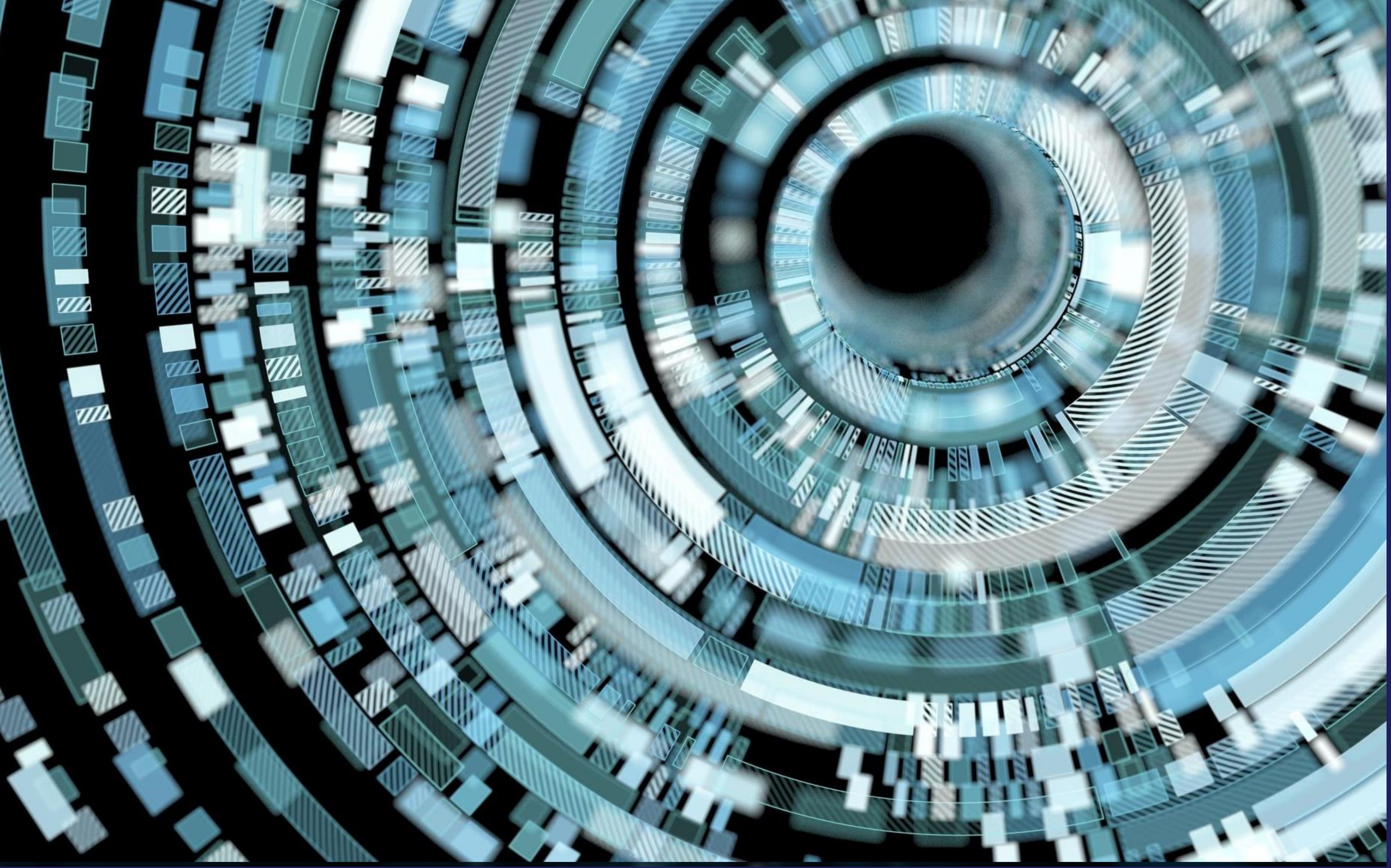


DORA and the changing regulatory landscape of cybersecurity requirements for crypto and financial institutions

SORAINEN

Mihkel Miidla, Partner, Sorainen (Estonia**)**

Agneta Rumpa, Senior Associate,
Sorainen (Latvia)

13.06.2024.

