Ellex Klavins

With DORA enforcement approaching rapidly, it's time to act!

What is DORA?

DORA is an EU regulation, which establishes a **comprehensive EU-wide regulatory framework** aimed at strengthening the digital operational resilience of financial entities. It requires financial entities to implement robust measures for managing ICT risks, handling ICT-related incidents, conducting rigorous testing and managing ICT third-party risks.

Who must comply?

The DORA regulation provides a list of entities required to comply with its requirements, covering a **wide range of financial service providers** as well as ICT third-party service providers:

- credit institutions;
- payment institutions, including payment institutions exempted pursuant to PSD2
- account information service providers
- electronic money institutions, including electronic money institutions exempted pursuant to EMI Directive
- investment firms
- CASPs and issuers of asset-referenced tokens
- central securities depositories
- central counterparties
- trading venues
- trade repositories
- managers of alternative investment funds
- management companies
- data reporting service providers
- insurance and reinsurance undertakings
- insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries
- institutions for occupational retirement provision
- credit rating agencies
- administrators of critical benchmarks
- crowdfunding service providers
- securitisation repositories
- ICT third-party service providers

Despite the broad coverage, **certain exemptions apply** based on the size and overall risk profile of the financial entities.

When?

DORA applies from 17 January 2025

What actions are required?

DORA addresses ICT risk via targeted requirements applicable to financial entities in the following **four key areas:** ICT risk management; ICT-related incident management; Digital operational resilience testing; and ICT third party risk managing.

The steps financial entities must take to fulfil their respective obligations will vary as they must be **proportionate** to their size, overall risk profile, and to the nature, scale and complexity of their services, activities and operations.

1. ICT risk management

ICT risk is any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment.

DORA requires financial entities to establish a sound, comprehensive, and well-documented **ICT risk management framework** as a part of their overall risk management system, implementing necessary **strategies, policies, procedures, ICT protocols and tools** that are necessary to duly and adequately protect all information assets and ICT assets, including computer software, hardware, servers, as well as to protect all relevant physical components and infrastructures, such as premises, data center and sensitive designated areas.

DORA sets forth specific requirements with respect to such elements of the ICT risk management framework as: usage and maintenance of **updated ICT systems, protocols and tools; protection** of ICT systems; **identification** of ICT supported functions, roles, responsibilities, sources of ICT risk, information assets and ICT assets, and processes dependent on third-party service providers; **detection** of anomalous activities; ICT business **continuity; learning; communication.**

Implementation of the ICT risk management framework must be set out in the **digital operational resilience strategy.** ICT risk management framework must be **documented**, subject to regular **review, audit and improvement.**

2. ICT-related incident management

ICT-related incident is a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity.

DORA requires financial entities to establish an **ICT-related incident management process** to detect, manage and notify ICT-related incidents.

Financial entities must also **classify** ICT-related incidents and **determine impact** of such incidents based on criteria set forth in the DORA.

Major incidents must be **reported** to national competent authorities using standard templates and procedures.

Ellex Klavins

3. Digital operational resilience testing

DORA requires financial entities to establish, maintain and review **a sound and comprehensive digital operational resilience testing programme.**

Digital operational resilience testing programme must provide for the execution of **appropriate tests**, such as: vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing.

Testing must be performed by **independent internal or external parties.**

Some financial entities are obliged to perform **advanced testing** of ICT tools, systems and processes based on threat-led penetration test (TLPT).

4. ICT third-party risk managing

ICT third-party risk is an ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements.

According to DORA, financial entities which use ICT services provided by ICT third-party service providers must **manage ICT third-party risk.**

As part of their efforts to manage ICT third-party risk, financial entities must adopt and regularly review a **strategy for ICT third-party risk management,** which must include, among other things, a policy on the use of ICT services supporting **critical or important functions** provided by ICT third-party service providers.

Contracting with ICT third-party service providers is highly regulated by DORA. Before concluding a contract on the use of ICT services, financial entity must carry out an **assessment of contractual arrangements** in line with criteria set out in the DORA, including with respect to conflict of interest, concentration risk, supervisory conditions, as well as must perform a **due diligence on prospective ICT third-party service provider** to assess its suitability. Contracts with the ICT third-party service providers must contain certain **key contractual provisions** specified by DORA, including with respect to the SLA, monitoring and audit, exit strategies.

Financial institutions must also maintain and update a **Register of contractual arrangements** with the ICT third-party service providers, explicitly identifying contractual arrangements related to critical or important functions.
Any planned contractual arrangement on the use of ICT services supporting critical or important functions must be **notified to competent authorities**.

A review of existing contractual arrangements with ICT third-party service providers must be conducted to ensure compliance with DORA requirements.

Ellex Klavins

Are the requirements limited to DORA?

Definitely not.

At the EU level, DORA is accompanied by **13 policy instruments** prepared by the European Supervisory Authorities: 8 regulatory technical standards (RTS), 2 implementing technical standards (ITS) as well as several guidelines and technical advice documents. Please note that RTS and ITS, just like DORA itself, are **directly applicable and legally binding for the financial entities** without the need for transposition into national law.

