ERA Forum
https://doi.org/10.1007/s12027-024-00793-w

ARTICLE

The digital operational resilience act: challenges and some reflections on the adequacy of Europe's architecture for financial supervision

Christopher P. Buttigieg[1] · **Beatriz Brunelli Zimmermann**[1]

Accepted: 12 June 2024

Abstract

The paper critically analyses the Digital Operational Resilience Act (DORA) within the European Union (EU) with respect to challenges such as supervision and the oversight framework coordination. It delves into the adequacy of the European System of Financial Supervision (ESFS) in ensuring compliance with this regulation, highlighting issues of fragmented supervision at national level and inconsistent approaches. The main argument suggests that while the DORA Regulation is a positive step for harmonising digital operational resilience regulation, it brings about challenges in supervisory convergence and cooperation due to the existing fragmented supervisory architecture. The authors propose potential solutions like a more centralised supervision model to address these challenges. The paper follows a structured format with an overview of the DORA Regulation, discussion on identified challenges, and a concluding section.

Prof. Christopher P Buttigieg Ph.D. is the Chief Officer responsible for Supervision at the Malta Financial Services Authority (MFSA), a member of the Board of Supervisors of the European Banking Authority and European Securities and Markets Authority (ESMA), was the Chair of the ESMA Data Standing Committee (until December 2022) and is currently the Chair of the ESMA Proportionality and Coordination Committee. He is an Associate Professor in the Banking and Finance Department of the University of Malta and has a PhD in Law Studies focusing on financial regulation from the University of Sussex (UK). The opinions expressed in this paper are those of the authors at the time of writing and do not necessarily reflect those of the MFSA, ESMA or EBA. Any errors or inaccuracies are attributable exclusively to the authors.

Ms. Beatriz Brunelli Zimmermann, is an Analyst in the MFSA's Supervisory ICT Risk and Cybersecurity Function. She is a University of Malta graduate and has attained a first-class degree in International Relations.

✉ C.P. Buttigieg
christopher.buttigieg@mfsa.mt

[1] Mriehel, Malta

Published online: 20 June 2024

Keywords Digital operational resilience act · Financial regulation · Financial supervision · Supervisory convergence · Centralisation · Cyber risk and operational risks

1 Introduction

In a dynamic financial world, regulation and supervision must be easily adaptable to remain effective. The development of business models which are largely based on technology, as well as the digitalisation of financial services, have created new challenges for financial supervision. The financial system has become more reliant on Information and Communications Technology (ICT) systems and developments in this field are constantly challenging the *status quo* and, at times, required and still require a quantum leap in the regulatory framework, and the knowledge, tools and systems adopted for financial supervision. In this regard, cyber risk is considered of systemic relevance[1] and is an area of operational risks which is being closely looked into by regulators across the globe.

In the European Union (EU), Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (hereinafter referred to as the 'Digital Operational Resilience Act' or the 'DORA Regulation'), has been adopted to provide a common regulatory framework for digital operational resilience in the financial services sector.

This paper critically reviews the DORA Regulation along the lines of three selected challenges: [i] ensuring supervisory convergence; [ii] limited centralisation on the development of solutions; and [iii] cooperation, coordination and fragmentation in the Oversight Framework. More broadly, this paper also reviews the adequacy of the European framework for the supervision of compliance with this regulation, namely the European System of Financial Supervision (ESFS). In the context of an interconnected financial system the framework for the regulation and supervision of ICT risk and cybersecurity is as strong as the weakest link. While the DORA Regulation creates a harmonised regulatory framework for digital operational resilience across the EU, supervision in Europe is fragmented and the approach to supervision at national level is inconsistent and, to a certain extent, inadequate to face the emerging challenges in this field.

This paper's main argument is that the DORA Regulation, albeit a very positive development, has created a number of challenges in regard to supervisory convergence, cooperation, coordination and fragmentation for authorities, supervisors and regulators. These challenges are not a 'DORA problem', instead it is important to recognise that the DORA Regulation has been designed to fit the architecture of system for financial supervision that is fragmented and that operates largely across sectoral lines.

[1] European Systemic Risk Board, 'Cyber Systemic Risk' (February 2020) <https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf?fdefe8436b08c6881d492960ffc7f3a9> last accessed 19.3.2024.

The authors believe that if the future of financial regulation and supervision is cross-sectoral, then new architectural designs that are more centralised and do not operate across sectoral lines should be considered by Europe, such as a twin-peaks model and/or the establishment of more direct supervisory mechanisms.

This paper is structured as follows: (2) an overview of the DORA Regulation and its main pillars; (3) the identification and discussion of three selected challenges, namely ensuring supervisory convergence, limited centralisation on the development of solution and cooperation, coordination and fragmentation in the Oversight Framework; (4) discussion; and (5) conclusions. The points on supervision made in this paper were expressed by one of the authors during a panel session on this topic held as part of the EUROFI conference in Ljubljana in September 2021.[2]

2 The digital operational resilience act (the DORA regulation)

The DORA Regulation was published in the EU Official Journal and proceeded to enter into force on 16 January 2023. The DORA Regulation will be fully applicable from 17 January 2025, following a two-year implementation period.

The DORA Regulation is a cross-sectoral regulation[3] that introduces a comprehensive and harmonised framework addressing various core components of ICT risk and cybersecurity with the final aim of increasing financial entities' digital operational resilience. The DORA Regulation will have implications for all stakeholders involved: the financial entities, ICT third-party service providers (ICT TPPs) and the financial supervisors, which will be responsible for the supervision and the overall monitoring of a financial entity's compliance vis-à-vis the DORA Regulation.

The DORA Regulation follows a set of recommendations by the European Supervisory Authorities (ESAs)[4] on the following: [i] legislative improvements relating to ICT risk management requirements in the EU financial sector;[5] and [ii] an EU-wide coherent cyber-resilience testing framework. In view of the: [i] challenges that ICT risks continue to pose on the resilience, performance, and stability of the EU financial system; and [ii] financial services industry reportedly experiencing more cyber-attacks than any other industry (before and during COVID-19), the Regulation is necessary to ensure a more coherent and harmonised approach to the regulation of

[2] See EuroFi, 'Digital operational and cyber-resilience: are EU proposals fit-for-purpose? (DORA, NIS…)?' (8.9.2021) <https://www.eurofi.net/session/digital-operational-and-cyber-resilience-are-eu-proposals-fit-for-purpose-dora-nis/> last accessed 8.3.2024.

