# Cyber and digital operational resilience: DORA implementation and international cyber-resilience initiatives

## 1. Ensuring cyber and digital operational resilience is increasingly challenging

The Chair emphasised that cyber risk and resilience are live topics for regulators and industry executives. Among their main concerns is the risk of a major cyber-attack. This is a challenging area of work. It is highly technical and possesses complex risks. The environment is also rapidly changing. As financial activities become more tech-driven, cyber and digital operational resilience challenges become ever greater. The attack surface is very large and the vectors are very fast moving. These risks are cross-sectoral as well, requiring an evolution of traditional risk management approaches. The growing importance of outsourcing and of third-party service providers presents a further challenge.

An industry representative remarked that delivering trust to consumers and businesses in Europe and around the world, which is the objective of payment schemes in particular, is increasingly challenging. The first level of trust for payment schemes is ensuring that the system works every time a customer executes a payment domestically or across borders. To deliver that consistently on a global basis requires significant infrastructure and systems operating in triplicate. Moreover, it is crucial to safeguard the system against cyber threats, ensuring its availability and the integrity of the data processed, in a landscape that is perpetually evolving. Substantial investments in cybersecurity are imperative, covering both IT and staff aspects. A global outlook is needed also, as most cybersecurity threats are cross-border. In addition, customers have to be protected from fraud. The debate on fraud predominantly focuses on what needs to be done after it occurs but the priority should be prevention. In Europe, thanks to the Payment Services Directive (PSD2), fraud rates have come down by about 20% over the last couple of years, but fraudsters continue to innovate.

A supervisor noted that though there has so far not been a major destabilising cyber-attacks directed at the European banking sector, the risks are real. The geopolitical situation has led to an increased threat level. In certain countries, there are frequent attacks by certain governmental parties. The highest increase is in distributed denial of service (DDoS) attacks. There is also an increase in attacks on third-party providers (TPPs) as attackers have managed to exploit vulnerabilities. Ransomware is a major threat as well, as it can disrupt critical services.

## 2. DORA implementation progress

### 2.1 Objectives and specificities of DORA

A regulator emphasised that the Digital Operational Resilience Act (DORA), which aims to enhance the operational and cyber-resilience of the financial sector is a ground-breaking regulation, which adopts a cross-sector approach and covers about 20 different types of financial entities. DORA addresses areas that are critical for firms, like information and communications technology (ICT) risk management, ICT incident management, resilience testing, management of third-party risks and stress testing.

That involves strengthening the approaches and the risk management capabilities of the financial entities concerned. An oversight of the most critical TPPs (CTPPs) that service financial entities is also being built across sectors. For those TPPs, the oversight task will be devolved to the European Supervisory Authorities (ESAs).

### 2.2 Progress made in the drafting and adoption of Level II requirements

A regulator detailed that there has been extensive consultation on the first batch of regulatory standards, which was submitted to the European Commission in January 2024. This involved close consultation with the private sector and all of the competent authorities. The first consultation on ICT risk management and incident reporting led to the identification of a number of issues in terms of proportionality, complexity and the level of prescriptiveness in the requirements. ICT risk management is a broad topic, so being proportionate is not easy. The consultation on incident classification was very beneficial and allowed a revision of the thresholds to ensure that smaller and non-complex entities are subject to proportionate requirements. Detailed work is needed on the register of information which concerns the contracts that financial entities have with TPPs. Designating the CTPPs, which are critical from a systemic perspective, will be key. This designation is being prepared gradually, with the objective of starting the oversight in January 2025.

The second batch of regulatory standards will be consulted on until the end of March 2024 and then submitted to the Commission in July. This covers aspects such as incident reporting, subcontracting and threat-led penetration testing (TLPT), which require fine-tuning. In terms of how this guidance fits with existing ESA guidance, the setup will supersede the entire set of existing guidelines and requirements in order to avoid duplications and overlaps.

A Central Bank official noted the importance of on-going consultations involving market participants in

order to identify the issues on which further clarity is needed. Different tools, such as Q&As will be provided to achieve this.

