

DORA and NIS2

Two EU legislative instruments.

How do they differ? What requirements do they bring? What challenges do they pose? For whom are they relevant?

Be prepared.

1 | Digital Operational Resilience Act (DORA)

DORA is an **EU regulation** that establishes a comprehensive framework for **harmonizing digital resilience processes and standards** to **strengthen the resilience** of digital operations in the financial sector. It is the world's first framework that allows **financial services supervisors** to **oversee third-party** providers of critical ICT services, including cloud service providers.

TO WHOM DOES DORA APPLY?

DORA applies to the vast majority of **financial services companies**, including **banks, insurance companies** and **investment firms**.

WHAT DOES DORA DETERMINE?

DORA sets out mandatory rules for the following areas:



Classification and reporting of ICT-related incidents



Resilience testing of ICT tools and systems



ICT risk management framework



Third-party risk management



Threat information sharing

2 | Network and Information System 2 (NIS2)

NIS2 is an **EU directive** that **sets general objectives for Member States'** national laws **on cyber security and ICT systems and networks**, with the aim of strengthening security across the EU. Unlike regulations, which are directly applicable, the implementation of NIS2 as a directive in the context of the Czech legislation is ensured by **amendments to the Act on Cyber Security** by the National Cyber and Information Security Agency (NÚKIB).

TO WHOM DOES NIS2 APPLY?

NIS2 increases the number of entities for which the laws regulating cybersecurity apply. Put simply, it is applicable to all **operators of regulated services** – ICT system operators, organizations in the banking and financial services, energy, health, water, and transportation sectors.

WHAT DOES NIS2 DETERMINE?

NIS2 is based on three fundamental pillars:



Definition of national cybersecurity strategies



Support for strategic cooperation and exchange of information between Member States



Application of measures to key sectors

NIS2 will apply to all entities providing services in the **key sectors** and meeting the "large company" condition, based on the recommendation by the European Commission.



Energy



Transportation



Banking and financial markets infrastructure



Healthcare



Public administration



Space



Water services (drinking water and wastewater)














Digital infrastructure and managed ICT service delivery

The Directive also affects other sectors such as **postal and courier services, waste management, chemical industry, food processing, manufacturing, and research.**

3 | NIS2 in the Czech Republic: The Act on Cyber Security

The Act on Cyber Security is an application of the NIS2, which among other things sets out the areas that the law must cover, including :

-  **Information Security Management**
-  **Cyber Incident Response**
-  **Business Continuity Management**
-  **Supply chain security**
-  **Secure procurement, development, and maintenance**
-  **Security Audit**
-  **Cyber hygiene practices and training**
-  **Cryptographic procedures and encryption**
-  **Human resources security**
-  **Access control**
-  **Asset management**
-  **Secure communications**

The first draft of the Czech Act on Cyber Security was submitted in the summer of 2023 and included **two regimes** – a higher regime and a lower regime, reflecting the principle of two-speed cybersecurity and thus relieving the burden of smaller organizations. Yet, the new Act is currently in the process of drafting again.

Member States have time until 17 October 2024 to bring NIS2 into national law.



