KPMG

DORA: ICT THIRD-PARTY SERVICE PROVIDERS

September 2025

A.

ICT Service Providers & the Relevance of DORA

1. Global Implications and Relevance of DORA

Digital operational resilience has become a key focus for regulators around the world as they seek to ensure that financial institutions and other critical sectors are able to withstand and recover from disruptions, particularly those stemming from cyber threats and technological failures. For the first time, the European Supervisory Authorities (ESAs) are extending their regulatory reach beyond the financial sector under DORA, directly overseeing third-party ICT service providers deemed as critical to the financial sector. This shift reflects the EU's recognition of the interconnectedness between financial stability and digital infrastructure, and the need for a pan-European oversight mechanism to manage systemic ICT risks.

Recent Global IT Service Provider Outages

CrowdStrike – 2024

Critical services and business operations were disrupted affecting millions.

Reliance Jio – 2023

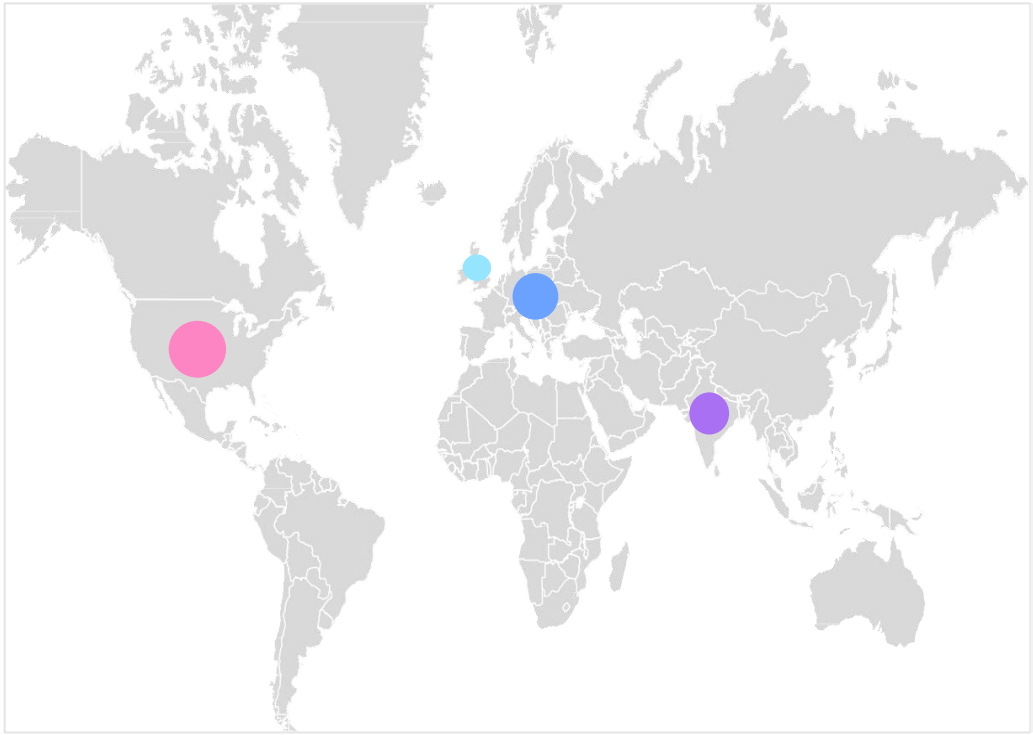
Reliance Jio encountered service disruptions due to technical issues, affecting mobile network services.

British Telecom – 2022

UK's largest telecommunications, faced technical glitches in its network affecting individuals and businesses.

SAP - 2022

SAP encountered technical issues with its software-as-a-service offerings, causing disruptions for European businesses.



Global Parallels to DORA

United Kingdom - Institutions are expected to evaluate the resilience and continuity of their third-party providers and incorporate these risks into their operational resilience strategies.

Singapore - The Monetary Authority of Singapore (MAS) issued guidelines on third-party service provider management, emphasising due diligence, contractual safety measures, and ongoing monitoring.

