NOTES ON NIS2

By Cesare Gallotti. Updated on 16/03/2024.

A few words about NIS 2

NIS 2 (EU Directive 2022/2055) entered into force on 17 January 2023.

NIS2 will have to be adopted by member states by October 2024.

- The number of subjects increased.
- It requires a risk analysis.
- The measures should be adapted to the context, thus also taking into account the spending capacity.

Subjects to whom NIS2 applies

The applicability depends on the sector and the size (more than 50 employees and turnover of more than 10 million Euros; therefore excluding small ones) of the organization. NIS2 is therefore applicable to:

- essential entities;
- important entities.

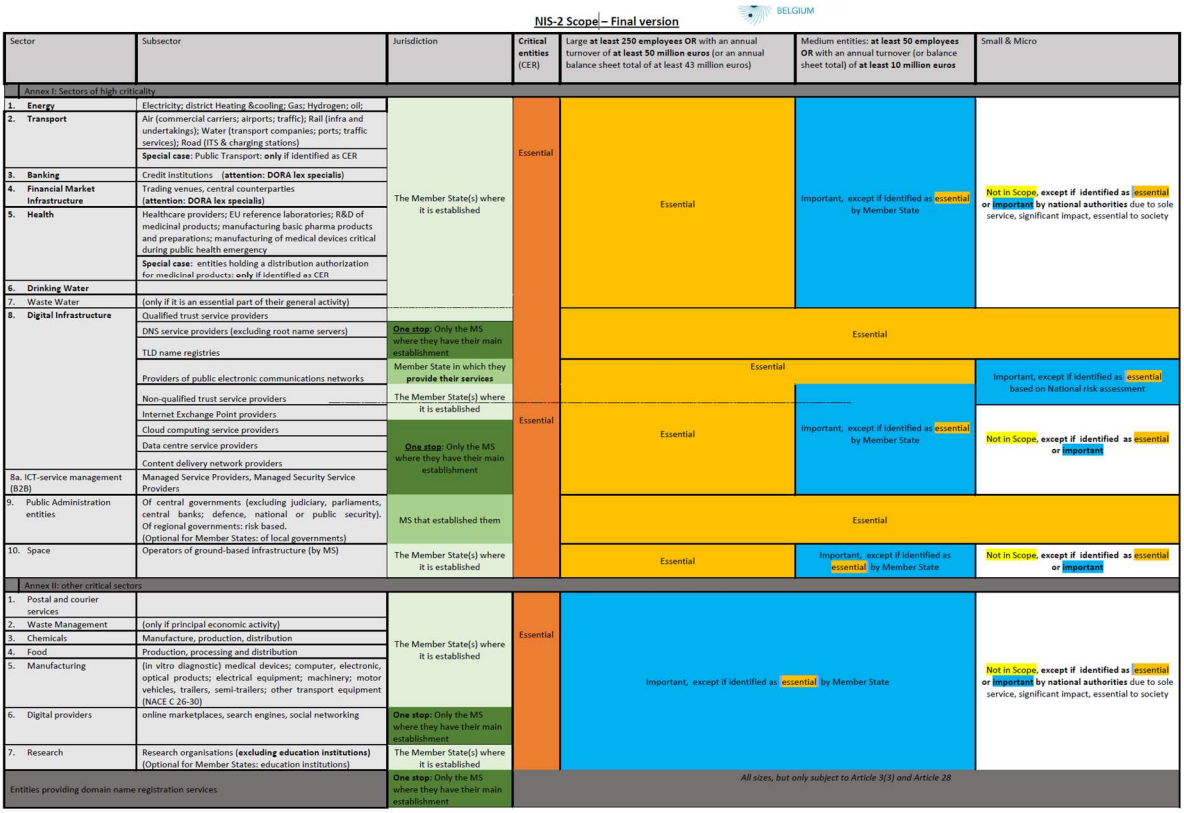
The practical difference is in terms of controls and sanctions.

NIS2 involves more companies than Italian Perimetro nazionale per la cyber sicurezza.

With NIS 2, entities will have to recognize themselves as entities that must apply NIS 2, it is no longer the authority that designates them as such. It is expected that entities will register according to rules that will be provided.

On the basis of the registrations, by 17 April 2025, Member States shall establish a list of essential and important entities and entities providing domain name registration services.

The diagram below can be found on the https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization website (my file "2023-NIS-2 Scope visual.pdf").



