Developing a cybersecurity strategy

How can providers of credit referencing services develop a successful, pragmatic **cybersecurity strategy** covering the recently adopted Digital Operational Resilience Act, along with NIS2 Directive and EU Cyber Solidarity Act on the horizon?

Marta Agatowska
Chief Legal Officer, BIK

Andrzej Karpiński
Director Security Department, BIK

BIK BIG InfoMonitor DFP DigitalFingerprints

GRUPA BIK

ACCIS DATA FOR CREDIT

DORA

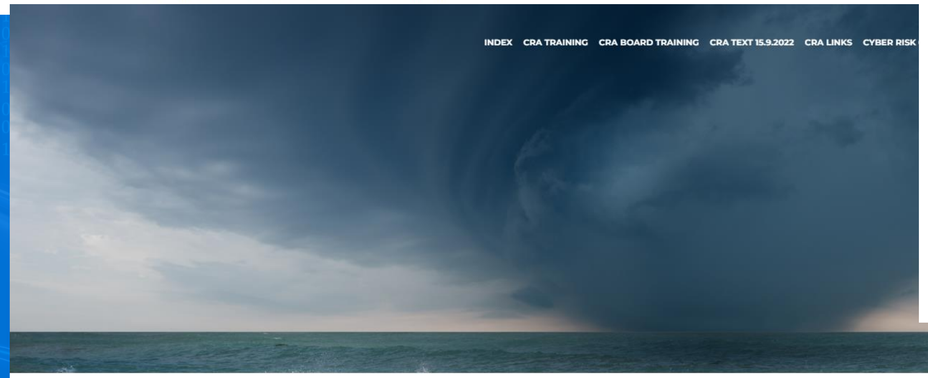
The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554

What is the Digital Operational Resilience Act (DORA)?

The Digital Operational Resilience Act (Regulation (EU) 2022/2554) solves an important problem in the EU financial regulation. Before DORA, financial institutions managed the main categories of operational risk mainly with the allocation of capital, but they did not manage all components of operational resilience. After DORA, they must also follow rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents. DORA explicitly refers to ICT risk and sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring. This Regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the entire financial system, even if there is "adequate" capital for the traditional risk categories.

According to Article 1, Subject matter:

1. In order to achieve a high common level of digital operational resilience, this Regulation lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities as follows:



NIS2

The NIS 2 Directive

December 2022 - the NIS 2 Directive was published in the Official Journal of the European Union as Directive (EU) 2022/2555.

Full name: The full name is "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)".

Deadlines: By **17 October 2024,** Member States must adopt and publish the measures necessary to comply with the NIS 2 Directive.

They shall apply those measures from **18 October 2024.**

Directive (EU) 2016/1148 (the NIS Directive) is repealed with effect from **18 October 2024.**

By **17 July 2024** and every 18 months thereafter, EU-CyCLONe shall submit to the European Parliament and to the Council a report assessing its work.

By **17 October 2024,** the Commission shall adopt implementing acts laying down the technical and the methodological requirements of the measures with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

CRA

The European Cyber Resilience Act (CRA)

Update, September 2022 - Proposed Articles of the European Cyber Resilience Act (CRA)

The proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, bolsters cybersecurity rules to ensure more secure hardware and software products.

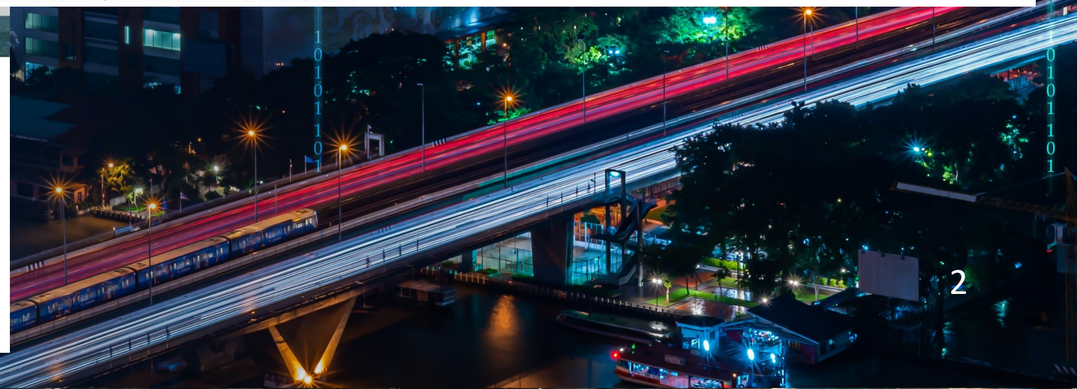
Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of €5.5 trillion by 2021.

Such products suffer from two major problems adding costs for users and the society:

- a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and

- an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

While existing internal market legislation applies to certain products with digital elements, most of the hardware and software products are currently not covered by any EU legislation tackling their cybersecurity. In particular, the current EU legal framework does not address the



NIS2 Directive
Digital Operational Resilience Act
EU Cyber Solidarity Act

https://www.digital-operational-resilience-act.com/

https://www.nis-2-directive.com/

https://www.european-cyber-resilience-act.com/

BIK BIG InfoMonitor DFP Digital Fingerprints

GRUPA BIK

ACCIS DATA FOR CREDIT

Developing a cybersecurity strategy

How can providers of credit referencing services develop a successful, pragmatic **cybersecurity strategy** covering the recently adopted Digital Operational Resilience Act, along with NIS2 Directive and EU Cyber Solidarity Acton on the horizon?

Marta Agatowska
Chief Legal Officer, BIK

Andrzej Karpiński
Director Security Department, BIK