Erion Murati

Governance of ICT Third-Party Risk under DORA

A Technical and Legal Assessment

Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA), applicable across the EU since 17 January 2025, establishes a harmonised framework for strengthening the digital operational resilience of financial entities. Among its requirements is the effective governance of ICT service providers, which are indispensable to core financial activities such as payments. This article examines the technical measures and legal requirements for managing ICT third-party risk, with particular attention to their practical implementation.

1 Introduction

ICT services are indispensable to the financial sector, as they enable core activities such as payments, trading, and insurance operations in an increasingly digital environment. At the same time, digitalisation and interconnectedness significantly increase exposure to cyberattacks and system disruptions, which may rapidly propagate across the financial system. This high level of dependence on ICT necessitates stronger digital operational resilience in order to safeguard the stability of financial markets. With the entry into force of the Digital Operational Resilience Act (DORA) (EU) 2022/2554 on 17 January 2025,[1] the EU established a comprehensive regulatory framework to strengthen the digital operational resilience of financial entities. They are required to implement a comprehensive ICT risk management framework encompassing governance arrangements, security measures, ICT-related incident management, operational resilience testing, and strict management and oversight of ICT third-party risks.[2] The primary responsibility for compliance with DORA rests with financial entities. Nevertheless, ICT third-party service providers – such as software vendors, IT service providers, data centres, and cloud service providers – also fall within the scope of DORA.[3]

In this context, the article examines the measures and requirements applicable to financial entities for the effective management of ICT third-party risk. First, it analyses the strategies that financial entities should adopt to identify, assess, and mitigate ICT third-party risks. Second, it clarifies and operationalises the definition of ICT services under DORA, with particular focus on the distinction between **"normal ICT services"** and "**ICT services supporting critical or important functions (CIF)"**. Finally, on this basis, the article examines the technical and legal requirements applicable to both categories of ICT services, combining knowledgeable analysis with practical and implementation-oriented considerations.

2 Strategy for ICT-Third Party Risk Management

Financial entities must implement a clear policy-based strategy and governance framework for managing ICT third-party risk, covering both categories of ICT services.[4] Among others, they are required to maintain a comprehensive and up-to-date register of all ICT contractual arrangements and, prior to contracting, to conduct thorough due diligence on ICT providers, assessing risks, security, reliability, and concentration risks, monitor this risk and establish appropriate contingency and exit strategies.[5]

Furthermore, as outlined below, all ICT contracts must include mandatory legal and technical provisions, the scope and depth of which depend on the category of ICT service provided. However, before determining the applicable requirement to the two men-

1 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 (DORA) https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng (Accessed: 21.7.2026).

2 Arts. 5, 6 and 28, Art. 30 DORA.



Dr. Erion Murati

Berater Informationssicherheit
datenschutz nord GmbH

E-Mail: emurati@datenschutz-nord.de

3 Art. 2 Abs. 1 lit. u DORA.

4 Art. 28 Abs. 1 DORA.

5 Art. 5 Abs. 2, lit. i; Art. 6 Abs.9; Art. 28 Abs.1,2,3,4 DORA.

tioned categories of ICT services, it is necessary first to clarify the meaning of ICT service.

2.1 Definition ICT Services under DORA

DORA regulates digital operational resilience in the financial sector to strengthen IT security, defining it as a financial entity's ability to ensure the integrity, reliability, and security of its ICT systems – directly or via ICT third-party providers – to support the continuous and high-quality provision of financial services.[6] To this end, financial institutions are required to identify relevant third-party service providers,[7] assess if they provide an ICT service, and if yes, conclude contracts with them. The Regulation defines "ICT services" broadly as "*digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider*", excluding traditional analogue telephone services. [8] DORA expressly justifies this expansive definition by emphasizing the need to capture risks arising from all types of ICT services in order to maintain a high level of digital operational resilience across the financial sector, including so-called "over-the-top" services.[9]

Nevertheless, despite some examples provided in the recitals, the definition of ICT services remains notably broad and indeterminate, thereby requiring further interpretation and practical clarification, in particular with regard to the key elements of "***digital and data***," "***services***," and "***ongoing basis***," which warrant more precise definition.

