DORA: The clock is ticking!

The Digital Operational Resilience Act (DORA), entered into force on the 16th of January 2023 and will be applicable from the 17th of January 2025. Its main purpose is to enhance and strengthen the cybersecurity practices of entities across the EU financial sector and to harmonise key requirements and reporting obligations. DORA aims to increase the resilience of financial institutions against cybersecurity threats, major incidents and operational disruptions.

The legislation introduces an overarching framework for the management of cybersecurity risk stemming both internally and from Third-party Providers (TPP). The implementation of DORA will depend on a series of Regulatory Technical Standards (RTS), which will progressively be published over the next two years. These are detailed documents that provide specific instructions for financial institutions to comply with the new regulation. The first of these were published earlier this year and EU financial institutions should not waste time in understanding their implications.

What are the 3 key points to consider at this stage?

DORA has already been approved yet it won't fully apply until early 2025. Moreover, many of the nitty-gritty details are still to be worked out and published by the regulatory bodies (e.g., the EBA). This delayed implementation, combined with the "to be clarified" status, might put even the most regulatory conscious firms into a state of "wait and see".

We strongly recommend that financial institutions do not fall into this category.

Here are the 3 main topics that we recommend management teams should discuss today.

1. **What function within your organisation should sponsor DORA implementation?**

The implementation of DORA requirements will likely introduce major changes. As with any regulatory implementation, the primary question should be, "Who shall be the sponsor/leader for this?". Based on what we see in the market, since this is a regulatory change, the regulatory arm (i.e., Risk or Compliance) generally picks up the tab and leads implementation. We believe that Information & Communication Technology (ICT) functions should also play a major role.

If we look at the key topics covered by DORA, it might not be obvious who should take the overall lead as all departments have a significant role to play in the implementation.

- **ICT Risk Management** – will require the development of risk management frameworks, definition of governance and roles and responsibilities, implementation of the approaches to identify, assess, response and recover from the ICT risks as well as the development of the Business Continuity and Operational Resiliency plans. *Risk could be a good candidate to address this point.*
- **ICT Incident Management** – will require a much more "technology centric" approach with the classification, centralisation, notification and reporting of the incidents. *IT should easily tackle these points*.
- **Digital Operational Resilience Testing** – focuses on cyber resilience testing and TIBER EU / TIBER IT simulation (i.e., Threat-led Penetration Test). *ICT will play the key role here.*

- **ICT Third-Party Risk Management** – requires the management of the third-party associated risks, harmonisation of contractual clauses and requirements and creation of the oversight framework for the service providers. *Risk and/or Compliance usually oversee such activities.*

As shown above, DORA implementation will require expertise from several departments and teams. In order to get more clarity, institutions should consider their business model.

We consider these points as a major differentiator on who should lead implementation. A Retail Bank with a strong risk culture should probably appoint their Risk function as the Project Lead. However, an E-Bank with a strong technological mindset, would be better positioned to smoothly implement the requirements by empowering their ICT function with this responsibility.

Despite the above, institutions should be careful to rely too much on only one aspect of the regulation. For example, an institution with a strong Risk function might focus primarily on the risk aspects of the regulation during the implementation and minimise the ICT points and vice versa.

Regardless of the approach, we believe that institutions should raise such questions and discuss associated risks and benefits before implementing DORA.

2. How can your organisation estimate the impact/cost of DORA?

Now is a crucial time for institutions to begin making the first steps to align their governance and ICT practices to the principles laid out in DORA. Institutions should try to identify high-level gaps, plan associated actions, develop initial roadmaps and most importantly try to assess the financial impacts these changes will bring. They can do this through an initial gap assessment.