[3] See Article 2 of the DORA Regulation for the full scope.

[4] European Banking Authority, 'ESAs Publish Joint Advice of Information and Communication Technology Risk Management and Cybersecurity', *European Banking Authority*, (10.4.2019) <https://www.eba.europa.eu/esas-publish-joint-advice-on-information-and-communication-technology-risk-management-and-cybersecurity> last accessed 4.3.2024.

[5] Joint Committee of the ESAs, 'Joint Advice of the European Supervisory Authorities: To the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector', *Joint Committee of the ESAs*, (10.4.2019) JC 2019 26 <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/4d2ad5e2-1570-48bd-819a-7cd9b4e8b157/JC%202019%2026%20%28Joint%20ESAs%20Advice%20on%20ICT%20legislative%20improvements%29.pdf?retry=1> last accessed 4.3.2024.

cyber risk. Notwithstanding relevant ESAs Guidelines on ICT risk and cybersecurity[6] and provisions emanating from several sectoral-specific EU legal instruments,[7] until the adoption and implementation of the DORA Regulation, ICT risk continues to be treated in different ways by National Competent Authorities (NCAs). The resulting inconsistent approaches have brought about a proliferation of individual national regulatory initiatives.

The DORA Regulation addresses lacunae, as well as the fragmentation and inconsistencies, within the current financial services regulatory and supervisory framework applicable in the field of ICT risk and cybersecurity and, more generally, digital operational resilience. For example, it creates a level playing field on supervisory powers where currently there is none (all supervisory authorities will have the same supervisory powers and enforcement measures). It also addresses the lack of incident reporting requirements for some sectors,[8] whilst avoiding dual-reporting regimes.[9] The DORA Regulation also introduces provisions on information sharing arrangements on cyber threat information and intelligence are on a voluntary basis.[10] This is a good starting point towards better participation in, and co-ordination of, the exchange of such information.[11]

In addition to the above, once fully applicable (17 January 2025), the DORA Regulation will introduce mandatory advanced testing through Threat-Led Penetration

[6]Namely, the EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04); EBA Guidelines on Outsourcing Arrangements (EBA/GL/2019/02); EIOPA Guidelines on ICT Security and Governance (EIOPA-BoS-20/600); EIOPA Guidelines on Outsourcing to Cloud Service Providers (EIOPA-BoS-20-002); and ESMA Guidelines on Outsourcing to Cloud Service Providers (ESMA50-157-2403). Note that these Guidelines are soft law-based and that Member States are not legally bound to apply such Guidelines in their jurisdictions. The ESAs employ a name and shame approach via the publication of compliance tables, which outline which Member States have decided to comply. Another limitation of such Guidelines is that they are sector specific and that the requirements were not harmonized across sectors, for instance ESMA did not have any guidelines governing ICT and security risk management.

[7]For a full schematic of the fragmentation across EU legal instruments in regards to ICT risk and cybersecurity see European Commission, 'Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014' SWD(2020) 198 final. 66.

[8]Most noticeably, the incident reporting mechanism established by Article 96 of Directive (EU) 2015/2366 (Payment Services Directive 2 or 'PSD2') over payment service providers.

[9]Amendments introduced to Directive (EU) 2015/2366 via Directive (EU) 2022/2556 (also referred to as the 'DORA Amending Directive) repeals the requirement for payment service providers to report incident under PSD2. Instead, these entities will report solely under the DORA Regulation, pursuant to Article 23 of the DORA Regulation. In addition, because the DORA Regulation is considered to be *lex specialis* to Directive (EU) 2022/2555 (Network and Information Security Directive 2 'NIS2'), the incident reporting mechanism established by Article 23 of that Directive will not apply to entities also falling within scope of the DORA Regulation – solely the incident reporting mechanism under DORA shall apply. Lastly, financial entities will still be expected to report incidents pursuant to Regulation (EU) 2016/679 (General Data Protection Regulation).

[10]Chapter VI of the DORA Regulation.

[11]Competent authorities need to be notified of financial entities' participation in such information sharing arrangements, pursuant to Article 43(3) of the DORA Regulation. This fact also contributes towards better coordination of such information sharing arrangements.

Testing (TLPT)[12] for financial entities meeting certain criteria.[13] Notwithstanding challenges brought about by the differences between DORA TLPT and the European Central Bank's (ECB) Threat Intelligence-based Ethnical Red Teaming (hereinafter referred to as TIBER-EU Framework),[14] DORA TLPT builds upon already established frameworks for advanced testing and guarantees mutual recognition of completion of the tests across Member States via an attestation to be issued by competent authorities.[15]

In addition, a noticeable increase in the use of cloud service providers has resulted in concerns regarding their systemic nature and impact.[16] In this regard, the DORA Regulation introduces the concept of ICT TPPs, which is a departure from the concept of outsourcing.[17] In this sense, Chapter V section I of the DORA Regulation introduces important requirements for the managing of ICT TPP risk at a financial entity-level, in addition to setting out key contractual provisions that a financial entity needs to have in place in its written contractual arrangements with ICT TPPs.[18]

As part of the managing of ICT TPP risk at a financial entity-level, financial entities will be required to maintain a Register of Information (RoI) with information on all of their contractual arrangements with ICT TPPs.[19] The purpose of the RoI is

[12] Pursuant to Article 26 of the DORA Regulation.

[13] The criterion for selection is to be specified by a Regulatory Technical Standard ('RTS') emanating from Article 26(11)(a) of the DORA Regulation.

[14] During trialogues, there was a strong emphasis by the Commission that advanced testing under the DORA Regulation should be achieved through a TIBER-EU test. However, during trialogues, it was agreed that financial entities could employ internal testers for red teaming (with the exception of significant banks) – this is a major departure from the TIBER-EU framework, which only allows external testers to be used. Other differences were introduced, such as provisions on pooled testing (see Article 26(4) of the DORA Regulation). At the same time, Article 26(11) of the DORA Regulation states that the RTS supplementing DORA TLPT needs to be developed in accordance with the TIBER-EU framework and in agreement with the ECB. These differences between the two testing frameworks have created many challenges and uncertainties surrounding DORA TLPT.

[15] Article 26(7) of the DORA Regulation.

[16] In fact, this was one of the reasons why the EIOPA and ESMA have adopted Guidelines on Outsourcing to Cloud Providers – efforts which predate the DORA Regulation.