### 2.3. Conditions for the success of DORA

#### *2.3.1 Future-proofing*

A regulator noted that this is a fast-evolving environment. Requirements must be designed to be future-proof, in order to accommodate future developments in a smooth and easy manner.

An industry representative agreed that the regime must be future-proof and also practically implementable which requires sufficient proportionality. The regulatory standards are a moving target and it is expected that there will be many questions remaining to be tackled and provisions that will need tweaking to ensure consistency, harmonisation and proportionality following the on-going consultations, notably concerning threat-led penetration testing.

Another industry representative suggested that common objectives should be set in terms of levels of availability and fraud to be reached over time. Much time is spent focusing on standards, but an equal amount of time should be spent on making progress towards improved outcomes, because standards evolve. With a joint goal to work towards, there will be more innovation in the space.

#### *2.3.2 Regulatory certainty*

Regarding possible concerns that CTPPs may have with the proposed oversight regime, an industry representative emphasised that the main concern is regulatory uncertainty, in terms of how to interpret the framework, which is very technical. That is especially likely to happen during the first implementation of DORA requirements. Policy dialogue should take place during this process but after it as well, so that the learnings of the first iteration of DORA can be taken into account to achieve a practical, implementable solution for the whole ecosystem with sufficient certainty. The on-going dialogue between the ESAs and the industry will also contribute to this objective.

A regulator observed that the ongoing consultations and meetings organised by the ESAs can be taken advantage of. This will allow ICT TPPs and financial entities to express views on the proposed standards, before documents are sent to the Commission for adoption. That should help to solve interpretation issues, and a Q&A mechanism will contribute to clarify matters further.

The Chair noted that there is also a need, within the framework, to focus on what matters the most and is most material, which requires pragmatism, proportionality and not losing track of the bigger picture. DORA is cross-sectoral, involves firms of all different shapes, sizes, and business models and has to work with different levels and chains of outsourcing, which creates complexity. Financial firms must not ignore either that they are responsible for the business they outsource.

#### *2.3.3 International consistency*

An industry representative noted that, for global players, it is important to have a harmonised regulatory regime, that looks at matters from a global perspective as well as a regional one, to make sure this regime is compatible with other jurisdictions. Good regulatory practice is also essential to encourage other regions to follow the benchmark that the EU is setting in terms of digital operational resilience regulation.

### 2.4 Areas that require further clarification

An industry representative observed that certain aspects of DORA need further clarification, for example, TLPT and how that will work in practice, and pool testing and whether it is feasible, especially in cloud environments.

The Chair noted that TLPT, or red teaming, is a new part of the framework, which is being extended beyond the European Central Bank's (ECB's) Threat Intelligence-based Ethical (TIBER-EU) approach. There is much to learn in that process, including how it fits with the chain of outsourcing.

### 2.5 Implementation work at industry level

A regulator observed that the preparation for DORA in the financial sector is progressing well, but implementation is approaching quickly, and involvement is needed from all stakeholders to ensure they are prepared for the start in January 2025.

An industry representative remarked that there is less than one year left for the DORA implementation. The main financial institutions have at least activated a gap analysis on DORA, and half of them also have a concrete and actionable roadmap. However, few of them have already implemented the contents of this roadmap in a practical way. Though there is some stress about that in the market, there is also a strong commitment, because there is a recognition of the importance of DORA for reaching an adequate level of protection and sufficient financial stability. The possibility of having an open dialogue with the authorities is also valued.

A Central Bank official noted that the CTPPs in particular, need to prepare and not wait for the beginning of 2025 to prepare for the oversight regime. Contractual arrangements need to be reviewed in the coming months.

Another industry representative stated that all cloud providers have been preparing very diligently and thoroughly for the implementation of DORA scheduled for January 2025. Different cross-functional teams have been set up to analyse the impacts of DORA and prepare for its implementation. This includes mapping out existing capabilities in many different areas such as ICT risk management, threat-led penetration testing to fit with DORA requirements and working on various legal and contractual aspects. This process should ensure that the necessary operational changes are made in a robust way and that the customer perspective is adequately taken into account.