Cybersecurity –

EU regulatory landscape

Purposes of the legal acts

- Counteracting the increasing cyber threats
- Protecting Critical Infrastructure
- Safeguarding personal data
- Digital Single Market
- Enhancing trust
- Regulating emerging technologies
- Improving international cooperation
- Creating framework for incident response

- EU cybersecurity legislation aims to create a secure, resilient, and trustworthy digital environment essential for modern society and economic stability.

Cybersecurity –

EU regulatory landscape

The legal acts

- **GDPR*** *(applicable from 2018)*
- **NIS2 Directive** *(to be implemented by Oct 2024)*
- **CER Directice** *(to be implemented by Oct 2024)*
- **CRA** (Cyber Resilience Act) *(not yet adopted)*
- **DORA** *(applicable from 17 Jan 2025)*
- **EU Cybersecurity Act** (effective from 2019; amendment in 2024?)
- **Cyber Solidarity Act** (not yet adopted)
- +Other relevant acts like the Data Act, AI Act, DSA
- +Sector based legal acts & other instruments, standards

- *Expanding scope (more sectors in scope)*
- *Expanding extraterritorial effect*

Cybersecurity –

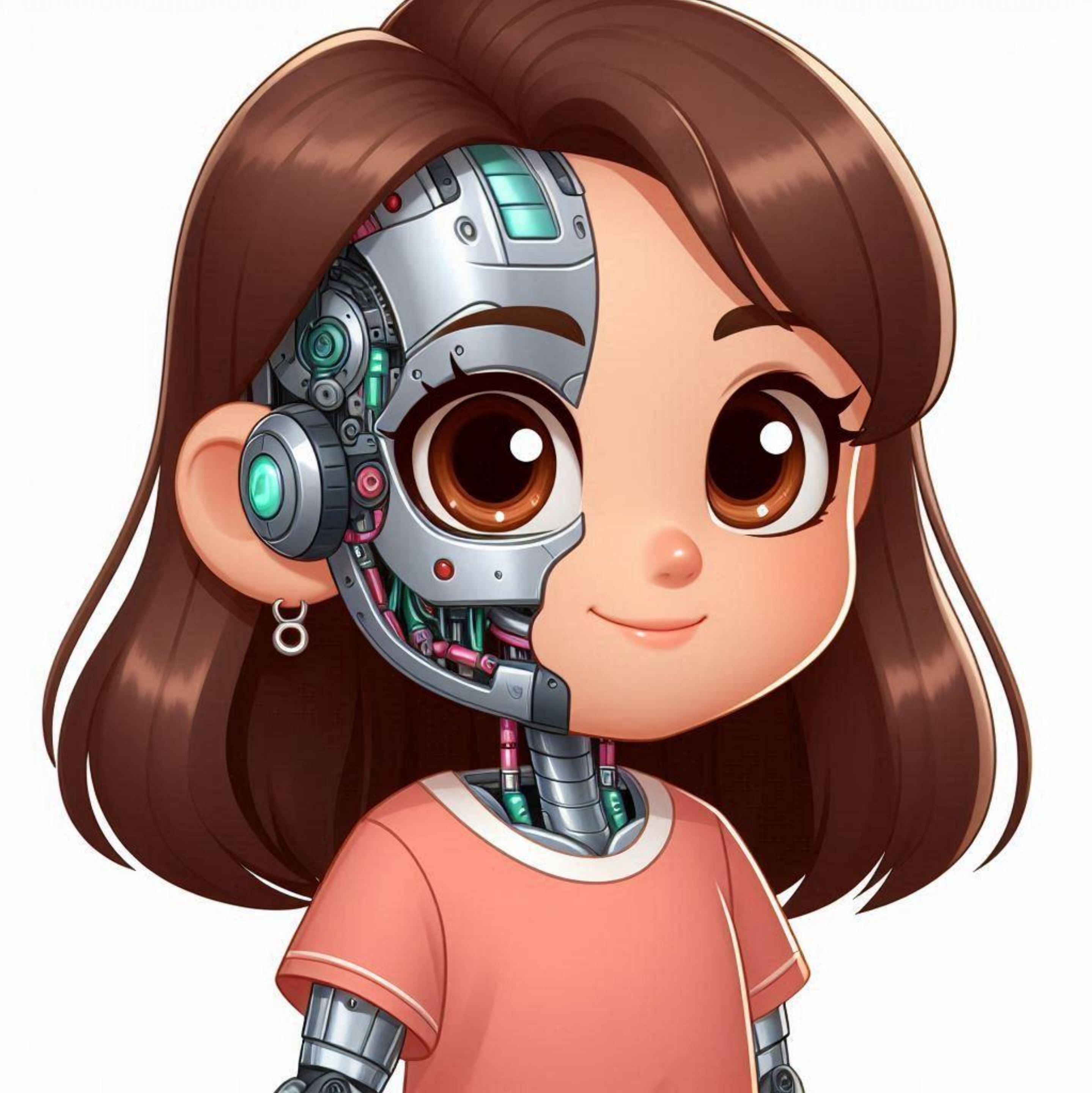
EU regulatory landscape

The legal uncertaintes. Overlapping and conflicting requirements.

- DORA vs GDPR
  - Effective in parallel. No derogations in DORA
- DORA vs NIS2
  - DORA is *lex specialis*
- *Cybersecurity Act and certifications*
- <u>Challenge:</u> Navigating the regulatory complexity and avoiding siloed approach.

How DORA changes the game for FIs,incl. CASPs

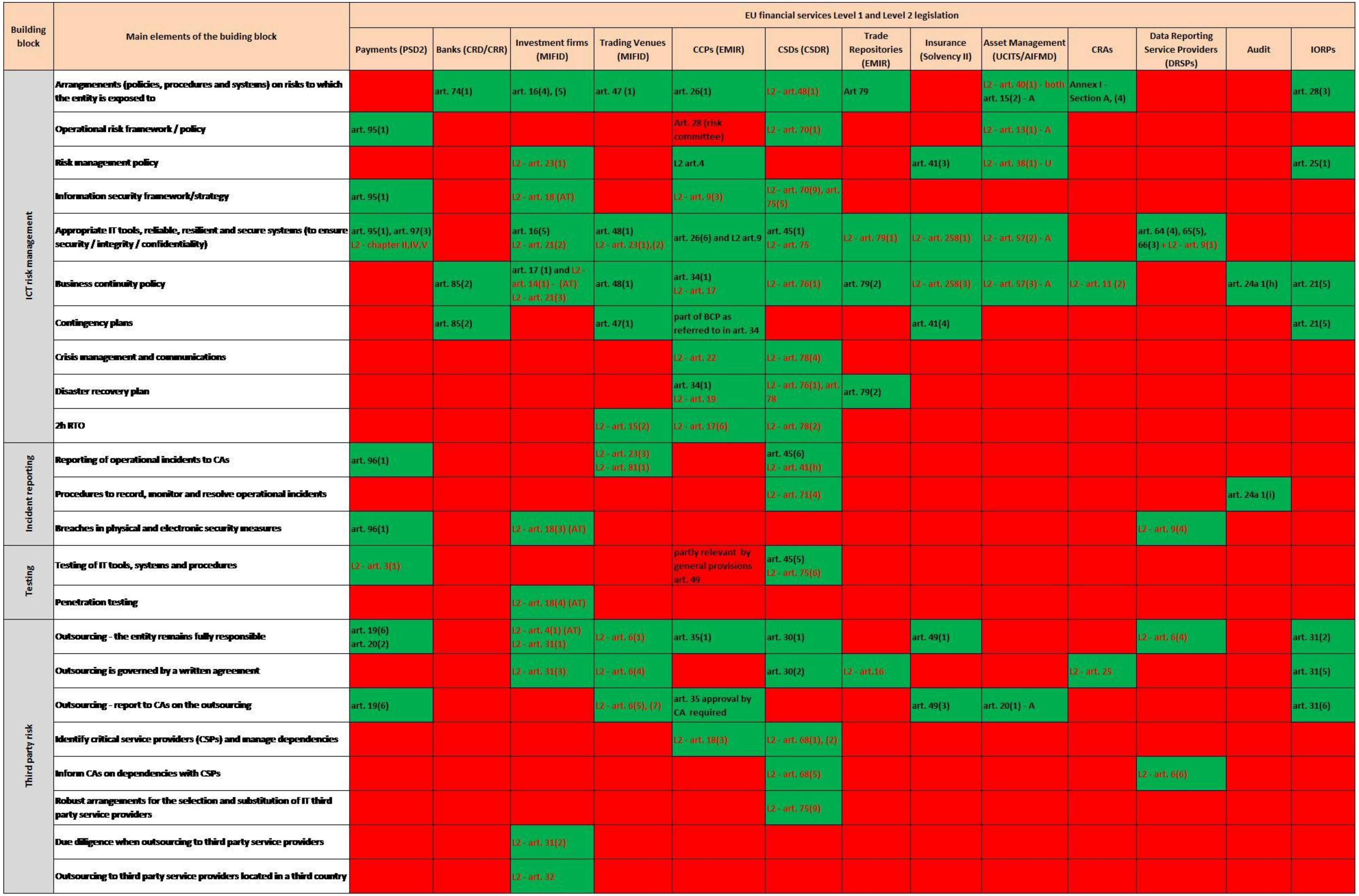
- Digital Operational Resilience Act (Regulation (EU) 2022/2554 + Directive (EU) 2022/2556)
- **Digital operational resilience**: ability to ensure operational integrity and reliability, directly or via ICT third-party service providers



