Final DORA level 2 regulation published

18 July 2024

The three European Supervisory Authorities (EBA, EIOPA and ESMA) published the second batch of level 2 rules under the Digital Operational Resilience Act ("DORA") on 17 July 2024.

Overview

This marks an important step in the legislative process for the detailed rules that supplement DORA, and gives clarity to businesses who are underway with implementing the changes required under DORA. Given that in-scope financial entities are required to comply with DORA from 17 January 2025, there is significant pressure to put changes in place by that deadline, and the lack of clarity while awaiting the final text of the level 2 rules has presented a challenge for both financial entities and IT suppliers.

Some of the level 2 rules (those that take the form of guidelines) are now treated as final. Those that take the form of regulatory technical standards ("RTS") and implementing technical standards ("ITS") still need to go through a further review process. They will need to be adopted by the European Commission and, in the case of RTSs, the European Parliament and the Council of the European Union will have an opportunity to scrutinise the draft and raise objections. Provided no objections are raised, the RTSs will enter into force. However significant changes at this stage are unlikely.

Businesses preparing for DORA will be disappointed that the final draft level 2 rules on subcontracting have not been published as expected, but will follow "in due course". Given the DORA subcontracting rules are among the most challenging in practice for financial entities and IT suppliers alike, it is hoped that when they are published, the amended level 2 rules will provide some clarity and address the practical obstacles of monitoring the entire subcontracting chain involved in delivering the types of IT systems that support the financial ecosystem.

Below we outline the significance of the new level 2 rules being finalised and what businesses impacted by DORA should do next.

Background

The DORA framework

The Digital Operational Resilience Act ("**DORA**") is an EU regulation designed to ensure that financial entities can withstand and recover from technology issues such as cyber events and technical failures.

DORA imposes extensive obligations on financial entities in relation to their ICT governance, risk management, security practices and vendor arrangements. DORA also imposes obligations directly on "critical" ICT third-party service providers – those which are systemically important because of the role they play in supporting the financial ecosystem. An overview on DORA is available in our Engage article here.

The main text of DORA is supplemented by important technical detail in a body of secondary legislation, known as the "level 2" rules. The level 2 rules published on 17 July 2024 were drafted by the three European Supervisory Authorities ("**ESAs**"): the European Banking Authority ("**EBA**"), the European Insurance and Occupational Pensions Authority ("**EIOPA**") and the European Securities and Markets Authority ("**ESMA**"). Of those level 2 rules, the RTS and ITS still need to go through a further review process as set out in the Overview section above. Significant changes at this stage are, however, unlikely.

The level 2 rules

The ESAs have divided the level 2 legislation that they are responsible for developing into two batches (see below for this division). The ESAs finalised most of the first batch in January 2024, following a consultation and feedback process involving a wide range of stakeholders. As of today, the second batch has also now been finalised, with the exception of the rules applicable to subcontracting arrangements (which are due to follow "in due course").

The level 2 rules consist of the following:

Batch 1

- RTS specifying criteria regarding ICT risk management
- RTS specifying the criteria for classification of ICT-related incidents
- Regulations specifying criteria (policy) for the critical ICT third-party service providers in the financial sector
- Draft Implementing Technical Standards to establish the templates for the register of information

Batch 2

- RTS on subcontracting ICT services supporting critical or important functions
- RTS and ITS on major incident reporting
- RTS specifying elements related to threat led penetration tests ("TLPT")
- Two RTS on the harmonisation of conditions enabling the conduct of the oversight activities:
    1. one focusing on the areas of the mandate having a direct impact on financial entities and ICT third party service providers; and

2. one focusing on the requirements to be followed by the competent authorities in relation to the joint examination team (as this only directly impacts the regulators themselves).

- Joint guidelines on the oversight, cooperation and information exchange between the ESAs and the competent authorities
- Joint guidelines on estimation of aggregated annual costs and losses caused by major ICT-related incidents

Notable changes in final drafts

Overall, the final texts do not substantially change the landscape for businesses who have been making preparations for DORA. However, there have been modifications in response to stakeholders' feedback which will impact the interpretation and/or scope of certain rules, such as:

- Changes to the **RTS specifying elements related to threat-led penetration tests** (**TLPT**) which will be welcome by many, such as:
    - amended criteria for selecting insurance and reinsurance undertakings required to perform TLPT by default, providing more predictability for market stakeholders;
    - increased thresholds for determining whether payment and e-money institutions are required to perform TLPT;
    - the introduction of a defined "joint TLPT" for financial entity groups that use shared ICT systems;
    - clarifications in relation to pooled testing; and
    - greater flexibility on the requirements of testers and threat intelligence providers, allowing engagement of testers who do not fulfil all the criteria provided risks have been appropriately mitigated.

