This is the European Union: A new era in digital regulation

May 2021

ALVAREZ & MARSAL
LEADERSHIP. ACTION. RESULTS.℠

Preparing for the challenges and opportunities ahead

CONFIDENTIAL – NOT FOR DISTRIBUTION

This is the European Union: A new era in digital regulation

Preparing for the challenges and opportunities ahead

The European Commission has published key legislative proposals as part of its digital strategy.

- The **Digital Services Act (DSA)** proposes a common set of rules for online intermediaries where users have their place of main establishment or residence in the EU to promote a safe and accountable online environment.
- The related **Digital Markets Act (DMA)** seeks to establish rules for major 'gatekeeper' platforms, aiming to deliver fair and open digital markets.
- As part of the **European data strategy**, **the Data Governance Act (DGA)**, proposes a largely voluntary framework for trusted and strengthened data sharing across the EU, in both the public and the private sectors.

The **financial sector** is front and centre in obtaining the benefits of a **global shift** to data-fuelled operations. The financial sector is using data to **increase customer services** and other significant goals such as **improving fraud detection**.

As a result, digital transformation programmes have been intensifying over the last few years to help manage safely and securely this ever-growing amount of data.

Digital Operational Resilience [Act] for the **financial sector** or **'DORA'** (2020/0266 (COD) Legislative Proposal) is a Proposed [1] European Parliament Act aimed at laying down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities, with a view to achieve a high-level of digital **operational resilience within the financial sector**.

Note:
1. The Proposed Act is in the adoption process currently with no defined deadline communicated by the EU. It is expected (unofficial estimates) that the adoption process will span 18-24 months starting December 2020.

This is the European Union: A new era in digital regulation

Preparing for the challenges and opportunities ahead

DORA aims to put into place a comprehensive **framework which shall enhance digital risk management, strengthen and streamline the financial entities conduct of ICT risk management**, establish a thorough testing of ICT systems, increase supervisors awareness of cyber risks and ICT-related incidents faced by financial entities, as well as introduce powers for financial supervisors to oversee risks stemming from financial entities dependency on ICT third-party service providers.

Increased threat of cyber attacks and ICT disruption

Use of digital, or Information and Communication Technologies (ICT) has in the last decades gained a pivotal role in finance, assuming today critical relevance in the operation of typical daily functions of all financial entities. While giving rise to opportunities, these have introduced risks giving rise to increased threat of cyber attacks and ICT disruption.

Detailed and comprehensive framework

The absence of detailed and comprehensive rules on digital operational resilience at an EU level has fragmented the single market, undermined the stability and integrity of the EU financial sector and jeopardised the protection of consumers and investors. DORA is an attempt to put in place a detailed and comprehensive framework on digital operational resilience for EU financial entities.

The key requirements and considerations encapsulated within DORA can be summarised into five headline themes

A&M's Cyber Risk Practice have laid out a three step plan to support organisations as they look to align against the DORA requirements

DORA headline themes

To ensure consistency around the ICT risk management requirements applicable to the financial sector, the proposed regulation shall **cover a range of financial entities regulated at union level**.

It is envisioned that such a coverage will facilitate a **homogenous and coherent application of all the components of the risk management on ICT-related areas**, while safeguarding the level playing field among financial entities in respect of their regulatory obligations on ICT risk.

Governance

Better alignment between financial entities business strategies and the conduct of the ICT risk management. The management body shall be required to maintain a crucial, active role in steering the ICT risk management framework and pursue to respect a strong cyber hygiene posture.

ICT Risk Management

Inspired from relevant international, national and industry-set standards, guidelines and recommendations, the requirements revolve around specific functions in ICT risk management (identification, protection and prevention, detection, response and recovery, learning and evolving and communication).

ICT Incident Reporting

Creation of a consistent incident reporting mechanism that will help to reduce administrative burdens for financial entities and strengthen supervisory effectiveness. The reporting shall be processed using a common template and following a harmonised procedure as developed by the ESAs.

Digital Operational Resilience Testing

Proportionate application of periodic digital operational resilience testing requirements, covering preparedness and identification of weaknesses, deficiencies or gaps, as well as the prompt implementation of corrective measures, depending on the size, business and risk profiles of financial entities.

Information Sharing

To raise awareness on ICT risk, minimise its spread, support financial entities defensive capabilities and threat detection techniques, the proposed regulation shall allow financial entities to set-up arrangements to exchange cyber threat information amongst themselves and intelligence through trusted environments.

Who?

What next?

