MAYER | BROWN

05 AUGUST 2024

# NEW EU CYBER RULES: IMPLEMENTATION OF NIS2 IN THE EU MEMBER STATES

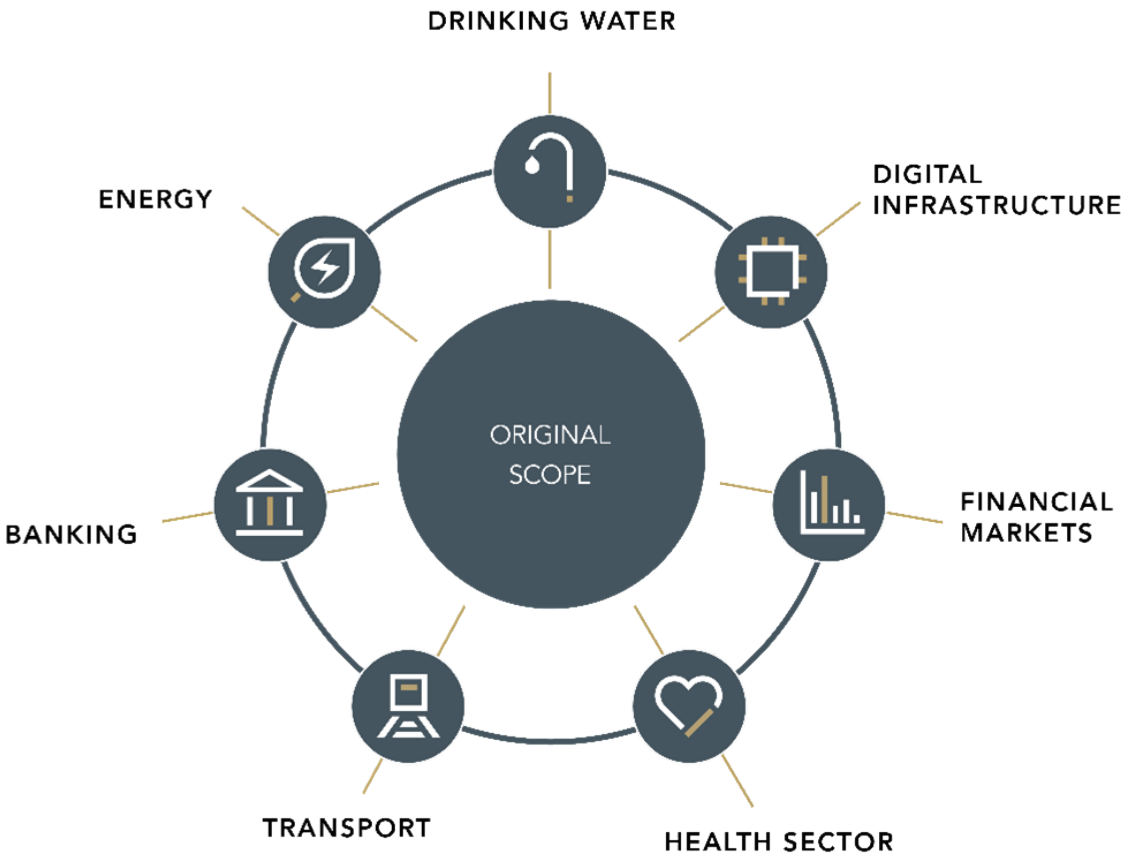
AUTHORS:
ANA HADNES BRUDER, DR. ULRICH WORM, BENJAMIN BECK, AMELIE KSINSIK, MICHELLE MAYER

