ECESBF
Erasmus Centre of Excellence in Sustainable Business and Finance

Co-funded by the European Union

European Dimension in International Finance: Focus on digitalization and sustainability

Digital Finance Package Part II_MiCA_DORA

Academic Coordinator, Lyudmila Muradova

Background

Under the legislation, not only must crypto companies keep the public informed about their pricing process and trading volumes in real time, but they must settle all trades the same day those trades happen. Exchanges must keep separate their own funds, including crypto, and funds belonging to their clients. The regulation also explicitly prohibits insider trading.

Most importantly, MiCA introduces a universal licensing approach for all EU member states, making it the most comprehensive legislation of its kind anywhere in the world.

MiCA is intended to close gaps in existing EU financial services legislation by establishing a harmonized set of rules for crypto-assets and related activities and services. Among other things, MiCA imposes restrictions on the issuance and use of stablecoins.

The rules for stablecoins will start applying after a transitional period of 12 months and could hence take effect from spring 2024

MiCA clarifications:

- Tokens defined as ‘financial instruments’ will be subject to the existing financial services rules (in particular, MiFIR / MiFID II).
- Tokens defined as ‘crypto-assets’ will be subject to to the bespoke pan-EU regime established by MiCA.
- Introduces rules regarding regulated crypto-asset services, including authorisation, passporting and ongoing supervision requirements for crypto-asset issuers (CAIs) and crypto-asset service providers (CASPs).

Products in scope

MiCA regulates activities involving "crypto-assets." The term crypto-asset is broadly defined as any "digital representation of a value or a right which may be transferred and stored electronically, using distributed ledger technology or similar technology" (Art. 3 (1) No. (2) MiCA). MiCA introduces three sub-categories of crypto-assets that are subject to different requirements adjusted to the risks they entail:

"Electronic money tokens" or "e-money tokens" (EMTs) are crypto-assets that purport "to maintain a stable value by referencing to the value of one official currency" (Art. 3 (1) No. (4) MiCA). Like traditional e-money, EMTs are electronic surrogates for coins and banknotes and are likely to be used for payment purposes.

"Asset-referenced tokens" (ARTs) aim "to maintain a stable value by referencing to any other value or right or a combination thereof, including one or more official currencies" (Art. 3 (1) No. (3) MiCA). For example, ARTs could be backed by a basket of different fiat currencies, commodities or crypto assets.

The third sub-group is a catch-all category for **all other crypto-assets** that are not EMTs or ARTs, which thus covers a wide variety of crypto-assets, including non-pegged payment tokens (*i.a.*, cryptocurrencies like Bitcoin or Ether) and utility tokens. MiCA lays down a few specific rules for utility tokens, defined as “a type of crypto-asset which is only intended to provide access to a good or a service supplied by the issuer of that token” (Art. 3 (1) No. (5) MiCA).

Services in scope

The services governed by MiCA are largely similar to MiFID regulation and trigger a licensing requirement for CASPs. These include:

- custody and administration of crypto-assets on behalf of third parties;
- operation of a trading platform for crypto-assets;
- exchange of crypto-assets for funds (i.e. fiat and other currencies);
- exchange of crypto-assets for other crypto-assets;
- execution of orders for crypto-assets on behalf of third parties;
- placing of crypto-assets (any marketing on behalf of, or for the account of, the offeror);
- providing transfer services for crypto-assets on behalf of third parties;
- reception and transmission of orders for crypto-assets on behalf of third parties;
- providing advice on crypto-assets;
- providing portfolio management on crypto-assets (i.e. where portfolios include one or more crypto-assets)

MiCA (in-scope)

Asset-referenced tokens (ART)

- Tokens aiming to maintain a stable value by referencing one or several assets, including fiat currencies, crypto-assets or commodities.

Electronic money tokens (EMT)

- DLT equivalents for coins and banknotes and used as payment tokens. EMTs must be backed by one fiat currency which is a legal tender.

