Sponsored briefing: The Digital Operational Resilience Act: the next chapter for cyber resilience in the EU financial sector

27 October 2023 09:00am | Guest Blog

Cyber security | VdA | Co-publishing

THE WHAT AND WHY OF DORA

The EU's financial sector is counting down towards a major legal document aimed at addressing cyber security concerns within this sector.

Since the consolidation of the digital era, cyber security has come under unprecedented focus, and EU legislative bodies have been working on establishing a solid framework that involves all market players, and that globally requires a proactive and adaptive approach to the increasing, evolving, and challenging dangers of cyber threats.

This includes, for example, the 2020 EU Cybersecurity Strategy (which aims to ensure a global and open digital society in Europe), and NIS 2 (which must be transposed by member states by 17 September 2024, and which replaces and repeals the Network and Information Security Directive, setting a new baseline for cyber security risk management and reporting).

The EU has also assumed as a priority the need to regulate cyber concerns in the financial sector, a highly regulated sector that routinely handles high-risk information, relies increasingly on innovative technological solutions (quite often through third-party service providers), and is a long-established target of technological threats, which may potentially have a critical financial, operational, and reputational impact.

In this context, stakeholders in the financial sector are now at the centre of a new, major, EU regulatory instrument: the Digital Operational Resilience Act (DORA).

DORA, which was approved in December 2022, entered into force in January 2023 and will be applicable throughout the EU from 17 January 2025 onwards to all relevant stakeholders in the financial sector such as, for example, credit and payment institutions, insurance and reinsurance undertakings, credit rating agencies, statutory auditors and audit firms, and ICT service providers.

As an EU Regulation, DORA will be directly applicable and does not require formal transposition by each member state into national law.

This currently gives these financial entities just over a year to prepare their structure, systems, corporate culture and compliance strategies for major adjustments to their cyber ecosystem – in practice, a 'just around the corner' deadline, if we consider the full scope and impact of DORA on entities within all the financial ecosystem, and spread over six major pillars, each with specific obligations and requirements.

DORA's six pillars set up obligations which require collaboration between legal, IT, compliance and commercial departments, as they force financial entities to conform in matters of: (1) governance and organisation; (2) ICT risk management; (3) ICT incidents; (4) resilience testing; (5) third-party ICT risks; and (6) information sharing.

Under these strategic pillars, financial entities are subject to various obligations:

Governance and organisation

Financial entities must implement internal governance and control frameworks that ensure effective and prudent management of all ICT risks, and create monitoring roles for arrangements with ICT third-party service providers .

They must also adjust the role of management bodies, which are responsible (and accountable) for defining, approving and overseeing arrangements related to the ICT risk management framework. They must engage in training to ensure sufficient know-how on ICT risks and their operational impact, must keep informed on arrangements with third-party ICT service providers, and must allocate budget to fulfil digital resilience needs.

ICT risk management framework

Financial entities must also prepare a solid, comprehensive and adequate ICT risk management framework (including a digital resilience strategy) to address ICT risks, and ensure high-level digital operational resilience according to the entity's needs, size and complexity.

This includes preparing appropriate strategies, policies, procedures, protocols and tools under this ICT risk management framework (subject to specific DORA requirements), with high standards of data security, confidentiality and integrity. These documents should address, among other topics, possible disclosure of ICT-related incidents or major vulnerabilities to clients, counterparts and the public.

They must also segregate ICT management, control, and internal audit functions, and manage cyber threats and ICT incidents by implementing anomalous activities/incidents detection mechanisms, an adequate ICT business continuity policy, backup policies and recovery methods, carrying out post-incident reviews and ensuring adequate staffing and internal monitoring.

Financial entities must also incorporate regulatory guidelines on information security/ICT controls.

ICT incident management, classification and reporting

Financial entities must ensure an ICT-related incident management process to detect, manage, monitor, follow-up and notify ICT-related incidents, and classify ICT-related incidents and their impact, based on specific criteria.

DORA requires for financial entities to report major ICT-related incidents to (i) the relevant regulator, within specific timeframes and parameters; and (ii) when these incidents have (or may have) an impact on the financial interests of service users and clients, also inform them of the incident and of the measures taken to mitigate adverse effects.

Digital operational resilience testing

Financial entities must prepare a digital operational resilience testing program under a risk-based approach, incorporating appropriate testing and vulnerability assessments.

Third-party provider risk management

DORA requires the Integrating of ICT third-party risk as an integral component of ICT risk within the ICT risk management framework.

This includes, among other provisions: (i) assuming responsibility for DORA compliance in arrangements with third-party ICT service providers; (ii) adopting and reviewing a strategy on third-party ICT risk; (iii) formalising the relationship with ICT providers in a contract with specific content, including service levels; (iv) maintaining a register of all ICT service contracts; (v) reporting to competent authorities, at least annually, on the number of new ICT service arrangements, categories of providers, type of contract and services/functions provided; (vi) ensuring that the ICT providers comply with high security standards and auditing/inspecting these providers, and terminating the contract if certain circumstances take place.