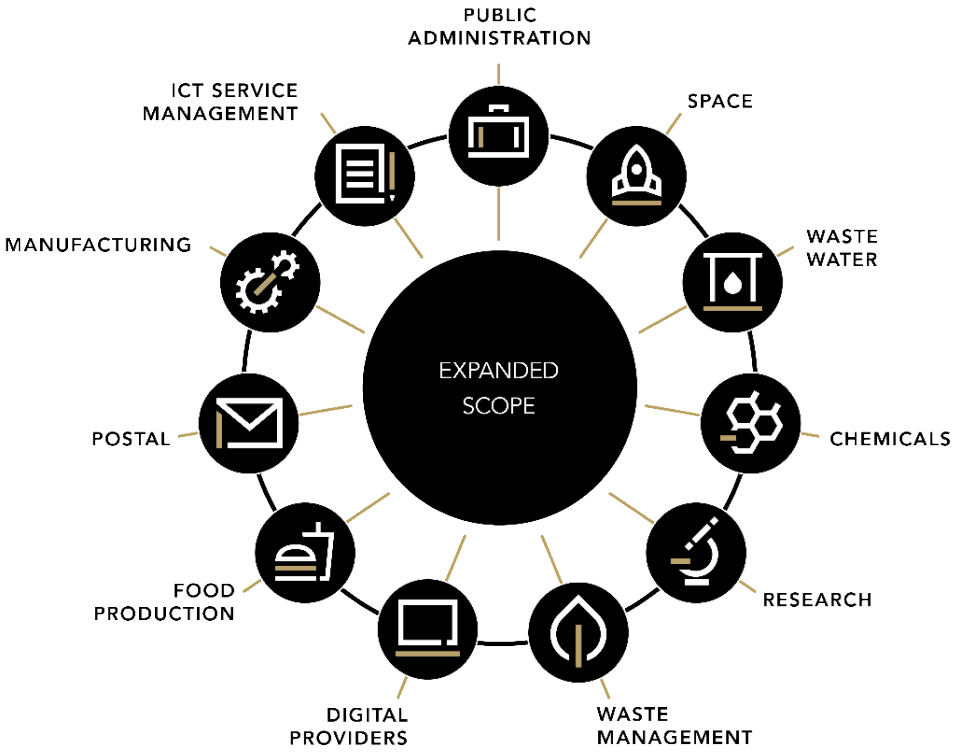
---

The Network and Information Security 2 Directive (EU) 2022/2555 ("NIS2") entered into force on 16 January 2023. NIS2 sets cyber rules for organizations whose services are considered essential or important for maintaining critical societal and economic activities, such as ensuring the flow of energy or financial transactions. As a Directive, NIS2 must be transposed into the national laws of the EU Member States before it can take direct effect. NIS2 generally requires Member States to adopt national implementing measures by 17 October 2024 and apply such measures from 18 October 2024.
This Legal Update provides a brief overview of the key points of NIS2 and shows the current status of implementation in the EU Member States.

## WHICH ORGANIZATIONS ARE IN SCOPE?

NIS2 applies to organizations that operate in certain sectors, which are listed in Annexes I and II of NIS2. Compared to the previous NIS Directive (EU) 2016/1148 ("**NIS**"), NIS2 covers a broader range of sectors, as illustrated below:

