PROFESSIONAL GUIDE DECEMBER 2023

Cybersecurity – DORA Practical Guide

AFG

CONTENTS

AFG wishes to thank the members of the Cybersecurity Working Group
who contributed to the drafting of this Guide,
and particularly its chairman, Wilfried Lauber (Amundi).

The Cybersecurity Working Group
is affiliated with the Ethics and Compliance Committee
chaired by Monique Diaz (AXA Investment Managers Paris).

Valentine Bonnet, head of Corporate Governance and Compliance (AFG),
coordinated this work.

Introduction

The DORA Regulation *(Digital Operational Resilience Act)* defines a detailed, comprehensive framework on digital operational resilience for financial entities, and therefore applies to asset management companies (AMC).

The regulation, which will come **into force on 17th January 2025**, imposes obligations on financial entities, but also on their digital service providers, which must review their procedures, contracts, mechanisms and tools on a regular basis to ensure information systems security.

What is operational resilience?

→ **The ability of a financial entity to rebuild, reassure and review it's operational capability, integrity and reliability (...) including through disruption.[1]**

DORA aims to steer the financial sector towards a real maturity that goes beyond each participant's individual operational resilience to strengthen the resilience of the sector as a whole. In addition to the financial actors that will be designated as systemic for the European financial system and other players involved in its implementation, DORA applies to ICT service providers, which will be subject to stringent requirements and a high level of oversight, for the long-term benefit of the sector.

What is an ICT service provider?

→ **An ICT service provider is an entity that provides an IT service, in the broad sense, whether as a cloud service, a hosted service or internally from your own data centre or infrastructure through software you use inside your organisation/company.. This covers all areas of information technology, including data storage, processing, entry and provision.**

This guide aims to be practical and actionable. Each chapter will be divided into four key sections:

Current situation: important points for verifying that you do in fact meet the requirements of DORA, since you have probably already implemented these practices.

What's new: requirements under DORA for which the next steps appear to be within reach.

Challenges: more complex requirements for which AMCs will need to take certain measures.

Keys for the board: these are key points that your board should focus on and which you can use in an elevator pitch.

Note: in this document, the term "board" refers to your management body.

1) See Art 3.1.