Scope

- **Most financial institutions**
  - Banks
  - payment institutions
  - account information service providers
  - electronic money institutions
  - **CRYPTO ASSETS SERVICE PROVIDERS, ISSUERS OF ASSET-REFERENCED TOKENS**
  - crowdfunding service providers

  and many more....
- **ICT provider**s to said FIs:
  - critical ones
  - others



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(5)	🟥	🟥	🟥	🟥	🟥	🟥	🟥
	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	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

Commission impact assessment on DORA

Timeline

- In force as of 16.01.2023
- Applies as of **17.01.2025**.
- Underlying documents (standards, guidelines):
  - 1st batch 17.01.2024.
  - 2nd batch 17.07.2024.

Further info on the European Commission’s website for DORA

DORA pillars

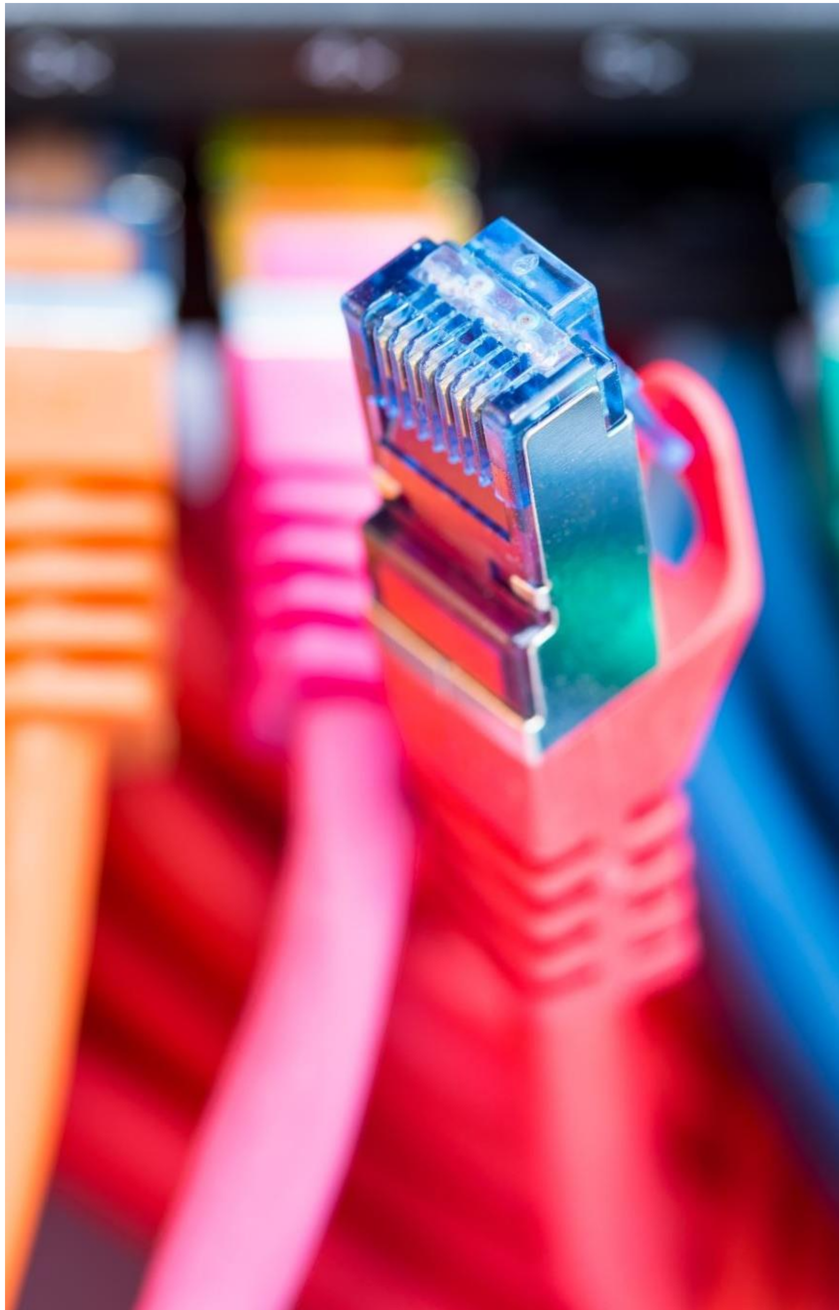
ICT Risk Management	ICT Incident Management, Classification, Reporting	Digital Operational Resiliance Testing	Managing ICT 3rd Party Risk (incl. CTTPs)	Information sharing

