Information and technology law course

LECTURE 4 – 5 / 3 – 7 OCTOBER 2023

FEDERICA CASAROSA – 2024/2025

NIS Directive

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

Art. 1(1)

- “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”.

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

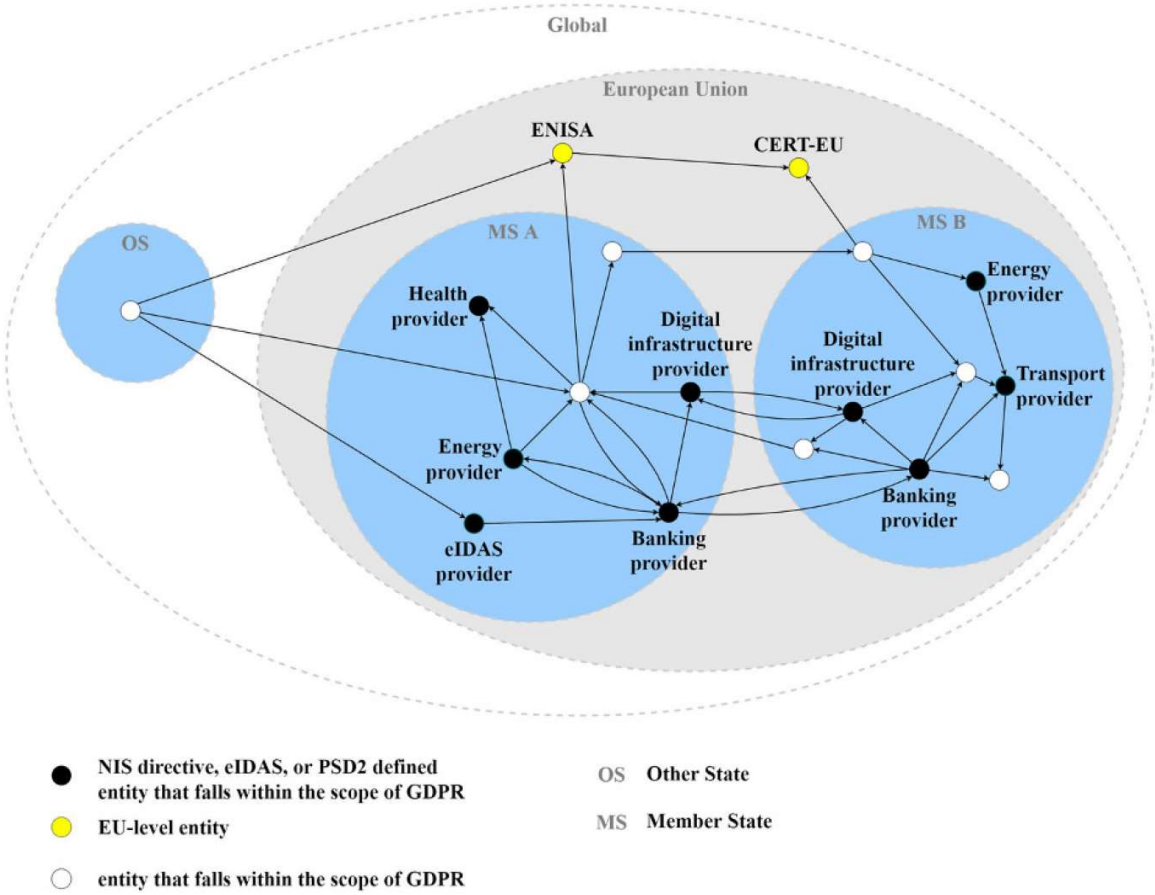


Fig. 2 Conceptualising a subset of stakeholders with hypothetical dependencies (source: own edit)

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;

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

(f) a risk assessment plan to identify risks;

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

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

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.