Cloud service providers are also looking at how to apply the DORA requirements in different service models, the

industry representative noted, including software as a service, platform as a service, infrastructure as a service and on-premises models. Depending on the environment, each necessitates a differentiated approach, which is a layer of complexity in itself. The control and responsibility inherent to each model is also being considered. The larger cloud providers are also working under the assumption that they will be classified as CTPPs. That involves preparing for the responsibilities and accountability towards customers mandated by DORA, as well as incorporating DORA principles in governance frameworks concerning all functional product and service layers. That will ensure that all cloud services and the associated potential risks are managed according to the DORA standards.

## 3. Challenges raised by the implementation of DORA

### 3.1 Challenges at industry level

A supervisor highlighted that there is a lack of IT expertise across financial institutions, including at board level. This is an important problem, because banks that have the proper expertise also manage to better identify risks. In addition, questionnaires, on-site inspections, cyber-incident reporting and targeted reviews, have shown that there are still gaps in risk control and failures in identifying risks and incidents, as well as an insufficient protection of IT assets.

An industry representative remarked that the additional budget needed for implementing DORA is an issue for many entities, as well as the timescale of the implementation. For smaller entities, the estimated cost is one or two million euros in the next couple of years, but for mid-size entities it is 10-20 million and for the biggest entities it is 40-100 million. Such additional budgets need to go through lengthy authorisation processes and the implementation is driven by tenders that take time to complete.

There is also an issue of skills and resources. The successful implementation of DORA requires firms to review their organisational model, with a more proactive approach of boards to cyber and IT risk management and also an empowerment of the second line of management. These organisational changes constitute the basis for an effective DORA roadmap, but there is at present a lack of skills for implementing them. The regulatory technical standards (RTSs) also detail the expectations in terms of technology, which is helpful, but implementing new skills and new technologies takes time. Companies are trying to leverage as much as possible existing solutions and processes to improve their cyber and digital resilience capabilities and reach the DORA target and are endeavouring in parallel to implement a new streamlined target architecture, leveraging new technologies.

A second industry representative agreed that budgetary concerns are an obstacle. There is a need to be mindful of smaller players and how they will manage to cope, because cyber and digital operational resilience must be implemented throughout the entire ecosystem.

### 3.2 Challenges for supervisors

A Central Bank official observed that the ESAs and national competent authorities (NCAs) face challenges in preparing for the implementation of DORA at three levels: IT, staff and establishing priorities. A first issue in the short term is properly setting up the reporting systems, which is challenging in terms of IT and timing. This has to be fixed in the most pragmatic and simplest way possible. The other two aspects concern the CTPP oversight regime. There is a need to have the adequate staff to conduct the oversight of CTPPs, which will primarily involve inspections. However, there is a scarcity of IT experts, which will require pooling resources and using a collaborative approach notably via the Joint Examination Teams (JETs), the new joint teams due to be set up between the ESAs and the NCAs for overseeing the CTPPs. Thirdly, priorities will need to be established for running the inspections, which will require a risk-based approach.

Responding to a question from the Chair about how resources should be best used, the Central Bank official indicated that some existing tasks, which will remain, might be streamlined or better prioritised, but supervisors will have to decide about recruiting new resources to increase their competence pool and plan ahead to ensure that the experts available can be mobilised for the most important tasks. Prioritisation is important to allocate resources in the best way.

A regulator explained that work on the oversight framework was initiated by the ESAs in the autumn of 2023, as the objective was to concentrate first on the development of the policy aspects, in order to allow the industry to start planning for implementation. Work on the oversight regime is proceeding quickly under the aegis of the ESA Joint Committee. A high-level group was created gathering experienced and high-level supervisors from all member states and across sectors to prepare the oversight setup. Oversight methodologies are being worked on and the resources needed to conduct this oversight on the ground are being evaluated. ESA resources will need to be complemented by resources provided by the NCAs for conducting the oversight. The objective is to leverage existing structures as much as possible in the context of the JETs. Other institutional arrangements created by DORA include an oversight forum and a joint oversight network.

