Digital Operational Resilience Act

ISG's Introduction to DORA Compliance and Risk Management

ISG

What is DORA?

Digital
Operational
Resilience
Act

The Digital Operational Resilience Act (DORA) is the European Parliament's attempt to foster technological development, financial stability, and consumer protection.

In the face of increasing cyber-attacks and other information and communications technology (ICT) breaches, digital resilience for the whole financial sector is becoming even more imperative.

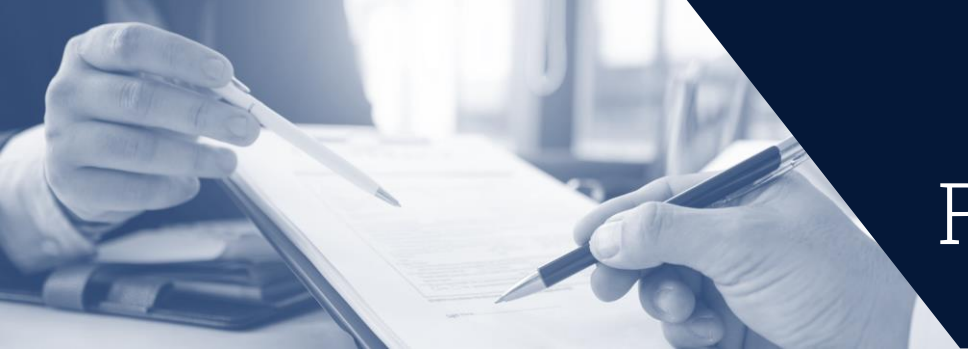
As a part of the EU's Digital Finance Package (DFP), DORA aims to develop a harmonized European approach to digital finance.

The European Council adopted the draft version of DORA in November 2022, which is designed to consolidate and mitigate ICT risks and ensure all financial system participants are subject to a common set of standards.

DORA requires firms to withstand all types of ICT related disruptions and threats

DORA's core aim is to prevent and mitigate cyber threats by ...

1. Governing the monitoring of ICT **third-party providers**
2. Overseeing critical ICT **third-party providers**
3. Addressing ICT risks and **strengthen digital resilience**
4. **Streamlining** ICT-incident **reporting and threat** intelligence exchange
5. Ensuring assessment of **preventive and resilience** measures
6. Providing access for **supervisors** to ICT incident-related **information**



Broader Applicability of DORA Regulations in the Provider Ecosystem

In contrast to previous regulations, DORA focuses on a broad range of financial institutions and their ICT third-party service providers, including providers of cloud computing services, software, data analytics services and providers of data center services. All companies in scope will need to comply with the DORA requirements once it is in effect and ensure their auditability. In addition, DORA also includes additional requirements for those financial institutions that already were in the scope of existing regulation (e.g., EBA Guidelines on outsourcing).

DORA

Outsourcing

Basic prerequisite

ICT third-party risk

Governance related requirements

ICT risk management requirements

ICT-related incident reporting

Digital operational resilience testing

Information sharing

○ **No additional requirements**

◔ **Only minor additional requirements**

◑ **Some additional requirements**

◕ **Major additional requirements**

● **All new requirements**

* *Scope of threat led penetration testing needs to be defined by ESAs (European Supervisory Authorities). Small und uncritical financial institutions are most likely not in scope.*

Are You Impacted by DORA?

Financial Institutions

Banks and associated companies

- Credit institutions
- Payment institutions incl. electronic money institutions
- Crypto-asset service providers
- Institutions for occupational retirement provision

Investment related companies

- Investment firms and managers of alternative investment funds
- Central securities depositories; central counterparties
- Trading venues and trade repositories
- Credit rating agencies
- Administrators of critical benchmarks
- Securitisation repositories
- Management companies

Insurance companies

- Insurance and reinsurance undertakings
- Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries

Service Providers

- Crypto-asset service providers
- Data reporting service providers
- ICT third-party service providers
- Crowdfunding service providers
- Non-Bank Financial service providers

** Any ICT third-party service providers not designated as critical would have the option to voluntarily "opt in" to the oversight*

DORA Rollout Timeline

2020

The European Commission, European Council Presidency and European Parliament proposed building a DORA framework

Nov 2022

The Council adopted a draft version of DORA

Jan 2023

The Council is asking for all RTSs (Regulatory Technical Standards) to be produced by 18 months. That reduces the adherence possibility to 6 months

2025

DORA comes into effect/ enters into force

End 2025

Penetration testing begins

3 Key Steps to Prepare for DORA Compliance - Financial Institutions

Are you a Financial Institution?

