The Digital Operational Resilience Act - DORA

9 December 2020
Speakers

**Ben Regnard-Weinrabe**
Financial Services Regulation, Fintech and Payments
London
**Contact**
+44 20 3088 3207
ben.regnard-weinrabe@allenovery.com

**Dr Catherine Di Lorenzo**
Data and Technology
Luxembourg
**Contact**
+352 44 44 5 5129
Catherine.DiLorenzo@AllenOvery.com

**Nikki Johnstone**
Financial Services Regulation, Fintech and Payments
London
**Contact**
+44 20 3088 2325
Nikki.Johnstone@AllenOvery.com

**Tom Anderson**
Risk Management, A&O Consulting
London
**Contact**
+44 20 3088 6435
Tom.Anderson@AllenOvery.com

**Heenal Vasu**
Financial Services Regulation, Fintech and Payments
London
**Contact**
+44 20 3088 1447
Heenal.Vasu@AllenOvery.com
Housekeeping notes

- On joining the session your microphone will be muted and your video will be turned off
- To activate the Q&A function click The Q&A box will appear on the right hand panel
- To submit a question use the Q&A function sending your question to “All Panellists”
- You will not be able to enable your video or un-mute your microphone during the session
- If you experience any technical issues and cannot submit these via Q&A please call +44 203 088 7196 or +44 203 088 7450
The Digital Operational Resilience Act - DORA

Agenda

1. Key concepts and interactions with other texts
2. Scope
3. ICT risk management
4. ICT-related incident reporting
5. Digital operational resilience testing
6. Managing of ICT third-party risk

‘ICT services’ means digital and data services provided through the ICT systems to one or more internal or external users.
Introduction | Regulation on digital operational resilience for the financial sector (DORA)

Proposal (COM(2020) 595 final) - 24/09/2020

Adoption date / Entry into force - ?

Applicability (except Art. 23 and 24*) - 12 months after the date of entry into force

Applicability Art. 23 and 24 - 36 months after the date of entry into force

*Requirement for threat-led penetration testing for significant financial entities

Target date for implementation of Digital Finance Package is 2024
Key concepts and interactions with other texts
Main texts under the current legal framework

Payment Services Directive (EU) 2015/2366
MiFID II Delegated Regulation

EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02), EIOPA Guidelines on cloud outsourcing – The Outsourcing Guidelines
EBA Guidelines on the notification of major operational or security incidents (EBA/GL/2017/10) – The Notification Guidelines
## Concepts under the current legal framework

<table>
<thead>
<tr>
<th>Outsourcing / IT function / security</th>
<th>Outsourcing Guidelines</th>
<th>Credit Institutions and CRD investment firms, payment institutions and electronic money institutions</th>
<th>vs use of ICT third-party service provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud outsourcing</td>
<td>EIOPA Guidance on Cloud Outsourcing</td>
<td>EIOPA: insurance firms FCA: all FSMA firms not covered by EBA Outsourcing Guidelines</td>
<td>vs use of ICT third-party service provider</td>
</tr>
<tr>
<td>ICT and security risk management</td>
<td>ICT Guidelines</td>
<td>Credit institutions, CRD investment firms, payment institutions and electronic money institutions</td>
<td>vs ICT risk management</td>
</tr>
<tr>
<td>Operational or security incident</td>
<td>Notification Guidelines</td>
<td>Payment institutions</td>
<td>vs ICT-related incidents</td>
</tr>
</tbody>
</table>
Key concepts

- Digital operational resilience
- ICT services
- ICT risk
- ICT-related incident
- Critical ICT third-party service provider
- Critical or important function
- ICT third-party service provider
Scope
Financial entities* and ICT third-party service providers: an entire ecosystem is impacted

**Banking sector***
- Credit institutions
- Payment institutions
- E-money institutions
- Investment firms
- Crypto-asset actors (MICA Regulation)

**Markets actors***
- CSDs
- Central counterparties
- Trading venues
- Trade repositories
- Data reporting service provider

**Investment funds sector***
- AIFMs
- ManCos

**ICT third-party service providers**

**Miscellaneous***
- Credit rating agencies
- Statutory auditors/ audit firms
- Administrators of critical benchmarks
- Crowdfunding service providers (Crowdfunding Regulation)
- Securitisation repositories

**Insurance sector***
- Insurance and reinsurance undertakings
- Intermediaries
- Institutions for occupational retirement pensions
ICT risk management
ICT risk management framework

**Audit and supervision**
- Regular audits of framework
- Provision information on ICT risks to authorities

**Components**
- Strategies, policies, procedures, ICT protocols and tools
- Information security management system
- Digital resilience strategy

**Documentation and review of framework**
- Must be documented
- Must be reviewed at least once a year
- Must be continuously improved

**Segregation of duties**
- Segregation of ICT management functions vs control functions

A sound, comprehensive and well-documented ICT risk management framework
Specific functions in ICT risk management

- Communication
- Identification
- Protection & prevention
- Learning & evolving
- Response and recovery
- Detection

ICT risk management
Reporting of major ICT-related incidents to competent authority