[17] The definition of an ICT TPP is an undertaking providing ICT services (see Article 3 point (19) read in conjunction with Article 3 point (21) of the DORA Regulation); whereas outsourcing is defined by the EBA Guidelines on Outsourcing as "*means an arrangement of any form between an institution* (. . .) *and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the* (. . .) *institution itself*." There are, therefore, two main differences between ICT TPPs and outsourcing: (1) ICT TPPs refer to ICT services only, whereas the outsourcing definition is much broader, although it does encompass ICT outsourcing; and (2) the DORA Regulation does not differentiate between a service that could have been undertaken by the financial entity itself, whereas the outsourcing definition does. This means that an ICT TPP is considered as such, even if the service performed by the ICT TPP could (or could not) have been undertaken by the financial entity. As such, the definition of an ICT TPP is much broader than that of outsourcing.

[18] See Article 30 of the DORA Regulation.

[19] Pursuant to Article 28(3) of the DORA Regulation. The RoI is to be supplemented by an Implementing Technical Standard ('ITS'), as mandated by Article 28(10) of the DORA Regulation. For the latest version available (to date) of the ITS see: European Supervisory Authorities, 'Final Report: On Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554' JC 2023 85. <https://www.esma.europa.eu/sites/default/

three-fold: [i] to help financial entities' own management of their ICT TPP risks; [ii] to ensure that supervisors can carry out effective supervision; and [iii] for the designation of Critical ICT TPPs ('CTPPs').[20] For the purposes of the designation of CTPPs, NCAs will receive the RoIs from all financial entities in their jurisdictions and send the RoIs to the ESAs Oversight Forum; the Forum will then, through the Joint Committee, use the data gathered to designate the CTPPs.[21] These CTPPs will be subject to a Union-level oversight framework (the 'Oversight Framework') which consists of a Lead Overseer, a Joint Oversight Network (JON) and the Oversight Forum. The Lead Overseer is, arguably, the most critical role in the Oversight Framework, as it is responsible for the actual on-going oversight of CTPPs, in addition to being empowered in terms of Articles 35 to 40 of the DORA Regulation. Each CTPP will be appointed a specific Lead Overseer, which is one of the ESAs.

3 Some challenges ahead

This section identifies and addresses three selected challenges related to the DORA Regulation, namely: [i] ensuring supervisory convergence; [ii] limited centralisation on the development of solutions; and [iii] cooperation, coordination and fragmentation in the Oversight Framework. These will be individually discussed in the following sub-sections.

3.1 Ensuring supervisory convergence

The first set of challenges relate to supervisory convergence in two areas, most noticeably proportionality and supervisory flexibility. In terms of proportionality, the DORA Regulation introduces a very robust proportionality principle based on the following: [i] exclusions to scope based on the size, risk and complexity of financial entities pursuant to Article 2(3) of the DORA Regulation; [ii] an overarching proportionality principle, *inter alia*, in the context of the implementation of requirements laid down in ICT risk management, as established by Article 4 of the DORA Regulation; [iii] the establishment of a simplified ICT risk management framework[22] (instead of a fully-fledged ICT risk management framework[23]) for a specific sub-set of financial entities; and [iv] exclusions and/or lighter requirements for financial entities that are classified as microenterprises, which can be found throughout the DORA Regulation.

files/2024-01/JC_2023_85_-_Final_report_on_draft_ITS_on_Register_of_Information.pdf> last accessed 7 March 2024. Recital (1).

[20] In accordance with the designation criteria to be supplemented by a delegated act, as referred to in Article 31(6) of the DORA Regulation. For the latest version available (to date) of the designation criteria see: European Commission, 'Commission Delegated Regulation (EU) . . . /... of XXX supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council by specifying the criteria for the designation of ICT third-party service providers as critical for financial entities'. Ares(2023)7798046.

[21] Pursuant to, respectively, Article 31(1) and 31(10) of the DORA Regulation.

[22] Article 16 of the DORA Regulation.

[23] As laid down in Articles 5 to 15 of the DORA Regulation.

One major limitation associated with the above-mentioned proportionality approach is that the DORA Regulation does not specify what is expected of financial entities when implementing the requirements – for example, Article 7 of the DORA Regulation states that financial entities shall use and maintain updated ICT systems, protocols and tools that are proportionate to their activities, but it does not specify what systems, protocols and tools would be proportionate to what activity or size of each entity. Whilst this approach allows for a greater flexibility in the application of requirements, it can also prompt doubt on whether the requirements should be more specific. The ESAs are mandated by the DORA Regulation to take into account proportionality when developing the Level 2 Texts. Against this backdrop, during the public consultation of the first set of Level 2 Texts, stakeholders have raised concerns on the need for more specific proportionality at a requirement level,[24] especially in the context of the RTS on ICT risk management.

Whilst proportionality has indeed been considered when developing the Level 2 Texts, more proportionality at a requirement level has not been introduced, despite the above-mentioned feedback. Here, it is important to consider the fact that the DORA Regulation is principle (and not technical based) and that the ESAs need to remain aligned to the content of the DORA Regulation when drafting the Level 2 Texts, in order to respect their specific mandates. Indeed, the fact that the ESAs have to constantly navigate between constraints imposed at a Level 1 and their specific mandates,[25] can introduce significant challenges to the drafting of Level 2 Texts.

Nonetheless, the adoption of a consistent approach towards supervision of proportionality goes hand in hand with adopting a consistent supervisory approach when carrying out supervision against the requirements of the DORA Regulation.[26] By ensuring a consistent approach, risks of regulatory arbitrage can be mitigated, and a fair level playing can be achieved across the Union.[27] In this vein, a difference must be made between a consistent set of rules and a consistent application of such rules through supervisory practices – whilst the DORA Regulation might guarantee the former, it does not directly achieve the latter.

Lastly, even though the DORA Regulation is cross-sectoral, considerations regarding the promotion of convergency and consistency in terms of the applicability of the proportionality principle need to duly take into account sectoral specificities. In order to do so, there must exist strong coordination mechanisms between the ESAs themselves and from each ESA to each NCA, as relevant – depending on whether the Member State adopts a fully centralised supervisory model or a sectoral approach. It is important that all of these stakeholders at European and national levels converge.

[24] See European Supervisory Authorities, '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' (17.1.2024). JC 2023 86. 117.

[25] Challenge which arises from constitutional issues, such as the balance of institutional balance of power at the EU level, the *Meroni* Doctrine and the comitology procedure.

[26] This was also one of the points raised by stakeholders during the public consultation of Level 2 Texts. See: European Supervisory Authorities (ft 26) 116-117.