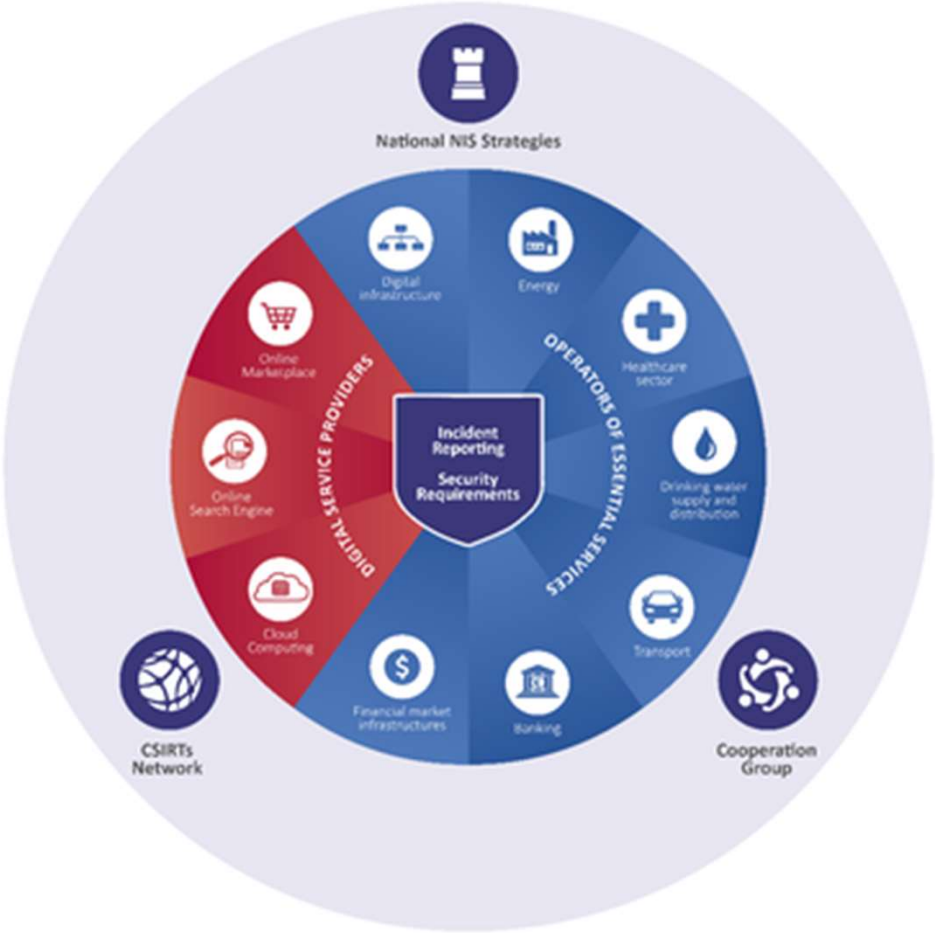
4. Member States shall inform the Commission about the remit, as well as the main elements of the incident-handling process, of their CSIRTs.

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

Target

Operators of essential services and

Digital service providers



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.

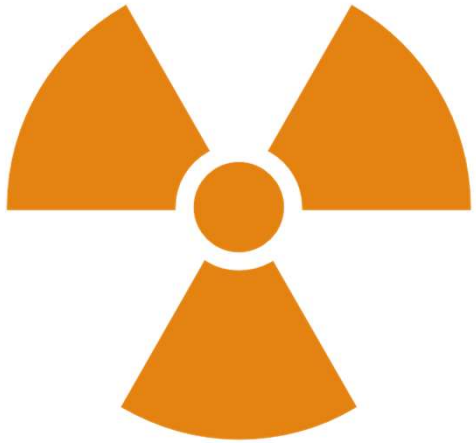
…

Critical incidents

Article 6 Significant disruptive effect

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;
- (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.



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.

