NISDUC

NIS Directive User Community

D3.4: NISDUC Lessons learnt – vol.3.5

Co-financed by the European Union

Connecting Europe Facility

Project acronym	NISDUC
Project title	NIS Directive User Community
Start date of the project	01/09/2020
Duration	36 months
Funding instrument	Connecting Europe Facility: Telecom (CEF Telecom)
Call for proposals	CEF-TC-2019-2 – Cybersecurity
Objective	Objective 4: Trans-European cooperation for effective joint cybersecurity operations and to build mutual trust/confidence
Agreement number	INEA/CEF/ICT/A2019/2072562
Action No	2019-EU-IA-0129

Deliverable type	Report
Deliverable reference number	D3.4 / V1.0
Activity contributing to the deliverable	Activity 3: Monitoring on the practices and experiences of the implementation of the NIS Directive
Due date	31/08/2023
Dissemination level	Public
Revision	V1.0

Contributors (ordered according to beneficiary numbers and alphabetical order of first names)

Hervé Cholez, Jocelyn Aubert, Nicolas Mayer (**LIST**)

Jacques Kellner, Sascha Maurer, Sheila Becker, Tim Mangold (**ILR**)

Nicolas Lempereur, Pierre-François Vandenhaute, Tim Masy (**BIPT-IBPT**)

Alexandre Dulaunoy, Gérard Wagener (**CIRCL.LU**)

Reviewers

Caroline Breure (**CCB**)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the authors’ views – the European Health and Digital Executive Agency (HaDEA) is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Table of contents

Lessons learnt from a collaborative approach involving Operators of Essential Services (OES), the National Competent Authority (NCA) and the Single Point of Contact (SPOC)

This section proposes best practices and experiences in the deployment of the NIS Directive based on a collaborative approach involving regulated entities (Operators of Essential Services (OES)) and regulation authorities (National Competent Authority (NCA) and the Single Point of Contact (SPOC)).

These practices refer to studies set up by, for Luxembourg, the **Institut Luxembourgeois de Régulation (ILR)**, the NIS identified SPOC, the NCA for the DSPs and for OES (except for banking and the financial market infrastructure), and, for Belgium, the **Belgian Institute for Postal services and Telecommunications (BIPT)**, the NIS sectoral authority for Digital Infrastructures in Belgium, both assisted by the **Luxembourg Institute of Science and Technology (LIST)**, a mission-driven Research and Technology Organization that develops advanced technologies and delivers innovative products and services to industry and society.

Overview of security regulations within the European Union

For several years now, the European Union has made security, protection against cybercrime and the protection of critical infrastructures one of its top priorities. To this end, EU has drawn on an ambitious legislative framework covering a broad spectrum of major economic entities, which in the event of malfunctioning could have disastrous consequences for the whole of Europe.

We offer here an overview of the NIS Directive, CER, the DORA regulations, GDPR, Cyber Solidarity Act, and Cyber Resilience Act. Indeed, the development of this legislative arsenal (whether these texts are published, in force, or still at the draft stage) can have a significant impact on potentially multi-regulated players.

NIS2 Directive (Network and Information Security, version 2)

The NIS2 Directive [1] aims to harmonize and strengthen cybersecurity across Europe, particularly in sectors heavily dependent on information and communication technologies. Published in the EU Official Journal on 14 December 2022, it must be transposed by Member States by 18 October 2024.

The Directive follows on from the NIS Directive [2], which was criticized for a lack of consistency between Member States and sectors, a low level of common knowledge of risks, and a lack of common response in the event of a crisis.

Target

The Directive covers 11 sectors of high criticality:

Energy		**Banking**
	Electricity	**Financial market infrastructures**
	District heating and cooling	**Health**
	Oil	**Drinking water**
	Gas	**Waste water**
	Hydrogen	**Digital infrastructures**
Transport		**ICT service management (business-to-business)**
	Air	**Public administration**
	Rail	**Space**

	Water
	Road

And 7 other critical sectors:

Postal and courier services		**Digital providers**
Waste management		**Research**
Manufacture, production, and distribution of chemicals		
Production, processing, and distribution of food		
Manufacturing		
	Manufacture of medical devices and in vitro diagnostic medical devices	
	Manufacture of computer, electronic and optical products	
	Manufacture of electrical equipment	
	Manufacture of machinery and equipment n.e.c.	
	Manufacture of motor vehicles, trailers, and semi-trailers	
	Manufacture of other transport equipment	

An essential or important entity is any public or private entity providing its services or carrying out its activity within the European Union, in one of the sectors referred to (see list above), and falling within one of the following cases:

- 50 or more employees or annual sales of 10 million euros or more.

or regardless of size:

- Designated as a critical entity within the meaning of CER Directive [3].
- Providing a public electronic communications network service, a publicly available electronic communications service, a trust service, a top-level domain name registry service, a domain name system service, or a domain name registration service.
- A public administration entity of central government or a public entity at regional level that provides services whose disruption could have a significant impact on critical societal or economic activities.
- In a context of risks identified at national level:
  - An entity that is essential to the maintenance of critical societal or economic activities.
  - An entity providing a service whose disruption could have a significant impact on public security, public safety, or public health.
  - An entity providing a service whose disruption could lead to significant systemic risk.
  - An entity of specific national or regional importance.

The table below summarizes the criteria, based on a Commission recommendation [4]:

Size of the entity	**Number of employees**	**Turnover (M€)**	**Annual balance sheet (M€)**	**High criticality sectors**	**Other critical sectors**
Intermediate and large	More than 250	More than 50	More than 43	Essential entity	Important entity
Medium	50-250	10-50	10-43	Important entity	Important entity
Micro and small	Less than 50	Less than 10	Less than 10	Not by default	Not by default

In cases where an entity does not fall under essential or important entity by default, Member States have specific criteria to determine if an entity is nevertheless essential or important (e.g., monopoly situation, essential cross-border service, particularly critical service, etc.).

Obligations

The NIS2 Directive lays down minimum rules for cyber security risk management. Each Member State is free to specify or add to these requirements (see national transpositions). Essential and important entities are all subject to the same rules; only the supervision regime (see Control and supervision section) varies.