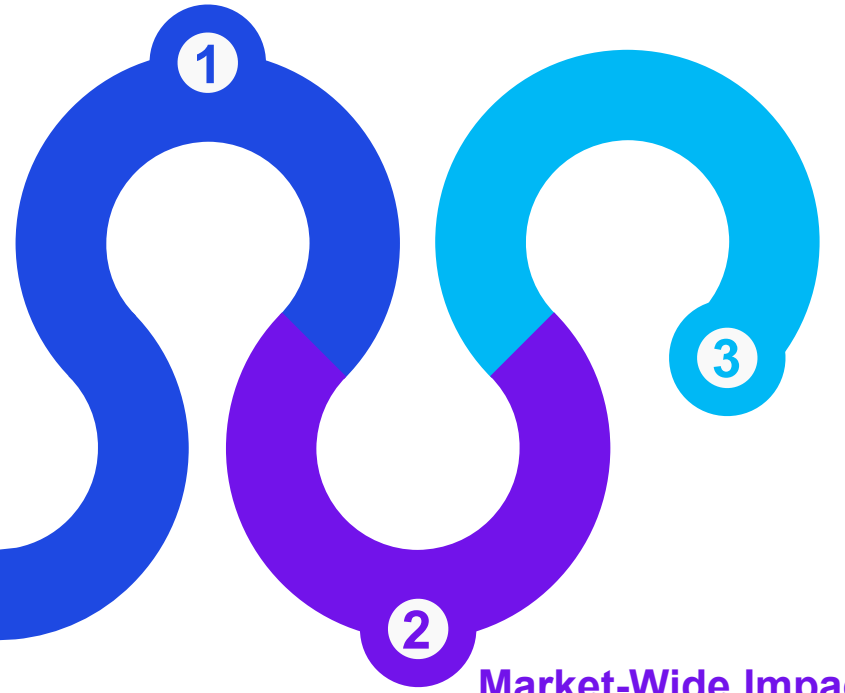
United States of America - Regulators consider systemic risks associated with widespread reliance on certain third-party providers, especially in cloud services.

2. ICT Service Providers – Resilience as the Operating Standard

While the number of ICT third party providers deemed as critical and directly in-scope ESA oversight will be concentrated, it will have ripple effects on the wider ICT service provider market. As resilience becomes the baseline operating standard clients expect, rather than a regulatory requirement for a select few. Early adoption and alignment may be crucial to surviving this market shift.

Critical Designation by ESAs

A limited number of ICT services providers shall be designated as critical and be subject to direct ESA oversight and supervision.



Strengthened EU Ecosystem

A more resilient, secure and harmonised financial and digital ecosystem across the EU.

Market-Wide Impact

Designation creates new benchmark for operational standards, prompting **all** providers to align to heightened expectations to remain competitive.

Competitive Advantage

DORA raises the operating standard for ICT service providers in the EU via direct oversight. Demonstrating alignment regardless of designation presents a significant opportunity in the market to differentiate from competitors.

Enhanced Trust & Market Credibility

ESA supervision signals a high standard of operational resilience and cybersecurity, boosting trust among financial institutions and regulators.

Market Maturity

All ICT service providers are incentivised to adopt best practises as high-levels of resilience becomes the baseline expectation.

Contractual Obligations

Ensures operational capabilities to meet DORA uplifted customer contractual requirements and customer assurance.