[27] Indeed, the importance of harmonisation of supervisory practices had been one of the points raised by the *De Larosiere* report. See: Jacques de Larosière, 'The High-Level Group on Financial Supervision in the EU' (2009, ECO/259-EESC-2009-1476) 33.

Another challenge is in relation to tight timelines. As previously stated, the DORA Regulation is producing a substantial number of Delegated Acts,[28] Technical Standards[29] and Guidelines[30] (often hereinbefore collectively referred to as 'Level 2 Texts') currently being developed by the ESAs. This creates challenges for both NCAs – which have to, *inter alia*, transition towards the supervision of new requirements, adopt and implement solutions for the receival of major ICT-related incidents, significant cyber threats and the RoI (both which are to be supplemented by Level 2 Texts), obtain expertise and establish and a TLPT cyber team and dedicate resources towards the Oversight Framework – and for financial entities, which have to comply with the requirements of the regulation, when several of such requirements have yet to be finalised.

The rationale behind adopting Level 2 Texts is largely two-fold: [i] by delegating drafting of highly technical texts to EU agencies such as the ESAs, the Commission can leverage on the ESAs technical expertise; and, perhaps most importantly, [ii] if these Level 2 Texts were drafted and subsequently discussed at a trialogue stage it would potentially take significantly more time for EU legislation to go from a proposal to an adoption stage. In other words, the Commission can leverage on Level 2 Texts as an attempt to supplement Level 1 Texts, concomitantly gaining time as such texts are drafted in between the date of adoption and the date of applicability of EU law. As expected, the downside is that stakeholders involved, including the ESAs, NCAs and financial entities have significantly less time to draft, implement and comply with the new rules as the measures emanating from Level 2 Texts would have

[28]There are two delegated acts that are currently being developed with respect to which the ESAs have provided advice to the European Commission, namely the criteria to designate ICT third-Party service providers as critical and the fees those service providers have to pay to be overseen and determining the amount of the oversight fees to be charged by the Lead Overseer to critical ICT third-party service providers and the way in which those fees are to be paid. See European Commission, 'Implementing and delegated acts – DORA' (22.2.2024) <https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en> last accessed 9.3.2024.

[29]Technical Standards currently being developed in this field: (1) RTS on ICT risk management framework (article 15) and RTC on simplified ICT risk management framework (Article 16(3)); (2) RTS on criteria for the classification of ICT-related incidents (Article 18(3)); (3) ITS to establish the templates for the register of information (Art 28(9)); (4) RTS to specify the policy on ICT services performed by ICT TPPs (article 28(10)); (5) RTS and ITS on content, timelines and templates on ICT-related incident reporting (Article 20); (6) RTS on TLPT (Art.26(11)); (7) RTS on subcontracting of critical or important functions (Art.30(5)); (8) RTS on oversight harmonisation (Art.41(1)); and (9) Guidelines on Oversight Cooperation (Art.32(7)). For a complete list see the following: European Supervisory Authorities, 'Digital Operational Resilience Act (DORA): public consultation on the first batch of policy products' (19.6.2023) <https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2023/Consultation%20Papers%20on%20DORA/1056506/Public%20consultation%20overview%20document.pdf> last accessed 9 March 2023; and European Supervisory Authorities, 'Digital Operational Resilience Act (DORA): Public consultation on the second batch of policy products' (8.12.2023) <https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2024/JC%20DORA/1064194/DORA%20public%20consultation%20on%20the%20second%20batch%20of%20policy%20products_overview%20document.pdf> last accessed 9.3.2024.

[30]Guidelines being developed in this field: (1) Guidelines on oversight cooperation between the ESAs and competent authorities (Article 32(7)); and (2) Guidelines on aggregated costs and losses from major ICT-related incidents (Article 11(1)). See *ibid*.

only been made available and adopted, in some cases, significantly after the Level 1 Text.

Indeed, the authors note that there have been several comments submitted as part of the public consultation on the first batch of Level 2 Text questioning the ESAs on whether the date of applicability of Level 2 Texts could be postponed (particularly in the case of the ITS supplementing the RoI and the RTS on ICT risk management[31]). This has also been a common complaint received by NCAs from financial entities.[32] Of course, postponing the date of applicability is not an option due to legal compliance with Level 1. In this context, it is then up to the NCAs to exert the necessary degree of discretionary supervisory flexibility *vis-à-vis* the requirements of the DORA Regulation, especially in relation to those requirements prescribed at a Level 2. Once again, the ESAs – considering their aforementioned role in the promotion of supervisory convergency and consistency – might have a future role to play in this regard. Nonetheless, supervisory convergence should be achieved in this regard.

3.2 Limited centralisation on the development of solutions

The DORA Regulation introduces the indirect need for NCAs to develop at least two solutions: [i] a solution for the receival and upstream reporting of major ICT-related incidents and significant cyber threats; and [ii] a solution for the receival and upstream reporting of the RoI.

In relation to [i], financial entities that experience an ICT-related incident that meet the criteria[33] specified by the DORA Regulation are obliged to report these incidents to the competent authority designated in terms of Article 19(1) subparagraph 2 of the DORA Regulation. The reporting of these incidents follows a three-tiered approach, comprised of an initial report, an intermediate report, and a final report[34] – to be submitted following the closure of a major ICT-related incident. In a timely manner (for each of the reports received), the NCA needs to relay these reports to several stakeholders, as relevant and applicable.[35] The DORA Regulation specifically mentions the following stakeholders: ESAs, ECB, national Computer and Security Incident Re-

[31] See, for example: European Supervisory Authorities (ft 26) 114 in respect of the ICT risk management framework; and European Supervisory Authorities (ft 21) 15 in respect of the RoI.

[32] See Malta Financial Services Authority, 'Feedback Statement to Queries Raised by Consulted Stakeholders on Regulation (EU) 2022/2554 on Digital Operational Resilience (the 'DORA Regulation')' (19.2.2024) <https://www.mfsa.mt/wp-content/uploads/2024/02/Feedback-Statement-to-Queries-Raised-by-Consulted-Stakeholders-on-Digital-Operational-Resilience.pdf> last accessed 9.3.2024. 4.

[33] The criteria are to be supplemented by an RTS. For the latest version of the criteria see: European Supervisory Authorities, 'Final Report on Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554' (17.1.2024) JC 2023 83 <https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_83_-_Final_Report_on_draft_RTS_on_classification_of_major_incidents_and_significant_cyber_threats.pdf> last accessed 10.3.2024.

