DORA Regulation Demystifying the Legal Acts

Guidelines on subcontracting ICT services supporting critical or important functions

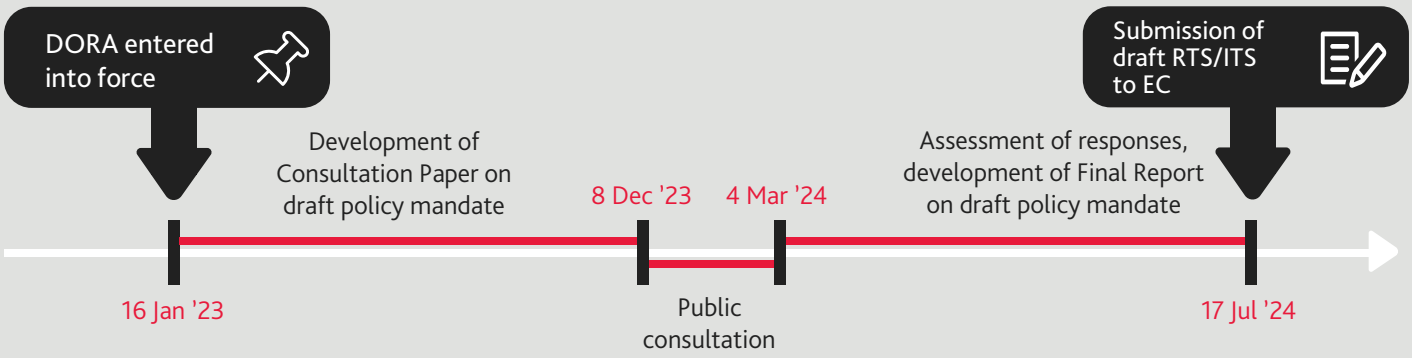
In a significant step aimed at strengthening digital resilience within the European Union's financial sector, the European Supervisory Authorities (ESAs), comprising the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA), in December 2023 have opened a public consultation on the second batch of mandates under the Digital Operational Resilience Act (DORA).

Policy Focus: Building a Robust Digital Framework

This comprehensive package encompasses four draft regulatory technical standards (RTS), one set of draft implementing technical standards (ITS) and two sets of guidelines (GL). These policy instruments aim to ensure a consistent and harmonised legal framework in the areas of major ICT-related incident reporting, digital operational resilience testing, ICT third-party risk management and oversight over critical ICT third-party providers. By addressing these critical aspects, the ESAs aim to fortify the digital infrastructure of financial entities and ensure a resilient and secure operational environment Scope and Timelines

Timeline

The consultation period is set to run until March 4, 2024, providing stakeholders and industry participants with a window to contribute their insights and feedback. This inclusive approach reflects the ESAs' commitment to gathering diverse perspectives and ensuring that the resulting regulatory framework is well-informed and effective.



We are pleased to share BDO's deep dive into the contents of the the Regulatory Technical Standards (RTS) on subcontracting ICT services supporting critical or important functions.

Aim of the RTS

The RTS aim to specify the elements that a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions to ICT third-party service providers. The RTS also set out the requirements and conditions for the use of subcontracted ICT services, such as risk assessment, contractual arrangements, monitoring and termination rights.

Scope and timeline

The RTS apply to all financial entities that are subject to Digital Operational Resilience for the financial sector (DORA), Regulation (EU) 2022/2554, which covers credit institutions, investment firms, insurance and reinsurance undertakings, payment service providers, electronic money institutions, central securities depositories, central counterparties, trade repositories, and credit rating agencies. The RTS also apply to ICT third-party service providers that provide ICT services supporting critical or important functions to financial entities. The public consultation on the draft RTS runs until 4 March 2024, and the ESAs aim to submit the final RTS to the European Commission for adoption in July 2024.