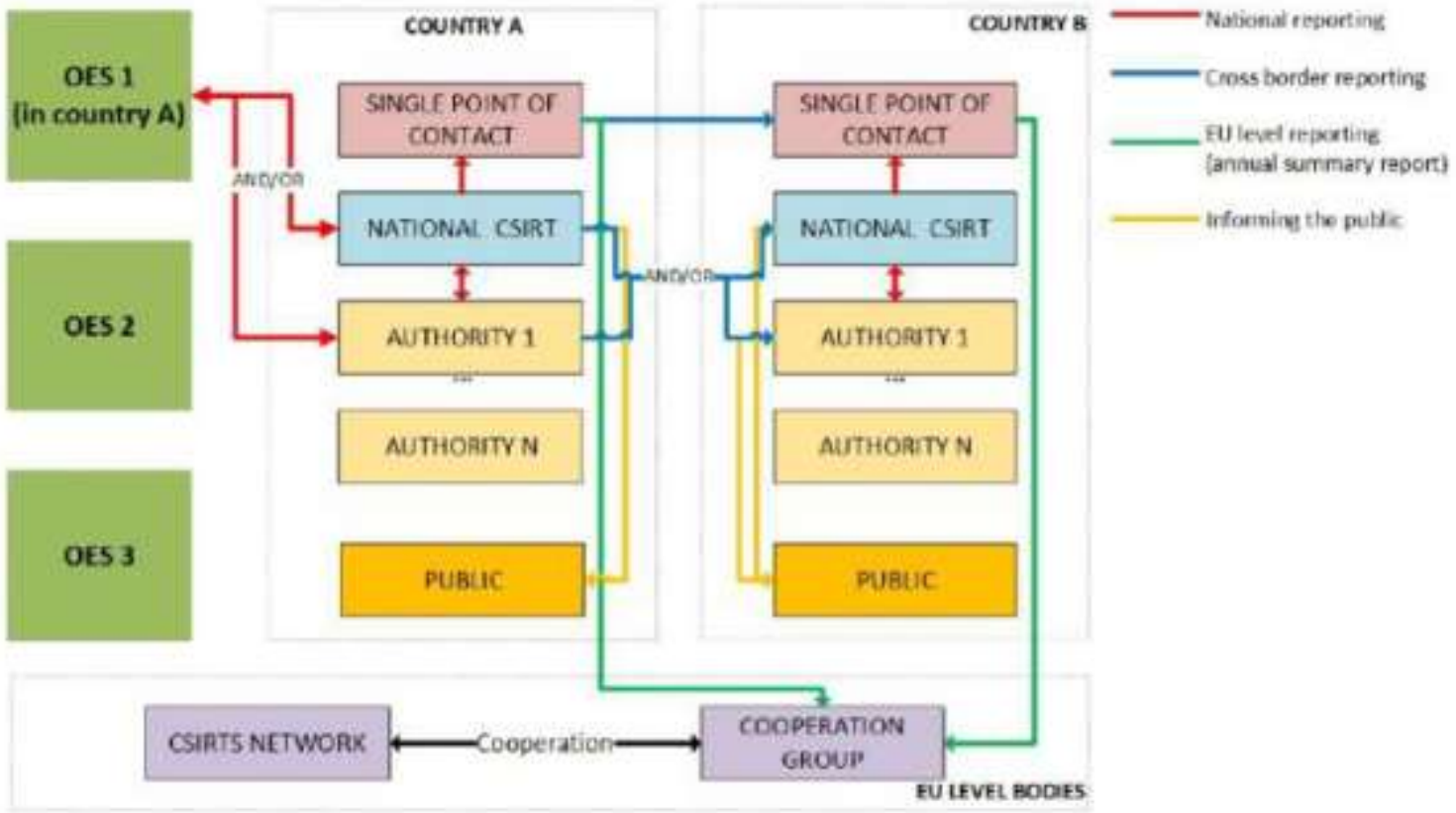
Incident notification – OSE

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.


COUNTRY A
COUNTRY B
OES 1
(in country A)
OES 2
OES 3
AND/OR
SINGLE POINT OF CONTACT
NATIONAL CSIRT
AUTHORITY 1
AUTHORITY N
PUBLIC
AND/OR
SINGLE POINT OF CONTACT
NATIONAL CSIRT
AUTHORITY 1
AUTHORITY N
PUBLIC
National reporting
Cross border reporting
EU level reporting
(annual summary report)
Informing the public
CSIRTS NETWORK
Cooperation
COOPERATION GROUP
EU LEVEL BODIES

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.

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.

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;

(d) monitoring, auditing and testing;

(e) compliance with international standards.

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

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;

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

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

(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.

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

Limited role of law enforcement authorities

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

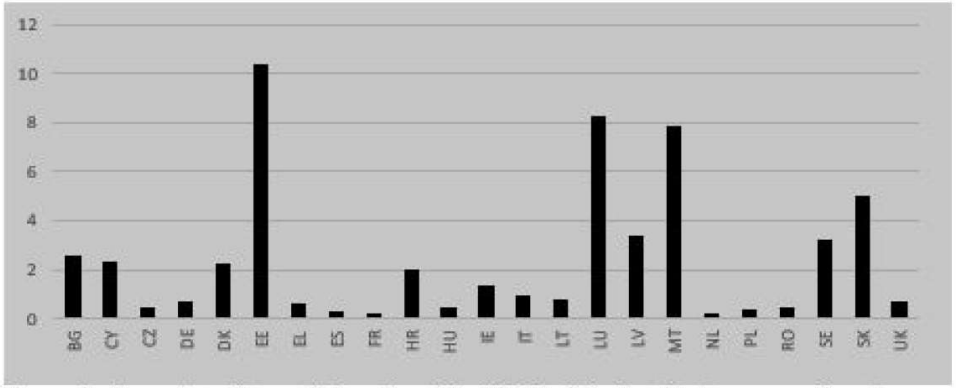


Figure 1: Operators of essential services identified by Member States across all sectors per 100 000 inhabitants[1]

Source: European Commission, 2020.

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

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

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**) – 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**	– **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**)

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.

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.