Despite the above changes, the TLPT rules as amended will still impose a high burden on those institutions that are subject to TLPT and their service providers, given that they involve testing on live production environments. Many will be hoping that the discretion afforded to authorities in assessing whether or not TLPT is justified for a given financial entity (even if they meet the relevant TLPT criteria) will result in relatively few financial entities (or groups of financial entities) being subject to TLPT requirements.

- Changes to the **RTS on major incident reporting** which will also be welcome by many, including:
    - time limits for reporting incidents – the 24 hour/72 hour window for reporting will begin from the submission of the previous notification/report, instead of the moment of classification of the incident (as per the last draft);
    - removal of the obligation for smaller financial entities to submit the initial notification in relation to incidents;

- simplification of the reporting template, including reducing the number of reporting fields from 84 to 59. For example, in the final incident report, financial entities will now not be required to provide information about an inability to comply with regulations or contractual breaches of SLAs, and a detailed breakdown of the costs and losses from the incident will no longer be expected (however gross details will still be required); and

- introduction of aggregated incident reporting where a single incident has impacted multiple financial entities.

- Changes to the Joint guidelines on estimation of aggregated annual costs and losses caused by major ICT-related incidents, aimed at reducing the reporting burden on financial entities who are required under DORA to estimate the aggregate annual costs and losses of major ICT-related incidents.

What about the subcontracting rules?

Publication of the draft RTS on subcontracting ICT services ("**Subcontracting RTS**") has been delayed with a statement from the ESAs that it will be published "in due course".

This leaves industry participants waiting for clarity on two of the most challenging issues raised by the current draft RTS on subcontracting:

- **How far down the subcontracting chain do financial entities need to go to comply with their monitoring obligations?** The current draft RTS requires the financial entity to monitor "subcontracting conditions … along the entire ICT subcontracting chain". Concerns have been raised as to the practical feasibility of monitoring the entire subcontracting chain, particularly given the expectation that this includes the review of contractual documentation entered into with those subcontractors.
- **Do the restrictions in the Subcontracting RTS apply to all subcontracting arrangements that support critical or important functions, irrespective of how material the subcontracted services are to those functions?** It is notable that the draft ITS to establish the templates for the register of information (the "Register ITS") only expects financial entities to document information about subcontractors where they "effectively underpin" ICT services supporting critical or important functions or material part thereof. However, the same qualification is not made in the Subcontracting RTS and it would be helpful to have this clarified. As noted above, monitoring of the entire supply chain will be difficult in practice if there is no materiality qualification.

Given the significant work involved in reviewing and amending IT service agreements in order to address DORA requirements, providing clarity on the above issues will be important for both financial entities and IT suppliers to help them assess which and how many subcontracting arrangements need to be reviewed. The time pressure to commence and conclude supplier contract amendments increases week on week.

Why is this important, and what should affected businesses do next?

Financial entities are required to comply with DORA from 17 January 2025 – a deadline which is likely to prove challenging for many financial entities given the volume of work required to meet DORA's extensive

requirements. Some have been hesitant to implement changes within their organisations before knowing precisely what to expect in the final level 2 rules, while others have prioritised early preparations in the hope that they will not need to re-do their work upon the final level 2 rules becoming available.

It is worth noting that changes could still be made to the level 2 rules before they become binding, but significant deviations from the final drafts are unlikely at this stage.

Financial entities can and should now ramp up their efforts to implement changes necessary to comply with DORA by the 17 January 2025 deadline. Similarly, IT suppliers will need to make the changes necessary, including the remediation of contracts, to ensure that financial entities can continue to use their services in a manner that meets regulatory expectations when DORA comes into effect.

Authored by Louise Crawford, Alex Nicol, and Magdalena Medarova.