[34] Article 19(4) of the DORA Regulation, to be supplemented by an ITS and an RTS. For the latest version of the reporting templates see European Supervisory Authorities (ft 31).

Article 19(7) of the DORA Regulation.

[35] Article 19(6) of the DORA Regulation.

sponse Teams (CSIRTs),[36] resolution authorities and other relevant authorities under national law. In the case of significant banks, NCAs shall receive major ICT-related incident reports and notifications of significant cyber threats and immediately transmit them to the ECB.[37] The ESAs, based on the reports received from the NCAs, shall assess whether the major ICT-related incident is relevant for NCAs in other Member States; and the ECB shall, where reported, notify the European System of Central Banks (ESCB). This assessment needs to be carried out in cooperation with the relevant NCA and the European Union Agency for Cybersecurity (ENISA).[38]

In relation to [ii], financial entities shall report at least yearly to the NCAs the number of new arrangements with ICT TPPs and, in addition to making it available to the NCA (upon its request) the full RoI or sections thereof.[39] The NCAs will then, on a yearly and aggregate basis, transmit all of the RoIs to the Oversight Forum.[40] As previously mentioned, the Oversight Forum will then use these RoIs for the purposes of designation of CTPPs.[41]

It is important to note that whilst the reporting mentioned in point [i] is an *ad hoc* report – i.e., reporting only takes place following a major ICT-related incident and/or a significant cyber threat; the report of the RoIs mentioned in point [ii] is a much more cumbersome yearly reporting from the financial entities to NCAs and from NCAs to the Oversight Forum. The scope of the reporting is also significantly larger, due to the complexity of the RoIs, considerations on the basis of reporting due to levels of consolidation and, more importantly, the high number of financial entities in scope of the DORA Regulation due to the fact that the Regulation is cross-sectoral.[42]

Whilst both reports have their own *sui generis* challenges, it is the authors' view that they share one important indirect limitation: the fact that NCAs will have to develop 27 different solutions to be implemented at national level for the purposes of receival and upstream transmission on all of these reports – assuming that each Member State implements just one solution for each reporting at national level. In addition, to the NCAs, it will most likely be the case that the ESAs themselves will have to implement their own solutions for purposes of receival of incident reports and the RoI.

In the case of major ICT-related incident reports and notifications of significant cyber threats, Article 21 of the DORA Regulation mandates the ESAs, through the

[36] Notwithstanding legal discretions introduced by Article 19(1) subparagraph 5 and Article 19(2) subparagraph 2, where Member States may require financial entities to also submit incident reports and significant cyber threat notifications, respectively, to the National CSIRT. Adopting this approach can create dual reporting.

[37] Article 19(1) subparagraph 2 of the DORA Regulation for the transmission of major ICT-related incidents and Article 19(2) subparagraph 1 of the DORA Regulation for the transmission of notifications of significant cyber threats.

[38] Article 19(7) of the DORA Regulation.

[39] Article 28(3) subparagraphs 3 and 4 of the DORA Regulation, respectively.

[40] Article 31(10) of the DORA Regulation.

[41] *Ibid*.

[42] Notwithstanding other challenges with the reporting of major ICT-related incidents and significant cyber threats, such as the fact that the upstream reporting to the ESAs and immediate reporting to the ECB are time sensitive and might mean that NCAs need to have 24/7 availability.

Joint Committee, to prepare a report on the feasibility of setting up a single EU hub for the centralisation of reporting of major ICT-related incidents. However, the deadline for the submission of the feasibility report is by the date of applicability of the DORA Regulation (17 January 2025). By such date, NCAs already need to have developed and put in operation solutions for the receival of major ICT-related incidents and notifications of significant cyber threats, thereby ensuring compliance with the DORA Regulation. Nonetheless, it is important to remember that a feasibility report is not a guarantee that an EU hub for centralisation of such reports will actually be established.

It is, therefore, the authors' view that the fact that NCAs will have to develop 27 different solutions is a suboptimal arrangement, with, potentially, a very high financial cost implication for all stakeholders involved; in addition to introduction risks in relation to lack of convergence of solutions. Indeed, more centralisation should be considered in this regard in the future, including on the RoI – which does not have a feasibility report, such as in the case with the single EU hub for incident reporting. Although the rationale for not centralising these two returns is not clear, it is understandable that the NCAs, as the day-to-day supervisors, are the financial entities' primary point of contact (and not the ESAs).

3.3 Cooperation, coordination and fragmentation in the oversight framework

As previously stated, the DORA Regulation establishes an Oversight Framework for the purposes of oversight on CTPPs – which are to be designated as such by the ESAs through the Joint Committee, in accordance with the designation criteria.[43] The Oversight Framework is comprised of multiple institutional players, both at national and supranational levels. At a European level, the Oversight Framework is comprised of the following: [i] the Lead Overseer; [ii] the Oversight Forum;[44] and [iii] the JON.[45]

In relation to [i], each CTPP shall be appointed a Lead Overseer – EBA, EIOPA or ESMA, in accordance with Article 31(1) point (b) of the DORA Regulation. The Lead Overseer is responsible for the conduct of oversight *vis-à-vis* CTPPs and it shall assess (through, for instance, inspections and request for information) whether the CTPP has the necessary rules, procedures, mechanisms and arrangements in place to manage the ICT risk which it may pose to the financial entities using its services.[46] In addition, the Lead Overseer has several powers – including hard law and soft law powers[47] – in relation to the CTPPs, both inside and outside of the Union.[48]

The activities of the Lead Overseer, namely general investigations or inspections, are assisted by Joint Examination Teams (JETs).[49] In the context of oversight activ-

[43] See ft. 22.

[44] Established by Article 32(1) of the DORA Regulation.

[45] Established by Article 34 of the DORA Regulation.

[46] Article 33(1) and (2) of the DORA Regulation.

[47] Hard law powers include the issuance of periodic penalties, pursuant to Article 35(6) of the DORA Regulation; whilst soft law powers refer to name and shame and/or comply or explain mechanisms, pursuant to Article 42(2) of the DORA Regulation.

[48] The powers of the Lead Overseer are specified in Articles 35 to 39 of the DORA Regulation.