The Directive requires entities to adopt a risk approach (all-hazards approach), and to put in place technical, operational, and organisational measures tailored to their degree of exposure to risk, their size, the likelihood and severity of incidents, and their societal and economic consequences. These measures address the following cybersecurity domains:

- Policies on risk analysis and information system security.
- Incident handling.
- Business continuity, such as backup management and disaster recovery, and crisis management.
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.
- Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure.
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.
- Basic cyber hygiene practices and cybersecurity training.
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption.
- Human resources security, access control policies and asset management.
- 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.

Entities are also required to report significant cyber security incidents to the competent authorities (CSIRT, national authority) without undue delay and no later than 24 hours after their discovery. As stated in Art. 23(3), an incident is considered significant if:

- *It has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned.*
- *It has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.*

This notification must be made in three stages:

- an **initial report** without undue delay or within 24 hours of discovery.
- a **detailed report** without undue delay and within 72 hours of discovery, and
- a **final report** within one month of the incident.

Lastly, the Directive requires entities' management bodies to approve risk management measures and supervise their implementation, with liability in the event of a breach of the Directive.

Control and supervision

The Directive gives national authorities enhanced supervisory powers, enabling them to carry out regular, targeted audits, on-site and off-site inspections, and to issue requests for information and access to documents or evidence.

The Directive provides for two types of control:

- *ex ante*, in the absence of security incidents
- *ex post*, following a security incident or because of evidence or indications.

An essential entity may be subject to both types of control, whereas an important entity may only be subject to *ex post* controls.

Sanctions

National authorities may issue warnings to audited entities that do not comply with the Directive, in particular, they may:

- issue warnings about infringements of the Directive by the entities concerned.
- adopt binding instructions or an order requiring the entities concerned to remedy the deficiencies identified or the infringement of the Directive.
- order the entities concerned to cease conduct that infringes the Directive and desist from repeating that conduct.
- order the entities concerned to ensure that their cybersecurity risk-management measures comply with the Directive or to fulfil the reporting obligations, in a specified manner and within a specified period.
- order the entities concerned to inform the persons regarding 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.
- order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline.
- order the entities concerned to make public aspects of infringements of the Directive in a specified manner.

Where an essential entity fails to take the necessary measures to remedy deficiencies or to comply with requirements, the national authorities may:

- temporarily suspend a certification or authorisation concerning all or part of the relevant services provided.
- issue a temporary ban on the exercise of management functions.

The Directive also imposes, in the event of non-compliance with these directives, a system of administrative penalties, common to all Member States, providing for at least:

- **for an essential entity:** a maximum fine of €10 million or 2% of annual worldwide turnover.
- **for an important entity:** a maximum fine of €7 million or 1.4% of annual worldwide turnover.

Directive on the resilience of critical entities (CER)

The Critical Entities Resilience Directive (CER) [3] aims to strengthen the resilience of critical infrastructure by defining a general framework that considers all risks, whether natural, human-made, accidental, or intentional. Published in the EU Official Journal on 16 January 2023, it must be transposed by Member States by 17 October 2024.

The Directive repeals and extends the 2008 European Critical Infrastructure Directive [5], by introducing new obligations and extending the covered sectors.

Target

Whereas the previous Critical Infrastructure Directive focused solely on the energy and transport sectors, the CER Directive is now aligned with the NIS2 Directive [1], and now covers 11 sectors, considering all critical entities as providers of essential services.

Energy		**Banking**
	Electricity	**Financial market infrastructures**
	District heating and cooling	**Health**
	Oil	**Drinking water**
	Gas	**Waste water**
	Hydrogen	**Digital infrastructures**
Transport		**Public administration**
	Air	**Space**
	Rail	**Production, processing, and distribution of food**
	Water	
	Road	
	Public transport	

The Directive applies to any public or private entity that:

- provides one or more essential services in one of the sectors referred to (see list above).
- operates and has its critical infrastructure located in the European Union.
- whose incident would have a significant disruptive effect on the provision of essential services.
- has been identified by a Member State.

As explained in NIS2 Directive section, entities falling within the scope of the NIS Directive are considered as entities providing essential services.

Obligations

The CER Directive requires a broad spectrum of risks to be considered. Given the complementarity nature of NIS2 and CER Directives, their coordinated implementation, challenges relating to the points of attention covered by NIS2 Directive are effectively excluded from the scope of the CER Directive.

The Directive requires entities to take technical, security and organisational measures to ensure their resilience, including measures necessary to:

- prevent incidents from occurring, duly considering disaster risk reduction and climate adaptation measures.
- ensure adequate physical protection of their premises and critical infrastructure, duly considering, for example, fencing, barriers, perimeter monitoring tools and routines, detection equipment and access controls.

- respond to, resist, and mitigate the consequences of incidents, duly considering the implementation of risk and crisis management procedures and protocols and alert routines.
- recover from incidents, duly considering business continuity measures and the identification of alternative supply chains, to resume the provision of the essential service.
- ensure adequate employee security management, duly considering measures such as setting out categories of personnel who exercise critical functions, establishing access rights to premises, critical infrastructure, and sensitive information, setting up procedures for background checks and designating the categories of persons who are required to undergo such background checks, and laying down appropriate training requirements and qualifications.
- raise awareness about the measures among relevant personnel, duly considering training courses, information materials and exercises.

In this sense, the Directive requires entities to carry out risk assessment at least every four years, to assess all relevant risks that could lead to an interruption of provision of essential services. In parallel, each Member State is itself required to carry out a national risk analysis, considering relevant natural and man-made risks, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid or other conflicting threats, including terrorist offenses.

Entities are also required to notify the competent authority without undue delay and no later than 24 hours after their discovery, of incidents that significantly disrupt or have the potential to significantly disrupt the provision of essential services. As stated in Art. 15(1), the following parameters should be considered, to determine the significance of a disruption:

- *the number and proportion of users affected by the disruption.*
- *the duration of the disruption.*
- *the geographical area affected by the disruption, taking into account whether the area is geographically isolated.*

This notification must be made in two stages:

- an **initial notification** without undue delay or within 24 hours of discovery.
- a **detailed report** no later than one month thereafter.

Lastly, Member States must adopt a strategy for enhancing the resilience of critical entities. This strategy aims to strengthen the ability of critical entities to prepare for, cope with, protect against, respond to, and recover from incidents that could disrupt the provision of essential services.

