Digital Operational Resilience Act (DORA)

With you today….

Jan Eberle

Director
Risk Assurance,
PwC

Carina Allmann

Manager
Risk Assurance,
PwC

Eduard Obernauer

Senior Associate
Risk Assurance,
PwC

Setting the Scene

Financial Services cyber risks and case studies

	Generic Threats			Financial Services Threats			
Key Cyber Threat Scenario	Ransomware encrypting data, threats to leak sensitive data	Increasing complexity and reliance on digital supply chain	Targeting the digital supply chain	Theft of funds from institutions via business email compromise	Theft of funds from individuals and institutions	Disruption of online services	Theft of personally identifiable information to defraud individuals
(Recent) Examples	**2021** **Fake browser update allowed threat actor to extort A Financial's data for $40 million**	**2021** **Vulnerability in legacy FTA software used in data extortion**	**2022** **Over $570 million was stolen following a compromise to DNS hosting infrastructure**	**2020** **Attackers arrange fraudulent transfer of $10 million through a business email compromise**	**2022** **North Korea-based threat actors stole $100 million abusing a vulnerability**	**2022** **Pro-Russian hacktivist Killnet launched DDoS attacks, with minimal impact**	**2022** **Data breach resulted in the personal details of 50,000 customers being compromised**

The evolution of digital risks related to the geopolitical context and the change in European regulations to manage ICT and Cyber risks

World Economic Forum annual meeting in Davos: The Global Cyber Outlook 2023

Key Takeaways

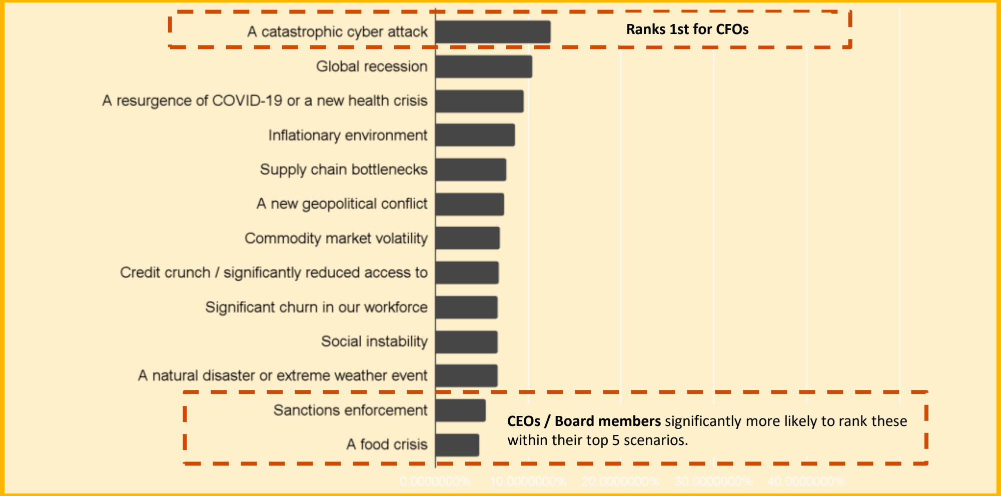
Global geopolitical instability has helped bridge the perception gap between the views of business and IT leaders on **the importance of managing cyber risk**. **A catastrophic cyber event** is at least somewhat likely in the next couple of years.

There is much more companies can do to increase resilience, including:

- improve e-skills and awareness,
- communication
- information sharing

CEOs Point of View: PwC 2023 Global Digital Trust Insights

PwC gathered the views of CEOs, CIOs and CISOs to better understand Cybersecurity & Privacy priorities and evolutionary trends between the first and second line of defense.

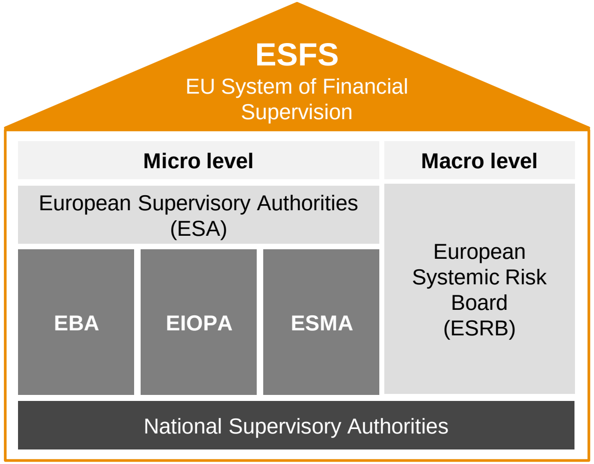


Ranks 1st for CFOs

CEOs / Board members significantly more likely to rank these within their top 5 scenarios.

