Digital Operational Resilience

Digital Operational Resilience Act (DORA)

Presenter: **Michiel Kuhlmann**
Date: 22 September 2022

eiopa
European Insurance and Occupational Pensions Authority

Image: AdobeStock

CONTENT

Introduction

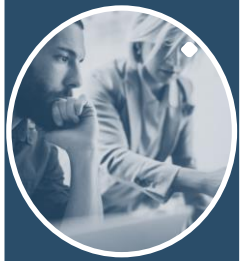
ICT risk management

ICT 3rd party risk management

Digital operational resilience testing

ICT-related incidents

Information sharing

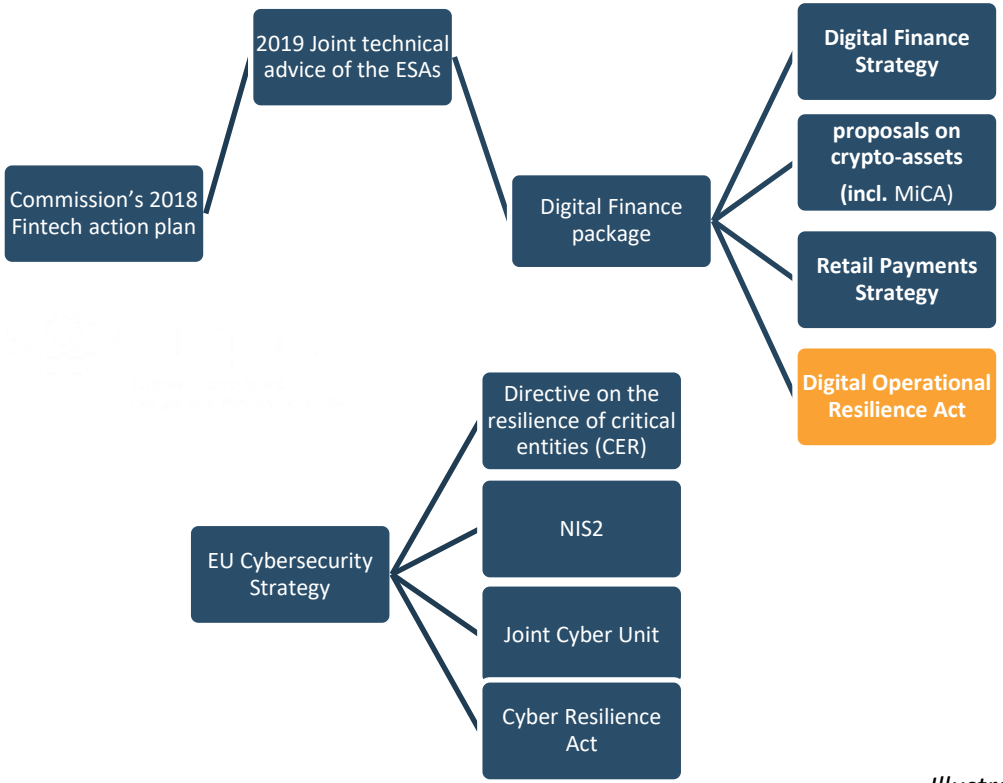


CTPPs oversight

INTRODUCTION

A Europe Fit for the Digital Age

Image: AdobeStock



Illustrative

INTRODUCTION

The Digital Operational Resilience Act (DORA) will strengthen the cyber resilience component of the European financial rulebook.

"…means the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly, through the use of services of ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality throughout disruptions;" (art 3 (1), DORA proposal)

<<This presentation is a simplification of the proposed legal framework and does not capture all aspects or nuances.>>

INTRODUCTION

*Table 7 – Mapping of existing (qualitative) provisions on digital operational resilience in the EU financial services L1 and L2 legislation**

