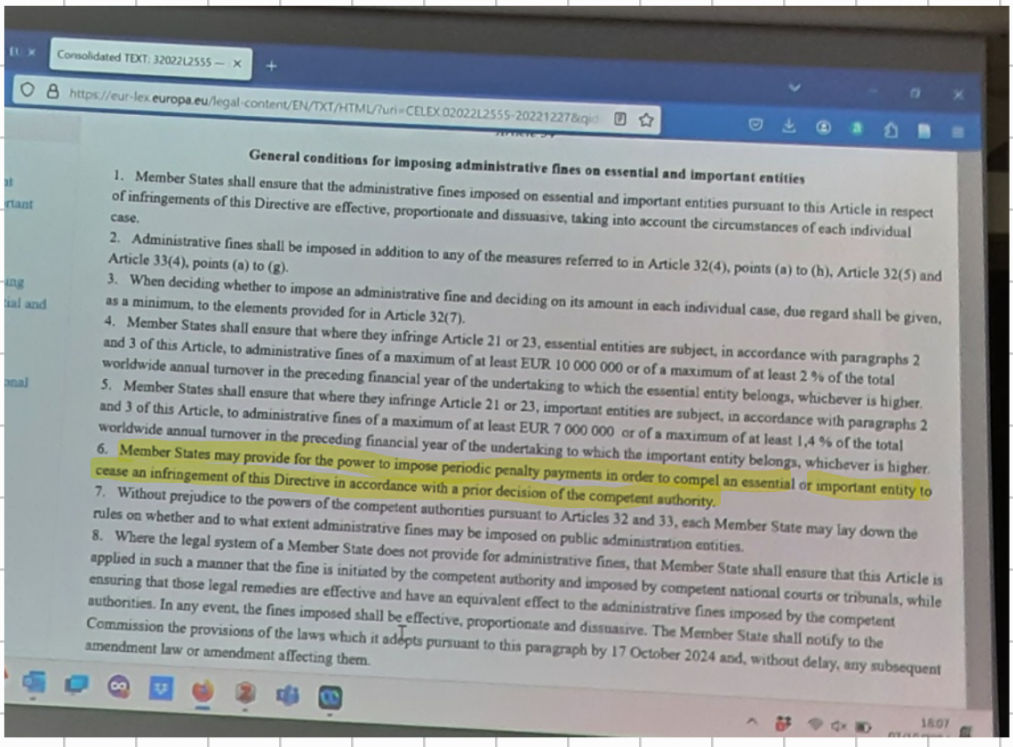
3. When deciding whether to impose an administrative fine and deciding on its amount in each individual case, due regard shall be given, as a minimum, to the elements provided for in Article 32(7).

4. Member States shall ensure that where they infringe Article 21 or 23, **essential entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover** in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.

5. Member States shall ensure that where they infringe Article 21 or 23, **important entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 7 000 000 or of a maximum of at least 1,4 % of the total worldwide annual turnover** in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.

2nd diff: sanctions are slightly smaller.

There is also the need to provide



We have a bit more. On NIS 1 we stopped at A.