CYBER AND DIGITAL OPERATIONAL RESILIENCE

GERRY CROSS
Director Financial Regulation, Policy and Risk - Central Bank of Ireland

DORA – One-step closer to finalization

The European Supervisory Authorities ("the ESAs"), who are tasked with jointly delivering the regulatory standards implementing the DORA ICT risk management framework, have come one-step closer to finalisation. On 17 January 2024, the Chair of the Joint Committee of the ESAs submitted the first batch of finalised DORA Level 2 regulatory standards to the Commission. This marks the first milestone in the DORA implementation, achieved through close collaboration by the ESAs and amongst members of the JC SC DOR, established to deliver these standards.

Prior to finalisation, the first batch of Level 2 policy products underwent a three month public consultation ending in September 2023 and the ESAs received more than 400 comments from interested parties. Following a comprehensive analysis and consideration of these comments, three final Level 2 regulatory technical standards (RTS) on ICT risk management, on major ICT-incident classification and on on ICT services performed by ICT third-party providers together with one implementation technical standard (ITS) on templates for a register of information (for ICT services provide by third-party providers) are now publically available.

The second batch of policy products is currently in public consultation until 4 March 2024. This batch contains a RTS and an ITS on the content, timelines and templates on incident reporting, a RTS on subcontracting of critical or important functions, a RTS on oversight harmonisation and a RTS on threat-led penetration testing (TLPT). Furthermore, the consultation includes two Guidelines, one on aggregated costs and losses from major incidents and one on the oversight cooperation between ESAs and competent authorities. Stakeholders in the DORA Regulation are invited to take this opportunity to provide important and valued feedback on the draft technical standards and guidelines to ensure a solid policy product that is addressing key ICT risks while also being implementable.

For 2024, firms should have a strong focus on implementing DORA.

For 2024, firms should have a strong focus on implementing DORA. From industry engagements, we understand that many sectors are already working in this regard and are progressing well in implementing DORA requirements into their ICT processes. However, it is of upmost importance that financial firms from all sectors effected by DORA identify their respective implementation challenges and have a sound implementation plan. In order to do this, all financial firms must have a detailed understanding of the various ICT systems and ICT assets supporting their business functions. In simple terms, firms need to know what ICT they have in order to adequate safeguard their ICT systems and assets in accordance with DORA.

Despite the different implementation efforts and understandings on ICT systems and assets, financial firms in different sectors are likely to have a different ICT risk management maturity that correlates with existing regulatory requirements. Sectors that currently have no or only light ICT requirements are encouraged to assess the new requirements DORA brings. Sectors where ICT risk management guidelines exist, for example issued by the EBA (Guidelines on ICT and security risk management, 2019) or by EIOPA (Guidelines on information and communication technology security and governance, 2020), need to perform a gap-analysis to identify additional requirements stemming from DORA.

DORA's oversight framework for critical third-party providers (CTTP) of ICT services to financial entities is currently been developed. The ESAs in collaboration with competent authorities are continuing to focus on developing organisational structures to deliver the CTPP oversight. A cross-ESA high-level group of senior members has been establish to drive forward the organisational aspect of the CTPP oversight, while the JC SC DOR continues to focus on policy work. A crucial tool will be the aforementioned register of information, finalised this January, and ESAs together with National Competent authorities are developing the necessary ICT infrastructures to collect and analyse ICT services provide by third-party providers to allow the designation of CTPPs.

FRANÇOIS-LOUIS MICHAUD

Executive Director - European Banking Authority (EBA)

The ESAs are getting ready for the implementation of DORA

The Digital Operational Resilience Act (DORA) will increase convergence and efficiency in supervisory approaches when addressing ICT third-party risk in the financial sector. Its implementation requires from the European Supervisory Authorities (ESAs – EBA, ESMA and EIOPA) to: (i) develop the adequate policy mandates and (ii) establish the oversight framework over critical third-party providers (CTPPs).

In 2023, the ESAs have advanced a wide range of policy mandates to detail the requirements for ICT risk management, the classification of ICT incidents, the ICT third-party service providers' policies and the template for the register of information. The final reports on these instruments were published and delivered to the European Commission in January. They build on the feedback received from stakeholders (e.g. on proportionality, complexity and the degree of prescriptiveness).