+ PROPORTIONALITY

ICT Risk Management

- **Documents, systems, tools**
- **Risk management**
  - DOR strategy
    - In line with business strategy
    - Risk tolerance
    - Detection, protection, prevention
- **Governance**
  - Responsibility: on the management

[Draft RTS (Delegated Regulation) on ICT Risk Management Framework]()



ICT Incident Management, Classification, Reporting

- **System for incident:**
  - monitoring
  - managing
  - logging
  - classifying
  - reporting

- **Reporting of major incidents to:**
  - Clients
  - Competent authorities

Draft RTS (Delegated Regulation) on classification of major incidents and significant cyber threats

Digital operational resilience testing

- **Basic testing**
  - All
  - Testing programme
  - ICT tool testing

- **Advanced testing**
  - For significant FIs

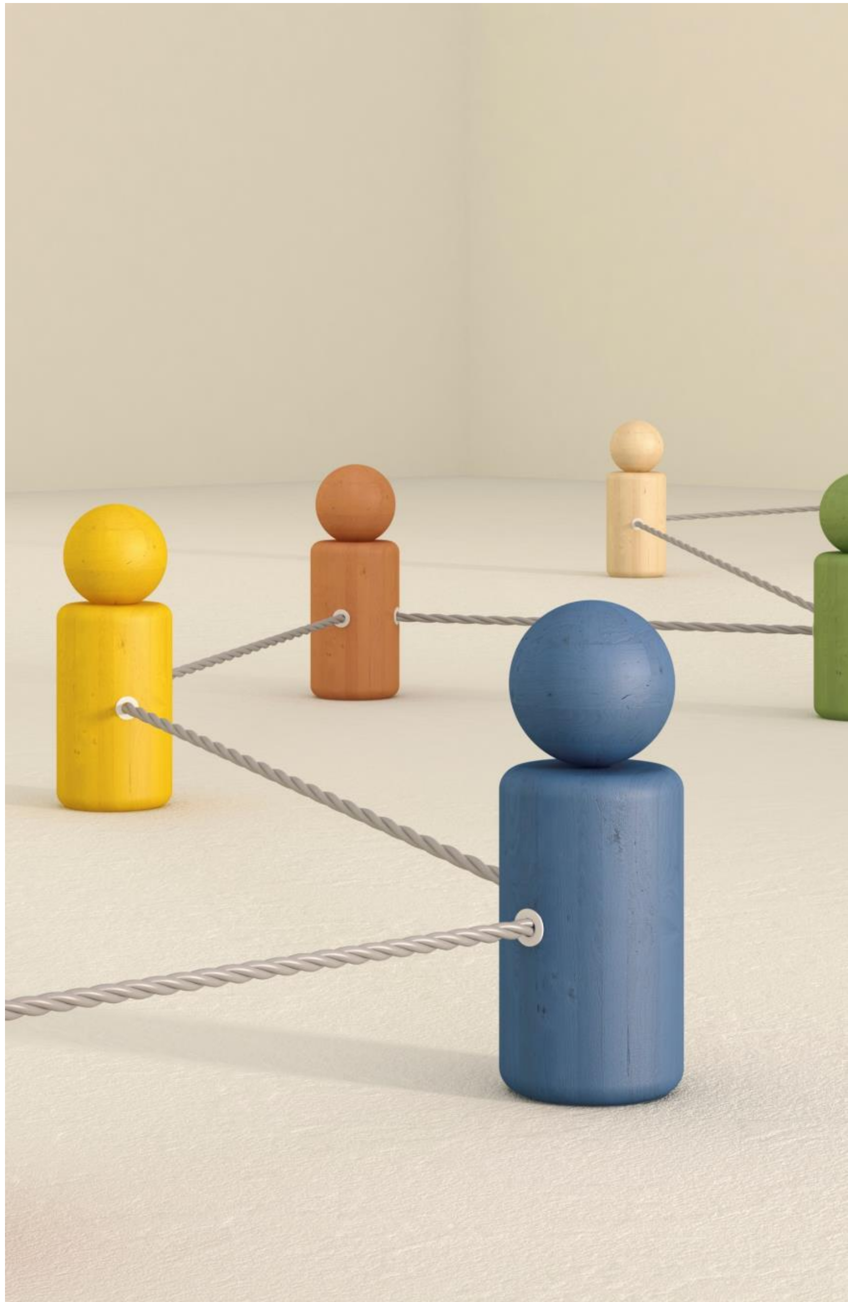
RTS TBA

Managing ICT 3P risk

- **Outsourcing-> All 3P arrangements**
- **Principles**
  - Strategy for 3P risk
  - Register contract information
  - Monitor
  - Criteria for contracts
- **Contractual provisions**
  - Minimum required conditions
  - Especially for critical functions
- **Special oversight for Critical Third Party Providers**

[Draft RTS (Delegated Regulation) on criteria for designating ICT service providers as critical]()

[Draft RTS (Delegated Regulation) to specify the policy on ICT services supporting critical or important functions]()