Other crypto-assets

- Tokens with a digital representation of value or rights which may be transferred and stored electronically.
- Utility tokens which provide access to a good or service and only accepted by the issuer of that token.
- Payment tokens which are not EMTs or security tokens.

MiCA-out of scope

EU financial instruments (regulated elsewhere)

- Digital assets governed by the existing financial services rules, as amended, including security tokens and derivatives on crypto-assets.

Other digital assets (including)

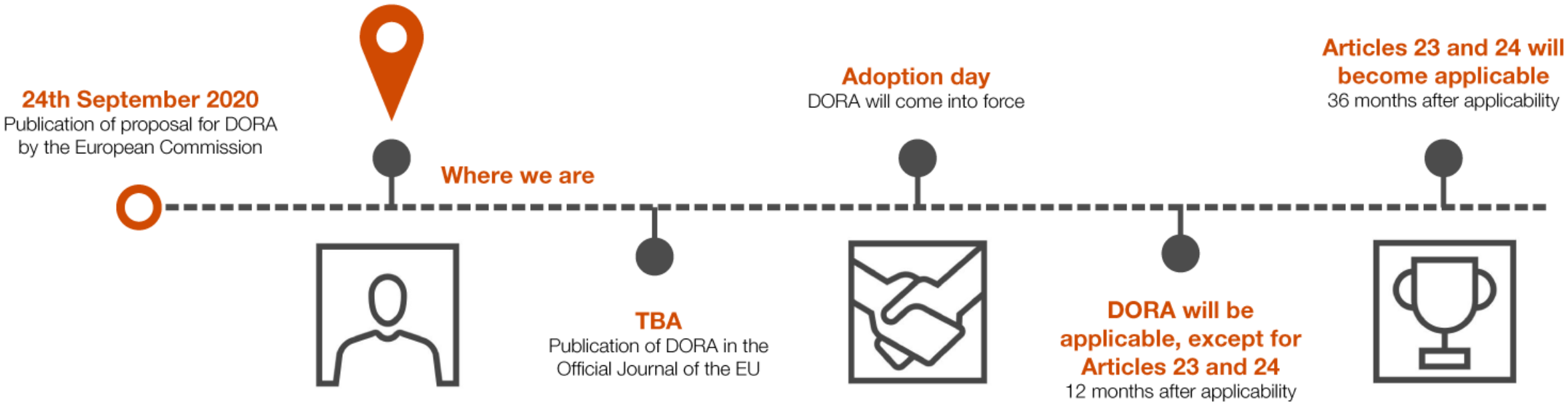
- Digital assets which cannot be transferred, are offered for free or are automatically created
- Central bank digital currencies (CBDCs)
- Non-fungible tokens (NFTs)
- Decentralised finance (DeFi) protocols

The Digital Operational Resilience Act. Background

The EU's aim with DORA is that of strengthening the financial sector's resilience to ICT-related incidents and introduces very specific and prescriptive requirements that are homogenous across EU member states. Critical ICT third-parties which provide ICT-related services to financial institutions, such as cloud platforms, data analytics and audit services, are also subject to this new regulation.

This act provides a very specific set of criteria, templates and instructions that will shape how financial organisations manage ICT and cyber risks. It demonstrates that EU regulators want to be very hands-on on the topic, with a considerable emphasis on reporting, communication, and assessments that need to take place on a frequent basis, enabled by standardised formats. As such, a single consistent supervisory approach will be adopted across the relevant sectors.

The Regulation on digital operational resilience for the financial sector, also known as the Digital Operational Resilience Act or DORA, was published in the Official Journal of the European Union on 27 December 2022. The Regulation entered into force on 16 January 2023 and will apply from 17 January 2025.

