A&L Goodbody

Financial Regulation Advisory

DORA - Technical standards on subcontracting

On 26 July 2024, the European Supervisory Authorities published final draft regulatory technical standards on the subcontracting of information, communication and technology services that support critical or important functions within financial entities.

23 Aug 2024

On 26 July 2024, the European Supervisory Authorities (**ESAs**) published final draft regulatory technical standards (**RTS**) on the subcontracting of information, communication and technology services that support critical or important functions (or material parts thereof) within financial entities (**Critical ICT Services**). The draft RTS are the final draft policy product to be published by the ESAs, as mandated under the Digital Operational Resilience Act (**DORA**).

The final draft RTS will be submitted to the European Commission for adoption, followed by publication in the Official Journal. The RTS will apply from the application date of DORA, 17 January 2025.

General observations

The final draft RTS on subcontracting introduce a significant number of additional requirements regarding the elements that must be incorporated into a contractual agreement between a financial entity and an ICT third-party service provider (**ICT TPP**) for the provision of Critical ICT Services.

The ESAs state that the final draft RTS have been developed taking into account existing requirements in the European Banking Authority's Guidelines on outsourcing arrangement and Guidelines on ICT and security risk management. While the Guidelines on outsourcing arrangements include a number of provisions on sub-outsourcing (at paragraphs 76 to 80), the requirements in the final draft RTS are a lot more detailed.

As is already made clear under DORA, Recital 3 of the final draft RTS emphasises that the use of subcontractors providing Critical ICT Services (**ICT Subcontractors**) by ICT TPPs "*cannot reduce the responsibilities*" of financial entities and their management bodies to manage their risks and to comply with the requirements in DORA, the RTS and other relevant legislative and regulatory requirements. Therefore, where the provision of Critical ICT Services to a financial entity depends on a long or complex chain of multiple ICT Subcontractors, it is essential that the financial entity identifies the overall chain of ICT Subcontractors.

Prior to the publication of the draft RTS, the Central Bank of Ireland provided some colour on the impact of proportionality on chain outsourcing in a speech on 1 July 2024 that stated:

"*So what then does this mean in this context? Well it means that firms that outsource remain responsible for all the activities that are outsourced. This means that they need to have ongoing knowledge about the overall functioning of the chain or "tree" of subcontracting arrangements and this means that there should be appropriate monitoring of the overall functioning of that "tree". It does not mean that each link in the chain needs to be monitored. And for example one way of fulfilling the responsibility may be to make sure that primary or material subcontractors themselves have in place an approach to subcontracting and due diligence that is robust and appropriate.*

Where more detailed monitoring should be required is in respect of those subcontractors that are material to the critical or important functions of the firm. And again this is fully embedded in the proportionality principle and the idea that expectations for oversight should be aligned with responsibility for the firm's activities whether or not they have been outsourced."

Recital 11 states that the requirements applicable to the use of intra-group subcontracting are the same as those applicable to non-intra-group subcontracting, regardless of the differences that may exist in the risks posed in both cases.

Obligations of financial entities under the final draft RTS

Risk profile and complexity of contractual arrangements

In relation to the overall the application of the RTS, a financial entity will need to consider its size and the overall risk profile and the nature, scale and elements of increased or reduced complexity of its services, activities and operations. This will include, for example, consideration of the type of Critical ICT Services covered by the contractual arrangements, the length of the chain of ICT Subcontractors, the location of each ICT Subcontractor and the impact on the transferability of the Critical ICT Service to another ICT TPP (amongst others).

Application of the requirements across a group

Where financial entities within the same group separately subcontract Critical ICT Services, the parent undertaking of the group will need to ensure that the conditions for subcontracting Critical ICT Services are applied by the financial entities in a consistent and effective manner at all levels.

Risk assessment and due diligence

When proposing to subcontract Critical ICT Services, a financial entity will need to conduct a risk assessment before entering into a contractual arrangement with an ICT TPP so that it has a clear and holistic view of the risks associated with the subcontracting and will be in a position to properly monitor and mitigate those risks. The RTS contain a detailed list of factors which, at a minimum, must be assessed by a financial entity.

In terms of ongoing compliance requirements, financial entities will also need to conduct the risk assessment periodically against possible changes in their business environment, including but not limited to changes in the supported business functions, ICT threats, ICT concentration risks and geopolitical risks.

Description and conditions under which Critical ICT Services may be subcontracted

When describing the Critical ICT Services to be provided, the written contractual agreement between the financial entity and the ICT TPP will need to identify which Critical ICT Services are eligible for subcontracting and under which conditions. In this regard, for each ICT Service to be provided, the RTS prescribe a detailed list of elements that must be reflected in the written contractual agreement (in addition to the elements specified in Article 30 of DORA, which must also be reflected in the contractual agreement). The RTS provide that the contractual agreement must specify, for example, that the ICT TPP is responsible for the provision of the services provided by the ICT Subcontractors and is required to monitor all subcontracted Critical ICT Services to ensure that its contractual obligations with the financial entity are continuously met and that the ICT TPP shall assess all risks associated with the location of the ICT Subcontractors and the location where the Critical ICT Services are provided from.