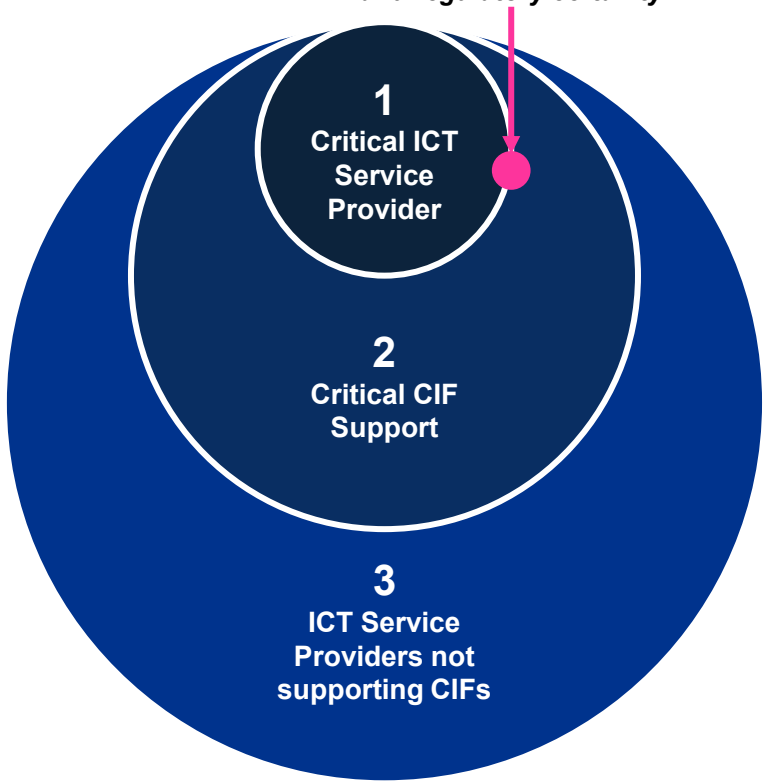
Regulatory Alignment & Scalability

Early alignment positions providers to adapt easily to future regulatory developments across the EU. Market harmonisation supports scalable service delivery and reduces compliance complexity for multi-jurisdiction providers.

3. ICT Service Provider Landscape

ICT service providers can strategically position themselves to meet evolving resilience expectations, regardless of inclusion within the finalised designation list expected to be published by the ESAs in late 2025.

ICT service providers may opt for voluntary critical designation. Demonstrating high resilience standards and providing competitive advantage and regulatory certainty



1. Critical ICT Service Providers

- Formally designated by the ESAs and those who have opted for voluntary designation.
- Subject to direct regulatory supervision and enhanced operational resilience requirements.

2. Critical CIF Support

- Non-designated ICT service providers supporting a critical or important function for their EU financial service customers.
- EU customers expect DORA as the baseline for resilience and operational standards.
- Not directly in-scope for ESA supervision.

3. ICT Service Providers not supporting CIFs

- Non-designated ICT service providers that currently do not support a critical or important function for their financial service EU customers
- Customer expectations increasingly demand leading practice standards
- Customer dependencies may evolve leading to reclassification.

4. DORA Implementation- Lessons Learned

KPMG has acquired substantial experience in conducting DORA engagements for financial institutions, providing bespoke insights derived from various lessons encountered. These insights are designed to assist ICT third-party service providers in effectively navigating a smooth and compliant DORA journey.

Lack of ownership & embedding into BAU

- Tendency to **prioritise programme-centric approach**.
- **Lack of** BAU ownership across **end-to-end resilience** lifecycle.

Resource constraints & proactive planning for uplifts

- **Proactive resource planning** is essential to deliver on technical uplifts and adhere to regulatory and reporting requirements.

Integration with existing capabilities

- **Limited integration** of business continuity & crisis management **capabilities**.
- Including **not leveraging existing data from BIAs** / BCPs and DR testing to inform resilience posture.

Unknown resilience of the subcontracting chain

- **Limited provider engagement** resulting in unknown subcontracting reliance

Programme structure not designed to demonstrate compliance

- Structured, phased DORA compliance approach **prevents concurrent, complex remediation.**

Limited reporting to inform decision making

- Existing **risk metrics underutilised** for resilience reporting.
- Issues include **poor data quality, incomplete asset mapping**, and data held in functional silos.

B.

The designation and oversight of critical third-party providers (CTPPs)

5. DORA Framework Insights: Designated CTPPs

The DORA oversight framework aims to mitigate financial entities growing dependence on ICT third-party providers and concentration on a small number of providers within the European Union through the designation and oversight of critical third-party providers (CTPPs).

