Presentation of the "Project for digital operational resilience regarding asset management: More digital means safer" (DORA) /INVERCO

VÍCTOR RODRÍGUEZ QUEJIDO, GENERAL DIRECTOR OF THE POLICY AND INTERNATIONAL AFFAIRS DIRECTORATE-GENERAL OF THE CNMV

09 May 2023

Good morning.

It is clear that technology is becoming more and more relevant in our lives, increasingly forming part of all the services and products we consume daily, how we interact with each other and how we work. And the financial sector is undoubtedly one of the areas in which technology is traditionally used more intensively.

Even though this growing dependency on digital technology implies obvious benefits in terms of efficiency, it also entails risks that should be adequately managed, one of the most relevant ones being cybersecurity in financial entities, which is precisely what we will deal with today.

Cybersecurity has for some time been an essential element to be taken into account, but this is becoming even more relevant as technological innovation grows continuously in an exponential manner. Artificial intelligence, distributed ledger technology or quantum computing are examples of technologies that are showing great development in the last few years, and which generate important additional challenges regarding cybersecurity.

The Digital Operational Resilience Act, known as DORA, with the legislator precisely being aware of the ever-increasing risk of cyber-attacks when drawing it up, aims to reinforce IT security in financial entities. To this end, it establishes certain standard requirements for the safety of the networks and information systems of these entities, while also for third parties that provide these essential services regarding information and communications technology (ICT), such as cloud platforms or data analysis services. DORA creates a regulatory framework according to which all companies will ensure they can withstand and respond to any kind of ICT-related disturbance or threat, while to recover from any potential impact deriving from these.

I will not delve into the details of this new regulation, but I would like to highlight a few circumstances related to cybersecurity.

Firstly, the increase in the amount of attacks year after year, while also in their types, persistence and complexity. This is the case as those attacking are increasingly sophisticated, professional, have greater resources and often have geopolitical or financial targets, for which reason financial entities are one of the favourite preys.

In second place, the financial system is becoming more interconnected and global, clearly increasing the risk of contagion in a highly digitalised environment and whose nature could become systemic, something which should obviously be avoided.

Finally, there has been an increase in the contracting of external technological services due to various factors such as the large volumes of data or the high specialisation required. This can potentially lead to two critical situations related to cybersecurity. The first would be a greater exposure to threats throughout the entire value chain, as the exposure to attacks is increased by adding various technological providers. To manage this risk, contracts must rigorously include the provider's obligations regarding cybersecurity. The guidelines for outsourcing services to cloud service providers, published by ESMA in May 2021, already clearly establish the appropriate procedure to manage contracts for this type of service and, concerning this, DORA includes a whole chapter giving an introduction to the requirements to be fulfilled by financial entities. Another possible scenario may also arise, in which a technological service provider providing services to an important part of the financial sector could suffer a serious attack, affecting the services offered to a large number of financial entities, which would mean a serious situation for the sector. DORA also considers this risk and establishes procedures to identify these critical providers and their supervision from bodies specifically created for this from the global European perspective. This will undoubtedly be an important challenge we will have to tackle jointly.

A moment ago I referred to the complexity of new attacks. Advanced persistent threats, known as APTs, are probably the greatest challenge we are to face at present. Attackers collect information on their target, this being known as intelligence work, for whatever time is necessary until a more efficient attack is configured, with ever-increasing resources and, therefore, becoming more dangerous. So as to be prepared for these persistent attacks, financial entities must carry out specific tests for this kind of threat. Therefore, this is not about taking the usual penetration tests but tests that check the critical systems with regard to APTs. This is not new, these advanced tests have been carried out for years, and DORA will only demand these for certain financial entities. What is more recent is the adoption of the European TIBER-EU test framework, which standardises these tests among the different jurisdictions that adopt it. In the case of Spain, the adaptation of this framework is called TIBER-ES and the financial entities that wish to may undergo its tests, as long as they have the required level of maturity regarding cybersecurity, as we must not forget that these tests are carried out against the systems under production.

An aspect of DORA we are aware is of concern to the sector and to actual supervisors is all that relating to proportionality when applying this regulation. DORA actually includes proportionality mechanisms in its articles.

Thus, Article 4 was included to establish the general proportionality principle that is to govern the application of and compliance with the Regulation by financial entities, taking into account aspects such as their size and the risk profile, together with the nature, scalability and complexity of their services, activities and transactions. Supervisors are to apply this principle in a sensible manner, so there is a balance between the appropriate management of the technological risk and the effort that is to be made by the financial entities.

As an example, some exceptions are established regarding compliance with certain requirements for micro-enterprises (those with less than 10 employees and a turnover or annual balance sheet under €2 million) which comprise a large part of the investment firms and fund management companies in Spain Similarly, "small and non-interconnected" investment firms are excluded from the application of a relevant number of obligations, with specific alternative obligations that are more in line with the resources of these types of entity being indicated.

On the other hand, additional obligations are included for central counterparty clearing houses, central securities depositories and data providers, as they usually have a key role in the system.

I will conclude with a final message that I consider relevant. At the CNMV we are aware of the challenge this new regulation poses to everyone. Therefore, we intend to carry out internal training actions for our technicians and we have also included in our Activity Plan for 2023 our objective to assess the degree of readiness for DORA of IFs and fund management companies, with a view to planning this Regulation which is to come into force in January 2025. For this, during the year we will draw up a questionnaire aimed at IFs and fund management companies with regard to the cybersecurity aspects included in this regulation, to analyse the results and get an idea on the situation regarding this issue. Our intention is to accompany the sector during the implementation of DORA, maintaining a permanent dialogue regarding this and working jointly to, among others, achieve a safer and more resilient financial system.

Thank you very much.