First, the element "***digital and data***" may be understood as referring to services that are intrinsically linked to the electronic processing, transmission, or storage of (bits and bytes of) data.[10] While this could encompass a wide range of digitally delivered services, such as software, data provision, and online platforms, doctrine suggests that the digital character must form the essential nature of the service and not merely constitute a subordinate or ancillary component.[11]

Second, under the EU law, "**services**" are commonly understood as activities performed for remuneration[12] rather than the mere transfer of rights. From this perspective, ancillary activities such as user support, SaaS-Platforms, bug-fixing, maintenance, or consultancy would qualify as (ICT) services, whereas the pure licensing of software code (typically characterized as a purchase or rental agreement) would not. However, the DORA Implementing Technical Standard (ITS) based on Art. 28(9) DORA[13] indicate that software licensing (excluding SaaS), defined as "the provision of software run on premises", would be a possible category of an ICT service. Nevertheless, Interpreted in light of DORA's objective of strengthening digital operational resilience, this functional distinction suggests that pure (no support or other related activities) software licensing arrangements fall outside the scope of ICT services.[14]

Finally, the requirement that ICT services be provided on an "***ongoing basis***" is generally interpreted as excluding one-off transactions,[15] such as the one-time delivery of a software licence (without active support such standard application like Microsoft Office Package) which typically constitute rights of use. Likewise, the purchase of the hardware devices and the transfer of ownership including a right to use and it is not in scope of DORA – with exclusion however to hardware as a services support such as for example fixing broken parts which will fall under DORA.[16] Additionally, services provided continuously or for a defined period of time, such as rented software or recurring digital support, are typically considered to meet this criterion.

2.2 DORA categories of ICT Services: Normal versus Supporting a Critical or Important Function (CIF)

Once a financial institution has established that the use of a given software or hardware solution qualifies as an ICT service, the next analytical step is to determine whether that service should be classified as a "**normal ICT service**" or as an "**ICT service supporting a critical or important function** (CIF). It is quite common for new EU cyber laws to make risk-based distinctions between different categories: for instance, the NIS-2 Directive 2022/2555[17] distinguishes between "**important**"" and "**critical**" entities, while the Cyber Resilience Act **(EU)** 2024/2847 instead distinguishes between "**standard**", **"important**," and "**critical**" products.[18] This risk-based distinction also serves to determine the applicable requirements – the more critical the service, product, or entity, the more stringent the requirements. Under DORA, too, the regulatory relevance of this classification lies in its direct impact on applicable obligations: enhanced contractual and technical requirements apply exclusively to ICT services that support a CIF, [19] whereas ICT services that do not meet the CIF threshold remain subject only to baseline requirements.[20]
Consequently, the ICT service classification determines whether the heightened safeguards are triggered. DORA defines an ICT

6 Art. 3 Abs.1 DORA.

7 Art. 3 Abs. 19 DORA.

8 Art. 3 Abs. 21 DORA.

9 Recital 35 and 63 DORA; A list of examples of ICT services can be found in Annex III (S12, S13, S14,) of the ESA Final Report on ITS register of information (10.1.2024).

10 An indicator for this understanding can be drawn from Art. 1Abs. lit. b of Directive (EU) 2015/1535, which refers to services involving the electronic processing and storage of data that are sent, transmitted, and received fully via electromagnetic means.

11 *Lauck*, Der IKT-Dienstleistungsbegriff in der DORA, BKR 2025, 124 (125); *Bernau/Lutterbach*, Digital Operational Resilience Act (DORA), BKR 2023,506 (507).

12 The term services is used for example in Art. 57 of the Treaty on the Functioning of the European Union ("TFEU"): Services shall be considered to be 'services' within the meaning of the Treaties where they are normally provided for remuneration, in so far as they are not governed by the provisions relating to freedom of movement for goods, capital and persons.

13 Commission Implementing Regulation (EU) 2024/2956 of 29 November 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to standard templates for the register of information, Annex III.

14 BaFin (2026) „Management des IKT-Drittparteienrisikos" available at https://www.bafin.de/DE/Aufsicht/DORA/Management_IKT_Drittparteienrisikos/FAQ/FAQ_node.html;jsessionid=2475F8F6FBC845EECE1340D33C64D611.internet972 (Accessed: 21.7.2026)

15 *Lauck*, Der IKT-Dienstleistungsbegriff in der DORA, BKR 2025, 124 (125); *Bernau/Lutterbach*, Digital Operational Resilience Act (DORA), BKR 2023,506 (p.126).

16 Art. 3 Abs. 21 DORA.

17 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32022L2555&qid=1784622349780 (Accessed: 21.7.2026).

18 *Murati* EU Cyber Resilience Act. *Datenschutz Datensich* 49, 89–91 (2025), https://doi.org/10.1007/s11623-025-2049-8 (Accessed: 21.7.2026).

19 Art. 3 Abs. 2 and Art. 30 Abs. 3 DORA.

20 Art. 30 Abs. 2 DORA.

CIF as a function whose disruption, failure, or defective performance would materially impair a financial entity's financial performance, the continuity or soundness of its services, or its ongoing compliance with authorisation conditions or other obligations under financial services law.[21] This definition provides the substantive benchmark against which all ICT services must be assessed.