First, proportionate rules and a principle-based approach were applied for the regulatory technical standards (RTS) on ICT risk management framework which now allow for further flexibility, more streamlined requirements and additional clarity. Similarly, in the RTS on ICT incident classification, smaller and non-complex entities have been exempted from the application of some requirements and many proposed classification thresholds increased. Second, regarding the overall complexity and prescriptiveness of the mandates, the RTS on risk management framework now integrates a risk-based approach by referring only to critical or important functions, or to ICT assets supporting critical or important functions[1]. In the same vein, the classification approach and criteria for major incidents have been simplified and streamlined to limit the burden to financial entities, focusing more on the impact of the incident.

The second set of policy products was published for consultation in December 2023 and will be finalised in July this year. This will complement the ICT-related incident reporting framework, provide further details on ICT sub-contracting and on threat-led penetration testing, as well as specify some of the requirements of the oversight framework. The ESAs expect the high-level of engagement from stakeholders (financial entities, industry representatives, associations) observed thus far will continue, to ensure that the policy products will be fit for purpose. Once all DORA policy mandates are available, the attention will turn to supervisors and the ESAs, for ensuring a convergent application of the new requirements for the financial entities.

The ESAs are now focusing on the operational set-up of the oversight and beyond, which includes the reporting of major ICT-related incidents and the set-up of information sharing mechanisms, to be ready for the application of DORA in January 2025. The ESAs have been preparing for this novel oversight framework in various ways, and ran a high-level survey to start map the provision of ICT services to the EU financial entities by ICT TPPs[2].

Their report identified around 15,000 ICT TPPs directly serving financial sector entities and showed that the frequently used ICT TPPs directly support many critical or important functions and provide a large range of services (e.g. software, network infrastructure, data centres, cloud computing and data analysis).

Second, the ESAs have engaged with financial entities, overseers and supervisors on the expectations for oversight framework, the risks posed by ICT TPPs to the financial sector and how these risks are currently assessed and mitigated.

Third, the ESAs are working closely together with supervisory authorities to establish a new common oversight framework, whereby one ESA will be designated as Lead Overseer for each of the CTPPs. This entails intensive work on new sets of processes and procedures, including the designation of the CTPPs, the conduct of general investigations and on-site inspections and the issuance of recommendations to CTPPs.

In 2024, European Supervisory Authorities will be focussing on the DORA oversight set-up.

Finally, the increasing interconnectedness of the financial sector requires supervisors to coordinate swiftly their actions in case of cyber-threats. The ESRB highlighted in a Recommendation the need for a coordination framework for systemic cyber incidents, inviting the ESAs to start preparing for its development, building on one of their roles under DORA, i.e. to develop communication channels to enable a coordinated response to ICT incidents with systemic impacts on the financial sector. The ESAs are setting up this framework, assessing synergies with other frameworks across the EU and already anticipating the supervisory community's need to intensify efforts in the identification and prevention of cyber risks, coordinating activities such as crisis management and contingency exercises.

1. *Article 3(22) of DORA defines critical or important function as "a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law".*
2. *See ESAs Report on the landscape of ICT third-party providers in the EU. The analysis was carried out on the basis of voluntary information provided by a sample of entities across the EU financial sectors.*

DENIS BEAU
First Deputy Governor -
Banque de France

DORA: 2024, a decisive year for a successful implementation

DORA "level 2" acts are under finalization. They end a successful rulemaking process, despite a constrained timeline. With technical standards on track, public and market actors must now overcome operational challenges, linked to resources and IT systems, to turn DORA into a reality. Considering DORA's enforcement starts in January 2025, prompt identification of strategic priorities is necessary for timely readiness.

DORA rightly levels up resilience requirements in a context of rising cyber threats, which can have system-wide destabilizing impacts. The recent ransomware attack against the US subsidiary of the Chinese bank ICBC which impacted the T-bill market liquidity, could have been not a so gentle reminder had the parent company not injected emergency capital. Under DORA, the main responsibility for enhancing operational and cyber resilience lies with financial entities. They must take necessary measures to align their governance and risk-management procedures with the new standards. 2024 is also the last year for them to review their existing contractual arrangements with third-party providers and make them compliant with DORA mandatory clauses, to help ensure more balanced contractual relationships.