NIS-2 Scope – Final version

BELGIUM

Sector	Subsector	Jurisdiction	Critical entities (CER)	Large **at least 250 employees OR** with an annual turnover of **at least 50 million euros** (or an annual balance sheet total of at least 43 million euros)	Medium entities: **at least 50 employees OR** with an annual turnover (or balance sheet total) of **at least 10 million euros**	Small & Micro
Annex I: Sectors of high criticality						
1. **Energy**	Electricity; district Heating &cooling; Gas; Hydrogen; oil;	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as** essential **or** important **by national authorities** due to sole service, significant impact, essential to society
2. **Transport**	Air (commercial carriers; airports; traffic); Rail (infra and undertakings); Water (transport companies; ports; traffic services); Road (ITS & charging stations)					
	Special case: Public Transport: **only** if identified as CER					
3. **Banking**	Credit institutions (**attention: DORA lex specialis**)					
4. **Financial Market Infrastructure**	Trading venues; central counterparties (**attention: DORA lex specialis**)					
5. **Health**	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency					
	Special case: entities holding a distribution authorization for medicinal products: **only** if identified as CER					
6. **Drinking Water**						
7. Waste Water	(only if it is an essential part of their general activity)					
8. **Digital Infrastructure**	Qualified trust service providers			Essential		
	DNS service providers (excluding root name servers)	**One stop**: Only the MS where they have their main establishment				
	TLD name registries					
	Providers of public electronic communications networks	Member State in which they **provide their services**		Essential		Important, except if identified as essential based on National risk assessment
	Non-qualified trust service providers	The Member State(s) where it is established			Important, except if identified as essential by Member State	
	Internet Exchange Point providers		Essential	Essential		Not in Scope, **except if identified as** essential **or** important
	Cloud computing service providers	**One stop**: Only the MS where they have their main establishment				
	Data centre service providers					
	Content delivery network providers					
8a. ICT-service management (B2B)	Managed Service Providers, Managed Security Service Providers					
9. Public Administration entities	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security). Of regional governments: risk based. (Optional for Member States: of local governments)	MS that established them		Essential		
10. Space	Operators of ground-based infrastructure (by MS)	The Member State(s) where it is established		Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as** essential **or** important
Annex II: other critical sectors						
1. Postal and courier services		The Member State(s) where it is established	Essential	Important, except if identified as essential by Member State		Not in Scope, **except if identified as** essential **or** important **by national authorities** due to sole service, significant impact, essential to society
2. Waste Management	(only if principal economic activity)					
3. Chemicals	Manufacture, production, distribution					
4. Food	Production, processing and distribution					
5. Manufacturing	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)					
6. Digital providers	online marketplaces, search engines, social networking	**One stop**: Only the MS where they have their main establishment				
7. Research	Research organisations (**excluding education institutions**) (Optional for Member States: education institutions)	The Member State(s) where it is established				
Entities providing domain name registration services		**One stop**: Only the MS where they have their main establishment	*All sizes, but only subject to Article 3(3) and Article 28*			

Entities defined as "critical" by Directive (EU) 2022/2557, better known as the CER Directive, will also fall within the scope of application.

Additional subjects may be added by national legislation.

Risk assessment

NIS2 is multi-risk: logical, physical, governance, technological lock-in, utilities. And it considers the "social and economic" impact and requires an "appropriate level" of security.

Belgium has a rather simple approach (but I don't fully understand how it works): https://ccb.belgium.be/en/choosing-right-cyber-fundamentals-assurance-level-your-organisation.

The impact table is interesting, because perhaps it could be reused to identify significant incidents (see below).

Impact Level HIGH

Description		
The threat is expected to have serious or catastrophic disruptive effects on organisations' network and information systems (economic), organisations' assets (financial), individuals (health, privacy, daily life, well-being), the nation (security and public order) or the functioning of international institutions on Belgian territory. Serious or catastrophic disruptive impact means that the threat has an impact as below:		
Healthcare	Over 200 [1] dead, chronically ill or with long-term disability	• Over 75.000 (3) people with short-term health problems. • Severe environmental pollution affecting our country's natural habitat.
Personal sphere	Loss of personal data of more than 1.000.000 persons (GDPR Art 4.)	Individuals may face significant consequences, which they should be able to overcome, albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, summons, deterioration in health, etc.)
Daily life	Significant Impact on daily life of 75.000 [2] people	
Wellbeing	Impact on welfare (e.g. housing, provision of food and drinking water) for more than 75.000 people	Ecological contamination with long-term effects on more than 75.000 people.
Financial	Financial impact of minimum € 1.500 [3] on 75.000 people.	• Critical damage to organisations' assets. • Critical financial losses in organisations.
Economics	Loss of more than 0.1% of GDP	• Impact on more than 25% of the essential services in the sector. • Severe deterioration or reduction in the ability to perform the organisation's mission such that the organisation cannot perform one or more of its primary functions. • Destruction of essential infrastructure. • Serious threat to economic prosperity.
Security and public order	National impact on the protection of the state and services that ensure security and public order	• Difficulties for the state, and even an inability, to secure a regulatory function or one of its vital missions. • There is serious reputational damage to the state. There is risk of loss of confidence in the state creating fear, uncertainty and doubt. • Protection of the achievements of the democratic rule of law and its shared values is no longer assured. • The physical security of citizens and the physical integrity of our country is no longer assured.
International Institutions	Significant impact on the operation of international institutions on Belgian territory	• International order based on international law and multilateral frameworks is no longer assured. • The effective functioning of the European Union is no longer assured.

