Grant Thornton

Countdown to compliance: Five practical steps for becoming DORA ready

12 August 2024

From 17 January 2025, the Digital Operational Resilience Act (DORA) applies to all financial entities operating within the European Union.

This wide-reaching legislation aims to strengthen the digital operational resilience of the financial services sector. Built upon five pillars, it contains rigorous requirements for ICT-risk management, incident reporting, testing, third-party risk management and information sharing.

Implementing DORA's requirements can be overwhelming, and knowing where to begin can be difficult. Below are **five practical steps** that firms can take to become DORA ready.

Understand the principle of proportionality

Because of the diverse nature of the financial services sector, DORA employs the principle of proportionality. This challenging but critical aspect of compliance means that entities' regulatory requirements will differ depending on their size and risk profiles and the scale, nature and complexity of their businesses.

For example, large institutions providing multiple services, such as Ireland's three pillar banks, must establish a fully-fledged ICT risk management framework that addresses all appropriate areas from DORA's Level 1 and Level 2 texts. However, smaller entities, such as boutique trading firms, can avail of a simplified ICT-risk management framework covering only the areas relevant to their function, services and industry.

Testing requirements also differ depending on proportionality. All entities must set up a general testing programme and comply with digital testing requirements, but through industry engagement with the Central Bank of Ireland (CBI) in recent months, the indication is that only about 10-15 institutions in Ireland will initially fall within scope of the advanced threat-led penetration testing requirements laid out in Articles 26 and 27.

The application of proportionality seeks to create a high standard for the sector as a whole, while protecting smaller organisations from unnecessary regulatory encumbrances. Since DORA does not take a one-size-fits-all approach to compliance, institutions should begin their compliance journey with a scoping exercise to confirm a right-sized approach to meet regulatory requirements without taking on needless regulatory burdens.

Perform a holistic gap assessment

DORA's five pillars touch many components of business operations, so organisations should analyse their entire operating model to determine which groups and business functions the legislation affects.

They should bring together the stakeholders from each affected area to ensure that everyone understands their role in the compliance journey. Business as usual will continue throughout the implementation timeline, and having a collaborative approach to the planning stage helps stakeholders align on DORA-related priorities and responsibilities from the get-go.

When conducting the business-wide gap assessment, entities should also inspect existing processes to determine if they can be used for DORA compliance. All firms practice digital operational resilience to some extent, and with a comprehensive review, in many instances they'll discover that they can enhance some of their existing procedures to satisfy DORA requirements.

Leveraging and improving existing procedures saves time and allows entities to focus their effort and resourcing on the areas where they'll need to start from scratch to build practices that achieve compliance.

Be strategic about remediation activities

When building a remediation roadmap, entities should address the compliance areas that need the most work first. Drafting new frameworks, evaluating them against the legislation and scrutinising their effectiveness will take time. Areas with significant compliance gaps must be addressed thoroughly, and an imminent implementation deadline can create unnecessary pressure on employees.

Whenever possible, businesses should align their remediation plans with existing transformation roadmaps. To remain competitive, many organisations are already executing transformation roadmaps—digital, operational, environmental, etc. These businesses should ground DORA changes within their existing plans.

For instance, if a current transformation roadmap has a timeframe for updating contracts with third-party suppliers, the business should incorporate the additional contractual changes required by DORA as part of that review cycle.

Document decision-making

While the CBI expects firms to be compliant as possible by 17 January 2025, it has also recognised that "the regulation of digital operational resilience is not a once-and-done exercise and that is optimal to adopt a multi-year, multifaceted perspective". When implementing largescale change programmes, certain business realities such as the lengthy process for updating third-party contacts, may prevent organisations from implementing all required changes within the timeframe in place.

The CBI will take such issues into account when evaluating compliance, but it has firm expectations that all entities must have established and begun work on an agreed implementation roadmap by the January deadline.

Firms should therefore be prepared to give an account of their DORA decision-making process. For instance, they should be able to explain the level of proportionality that they applied to their programme of work, show documentation of their framework development and remediation plan and provide evidence of just cause for any implementation delivery extending beyond the deadline along with a timeline for completion.

Ensuring oversight and alignment through risk and compliance functions (second line) and objective review and challenge from internal audit (third line) will show the application of a holistic delivery model to meet DORA requirements.

Plan to test digital operational resilience regularly

DORA requires that firms test digital operational resilience regularly (with the principle of proportionality determining the frequency of the review cycle), so DORA frameworks need to stay top of mind within organisations even after implementation projects stand down next year.

By increasing entity-wide awareness about maintaining digital operational resilience, businesses can help all employees understand that DORA frameworks shouldn't exist in silos: they need to evolve alongside business practices. Any large-scale change—restructuring, operational changes, systems updates, etc.—should prompt an evaluation of the existing framework.

For instance, if a firm decides to overhaul its technology systems in 2026, then the DORA framework—despite only being a year old—may need updating to ensure continued compliance and meet the evolving business model of today.

How Grant Thornton can help with DORA compliance

At the outset, implementing DORA requirements can be daunting. The depth and breadth of requirements across areas such as incident reporting and third-party risk management require action, and knowing where to begin can be tricky.

We support institutions of all sizes in their ongoing journey to DORA compliance. Our first-hand experience, bolstered by our involvement with our EU network of firms, brings strength to our service offerings, and our clients attest that by clarifying the scope and key dependencies, we have helped them avoid potential pitfalls and ensured compliance to the standard required.

We can provide differing combinations of services to create a best-fit model for DORA implementation that meets your organisation's specific needs and ensures compliance by the January 2025 deadline.