Control and supervision

The Directive gives national authorities powers and means to:

- conduct on-site inspections of the critical infrastructure and the premises that the critical entity uses to provide its essential services, and off-site supervision of measures taken by critical entities.
- conduct or order audits in respect of critical entities.
- assess whether the measures taken by the entities to ensure their resilience meet the requirements set out in the Directive.
- access any evidence of the effective implementation of those measures, including the results of an audit conducted by an independent and qualified auditor selected by that entity and conducted at its expense.

- order the critical entities concerned to take the necessary and proportionate measures to remedy any identified infringement of the Directive, within a reasonable time limit set by those authorities, and to provide those authorities with information on the measures taken.

Sanctions

The Directive does not lay down a system of penalties applicable to breaches of the measures but leaves it up to the Member States to determine effective, proportionate, and dissuasive penalties.

Regulation on digital operational resilience for the financial sector (DORA)

The Digital Operational Resilience Act [6] provides a detailed and comprehensive framework on digital operational resilience for financial entities. It obliges European financial players to take a series of measures to guarantee the continuity of their services and, more broadly, their digital resilience, while introducing a direct monitoring mechanism for critical ICT service providers at EU level. Published in the EU Official Journal on 14 December 2022, it will come into force in 17 January 2025.

It is important to note that DORA represents *lex specialis* for NIS2, which means that entities under DORA do not need to comply also specifically for NIS2, but that compliance under DORA is considered being compliant under NIS2.

Target

The DORA regulation applies to a very wide range of financial entities in the financial sector, including:

- credit institutions.
- payment institutions.
- electronic money institutions.
- investment firms.
- crypto-asset service providers.
- central securities depositories.
- central counterparties.
- trading venues.
- trade repositories.
- management companies.
- data reporting service providers.
- insurance intermediaries, reinsurance intermediaries, and ancillary insurance intermediaries (large enterprises).
- institutions for occupational retirement provision.
- credit rating agencies.
- administrators of critical benchmarks.
- crowdfunding service providers.
- securitisation repositories.

as well as ICT third-party service providers, operating within the European Union in financial services.

Obligations

The regulation establishes 5 essential pillars of digital operational resilience, proposing various requirements that financial institutions must implement:

ICT risk management framework

Financial entities must have a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risks quickly, efficiently, and comprehensively and to ensure a high level of digital operational resilience.

ICT-related incident management and reporting

Financial entities shall define, establish, and implement an ICT-related incident management process to detect, manage and notify ICT-related incident.

All ICT incident and significant cyber threats must be recorded, classified, and assessed based on the following criteria:

- the number and/or relevance of clients or financial counterparts affected and, where applicable, the amount or number of transactions affected by the ICT-related incident, and whether the ICT-related incident has caused reputational impact.
- the duration of the ICT-related incident, including the service downtime.
- the geographical spread regarding the areas affected by the ICT-related incident, particularly if it affects more than two Member States.
- the data losses that the ICT-related incident entails, in relation to availability, authenticity, integrity or confidentiality of data.
- the criticality of the services affected, including the financial entity's transactions and operations.
- the economic impact, in particular direct and indirect costs, and losses, of the ICT-related incident in both absolute and relative terms.

Major ICT incidents should be reported to the competent authority within a timeframe and using a common template, both to be specified.

This notification will take place in three stages:

- an **initial notification**.
- an **intermediate report** after the initial notification, as soon as the status of the original incident has changed significantly or the handling of the major ICT-related incident has changed based on new information available, followed, as appropriate, by updated notifications every time status update is available, as well as upon a specific request of the competent authority.
- a **final report**, when the root cause analysis has been completed, regardless of whether mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates.

Financial entities will also be able to report significant cyber threats on a voluntary basis.

Digital operational resilience testing

Financial entities, other than microenterprises should establish, maintain, and regularly review a digital operational resilience testing program as an integral part of their ICT risk management framework.

This digital operational resilience testing program should:

- include a wide range of assessments, tests, methodologies, practices, and tools to be applied.
- cover tools and ICT systems, and at least once a year, all systems and tools supporting critical or important functions.
- ensure testing is conducted by internal or external independent parties.
- include procedures and strategies for prioritizing, classifying, and resolving all issues identified during testing.
- define review and validation procedures for the implementation of remediation plans.

Furthermore, large, and cyber-mature financial entities shall carry out at least every 3 years advanced testing by means of threat-led penetration testing (TLPT)[1].

ICT third-party risk management

The regulation requires entities to consider and manage the risks associated with third-party ICT service providers, meaning managing ICT third-party risks as an integral components of ICT risk within their ICT risk management framework. To this end, a set of key principles is defined, including:

- adoption and maintenance of a strategy on ICT third-party risk, that include a policy on the use of ICT services for critical or important functions provided by ICT third-party service providers.
- maintenance and update a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.
- conduction of due diligence and assessment on prospective ICT third-party service providers before entering a relationship.
- inclusion in contractual arrangements of clauses enabling termination of the relationship in the event of ICT third-party service provider default (e.g., significant breach by the provider of applicable laws, regulations or contractual terms, evidenced weakness pertaining to the overall ICT risk management of the provider, etc.).
- definition of exit strategies and plans considering risks that emerge at the level of ICT third-party providers, in particular a possible failure on their part, a deterioration of the quality of the services provided, any business disruption, or the termination of contractual arrangements.
- continuous monitoring of the relationship.

Cybersecurity information sharing

The regulation suggests financial entities to exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cybersecurity alerts and configuration tools.

Control and supervision

The regulation gives competent authorities powers and means to:

- have access to any document or data held in any form that it considers relevant to the performance of its duties and receive or take a copy of it.
- carry out on-site inspections or investigations.
- require corrective and remedial measures for breaches of the requirements.

Sanctions

The regulation does not lay down a system of penalties but leaves it up to the Member States to adopt any type of measure, including financial measures to ensure that financial entities to comply with their legal obligations.

[1] "*a framework that mimics the tactics, techniques and procedures of real- life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems*". Art.3 (17).

Critical ICT service providers may also be subject to sanctions for non-compliance, including financial penalties and daily penalty payments amounting to a maximum of 1% of the worldwide sales of the ICT service provider concerned, for a total period of up to 6 months.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) [7] frames data processing equally throughout the European Union. It updates and modernises the principles of the 1995 Data Protection Directive [8]. Coming into force on May 25, 2018, it is the reference text for the protection of personal data and is designed around three objectives:

- strengthening people's rights.
- make data processors more accountable.
- give credibility to regulation through enhanced cooperation between data protection authorities.