The DORA framework puts mechanisms in place to:

- Evaluate the robustness and effectiveness of internal rules, processes and governance mechanisms of CTPPs.
- Mitigate systemic and concentration risks by identifying dependencies.
- Provide a proportionate and risk-based oversight approach tailored to systemic impact of each critical provider.
- Monitor how effectively CTPPS manage ICT risks to ensure secure and resilient service delivery for financial entities.

European Supervisory Authorities (ESAs)

- Oversees third-party providers designated as critical at a European Union (EU) level.
- Comprised of EBA, EIOPA and ESMA.

Regulatory Oversight

- Annual oversight and prioritisation of supervisory focus.
- Rights to conduct investigations, on-site inspections and request information.
- Review of ICT risk management, security practices and incident handling.
- Collaboration with other regulatory bodies to ensure consistency.

Information Exchange & Coordination

- Central repository for contractual arrangements with CTPPS.
- Information-sharing across Financial Supervisory Authorities.
- Coordination protocols for managing systemic incidents.

Key Framework Objectives:

Strengthening Financial Stability

- Safeguard the stability of the financial system at a EU level.
- Preserve the integrity of the EU financial services market.

Resilience Enhancements

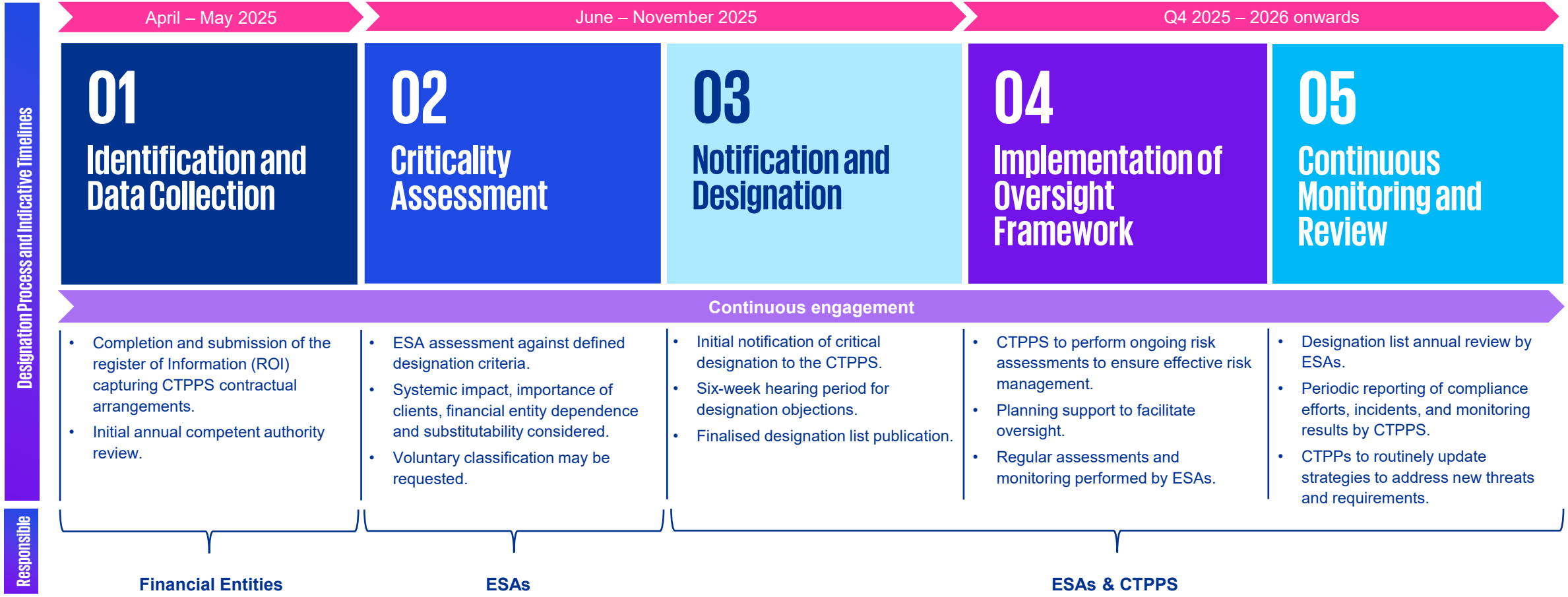
- Enhanced operational resilience for all financial entities (FEs) dependent on critical third-party providers for ICT services.