The Commission's Guidelines of 13.9.2023 suggest to consider the following threats, again in a multi-risk logic:

- sabotage
- theft
- fire
- flood
- telecommunication issues
- problems with power outages
- any unauthorised physical access that could compromise the availability, authenticity, integrity or confidentiality of the data stored, transmitted or processed or of the services offered by or accessible through such information and network systems
- system failures
- human errors
- malicious actions
- natural phenomena.

Comment

I hope is that, if guidelines will be issued on how to carry on a risk assessment, they will not be based on the formal, but not useful, approach based on assets, threats and vulnerabilities. I hope that they will give room to the event-based approach. I always say that a detail of all the assets is not useful for risk assessment (it is instead necessary for operational activities).

Security measures

The Directive identifies (Article 21(2)) risk management measures, namely:

(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.

Perri says there's an catalogue on skills assessment, but I didn't find it (or maybe I misunderstood); perhaps in interpretations.

By 17 October 2024, the Commission shall adopt implementing acts laying down the technical and methodological requirements of the above measures as regards providers of:

- DNS services,
- top-level domain name (TLD) registries,
- cloud computing services,
- data center services,
- content delivery networks,
- managed services,
- managed security services,
- online marketplaces,
- online search engines,
- social networking service platforms,
- trust service providers.

Some predict that the following should therefore apply:

- sector-specific requirements set by the Commission (or, alternatively, requirements recommended by ENISA or national authorities);
- common basic requirements (or, alternatively, ISO/IEC 27001 certification).

Belgium (like Italy) proposes a list of measures based on the NIST CSF: https://ccb.belgium.be/en/cyberfundamentals-framework.

At present (13 March 2024) the measures to be taken have not been established. In Italy we know that now, for subjects under NIS, those of the National Framework for Cybersecurity and Data Protection (https://www.cybersecurityframework.it/framework2) are required and so in other countries. Perhaps with NIS 2 other patterns will follow.

Please note that the measures established by the member States and referred to in Article 21(1) of NIS2 should apply to all operational activities and services of the entity, not only to specific IT resources or critical services provided by the entity. My interpretation: if an entity has "secure" and "insecure" services, it can be hacked by exploiting the deficiencies of "insecure" services and then, with lateral movements, compromising the "secure" ones as well. For preventing this, the entity must apply security measures to all of its activities and services.

Comment

Personally, I hope that ISO/IEC 27001 will be adopted or, as an alternative, entities will have the permission to choose their IT security framework. I support ISO/IEC 27001 because Italy can participate in its updates and extensions.

In all cases, I recommend that you start implementing ISO/IEC 27001, on which, if necessary, you can add the specific requirements that will be made. An ISO/IEC 27001 implementation can be easily converted to NIST CSF or others.

Incident management

As already provided for by the NIS 1 Directive, NIS 2 also provides for the obligation to notify the CSIRT and the competent authorities (as well as the recipients of the service themselves) of significant incidents (IT incidents capable of significantly impacting the provision of the service).

Communications to the CSIRT must be made (art. 23):

- Within 24 hours of becoming aware of the incident with an early warning notification (this is to mitigate the potential spread of incidents and to allow you to call for assistance);
    - it must provide the data that is strictly necessary if the significant incident is suspected to be the result of unlawful or malicious acts or if it is likely to have (i.e. is likely to have) a cross-border impact;
    - it must contain an initial assessment of the significant incident, including its severity and impact, as well as, where available, indicators of compromise.
- Within 72 hours of becoming aware of the incident with updates to the information provided with the early warning.
- Within 1 month of becoming aware of the incident with a final report to complete the reporting process (this is in order to be able to draw valuable lessons from individual incidents);
    - The report must be inclusive of its severity and impact, the type of threat or underlying cause that likely triggered the incident, the mitigation measures taken and ongoing and, where appropriate, the cross-border impact of the incident.

Some entities are subject to multiple regulations and therefore different ways of reporting incidents. In some cases, integration of the several requirements can be complex.

Articles:

- Article 23 sets out when notification is mandatory;

- Article 30, indicates when the notification is voluntary (other incidents, threats, near misses, including by other parties).

In NIS2 there is a definition of "significant incident" in Article 23(3): it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned or it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

An entity needs to be better define what a "significant incident" is in its context and perhaps the impact table used to assess the risk can help.

NIS 2 also uses "near misses". Near miss is “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” (art. 6).

NIS2 establishes the European Network of Cyber Crisis Liaison Organisations (EU-CyCLONe).

Other topics

NIS2 includes additional topics:

- Cooperation between Member States
- Penalties
- National Contact Points
- Role of ENISA

These, however, do not fall within my competence and I have not studied them in depth.

Bibliography

Center for cyber security Belgium website: https://ccb.belgium.be/en/choosing-right-cyber-fundamentals-assurance-level-your-organisation. Thanks to Alessandro Cosenza for having recommended it to me.

Presentation "Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union ("NIS2 directive")".

EU website: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new. However, it does not provide any information that I think is useful.

Interpretative criteria for the Commission's NIS2: https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive. Thanks to Pierluigi Perri.

Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/EC). Thanks to Giancarlo Caroti.