Target

The GDPR is aimed at any private or public structure that collects and/or processes data, regardless of its sector of activity or size. The regulation applies to all organisations established on the territory of the European Union, but also to any organisation established outside the European Union, but whose activity directly targets European residents.

The regulation also concerns subcontractors who would process or collect personal data on behalf of another entity.

Obligations

The regulation imposes a series of obligation on data controllers, including:

- provide data subjects with general information on the processing of personal data, including the identity of the data controller and potential subcontractors, the purpose of data processing, the mandatory or optional nature of responses, their rights, any data transmission, the use of browsing data (cookie).
- obtain clear and informed consents from data subjects at the time of data collection.
- guarantee data subject’s rights: right to access, right to correction, right to erasure, right to restriction of processing, right to data portability, right to object to processing, right to not be subject to automated decision making.
- implement appropriate measures to ensure optimal security and confidentiality of personal data (e.g., pseudonymization, impact analysis, penetration tests, etc.).
- maintain and regularly update a data processing register.
- in certain cases, appoint a Data Protection Officer (DPO).
- internally document personal data breaches and notify breaches presenting a risk to the rights and freedoms of individuals to the competent authority, and in certain cases where the risk is high, to the individuals concerned. These notifications must be notified without undue delay and, where feasible, not later than 72 hours after the discovery.

Control and supervision

The competent authority is responsible for monitoring the application of the regulation, to protect the fundamentals rights and freedoms of natural persons regarding processing and to facilitate the free flow of personal data within the European Union. To this end, the competent authority has an arsenal of investigative, corrective, authorisation, and advisory powers at its disposal, including:

- **Investigative powers:**
    - to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks.
    - to carry out investigations in the form of data protection audits.
    - to carry out a review on certifications issued.
    - to notify the controller or the processor of an alleged infringement of the regulation.
    - to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks.
    - to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.
- **Corrective powers:**
    - to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of the regulation.
    - to issue reprimands to a controller or a processor where processing operations have infringed provisions of the regulation
    - to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to the regulation.
    - to order the controller or processor to bring processing operations into compliance with the provisions of the regulation, where appropriate, in a specified manner and within a specified period.
    - to order the controller to communicate a personal data breach to the data subject.
    - to impose a temporary or definitive limitation including a ban on processing.
    - to order the rectification or erasure of personal data or restriction of processing and the notification of such actions to recipients to whom the personal data have been disclosed.
    - to withdraw a certification or to order the certification body to withdraw a certification issued, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met.
    - to impose an administrative fine, in addition to, or instead of measures, depending on the circumstances of each individual case.
    - to order the suspension of data flows to a recipient in a third country or to an international organisation.
- **Advisory powers:**
    - to advise the controller in accordance with a prior consultation procedure.
    - to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data.
    - to authorise a processing if the law of the Member State requires such prior authorisation.
    - to issue an opinion and approve draft codes of conduct.
    - to accredit certification bodies.
    - to issue certifications and approve criteria of certification.
    - to adopt standard data protection clauses.
    - to authorise contractual clauses.
    - to authorise administrative arrangements.

  - to approve binding corporate rules.

Sanctions

When breaches of the regulation or the national law are brought to its attentions, the competent authority may:

- issue a call to order.
- enjoin compliance with the law, including under penalty.
- temporarily or definitively restrict processing.
- suspend data flows.
- order compliance with requests to exercise individual rights, including under penalty.
- impose an administrative fine of up to 20 million euros, or in the case of a company, up to 4% of worldwide annual sales.

Cyber Solidarity Act

The EU Cyber Solidarity Act [9] is a proposal for a regulation of the European Commission which aims to strengthen the EU's solidarity and increase the capacities to prepare, detect and respond to cybersecurity threats and incidents. This section is based on the first draft of the proposal published on 18th April 2023, so the content is still up for changes under the negotiations on EU-level.

The Cyber Solidarity Act tries to achieve its goals by introducing:

- A European Cyber Shield
- A Cyber Emergency Mechanism
- A Cybersecurity Incident Review Mechanism

The actions proposed under the Cyber solidarity act are strongly linked to existing legislations at Union level such as the NIS2 Directive or the Cybersecurity Act.

Target

The Cyber Solidarity Act mainly targets **public authorities** of the Member States to coordinate the different actions between Member States. In particular, it targets:

- National authorities:
  - Single Point of Contact according to the NIS2 Directive [1]
  - National Security Operations Centres (National SOCs)
  - National cyber crisis management authorities / CSIRTs
- International authorities:
  - Cross-border SOCs
  - ENISA
  - EU-CyCLONe

Private entities operating in highly critical sectors (as defined in NIS2 Directive [1]) across the Union are as well targeted by the Regulation as such that they may participate in a coordinated preparedness testing exercise for entities. This includes enterprises from the following sectors:

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health

- Drinking water
- Digital infrastructures
- ICT service management (business-to-business)
- Public administration
- Space

Trusted providers or managed security service providers as defined by NIS2 Directive [1] are another group targeted by the regulation to support the public and private entities in case of a cyber emergency.

Obligations

Establishment of the European Cyber Shield, which will consist of all National SOCs and Cross-border SOCS.

- National SOCs need to be designated by each Member State.
- Cross-border SOCs may be created when a "*Hosting Consortium*" of at least 3 Member States represented by their National SOC(s) express their interest in working together to establish a Cross-border SOC.
- Cross-border SOCs need to cooperate and exchange relevant information relating to cyber security (threats, vulnerabilities, alerts, recommendations…) to help preventing, detecting, responding, and recovering from incidents or limiting their impact.
  A high level of interoperability needs to be guaranteed between Cross-border SOCs to fully profit from the information exchange. Cross-border SOCs furthermore have the obligation to share their information with Union entities such as the EU-CyCLONe, CSIRTs network and the Commission.
- Member States participating in the European Cybershield need to ensure that sufficient data and physical security measures are implemented to avoid a negative impact on the security interests of the European Union.

Establishment of the Cyber Emergency Mechanism by funding from DEP (Digital Europe Programme) to improve the European Union's resilience against cyber threats.