Information Sharing

- Learning from the incidents
- Exchange of information and intelligence on cyber threats

Supervision

- Access to documents/data
- On-site inspections & investigations
  - Summoning representatives
  - Interviewing any persons

- Require corrective/remedial measures

Sanctions

- Order to cease conduct (temp/perm)
- Fines
- Public notices
- Administrative (and criminal?) penalties
- Determined locally

Takeaways

Phase A

1. Internal Audit
2. Educate, Follow
3. Compare 1+2
4. Prepare & Introduce

Phase B

1. Protect & Prevent
2. Recover & Evolve

Leverage & Monetize

Turn to our Sorainen team for legal advice:

On DORA:

- Gap analysis between the existing and required ICT security arrangements
- Develop ICT framework
- Assist in preparing the policies & procedures
- Audit of third-party provider registers and arrangements (contracts)
- Incident reporting
- Assessment of proportionality

On other matters:

- Financial institution regulatory advice from licencing to assisting with regulator’s inspections
- Regulatory advice on cybersecurity compliance
- Privacy and data protection advice
- Regulatory advice on emerging technologies (AI, IoT)

Mihkel Miidla,

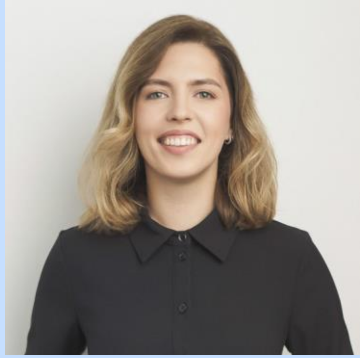
Estonia

mihkel.miidla@sorainen.com

Agneta Rumpa,

Latvia

agneta.rumpa@sorainen.com



Akvilė Jurkaitytė,

Lithuania

akvile.jurkaityte@sorainen.com