The RTS and ITS accompanying DORA provide detailed requirements on key areas such as ICT risk management frameworks, incident reporting procedures, resilience testing, and oversight of critical third-party providers, ensuring harmonized implementation across the EU financial sector. These standards **specify practical measures** to operationalize DORA's objectives and ensure consistency in compliance.

Locally in Latvia some elements of DORA are furthermore elaborated in the draft **Law on Digital Operations Resilience of Financial markets.**

What about NIS2?

The NIS2 Directive is an EU cybersecurity framework that establishes cybersecurity risk-management and reporting obligations, applicable as of October 2022 to **essential and important entities across critical sectors.** In Latvia, NIS2 has been transposed into the National Cybersecurity Law.

A financial entity or ICT third-party service provider **may fall under the scope of both DORA and NIS2.** To avoid unnecessary overlap of obligations, the European Commission has clarified that DORA is a sector-specific regulation, meaning financial entities subject to DORA need only comply with the risk management and reporting requirements outlined in it. However, this **does not exempt financial entities from all obligations under NIS2 /National cybersecurity law.** For example, each financial entity must assess whether it qualifies as an essential or important entity under NIS2 /National cybersecurity law and, if so, must register with the National Cybersecurity Center of Latvia by 01.04.2025.

Ellex Klavins

Our approach

If you have yet to begin your journey toward DORA compliance, we recommend the following phased approach:

	Scope of work	Parties engaged
STEP 1 Assessment of compliance obligations	Assessment of: •Financial entity's obligation to comply with DORA and / or NIS2 •Scope of obligations (full scope vs simplified)	Ellex Kļaviņš
STEP 2 High level scope & gap analysis	•Mapping the financial entity's obligations under DORA •Conducting a high-level assessment of the entity's compliance with each set of obligations based on the mapping	Ellex Kļaviņš
STEP 3 Defining implementation strategy	Defining a strategy to address the non-compliances identified in Step 2, specifying: •Actions to be taken •Involved parties •Timeline •Expected outcomes/deliverables	Ellex Kļaviņš Financial entity IT consultants (internal or external)
STEP 4 Implementation	Implementation of the strategy defined in Step 3	Ellex Kļaviņš Financial entity IT consultants (internal or external)

If your internal IT manpower is insufficient to implement DORA requirements, we can recommend trusted service providers to establish a highly effective implementation team.

DORA compliance will be a key focus for financial supervisory authorities in 2025

Ellex Klavins

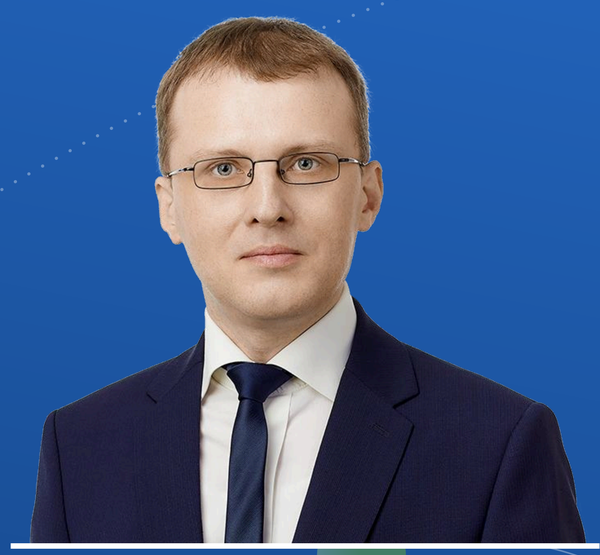
Our Team

To support your journey toward full DORA compliance, we will assemble a dedicated and highly experienced team.

Zane Veidemane Bērziņa
Associate Partner
Co-Head of the Banking & Finance practice group

Our team will be led by attorney at law **Ms. Zane Veidemane Bērziņa**, Co-head of Banking & Finance practice group at Ellex Klavins. Zane has extensive experience in financial regulatory matters gained throughout her two decades long career in a law firm as well as in-house in one of the leading credit institutions.

She advises banks and other financial service providers on a wide range of complex issues, with a particular focus on regulatory compliance, including market entry, licensing, internal controls, new product launches, supervisory matters, as well as acquisitions and restructuring within the financial sector.



Dr. sc. comp. Marats Golovkins
Associate

Zane will be supported by **Dr. sc. comp. Marats Golovkins**, a lawyer with a unique background in both law and IT. He works within the Industry & Regulatory practice group at Ellex Klavins, specializing in areas where the synergy of legal and IT expertise is essential.

Before obtaining his legal qualifications (Bachelor's and Master's degrees in law) and joining Ellex Klavins in 2018, Marats was, among other roles, a researcher at the Department of Computer Science at the Electronics Research Laboratory at the University of California, Berkeley, USA, in 2005. From 2004 to 2005, he was a researcher at the Computer Science Laboratory LIAFA at Paris Diderot University (Paris 7) in France, and from 2000 to 2004, he worked as a computer programmer and systems analyst at Exigen Latvia.

To begin your DORA compliance journey with Ellex Klavins, please contact Ms. Zane Veidemane Berzina

+371 26350188
or
zane.veidemane.berzina@ellex.legal

Ellex Klavins