- The European Commission should identify relevant sectors from the list of highly critical sectors as defined by Annex I of NIS2 Directive [1] that should undergo the coordinated preparedness testing at EU Level.
- The NIS-Cooperation Group shall develop risk scenarios to prepare a coordinated preparedness testing of entities.
- A Cybersecurity Reserve will be established by the Commission and can be used by cyber crisis management authorities and CSIRTs of Member States to respond to significant or large-scale incidents impacting entities operating in critical sectors. The EU Cybersecurity Reserve should always act in the interest of the Union and its Member States by for example procuring services from trusted service providers.
- Creation of pool of trusted providers which can intervene on request of a Member State to respond to a large-scale incident:
  - Trusted service providers must fulfil different obligations to be considered for procuring services to the EU Cybersecurity Reserve. These obligations include:
    - Proof that its personnel have high standards in regard to their integrity independence, and a high level of cybersecurity knowledge and expertise to provide the service.

    - Proof that the provider as the appropriate security clearance and the necessary level of security for its systems and the necessary hardware and software equipment to be able to provide the service in the Member State(s) or potentially as well in third countries.

Cybersecurity incident review mechanism

- ENISA shall review, at the request of the Commission, EU-CyCLONe or the CSIRTs network, significant or large-scale cybersecurity incidents. The report should cover the main causes, vulnerabilities and lessons learned of the specific incident.

Control and supervision

The EU Cybersecurity Reserve shall be implemented by the Commission and ENISA. The Commission will be responsible for monitoring the implementation, application and the compliance of the regulation and report their evaluation to the European Parliament and to the Council.

Sanctions

No direct sanctions are currently mentioned in the proposal of the Cyber Solidarity Act.

Cyber Resilience Act

The proposal for the Cyber Resilience Act [10] introduces cybersecurity requirements for hardware and software products containing digital elements that are sold on the EU market. This section is based on the first draft of the proposal published on 15th September 2022, so the content is still up for changes under the negotiations on EU-level.

Different objectives will be covered by the Cyber Resilience Act to assure that manufacturers remain responsible for the cybersecurity of their products throughout the product's life cycle:

- Obligate manufacturers to follow a security by design approach.
- Introduce a cybersecurity framework to evaluate compliance of hardware and software products.
- Enhance the transparency on cybersecurity properties of the product.
- Ensure a safe usage by consumers and businesses.

Target

The Cyber Resilience Act applies to all products with digital elements which have a data connection to a device or network and if they are not excluded from the Act.

Products with digital elements are "*any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately*" (Cyber Resilience Act [10], Art 3 (1)). Some examples of such products are photo editing tools, hard drives, smart speakers, games, firewalls, CPUs etc.

Excluded from the Cyber-resilience Act are:

- Medical devices falling under Regulation (EU) 2017/745 [11] or Regulation (EU) 2017/746 [12].
- Vehicles and systems or components designed for vehicles falling under Regulation (EU) 2019/2144 [13].
- Products parts or equipment related to aircraft falling under Regulation (EU) 2018/1139 [14].
- Products for national security or military purposes.

Obligations

Manufacturers of products with digital elements need to do an assessment of the cybersecurity risk of the product they want to launch on the EU market.

Essential security requirements for products with digital elements are that:

- They need to be designed, developed, and produced with appropriate level of cybersecurity.
- They need to be delivered without any known vulnerability.
- They should have a secure configuration by default and a reset function.
- They need to be protected from unauthorised access.
- They need to protect the confidentiality and integrity of the data handled by the product.
- Data processing should be limited to what is necessary for the use of the product.
- The availability of essential functions needs to be protected by e.g., including a protection against DoS attacks.
- The negative impact that the product could have on the availability of other services needs to be minimized.
- The attack surface of the product needs to be limited.
- The impact of an incident needs to be limited.
- They need to monitor activity to provide security related information (e.g., access of data).
- They need to foresee the possibility to close vulnerabilities through security updates.

Manufacturers of products with digital elements need to comply with different requirements regarding vulnerability handling:

- Identify and document vulnerabilities and components used in the product and identify the top dependencies of the product.
- Provide security updates to address without delay the known vulnerabilities.
- Regularly review and test the security of the product.
- Publicly make available information about fixed vulnerabilities including information for the users helping them to remediate against them.
- Put in place a policy to coordinate vulnerability disclosure.
- Facilitate the sharing of information about vulnerabilities by e.g., providing a contact address to the reporting of vulnerabilities.
- Put in place a mechanism which allows to securely distribute security updates.
- Security updates need to be distributed without delay and free of charge.

Manufactures need to make sure that their products with digital elements are accompanied by different information and instructions to the user such as:

- The name of the manufacturer.
- A point of contact to report cybersecurity vulnerabilities.
- Serial number of the product.
- Explanations about the intended use of the product.
- Usage behaviour that might pose a cybersecurity risk.
- A link where the software bill of materials can be accesses.
- The link to the EU declaration of conformity, a description of the technical support available and detailed instructions to ensure the secure use of the product throughout its whole life cycle.
- How a change of the product might affect its security.

- How security updates will be installed.
- How users can securely remove their data from the product at the end of its life cycle.

A conformity assessment needs to be performed by the manufacturer to prove compliance with the different obligations mentioned above. For most products a self-assessment using the internal control procedure as described in the Cyber resilience act is sufficient.

Some products are classified as Critical "*Class I*" or Critical "*Class II*" products. For critical "*Class I*" product a third-party conformity assessment will be necessary if it has not applied solely harmonised EU standards. For Critical "*Class II*" products only a third-party assessment is accepted, and a self-assessment is not accepted as proof of compliance anymore.

The classification of a product as critical has been done by considering different criteria like the functionality of the product (e.g., critical software), the intended use (e.g., industrial control/NIS2) or other criteria like e.g., the extent of impact.

Some examples of critical products from "*Class I*" or "*Class II*" are:

Critical "*Class I*"	**Critical "*Class II*"**
• Browsers • Mobile device management software • Firewalls • Remote access software • Password managers	• Smartcards / tokens • Industrial firewalls • Operating systems for servers, desktops, and mobile devices • General purpose microprocessors

Manufactures also have the obligation to report to the ENISA, within 24 hours of becoming aware of it, any vulnerability in the product with digital elements that has been exploited. ENISA will forward the notification to the designated CSIRT in accordance with the processes described in the NIS2 Directive [1].

Importers and distributors of products with digital elements should furthermore assure that they only place products on the market that comply with the Cyber Resilience Act by e.g., verifying the conformity assessment, the technical documentation and/or by making sure that the CE label is on the product.