Increased Transparency and Accountability

- Clarity around critical service providers, dependencies and concentration levels.
- Streamlined supervisory approach for efficiency.

6. Regulatory Designation Process

Below is an overview of the critical designation process that ICT third-party service providers can expect. A clear view of process steps, timelines and criteria is key for anticipating supervisory expectations and preparing for enhanced oversight.



Please note that documented timelines are subject to change and are dependent on levels of supervisory engagement.

C.

ICT Service Provider Next Steps & KPMG Services

7. ICT Service Provider Next Steps

A comprehensive DORA approach is required to effectively identify, assess, and manage ICT risks while establishing and ensuring digital trust with customers.

Designation Strategy

ICT service providers need to immediately determine their designation strategy. Addressing questions like:

- Have we conducted an initial designation assessment?
- Will we opt-in, accept or challenge designation?
- Do we need to create a DORA implementation plan?

DORA Readiness

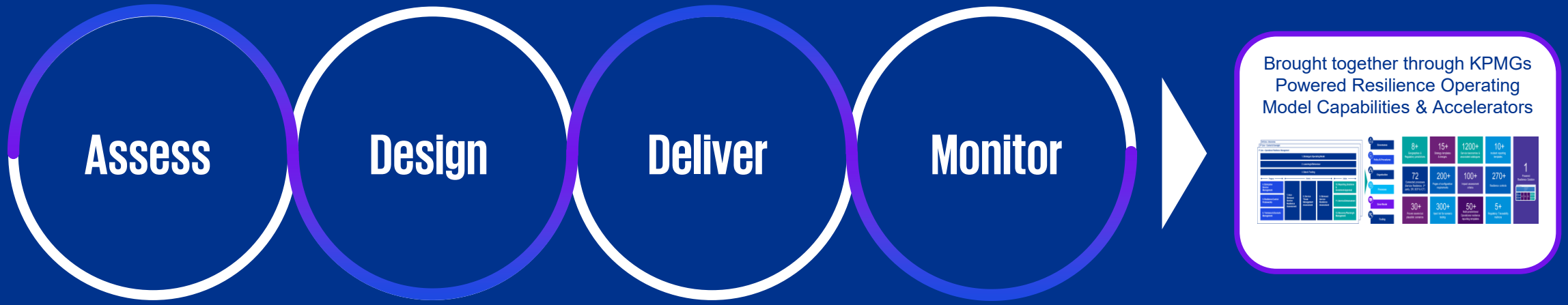
- ICT service providers should evaluate current practices against DORA requirements, identifying gaps and ensuring compliance.
- If currently implementing a DORA programme, benchmark progress and ensure ability to operationalise uplifts identified.

Ongoing Compliance

- ICT service providers need to demonstrate ongoing compliance with DORA to both the ESAs and their customers.
- KPMG can support the design and implementation of a DORA operating model that is both sustainable and scalable, ensuring long-term compliance and resilience.

