D O R A

Digital Operational Resilience Act

First Council Working Party

Banking and finance

30/09/2020

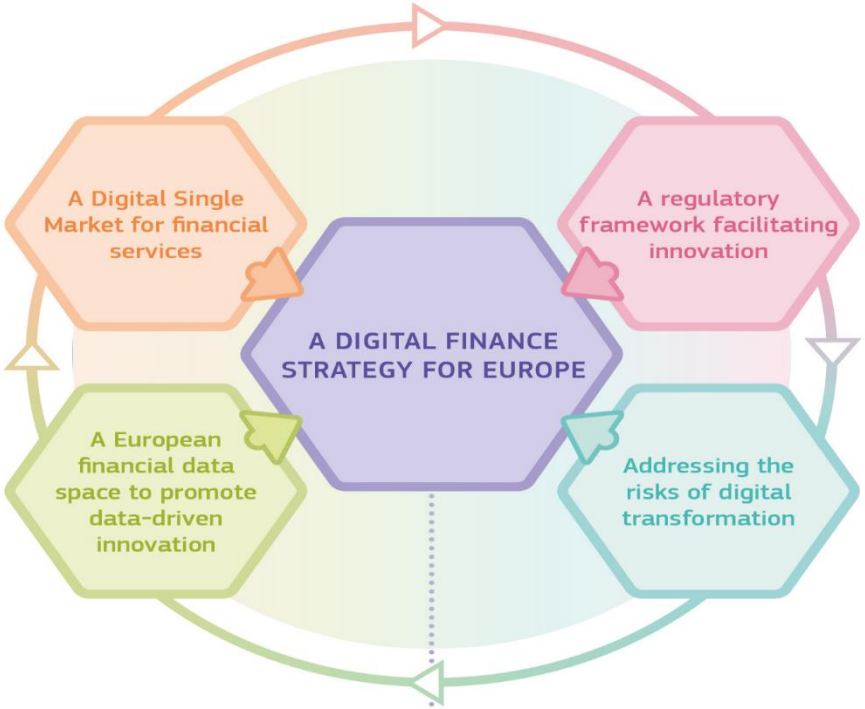
Update

Digital Finance Package

24 September

Proposal for a Regulation on the digital operational resilience of the financial sector (DORA) accompanied by a Directive

European Commission



THE BENEFITS OF DIGITAL FINANCE

Better financial products for consumers and new ways of channelling funding to EU businesses, in particular SMEs.

Supports Europe's economic recovery strategy and opens up new channels to mobilise funding to support the Green Deal and the New Industrial Strategy for Europe.

Cross-border digital finance will enhance financial market integration in the Banking Union and the Capital Markets Union.

Strengthen Europe's ability to retain and reinforce our open strategic autonomy in financial services.

European Commission

Mitigating risks of digital transformation by strict and common rules on digital operational resilience

During the pandemic, cyberattacks on financial institutions have risen by 38%.

- All financial entities will be subject to operational resilience requirements to ensure a safe financial system across sectors and avoid a domino reaction.
- Critical ICT third-party providers (e.g. cloud computing services) will be subject to oversight to ensure they do not pose undue operational risks for finance.

Background

2018 Fintech Action Plan

2019 ESAs joint technical advice

Internal work streams and international work (e.g. BCBS, G7, FSB, etc.)

December 2019 – roadmap and public consultation

Public consultation feedback

99 responses

Wide support for a comprehensive framework based on four building blocks:

- ICT risk management framework based on key common principles
- Reporting of major incidents using uniform criteria, templates, mechanisms and to a single authority
- Voluntary sharing of threat intelligence could be extended to other sectors
- Test, regularly update and review ICT systems and tools to withstand ICT disruptions and to assure operational resilience
- Manage third party risk via outsourcing rules and an EU direct oversight framework
- Carefully explain and address the interaction with the NIS Directive

Member States consultations

Expert Group on Banking, Payments and Insurance (EGBPI)

18 May 2020

16 July 2020

Impact assessment

	ICT risk management	Reporting and threat intelligence	Testing	ICT third party risk
"Do nothing" scenario	Status-quo for EU financial services rules + NIS Directive	Status-quo for EU financial services rules + NIS Directive Voluntary threat intel	Based on national rules	Status-quo on outsourcing based on ESAs guidelines (indirect supervision)
Option 1	Capital buffer + NIS Directive	Same as "do nothing"	EU – wide resilience stress tests	Capital buffer
Option 2	Comprehensive EU rules in financial services legislation + NIS Directive	Comprehensive EU rules in financial services legislation + NIS Directive Voluntary threat intel	Comprehensive EU rules on digital operational resilience testing + mutual recognition of testing results	EU oversight framework
Option 3	Comprehensive EU rules in financial services legislation + out of NIS completely	Comprehensive EU rules in financial services legislation + out of NIS completely Compulsory threat intel	Comprehensive EU rules on digital operational resilience testing + cross-authority testing under ESAs coordination	New EU Authority (direct supervision)

Option 2 (preferred option)

ICT risk management	• ICT governance and risk management framework – principle and risk based applicable to all financial entities
Incident reporting and information sharing	• Enhanced and extended reporting of ICT-related incidents to those sectors currently not covered by EU rules • Streamlined reporting with common reporting templates, deadlines, one competent authority to report to, etc. • Promote/support voluntary schemes on threat intelligence sharing between financial institutions.