Without delay
- No later than end of business day
- Except if incident later than 2 hours before end of business day
- Except if reporting channels not available

No later than 1 week after the initial notification
- Every time a relevant status update is available
- Upon specific request of competent authority

When the root cause analysis has been completed and when the actual impact figures are available to replace estimates
- BUT not later than one month from the initial report

Competent authority to provide feedback or guidance

Information to service users/clients and under other reporting regimes (e.g., NIS, GDPR) may be necessary in addition to the above reporting

Where the incident has or may have an impact on the financial interests of service users and clients, information without undue delay about the major ICT-related incident and information, as soon as possible, on all measures which have been taken to mitigate the adverse effects of such incident
Digital operational resilience testing
**General requirements: testing of ICT tools and systems for all financial entities**

ICT risk management framework must include a sound and comprehensive digital operational resilience testing programme (DORTP), in consideration of proportionality principle

DORTP to include range of assessments, tests, methodologies, practices and tools
Procedures and policies to prioritise, classify and remedy issues and ensure all are fully addressed

DORTP to be conducted on a risk-based approach

Lists of appropriate tests to be executed in article 22 DORA

Additional threat-led penetration testing for significant financial entities article 23 DORA

At least yearly testing of all critical ICT systems and applications

Tests undertaken by (internal or external) independent parties
Managing of ICT third-party risk
General principles

Financial entities shall manage **ICT third-party risk** as an **integral component of ICT risk**

Remain fully responsible for the discharge of their obligations

New elements

- Strategy on ICT third-party risk
- Yearly reporting to authorities re. use of ICT services

Management of ICT third party risk using **proportionality principle**

- **Adoption and regular review of a strategy on ICT third-party risk**
- **Register of Information** in relation to all contractual arrangements on the use of ICT third-party services
Entering into a contractual arrangement

1. Critical or important functions

2. Supervisory conditions

3. Risk identification and assessment (including concentration, sub-outsourcing and third-country risk)

4. Due diligence on third-party service provider

5. Conflicts of interest

6. Conclusion of contract

7. Monitoring of risks and third-party service provider

8. Termination and exit plan

Not possible to use of an ICT third-party service provider established in a third country that would be designated as critical if it was established in the Union
Managing of ICT third-party risk

**Documentation**

- Termination rights and exit strategies
- Description of functions and services (incl. conditions for sub-contracting)
- Locations of functions and services and of data processed
- Accessibility, availability, integrity, security and protection of personal data and on ensuring access, recover and return of data
- Monitoring rights by financial entity and cooperation with authorities
- BCPs and ICT security measures, etc.
- Notice periods and reporting obligations and assistance obligation of the third-party service provider
- Full service level descriptions

Single written document (incl. SLAs)
Managing of ICT third-party risk

Oversight framework of critical ICT third-party service providers

Step 1
- Designation of critical ICT third-party service providers by the ESAs – List yearly updated
- Criteria include
  - systemic impact of services
  - systemic importance of beneficiaries of services
  - critical or important functions, substitutability
  - number of Member States involved

Step 2
- Appoint either EBA, ESMA or EIOPA as Lead Overseer
- Mission: assess whether each critical ICT third-party service provider has in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risks which it may pose to financial entities

Step 3
- Supervision by the Lead Overseer: recommendations, right to information, inspection and investigation
- Competent authorities may require financial entities to temporarily suspend the use or deployment of a service provided by a critical ICT third-party provider until the risks identified in a recommendation addressed to it by the Lead Overseer have been addressed, or even to terminate the relevant contractual arrangements
Key takeaways

1. Uplift will vary between sectors – eg banking sector entities may be more familiar with the requirements than AIFMs

2. ICT third-party service providers may now be regulated entities

3. Even if not regulated, ICT third-party service providers may need to adapt their contracting, service provision and pricing to reflect the obligations of their clients

4. Preparation:
   - Undertake a GAP analysis early to give time for any compliance build-out
   - Specific to business, strategy, financial plan and current regulatory framework
   - Look at processes, policies and procedures that you may have to adapt
   - Allocate budget and workforce – focus on people competences
   - Don’t underestimate the complexity of implementation
Questions?

These are presentation slides only. This document is for general guidance only and does not constitute advice.

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. Allen & Overy LLP is a limited liability partnership registered in England and Wales with registered number OC306763. Allen & Overy (Holdings) Limited is a limited company registered in England and Wales with registered number 07462870. Allen & Overy LLP and Allen & Overy (Holdings) Limited are authorised and regulated by the Solicitors Regulation Authority of England and Wales.

The term partner is used to refer to a member of Allen & Overy LLP or a director of Allen & Overy (Holdings) Limited or, in either case, an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP’s affiliated undertakings. A list of the members of Allen & Overy LLP and of the non-members who are designated as partners, and a list of the directors of Allen & Overy (Holdings) Limited, is open to inspection at our registered office at One Bishops Square, London E1 6AD.

Allen & Overy is an international legal practice with approximately 5,500 people, including some 550 partners, working in more than 40 offices worldwide. A current list of Allen & Overy offices is available at allenovery.com/global/global_coverage.

© Allen & Overy LLP 2020