DORA will add new and enhanced requirements to your existing compliance activities.

It is critical for Institutes to identify actions they can take now, before the primary legislation is finalized and Level 2 standards from the ESAs are available.

As a Financial Institution you should consider the following steps:

1. **Identify** potential downstream impact by mapping the 5 DORA chapters to policies, structures, processes & operating model.

2. **Assess** your environment for any gaps and missing requirements – then evaluate your operational risk according to your risk appetite within DORA norms.

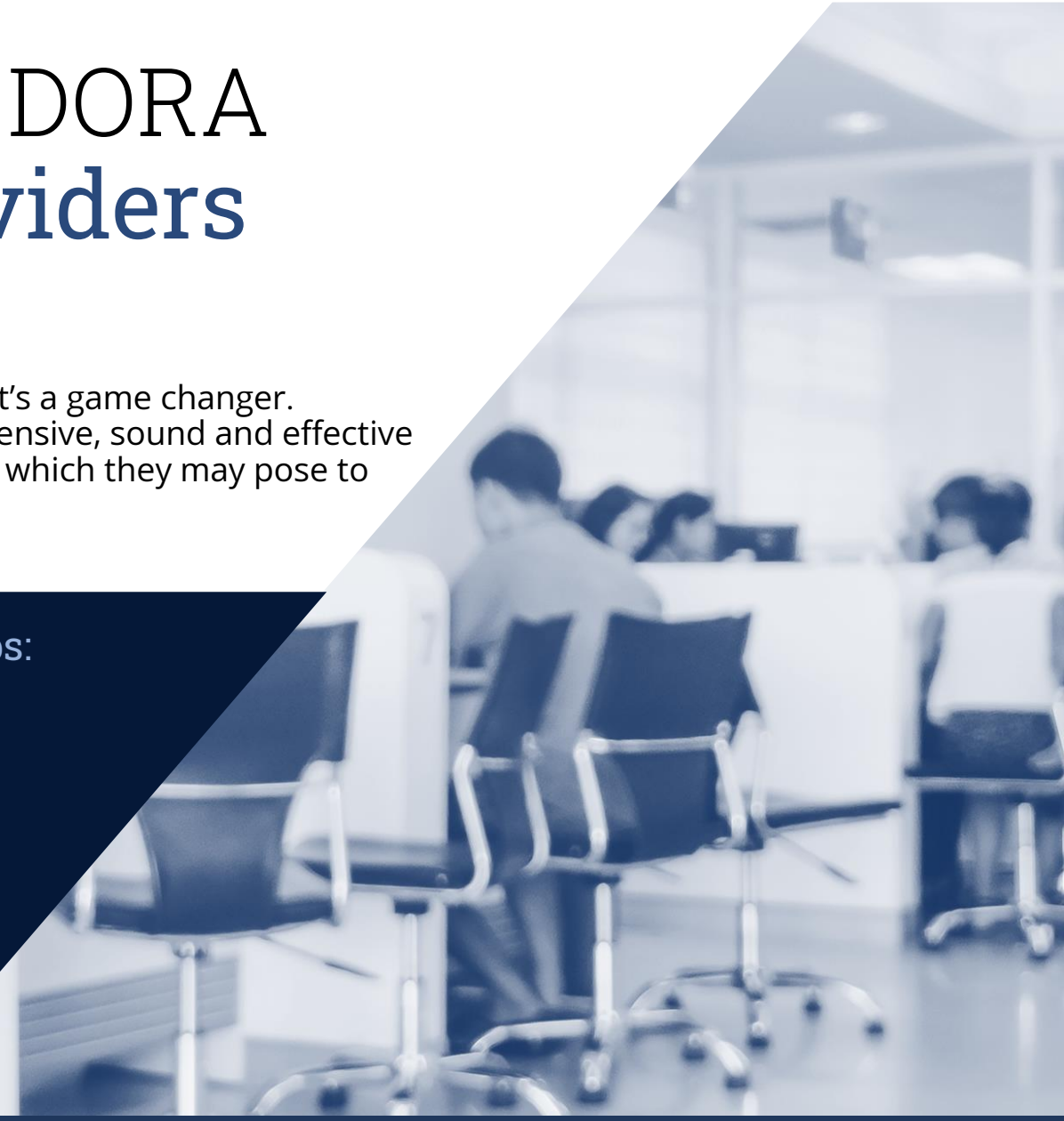
3. **Build** a realistic mitigation roadmap (e.g., for two-years), including a review and, if necessary, renegotiation of relevant contracts to meet mandatory components.