Moving on to public authorities, one major challenge to make DORA work is to set up a fully operational reporting system by January 2025. For instance, the framework for incident and cyber threat notification and response is likely to generate a complex reporting architecture, as it requires coordination between multiple financial, NIS and enforcement authorities with various missions. All options for streamlining it, to inform the right people at the right time, should be pursued rapidly, such as dual and harmonized reporting from financial entities to DORA and NIS authorities. Large scale cyber crisis exercises, an increasingly common practice, will be inevitable here to ensure an effective setup. Another significant task relates to contractual registers of information, which will be crucial for mapping service providers within the supply chain and identifying the critical ones; they will also be used as the main database for critical third-party ICT-service providers (CTPP) supervision.

While financial entities should expect the reporting template to be comprehensive and prepare to manage this requirement, supervisors need to develop appropriate tools to process this data flow. European shared platforms are obviously preferable to fragmented systems with 27 national legs. We therefore call for promptly agreeing on efficient transmission hubs and workable formats for swift information sharing.

With technical standards on track, public and market actors must now overcome operational challenges.

Supervisors will have a brand new mission in the oversight of CTPPs. Compliance and preparation challenges are maximal: authorities need to start their oversight tasks as soon as possible, by 2025, since the dependencies on major providers are already critical for EU's financial stability and sovereignty. Two drivers will be key to build the oversight framework.

First, technical standards should sufficiently empower public authorities to deliver on their oversight mandate; this is one of the most important issues of the public consultation.

Second, EU authorities will have to allocate adequate staff and expertise to the Joint Examination Teams (JETs) in charge of overseeing CTPPs. This effort will be substantial in the current resources-limited environment. This requires a considerable amount of preparatory work with ESAs and NCAs to agree on a target organization, pooled sources and common operating methodologies and tools in the course of 2024.

Last but not least, getting ready for the oversight framework is a big challenge for service providers. Major players, which are likely to be designated as CTPP, should take advantage of 2024 and proactively tackle their preparedness issues. Indeed, in the upcoming more supervised ICT market, those who provide high-quality and secure services will benefit from a competitive advantage. In parallel, it is only natural that authorities shortly give a first taste of their expectations to CTPPs to fuel the supervisory dialogue.

In the longer run, an enlargement of DORA's scope will be worth considering. It could make sense to use the review clause to extend DORA's requirements to other critical areas of the EU financial sector, such as payment systems and payment technical providers.

ANNELI TUOMINEN

Member of the Supervisory Board - European Central Bank (ECB)

Digital Operational Resilience Act: the next step in a connected digital world

The Digital Operational Resilience Act (DORA) aims to achieve a high common level of digital operational resilience across European financial entities. This is a welcome step in an increasingly connected world that is ever more exposed to cross-border information and communication Technology (ICT) risks and cyber risks.

The Act lays down requirements for ICT risk management, reporting major ICT-related incidents to supervisory authorities, digital operational resilience testing and the sound management of ICT third party risk. It provides a direct legislative basis for the work we have been performing for several years as part of our supervisory priorities[1], including collecting information on cyber incidents from banks. In addition, it establishes an oversight framework for critical ICT third party service providers.

The joint committee of the European Supervisory Authorities submitted the first set of final draft technical standards to the European Commission, addressing items such as ICT and third party risk management as well as incident reporting frameworks.[2] The ECB welcomes these final draft technical standards. Given the tight timeline for developing the legislation and its potentially complex implementation, I believe that stakeholders may find it challenging to meet all the requirements in a timely manner, particularly the new ones relating to threat-led penetration testing (TLPT) and oversight of critical third party providers (CTPPs).

However, there are ways of facilitating a successful outcome, including interaction with stakeholders, which will be key. For example, oversight of CTPPs will be an important addition to the regulatory and supervisory framework. The criteria used to define the list of CTPPs will be very important. It will therefore be essential to involve the relevant stakeholders at this stage. At this juncture, it may also be worth considering consistency and interoperability between authorities from other jurisdictions. In addition, oversight of CTPPs will require close monitoring and possibly on-site inspections similar to those carried out for financial intermediaries. It is important that CTPPs will be ready to take part in these discussions.

DORA is a step in the right direction, that will help us manage ICT and cyber risk together.

Regarding the set up and organisation of the work of the joint examination teams (JETs), we will need to go through a full oversight cycle before we are able to establish a comprehensive operating process for them. Further clarification on the number of CTPPs and the type of resources needed, for instance, could help to ensure that the competent authorities provide the appropriate level of support. By building on their shared experience, regulators and supervisors should ensure that priorities for the JETs are correctly established. They should also ensure the teams have the requisite balance of competencies and flexibility to perform the tasks assigned to them. How the teams actually operate is likely to evolve over time.

