The Digital Operational Resilience Act (DORA)

An intelligence-led, expert-driven, strategic approach to global cybersecurity challenges affecting your organisation – your people, your operations, and your reputation.

DORA is the European Union's initiative to increase resilience against cyber attacks and Information and Communications Technology (ICT) related disruptions to financial entities across Europe and of their ICT and Cloud providers. The European Parliament and Council of Ministers published the finalised DORA text in June 2022. The act entered into force on the 16th of January 2023, after its publication in the Official Journal of the EU.

As a global leader in operational resilience and regulatory compliance, FTI Cybersecurity is expertly placed to help your business navigate and implement DORA's requirements. Through a comprehensive, bespoke programme which focuses on evaluating your current posture, harmonising existing resilience-focused activities, and providing fiscally- and organisationally- appropriate roadmaps to ensure continued progress, FTI Cybersecurity will guide your enterprise towards a compliant and resilient future.

DORA PRESENTS ITS REQUIREMENTS ACROSS 5 KEY PILLARS:

- ICT Risk Management
- ICT Incident Reporting
- Digital Operational Resilience Testing
- Information and Intelligence Sharing
- ICT Third-Party Risk Management

DORA has significant implications for financial services organisations and many third-party providers, with numerous requirements across all aspects of digital operational resilience.

Penalties and consequences for failure to comply with DORA are severe: a periodic 1% penalty payment of the average daily worldwide turnover may be applied.

Compliance with DORA requires a unified approach across the above areas, and most firms will likely require external support from partners with deep expertise.

Our Services

DORA builds on existing risk management requirements and ties several recent EU initiatives into one to create a harmonised approach across the EU. The detailed requirements for each key category of compliance, along with FTI Cybersecurity's capability to support these, are outlined below:

ICT Risk Management

- Define an appropriate governance model
- Develop an efficient risk management framework and support its deployment
- Perform risk assessment
- Provide expertise to develop cyber secure ICT systems
- Define, implement, and operate a comprehensive detection system for cyber attack detection, analysis, and reaction
- Design and test BCP and DR

ICT Incident Reporting

- Define, implement, test, and update a comprehensive incident response plan
- Propose a framework and an operating model to report the ICT-related cyber incidents

Digital Operational Resilience Testing

- Establish a digital operational testing plan in line with national regulations and the enhanced ICT risk framework with scope, approach and methodologies, timing, responsibilities, correction effects
- Assess response and recovery and recommend improvement and risk migration strategies for all impacted ICT systems and stakeholders
- Implement the testing plan

Information and Intelligence Sharing

- Design a process and an operating model for information sharing to integrate this information into cyber detection and investigation capabilities and in the risk management process

ICT Third-Party Risk Management

- Define requirements and service legal agreements for the contracts with third parties, according to enhanced ICT third-party risk framework and assessment on the scope of the third party
- Identify cyber attack reporting and contribution to incident response plan

FTI Cybersecurity's recommended approach includes a series of activities across the three stages of diagnosis, design, and implementation. Our team of experts will work with the client to tailor the approach as required, depending on the particular circumstances. For example, any work that has already been completed and any that is already in progress or planned.

Stage 1: Diagnostic Stage	Stage 2: Design Stage	Stage 3: Implementation Stage	Transition to Run
The purpose of the Diagnostic stage is to understand your organisation's maturity in respect of DORA compliance; the outcomes of the diagnostic will be summarised in a gap analysis document and your prioritised actions for the following stages will be outlined in an action plan.	In the Design stage, we help you to design, plan and prepare a comprehensive DORA compliance programme with activities, milestones, teams and associated programme governance.	During this stage, we will begin putting the governance, process and procedures in place for each pillar. We will also start writing the policies and implementing controls and technical measures.	Throughout the Implementation stage, the changes identified and carried out in previous stages will be embedded with the organisation, through efforts such as training workshops and control implementation.

CASE STUDY

Providing a Cybersecurity Assessment and Resilience Plan for a Multinational Corporation

SITUATION

FTI Cybersecurity was retained to provide an independent cybersecurity assessment and resilience plan with respect to the Client's current cybersecurity maturity, and to provide recommendations based on the findings of that assessment to strengthen the Client's overall resilience against potential cyber threats and vulnerabilities.

OUR ROLE

FTI Cybersecurity conducted a thorough review of all written information technology security policies, processes, and procedures and interviews of members of the Information Systems department.

While onsite, the team visited the data centre and observed physical protection measures and reviewed the company's backup and disaster recovery procedures.

