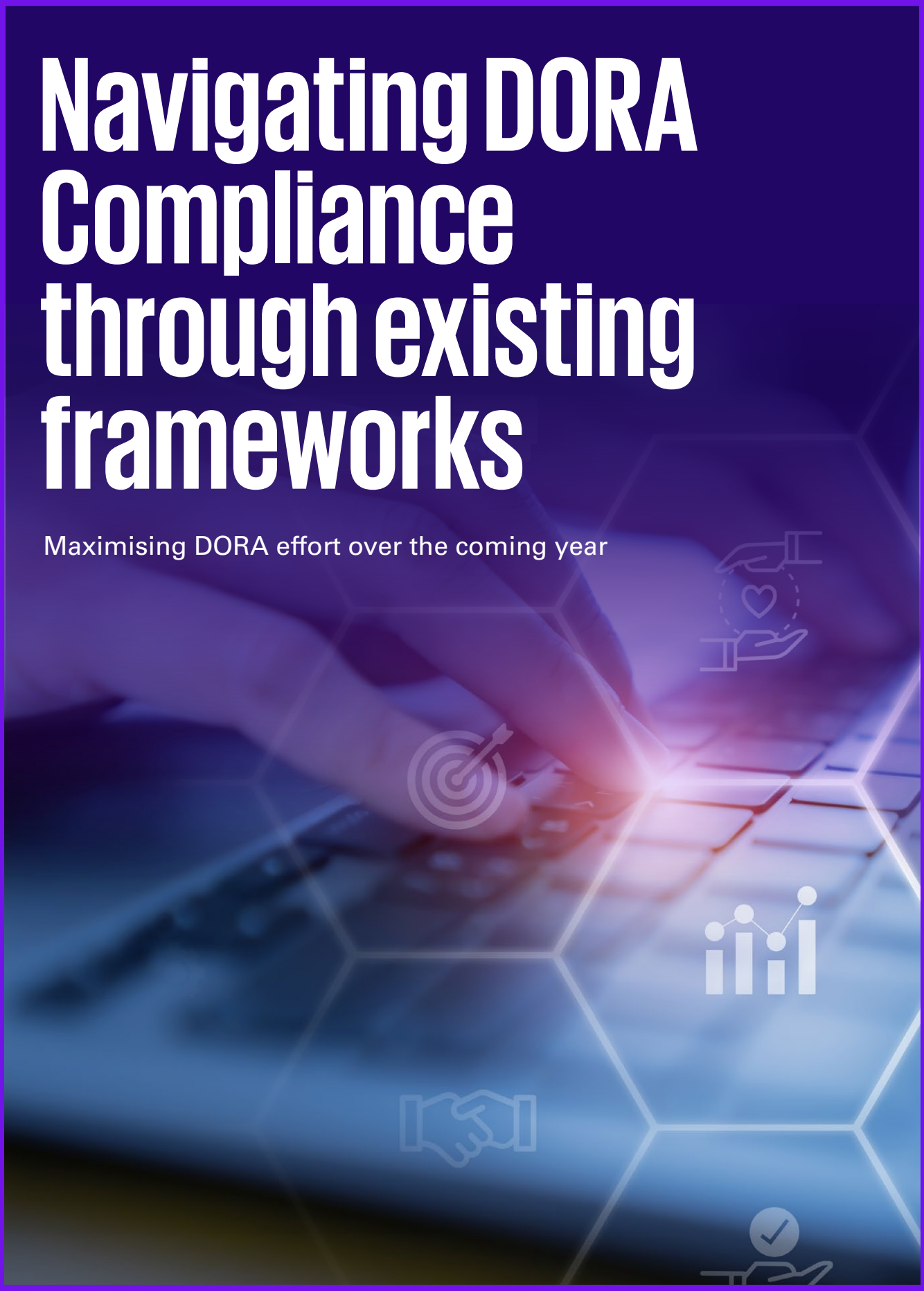
KPMG

Navigating DORA Compliance through existing frameworks

Maximising DORA effort over the coming year



The Digital Operational Resilience Act (DORA) was published in the Official Journal of the EU in December 2022. As such, this time last year, firms were getting to grips with unpacking DORA including how DORA would apply to their business, what organisational and technical changes would be required as a result, and the level of investment needed to ensure compliance.

Over the last 12 months, many firms moved into assessing their current activities across the DORA focus areas to understand where their gaps may exist. Some firms have since moved into the remediation of these areas through implementation of uplifts or net-new items as required under DORA. These areas include governance, processes and technology change.

Through our support of the assessment and implementation journey, we have seen firms discover that while there are some new, specific areas which are called out under DORA, there are possibilities to leverage existing frameworks and processes that many regulated entities already have in place. Specifically considering the existing Outsourcing, Operational Resilience and IT & Cybersecurity Risk guidance previously released by the Central Bank and European Supervisory Authorities.