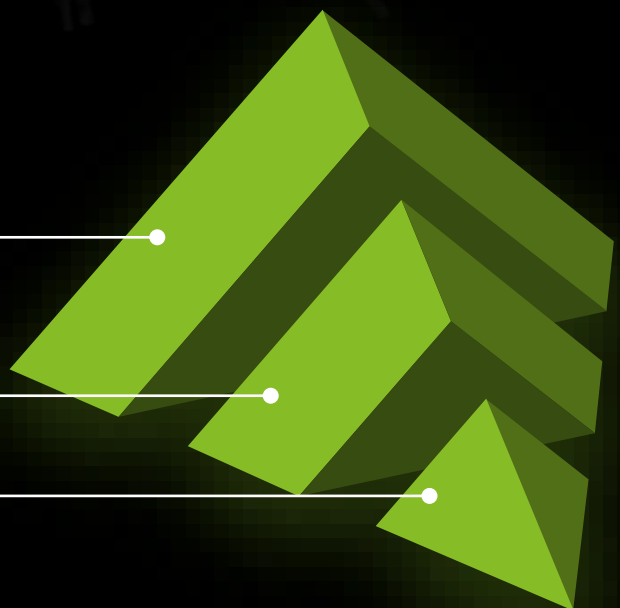
EU Directive:
NIS2



National Law:
The Act on Cyber Security



Lower and higher regimes



4 | DORA as a *Lex Specialis* for Financial Institutions

Regarding the identification of the relationship between DORA and NIS2, the European Commission considers DORA a *Lex Specialis* for financial sector entities, meaning that in practice, the DORA requirements take precedence over any overlapping regulatory texts, such as the NIS2 or the ESA.

What applies to whom? RELEVANT ENTITIES

DORA	Investment funds, Payment institutions, Insurance companies, Bank & Financial Market Instruments	ICT service providers	Entities in the transport, energy, healthcare and other sectors	NIS2
ICT risk management (Chapter II)	●	●	●	Cybersecurity risk-management measures and reporting obligations (Chapter IV, Section 20-21) Governance and Cybersecurity risk-management measures
ICT-related incidents management, classification and reporting (Chapter III)	●	●	●	Cybersecurity risk-management measures and reporting obligations (Chapter IV, Section 23) Reporting obligations
Digital operational resilience testing (Chapter IV)	●	●	●	Cybersecurity risk-management measures and reporting obligations (Chapter IV, Section 24) Using European cyber security certification systems
Managing of ICT third-party risk (Chapter V, Section I) Key principles for a sound management of ICT third-party risk	●	●	●	Jurisdiction and Registration (Chapter V)
Managing of ICT third-party risk (Chapter V, Section II) Oversight framework of critical ICT third-party service providers	●	● ●	●	Cybersecurity risk-management measures and reporting obligations (Chapter IV, Section 22) Union level coordinated security risk assessments of critical supply chains
Information sharing arrangements (Chapter VI)	●	●	●	Information sharing (Chapter VI)
Competent authorities (Chapter VII)	●	●	●	Supervision and enforcement (Chapter VII)

5 | How can we help?

At Deloitte, we offer comprehensive, holistic services that benefit numerous organizations. Such services include GAP analyses as well as implementation of steps leading to regulatory compliance.



GAP Analysis and Implementation

We analyze existing processes, applications, and staff in the context of relevant rules, propose an implementation roadmap considering your technological, process, and organizational readiness, draft specific changes, and assist in their implementation.



Incident reporting and threat analysis sharing

We help clients adapt to the new reporting rules and align their internal processes to optimize resource allocation. We also assist in the development and integration of a cyber threat sharing process.



Risk Management Framework

To meet the relevant requirements, robust risk management processes should be in place. We help organizations align their business strategies and cyber risks and maintain a comprehensive and effective risk management framework.



Threat-based resilience testing and penetration testing (TLPT)

We perform vulnerability scanning, penetration testing, and robust business continuity and disaster recovery testing. Our cyber practice provides the highest quality penetration testing services of its kind, thanks to our highly skilled professionals and technical background.



Third-Party Risk Management and Monitoring (TPRM)

We provide evaluations of entities' response and recovery strategies and assess whether their plans adequately address the rules applicable to ICT risk management. Deloitte's TPRM framework is based on best practices and reflects global regulatory requirements. Thus, we provide a holistic solution in managing complexities within third-party ecosystems.

Feel free to contact us

Jakub Höll
Director

+420 734 353 815
jholl@deloittece.com



Martin Antoř
Manager

+420 734 783 919
mantos@deloittece.com



Viktor Paggio
Manager

+420 725 009 732
vpaggio@deloittece.com