In the banking context, for example, ICT services are generally considered to support a CIF where they are indispensable to core regulated activities or regulatory compliance. Typical examples include core banking systems processing deposit and loan data, payment and settlement systems, customer authentication and access management solutions, and critical data hosting or cloud services used for production environments or regulatory data. Conversely, ICT services supporting ancillary, non-core, or easily substitutable activities – such as general office productivity software, calendar tools, or non-critical internal communication platforms – will typically not qualify as CIF-related.

As underlined, the distinction between CIF[22] and non-CIF[23] ICT services directly determine the scope and intensity of obligations that financial institutions may impose on ICT service providers, including requirements relating to resilience, monitoring, audit, access, and termination rights. As a core element of DORA's risk-based regulatory framework, the classification of ICT services is left to methodological discretion. Rather than imposing a rigid taxonomy, DORA requires financial institutions to design, document, and apply an internal classification methodology aligned with their business models, operational complexity, and risk profiles.[24] To prevent, however, both over-classification and under-classification of ICT services, DORA requires financial institutions to implement a structured and well-documented governance framework that also considers the proportionality principle.[25] In particular, financial institutions must:

- apply correctly the definition of CIF, formally document their ICT service classification methodology in an internal policy, which is transparent and capable of justification to competent supervisory authorities;[26]
- conduct appropriate pre-contractual due diligence,[27] and maintain a register of all ICT third-party arrangements, distinguishing between CIF-related and non-CIF services;[28]
- rely on further criteria specified in the RTS developed by the European Supervisory Authorities. [29]

To conclude, it is likely that the more ICT services are designed as CIF, the more likely is that their providers will be designated separately as **"critical ICT third-party service provider"**[30] which are subject to enhanced regulatory oversight by the European Supervisory Authorities.[31]

21 Art. 3 Abs. 22 and Recital 70 DORA.
22 Art. 3 Abs. 22 and 30 Abs. 3 DORA.
23 Art. 3 Abs. 21 and 30 Abs. 2 DORA.
24 Recital 63 and Arts. 4 and 28 Abs.1 DORA.
25 Art. 28 Abs. 1lit. b, lit. ii DORA.
26 Art. 28 Abs. 2 DORA.
27 Art. 28 Abs. 4 lit. a DORA.
28 Art. 28 Abs. 3 DORA.
29 See Arts. 1 & 5 of RTS on ICT third-party policy (2024/1773) that it supplements Art. 28(10) DORA and requires every financial entity to have a policy, review annually, covering how they classify and manage ICT services supporting CIFs. It requires to define a Methodology (Art. 3(2) RTS) and also lists factors to be considered for the ICT classification.
30 Art. 2 Abs. 23 DORA.
31 Arts. 31–33 DORA.

2.3. Assessment of DORA legal and technical requirement

DORA requires that third-party ICT risk management obligations be formally set out in written contractual arrangements. It distinguishes between basic legal and technical requirements applicable to all ICT services, and enhanced legal and technical requirements applicable only to ICT services supporting a CIF. These requirements are further examined below.

2.3.1 For all ICT Services (Art. 30 (2) DORA

Financial entities must ensure that all ICT service contracts are concluded in writing and clearly allocate rights and obligations, describe the ICT services and functions provided, specify locations of service delivery and data processing, and include service level agreements, incident assistance obligations, regulatory cooperation clauses, termination rights, and participation in ICT security awareness programmes. [32] Other being said, these contractual safeguards ensure legal enforceability, effective regulatory oversight, and the orderly termination or continuity of ICT services in support of digital operational resilience.

Furthermore, DORA makes it explicit that financial entities "*may only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards*." [33] From a technical perspective, DORA therefore requires ICT contracts to embed concrete information security and data governance controls covering the availability, authenticity, integrity, and confidentiality of both personal and non-personal data.[34] This includes documented TOMs, secure access controls, incident response and assistance mechanisms, and clearly defined procedures for data access, recovery, and return in accessible formats (e.g. CSV, XML, PDF) upon contract termination, insolvency, or service discontinuation.

In addition, financial entities may require normal ICT service providers[35] to demonstrate compliance with appropriate information security standards, such as ISO/IEC 27001, either through formal certification or through well-documented internal ISMS policies and controls. Collectively, these technical requirements operationalise DORA's objectives of digital operational resilience, transparency, and service continuity across both on-premises and cloud-based ICT environments, while reducing concentration and operational risk.