Act Now to Ensure the Compliance from Day One

3 Key Steps to Prepare for DORA Compliance - Service Providers

Are you a Service Provider?

DORA's requirements include the direct oversight of service providers. That's a game changer. Critical ICT Third-Party Providers will be required to have in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risks which they may pose to Financial Entities.



As a Service Provider you should consider the following steps:

1. **Determine** if you are, in fact an ICT service provider for financial entities.

2. **Decide** if you are willing to pay the (extra) price to be part of the financial industry. Are you prepared for the consequences of constantly evolving regulatory requirements?

3. If so, **identify** the potential impact, **perform** a gap analysis and **define** a distinct roadmap.

Companies that will be classified as Critical ICT Third-party Providers must have an establishment or a subsidiary located in the EU

ISG Banking Compliance Management Framework

Compliance with DORA requirements is essential for staying in business. The penalty for non-compliance can be as high as the average daily worldwide turnover of the company until compliance is achieved.

All institution should review existing and new contracts against mandatory components.

For third-party ICT service providers, early compliance provides a competitive advantage and an opportunity to increase market share.

Your solution to the organizational and technical implementation of DORA

ISG's **Banking Compliance Management Framework** helps you comply with DORA regulations to ensure you implement the right policies, guidelines and processes.

Assessment	Compliance Roadmap	Implementation
Gain a thorough understanding on your current policies and procedures as well as through interviewing your SMEs.	Evaluate, establish and prioritize your DORA compliance roadmap based on the assessment findings and our expert's advice.	Walk you through each step hands-on, and stick with it through completion.

DORA Incident Reporting*	DORA End-to-end Testing*
Define, develop and implement a compliant Incident Reporting and End-to-End Testing approach.	

**Once the guidelines are finalized by the ESAs*

DORA Chapters				
ICT Risk Management (incl. governance)	ICT Incident Reporting	Resilience Testing	ICT Third-party Risk	Information Sharing

Our DORA solution touches on all following key elements

Policies and Instructions	Structures and Procedures	Retained Organization	Third-party Provider	Cybersecurity

ISG Banking Compliance Management Framework

How compliant is your company with the existing and new regulations?

Your solution to European Supervision and National Supervision compliance

With technology advancement, Financial institutions are facing tighter regulations to protect consumers, maintain financial stability and prevent illegal activities. ISG's Banking Compliance Management Framework not only helps you comply with DORA, but also with European Supervision and National Supervision regulations, for example: The Bank of England's Prudential Regulation Authority (PRA) Supervisory Statement SS2/21, EBA Guideline on Outsourcing, German Banking Act (KWG, incl. MaRisk), and Austrian Banking Act (Bankwesengesetz).

Compliance Readiness
We provide insights not only into existing but also soon-expected regulations.

Protect against Penalities
By getting compliant, we prevent you from paying high penalties (up to 1% of turn-over).

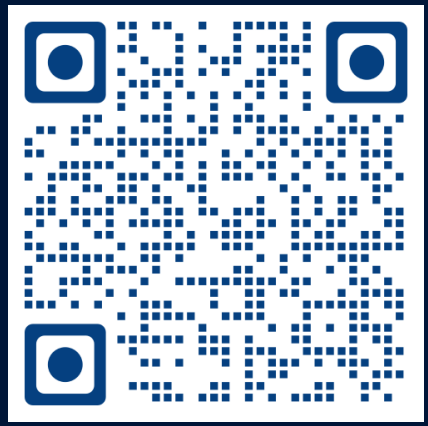
Customer Trust
We support you in improving customer trust by innovating your organizational setup.

One-hour Free Expert Call

We like to offer you a free expert call, in which we discuss:

- Current challenges in banking regulation and compliance
- ISG's end-to-end Compliance Management Framework
- Your situation and identify next steps

isg-one.com/contact-us



Let's discuss >>

isg-one.com

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 900 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,600 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit www.isg-one.com.