Control and supervision

Member states will designate a notifying authority responsible for setting up the procedures for the assessment and notification of a conformity assessment body. A conformity assessment body needs to be implemented.

Notified bodies will carry out conformity assessments and inform the notifying authority of refusals, restrictions, suspensions, or withdrawal of a certificate as well as circumstances negatively affecting the notifications.

The Commission will coordinate the cooperation between the notified bodies.

A market surveillance authority will be implemented in every Member State to ensure the implementation of the regulation. The market surveillance authority can carry out an evaluation of a product with digital elements to assess its compliance with all the different requirements. If the non-compliance is not restricted to the national market, the authority should inform the Commission and other Member States of the results of their analysis.

The Commission can ask, based on information received by the ENISA, the relevant market surveillance authority to perform a compliance testing of a product.

Sanctions

The non-compliance with the essential requirements for products with digital elements can be subject to fines going up to 15 000 000 EUR or 2,5% of the worldwide total turnover for the preceding financial year whichever of both is higher.

The non-compliance with any other obligation of the Cyber Resilience Act can be sanctioned with fines of up to 10 000 000 EUR or 2% of the worldwide total turnover for the preceding financial year whichever of both is higher.

A manufacturer that sends incorrect, incomplete, or misleading information may be subject to a fine going up to 5 000 000 EUR or up to 1% of the worldwide total turnover for the preceding financial year whichever of both is higher.

The amount of the penalty will be fixed considering information like the severity, duration and consequences of the infringement, the market size of the operator and whether other national surveillance authorities already applied a fine for the same operator and the same infringement.

Summary table

	NIS2	CER	DORA	GDPR	Cyber Solidarity Act	Cyber Resilience Act
Target	Essential and important entities from 11 sectors of high criticality and 7 other critical sectors	Critical entities from 11 sectors	Financial entities in the financial sector, and ICT third-party service providers	Any private or public structure that collects and/or processes data	Mainly Public Authorities	Mainly manufacturers of products with digital elements
Main objective	Cybersecurity	Resilience	Digital operational resilience	Personal data protection	Solidarity between EU Member states	Increase cybersecurity of products with digital elements
Obligations						
Risk management	●	●	●	◐[2]	●	●
Supply chain security	●	-	●	-	-	●
Business continuity	●	●	●	-	●	-
Incident handling	●	●	●	●	●	●
Incident notification	●	●	●	●	●	●
Delay of notification (if any)	24h	24h	tbd[3]	72h	-	24h
Information sharing	-	-	◐[4]	-	●	●

[2] Whenever personal data processing is "*likely to result in a high risk*" to the rights and freedoms of individuals, a specific risk assessment, called a Data Protection Impact Assessment (DPIA) should be completed.

[3] Timeframe should be specified.

[4] The regulation suggests financial entities to exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cybersecurity alerts and configuration tools.

Control and supervision						
Audits	●	●	●	●	-	●
Inspections	●	●	●	●	-	●
Request for information access	●	●	●	●	-	●
Sanctions						
Warnings	●	tbd[5]	tbd[6]	●	-	-
Suspension of authorisation	●	tbd[5]	tbd[6]	●	-	-
Administrative penalties / fines	**Essential entity:** at least 10 million euros or 2% of annual worldwide turnover. **Important entity:** at least 7 million euros or 1.4% of annual worldwide turnover	tbd[5]	tbd[6]	up to 20 million euros, or in the case of a company, up to 4% of worldwide annual sales	-	up to 15 million euros or 2,5% of the worldwide total turnover
	NIS2	**CER**	**DORA**	**GDPR**	**Cyber Solidarity Act**	**Cyber Resilience Act**

[5] The Directive does not lay down a system of penalties applicable to breaches of the measures but leaves it up to the Member States to determine effective, proportionate, and dissuasive penalties; this will be specified in national transpositions.

[6] The regulation does not lay down a system of penalties but leaves it up to the Member States to adopt any type of measure, including financial measures to ensure that financial entities to comply with their legal obligations; this will be specified in national transpositions.

Lessons learnt from Computer Security Incident Response Teams (CSIRTs)

In this section, best practices are proposed from the perspective of the Computer Incident Response Center Luxembourg (CIRCL), the CSIRT for the private sector, communes, and non-governmental entities in Luxembourg. Referring to Art. 9 (1) of the NIS Directive [2], a Member State designates one or more CSIRTs to 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, and responsible for risk and incident handling in accordance with a well-defined process. For the local NIS Directive implementation in Luxembourg, two CSIRTs were referenced: GOVCert and CIRCL, with GovCERT focusing on governmental entities and CIRCL on the private ones.

Geographical impact assessment

A recurrent question that arises is the geographic impact assessment of an outage, data leak or incident. In some tightly interconnected systems spread over multiple entities this is sometimes technical challenging. The technical challenges are often followed by organizational and compliance ones. From an historical point of view, the geographic assessment in natural incidents was quite straight forward as one could see how far the incident spread and a detailed map of impacted geographic assessment could be drawn. When the GDPR entered into force regulators asked geographic impact assessment when data leaks occurred. In case of a cross-border online business this is challenging as people from multiple countries are impacted. This challenge remains and amplifies in other regulations such as NIS / NIS2. An example is the ransomware group who compromised an operator of essential services and has access to technical documentation or access system putting at risk physical security.

In the text below is written some guidelines from an incident response point of view for doing such impact assessments.

Preparatory actions

The key of a quick and successful analysis depends on the preparatory actions and the understanding of business logic complementing technical analysis as forensic analysis. In case a technical analysis is outsourced to a third party, it is advised to ensure that the contracting party has enough of business logic understanding.

Technical preparation

Various actions could already be taken in advance to prepare such geographic assessment.

Regulator requirement analysis

The reading of the regulator reporting requirements in advance helps to assess which data is required by the regulator. A mapping between these requirements with the various data types could be done.

Establishment of a geographic index

To establish such an index a mapping of the various pieces of data according to the required geographic granularity. An example is an index of assets with their location. If a type of assets is impacted the geographic.

To create such an index, geographic data must be available. The easiest is to collect this data at the initial source for instance in an asset manager process. In that case when the assets are encoded geographic meta data is encoded.

