Digital Operational Resilience Act (DORA) as a Service

The Digital Operational Resilience Act (DORA) (Regulation EU 2022/2554) harmonises rules across the EU and is a mandatory EU regulation that has had effect since January 2025, requiring financial institutions to manage risks and strengthen IT security and resilience.

Accelerating continuous resilience with CGI's expert-led DORA service model.

Mature, Manage, and Maintain

CGI's DORA services are modular and designed to align to your current maturity stage.

- **Mature** helps build robust foundations through analysis of your posture, risk assessments, and supporting governance design and implementation.
- **Manage** helps operationalise ICT Risk Management, Incident Response automation, and third-party risk management.
- **Maintain** gives assurance to ongoing operational resilience, through threat-led testing, disaster recovery tests, and enhanced reporting. All of these are underpinned by our extensive, trusted, cyber security service offerings.

Scope

CGI approaches DORA through three modular considerations:

1. ## Organisational Pillars

   We take DORA's five pillars (ICT Risk Management, Incident Management, Testing, Third Party Risk Management (TPRM), and Business Continuity) and map them to your business domains, including: risk, compliance, CIO/CTO functions, Security Operations, Procurement/Vendor Management, and Legal. We will work with you to assess your maturity across these functions, not just at a system-by-system level. This aligns with your governance models and illustrates where responsibilities are.

2. ## Critical Business Services / Capabilities

   Digital resilience is assessed and reviewed against DORA, for your most critical business services including: payments, trading, customer onboarding and offboarding, core banking, and claims handling. We will explore supporting ICT chains such as networks, applications, third parties, and data flows. This approach avoids extensive and costly audits, while ensuring materiality and business continuity alignment.

3. ## Material ICT Assets / Dependencies

   For each of your critical business services, we will work with you to identify and assess key applications and infrastructure, third-party dependencies, and any high-impact failure points. This will assure technical recommendations are made against the areas of highest risk.

Approach and Outcomes

We will adopt the following intersecting levels to inform our delivery approach:

Discover

We will work with you to understand your operational context, business services, and regulatory exposures. Through this, we identify those business services which are most critical and their supporting ICT environments. Organisational roles in risk, compliance, IT and procurement are also reviewed, and DORA is then mapped to your operating model and key functions.

Assess

The five pillars of DORA are mapped to existing capabilities and then evaluated. Current controls, governance models, incident response processes and third-party oversight are analysed. We achieve this through a qualitative gap analysis against DORA, with control maturity scoring and heat map outputs illustrating strengths and weaknesses across the organisation.

Prioritise

We will then collaborate with you to focus on the areas with the highest operational and regulatory impact. Findings are prioritised based on risk to business continuity, third-party exposure and / or regulatory non-compliance. Remediations are also likewise grouped by business criticality not just on a system-by-system basis. We then deliver you a targeted action map, highlighting timelines and business owners, and will also be able to include additional support with implementations where requested.

Recommend

The roadmap towards compliance and enhanced operational resilience is then defined. We deliver tailored, risk-proportional recommendations for your specific business, rather than generic controls. We can design improvements to your governance, process automation, testing, and reporting regimes. Maturity is further enhanced with additional uplift activities proposed in line with our Mature, Manage, and Maintain model.

Validate

CGI will work with you to design, facilitate and execute tabletop exercises, Threat Led Penetration Tests (TLPTs), or recovery simulations. This will support the testing and validation of incident management, third-party engagement and responses, and resiliency procedures.

Assured Operational Resilience

Strong operational resilience is built through clarity, prioritisation, and continuous assurance. CGI helps you move beyond point-in-time compliance toward sustained, exercised resilience. Contact us to learn how our cyber services can help you meet DORA expectations today, while strengthening your resilience for tomorrow.

Key Capabilities

Leveraging our decades of trusted partnerships, CGI helps clients (especially those with cross-border operations) ensure compliance and advance operational resilience.

- Readiness and gap analysis
- Third-party Risk Management
- Governance framework design and implementation
- Business Continuity / Disaster Recovery Planning
- Cyber risk management
- Ongoing Assurance and Reporting
- Threat-led testing (red / purple teaming)

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-focused to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information

Visit: Cyber security | Email us at: cyber.enquiry.uk@cgi.com