DORA Regulation Demystifying the Legal Acts

RTS on criteria for the classification of ICT-related incidents

In June 2023, the first wave of Draft RTS (Regulatory Technical Standards) and ITS (Implementing Technical Standard) was published by the European Supervisory Authorities. The objective of these additional Policy Products is to provide detailed specifications and guidelines on how certain provisions in the basic legislative Act should be implemented across the EU.

These Policy Products aim to:

- Harmonise the application of the rules and regulations in the financial sector
- Cover areas such as reporting requirements, risk management, disclosure obligations, and other operational aspects of financial services
- Enhance transparency, consumer protection, and the stability of the financial system

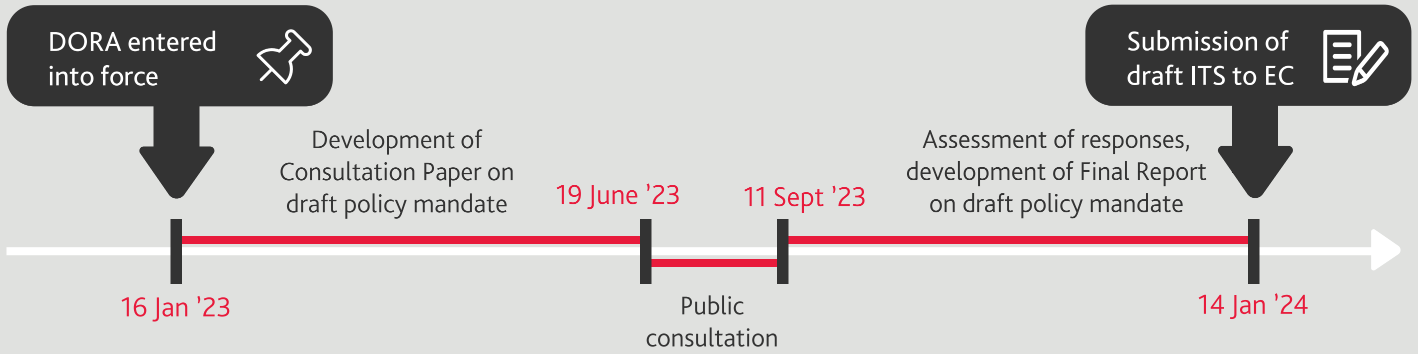
Scope and Timelines

The first batch of Policy Products have been published for consultation in Draft form and consist of:

- RTS to specify the policy on ICT services performed by ICT third-party providers (Article 28(10))
- RTS on criteria for the classification of ICT-related incidents (Article 18(3))
- ITS to establish the templates for the register of information (Art.28(9))
- RTS on ICT risk management framework (Article 15) and RTS on simplified ICT risk management framework (Article 16(3))

We are pleased to share BDO's deep dive into the contents of the RTS on Criteria for the Classification of ICT-related Incidents.

The current timeline foresees a final draft of this RTS to be published by 16 January 2024.



DORA entered into force

Submission of draft ITS to EC

Development of Consultation Paper on draft policy mandate

19 June '23

11 Sept '23

Assessment of responses, development of Final Report on draft policy mandate

16 Jan '23

Public consultation

14 Jan '24

RTS on criteria for the classification of ICT-related incidents

In today's interconnected digital landscape, the financial sector plays a pivotal role in ensuring operational resilience and cybersecurity. To address the evolving challenges posed by ICT-related incidents, the European Union has introduced Regulation (EU) 2022/2554 on digital operational resilience for the financial sector. This RTS aims to harmonize and streamline incident reporting requirements across diverse financial entities, fostering a resilient and secure digital environment.

Key Goals

This RTS emphasizes several critical objectives:

- **Harmonization and Streamlining:** DORA seeks to establish uniform standards for the classification, management, and reporting of ICT related incidents. The scope of DORA encompasses a wide array of financial entities, from traditional banks to emerging fintech companies.
- **Proportionality:** Recognizing the diverse nature and risk profiles of financial entities, DORA emphasizes proportionality. It tailors the criteria and materiality thresholds to ensure that they are equitable for entities of varying sizes and risk profiles while minimizing reporting burdens for smaller financial institutions.
- **Continuity and Alignment:** The RTS builds upon existing incident reporting frameworks, ensuring a seamless transition for financial entities that were already subject to reporting requirements. It leverages provisions from established guidelines such as the EBA Guidelines on major incident reporting under PSD2, promoting alignment and consistency.
- **Consistency with Operational Risk Frameworks**: Given the interconnectedness of DORA and existing frameworks, there is a concerted effort to maintain consistency, particularly concerning the assessment of economic impact. This alignment aims to prevent conflicting requirements and facilitate a comprehensive approach to operational risk.