DORA EU adoption process

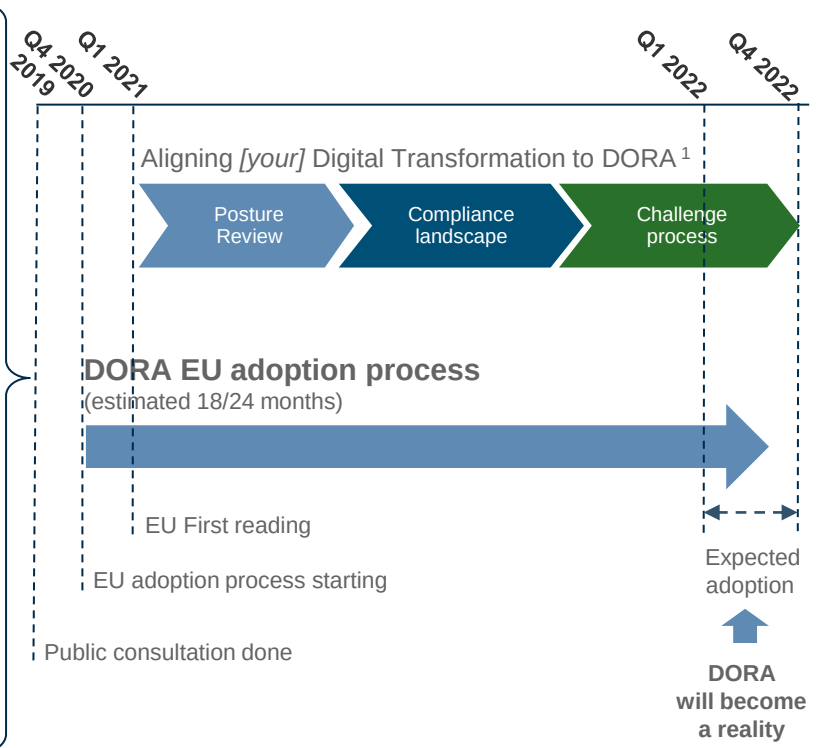
Opportunity to ease the achievement

While the EU commission is proceeding with adoption process, the targeted companies could take advantage to start a proper trajectory. The main goal will be to evaluate all the *(potential)* gaps and include the remediation actions in their own digital programmes *(Digital Services Act, Digital Market Act)* and strategic planning.

The estimated timeline of 18/24 months *(unofficial estimate)* is good to prepare and deliver a multi-step journey, avoiding any effort compression and justifying the roadmap by business risk reduction, including investment alignment with the annual budget.

Entities impacted *when DORA in force*

- Credit institutions
- Trading venues
- Institutions for occupational retirement pensions
- Payment institutions
- Trade repositories
- Credit rating agencies
- Electronic money institutions
- Managers of alternative investment funds
- Statutory auditors and audit firms
- Investment firms
- Management companies
- Administrators of critical benchmarks
- Crypto-asset service providers
- Issuers of crypto-assets
- Issuers of asset-referenced tokens
- Issuers of significant asset-reference tokens
- Central securities depositories
- Central counterparties
- Data reporting service providers
- Insurance and reinsurance undertakings, intermediaries and ancillary insurance intermediaries
- Crowdfunding service providers
- ICT third party providers
- Securitisation repositories



Note:

1. The Proposed Act is in the adoption process currently with no defined deadline communicated by the EU. It is expected (unofficial estimates) that the adoption process will span 18-24 months starting December 2020.

Aligning [your] digital transformation to DORA

A&M's experienced professionals can support organisations through a three-step journey as they look to align against the proposed [1] DORA requirements.

	1. Review of current digital environment	2. Evaluate the compliance [1] landscape	3. Challenge the process
DORA Topics Covered	**Understanding the readiness of all the "building blocks:** • ICT/digital company's landscape • ICT risk management framework • Information sharing operating model • ICT third-party providers risk • Oversight of third-party providers (including outsourcing) • Multi-vendor and interoperability requirements	**Evaluate the status of current requirements, and gap assess against the expected target posture** • EU NISD2 Directive • European Banking Authority (EBA) guidelines on outsourcing arrangements • European Insurance and Occupational Pensions Authority (EIOPA) guidelines on outsourcing to cloud service providers • European Securities and Markets Authority (ESMA) cloud outsourcing guidelines • European Central Bank (ECB) Regulation no. (ECB/2014/28) on oversight requirements for systemically important payment systems • ECB Cyber resilience oversight expectations for financial market • International Organisation of Securities Commissions (IOSCO) principles on outsourcing • Basel Committee on Banking Supervision (BCBS), Sound Practices: implications of fintech developments for banks and bank supervisors, 2018 • Financial Stability Board (FSB) consultation on effective practices for cyber incident response and recovery • FSB, Third-party dependencies in cloud services: considerations on financial stability implications	**Evaluate the consistency of the incident management process mechanism;** **Evaluate any potential hidden gaps and/or synergies with shared 'digital environments' (e.g., services providers, parent companies, etc.)** • ICT and security incident reporting requirements • Processes Testing (mainly incident related ones: ICT, Cyber, etc.) • Consistence of processes and governance related to payment systems and schemes. Certifications included (e.g., PCI-DSS, ISO 27001, etc.)