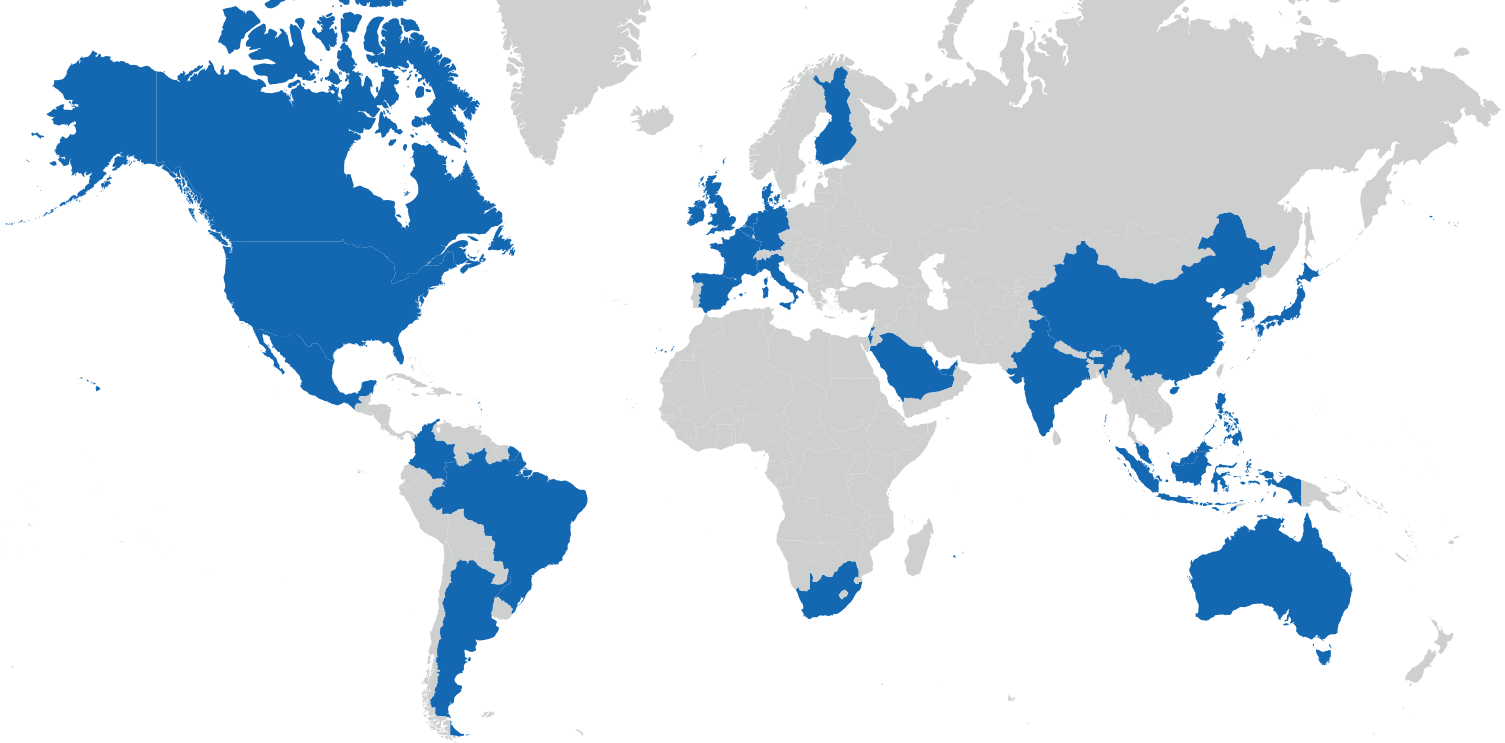
We also assessed the company's threat profile, determined the most common cybersecurity threats the company may face, and conducted a bespoke security awareness training to the IT help desk, applications support, business solutions, services support, and telecommunications teams.

OUR IMPACT

After reviewing the documents and information collected via interviews, we provided a prioritised implementation roadmap to address security gaps, improve mitigation strategies and cybersecurity measures, and meet industry standards. The recommendations spanned areas from IT Staffing to Tooling to Security Processes.

To help with implementation, we deployed a dedicated expert to act as interim CISO, who later transitioned the work to an in-house leader, a new, dedicated CISO.

To find out more about how our services and solutions can help your business, please contact us or visit us at www.fticybersecurity.com



Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, and global private sector institutions

Globally Positioned

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

No other firm in the space has a crisis communications practice

Integration of FTI Consulting's expertise across the platform

1982

Year Founded and $4.9B equity market cap*

9/10

Advisor to 9 of the world's Top 10 bank holding companies

7,500+

Employees Worldwide

NYSE:FCN

Publicly traded

98/100

Advisor to 98 of the world's top 100 law firms

59

59 of Fortune Global 100 corporations are clients

Number of total shares outstanding as of October 20, 2022, by the closing price per share on October 27, 2022.

ANTHONY J. FERRANTE
Global Head of Cybersecurity
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

JORDAN RAE KELLY
Head of Cybersecurity, Americas
Senior Managing Director
+1 202 312 9140
jordan.kelly@fticonsulting.com

DAVID DUNN
Head of Cybersecurity, EMEA & APAC
Senior Managing Director
+44 7816 251410
david.dunn@fticonsulting.com

02162023 | VN02598-v04