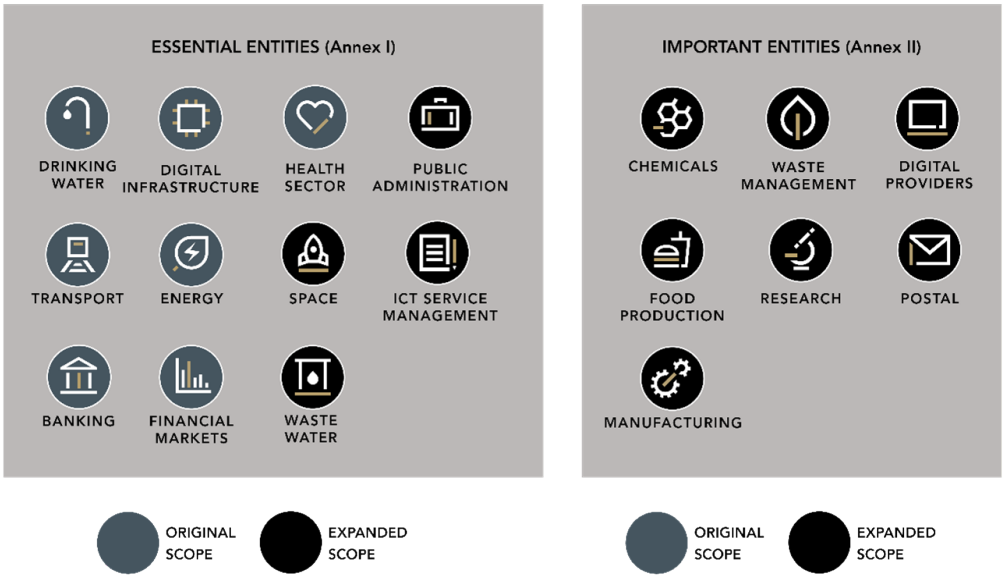

DRINKING WATER
ENERGY
DIGITAL INFRASTRUCTURE
ORIGINAL SCOPE
BANKING
FINANCIAL MARKETS
TRANSPORT
HEALTH SECTOR




Unlike NIS, NIS2 establishes uniform criteria for determining which entities operating in these sectors fall within its scope. All entities that are at least **medium-sized enterprises** as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC, or that exceed the thresholds for medium-sized enterprises, fall within its scope:

- **Medium Sized**: At least 50 employees **or** annual turnover and/or annual balance sheet total of EUR 10 million;
- **Large:** At least 250 employees **or** annual turnover and/or annual balance sheet total of EUR 50 million

Entities that are of a type listed in Annex I of NIS2 and that are large (*i.e.* exceed the thresholds for medium-sized enterprises) are considered **essential entities**. All other in-scope entities are considered **important entities**, including those listed in Annex I that are only medium-sized:




## WHAT ARE THE KEY OBLIGATIONS?

Compared to NIS, NIS2 imposes more stringent risk management and reporting requirements on in-scope entities. For example, NIS2 introduces more detailed incident reporting requirements, including reporting content and timelines. In addition, NIS2 provides a minimum set of appropriate technical and organizational measures that in-scope entities must implement, including supply chain due diligence.
A key aspect of NIS2 is that management bodies of in-scope entities are accountable for the cybersecurity framework, as they must approve the risk management measures taken, oversee their implementation, and can be held liable if the entity fails to comply with NIS2.
NIS2 requirements apply to both essential and important entities. In general, there is no less stringent regime for important entities, but there are some differences. For example, essential entities are subject to ongoing supervision, while important entities are supervised only when the authorities receive indications of non-compliance. In addition, the fines for non-compliance are higher for essential entities:

- **Essential entities**: up to 10 million euros or at least 2% of the total annual global turnover.
- **Important entities**: up to 7 million euros or at least 1.4% of the total annual global turnover.

## WHY IS IT IMPORTANT TO TRACK THE NATIONAL IMPLEMENTING LEGISLATION?

As a directive, NIS2 sets out **minimum requirements** for cybersecurity risk-management measures and reporting obligations across the sectors that fall within its scope. EU Member States are not precluded from adopting or maintaining a higher level of protection. NIS2 provides a floor, but not a ceiling.
For example, EU Member States may impose more stringent measures in the following areas:

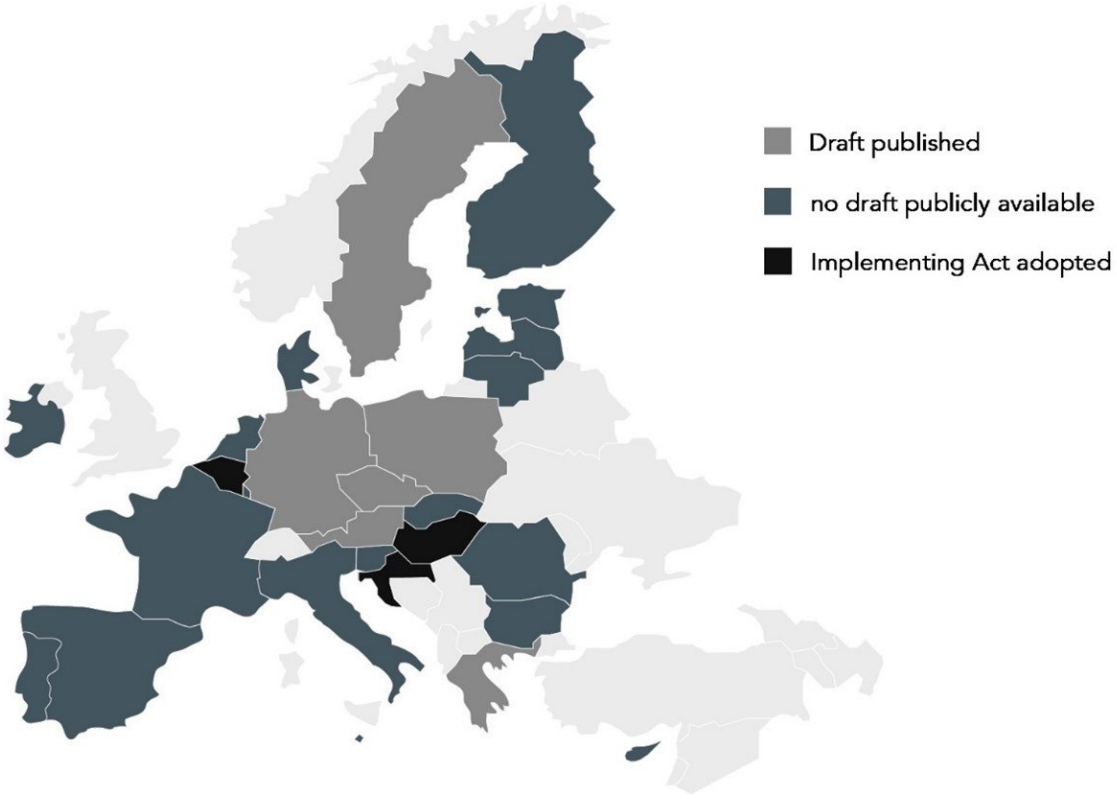
- **Liability of Management Bodies:** NIS2 requires EU Member States to ensure that management bodies can be held liable for failing to meet their cyber obligations. However, the level of liability is not fixed and may include criminal liability;
- **In-Scope Entities**: While EU Member States cannot go below the minimum scope of NIS2, they could extend the scope of the national implementing legislation to include additional entities not generally covered by NIS2, e.g. operators of certain infrastructure in the relevant sectors;

- **Cyber Risk-Management:** As NIS2 only sets the baseline for cybersecurity risk management measures, EU Member States could impose more stringent measures, such as those related to testing or supply chain due diligence.

Tracking national implementing legislation is also recommended for simple reasons such as knowing who the competent supervisory authorities are and where to file incident reports.

## CURRENT STATE OF IMPLEMENTATION

Some EU Member States, such as Belgium, Hungary and Croatia, have already adopted NIS2 implementing legislation. Other EU Member States such as Germany, Poland and Sweden have already published drafts of their NIS2 implementing legislation. However, it is becoming clear that not all EU Member States will be able to adopt national implementing measures by 17 October 2024 (end of the transposition period). Some EU Member States, such as the Netherlands and Denmark, have already indicated that they are unlikely to meet the deadline.
The **current state of implementation** in the EU Member States is shown in the map below:




*The map above is based on information from publicly available sources. The information may not be complete or current.*

## NEXT STEPS

First, organizations operating in the sectors covered by NIS2 need to assess in greater detail whether they fall under NIS2. Second, in-scope entities will benefit from early compliance efforts, even if not all national implementations have been adopted at this time.
In-scope entities will need to assess the cybersecurity program that is already in place and whether there is need for improvement in areas such as risk management, incident handling, business continuity procedures

and supply chain due diligence. In addition, management bodies should ensure that they are capable of assuming risk management responsibilities once the NIS2 implementing legislation is applicable, and undertake the necessary training.
As noted above, NIS2 only sets minimum requirements. Therefore, in-scope organizations operating in multiple EU Member States should pay particular attention to potential differences in national implementing legislation, as this may affect the scope of obligations that organizations must comply with.

## AUTHORS


ASSOCIATE

BENJAMIN BECK

DÜSSELDORF +49 211 86224 124

FRANKFURT

BENJAMIN.BECK@MAYERBROWN.COM

PARTNER

ANA HADNES BRUDER

FRANKFURT +49 69 7941 1778

ABRUDER@MAYERBROWN.COM

PARTNER

DR. ULRICH WORM

FRANKFURT +49 69 7941 2981

UWORM@MAYERBROWN.COM