Legal Issues in Computer Security 2023
NIS (and NIS 2)

Mirosław Kutyłowski

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022
on measures for a high common level of cybersecurity across the Union,
amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972,
and repealing Directive (EU) 2016/1148 (**NIS 2 Directive**)

Changes effective since 2024, until this time: NIS Directive from 2016

Why important?

The cases like recent press articles on a factory in Bydgoszcz producing explosives

Goal: make it impossible to happen through cybersecurity obligations

NIS2 versus NIS:

1. management bodies of „essential entities” must approve cyberscurity risk management and are liable for infridgements

2. **members of the management bodies of essential and important entities are required to follow training,**

3. **state-of-the-art approach**

4. **all-hazards approach – an obligatory list of protection areas but understood as a minimal one**

5. **entities from outside EU – representatives in EU where activities take place**

Goals

… to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market.

In fact: minimal level of cybersecurity

Concrete measures

(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.

Scope

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.

Scope --- regardless of size:

(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;

Scope

(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.

Scope

3. Regardless of their size, this Directive applies to entities identified as critical entities under Directive (EU) 2022/2557. (gas, oil, heating, water,drinking water and waste water, transportation, banking, financial services, health, digital infrastructure, space services)

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

5. Member States may provide for this Directive to apply to:

(a) public administration entities at local level;

(b) education institutions, in particular where they carry out critical research activities.

does not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.

Member States may exempt specific entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in paragraph 7 of this Article, from the obligations laid down in Article 21 or 23 with regard to those activities or services.

The obligations laid down in this Directive **shall not entail the supply of information the disclosure of which would be contrary to the essential interests** of Member States' national security, public security or defence.

safeguards

Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities in accordance with this Directive only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of entities concerned.

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;

(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) …

Important entities

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.

List:

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.

Sector specific acts:

Where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VII, shall not apply to such entities.

Equivalence

… **shall be considered to be equivalent** in effect to the obligations laid down in this Directive where:

(a) cybersecurity risk-management measures are at least equivalent in effect to those laid down in Article 21(1) and (2); or

(b) the sector-specific Union legal act provides for immediate access, where appropriate automatic and direct, to the incident notifications by the CSIRTs, the competent authorities or the single points of contact under this Directive and where requirements to notify significant incidents are at least equivalent in effect to those laid down in Article 23(1) to (6) of this Directive.

Minimum harmonisation

This Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law.

Some definitions

‘**security of network and information systems**’ means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems;

‘national cybersecurity strategy ’ means a coherent framework of a Member State providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them in that Member State;

‘**near miss**’ means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise;

‘incident’ means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;

‘large-scale cybersecurity incident’ means an incident which causes a level of disruption that exceeds a Member State’s capacity to respond to it **or** which has a significant impact on at least two Member States;

‘risk’ means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

‘cyber threat’ means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881; -- **(on ENISA:** *any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons*;**)**

‘significant cyber threat’ means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity’s services by causing considerable material or non-material damage;

‘vulnerability’ means a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat;

‘domain name system’ or ‘DNS’ means a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources;

‘DNS service provider’ means an entity that provides:
(a)publicly available recursive domain name resolution services for internet end-users; or

(b)authoritative domain name resolution services for third-party use, with the exception of root name servers;

‘cloud computing service’ means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations;

‘**data centre service**’ means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control;

‘content delivery network’ means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;

‘social networking services platform’ means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations;

‘**public administration entity**’ means an entity recognised as such in a Member State in accordance with national law, not including the judiciary, parliaments or central banks, which complies with the following criteria:
(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;

(b) it has legal personality or is entitled by law to act on behalf of another entity with legal personality;

(c) it is financed, for the most part, by the State, regional authorities or by other bodies governed by public law, is subject to management supervision by those authorities or bodies, or has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities or by other bodies governed by public law;

(d)it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital;

‘entity’ means a natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;

‘**managed service provider**’ means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers’ premises or remotely;

‘**managed security service provider**’ means a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management;

‘**research organisation**’ means an entity which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions.

National cybersecurity strategy

Each Member State shall adopt a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include:

(a) objectives and priorities of the Member State's cybersecurity strategy covering in particular the sectors referred to in Annexes I and II;

(b) a governance framework to achieve the objectives and priorities referred to in point (a) of this paragraph, including the policies referred to in paragraph 2;

(c)a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level, underpinning the cooperation and coordination at the national level between the competent authorities, the single points of contact, and the CSIRTs under this Directive, as well as coordination and cooperation between those bodies and competent authorities under sector-specific Union legal acts;

(d) a mechanism to identify relevant assets and an assessment of the risks in that Member State;

(e) an identification of the measures ensuring preparedness for, responsiveness to and recovery from incidents, including cooperation between the public and private sectors;

(f) a list of the various authorities and stakeholders involved in the implementation of the national cybersecurity strategy;

(g) a policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2557 for the purpose of information sharing on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate;

(h) a plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens.

2. As part of the national cybersecurity strategy, Member States shall in particular adopt policies:

(a) addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services;

(b) on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products;

(c) managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under Article 12(1);

(d) related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables;

(e) promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures;

(f) promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities;

(g) supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure;

(h) including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in accordance with Union law;

(i) strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this Directive, by providing easily accessible guidance and assistance for their specific needs;

(j) promoting active cyber protection.

Competent authorities and single points of contact

1.
Each Member State shall designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VII (competent authorities).

3.
Each Member State shall designate or establish a single point of contact. Where a Member State designates or establishes only one competent authority pursuant to paragraph 1, that competent authority shall also be the single point of contact for that Member State.

National cyber crisis management frameworks

1.
Each Member State shall designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities). Member States shall ensure that those authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them. Member States shall ensure coherence with the existing frameworks for general national crisis management.