2.3.2 For ICT Services supporting CIF (Art. 30(3) DORA

For ICT services supporting (CIF), baseline contractual obligations are further strengthened by requiring explicitly governing subcontracting conditions and controls, more granular, monitorable SLAs, early-warning notice and incident reporting duties, enforceable rights of access/inspection/audit for the financial entity and competent authorities, and binding exit/transition arrange-

32 Arts. 28 Abs. 2 and 30 Abs.2 DORA.
33 Art. 28 Abs. 5 DORA.
34 Practically, this means the ICT provider must commit to: (a) Keep data accessible and usable when needed (availability); (b) Ensure data and communications are genuine and protected against alteration (authenticity and integrity); and (c) Prevent unauthorised data access or disclosure (confidentiality).
35 Art. 3 Abs. 31 DORA.

ments to ensure continuity during disengagement.[36] Likewise, ICT arrangements supporting CIF are subject to a heightened technical assurance threshold under DORA, which requires financial entities, prior to entering into contractual arrangements, to assess whether ICT third-party service providers *"apply the most up-to-date and highest-quality* ***information security standards****"*.[37] In practice, this expectation is commonly evidenced through recognised standards certifications or attestations, such as ISO/IEC 27001 or SOC 2. While for normal ICT services such certifications may remain facultative, for ICT services supporting CIF the evidence of recognised certification standards is mandatory.

In addition, it is required that contractual arrangements explicitly reflect the provider's obligation to implement and regularly **test business continuity** and contingency plans, alongside maintaining ICT security measures, tools, and policies that are commensurate with the regulated nature of the services provided.[38] This encompasses formal security governance, vulnerability and patch management, continuous monitoring and detection capabilities, documented recovery strategies, and periodic resilience testing, including disaster recovery exercises, all aimed at ensuring service continuity and timely restoration following disruptive events.

Moreover, ICT third-party service providers need to actively participate in and fully cooperate with the financial entity's **threat-led penetration testing** (TLPT) framework.[39] This duty goes beyond mere consent to testing and entails operational cooperation throughout the testing lifecycle, including scoping and planning, coordination of testing windows, facilitation of necessary access, support during execution, and structured remediation and follow-up actions. Collectively, these enhanced technical requirements ensure that CIF-supporting ICT services are not only secure by design, but also contractually enforceable in operation, underpinned by auditable evidence, validated resilience testing, and effective supervisory assurance mechanisms.

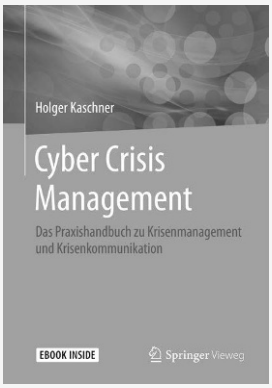
3 Conclusion

DORA establishes a comprehensive, risk-based framework for managing ICT third-party risk in the financial sector, placing primary responsibility on financial entities while extending clear obligations to ICT service providers. By requiring financial institutions to identify, assess and classify ICT services, distinguish between normal ICT services and those supporting CIF, and apply proportionate legal and technical safeguards, DORA ensures that regulatory requirements are closely aligned with operational risk. Effective compliance with DORA therefore depends not only on formal contractual alignment, but also on the practical implementation of governance structures, security controls, resilience testing, and exit strategies. In this respect, DORA represents a shift from a purely contractual approach to a holistic resilience regime, in which ICT third-party risk management becomes a core component of financial stability and supervisory oversight.

36 Arts. 30 Abs. 3 lit. a-b, lit. e-f; Art. 28 Abs. 8 DORA.
37 Art. 28 Abs. 5 DORA.
38 Art. 30 Abs. 3 DORA.
39 Arts. 30 Abs. 3 lit. d. in conjunction with Arts. 26 and 27 DORA.

Springer Vieweg

System- und Datensicherheit



H. Kaschner
Cyber Crisis Management
Das Praxishandbuch zu Krisenmanagement und Krisenkommunikation
2020, XII, 223 S. 10 Abb. Book + eBook. Brosch.
€ (D) 34,99 | € (A) 35,97 | *CHF 39.00
ISBN 978-3-658-27913-4
€ 26,99 | *CHF 31.00
ISBN 978-3-658-27914-1 (eBook)

- Das Praxishandbuch in deutscher Sprache zu Krisenmanagement und Krisenkommunikation
- Hilft auch zur Vorbereitung auf und Prävention von Cyber-Krisen
- Mit zahlreichen Abbildungen und Checklisten

Ihre Vorteile in unserem Online Shop:
Über 280.000 Titel aus allen Fachgebieten | eBooks sind auf allen Endgeräten nutzbar | Kostenloser Versand für Printbücher weltweit.

€ (D): gebundener Ladenpreis in Deutschland, € (A): in Österreich. * : unverbindliche Preisempfehlung. Alle Preise inkl. MwSt.

Part of SPRINGER NATURE

springer.com/informatik

A88197