Skadden

# Cybersecurity and Data Privacy Update

November 2, 2023

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

**David A. Simon**
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

**Alistair Ho**
Associate / London
44.20.7519.7005
alistair.ho@skadden.com



One Manhattan West
New York, NY 10001
212.735.3000

## DORA — Key Considerations for Alternative Investment Funds

### A. Introduction

The EU Digital Operational Resilience Act (Regulation (EU) 2022/2554) (DORA) creates a regulatory framework intended to enhance the operational resilience of the financial sector by establishing uniform requirements for the security of network and information systems. Forming part of the EU's Digital Finance Package (DFP), aimed at developing a harmonised European approach to digital finance, DORA is designed to ensure that financial institutions operating in the European Union, including alternative investment funds (AIFs or Funds), can effectively mitigate information and communication technology (ICT) risks and manage disruptions. Financial entities, including AIFs, will need to start assessing their operational resilience and understanding the actions required across the Fund to ensure compliance.

DORA's operational provisions take effect on 17 January 2025, giving AIFs just over 14 months to bring the Fund into compliance. Obligations under DORA are to be further detailed in regulatory technical standards (RTS) and implementing technical standards (ITS) — the first set of RTS and ITS, which are currently in draft, will be submitted to the European Commission by 17 January 2024 for adoption.

### B. Management-Led Regulation

At the heart of DORA's design is the recognition of the key role in ensuring the Fund's operational resilience played by the management body, defined as the body or bodies "empowered to set the entity's strategy, objectives and overall direction, and which oversee and monitor management decision-making and include persons who effectively direct the business of the entity"[1] (the Management Body).

DORA places the ultimate responsibility for compliance on the Management Body, requiring it to define, approve, oversee and remain accountable for a Fund's ICT risk management framework. An AIF's Management Body therefore needs to ensure it keeps informed of DORA's evolving requirements and best practices — this includes understanding the Fund's ICT risks and ensuring that appropriate measures are implemented to mitigate them.

### C. Overview of Substantive Requirements

DORA sets out a range of substantive requirements that AIFs will need to comply with, including:

[1] Article 3(30), DORA.

# DORA — Key Considerations for Alternative Investment Funds

## 1. Risk Management Framework

DORA mandates the establishment of a comprehensive and documented ICT risk management framework. AIFs should ensure that they have developed and implemented:

- **Policies and Procedures:** Comprehensive policies and procedures are required to allow AIFs to adequately identify, assess, manage and monitor ICT-related risks. Backup policies and procedures and a comprehensive ICT business continuity policy are also required.
- **Appropriate Measures:** AIFs will need to adopt appropriate measures, commensurate with their activities, to "continuously monitor and control the security and functioning of ICT systems"[2], "detect anomalous activities"[3] and mitigate ICT-related risks. Such measures may include encryption, access controls and end-point detection and response systems.
- **Cybersecurity Training:** Adequate training for personnel is essential to enhance awareness of digital threats and improve response and mitigation capabilities.
- **Cybersecurity Testing:** Regular cybersecurity testing (*e.g.*, threat-led penetration tests and vulnerability assessments) should be undertaken, and will be required for certain Funds, to allow for the ongoing identification and remediation of issues and vulnerabilities. Additionally, simulation exercises are recommended to assess preparedness for potential disruptions.

## 2. Third-Party Risk

Recognising the interdependencies in the financial ecosystem, DORA emphasises the significance of managing risks associated with third-party ICT service providers:

- **Third-Party Risk Strategy and Register:** AIFs will need to establish a strategy for managing third-party risks and maintain a register of agreements with ICT service providers.
- **Contracting With ICT Service Providers:** Contracts with ICT service providers will need to follow specific requirements (with more extensive requirements applying to contracts which support critical or important functions), including provisions for effective oversight, audit and compliance with DORA's mandates. AIFs will need to review and update their template ICT service provider agreements and consider re-papering existing ICT service providers.

  AIFs will need to review their ICT service provider diligence and onboarding procedures to ensure that they include (i) risk assessments, (ii) due diligence (including in relation to service provider subcontracting arrangements), (iii) selection, governance and approval, and monitoring processes, and (iv) exit/termination strategies.
- **Critical ICT Service Providers:** DORA introduces the concept of "Critical ICT third-party service providers", which will be subject to direct oversight by the relevant European Supervisory Authority. Critical ICT service providers will be designated by the Joint Committee of European Supervisory Authorities[4], based on certain criteria, including the:
  - expected systematic impact on stability, continuity or quality of financial services were the provider to face a large-scale operational failure to its provision of services;
  - systematic character or importance of financial institutions that rely on it;
  - degree of reliance of those financial institutions on the provider's services in relation to the critical or important functions of those institutions; and
  - degree of substitutability of the provider.