Option 2 (preferred option)

Digital operational resilience testing	• Basic testing – all financial entities • Advanced testing – only significant financial entities • Testing results – shared with and recognised by competent authorities across the Member States
ICT third party risk	• Indirect supervision – heightened outsourcing rules and oversight tools for supervisors • Direct oversight of critical ICT third party service providers

Legislative package

Regulation

- Further harmonisation & streamlining existing (limited) rules on ICT risk management and ICT-related incident reporting
- New bespoke rules on digital testing, information sharing and management of ICT third-party risk, including an Oversight framework to monitor digital risk of critical ICT third party service providers

Directive

- Amendments to financial services directives to introduce cross-references to the Regulation and update empowerments for technical standards

Regulation

Scope (Article 2)

- 20 types of regulated Union financial entities
- out of scope: payment systems, card payment schemes, some system operators and participants under SFD, the Union registry for emission allowances

Proportionality

- exemptions (lighter regime for microenterprises)
- tailored rules for certain categories (advanced digital testing only for *significant* financial entities)
- tailored rules for certain aspects (ICT-related incident reporting only for *major* ICT-related incidents)

ICT governance
(Article 4)

Definition, approval, control and accountability to implement arrangements that give effect to the ICT risk management framework

Approval, controls, review processes to implement ICT business continuity and disaster recovery plans, ICT audit plans and ICT third-party risk

Full responsibility and accountability of the management body

Clear roles and responsibilities for all ICT-related functions

Setting ICT risk tolerance levels

Appropriate allocation of ICT investments

Regular ICT training for the management body

ICT risk management requirements

(Articles 5 to 14)

Identify
(Article 7)

Business functions	Supporting information assets	ICT system configurations	Interconnections with internal and external systems
Sources of ICT risk	All ICT systems accounts	Network resources and hardware equipment	Critical physical equipment
All processes dependent on and interconnections with ICT third-party service providers	**Proportionality for microenterprises:** **-** no risk assessment upon major changes in the network and information system infrastructure - no specific ICT risk assessment on all legacy ICT systems.		

Protect and Prevent

(Article 8)

Resilience, continuity and availability of ICT systems &
Security, confidentiality and integrity of data

Continuous monitoring and control of ICT systems and tools
Minimise risk

Risk based approach

Information security policy

limit physical and virtual access to ICT systems	protocols on strong authentication	change management	patching / updates

Detect
(Article 9)

Prompt detection of anomalous activities

Multiple layers of control

Identification of single points of failure

Devote resources and capabilities

Respond & Recover

(Articles 10 and 11)

ICT Business Continuity Policy

ICT Disaster Recovery Plans

- Resume activities and limit damage

Back-up policies

Recovery methods

Flexible RTOs

Proportionality for microenterprises

- no audit ICT Disaster Recovery Plans
- no test scenarios of cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities
- no crisis management function
- no reporting to competent authorities of all costs and losses caused by ICT disruptions and ICT-related incidents

Learn and Evolve
(Article 12)

- Information gathering on vulnerabilities and cyber threats
- Post-incident reviews after significant ICT disruptions
- Analysis of causes of disruptions
- Reporting to the management body
- ICT security awareness programs and trainings

Communicate
(Article 13)

Communication plans to clients, counterparts and the public

At least one person to implement the communication strategy for ICT-related incidents

ICT-related incident reporting

(Articles 15 to 20)

General requirements	• Establish and implement a management process to monitor and log ICT-related incidents • Classify ICT-related incidents based on criteria detailed in the regulation and further developed by the ESAs
Reporting of *major* ICT-related incidents to competent authorities	• Common templates and harmonised procedures developed by the ESAs • Initial, intermediate and final reports • Obligation to inform users and clients where impact on their financial interests • Competent authorities to provide details of the incidents to other institutions or authorities: ESAs, ECB and single points of contact designated under the NIS Directive

Digital operational resilience testing

(Articles 21 to 24)

Basic testing	• All financial entities
Advanced testing	• Only financial entities identified as *significant* by competent authorities (based on criteria in this regulation and further developed by the ESAs) • Advanced testing based on TLPTs • Mutual recognition of TLPT results

ICT third-party risk

(Articles 25 to 39)

Harmonisation of key elements of relationships with ICT third-party service providers	• Minimum crucial aspects for a complete monitoring of ICT third-party risk in the conclusion, performance, termination and post-contractual stages of contractual arrangements
Union oversight framework for critical ICT third-party service providers	• Designation of critical ICT third-party service provider by the ESAs • ESAs as Lead Overseers with powers to monitor • Oversight Forum ensures cross-sectoral coordination in relation to all maters on ICT risk and carries out preparatory work for individual decisions and collective recommendations