[49] Established by Article 40(1) of the DORA Regulation.

ities *vis-à-vis* a single CTPP, there shall be designated a Lead Overseer and a JET. The JETs are composed of the following: the ESAs and the NCAs supervising the financial entities that make use of that CTPP and, on a voluntary basis, one NCA from the Member States where the CTPP is established and (where applicable) a representative from the nationally designated competent authority for the purposes of the NIS 2 Directive.[50]

Regarding [ii], the Oversight Forum is a sub-committee that supports the work of the Joint Committee and the Lead Overseers in the area of ICT TPP risk. The forum is required to regularly discuss relevant developments and, more importantly, it carries out a collective assessment of the findings of the activities of the Oversight Framework and promotes coordination measures.[51] The Oversight Forum is composed of several stakeholders, as specifically provided in Article 32(3) of the DORA Regulation. These stakeholders are, *inter alia*: Chairpersons and Executive Directors of each ESA, NCAs (and, where applicable, and additional representative), representatives from the European Systemic Risk Board (ESRB), ECB, ENISA and, where applicable, a representative from the nationally designated competent authority for the purposes of the NIS 2 Directive.

Lastly, point [iii] relates to the JON, which is established for the purpose of coordination oversight activities and to ensure a consistent approach among the three Lead Overseers.

Whilst the Oversight Framework plays a role in the oversight of CTPPs, NCAs remain responsible for the follow-up of the recommendations provided by the Lead Overseer at national level. In other words, "*NCAs are the primary point of contact for financial entities under their supervision. The competent authorities are responsible for the follow-up concerning the risks identified in the recommendations concerning financial entities making use of services provided by CTPPs*.[52]" This means that financial entities making use of services provided by CTPPs need to, at an organisational level, appropriately manage the risks identified via the Oversight Framework. In turn, NCAs need to ensure that financial entities are indeed managing such risks. As a measure of last resort, NCAs can require financial entities to terminate, in part or completely, the relevant contractual arrangements concluded with the CTPP.[53] Oversight harmonisation is technically supplemented by a RTS on harmonisation of

[50] Recital (20) of the DORA Regulation explains that "cloud computing service providers is one category of digital infrastructure covered by Directive (EU) 2022/2555". These cloud service providers will have to put in place the necessary cybersecurity measures, as specifically set out in NIS 2. These cloud service providers will, most likely, be designated as CTPPs under the DORA Regulation. Therefore, recital (20) clarifies the activities of the Oversight Framework are complementary to the supervision carried out pursuant to NIS 2 by competent authorities. NIS 2 competent authorities, where meetings concern cloud service providers, will participate as representatives in the Oversight Framework to ensure consistency – in the absence of a cross-sectoral and single authority for oversight of CTPPs.

[51] Article 32(2) of the DORA Regulation.

[52] European Supervisory Authorities, 'Consultation Paper Draft joint guidelines on the oversight cooperation and information exchange between the ESAs and the competent authorities under Regulation (EU) 2022/2554' (27.11.2023) <https://www.esma.europa.eu/sites/default/files/2023-12/JC_2023_71_-_CP_on_draft_Guidelines_on_oversight_cooperation.pdf>.17.

[53] Article 42(6) of the DORA Regulation.

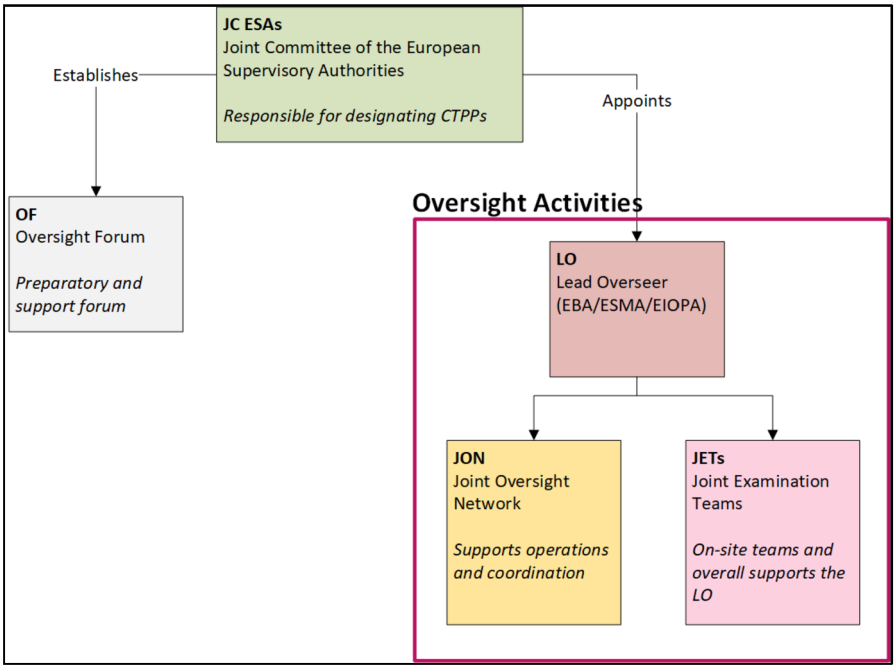

Fig. 1 Structure of the Oversight Framework. Source: Author's own compilation

conditions enabling the conduct of oversight activities[54] and Guidelines on oversight cooperation and information exchange between ESAs and NCAs.[55]

When the DORA Regulation was still at proposal stage, the Joint Chairs of the ESAs produced an opinion on the legislative proposal.[56] The opinion, *inter alia*, argued that the Oversight Framework had a number of limitations, it needed more streamlined and effective governance, it was too complex and that "(…) *it would require an unprecedented cooperation between our authorities in the oversight of cross-sectoral CTPPs* (…)".[57] As an alternative, it was suggested that a joint-ESA executive body should be established, and it assume the majority of the tasks now associated with the Lead Overseer and the Oversight Forum.

[54]For the latest version to date see: European Supervisory Authorities, 'Consultation Paper Draft regulatory technical standard on the harmonisation of conditions enabling the conduct of the oversight activities under Article 41(1) points (a), (b) and (d) of Regulation (EU) 2022/2554' (27.11.2023) <https://www.esma.europa.eu/sites/default/files/2023-12/JC_2023_69_-_CP_on_draft_RTS_on_oversight_harmonisation.pdf>.

[55]For the latest version to date refer to: European Supervisory Authorities (ft 31).

[56]See Joint Chairs of the European Supervisory Authorities (ESAs). 'DORA: Joint ESAs letter regarding the legislative proposal for a regulation on digital operational resilience for the financial sector' (10.2.2021) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6107_2021_INIT> 2020/0266(COD).

[57]*Ibid* 5.

