DORA Regulation Demystifying the Legal Acts

RTS & ITS Reporting & Templates major incidents and significant cyber threats

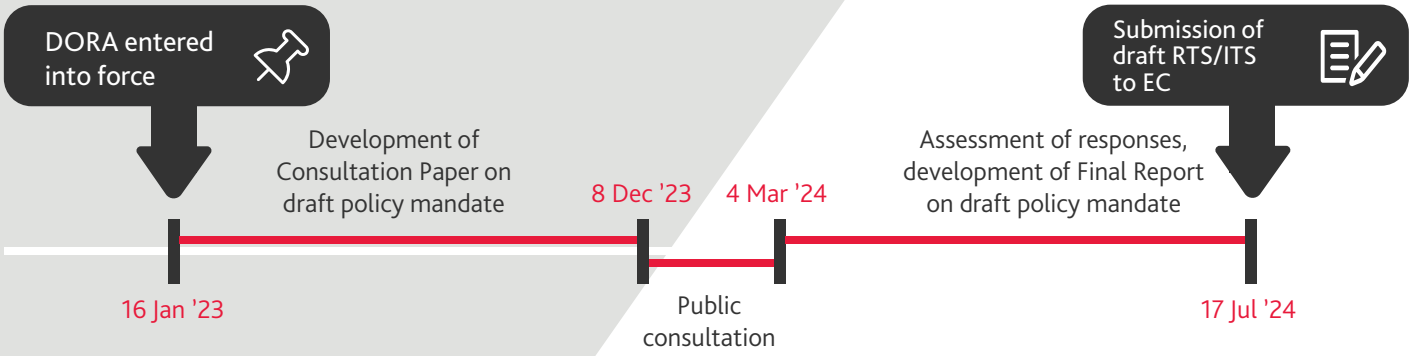
In a significant step aimed at strengthening digital resilience within the European Union's financial sector, the European Supervisory Authorities (ESAs), comprising the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and 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 the consultation paper that includes two set of standards:

A. Regulatory technical standards (RTS) on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents; and

B. Draft Implementing Technical Standards (ITS) On the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat.

These RTS and ITS are closely linked to the draft RTS on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under the DORA Regulation, which was publicly consulted on by 11 September 2023. (Check out the DORA Incident classification)

Scope and timeline

This RTS and ITS 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 and ITS 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.

Aim of the RTS

The RTS aim to establish the content of the notification and reports for major incidents and significant cyber threats, and determine the time limits for reporting major incidents.

Summary of RTS

The RTS seeks to harmonise incident reporting across the EU, ensuring timely and efficient communication of major incidents. The time limits and content requirements are aligned with NIS2, ensuring consistency across regulations. The draft RTS covers the following aspects:

- **Consistency in Reporting:** The RTS establishes a uniform framework ensuring consistent reporting of mandatory incidents across all financial entities, thereby aiding regulators in comprehensively understanding the scale and impact of these incidents across the sector. Additionally, it distinguishes between these obligatory reports and the optional reporting of significant cyber threats. While financial entities are required to uniformly report major ICT-related incidents, they have the discretion to report significant cyber threats, which, although optional, plays a crucial role in proactive cyber threat management and enhances the sector's overall digital resilience.

- **Timeliness of Response:** The RTS sets clear deadlines for reporting incidents, which is critical for timely responses and mitigations. The stipulation of an initial report within four hours from classification of the incident as major, but no later than 24 hours from the time of detection of the incident after the FE has classified the incident as major, underscores the urgency and seriousness with which such incidents must be treated. Financial Entities are also required submit an intermediate report within 72 hours and a final report within 30 days from the classification of the incident as major, or sooner when regular activities have been recovered and business is back to normal.

- **Comprehensive Coverage:** The detailed content requirements in the RTS ensure that reports are comprehensive, covering aspects such as the nature, impact, and remedial actions taken. This comprehensive data is vital for regulatory authorities to assess the incident's severity and potential systemic risk.

- **Balancing Operational Capacity**: While emphasizing rapid reporting, the RTS also considers the operational capacity of financial entities, especially smaller ones. This balance is critical to ensure that the reporting requirements are robust yet feasible for all entities.

Aim of the ITS

The ITS aims to provide standard forms, templates, and procedures for financial entities to report major ICT-related incidents and notify significant cyber threats.

Summary of ITS

The ITS complements the RTS by providing the actual tools - in the form of templates and procedures - to facilitate the reporting of major ICT-related incidents and cyber threats. Its significance lies in the following aspects:

- **Facilitation of Reporting:** By providing standardized forms and templates, the ITS makes the reporting process more straightforward for financial entities. This facilitation is particularly beneficial for smaller entities that might lack the resources to develop such reporting mechanisms independently.

- **Ensuring Detail and Clarity:** The standardized forms ensure that all necessary details are captured in a report. This clarity is essential for effective analysis and response by regulatory authorities.

- **Enhancing Data Quality and Analysis:** Standardized reporting not only aids in immediate incident response but also contributes to the long-term analysis of trends and vulnerabilities within the financial sector. High-quality data from these reports can inform future cybersecurity policies and resilience strategies.

Aspect	Major Incident	Significant Cyber Threat
Nature of Reporting	Mandatory	Optional
Types of Reports Required	Initial, Intermediate, Final	Single notification, which should be submitted as soon as possible after the detection of the threat.
Reporting Timelines	▸ **Initial notification:** 4 hours from the moment of classification of the incident as major, but no later than 24 hours from the time of detection of the incident. ▸ **Intermediate report:** within 72 hours from the classification of the incident as major or sooner; ▸ **Final report:** 30 days from the classification of the incident as major, or sooner	▸ **Initial notification:** 4 hours from the moment of classification of the incident as signifcant, but no later than 24 hours from the time of detection of the incident. ▸ **Intermediate report:** within 72 hours from the classification of the incident as significant or sooner; ▸ **Final report:** 30 days from the classification of the incident as significant, or sooner
Reporting Format	Single template that covers the initial notification, intermediate report and final report, with data fields indicating which fields are expected to be submitted with the respective report.	Template that covers only the essential data fields, most of which are conditional depending on the nature of the threat.
Key Data Fields to be Reported	37 types of data, covering general information about the reporting entity, the impact of the incident, the classification criteria met, the handling of the incident, the root cause of the incident and the measures taken to prevent similar incidents in the future.	9 types of data, covering general information about the reporting entity, the description of the threat, the potential impact, the classification criteria that would have triggered a major incident report, the status of the threat, the actions taken to prevent materialisation, the notification to other stakeholders and the indicators of compromise.

The RTS on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and ITS on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat under DORA represent significant steps towards a unified and efficient framework for managing digital operational resilience in the EU financial sector. By standardizing reporting procedures and timelines for major ICT-related incidents and cyber threats, these standards aim to enhance the sector's ability to respond to and recover from such events, thereby protecting the financial markets and their participants.

With the ESAs aiming to submit the final RTS and ITS 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, et.

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