Hash databases

Hashes help to identify files quicker than comparing them individually. A databases of these hashes help handle huge sets of discovered files to discover if they are known or unknown.

The public one available database such as those offered by NIST[7] or CIRCL[8] don't have hashes of internal files of the organization.

Setup of unstructured data analysis process

In case of data leak, victims are often confronted with huge data volumes that are unstructured. A setup of unstructured data analysis process helps to process the leaks quicker. There are open-source solutions to process unstructured data such as AIL-Framework [15] that can be installed on premises, installed in the cloud, or operated by third parties. The essence is to have the right keywords, regular expressions and, Yara[9] rules tightly bound to your business activities and geographic areas. Those tools help then to do the matching in unstructured data. If the operation of such a process is too costly there are some organizations that offer such services.

An attacker leaks emails claiming from a given organization. The attacker publishes numeric directories. In each directory numeric email files in the *eml* format. Searching in the content of such files with standard text processing tools is challenging due to encoding issues. Those files might include data chunks encoded in base64 which needs to be decoded first. Tools like AIL-framework do this recursive decoding where it applies keyword, regular expression matching and Yara rules on the final decoded items.

Compliance preparation

For the creation of various indexes or registers, GDPR processing activities might be updated or created. For instance, if geographic data is collected from customers, it must be reflected in the processing activities.

Incident response actions

A frequently observed case is where a threat actor claimed to leak partial information[10]. In that case the following actions might be necessary:

- Download the data of the threat actor.
- Verify the data of the threat actor.
- Do an analysis of the data the threat actor has.

The purpose of these analysis is to reply to a set of questions such as:

- Which data the threat actor had access?
- Did the threat actor tamper with the data?
- Which assets were impacted?
- What can the threat actor do with the collected data?

[7] https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl

[8] https://circl.lu/services/hashlookup

[9] YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples.

[10] https://www.ransomlook.io/

- Can the data be exploited by less advanced threat actors?
- PII (personal identifiable information) assessment
- Geographic assessment
- Meta data collection from the threat actors

Meta data collection

Meta data sometimes reveals how threat actors are working for instance during which times they are working. If they have regular working hours, if they respect public holidays. Those pieces of information can be derived from time stamps. Other meta data such as directory structuring or enumeration capabilities of URLs gave insights of inner working. Some threat actors put their data in a single directory others order them by directories, some directories correspond to some names such as machine names. Other directories follow a numbering scheme. Sometimes the threat actors also packages data in archives which may include additional timestamps and used tools in the respective meta data.

Data analysis

When threat actors publish data and do their claims, it is often advised to check those claims. Some threat actors use mis- or disinformation techniques meaning that they don't necessarily have the data or generate fake data. Other threat actors created a mix of old data leaks that are already handled. Other threat actors tamper with the data to discover who is using their leaked data. The processing of a huge number of files especially for large data leaks gets quickly overwhelming. A commonly used technique is to reduce the dataset of files that needs to process by excluding known files. Those known files can be identified either by querying a previously created database established in preparatory action. An alternative is to use public hash services or data sets such as offered by NIST[7] or CIRCL[8].

Summary of activities and outcomes of the NISDUC project

This part of the document is meant to give an overview of all the different activities undertaken, the accomplishments and the outcomes achieved by the NISDUC project. Furthermore, this part will take a step back and see what remaining challenges need to be tackled when it comes to the overall goal of the NISDUC project.

Before being able to go into the results of the Project, we will rewind and explain the reasons for the need of the NISDUC project and its objectives. The importance of cybersecurity for our society is more than ever displayed in the current geographical situation around the globe and especially in Europe. Even though this situation was not thinkable during the application of the NISDUC call, cybersecurity was already a hot topic, and this has not changed over the last couple of years, quite the inverse. However, we can see that the concepts of cybersecurity being considered as a purely technical topic have quite changed in the last years. No longer is it possible to discuss cybersecurity solely among technical experts or to consider cybersecurity as a local (organisation level or individual) matter. The key idea of NISDUC was and is to create and elaborate a user community around the NIS Directive [2] and NISDUC project [17] with the overall objective to allow the evolving of a trusted environment where we feel safe in sharing information among ourselves. More precisely to develop a set of activities for raising awareness, competencies and capabilities for national authorities and operators.

For this set of activities, the NISDUC project focussed on the following main areas:

- Development of training material for supporting operators to be compliant to the NIS Directive.
- Lessons learned of the implementation of the NIS Directive.
- Annual NISDUC conference to share knowledge and exchange experiences.

In order to develop training material for operators, various activities were held throughout the project. A reference framework for competencies needed to be established for defining the knowledge, skills and behaviours that are required by the operators. Therefore, analyses have been driven to identify the needs of the operators via surveys and interviews. In total, 7 interviews were held with operators from Luxembourg and Belgium. The domains and respective roles covered risk management - information security risk manager, incident management and notification – chief information security officer – process/unit manager, security policy measures – chief information security officer – compliance manager. These domains and roles were addressed through three different modules as they cover different types of competencies. Out of these modules, training and support materials were developed. A first pilot session was held during the first annual conference in May 2022 in Luxembourg with 15 participants from operators and a second pilot session was held during the second annual conference in April 2023 in Belgium with 22 participants.

Besides the development of the training material and the pilot sessions for operators, the NISDUC project gathered experiences and developed best practices for the implementation of the NIS Directive. This explains why we have published in total 4 deliverables (including this document). These deliverables are targeting operators, national competent authorities (NCA) for NIS as well as Computer

Security Incident Response Teams (CSIRTs). The different deliverables are covering different lessons learned and can be found on a dedicated section of the NISDUC project website[11]. Each project partner contributed with their own experience and knowledge of the different parts of the documents. This means that every deliverable has a more theoretical part like sector modelling via a collaborative approach (D3.1), incident notification threshold definition, telecom sector and the NIS2 proposal (D3.2), systemic analyses of the ecosystem, cybersecurity of operational technology, risk management feedback (D3.3). Every deliverable also has a more practical part on automation driven data sharing (D3.1), voluntary data sharing aspects (D3.2) and evidence-driven reporting from an incident response perspective (D3.3).

