DORA – safeguarding the resilience of finance

Joint ESAs public event on DORA

6 February 2023

Mattias Levin

Directorate-General for Financial Stability, Financial Services and Capital Markets Union
Background

• Financial sector increasingly dependent on technology / tech companies for provision of financial services

• Makes financial sector vulnerable to problems with underlying tech, e.g. caused by cyber attacks

• Cyber risks partially addressed at EU level:
  - General rules: partial application finance, unevenly implemented
  - Financial services rules: patchy, inconsistent, fragmented
Upgrade EU rules to promote resilience

- Dedicated framework to safeguard digital operational resilience for finance – DORA [2022]
- Links to general framework
  - Substitutes (core provisions) via lex specialis status
    - NIS2 – Directive on measures for a high common level of cybersecurity [2022]
  - Complements
    - CER – Directive on resilience of critical entities [2022]
    - CSA – Cybersecurity Act [2019]
    - CRA – Cyber Resilience Act [under negotiation]
Scope

• Wide range of financial entities regulated at EU level
  • credit institutions; payment institutions; account information service providers, electronic money institutions; central securities depositories; central counterparties; investment firms; trading venues; trade repositories; data reporting service providers; managers of alternative investment funds and management companies; insurance and reinsurance undertakings; insurance and reinsurance intermediaries and ancillary insurance intermediaries; institutions for occupationnel retirement provision; administrators of critical benchmarks; securitisation repositories; actors in the crypto-assets area (crypto assets service providers, issuers of asset-referenced tokens); crowdfunding service providers; credit rating agencies.

• Exemptions and proportionality
  • Exemptions or simpler rules foreseen by the sector rules in the financial services acquis
  • Microenterprises
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT risk management</td>
<td>• Set of key principles and requirements on ICT risk management framework</td>
</tr>
<tr>
<td>ICT-related incident reporting</td>
<td>• Harmonise and streamline reporting + extend reporting obligations to all financial entities</td>
</tr>
<tr>
<td>Digital operational resilience testing</td>
<td>• Subject financial entities to basic testing or advanced testing (e.g. TLPTs)</td>
</tr>
<tr>
<td>ICT third-party risk</td>
<td>• Principle-based rules for monitoring third-party risk, key contractual provisions + oversight framework for critical ICT TPPs</td>
</tr>
<tr>
<td>Information sharing</td>
<td>• Voluntary exchange of information and intelligence on cyber threats</td>
</tr>
</tbody>
</table>
1. ICT risk management
(Articles 5-16)
2. Incident reporting
(Articles 17-23)

General requirements

- Establish and implement a management process to monitor and log ICT-related incidents
- Classify ICT-related incidents based on criteria set out in DORA and to be further developed by the ESAs

Reporting of major ICT-related incidents to competent authorities

- To national competent authorities (NCAs)
- Harmonized reporting content and templates
- Initial notifications, intermediate and final reports
- NCAs to provide details to institutions and authorities (ESAs, ECB, NIS2 authorities)
- Voluntary notification of significant cyber threats to NCAs
3. Testing
(Articles 24-27)

Basic testing
• All financial entities

Advanced testing
• Financial entities identified by competent authorities
• Tests done every 3 years, frequency can be adjusted by CAs
• Mutual recognition of TLPT results
• Use of external and internal testers (with safeguards)
### 4. Third party risk
(Articles 28-44)

<table>
<thead>
<tr>
<th>General principles</th>
<th>Harmonisation of key elements of relationship with ICT third-party service providers</th>
<th>Union Oversight framework for critical ICT third-party service providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Full responsibility of the financial entity</td>
<td>• Description of functions and services;</td>
<td>• Designation by the ESAs</td>
</tr>
<tr>
<td>• Strategy on ICT third-party risk</td>
<td>• Indication of the location / storage of data</td>
<td>• ESAs as Lead Overseers with powers to monitor &amp; issue recommendations</td>
</tr>
<tr>
<td>• Register of Information</td>
<td>• Assistance by the ICT third-party service provider</td>
<td>• Oversight Forum - cross-sectoral coordination on all ICT risk matter</td>
</tr>
<tr>
<td>• Preliminary assessment of concentration risk…</td>
<td>• Right to monitor and inspect…</td>
<td>and preparatory work for individual decisions and collective</td>
</tr>
</tbody>
</table>
<pre><code>                                                                               |                                                                               | recommendations                                                        |
                                                                               |                                                                               | • Joint Oversight Network – coordination between LOs                    |
</code></pre>
DORA – latest developments

**Level 1**
- Publication in the Official Journal in December 2022
- Entry into force 20 days after – applicable from 17 January 2025

**Level 2**
- ESAs to develop level 2 acts further specifying certain requirements (2024)
- Commission to propose delegated acts (criticality, oversight fees) based on ESA advice (2024)
Thank you

© European Union 2023

Unless otherwise noted the reuse of this presentation is authorised under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0) license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.

Slide xx: element concerned, source: e.g. Fotolia.com; Slide xx: element concerned, source: e.g. iStock.com