Contractual arrangements

(Articles 25-27)

General principles

- Financial entities' full responsibility
- Proportionality
- ICT third party risk strategy
- Documentation and evidence
- Register of Information
- Pre, during and post contractual principles

Preliminary assessment of ICT concentration risk

Key contractual provisions

- Description of all functions and services, service level
- Indication of location and storage of data
- Accessibility, availability, integrity, security and protection of personal data
- Full service descriptions
- Notice periods and reporting obligations of the third party provider
- Assistance by the third party provider
- Right to monitor
- Termination and exit strategies

Oversight framework

(Article 28) Designation of critical ICT third-party providers (CTPPs) by the ESAs

1. ICT third-party provider's failure would trigger systemic impact

(stability, continuity or quality of the provision of financial services)

- number of financial entities to which the respective ICT third-party service provider delivers services

2. Systemic character (or importance) of the financial entities themselves

- number of G-SIIs / O-SIIs relying on the respective ICT third-party service provider
- interdependence between G-SIIs or O-SIIs

3. Services (supporting critical or important functions) ultimately involve the same ICT third-party service provider

(directly or indirectly)

4. Degree of substitutability of the ICT third-party service provider

- Lack of real alternatives (even partial)
  - limited number of providers
  - market share
  - technical complexity
- Difficulties to partially or fully migrate data and workloads to another ICT third-party service provider due to costs or risks

5. Number of Member States in which the relevant ICT third-party service provider provides services

6. Number of Member States in which financial entities using the relevant ICT third-party service provider are operating

European Commission

Oversight framework
(Article 28) continuation

EXEMPTION

Designation does not apply to ICT third-party service providers subject to oversight frameworks established for the purposes of supporting Treaty objectives referred to in Article 127(2) TFEU

VOLUNTARY OPT-IN

ICT third-party service providers not included may request to be subject to the Framework

LEAD OVERSEER

One ESA is appointed as Lead Overseer for each critical ICT third-party provider

(based on the value of assets of financial entities in the remit of the respective ESA)

Oversight framework

(Articles 29 and 35) Role of Oversight Forum

Oversight Forum

Cross-sector coordination on ICT third party risk	• Oversight Forum prepares draft joint positions and common acts of the Joint Committee
Ex-ante (oversight activities)	• Lead Overseer consults the Oversight Forum before exercising powers and before addressing recommendations to the CTPPs
Ex - post (collective recommendations)	• Fosters best practices on ICT concentration risk and explores mitigants for cross-sector risk transfers •Submits comprehensive benchmarks of critical ICT third-party service providers to be adopted by the Joint Committee

Oversight framework

(Articles 29) Structure of the Oversight Forum

Joint Committee ->Sub Committee
Oversight Forum

- Chairpersons of the ESAs
- One high-level representative from each relevant national competent authority
- Observers: Executive Director of each ESA, one representative from the Commission, the ESRB, ECB and ENISA

Oversight framework

(Articles 30 – 39 Tasks, powers, conduct)

Tasks	•ICT requirements and related physical security, overall risk management processes and related governance arrangements, handling of ICT incidents •data portability insofar allowing an effective termination •ICT testing processes •Use of national and international standards
Powers to monitor	•Request all relevant information and documentation •Conduct general investigations and inspections •Request reports •Address recommendations
Periodic penalties	• non submission of documents, refusal to grant accesses and submit to inspections etc.
Conduct	• Lead Overseers assisted by national experts in the examination teams • NCAs will ensure follow-up and enforcement
International cooperation	

Information sharing
(Article 40)

Voluntary exchange amongst financial entities of cyber threat information and intelligence in trusted communities

indicators of compromise	tactics	techniques	procedures	cyber security alerts	configuration tools

Competent authorities
(Articles 41-49)

- Cooperation with NIS structures and authorities
- Cross-sector exercises, communication and cooperation
- Administrative penalties and remedial measures
- Professional secrecy

Amendments

(Articles 52-55 and Directive)

Necessary updates in the current operational risk or risk management requirements in subsector financial legislation to ensure full consistency with the DORA proposal

- Regulation (EC) No 1060/2009 (CRAR)
- Regulation (EU) No 648/2012 (EMIR)
- Regulation (EU) No 600/2014 (MiFIR)
- Regulation (EU) No 909/2014 (CSDR)
- Directive 2006/43/EC (Audit)
- Directive 2009/65/EC (UCITS)
- Directive 2009/138/EU (Solvency II)
- Directive 2011/61/EU (AIFMD)
- Directive EU/2013/36 (CRD IV)
- Directive 2014/65/EU (MiFID II)
- Directive(EU) 2015/2366 (PSD II)
- Directive EU/2016/2341 (IORPs)

Next steps

Council	• refer to information by PCY
European Parliament	• own-initiative report on digital finance on 5 October