8. Summary of our services across the DORA journey

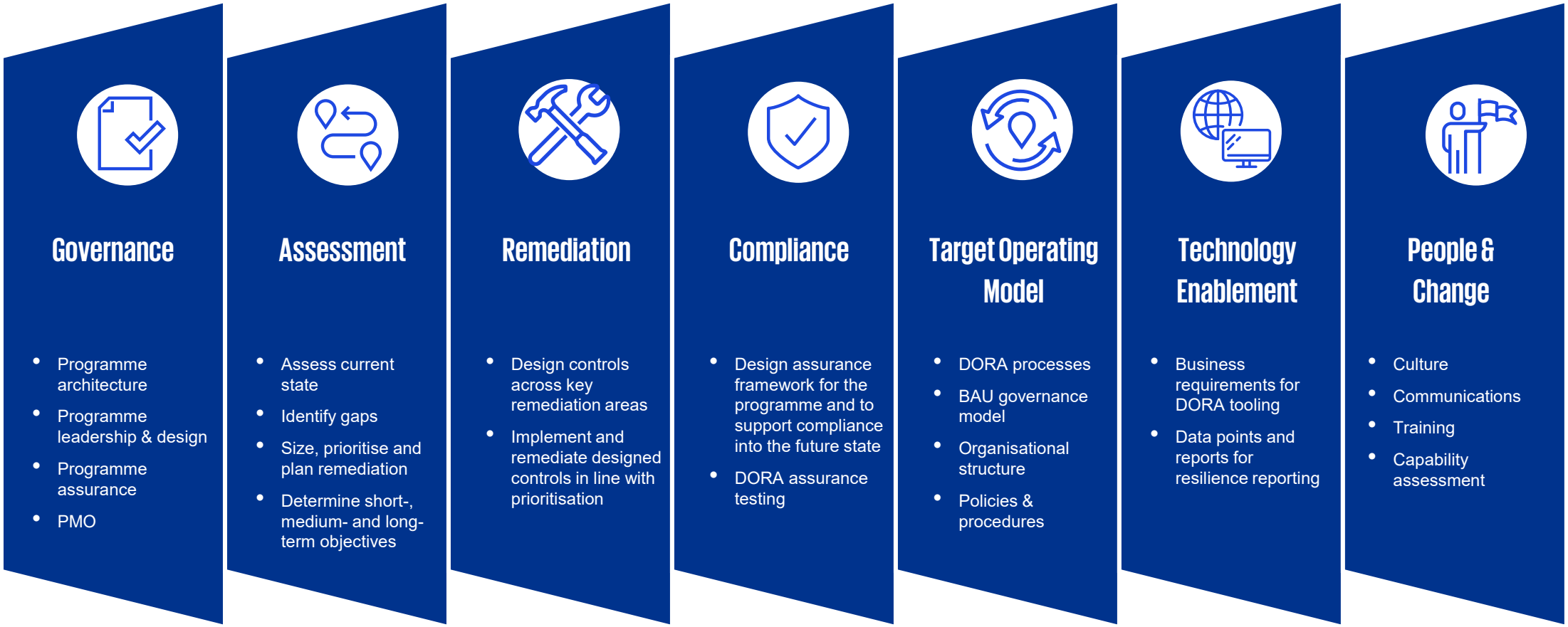
KPMG has been working with a number of significant European Institutions on their DORA programmes from assessment through to supporting implementation. A detailed gap analysis is performed in the "Assess" phase and using the output from this, we work with our clients to design a DORA programme which will allow them to successfully achieve compliance in a way that is bespoke to their organisation and any specific complexities which may exist.



- Evaluation and assessment of designation as a critical provider and the notification process as well as current position, gaps and uplifts to meet compliance objectives
- Mobilise multi-disciplinary team across Law, Governance, Technology, Cyber, Resilience, Third Party Management and Data Governance
- Harmonisation approach blueprint in line with any existing in-flight Resilience initiatives
- Institutionalise an outcome based on Resilience capability that facilitates DORA compliance requirements

9. Our Services Across a Successful DORA Programme

Below we have outlined key components of a successful DORA programme and an illustrative scope of what each of these components may include. These are all services which our multi-disciplinary team has extensive experience in providing to large institutions.



KPMG

kpmg.ie

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Document Classification: KPMG Public

Jackie Hennessy

Partner, Technology Risk Consulting

Email: jackie.hennessy@kpmg.ie

Mobile: +35317004171

Carmen Cronje

Director, Technology Risk Consulting

Email: carmen.cronje@kpmg.ie

Mobile: +353870504455

Devin Van Rooyen

Manager, Technology Risk Consulting

Email: devin.vanrooyen@kpmg.ie

Mobile: +353872859747

Sarah Twomey

Senior Associate, Technology Risk Consulting

Email: sarah.twomey@kpmg.ie

Mobile: +353860318101