In terms of follow-up to the recommendations provided by NCAs to financial entities making use of services provided by CTPPs, the Joint Chairs also argued that the ESAs should be further empowered, and that follow-up should happen at EU-level. Indeed, as it stands, there are limited requirements for CTPPs under the DORA Regulation – instead, the majority of requirements are in place for financial entities making use of services provided by the CTPPs. In addition, leaving the follow-up at the hands of NCAs could result in inconsistent approaches and have an impact on the effectiveness of the Oversight Framework.[58] These recommendations were not taken up, with the exception of the creation of the JON for the purposes of coordination of approaches between Lead Overseers.

4 Discussion

The establishment of the ESFS post-2009 global financial crisis represented a shift towards more centralisation, coordination, convergence and consistency within financial supervision in the EU.[59] The DORA Regulation is indeed an interesting case-study for the purposes of investigating cross-sectoral coordination, consistency, cooperation, convergence, and centralisation within the ESFS. This paper has introduced and discussed three challenges that the authors believe that supervisors are having or will have to face in the future, namely: [i] ensuring supervisory convergence; [ii] limited centralisation on the development of solutions; and [iii] cooperation, coordination and fragmentation in the Oversight Framework. More broadly, it is the authors' view that these challenges illustrate that there are still issues in relation to coordination, consistency, cooperation, centralisation and convergence that are yet to be solved by the ESFS, especially in the context of cross-sectoral undertakings.

In relation to [i], the DORA Regulation's principle-based nature coupled with its proportionality principle gives little specific guidance on how financial entities are expected to fulfil requirements emanating from the DORA Regulation. In addition, tight deadlines for its implementation have prompted NCAs to issue statements regarding supervisory flexibility. In this context, promoting supervisory convergence and consistency of supervisory practices is one of the many mandates of the ESAs,[60] considering that supervision remains de-centralised and at the hands of NCAs.[61] The

[58] *Ibid* 7.

[59] Pablo Iglesias-Rodriguez, 'Supervisory Cooperation in the Single Market for Financial Services: United in Diversity?' (2018) 41(3) *Fordham International Law Journal*, 621.

[60] See Article 1 of the ESAs founding regulations, namely Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24.11.2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC [L 331/12]; Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24.11.2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC [L 331/48]; and Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24.11.2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC [L 331/84].

[61] Certain exceptions apply via direct supervisory mechanisms, such as the ECB's supervision of significant banks via the Single Supervisory Mechanism (SSM), and ESMA's direct supervision over credit rating agencies, trade repositories and administrators of critical benchmarks.

promotion of such convergency and consistency is supported by instruments such as exchange of information via sub-committees, task forces, groups, Q&As and supervisory handbooks, in addition to soft law-like mechanisms, such as peer reviews and comply and explain. Whilst it is the authors' opinion that the ESAs have indeed managed to address grave lacunae left by the ESFS' predecessor (namely the Lamfalussy Architecture) in terms of convergence and consistency; literature continues to question to what extent these soft law-like mechanisms are indeed appropriate and sufficient to promote convergence and consistency across the Member States.[62]

Regarding [ii], the fact that 27 EU Member States have to develop different solutions for the same two purposes (reporting of major ICT-related incidents and the notification of significant cyber threats and the receival of the RoI) is a significant limitation and could imply duplication of costs across the Union. More importantly, there need to be strong convergence and cooperation mechanisms in place to ensure that all of these 27 different solutions are, to the extent possible, harmonised across Member States.[63] In the context of the RoI, this is particularly important in order to ensure that the Oversight Forum receives complete and quality data for the purposes of the designation of CTPPs. The ITS on the RoI offers little convergence at a technical level, because the ESAs were simply not mandated at Level 1 to develop specifications in relation to the reporting from financial entities to NCAs and any subsequent upstream reporting thereafter.[64] In addition, because the ESAs developed the ITS on the RoI to be technologically neutral via open tables,[65] this convergence becomes even more important.

Lastly, in relation to [iii] on the cooperation, coordination and fragmentation in the Oversight Framework, notwithstanding the RTS and Guidelines on harmonisation,[66] the authors' share the previously-mentioned Joint Chairs of the ESAs' views and also perceive the Oversight Framework as unnecessarily complex and sub-optimal – as it introduces risks in relation to inconsistent follow-up and the need for unprecedented cooperation among several stakeholders. Ensuing the applicability of the DORA Regulation, NCAs must dedicate resources not only to the supervision of their financial entities, but also of CTPPs. They should do so in accordance and coordination with all stakeholders involved, including stakeholders at a national level, such as NIS 2 competent authorities.[67]

[62] See, for instance: Kostas Botopoulos, 'The European Supervisory Authorities: role-models or in need of re-modelling?' (2020) 21, *ERA Forum* <https://doi.org/10.1007/s12027-020-00609-7>183.

[63] The authors are aware of some developments related to the creation of a task force for this purpose, however the contours of such harmonisation are yet to be defined.

[64] European Supervisory Authorities (ft 21) 4.

[65] *Ibid* recital (6).

[66] Indeed, most harmonisation requirements emanate from the Guidelines on Harmonisation. Guidelines promote a common understanding but are not legally binding. It is up to the Member States to comply or not to comply with such guidelines. Usually, the consequences for non-compliance with guidelines is soft law-based, through name and shame and comply and explain mechanisms. For example, the ESAs compile and make publicly available a compliance table, with *inter alia* information on those Member States that have not complied and the reason for such.

[67] It should be note that this type of national coordination, including with NIS 2 authorities, is not covered by the relevant RTS and Guidelines supplementing the Oversight Framework.

At a European level, the three ESAs must collaborate closely within the remit of the Joint Committee, the Oversight Forum and the JON. Matters are further complicated by the fact that CTPPs probably do not just offer their services to a particular sub-sector within the financial services sector, but to the sector in its entirety (*e.g.*, it is not likely that a cloud service provider would only provide cloud hosting services to insurance undertakings). Therefore, one questions why no further centralisation was adopted. Indeed, in the Commission impact assessment to the proposal for the DORA Regulation, the Commission considered the setting up of a specific EU-level authority within the financial services sector responsible solely for the supervision of CTPPs. However, this option was not taken up due to perceived high projected costs and, most importantly, because CTPPs do not just offer services to the financial sector, but to other sectors as well.[68] It is not clear, however, how the setting up of the Oversight Framework addresses the issue of supervising CTPPs that operate across sectors within the EU.