4.
Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan shall lay down, in particular:

(a) the objectives of national preparedness measures and activities;

(b) the tasks and responsibilities of the cyber crisis management authorities;

(c) the cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels;

(d) national preparedness measures, including exercises and training activities;

(e) the relevant public and private stakeholders and infrastructure involved;

(f) national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.

Computer security incident response teams (CSIRTs)

Each Member State shall designate or establish one or more CSIRTs. The CSIRTs may be designated or established within a competent authority.

The CSIRTs shall comply with the requirements set out in Article 11(1), shall cover at least the sectors, subsectors and types of entity referred to in Annexes I and II, and shall be responsible for incident handling in accordance with a well-defined process.

Poland: CSIRT NASK, CSIRT GOV, CSIRT MON

3.
Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholders. To that end, Member States shall ensure that each CSIRT contributes to the deployment of secure information-sharing tools.

7.
The CSIRTs may establish cooperation relationships with third countries' national computer security incident response teams. As part of such cooperation relationships, Member States shall facilitate effective, efficient and secure information exchange with those third countries' national computer security incident response teams, using relevant information-sharing protocols, including the traffic light protocol. The CSIRTs may exchange relevant information with third countries' national computer security incident response teams, including personal data in accordance with Union data protection law.
8.
The CSIRTs may cooperate with third countries' national computer security incident response teams or equivalent third-country bodies, in particular for the purpose of providing them with cybersecurity assistance.

1. The CSIRTs shall comply with the following requirements:

(a) the CSIRTs shall ensure a high level of availability of their communication channels by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times; they shall clearly specify the communication channels and make them known to constituency and cooperative partners;

(b) the CSIRTs' premises and the supporting information systems shall be located at secure sites;

(c) the CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular to facilitate effective and efficient handovers;

(d) the CSIRTs shall ensure the confidentiality and trustworthiness of their operations;

(e) the CSIRTs shall be adequately staffed to ensure availability of their services at all times and they shall ensure that their staff is trained appropriately;

(f) the CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of their services.

The CSIRTs may participate in international cooperation networks.

3. The CSIRTs shall have the following tasks:

(a) monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;

(b) providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;

(c) responding to incidents and providing assistance to the essential and important entities concerned, where applicable;

(d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;

(e) providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;

(f) participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;

(g) where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1);

(h) contributing to the deployment of secure information-sharing tools pursuant to Article 10(3).

The CSIRTs may carry out proactive non-intrusive scanning of publicly accessible network and information systems of essential and important entities. Such scanning shall be carried out to detect vulnerable or insecurely configured network and information systems and inform the entities concerned. Such scanning shall not have any negative impact on the functioning of the entities' services.

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;

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

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

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, …. 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:

(a) information describing the vulnerability;

(b) the affected ICT products or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited;

(c) the availability of related patches and, in the absence of available patches, guidance provided by the competent authorities or the CSIRTs addressed to users of vulnerable ICT products and ICT services as to how the risks resulting from disclosed vulnerabilities can be mitigated.

Cooperation at national level

1.
Where they are separate, the competent authorities, the single point of contact and the CSIRTs of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive.

Cooperation Group

1.
In order to support and facilitate strategic cooperation and the exchange of information among Member States, as well as to strengthen trust and confidence, a Cooperation Group is established.

2.
The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 7.

3.
The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) and the competent authorities under Regulation (EU) 2022/2554 may participate in the activities of the Cooperation Group in accordance with Article 47(1) of that Regulation.

CSIRTs network

1.
In order to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States, a network of national CSIRTs is established.
2.
The CSIRTs network shall be composed of representatives of the CSIRTs designated or established pursuant to Article 10 and the computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU). The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively provide assistance for the cooperation among the CSIRTs.

Governance

1. L

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.

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.L

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.

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 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.

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.

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.

Use of European cybersecurity certification schemes

1.

In order to demonstrate compliance with particular requirements of Article 21, Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. Furthermore, Member States shall encourage essential and important entities to use qualified trust services.

2.

The Commission is empowered to adopt delegated acts, in accordance with Article 38, to supplement this Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881. Those delegated acts shall be adopted where insufficient levels of cybersecurity have been identified and shall include an implementation period.

Standardisation

1.

In order to promote the convergent implementation of Article 21(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security of network and information systems..

Registry of entities

1.

ENISA shall create and maintain a registry of
DNS service providers,
TLD name registries,
entities providing domain name registration services,
cloud computing service providers,
data centre service providers,
content delivery network providers,
managed service providers,
managed security service providers,
as well as providers of online marketplaces,
of online search engines and of social networking services platforms,

on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to that registry, while ensuring that the confidentiality of information is protected where applicable.

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 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.

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

(a)
issue warnings about infringements of this Directive by the entities concerned;

(b)
adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or the infringements of this Directive;

(c)
order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct;

(d)
order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period;

(e)
order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat;

(f)
order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;

(g)
designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 21 and 23;

(h)
order the entities concerned to make public aspects of infringements of this Directive in a specified manner;

(i)
impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (h) of this paragraph.

…
If the requested action is not taken within the deadline set, Member States shall ensure that their competent authorities have the power to:

(a)
suspend temporarily, or request a certification or authorisation body, or a court or tribunal, in accordance with national law, to suspend temporarily a certification or authorisation concerning part or all of the relevant services provided or activities carried out by the essential entity;

(b)
request that the relevant bodies, courts or tribunals, in accordance with national law, prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising managerial functions in that entity.
.

Supervisory and enforcement measures in relation to important entities

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

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

~~(ad hoc audits)~~

(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;

Supervisory and enforcement measures in relation to important entities

(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.

Implementing Acts

European Commision

as specified by the Regulation

Reviewing mechanism

In 2027 and every 36 month