Information sharing

Financial entities may exchange cyber threat information and intelligence among themselves, if this enhances their digital operational resilience, takes place within a trusted community, and is done under information-sharing arrangements that protect the potentially sensitive nature of the information.

WHAT NOW? HOW TO PREPARE FOR DORA

DORA's provisions have a wide range of application, both in scope and intensity, and is bound to have an overarching impact on the market.

At this stage, two sets of main players are central to DORA's incorporation into the EU financial ecosystem.

The first set of protagonists will be the European supervisory authorities, which will, on the one hand, be essential in applying DORA proportionately and fairly, taking into account various factors (including the type, nature and dimension of each financial entity) when enforcing DORA – certain national regulators have already manifested concerns with the need to ensure that DORA does not result in disproportionate, unequal or unfair scenarios for different types of financial entities.

On the other hand, they are responsible for establishing legal and technical standards that will guide, detail and clarify the terms of application of legal, operational and technical DORA requirements. This market dialogue has already started: EBA, EIOPA and ESMA launched a public consultation on the first batch of policy products under DORA, including four draft regulatory technical standards, and one set of draft implementing technical standards. Inputs were received until 11 September 2023, and conclusions are underway.

The second set of DORA protagonists are financial entities themselves, for which 2024 will be a crucial year. To this effect, financial entities must focus on creating a DORA compliance programme – including, at least, the following steps:

1. Team onboarding: Creating a DORA taskforce that involves top legal, IT, financial and compliance decision makers, to ensure an across-the-board approach. Crucially, management must be actively involved: with DORA placing a focus on management and for a shift in corporate culture and governance, a top-down approach is key.

2. Logistics and financials: Allocating budget and preparing a compliance roadmap.

3. Cleaning house:

(a) Identifying all existing/necessary documentation, including arrangements with third-party ICT service providers, internal policies and strategies, contractual templates, engagement policies with regulators, clients, users, counterparties and the market. Identifying relevant systems, IT protocols, software licences and other cyber-sensitive resources.

(b) Preparing/adjusting internal and external documentation.

4. Third-party arrangements: Given DORA's focus on contractual compliance and on third-party ICT providers' standards, specific attention needs to be given to preparing/adjusting/renegotiating contractual templates for ICT providers, and to the possible renegotiation or termination of contracts. Financial entities must also establish new minimum legal and technical criteria for engagement with service providers.

5. Team awareness: Setting up internal training programmes, considering seniority, responsibility and roles within the financial entity. DORA requires the creation or adjustment of specific legal, technical and compliance roles, and training is essential.

6. Incorporating the whole legal ecosystem: Ensuring that the DORA compliance strategy is compatible with, and takes into consideration, other applicable legal instruments, such as the General Data Protection Regulation and sector-specific legislation and EBA guidelines.

7. Participating in the process: Given that certain DORA provisions are to be developed by the competent supervisory authorities, financial entities must pay attention to stakeholder discussion, awareness and training initiatives on DORA (including public consultations launched on DORA standards and interpretation).

In a nutshell, DORA is set to represent a shift in paradigm for digital resilience in the financial sector, with a focus that will no longer be solely on the general concept of compliance, but rather on 'resilience' and on keeping up with the times in what concerns cyber threats – with all this entails in terms of internal preparation and culture shifting.
Financial entities must be aware, prepared and ready to go for DORA, starting on January 2025. This will require a multi-disciplinary approach and a clear strategy towards a legal act that requires an 'all-in' attitude towards digital resilience but can't be achieved through a 'one size fits all' approach. An individual, personalised, business-sensitive compliance programme must be implemented by all DORA subjects – sooner rather than later.

For more information, please contact:

Inês Antas de Barros joined VdA in 2007. Partner of the information, communication and technology practice area, she focuses her practice on electronic communications, information technology and privacy and information security. In such capacity, she has been involved in data privacy and other similar projects which raise complex issues across multiple jurisdictions and/or legal or regulatory areas (including health, pharmaceutical, insurance, banking and telecommunications).

Such projects include conducting data protection risk management reviews; dealing with international flows of personal data; advising on the implementation of privacy compliance programmes; the roll-out of a global whistleblower hotline; drafting privacy policies, codes of conducts, cross-border data transfer agreements, charters for the use of information and communication methods as well as guidance for data privacy officers.

Isabel Ornelas joined VdA in 2006. Managing associate of the information, communication and technology practice area. In such capacity she has been involved in several transactions, in Portugal and abroad.

She has worked in particular in the field of privacy and data protection, having taken an active role in several privacy compliance audits carried out by companies in various sectors (in particular, banking and finance, health, insurance and telecommunications), in the set-up of privacy policies and ethics lines, as well as providing project-oriented legal counselling in various operations and market products and services, particularly those including international data transfer.

She also organised training sessions and workshops.

www.vda.pt/en