Module	**Digital Operational Resilience**
Jurisdiction	**European Union**
Legal Expert	**Martin Polaine** Barrister (England & Wales), Brooke Chambers Barristers – BrookeChambers linkedin.com/in/martin-polaine-fciarb-faiadr-961363132

Module Application

Does a financial entity employ measures for digital operational resilience in line with regulatory requirements?

Does the financial entity have an effective ICT risk management framework?

Does the financial entity identify, assess, and manage ICT risks by documenting ICT assets, functions, and responsibilities, and implementing measures to protect, prevent, and detect threats?

Does the financial entity have ICT business continuity policy and recovery plans in case of severe disruptions?

Does the financial entity define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents?

Does the financial entity establish digital operational resilience testing programmes?

Does a financial entity integrate ICT third-party risk management framework into its comprehensive ICT risk management framework?

Does a financial entity designated as a critical ICT third-party provider engage with the ESAs and Lead Overseer, implement ICT risk management, comply with annual assessments, cooperate in investigations, and pay oversight fees?

Module Scope

The Digital Operational Resilience Act (DORA) is a European Union regulation designed to ensure that financial entities maintain robust security and resilience in their information and communication technology (ICT) systems. Effective from January 17, 2025, DORA aims to protect the EU's financial sector from ICT-related disruptions and cyber threats by setting uniform standards for risk management, incident reporting, third-party oversight, and operational resilience testing.

DORA applies to a broad spectrum of financial entities regulated within the EU, including but not limited to:

- Core financial institutions: Banks, payment institutions, electronic money institutions, and occupational pension institutions must comply with DORA to safeguard their ICT systems and maintain stability across financial operations.

- Service providers and emerging sectors: DORA's reach extends to financial service providers in developing sectors, such as crypto asset services, account information services, data reporting, crowdfunding, and ICT third-party service providers essential to financial institutions.
- Investment firms and fund managers: Investment firms, alternative investment funds, fund management companies, credit rating agencies, and administrators of critical financial benchmarks are included within DORA's regulatory scope. This helps standardise resilience across critical market activities.
- Market infrastructure providers: Key infrastructure providers, such as central securities depositories, central counterparties, trading venues, and trade and securitisation repositories, fall under DORA. These institutions play an essential role in EU financial markets, and DORA ensures their resilience against ICT risks.
- Insurance and reinsurance sectors: DORA also covers insurance companies, insurance intermediaries, and reinsurance businesses, requiring them to implement ICT resilience strategies to protect policyholders and maintain trust in financial services.

Key requirements of DORA for financial entities

- ICT risk management framework: Financial entities, excluding micro-enterprises, must adopt robust ICT risk management frameworks. These frameworks should include governance and control measures, such as documented risk policies, procedures, and tools, to effectively manage and respond to ICT risks.
- Incident management and reporting: Entities are required to establish processes to detect, classify, and manage ICT-related incidents. For significant incidents, they must notify their designated authorities, who may escalate the report to higher bodies like the European Central Bank or European Banking Authority.
- Operational resilience testing: Financial entities must regularly test their operational resilience. This includes comprehensive digital resilience testing and threat-based penetration testing every three years, conducted by certified professionals to ensure the organisation can withstand potential cyber threats.
- Third-party ICT risk management: DORA mandates that financial entities assess and manage ICT risks posed by third-party providers. This includes contractual safeguards, regular assessments of dependency risks, and alternative solutions to mitigate potential threats.
- Oversight of critical ICT third-party providers: The European Supervisory Authorities (ESAs) are responsible for overseeing critical ICT third-party providers. Each designated critical provider is monitored by a lead overseer, who has the authority to request information, conduct investigations, and recommend remedial actions to ensure the provider's resilience.
- Information sharing and collaboration: Financial entities may exchange cyber threat information within trusted communities to enhance their digital resilience, as long as it complies with data protection and competition regulations.

Our expert's profile

MARTIN POLAINE
Barrister

PRACTICE AREAS

International Arbitration, Regulatory and Compliance (including corporate investigations, ESG, anti-corruption, AML/financial regulatory and sports governance), Public International Law, International Trade, Corporate and Institutional Governance

BROOKE CHAMBERS

MARTIN POLAINE is a barrister (England & Wales) of more than 35 years' experience and an arbitrator. He is a Fellow of both the Chartered Institute of Arbitrators (FCIArb) and a Fellow of the Asian Institute of Alternative Dispute Resolution (FAIADR).

Martin has advised states, corporates and individuals across Africa, Asia and Europe on dispute resolution and public international law. He has extensive experience in both civil law and common law states and his practice includes international arbitration (both commercial and state-investor), regulatory and compliance (including corporate investigations, ESG, anti-corruption, AML/financial regulatory and sports governance), public international law, international trade and most aspects of corporate and institutional governance.

Having a keen interest in professional regulation, Martin has advised law societies and other professional bodies on a range of issues, including the use of quality assurance standards (Lexcel, ISO standards and others), the drafting of codes of conduct and financial regulatory compliance.

He is a published author of legal texts (with Oxford University Press and others), a Teaching Fellow at the College of Law (Sydney), where he tutors LLM students, and Co-Chair of the Inter-Pacific Bar Association's Legal Training & Development Committee.

About LexisNexis Regulatory Compliance®

LexisNexis Regulatory Compliance® helps you forge a clear path to compliance.

With LexisNexis® content know-how at the core, our compliance registers, alerts, and information-driven solutions make compliance uncomplicated for GRC professionals across the globe.