DORA will have a significant impact on banking supervision activities. First, supervisory practices will have to adapt to overseeing new types of entities and working in a new operating environment where innovation is continuous and driven largely by technology. Second, the Act will help to reinforce supervisory activities. For instance, as mentioned earlier, it will help to improve the cyber-incident reporting framework in place since 2017 by streamlining it and making it more consistent. DORA will also create several new tasks, including conducting TLPT and the contribution to JETs in charge of the oversight of critical third party service providers.

To perform these tasks, we will need to update the existing methodologies and toolkits used to supervise ICT risk and monitor the impact of technology on business models. The improved understanding of ICT risk introduced by DORA will need to be integrated into the overall supervisory view on banks' safety and soundness. A specific approach will be needed for CTPPs due to their specific technical nature and the additional amount of work overseeing them is likely to generate.

Finally, let me add that a mechanism for sharing information and achieving a common level of digital resilience is very important since digitalisation affects operational resilience and banks become more dependent on third party service providers. At the same time, we should not forget that having DORA in place, does not mean that all risks are managed. We need to closely monitor the evolution of more sophisticated cyber threats originated by criminal and government attackers. DORA is a step in the right direction that will help us rise to these challenges together.

1. *ECB Banking Supervision (2023), "SSM supervisory priorities for 2024-2026".*
2. *Joint Committee of the European Supervisory Authorities (2024), "Final report - Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554", January.*

FERNANDO RESTOY
Chair - Financial Stability Institute (FSI)

The oversight of CTPP: the need for further international consistency

Despite recent developments in several jurisdictions, including the EU, the prevalent approach is an indirect oversight approach, in which financial institutions are expected to manage their risks arising from acquiring third-party services. The regulatory and supervisory focus therefore is on the assessment of the adequacy of financial institutions' outsourcing and contractual frameworks. These frameworks should ensure that financial institutions have, among other things, an assurance process regarding third parties' operational resilience.

This indirect oversight approach is not enough to address potential systemic risks arising from critical third parties. The FSB recognises this limitation of the approach but notes that many financial authorities may not have the legal powers to adopt a direct approach. The FSB report on third-party risk management and oversight therefore proposes some tools to help financial authorities identify systemic third-party dependencies and spot and manage potential systemic risks.

However, authorities in a few jurisdictions are moving towards a more direct oversight approach. The Digital Operational Resilience Act (DORA) in the EU is an example. Those jurisdictions that have implemented or are in the process of implementing a direct oversight approach need to address a few practical challenges.

At the national level, authorities need to keep financial institutions incentivised to take third-party risk management seriously, despite the fact that critical third parties are already subject to oversight by financial authorities. This can be addressed by regular assessments by financial authorities of their third-party risk management.

In addition, the oversight of critical third parties should not just be a dialogue between the authorities and the third parties. There should be regular interaction that involves the financial institutions. This way, all parties will have a common understanding of the authorities' concerns and expectations, how they are addressed by critical service providers and how they should inform financial institutions' risk management.

It is also important to avoid subjecting critical third parties to multiple assurance processes – from financial institutions (because of the requirements under the indirect approach) and from the competent authorities. In that regard, coordination with other relevant national authorities that also oversee critical third parties in the financial sector is important. Indeed, in some jurisdictions there may be national frameworks for critical infrastructures and critical third parties outside the remit of financial authorities (eg Australia's Security of Critical Infrastructure Act 2018).

For global third-party critical service providers, there may be a need for a global oversight regime.

At the cross-border level, differences in approaches have implications for the scope for fruitful coordination. That justifies the DORA requirement for critical third parties to establish subsidiaries to facilitate enforcement actions. It is deemed that "there are no suitable alternative mechanisms… by way of effective cooperation with financial supervisors in third countries" given that there is an "absence of comparable arrangements in other jurisdictions…". Yet, at the same time, in exercising its relevant powers in third countries (ie for critical third parties that provide services to EU financial institutions from outside the EU), DORA states that relevant authorities of the third country should be informed of, and not have objected to, the exercise on their own territory of the activities of the EU Lead Overseer.

That points to the need to further develop mechanisms to facilitate international cooperation. This includes the establishment of a global methodology for identifying critical third parties and of global resilience standards for critical third parties.