The above-mentioned challenges could have been largely tackled by the development of a convergent and harmonised understanding of requirements emanating from the DORA Regulation, a single set of technological solutions and a more centralised architecture for oversight of CTPPs. This would also have brought more clarity to the NCAs and operators themselves. Indeed, whilst it is true that the DORA Regulation is not yet applicable and that it still remains to be seen whether the aforementioned challenges will be tackled and how, the fact is that many of these challenges reflect limitations stemming from wider issues within the ESFS. This is because the DORA Regulation was created to fit the architectural design of the ESFS, which is inherently complex and fragmented. In an environment of cross-border business and freedom to provide services, fragmentation brings risk to the effectiveness of financial supervision. This is true also in the field of the supervision of ICT and cyber risks.

Indeed, one may argue that Europe is still too fragmented from a supervisory perspective. We now have five bodies[69] (about to become six, considering the new Anti-Money Laundering Authority) responsible for convergence and over sixty authorities at national levels responsible for financial supervision within their own jurisdictions. Therefore, the extent to which the current sectoral institutional architecture for financial supervision of the financial industry is still adequate is a pertinent question. This is further exacerbated by the fact that cross-sectoral matters (such as the DORA Regulation) that require a high level of cooperation, convergence and coordination are on the rise.[70]

The authors believe that one alternative would be the creation of a cross-sectoral framework for financial supervision in the EU, based on the twin-peak model.[71] In such a model, one authority would be responsible for prudential supervision (including the supervision of cyber risks and, more broadly, operational risks) and the other

[68] See European Commission (ft 9) 49.

[69] The three ESAs, ESRB and the ECB.

[70] Sustainable finance is yet another good example of this.

[71] The authors note that other authors have raised the same recommendation for Europe, considering the role of conglomerates, see: Dirk Schoenmaker and Nicolas Véron, 'A 'Twin Peaks' Vision for Europe' in Andrew Godwin and Andrew Schmulow (eds), *The Cambridge Handbook of Twin Peaks Financial Regulation*, (Cambridge University Press 2021).

authority would focus on conduct supervision. The underlying idea is that market developments have been gradually erasing the traditional sectoral lines and that giving (or distributing) ownership of a particular supervisory issue is not the most efficient and effective approach.[72] By adopting a more centralised model, Europe would essentially simplify the current architecture and promote centralisation of supervision and supervisory practices. Of course, this would incur deep changes to the *status quo*, considering that Europe's sectoral model has been inherited from the old Lamfalussy architecture,[73] which also relied on a sectoral design.

In addition to the twin-peak model, Europe could also benefit from the introduction of other direct supervisory mechanisms,[74] where applicable, as an avenue towards achieving more gradual centralisation. In this vein, the Commission has stated that, in line with the action plan on the establishment of a Capital Markets Union, it will seek to propose direct supervisory mechanisms in appropriate areas, and, in this spirit, it has included mandates for ESAs oversight in the DORA Regulation via the Oversight Framework.[75] However, as previously argued, the authors believe that the Oversight Framework is not sufficiently centralised and could have benefited from a more streamlined design, including that of a direct supervisory mechanism of CTPPs by the three ESAs.

Considering the above, it is important to note that the establishment of direct supervisory mechanisms involve the delegation of powers from national to the supranational – and achieving the necessary level of political will to do so is no easy task. Indeed, the necessary political will towards reform and, more importantly, towards delegation of power to the supranational within the context of the ESFS often happens in the aftermath of a crisis.[76] Therefore, the ESFS is inherently a reactive (rather than proactive) institutional set-up, as it waits for crisis to unveil in order to adopt the necessary reforms.[77]

5 Conclusion

The DORA Regulation is a much-needed addition to Europe's single rulebook as it addresses and harmonises requirements on ICT risk and cybersecurity across the Union – something which was previously lacking. At the same time, it is important

[72] Jeroen J. M. Kremers, Dirk Schoenmaker and Peter J. Wierts, 'Cross-Sector Supervision: Which Model? (2003) *Brookings-Wharton Papers on Financial Services* <http://dx.doi.org/10.1353/pfs.2003.0004> 227.

[73] Lamfalussy's Committee of the European Banking Supervisors (CEBS), the Committee of European Insurances and Occupational Pensions Supervisors (CEIOPS) and the Committee of European Securities Regulators (CESR) became, respectively, EBA, EIOPA and ESMA following the ESFS reform.

[74] Such as the SSM and ESMA's direct supervision over credit rating agencies, trade repositories and administrators of critical benchmarks.

[75] European Commission, 'Report from the Commission to the European Parliament and the Council on the operation of the European Supervisory Authorities (ESAs) (2022) COM(2022) 228 final. 12.

[76] Beatriz B. Zimmermann & Christopher P. Buttigieg, 'A History of Continuous Power Delegation: The Establishment and Further Development of the European System of Financial Supervision' (2023) *Law and Financial Markets Review* <https://doi.org/10.1080/17521440.2023.2181671> 14.

[77] *Ibid*.

to note that designating cross-sectoral laws in the context of a sectoral-based architecture for financial supervision (in addition to variables at national levels) is no easy task and that unprecedented level of coordination and cooperation as needed. This paper's main argument is that the DORA Regulation, albeit a very positive development, has created a number of challenges with regard to supervisory convergence, cooperation, coordination and fragmentation for authorities, supervisors and regulators.[78] In an environment of cross border business and freedom to provide services, fragmentation brings risk to the effectiveness of financial supervision. This is true also in the field of the supervision of ICT risk and cybersecurity. The three challenges presented in this paper were just some selected examples of such.

However, it is important to recognise that this is not inherently a 'DORA problem': indeed, the DORA Regulation has been created to fit the architectural design of the ESFS, which is inherently complex and fragmented, and operates along sectoral lines. If the future of financial regulation and supervision is cross-sectoral, then new architectural designs that are more centralised and do not operate across sectoral lines should be considered. In terms of such design, the authors believe that Europe could benefit from further centralisation, either through the adoption of a twin-peaks model and/or the establishment of more direct supervisory mechanisms. Throughout history, major overhauls to the architecture of financial supervision in Europe have only taken place post-crises. In this context, Europe has assumed a reactive (rather than proactive) stance. If further centralisation is needed, do we really need to wait for another crisis to reform the ESFS along these lines?

Funding Open Access funding provided by the University of Malta.

Declarations

Competing Interests The authors declare no competing interests.

[78] The authors acknowledge that the DORA Regulation is not yet applicable. In this sense, the authors invite scholarship to continue to investigate whether such challenges have been resolved and/or whether new challenges have arisen, as supervisors gain more experience and clarity in terms of the DORA Regulation.