Building block	Main elements of the buiding block	EU financial services Level 1 and Level 2 legislation												
		Payments (PSD2)	Banks (CRD/CRR)	Investment firms (MIFID)	Trading Venues (MIFID)	CCPs (EMIR)	CSDs (CSDR)	Trade Repositories (EMIR)	Insurance (Solvency II)	Asset Management (UCITS/AIFMD)	CRAs	Data Reporting Service Providers (DRSPs)	Audit	IORPs
ICT risk management	Arrangmenents (policies, procedures and systems) on risks to which the entity is exposed to		art. 74(1)	art. 16(4), (5)	art. 47 (1)	art. 26(1)	L2 - art.48(1)	Art 79		L2 - art. 40(1) - both art. 15(2) - A	Annex I - Section A, (4)			art. 28(3)
	Operational risk framework / policy	art. 95(1)				**Art. 28 (risk committee)**	L2 - art. 70(1)			L2 - art. 13(1) - A				
	Risk management policy			L2 - art. 23(1)		L2 art.4			art. 41(3)	L2 - art. 38(1) - U				art. 25(1)
	Information security framework/strategy	art. 95(1)		L2 - art. 18 (AT)		L2 - art. 9(3)	L2 - art. 70(9), art. 75(9)							
	Appropriate IT tools, reliable, resilient and secure systems (to ensure security / integrity / confidentiality)	art. 95(1), art. 97(3) L2 - chapter II,IV,V		art. 16(5) L2 - art. 21(2)	art. 48(1) L2 - art. 23(1),(2)	art. 26(6) and L2 art.9	art. 45(1) L2 - art. 75	L2 - art. 79(1)	L2 - art. 258(1)	L2 - art. 57(2) - A		art. 64 (4), 65(5), 66(3) - L2 - art. 9(1)		
	Business continuity policy		art. 85(2)	art. 17 (1) and L2 - art. 14(1) - (AT) L2 - art. 21(3)	art. 48(1)	art. 34(1) L2 - art. 17	L2 - art. 76(1)	art. 79(2)	L2 - art. 258(3)	L2 - art. 57(3) - A	L2 - art. 11 (2)		art. 24a 1(h)	art. 21(5)
	Contingency plans		art. 85(2)		art. 47(1)	part of BCP as referred to in art. 34			art. 41(4)					art. 21(5)
	Crisis management and communications					L2 - art. 22	L2 - art. 78(4)							
	Disaster recovery plan					art. 34(1) L2 - art. 19	L2 - art. 76(1), art. 78	art. 79(2)						
	2h RTO				L2 - art. 15(2)	L2 - art. 17(6)	L2 - art. 78(2)							
Incident reporting	Reporting of operational incidents to CAs	art. 96(1)			L2 - art. 23(3) L2 - art. 81(1)		art. 45(6) L2 - art. 41(h)							
	Procedures to record, monitor and resolve operational incidents						L2 - art. 71(4)						art. 24a 1(i)	
	Breaches in physical and electronic security measures	art. 96(1)		L2 - art. 18(3) (AT)								L2 - art. 9(4)		
Testing	Testing of IT tools, systems and procedures	L2 - art. 3(1)				**partly relevant by general provisions art. 49**	art. 45(5) L2 - art. 75(6)							
	Penetration testing			L2 - art. 18(4) (AT)										
Third party risk	Outsourcing - the entity remains fully responsible	art. 19(6) art. 20(2)		L2 - art. 4(1) (AT) L2 - art. 31(1)	L2 - art. 6(1)	art. 35(1)	art. 30(1)		art. 49(1)			L2 - art. 6(4)		art. 31(2)
	Outsourcing is governed by a written agreement			L2 - art. 31(3)	L2 - art. 6(4)		art. 30(2)	L2 - art.16			L2 - art. 25			art. 31(5)
	Outsourcing - report to CAs on the outsourcing	art. 19(6)			L2 - art. 6(5), (7)	art. 35 approval by CA required			art. 49(3)	art. 20(1) - A				art. 31(6)
	Identify critical service providers (CSPs) and manage dependencies					L2 - art. 18(3)	L2 - art. 68(1), (2)							
	Inform CAs on dependencies with CSPs						L2 - art. 68(5)					L2 - art. 6(6)		
	Robust arrangements for the selection and substitution of IT third party service providers						L2 - art. 75(9)							
	Due diligence when outsourcing to third party service providers			L2 - art. 31(2)										
	Outsourcing to third party service providers located in a third country			L2 - art. 32										

** The different elements of the building blocks (column 2) are illustrative and non-comprehensive. Legend: white= provisions missing in the EU financial services legislation; green cells = provisions exist in the EU financial services legislation; L2 = level 2 legislation.*

INTRODUCTION

About:

- Regulation status
- Interaction with other legal acts (e.g. NIS directive)
- Exemptions & proportionality (size, complexity, risk profile …)
- Administrative penalties and remedial measures by CA

Scope:

✓ (re)insurance undertakings
≠ art 4 SII

✓ (re) insurance intermediaries
≠ Microenterprises, SME

✓ IORPS
> 15 members

✓ ICT third party service providers

✓ …

Timeline:

- Date of entering into force:
  Q1 2023 (expectation)
- Date of application:
  + 24 months
- Various ITS/RTS DL - Draft
  +12 months
  +18 months
  +24 months

INTRODUCTION

ICT risk management	ICT 3rd party risk management	Digital operational resilience testing	ICT-related incidents	Information Sharing	CTPP oversight
▪ Principles and requirements on ICT risk management framework	▪ Monitoring third-party risk providers ▪ Key contractual provisions	▪ Basic testing ▪ Advanced testing	▪ General requirements ▪ Reporting of major ICT-related incidents to competent authorities	▪ Exchange of information and intelligence on cyber threats	▪ Oversight framework for critical ICT TPPs

ICT RISK MANAGEMENT

Strong & Effective

Image: AdobeStock

New rules:

- ICT systems, protocols and tools
- Risk Management
  - **ICT Risk management framework**
    - Strategies, policies, procedures, protocols and tools
    - Digital operational **resilience strategy**
      - Supports business strategy & objectives
      - Risk tolerance limits
      - Incident detection, protection and prevention
      - Implementing digital operational resilience testing
- Governance
  - Governance and control framework management
  - **Role for AMSB** - define, approve, oversee and accountable for the implementation of ICT risk management framework

To be further specified:

- ICT security policies, procedures, protocols and tools
- Protect & Prevent, Detect, Respond & Recover

MANAGEMENT OF ICT 3RD PARTY RISK

Strengthen & Adapt

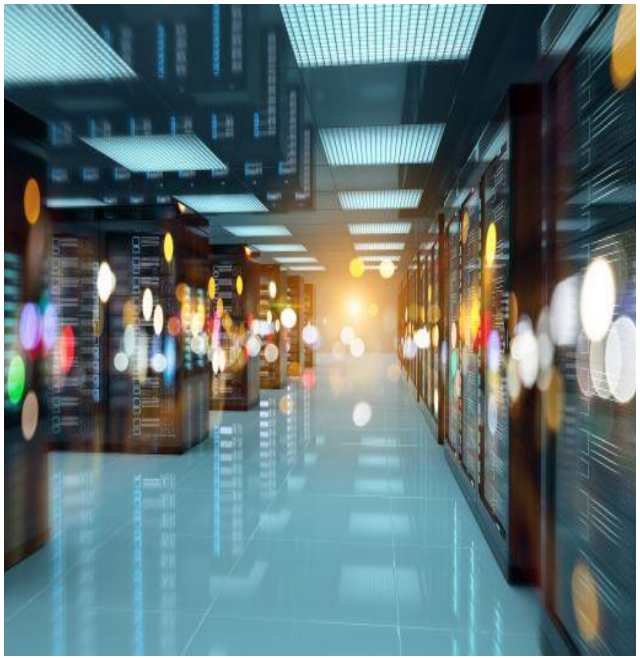


Image: AdobeStock

New rules:

- General principles
  - Adopt **a strategy** on ICT third-party risk (incl policy on the use of TP ICT for critical/important functions)
  - **Register of Information** on all contractual arrangements
  - Monitoring of ICT third-party risk
  - Criteria (entering) contractual arrangement

- Key contractual provisions
  - **Minimum** (description, conditions subcontracting for critical or important function, location etc.)
  - **For critical/important functions** (TLPT, unrestricted rights of access, exit strategies etc.)

To be further specified:

- Templates for the purposes of the register of information
- The content of the policy regarding critical/important functions
- The elements to be taken into account when subcontracting critical or important functions

DIGITAL OPERATIONAL RESILIENCE TESTING

Fix overlaps & Recognition

Image: AdobeStock

New rules:

- General requirements
  - **Digital operational resilience testing programme**
    - Testing of ICT tools and systems

- Advanced testing of ICT tools, systems and process using TLPT
  - Only for financial entities **identified as significant** by CA
  - **Identify** all (incl. outsourced) relevant underlying ICT processes, systems and technologies supporting critical or important functions and ICT services
  - **Threat led penetration testing** (internal or external testers)
  - Every 3 years (but CA can request to reduce or extend)
  - **Pooling and mutual recognition** of TLPT Results

To be further specified:

- The criteria for significance
- Rules on use internal testers
- Scope of TLPT testing and testing methodology

ICT INCIDENT REPORTING

Streamline & Awareness

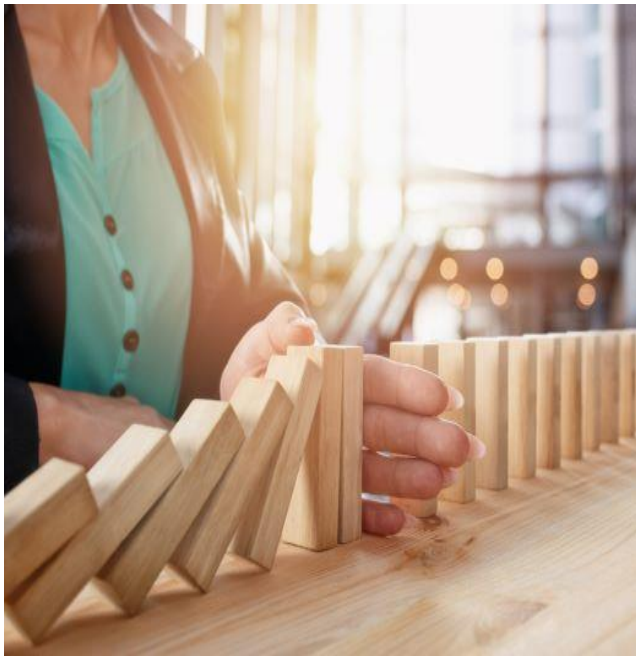


Image: AdobeStock

New rules:

- General requirements
  - An **incident management** process to detect, monitor and log ICT-related incidents
  - **Record** all ICT-related incidents and significant cyber threats
  - Appropriate procedures and processes to **monitor, handling and follow-up** of ICT-related incidents
  - **Classification** of ICT-related incidents and cyber threats
- Major ICT-related incidents & threats
  - Incidents - **Reporting** to CA (initial notification, intermediate & final report) & possibly clients
  - Threats - voluntary to CA

To be further specified:

- Criteria to determine materiality incidents and threats
- Templates, procedures for reporting major incidents & threats
- Time limits for initial notification & reports

INFORMATION-SHARING ARRANGEMENTS

Leveraging on knowledge

Image: AdobeStock

New rules:

- Financial entities may **exchange** amongst themselves cyber threat information and intelligence:
  - Indicators of compromise
  - Tactics, techniques, and procedures
  - Cyber security alerts
  - Configuration tools

- However:
  - within **trusted communities** of financial entities
  - protect the potentially sensitive nature
  - **notify CA** when participating.

CTPPS OVERSIGHT

Systemic & Awareness

Image: AdobeStock

New rules:

- Union Oversight framework for critical ICT third-party service providers

  Only for those **designated by the ESAs**, not if part of financial entity or intra group or no cross border.
  - ESAs as Lead Overseers with powers to **monitor** the ICT Risk that the CTPPs may pose to financial entities.
  - Lead Overseer shall assess them and can issue **recommendations** (after consulting the Oversight Forum).
  - Possibility to impose a periodic penalty payment up to 1% of the average daily worldwide turnover.
  - CA shall inform relevant financial entities of the risks identified in the recommendations addressed to CTPPs.
  - CA may request as measure as last resort to suspend use of service or terminate contractual arrangement.

ONGOING WORK & KEY TAKEAWAYS

Fit for the Digital Age

Image: AdobeStock

DORA

ICT risk management	ICT 3rd party risk management & CTPP oversight	Digital operational resilience testing	ICT-related incidents	Information Sharing	ICT 3rd party risk management & CTPP oversight
▪ Principles and requirements on ICT risk management framework	▪ Monitoring third-party risk providers ▪ Key contractual provisions	▪ Basic testing ▪ Advanced testing	▪ General requirements ▪ Reporting of major ICT-related incidents to competent authorities	▪ Exchange of information and intelligence on cyber threats	▪ Oversight framework for critical ICT TPPs

What's next

- ✓ Awaiting final approval DORA
- ✓ Setting up the work in cross sectoral environment (ESAs and NCAs)
- ✓ Upcoming industry workshops and public consultations

THANK YOU!

For more information visit:
https://www.eiopa.europa.eu

eiopa
European Insurance and
Occupational Pensions Authority

Image: AdobeStock