Note:
1. The Proposed Act is in the adoption process currently with no defined deadline communicated by the EU. It is expected (unofficial estimates) that the adoption process will span 18-24 months starting December 2020.

A&M people

Lorenzo Grillo

Managing Director, Head of EMEA Cyber Risk Services team

- With more than 30 years of experience in Information Technology (IT) and 25 years of experience in information security, Mr. Grillo has advised the top management and board of directors of many enterprise organisations and private equity firms on sell-side and buy-side due diligences and risk assessment for their portfolio companies.
- Mr. Grillo's notable assignments include helping several financial services organisations' management teams justify cybersecurity investments by leading an information security risk evaluation and developing, and then implement, a program to mitigate business risks in case of data confidentiality, integrity and availability loss. He led the global European information security organisation and skill assessment for a leading insurance company. Mr. Grillo also improved a European bank's ability to manage incident detection and response effectively and efficiently.
- Experience across various industries, including financial services, telecommunications, manufacturing, retail, healthcare, energy and utilities, media and technology.

Angshuman Rajkhowa

Managing Director, Financial Industry Advisory Services

- With more than 18 years of extensive banking experience, Mr. Rajkhowa has previously worked in several large global banks including – Royal Bank of Scotland, ABN AMRO, Standard Chartered, Australia and New Zealand Banking Group and Citicorp across Europe, Asia and the Middle East.
- Mr. Rajkhowa has a proven track record of developing and delivering non-conventional solutions to meet customer needs. Skilled at working with multinational teams in numerous locations to strategies, develop and implement solutions and Services. He has held leaderships positions in Strategy, Product Management, Project & Vendor Management, Operations, Client Service and Business Management & Planning.
- Mr. Rajkhowa served on the Management Board of Global Transaction Services during the separation/integration of ABN/RBS, representing Strategy & Business Planning and was member of the Transaction Services Risk Committee.

Libero Marconi

Director, EMEA Cyber Risk Services team

- With more than 26 years of experience in Information Technology (IT) and 21 years of experience in Cybersecurity, Mr. Marconi has played roles of Board member and CTO of two leading Italian Certification Authorities. He also provided managing advisory for several Certification Authorities in Germany, Denmark, Spain and Brazil, with deep knowledge of eIDAS EU regulation, Swiss ZertES and accreditation process of Qualified Trust Service Providers.
- Mr. Marconi's notable assignments include helping several financial institution in review their cyber security investments, leading Cybersecurity risk evaluation and designing the operational model, including the establishment of Information Security Organisation and Governance, Risk and Compliance Management.
- Experience across various industries, including financial services, telecoms, aerospace, manufacturing, pharmaceutical, energy and utilities, technology, e-government and smart card manufacturer.

A&M cyber security experience

A&M professionals have experiences in several market sectors and countries

Corporate

- **Financial services organisation:** complete cyber risk evaluation for all the business lines, cyber organisation and skill assessment, three-year roadmap to mitigate cyber risk, integration with Operational Risk framework.
- **Various payment companies:** cyber security risk evaluation to help the CEO to properly manage their cyber risk, including cyber risk framework definition, business impact and threat assessment, NIST control assessment, detailed three-year roadmap, interim CISO role.
- **Leading European insurance:** Security organisation and process assessment to analyse the security resources (internal and external) skill sets and their activities in each of the company sites in Europe, evaluate the current organisation and processes, provide a possible structure optimisation.
- **Telco Group:** Information Security assessment and integration roadmap of different security companies inside the Telco group, including SIEM platform analysis, security services by each company and security vendor partnerships, to obtain a blueprint of the target services proposition, the target architecture (hardware and software), and the target number of SOCs and the related people (amount and skills).
- **Global pharmaceutical company:** Assessment of the security (logical and physical) impacts and threats for one of their leading production site, obtaining a three-year security roadmap to mitigate business risks for that plant.

Private equity

- **Sell-side and buy-side DDs:** analysis of the security postures of various companies.
- **Rapid cyber security assessments:** cyber security assessment on anti-malware in different portfolio companies for a Private Equity firm, comparing the status with a market benchmark and make some recommendations and quick wins.
- **Cyber risk evaluation and organisation assessment:** complete cyber risk evaluation with multi-year roadmap to mitigate risk for various portfolio companies in fintech, technology, manufacturing, services and financial sector.
- **Interim roles:** Shadow management or interim roles (e.g. CISO) to implement and govern the cyber strategy and the related program of the portfolio company.
- **Breach response:** certified by the National Security Agency as a Critical Incident Response Assistance (CIRA) firm, cyber crisis management including cyber war room management, root-cause forensics and executive advisory services.

0000