  ICT service providers may also opt-in to oversight if not designated. Critical ICT service providers (whether designated or opt-in) would be subject to additional obligations, including the requirement to establish an EU subsidiary, recordkeeping, reporting and payment of oversight fees.

  An AIF should consider whether any of its ICT service providers may be categorised as 'critical' and how this might impact the services received. For example, financial institutions will only be permitted to make use of the services of a third-country critical ICT service provider if such provider establishes a subsidiary in the EU. AIFs may find themselves in breach of DORA if they continue to use existing service providers which are designated as (or opt-in to be) critical ICT service providers and which do not comply with their DORA obligations.

## 3. Incidents Management, Classification, Reporting and Review

DORA outlines a structured approach for AIFs to manage ICT-related events, including to identify, manage and notify ICT-related incidents. "Major" incidents will need to be notified to competent authorities "without delay"[5] when the Fund becomes aware of them, using mandatory reporting templates. In certain cases, notifications to customers may also be

[2] Article 9(1), DORA.

[3] Article 10(1), DORA.

[4] The Joint Committee of European Supervisory Authorities is a forum with the objective of strengthening cooperation between the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA).

[5] Article 19, DORA.

required. AIFs will need to review their cybersecurity incident/personal data breach response plans and update them to ensure they contain the required processes and procedures.

### 4. Information Sharing

DORA permits information sharing among financial institutions to enhance compliance and collective resilience against digital threats, provided that those institutions notify the competent authorities of their participation in such information sharing arrangements.

## D. What Should AIFs Do Now?

### 1. DORA Implementation Team and Governance

AIFs should appoint a dedicated cross-functional implementation team, overseen by the Management Body, to ensure compliance with DORA's requirements. The dedicated team should include a range of relevant stakeholders (including input from group and local entity levels, as well as the AIF's portfolio) to ensure consistent risk management practices.

### 2. Mapping and Gap Analysis

A comprehensive mapping of digital activities, systems, dependencies and third-party service provider contracts should be undertaken by the cross-functional team to identify the Fund's current state of operational resilience. A gap analysis should then be performed to identify areas where current practices fall short of DORA's requirements. AIFs may look to leverage parallels with existing cybersecurity standards with which they comply — *e.g.*, NIST or ISO 27001 — and may wish to engage consultants and/or legal counsel to assist in conducting the gap assessment and advise on how DORA's requirements apply in the context of the AIF's activities.

AIFs should consider the following stages when conducting a gap analysis:

a. **Scope the DORA Framework Requirements.** Identify the compliance requirements under DORA, as outlined above, and understand how they apply to each entity in the group structure and to the group as a whole.

b. **Map Internal Procedures and Processes.** A comprehensive mapping of digital activities, systems, dependencies and ICT service provider contracts should be undertaken to identify the Fund's current state of operational resilience in comparison to the standards required by DORA, including the RTS and ITS.

   i. *ICT Risk Management Framework.* Review the existing suite of ICT policies and procedures to provide an overview of the AIF's formalised risk management framework, including governance — *e.g.*, whether the AIF's control function directly reports to and advises the AIF's Management Body. Identify whether the AIF has formalised its:

      a. view of ICT risk. Work with relevant stakeholders to document the approved tolerance levels for ICT risk and the strategies implemented to manage such risk;

      b. policies and procedures on the management and operation of ICT assets, with a view to ensuring the security of networks against intrusions and data misuse, and preserving the availability, authenticity, integrity and confidentiality of data;

      c. policies on the use of encryption and cryptographic controls;

      d. procedures to identify and manage ICT system capacity requirements, enabling continued monitoring and optimisation;

      e. procedures for vulnerability and patch management, data and system security, logging and network security;

      f. policies on ICT project and change management, including the elements necessary to ensure effective management, practices and methodologies relating to the acquisition, development and maintenance of, and changes to, ICT systems; and

      g. physical and environmental security policies. Consider whether these have been designed according to the identified threat landscape, classification and risk profile of ICT assets used by the Fund.