Furthermore, for third parties that may be critical across multiple jurisdictions, there is a special need to adopt a robust oversight regime entailing the coordinated participation of relevant national authorities working under mutually agreed procedures and distribution of functions. That global oversight regime, which could take the one currently applied to Swift as a reference, should foresee regular cross-border resilience testing.

PAOLO CARCANO
Partner - PricewaterhouseCoopers Business Services S.r.l.

How DORA & RTS shift the business paradigm of IT & Cyber Risk

Ensuring Digital Resilience: DORA & RTS as catalysts for Financial Services

In response to the dynamic shifts in the market and the evolving landscape of cyber threats, European regulatory bodies have taken decisive actions to shape a future where financial institutions stand more resilient against digital risks. Leading this charge is the DORA, enacted by the EU Commission in 2022 and slated to be directly applicable from January 2025. DORA mandates specific cybersecurity measures for financial entities operating in Europe, ensuring their readiness to prevent, withstand, and respond to potential cyber threats.

DORA presents itself as a highly sophisticated regulatory framework. To reinforce these efforts, the European Supervisory Authorities (ESAs) are issuing additional norms, including Regulatory Technical Standards (RTS), Implementing Technical Standards (ITS), and Guidelines (GL). Furthermore, the ECB is also publishing additional regulations. Notable among these are the *Cyber Stress Test* (*crafted to fortify the resilience of the financial system, the Cyber Stress Test involves the implementation of a series of supervisory controls) and the TIBER-EU Framework (aims to enhance cyber resilience through controlled cyber-attacks).*

Together, these measures meticulously outline indispensable organizational and technological requirements for effectively managing relevant threats, with a particular focus on the ransomware threat, transforming DORA from a conceptual idea into a tangible reality. The DORA is thus situated among a series of complex regulations that European regulatory bodies have been implementing in recent years, even addressing highly innovative themes.

Notable among these are the *AI Act* (which establishes ethical guidelines for AI systems, emphasizing human control and cybersecurity), the *Digital Services Act*, and *Digital Markets Act* (aimed at ensuring digital security, protecting user rights, and promoting fair competition).

DORA & RTS reshapes ICT & Cyber Risk by prioritizing end customer trust.

Cybersecurity trends in EU: escalating threat landscape

The numerous regulations introduced by European regulatory bodies are clearly reflected in alarming threat intelligence analyses. Over the years, these analyses have highlighted a growing trend of cyber attacks and an increase in the number of victims. Moreover, the World Economic Forum's "Global Risk Report 2023" predicts a complex and catastrophic cyber attack on the entire European financial system by 2025. Additionally, the WEF has also studied the ongoing rise in economic damages caused by cybercrime: from $3 trillion in 2015 to $6 trillion in 2021, with the potential to reach $10.5 trillion annually by 2025. The critical role of European regulations becomes evident in the face of a growing cyber threat. In light of this data, the implementation of DORA, RTS, and regulations issued by the ECB becomes crucial in addressing threats and safeguarding the European financial system.

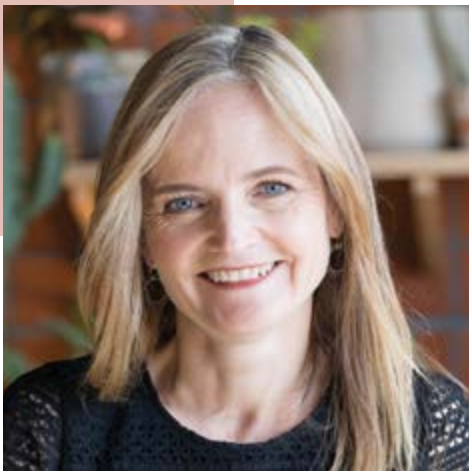
ECB Cyber Stress Test as the first practical application of DORA pillars for banking sector

DORA requires financial institutions to review their organizational models to ensure a strengthened involvement of top management in strategic decision-making and risk assessments. This involves securing adequate financial and organizational resources based on strategic choices and risk evaluations. However, it is important to emphasize that the commitment required by DORA goes beyond corporate leadership, involving business functions as well and setting priorities for the implementation of resilience solutions.

DORA is revolutionizing the landscape of ICT and cyber risks by placing the end customer at the forefront and ensuring trust in financial services. In this contest, the traditional Disaster Recovery (DR) and Business Continuity (BC) plans, designed primarily for scenarios affecting availability are now deemed inadequate.

