



OneSumX Operational Resilience Package

The European Union's (EU) Digital Operational Resilience Act (DORA) introduces a comprehensive regulatory framework to bolster the operational resilience of financial services across the EU. By standardizing how financial entities manage Information and Communication Technology (ICT) risks, DORA aims to minimize disruptions to financial markets while enhancing sector-wide resilience.

At Wolters Kluwer, we are committed to supporting regulated entities in navigating the increased obligations imposed by DORA compliance, particularly Article 30, which requires financial entities to place specific demands on their ICT providers. While these provisions enhance operational strength, they also introduce new compliance complexities.

The OneSumX Operational Resilience Package has been designed to help financial entities address these challenges efficiently. By simplifying the compliance process and ensuring alignment with DORA's regulatory requirements, the package reflects our focus on delivering resilient, secure, and cost-effective ICT solutions.

Operational Resilience Package

1. *OneSumX DORA Addendum* (available now)

The OneSumX DORA addendum incorporates key Article 30 contractual provisions for an annual fixed fee. This approach provides cost stability while meeting essential compliance requirements. Below are examples of key provisions that offer cost predictability:

- **Threat-led Penetration Testing (TLPT):** Participation in ESA-mandated TLPT, proportional to Wolters Kluwer FRR's control.
- **Enhanced audit rights:** Extended information, access, and audit capabilities.
- **ICT incident management:** Assistance with ICT incidents based on our level of control over affected ICT assets.

Why choose OneSumX?

- ✓ **Streamlined bank regulatory compliance:** Simplifies adherence to DORA's stringent regulatory requirements, reducing complexity and ensuring adherence.
- ✓ **Operational transparency:** Provides comprehensive audit artifacts and contractual clarity for full accountability.
- ✓ **Cost predictability:** Annual fixed fees ensure stability and budget planning.
- ✓ **Proactive support:** Regular updates ensure alignment with evolving standards and industry best practices.



2. OneSumX DORA audit bundle (First delivery: April 15, 2025)

The OneSumX DORA audit bundle is a curated set of audit and assurance documents designed to uphold transparency, accountability, and operational resilience.

This bundle helps financial entities stay resilient by ensuring compliance with evolving industry standards and regulatory requirements while seamlessly adapting to future best practices.

Key deliverables include:

#	Type	Artifact description	Frequency
1	Assurance	Service-level SOC2 Type 2 Report (Regulatory Reporting)	Annual
2	Assurance	Penetration Test Report for Licensed Products	Annual
3	Assurance	Microsoft Azure SOC2 Type 2 & CSA STAR Attestation	Annual
4	Monitoring	Service Report (Customer Support Ticket Status)	Quarterly
5	Monitoring	SaaS availability reports	Monthly
6	Monitoring	Updated List of FRR Subcontractors	Annual

With the OneSumX Operational Resilience Package, your organization can confidently navigate DORA compliance, enhance operational resilience, and mitigate ICT risks effectively.



Frequently Asked Questions

What is the OneSumX Operational Resilience Package?

To help you meet the January 17, 2025 compliance deadline, we offer a standardized OneSumX Operational Resilience Addendum and a comprehensive information package. This ensures financial entities can address the time-sensitive contractual requirements of Article 30, saving time and reducing compliance pressures.

Is OneSumX an ICT Service under DORA?

Whether deployed on-premise or SaaS, OneSumX may qualify as an ICT service under DORA. Regulated financial entities are encouraged to perform their evaluations to determine if OneSumX qualifies as a critical or important function under DORA guidelines.

Why address compliance now instead of waiting for the next contract renewal?

Respondents to JC 2023 84 highlighted challenges with off-cycle contract updates and suggested a forward-looking approach. However, the ESAs reaffirmed that full DORA compliance is required by January 17, 2025. Acting now with the OneSumX Operational Resilience Package ensures you avoid disruption and achieve timely compliance, mitigating regulatory risks.

How does the Resilience Package enhance my operational resilience?

The package strengthens your operational resilience by providing the following:

- Standardized contractual with strengthened audit and termination clauses
- Support for Threat-Led Penetration Testing (TLPT)
- Enhanced audit rights and transparency

Wolters Kluwer FRR is committed to further investment in new processes and certifications tailored to DORA requirements.

Will the DORA Addendum override my current contractual terms?

No, the OneSumX DORA Addendum supplements your existing service levels and contractual terms, ensuring compliance with the mandatory DORA Article 30 provisions. The audit bundle complements the due diligence artifacts already provided under your existing agreements with Wolters Kluwer FRR.





By choosing the OneSumX Operational Resilience Package, you gain a proactive partner in navigating DORA compliance, bolstering resilience, and ensuring business continuity.

Learn more about the OneSumX for Finance, Risk and Regulatory Reporting solutions. [Click here.](#)

© 2025 Wolters Kluwer Financial Services, Inc.
All Rights Reserved.



OneSumX[®]
by Wolters Kluwer

What if I need additional services beyond the Resilience Package?

The addendum includes a rate card for services not explicitly covered, reflecting the specialized security and resilience expertise required to support regulated entities' obligations under DORA. These rates differ from standard Professional Services fees.

Does the package include DORA's Register of Information reporting templates?

The templates are offered as a separate product. For further details, please get in touch with your Wolters Kluwer FRR account manager.

Is Wolters Kluwer FRR obtaining a Legal Entity Identifier (LEI)?

We are securing LEI codes for relevant legal entities to meet the latest EU Journal requirements (published November 29, 2024). This ensures alignment with DORA's Register of Information provisions.

Who can I contact for further information?

For further assistance, contact your FRR account manager or email us at frr-compliance@wolterskluwer.com.