## 4. Success factors of the CTPP oversight regime

An official welcomed the direct oversight regime of DORA, but stressed that it will not replace, but complement, existing due diligence obligations. The banks that use CTPPs will have to continue doing their own due diligence, in order to properly manage operational and third-party risk. Moreover, the direct oversight regime must not be considered as a bilateral dialogue between the CTPPs and the regulator. Financial institutions have to be involved. All relevant parties should be brought into the framework in order to identify collectively potential vulnerabilities and

supervisory priorities and define the actions that the CTPPs need to conduct in order to address these vulnerabilities. This is quite complex, as CTPPs offer services to many different types of firms in different countries around the world. Ways therefore need to be found to make this system effective and sufficiently economical, which may involve co-operation across financial institutions and joint audits. There should be continued exploration of the possibilities for optimising current supervisory processes and inspections that concern the same providers. Some developments in Europe are also quite promising, such as the certification regime for cloud service providers.

The official added that international co-operation is quite a challenge in this field, because there are different regulatory regimes in different jurisdictions. In most countries the oversight regime largely relies on the due diligence performed by the entities themselves. The DORA direct oversight regime is still unique, but there are other regional arrangements, for example in South East Asia, to consider, although they do not have the same degree of concreteness and prescriptiveness. Beyond the implementation of DORA, efforts must be made to foster more co-operation and consistency at the international level. Consideration should be given to put in place a common supervisory regime for some global CTPPs along the lines of the regime employed to oversee SWIFT.

A regulator suggested that, with regard to the CTPP oversight regime, the thinking in terms of organisation and resources is in three main areas. One is staff, meaning the amount of people that can be put on the ground, but there are also skills and technology. Many experienced supervisors have been dealing with ICT risk in the past, so their skills can be leveraged. Initiatives can also be put in place to upgrade skills. There is an arrangement with the Directorate-General for Structural Reform Support of the Commission to upscale some of the skills of the supervisors for example. Technology can also be leveraged for this new type of supervision. Due diligence through surveys is conducted to better understand the characteristics of CTPPs and anticipate the needs in terms of the supervision of the 15,000 TPPs identified in the last survey. Not all of them have the same size, but many are relatively important for financial entities.

## 5. Measures needed to ensure cyber and digital operational resilience

### 5.1 Stress testing

A supervisor detailed that a stress test is being carried out currently in the EU banking sector by the ECB. The cyber resilience stress test is a severe but plausible cyber-related scenario. The purpose is to evaluate with detailed questionnaires the capacity of banks to respond and recover after an attack, rather than assess the controls preventing cyber-attacks. 28 banks are also participating in an IT recovery test. The ECB has assessors who will validate the answers. The governance and communication of the banks are also evaluated, because after a serious cyber-attack the way in which banks are able to communicate to the outside world is important. The objective is to identify possible weaknesses in the cyber-resilience framework of the banks, resulting in bank specific findings and recommendations to mitigate these. This will be a learning exercise for banks and supervisors.

### 5.2 Tackling systemic cyber-risks

An industry representative stressed that there must be a systemic approach to operational resilience, beyond resilience at firm level. All parts of the ecosystem, including regulators, consumers and firms, must work together to fight fraud,. Organisations must also assist each other. Such defensive work never ends, because fraudsters are very skilled. Whenever something is found that is supposed to stop fraud, the fraudsters will evolve to attack that too. The Chair noted that the ecosystem dimension is taken into account in DORA implementation preparations.

A supervisor highlighted that the European Systemic Risk Board (ESRB) has been doing a great deal of work on the systemicity of cyber crises. That is an important and very challenging area. The tools and approach needed to tackle these still need specifying. There is also a need to be agile to adapt to the changing risk environment, which means that the approach should not be too rule-based. Public-private partnerships are also needed.