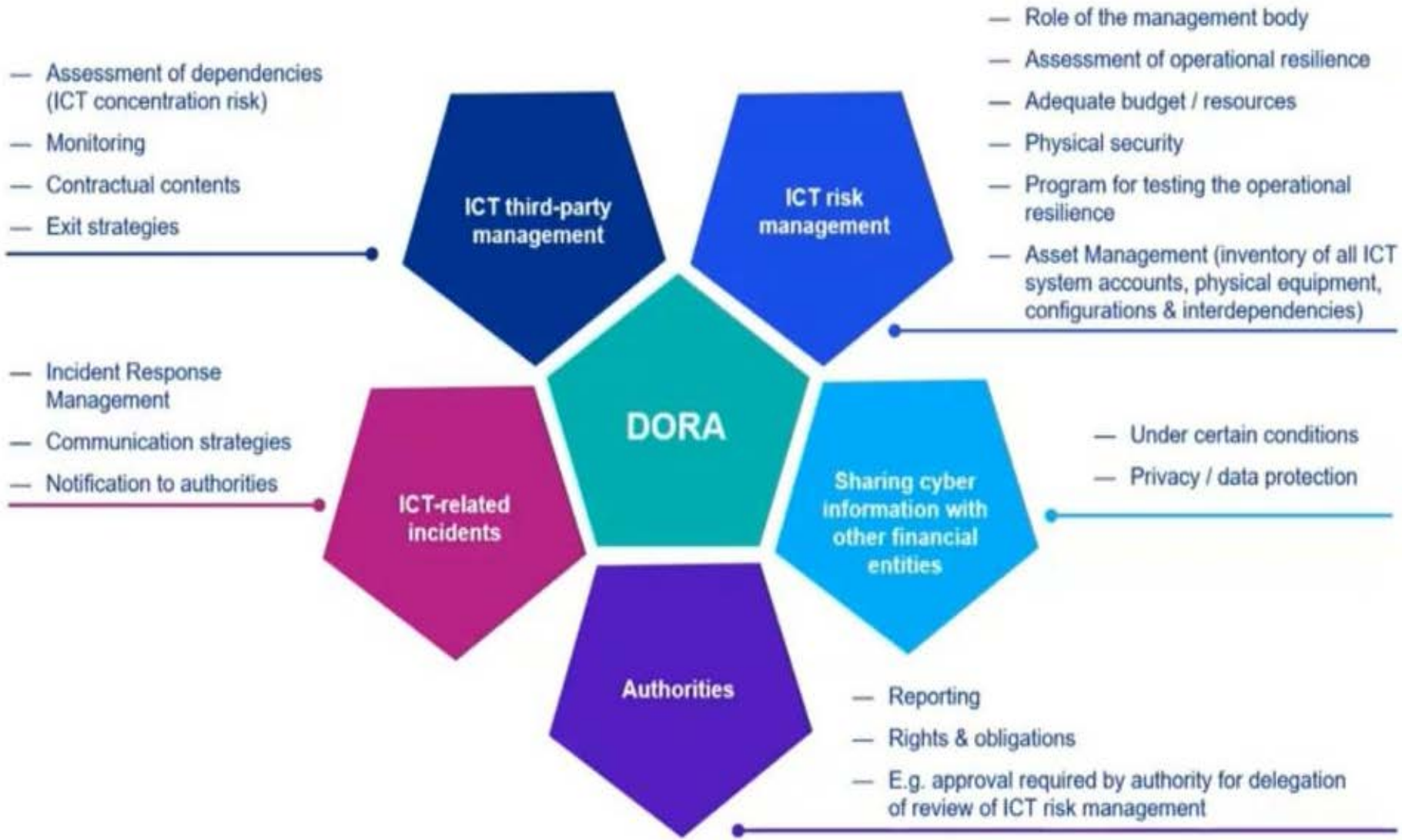


https://www.pwc.com/mt/en/publications/technology/dora.html

https://kpmg.com/fi/fi/home/Pinnalla/2021/08/digital-operational-resilience-act-dora.html

The essence of DORA is divided across **5 core pillars** that address various aspects or domains within ICT and cyber security, providing a comprehensive digital resiliency framework for the relevant entities

- ICT risk management
- ICT-related incident reporting
- Digital operational resilience testing
- ICT third-party risk
- Information sharing