The creation of a community is of utmost importance to enable and facilitate a trusted environment for sharing different kinds of information and knowledge. Therefore, an annual conference called NISDUC Conference has been organised starting from the second project year. The first conference "*How to tackle the implementation of NIS/NIS2?*"[12] was held on the 10th and 11th May in Luxembourg in the Chambre des Commerce with 180 registrations. The second NISDUC Conference "*From NIS to NIS2.0: a path to take*"[13] on 25th and 26th April in Brussels in the Double Tree by Hilton with 219 registrations. Both conferences had participants from operators from all over Europe as well as other competent authorities.

The number of registrations exceeded our expectations and is a great indicator for a need of a community with operators and with competent authorities. Therefore, the sustainability of this annual conference is very crucial, and the different partners are already working on the next conference to be held in 2024.

The project is coming to an end, but challenges are not all tackled as this is an ongoing evolution. The domain of cybersecurity is not standing still, which is already proven buy the different initiatives and directives from the European Commission (Cyber Solidarity Act [9], Cyber Resilience Act [10]). Even if the project itself is ending, the work is far from over, especially as the NIS2 Directive [1] has come into place in January 2023 and needs to be transposed by fall 2024 in the member states. NIS2 leads to not only the need for integrating new security measures but is also covering a lot more sectors and entities, which shows even more the importance of a community.

The importance of supervision in cybersecurity lies in assuring an overall minimum level of maturity in cybersecurity. NIS2 will allow competent authorities to further raise awareness and to further strengthen the level of cybersecurity throughout the different sectors, as especially in cybersecurity, the weakest link will define the strength of the whole network. NIS2 comes with some big changes with respect to the previous NIS Directive. NIS2 improves the supervision model as the governance bodies of operators have liability towards cybersecurity and they need to be able to make informed decisions.

[11] https://www.nisduc.eu/publications/nisduc-lessons-learnt

[12] https://www.nisduc.eu/first-conference

[13] https://www.nisduc.eu/second-conference

NIS2 also holds new concepts for operators, like assuring the supply chain security. These concepts might not be new in ICT domains but are new to other operational sectors. For most of the sectors the interplay with the CER will also be a crucial topic, and even if DORA is a considered as *lex specialis*, there will be still some interplays with NIS2 where clarifications are necessary.

All these points show the challenges that still lay ahead and why a community is needed and why the work of the NISDUC project is not over even if the funding is. The partners will still be working in the future to keep up the discussions among competent authorities together with operators to assure a common understanding of the matter.

List of abbreviations

Abbreviation	Translation
CER	Critical Entities Resilience
CIRCL	Computer Incident Response Center Luxembourg
CSIRT	Computer Security Incident Response Team
DEP	Digital Europe Programme
DORA	Digital Operational Resilience Act
DoS	Denial-of-service
DPO	Data Protection Officer
DSP	Digital Service Provider
ENISA	European Union Agency for Cybersecurity
EU CyCLONe	European Cyber Crisis Liaison Organisation Network
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IP	Internet Protocol
NCA	National Competent Authority
NISDUC	NIS Directive User Community
NIST	National Institute of Standards and Technology
OES	Operator of Essential Services
PII	Personal Identifiable Information
SOC	Security Operations Center
SPOC	Single Point of Contact
TLPT	Threat-Led Penetration Testing
URL	Uniform Resource Locator

Terms and definitions

Base64	Group of binary-to-text encoding schemes that represent binary data (more specifically, a sequence of 8-bit bytes) in sequences of 24 bits that can be represented by four 6-bit Base64 digits [16].
Cloud computing service	A digital service that enables access to a scalable and elastic pool of shareable computing resources [2].
Digital Service	Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services [2]. For the scope of the NIS Directive, only three types of services (as defined in Annex III of the Directive) are considered: • Cloud computing service. • Online marketplace. • Online search engines.
Digital Service Provider	An entity that provides digital service(s).
DoS attack	A denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network [18].
EU CyCLONe	The European Cyber Crisis Liaison Organisation Network is a cooperation network for Member States national authorities in charge of cyber crisis management. The network was launched in 2020 and formalized on 16th of January 2023 with entrance into force of NIS2 Directive [1] art 16.
National Competent Authority	An authority designated by each Member State in charge of monitoring the application of the NIS Directive at national level [2].
Network and information system	(a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC, (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, (c) perform automatic processing of digital data; or digital data stored, processed, retrieved, or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection, and maintenance [2].
NIS Cooperation Group	The Network and Information Systems Cooperation Group was established by the NIS Directive [2] to ensure cooperation and information exchange among Member States. Its overall mission is to achieve a high common level of security for network and information systems in the European Union. It supports and facilitates the strategic cooperation and the exchange of information among EU Member States. The NIS Cooperation Group's tasks are explicitly described in Article 11 of the NIS Directive.
NIS Directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common

	level of security of network and information systems across the Union
Operator of Essential Services	A public or private entity of a type referred to in Annex II of NIS Directive, which meets the criteria laid down in Article 5(2) of the NIS Directive [2].
Security of network and information systems	The ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems [2].
Single Point of Contact	An entity designated by each Member State in charge of exercising 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 and the CSIRTs network [2].

Bibliography

[1] Official Journal of the European Union, 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 (NIS2 Directive). 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[2] Official Journal of the European Union, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. 2016. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[3] Official Journal of the European Union, Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj

[4] Official Journal of the European Union, Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. 2003. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361

[5] Official Journal of the European Union, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. 2008. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2008/114/oj

[6] Official Journal of the European Union, Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[7] Official Journal of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[8] Official Journal of the European Union, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 1995. [Online]. Available: https://eur-lex.europa.eu/eli/dir/1995/46/o

[9] Official Journal of the European Union, Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents. 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0209

[10] Official Journal of the European Union, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454

[11] Official Journal of the European Union, Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council

Directives 90/385/EEC and 93/42/EEC. 2017. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2017/745/oj

[12] Official Journal of the European Union, Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU. 2017. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2017/746/oj

[13] Official Journal of the European Union, Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166. 2019. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/2144/oj

[14] Official Journal of the European Union, Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91. 2018. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2018/1139/oj

[15] AIL framework – Analysis Information Leak framework, https://github.com/CIRCL/AIL-framework

[16] Wikipedia, Base64. [Online]. Available: https://en.wikipedia.org/wiki/Base64

[17] NIS Directive User Community (NISDUC) project website. [Online]. https://www.nisduc.eu/

[18] Wikipedia, Denial-of-service attack. [Online]. Available: https://en.wikipedia.org/wiki/Denial-of-service_attack