   Additionally, whilst policies and procedures are informative, the mapping process should utilise working sessions with stakeholders to identify how such policies and procedures compare against operational reality. Furthermore, stakeholder workshops can assist in understanding whether the existing formalised framework is being applied in a coherent and consistent manner. Exceptions should be recorded, with consequences for noncompliance.

   ii. *Organisational Measures.* Review personnel onboarding procedures to determine whether new joiners are made aware of relevant policies and procedures and are adequately informed of their

ICT responsibilities and reporting channels. Review identity management and access controls to identify whether individuals are allocated appropriate user rights at all stages of their employment, including the revocation of all rights post-termination.

iii. *Training.* Review ICT training conducted by all personnel, including directors, officers, employees and contractors, to identify the level of cybersecurity awareness within the organisation and determine whether specific ICT security awareness and digital operational resilience training elements are incorporated.

iv. *Incident Reporting.* Review incident identification, reporting, management and remediation procedures. Consider how ICT-related incidents are identified and reported internally and whether, once reported, such incidents are appropriately classified and escalated. Identify any incident response team and escalation paths, which should include board-level involvement and procedures for engaging external stakeholders (*e.g.*, cybersecurity experts or legal counsel) as required. Determine whether the existing procedures allow for appropriate notifications to be made to applicable regulators and affected customers within the strict timescales required under applicable laws (see Section C.3). Additionally, consider how incidents are documented and post-incident review is undertaken and how learnings are implemented.

v. *Business Continuity and Disaster Recovery.* Evaluate the AIF's ICT business continuity and disaster recovery policies, including scope, time-frames (including maximum recovery times), criteria of activation, governance and organisation. Assess how such policies are tested (*e.g.*, through tabletop exercises and simulations) and how any identified issues are remediated.

vi. *Cybersecurity Assessments.* Review cybersecurity testing procedures (including vulnerability assessments and penetration testing) and the processes for recording and remediating identified issues. Evaluate the scope and frequency of testing to determine appropriate coverage. Consider how priorities are allocated to identified issues and how the responsibility for remediation is assigned and resourced.

vii. *ICT Provider Risk Management.* Identify existing ICT providers and ensure risk assessments have been documented as part of vendor onboarding and updated based on ongoing monitoring. Work with relevant stakeholders to determine how such risk assessments are undertaken and to understand the AIF's tolerance of, and strategies for, managing risk — *e.g.*, limiting reliance through supplier diversification — particularly in relation to any critical ICT service providers. Assess known and potential risks against the AIF's determined risk tolerance and existing policies to ensure alignment of practice with any formalised vendor management processes. Collate and review existing ICT service provider contracts and determine whether a re-papering exercise may be required to account for the specific provisions required under DORA.

viii. *Information Sharing.* Identify any current practices by which threat intelligence information is shared with third parties and authorities within the financial sector to strengthen compliance and community resilience against digital threats, including the types of information shared and how such sharing is undertaken. Consider what safeguards are put in place when sharing such information, including in relation to business confidentiality and the protection of personal data.

c. **Identify Gaps.** By comparing the applicable DORA requirements against the results of the mapping exercise, the Fund can identify and assess existing gaps. Certain areas may require little adjustment, whilst other areas may require significant updates. Some areas (*e.g.*, ICT service provider risk registers) may not form part of current practices at all.

### 3. Roadmap and Implementation

Based on the outcomes of the mapping and gap analysis, AIFs should develop and implement a comprehensive roadmap — prioritising key business functions and regulatory requirements — to ensure that the Fund is compliant with DORA prior to its effective date. Where applicable, AIFs will need to determine what actions should be taken at group and/or local entity levels. It is critical to ensure engagement and accountability for implementation from relevant stakeholders, including the Management Body (which is ultimately responsible for DORA compliance).

### 4. Monitor Implementation

DORA requires that AIFs continue to monitor the effectiveness of their implemented strategies, including by mapping ICT risks over time and analysing "the frequency, types, magnitude and evolution of ICT-related incidents."[6] In addition to implementing procedures to track implementation progress and validate gaps have been closed, AIFs will need to continue monitoring digital activities, systems, dependencies and ICT service provider relationships post-implementation to ensure operational resilience remains compliant.

## E. Conclusion

DORA is not just an information technology issue; it is a business concern. AIFs need to take proactive steps to align with DORA's requirements. A DORA implementation team should be appointed to assess how DORA applies to the Fund and conduct a gap analysis against the existing ICT framework. Identifying gaps will enable AIFs to develop a tailored and realistic action plan to navigate the complexities of DORA implementation and will ensure the Fund is equipped to take the steps necessary for DORA compliance.

[6] Article 13, DORA.