— Assessment of dependencies (ICT concentration risk)
— Monitoring
— Contractual contents
— Exit strategies
ICT third-party management
ICT risk management
— Role of the management body
— Assessment of operational resilience
— Adequate budget / resources
— Physical security
— Program for testing the operational resilience
— Asset Management (inventory of all ICT system accounts, physical equipment, configurations & interdependencies)
— Incident Response Management
— Communication strategies
— Notification to authorities
ICT-related incidents
DORA
Sharing cyber information with other financial entities
— Under certain conditions
— Privacy / data protection
Authorities
— Reporting
— Rights & obligations
— E.g. approval required by authority for delegation of review of ICT risk management

ICT risk management

The proposal establishes a set of requirements on the ICT risk management framework, including:

- Set-up and maintain resilient ICT systems and tools that minimize the impact of ICT risk.
- All sources of ICT risks should be continuously identified in order to set-up protection and prevention measures.
- A prompt detection of anomalous activities should be established.
- Dedicated and comprehensive business continuity policies and disaster and recovery plans should be in place, ensuring a prompt recovery after an ICT-related incident.
- Establish mechanisms to learn and evolve both from external events as well as the entity's own ICT incidents.

ICT-related incident reporting

- Establish and implement a management process to monitor and log ICT-related incidents.
- Classify the incident according to the criteria detailed in the regulation and further developed by the ESAs including EBA, EIOPA and ESMA.
- Ensuring the reporting of incidents to the relevant authorities using a common template and a harmonised procedure as established by the respective supervisory authority.
- Submit initial, intermediate and final reports on ICT-related incidents to the firm’s users and clients.

Digital operational resilience testing

- Elements within the ICT risk management framework should be periodically tested for preparedness.
- Any weaknesses, deficiencies or gaps must be identified and promptly eliminated or mitigated with the implementation of counteractive measures.
- Digital operational resilience testing requirements must be proportionate to the entities' size, business and risk profiles.
- Conduct Threat Led Penetration Testing (TLTP), also known as a Red / Purple Team Assessment, to address higher levels of risk exposure.

ICT third-party risk

- Ensure sound monitoring of risks emanating from the reliance on ICT third-party providers.
- Harmonising key elements of the service and relationship with ICT third-party providers to enable a ‘complete’ monitoring.
- Ensure that the contracts with the ICT third-party providers contain all the necessary monitoring and accessibility details such as a full service level description, indication of locations where data is being processed, etc.
- Promote convergence on supervisory approaches on the ICT third-party risks by subjecting the service providers to a Union Oversight Framework.

Information sharing

The guidelines encourage collaboration among trusted communities of other financial entities. This collaboration will:

- enhance the digital operational resilience of financial entities
- raise awareness on ICT risks
- minimise ICT threats' ability to spread
- support entities' defensive and detection techniques, mitigation strategies or response and recovery stages.

Financial entities are encouraged to exchange amongst themselves cyber threat information and intelligence through arrangements that protect the potentially sensitive nature of the information shared.

- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593
- https://www.cnbc.com/2022/12/07/crypto-regulation-europes-mcguinness-pushes-for-global-rules-after-ftx-collapse.html#:~:text=The%20European%20Union%20agreed%20in,start%2012%20months%20from%20now.
- https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_7529
- https://www.akingump.com/en/news-insights/eu-close-to-introducing-groundbreaking-law-to-regulate-crypto.html
- https://www.mayerbrown.com/en/perspectives-events/publications/2022/12/eu-markets-in-crypto-assets-mica-regulation-expected-to-enter-into-force-in-early-2023
- https://www.coindesk.com/consensus-magazine/2023/01/24/european-union-mica-crypto-regulation/
- https://www.pwc.com/gx/en/new-ventures/cryptocurrency-assets/pwc-global-crypto-regulation-report-2023.pdf
- https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/
- https://www.digital-operational-resilience-act.com/
- https://kpmg.com/fi/fi/home/Pinnalla/2021/08/digital-operational-resilience-act-dora.html
- https://www.pwc.com/mt/en/publications/technology/dora.html
- https://www.linklaters.com/en/insights/blogs/fintechlinks/2018/march/european-commission-fintech-action-plan