The most basic type of such gap assessment for DORA can take the following form:

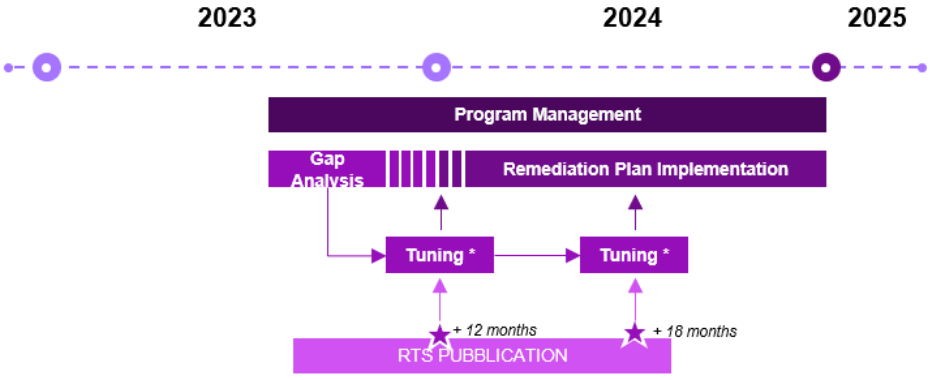
DORA Principles	Article(s)	Current State	Target State	Main Difference	Action Plan	Priority
…	…	…	…	…	…	…

This gap analysis should be performed via document review, interviews, workshops and walkthroughs. Upon completion, the institutions should be able to clearly state:

1. What is our current level of compliance?
2. What areas should we further improve?
3. How significant are the gaps?
4. What is the path to full compliance?

By answering these questions, institutions will be better prepared to integrate any further changes that might come with forthcoming RTS and be able to be more precise in their budget planning for the years leading up to DORA implementation.

The global timeline below can help to visualise the potential planning.



** Tuning of the remediation plan based on details specified in RTS*

3. After an initial gap assessment, what should be my next move?

ICT Third-party Management!

As stated earlier, further RTS will be published. Regardless of the uncertainties on the subjects covered by the RTS, it can be normal to adapt a reactive strategy. However, our view is that entities that fall under the scope of DORA should be more proactive - especially, when it comes to the topic of Third-party Risk Management.

DORA dedicates a full chapter to ICT Third-party Risk Management and we believe this should be the topic that institutions should get a head start on. In particular, institutions should maintain, at entity, sub-consolidated and consolidated levels, a register of information on all contractual arrangements of ICT services provided by ICT Third-party Providers (TPPs). The requirement to maintain a register will oblige entities to gather a certain amount of information about their contracts with the ICT TPPs and about the ICT TPPs themselves. As entities may rely on a large number of the ICT third parties, the gathering, processing and digitisation of this information will be a challenge and will require significant time to complete.

Moreover, it is always advisable to ensure that compliance reviews are done periodically in regard to any existing guidelines from the local National Competent Authorities (NCAs) since they are guided by the EU-level regulations. In Luxembourg, CSSF circular 22/806 should be used for this purpose. Institutions could use this circular to review:

- The scope of their outsourced activities
- The critical or important criteria for the activities, as required by DORA
- The existence of outsourcing policies and whether they meet the relevant requirements
- The outsourced activities which qualify as ICT and many more aspects addressed by DORA

Conclusion

At Avantage Reply we believe in an old adage “The best defence is a good offence”. Thus, when it comes to new and sometimes uncertain regulatory changes, we propose a proactive approach rather than a “wait and see” strategy. With DORA, institutions can already begin to ask questions such as, “Who should lead this? How much will it cost? How well are we prepared? What information do we lack?”. We know this because we have seen and heard these questions being raised at the highest levels with our clients. We hope that the points raised in this article can serve as a good starting point towards your path to DORA implementation.

Contact us today for a personalised consultation on your DORA compliance implementation strategy.

Avantage Reply (Luxembourg)

Gwenaël Gavray
Partner
g.gavray@reply.com

Avantage Reply (Paris)

Olivier Debliquy
Associate Partner
o.debliquy@reply.com

Avantage Reply (Brussels)

Nicolas Pavlovitch
Partner
n.pavlovitch@reply.com