Summary of the RTS

The draft RTS consists of eight articles that cover the following aspects:

- **Article 1** specifies the elements of increased or reduced risk that should be considered by financial entities when applying the RTS, such as the location, number and nature of ICT subcontractors, the data processing and storage, the transferability and continuity of the ICT service, and the concentration risks.
- **Article 2** sets out the requirements for the group application of the RTS, where the parent undertaking is responsible for ensuring the consistent and effective implementation of the subcontracting conditions in its subsidiaries.
- **Article 3** requires financial entities to decide whether an ICT service supporting critical or important functions may be subcontracted only after having assessed various aspects, such as the due diligence processes, the involvement and information rights of the financial entity, the replication of contractual clauses, the abilities and resources of the ICT third-party service provider and the subcontractor, the impact of a possible failure of a subcontractor, the geographical and concentration risks, and the audit, information and access rights of the competent authorities and the financial entity.
- **Article 4** requires financial entities to identify in the written contractual arrangements which ICT services support critical or important functions and which of those are eligible for subcontracting and under which conditions. The article also specifies the minimum content of the contractual arrangements, such as the monitoring and reporting obligations, the location and ownership of data, the incident response and business continuity plans, the ICT security standards, and the termination rights of the financial entity.
- **Article 5** requires financial entities to fully monitor the ICT subcontracting chain and document it, including on the basis of the information provided by the ICT third-party service provider, and to monitor the subcontracting conditions and key performance indicators.
- **Article 6** requires financial entities to ensure that they are informed of any material changes to the subcontracting arrangements with a sufficient advance notice period, to assess the impact on the risks they are exposed to, and to approve or object to the changes before their implementation. The article also gives the financial entity the right to request modifications to the proposed subcontracting changes if they exceed its risk appetite.
- **Article 7** gives the financial entity the right to terminate the agreement with the ICT third-party service provider in case of non-compliance with the subcontracting conditions, such as implementing material changes despite the objection of the financial entity, or subcontracting an ICT service that is not permitted to be subcontracted.
- **Article 8** specifies the entry into force of the RTS, which is 20 days after their publication in the Official Journal of the European Union.

The current public consultation on the second batch of mandates, including Regulatory Technical Standards (RTS) on subcontracting ICT services, underscores the commitment to a robust and secure digital framework. As financial entities navigate the consultation period until March 4, 2024, it is imperative for them to actively participate, offering insights and feedback to shape the regulatory landscape. Organizations subject to DORA must diligently assess the draft RTS's detailed requirements, such as risk assessments, contractual arrangements, and monitoring obligations. Taking proactive steps, financial entities should prioritize internal assessments and due diligence processes to align with the forthcoming regulations. Additionally, fostering collaboration with ICT third-party service providers is crucial for compliance. With the ESAs aiming to submit the final RTS to the European Commission in July 2024, stakeholders should use this opportunity to strengthen their digital operational resilience, ensuring a seamless transition into the new regulatory landscape.

How BDO can help?

Assess the extent to which the DORA regulation applies to your organisation

Perform a DORA gap analysis and assess your current level of compliance considering available RTS and ITS Policy Products

Define a prioritised security roadmap that includes DORA specific requirements for your organisation, but which also keeps an eye on compliance with other applicable legislation and regulations.

Assist with project management and/or hands-on execution of the security roadmap, e.g. putting in place key policies and procedures, performing resilience testing, managing the penetration testing and implementation of subsequent recommendations, performing third-party/ vendor risk assessments, ...

For more information on DORA, please contact one of our local subject matter experts:

BDO Austria

Mario Neubauer
mario.neubauer@bdo.at

BDO Belgium

Christophe Daems
christophe.daems@bdo.be

BDO Croatia

Roko Vodopija
roko.vodopija@bdo.hr

BDO Czechia

Tomas Kubicek
tomas.kubicek@bdo.cz

BDO Denmark

Mikkel Jon Larssen
mla@bdo.dk

BDO Finland

Markys Aurala
markus.aurala@bdo.fi

BDO Malta

Ivan Spiteri
ivan.spiteri@bdo.com.mt

BDO Mauritius

Krishna Radhakeesoon
krishna.radhakeesoon@bdo.mu

BDO NL

Maurice Koetsier
maurice.koetsier@bdo.nl

BDO Germany

Aykut Bussian
aykut.bussian@bdo.de

BDO Slovakia

Tibor Vincze
vincze@bdoslovakia.com

BDO Slovenia

Andrej Baričič
andrej.baricic@bdo.si

BDO USA

James MacDonnell
jmacdonnell@bdo.com

BDO UK

Rachel Fallon
rachel.fallon@bdo.co.uk

▶ Follow us

▶ www.bdo.com.mt