In that same time, the European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs), who primarily ensure that companies are financially resilient and able to continue operating during serious disruptions, hit their published timelines for the four regulatory technical standards (RTS) and one implementing technical standard (ITS) which further clarify expectations.

The first set of final draft RTSs under DORA were published on the 17th of January 2024, dealing with the following areas:

- ICT Risk Management Framework and Simplified ICT Risk Management Framework
- Criteria for the classification of ICT -related incidents
- Policy on ICT services supporting critical or important functions provided by ICT third-party service providers (TPPs)
- Establishing templates for the Register of Information in relation to contractual arrangements with ICT third party service providers

The second tranche of standards, which are currently going through public consultation and due for finalisation on the 17th of June 2024, will provide further guidelines on the following areas:

Guidelines on estimation of aggregated costs and losses caused by major ICT-related incidents

Threat-led penetration testing

Harmonisation of oversight conditions

Reporting of major ICT-related incidents

Determination and assessment when sub-contracting ICT services supporting a critical or important functions

Feasibility report on further centralisation of incident reporting through the establishment of a single EU hub for major ICT-related incident reporting

Call for advice on the criticality criteria and fees

Guidelines on estimation of aggregated costs and losses caused by major ICT-related incidents

Guidelines on oversight cooperation and information exchange between the ESAs and competent authorities

As organisations are implementing DORA requirements, we're sharing some key insights from our work in this area to date.

What is DORA?

DORA will aim to harmonise existing legislation and supplement existing gaps with the introduction of new regulations to establish a unified digital framework whereby firms ensure they can adapt and endure all types of ICT-related disruptions and threats, in order to prevent and mitigate cyber threats.

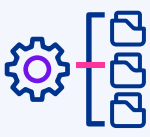
DORA sets out several objectives to increase the collective digital resilience of the financial sector and beyond including ICT vulnerability management, ICT risk management and ICT third party risk, exchange of ICT threat intelligence and streamlining the approach to regulatory reporting.

DORA focuses in particular on the following areas:

ICT risk management

ICT related incident reporting

Digital operational resilience testing



ICT Third Party risk management

Information and intelligence sharing

Timeline for Implementation

DORA requirements will apply in full from the 17th of January 2025, which is now less than a year away. The focus of firms should now be shifting from completing DORA assessments and gap analyses, towards a risk-based approach for implementation which puts embedding DORA by design and compliance monitoring at its core.

DORA continues the themes and expectations as defined through accountablilty frameworks, which may result in rights to access, fines and remedial measures.

Questions to consider today:

01. Do you have a clear set of steps to support the implementation of your DORA programme by January 2025?

02. Have you identified areas where you need upliftment and sized the associated resource requirements?

03. Do you have dedicated DORA resources, team with defined responsibilities and a governance forum that will be ready to transition to BAU over the next year?

04. Do you have the necessary inhouse skills, capabilities and expertise to implement and oversee the various aspects of the remediation programme?

05. Are your key stakeholders aware of the DORA requirements applicable to their area of the business?

06. Do you have a defined methodology and monitoring approach to ensure future compliance by January 2025 and beyond?

Key remediation areas:

Below are the key focus areas companies should consider when assessing their DORA compliance:

1

ICT Risk Management

- Governance and organisation
  - Entity scoping
  - Management accountability
- Risk functions, roles & responsibilities
  - ICT risk management framework
  - Defined control function
- Dedicated Digital Operational Resilience Strategy
- ICT systems, protocols & tools
- ICT asset identification, classification and inventory maintenance
- ICT business continuity policy, response and recovery plans and testing
- Business impact analysis
- Crisis management function

2

ICT Third Party Risk Management

- Third party ICT risk management strategy
- Register of information of all ICT third party service provider contractual arrangements
- Concentration risk assessments
- Contract review
- Third party supplier register
- Third party audit schedule
- Exit strategies

3

Digital Operational Resilience Testing

- Digital operational resilience testing strategy
- Digital operational resilience testing programme
- Testing of controls on ICT tools & systems
- Vulnerability assessments
- Threat-Led Penetration Testing (TLPT)
- Disclosure requirements

4

ICT Related Incidents

- Incident classification and threats
- Incident detection, management & monitoring
- Review of response & recovery plans
- Incident management training
- Periodic scenario testing
- Internal ICT incident escalation procedures
- Reporting of major ICT incidents

5

Information Sharing

- Information sharing arrangements
- Notifications to relevant authorities of participation in information sharing arrangements

6

Oversight of Critical Third Party providers

- Third party criticality assessments

Lessons learned from DORA implementation

Our teams have been working with Large Financial Services firms over the past year on DORA implementation programmes, which have resulted in implementation observations and lessons learned from our clients:

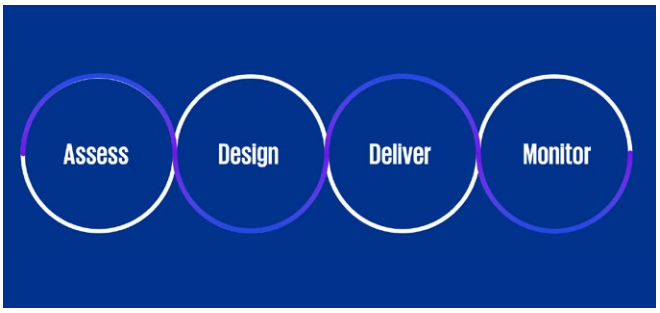
- **Alignment with existing resilience programmes** – Globally active firms need to embed DORA compliance within their broader strategic resilience capabilities. There is a real opportunity here to align digital resilience with these existing programmes and operating models.
- **Technology impacts** – DORA may drive technology uplifts and remediation, consider technology roadmap and operationalisation of controls.
- **Standardised Nomenclature** – Review and where appropriate adopt DORA definitions allowing a level of standardisation of taxonomy across resilience, risk & recovery domains.
- **Testing Obligations** – Review opportunities to build convergence by design into testing approaches, as such, harness synergies in existing testing approaches instead of starting from scratch.
- **Compliance transition** – Agree a compliance position and consider transition from DORA ready to DORA compliant as implementation progresses.

How KPMG can help:

DORA requirements will apply in full to both financial entities and ICT Service Providers by the 17th of January 2025. These will include any potential further clarifications from the ESAs as a result of the finalisation of the second tranche of the regulation.

Our team of technology risk and cyber experts have extensive knowledge across the Digital Operational Resilience obligation areas, paired with deep Governance, Risk and Compliance expertise. We have delivered DORA support programmes to leaders in the financial sector and aided numerous clients on their wider Operational Resilience journeys over the years.

The KPMG view on the DORA compliance journey takes us through 4 key stages:



Assess:

While some requirements will only involve minor improvements to existing processes and structures, there will be other areas which will require specific expertise, planning, time and collaboration across different organisational functions. To understand the implementation effort required to achieve DORA compliance, the first stage that all clients need to go through, is the assessment of their current frameworks to be able to size, prioritise and plan for remediation and reviewing these in the context of their short-, medium- and long-term resilience objectives.

Design:

During DORA design, it is crucial to establish a fit-for-purpose DORA programme that shifts the focus to how DORA is going to be implemented for your business. This may include the design of control frameworks across key remediation areas, the design of a Target Operating Model (TOM) to support DORA through the transition to the business-as-usual environment, establishing a DORA compliance function to continuously review the DORA compliance status, and determining the right technology to support the implementation of DORA.

Deliver:

Based on the prioritisation of delivery elements defined during the design phase, it's time for executing the remediation.During delivery, we support our clients to implement and remediate the controls in line with the agreed prioritisation and we support the deployment of technology which allows clients optimise DORA processes and controls, achieve scale and consistency, and enhance the ability to manage risk and compliance.

Monitor:

Lastly, KPMG have continuous DORA assurance offerings, to carry your organisation from January 2025 and beyond as you continue to monitor and ensure ongoing compliance with DORA requirements.

KPMG offers a resource-on-demand model which can be tailored to suit your organisational needs as you continue along your DORA compliance journey, and specifically, we can help you with the following:

Allow KPMG to assist with:

- ✓ Gap analysis to assess DORA compliance
- ✓ DORA Programme Support via programme design, governance, and assurance
- ✓ Target Operating Model (TOM) design
- ✓ Technical remediation support across ICT risk management, infrastructure, business continuity, IAM, digital testing, incident management and third-party risk
- ✓ People and change management via trainings, skills plans, communication packs, etc.
- ✓ Technology enablement
- ✓ Compliance Programme to ensure future alignment

Whether you require additional resources or expert knowledge, the skills across our Consulting practice can be drawn upon to aid with the various aspects of your DORA programme.

If you would like to discuss the potential impact of DORA on your business, please contact our Digital Operational Resilience experts below.

Contacts

Dani Michaux
EMA Cyber Lead
KPMG Ireland
e: dani.michaux@kpmg.ie

Jackie Hennessy
Partner, Technology Risk Consulting
KPMG Ireland
e: jackie.hennessy@kpmg.ie

Diarmuid Curtin
Director, Risk Consulting
KPMG Ireland
e: diarmuid.curtin@kpmg.ie

Carmen Cronje
Director, Risk Consulting
KPMG Ireland
e: carmen.cronje@kpmg.ie

kpmg.ie

Produced by: KPMG's Creative Services. Publication Date: January 2024. (10030)