Classification Criteria and Materiality Thresholds

One of the fundamental aspects of the RTS is the establishment of clear and comprehensive classification criteria and materiality thresholds. These criteria are essential for determining the severity of incidents and guiding appropriate responses. To strike a balance between accuracy and practicality, the criteria are designed to be interdependent, reflecting the nature, scale, and complexity of services offered by financial entities.

Major Incidents and Cyber Threats

The RTS introduces a qualitative and quantitative approach to identifying major incidents, emphasizing the significance of an incident's impact. Major incidents are determined based on a combination of primary and secondary criteria, encompassing factors like the number of affected clients, data losses, and reputational impact.

Primary data

Clients / financial counterparts

- Relative thresholds: 10% of total # of clients, counterparts using the affected service.
- Absolute threshold: 50 000 clients affected

Transactions affected

- Relative threshold: 10% of the volume of transactions
- Absolute threshold: EUR 15 000 000 value of transactions

Data losses

- Binary threshold (yes/no answer): any loss of critical data related to availability, authenticity, integrity or confidentiality

Critical Services affected

- Binary threshold (yes/no answer):
- Impact on any critical service and whether the incident has escalated to the senior management or management body

Secondary data

Reputational impact

- Binary threshold (yes/no answer):
- - e.g. based on the attraction of media attention, the complaints received from various clients or financial counterparts, incompliance with regulatory requirements

or

- - loss of clients or financial counterparts

Duration and service downtime

- Quantitative threshold: downtime of critical functions longer than 2 hours
- Duration: Quantitative threshold: 24 calendar hours.

Geographical spread

- Dependent binary threshold (yes/no answer). indicating whether the incident has had a material impact in two or more Member States

Economic Impact

- Single absolute threshold: EUR 100 000 or above for the gross direct and indirect costs and losses incurred by the incident

Additionally, the RTS addresses significant cyber threats, acknowledging their potential to disrupt critical functions. Financial entities are encouraged to report these threats voluntarily, enabling a proactive approach to cybersecurity.

Reporting Framework

Financial entities subject to DORA's provisions are required to adhere to a three-tiered reporting framework, including an initial notification, interim reports, and final reports. This structured approach ensures timely and comprehensive reporting, facilitating efficient incident response.

Recurring Incidents

Recognizing that recurring incidents can signal underlying deficiencies, the RTS addresses the aggregation of minor incidents over a defined period. If these incidents share a common root cause, nature, and impact, they are collectively considered major, promoting a holistic view of risk management.

Relevance to Competent Authorities

The RTS also emphasizes the importance of information exchange among competent authorities in different EU Member States. The regulation outlines criteria for assessing the relevance of major incidents to authorities in other jurisdictions, promoting cross-border cooperation and safeguarding the financial sector's stability.

In summary, the RTS provides a standard framework for classifying ICT-related incidents under DORA. By setting materiality thresholds for major incidents and establishing a clear protocol for reporting significant cyber threats, it enables financial entities to effectively manage and respond to incidents in a consistent manner. This framework is designed to meet the unique needs and risk profiles of various financial entities while fostering a collective commitment to operational resilience and cybersecurity within the sector. As financial institutions navigate the evolving digital landscape, these standards stand as a vital tool for ensuring the integrity and stability of the financial sector's digital operations.

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 Belgium
Christophe Daems
Christophe.daems@bdo.be

BDO Czechia
Martin Horicky
martin.horicky@bdo.cz

BDO Denmark
Mikkel Jon Larssen
mla@bdo.dk

BDO Malta
Ivan Spiteri
ivan.spiteri@bdo.com.mt

BDO UK
Harry Wallace
harry.wallace@bdo.co.uk

BDO NL
Ronald Westerveen
Ronald.Westerveen@bdo.nl

BDO Czechia
Tomas Kubicek
tomas.kubicek@bdo.cz

BDO Germany
Aykut Bussian
aykut.bussian@bdo.de

BDO USA
James MacDonnell
jmacdonnell@bdo.com

BDO UK
Rachel Fallon
rachel.fallon@bdo.co.uk

▶ Follow us

▶ www.bdo.com.mt

'BDO', 'we', 'us', and 'our' refer to one or more of BDO International Limited, its network of independent member firms ('the BDO network'), and their related entities. The BDO network is an international network of independent public accounting, tax and advisory firms which are members of BDO International Limited and perform professional services under the name and style of BDO (hereafter: 'BDO member firms'). BDO International Limited is a UK company limited by guarantee. It is the governing entity of the BDO network.

BDO