DORA and Cyber Stress Tests both highlight the risk of data integrity loss, rather than solely focusing on their unavailability resulting from ransomware attacks. This risk materializes because systems are often restored after an attack using a non-real-time-synced backup, requiring data reconciliation actions that may extend over several days. These extended RTOs translate into significant economic and reputational impacts. Therefore, appropriate contingency solutions should be implemented during such RTO periods.

From our standpoint, the 2024 ECB Cyber Resilience Stress Test has challenged European banks with a scenario of core system disruption lasting an average of three days, peaking up to seven days. This scenario demands a profound reevaluation of recovery solutions, where Business functions are tasked with defining new contingency measures capable of safeguarding client interests. The subsequent impact assessments reach significant values, against which the investments in IT and cyber resilience mandated by DORA find a deep business justification.



CHARLOTTE HOGG

Executive Vice President and Chief Executive Officer - Visa Europe

Increasing digitalization requires a considered stock-take of cyber and operational resilience

Over the last decade, a steady stream of innovation has made digital payments easier and more convenient for everyone. We pride ourselves on the knowledge that a Visa transaction will always work. Visa performs at as close to perfect reliability as is possible in our industry – or any – something which requires an enormous amount of careful investment and management.

To underscore the scale of this achievement; the Visa network handles up to 65,000 transactions a second, all of which have 27 different routing options, across digital and physical network infrastructure which could stretch around the world over 400 times to ensure payments work seamlessly for merchants and consumers in real time. This contribution to Europe's payments landscape is something we are rightly proud of.

This does not however mean that we are complacent about cyber and operational resilience. Our response is constantly evolving, underscored by €8 billion in technology investments over the past five years and over a thousand cybersecurity specialists to deliver on our availability and resilience promise. Visa is also a first mover in leveraging the benefits of AI and data infrastructure, already having invested €2.5 billion towards risk management in the past decade. Responding to the constantly changing and increasingly borderless cyber attackers remains a challenge – for example, cyber terrorists can coordinate ATM runs across multiple jurisdictions, from another part of the world, in real time which require leveraging global data to detect and respond to them. Through a complex interlinking of innovation and expertise, we have been able to reduce fraudulent Visa transactions to less than 0.1% across Visa transactions – a historic low – preventing over €20 billion in fraud annually.

Visa's payment network is built around the truism that everything that can break at internet scale will break – and therefore, you cater to that with what we call pessimistic design. This means building the network in a manner that can handle a lot of unexpected turbulence – like natural disasters, technology disruptions, cyber threats – but also a sudden surge in demand for digital payments, as we have witnessed over the past few years. What we learnt from the complex threat landscape is that our network continues to be highly resilient.

In Europe, political appetite is growing for regional alternatives to global payment networks like Visa to reduce overreliance on certain or global networks. Whilst an important concern, developments must ensure there remains many options available to Europe's consumers and merchants to prevent a single point of failure and to ensure the best resilience practices are available to Europeans. We consider a well-functioning European payment landscape to be a shared goal with policymakers and want to contribute through our expertise and network to make this a success.

As the tech gets better, we also observe criminals focusing on the weakest link in the payments chain - people. Scams are increasingly sophisticated, and anyone can be caught out. To mitigate this on our network Visa is working with clients to educate consumers – and make sure they can get their money back.

Other networks face different challenges. Instant credit transfer transactions volume is growing in Europe but faces a heightened vulnerability to fraud due to faster settlement times. For example, instant payments can be a lot like sending cash in the sense that once you send it, it's gone. If you are duped into sending money to someone misrepresenting their identity, that money may be gone forever. Similar challenges exist in crypto and digital currencies, where there is no "claw back" mechanism if you make a transfer to some anonymous scammer's wallet. When using any of these new technologies, it's important to know who exactly you're dealing with on the other end of the transaction.

As the tech gets better, we also observe criminals focusing on the weakest link in the payments chain – people.

European regulation is setting new parameters to level up risk and fraud management across the financial services sector as well as providing regulators with more insight on current risk management practices employed by firms today. Nevertheless, the levels of sophistication and the level of the best performing sectors, like payments, is the product of many years of innovation and expertise. It is important regulatory frameworks remain proportionate, principle based and reduce duplication where possible to give firms the necessary flexibility and focus on achieving the best resilience possible.

We are however optimistic about the current regulatory approach and Visa stands ready and confident to meet our clients' expectations in meeting the new requirements.