Any changes to existing contractual agreements between the financial entity and ICT TPP that are necessary to comply with DORA must be implemented in a timely manner and as soon as possible. The financial entity will be required to document the planned timeline for implementation.

Conditions for subcontracting relating to the chain of ICT Subcontractors

When permitting subcontracting of Critical ICT Services, the written contractual agreement must also provide that:

- the chain of ICT Subcontractors will be identified in accordance with Article 3(1)(b) of the RTS
- the identification of the chain of ICT Subcontractors remains up to date over time to allow for the financial entity to discharge its obligation to maintain and update the register of information.

To maintain the financial entity's overall responsibility for Critical ICT Services that are subcontracted, the written contractual agreement must enable the financial entity to effectively monitor the Critical ICT Services and take appropriate corrective actions without undue delay. In particular, the contractual agreement must include elements enabling the financial entity to fulfil its obligation to monitor the ICT risk that may arise in relation to its use of Critical ICT Services provided by ICT Subcontractors.

The contractual arrangements must also include:

- provisions to enable the financial entity to assess whether and how the potentially long or complex chain of ICT Subcontractors may impact its ability to fully monitor the contracted functions and the ability of the competent authority to effectively supervise the financial entity
- provisions to enable the financial entity to obtain information from the ICT TPP on contractual documentation between the ICT TPP and the ICT Subcontractors and relevant performance indicators, considering the provisions of Article 30(3)(e) of DORA (i.e. the right to monitor ICT TPP performance on an ongoing basis) and of Article 8(2) of Commission Delegated Regulation (EU) 2024/1773 (audit and access rights)

Material changes to subcontracting arrangements for Critical ICT Services

In the case of a proposed material change to the subcontracting arrangements for a Critical ICT Service, the written contractual agreement must require that the financial entity is informed of the proposed changes within a notice period sufficient to assess the impact of the risks the financial entity is or might

be exposed to, as well as whether the changes might affect the ability of the ICT TPP to meet its obligations under the contractual agreement.

The written contractual agreement must also require that the ICT TPP implements the material change only after the financial entity has either approved or not objected to the change by the end of the notice period.

If the risk assessment referred to above finds that the planned subcontracting or changes to subcontracting by the ICT TPP exceed the financial entity's risk tolerance, the financial entity must, before the end of the notice period, inform the ICT TPP of its risk assessment results and object to the changes and request modifications to the proposed subcontracting changes before their implementation.

Termination of the contractual arrangement

Article 28(7) of DORA sets out the circumstances in respect of which a financial entity must have the right to terminate a contractual arrangement for the provision of ICT services generally. Article 7 of the RTS specifies additional circumstances under which a financial entity has a right to terminate a contractual arrangement for the provision of Critical ICT Services for example, where an ICT TPP implements material changes to subcontracting arrangements despite objections or requests for modifications from the financial entity or subcontracts a Critical ICT Service without approval.

Next steps

The aim of the RTS is to ensure that financial entities can effectively manage and oversee the risks associated with ICT subcontracting, particularly when such services are critical or important to their functions. The comprehensive nature of the RTS underscores the importance of structuring and documenting contractual arrangements in a robust and thorough manner, covering the entire lifecycle of ICT service provision. It is therefore essential for financial entities to integrate the RTS into their operational frameworks promptly and effectively, including through adjustments to their contractual agreements and risk management practices. Although DORA implementation projects are already underway, financial entities will now need to review the requirements in the final draft RTS and assess if their existing contractual agreements and standard contract templates will require uplifts.

It is also important to acknowledge that compliance with DORA will require on-going monitoring and enhancements when necessary. The Central Bank of Ireland has stated that the regulation of digital operational resilience is "*not a once-and-done exercise*" and it is "*optimal to adopt a multi-year, multifaceted perspective*". Therefore, financial entities must also be prepared to adapt to regulatory and environmental changes, ensuring that their contractual arrangements are compliant and equipped to manage and respond to the associated risks effectively, particularly against a backdrop of increasing reliance on ICT services and the evolving cyber threat landscape.

For further information on DORA and its impact on your firm, please contact Patrick Brandt, Partner, Ciara Brady, Senior Associate, Louise Hogan, Senior Associate, Sarah Lee, Senior Knowledge Lawyer or any member of ALG's Financial Regulation Advisory team, or alternatively, visit ALG's DORA Hub.

Date published: 23 August 2024