Classification and framework of DORA

The "DORA Regulation" creates a binding framework for action in the future



ESFS
EU System of Financial Supervision
Micro level
Macro level
European Supervisory Authorities (ESA)
EBA
EIOPA
ESMA
European Systemic Risk Board (ESRB)
National Supervisory Authorities

Enactment

DORA entered into force on **January 16, 2023**
Subsequent specifications in form of RTS* and ITS* are planned.

Transition period

After entry into force, there is a transition period of 24 months in total for implementation.

Framework

EU law

Need to strengthen digital operational resilience

Proportionality

Consideration of differences such as business model, size or risk profile

Supervisory Practice

Access to information on ICT incidents and creation of an immediate review possibility of ICT services

Reporting procedure

Creation of a uniform procedure for the classification and reporting of ICT incidents.

Fines

Member states may apply administrative penalties or remedial measures

Implementation in Europe

Harmonisation of current gaps and overlaps in national and Union-wide legislation on ICT risks

**RTS: Regulatory Technical Standards and ITS: Implementing Technical Standards*

The essence of DORA

‘Digital Operational Resilience’

What does it really mean?

“

The ability of a finance entity to **build**, **assure** and **review** its operational integrity and reliability by ensuring…

… either directly or indirectly through the use of services provided by **ICT third-party services providers,**…

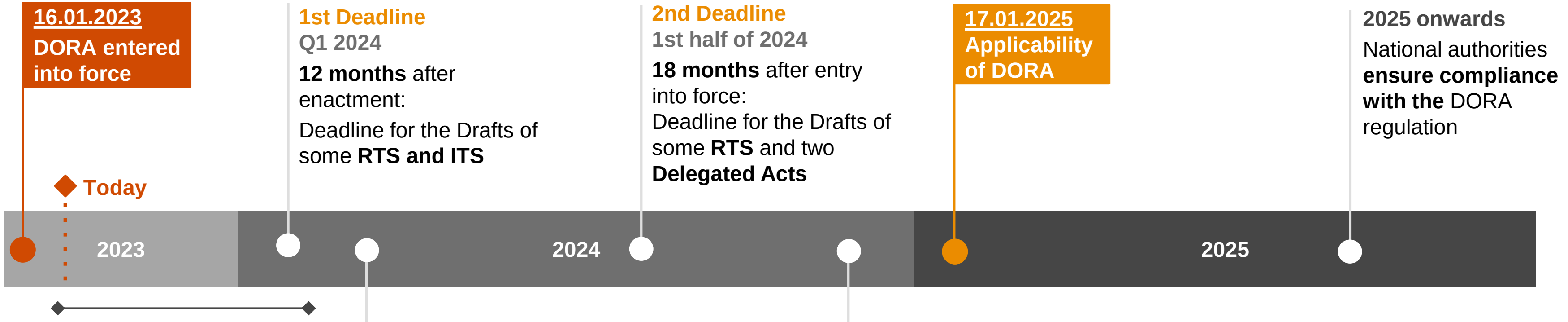
... the **full range of ICT-related capabilities** needed to address the security of the network and information systems which a financial entity uses…

… and which support the **continued provision** of financial services and their quality, **including throughout disruption**”

”

DORA Roadmap

The road to entry into force



16.01.2023
DORA entered into force

Today

Jun-Sep
Nov-Jan‘24
Public consultation phases for RTS / ITS

1st Deadline
Q1 2024
12 months after enactment:
Deadline for the Drafts of some **RTS and ITS**

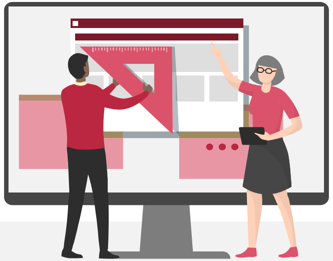
Early 2024
Expected publication of the **consultation versions** of two delegated regulations

2nd Deadline
1st half of 2024
18 months after entry into force:
Deadline for the Drafts of some **RTS** and two **Delegated Acts**

3rd Deadline
End of 2024
24 months after effective date:
Deadline for the **ESA report**

17.01.2025
Applicability of DORA

2025 onwards
National authorities **ensure compliance with the** DORA regulation



**Note: The future dates listed are estimates and intended only to provide a basic time frame.*

Scope and Proportionality

Scope

All participants on the financial markets, including banks, insurance undertakings and intermediaries, asset managers, crypto asset providers and more - below is a non-exhaustive list

- Credit Institutions
- Payment Institutions
- Electronic money institutions
- Investment firms
- Crypto-asset service providers
- Trading venues
- (Re)Insurance undertakings
- (Re)Insurance intermediaries
- Occupational retirement provision
- Credit rating agencies
- Crowdfunding service providers
- Account information service providers

ICT third-party service providers

Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards

Proportionality Principle

Size and overall risk profile, as well as the nature, scope and complexity of their services, activities and operations

DORA Spotlight

Subject areas may be grouped into five (5) pillars

ICT risk management

- Identification of **critical or important business functions** and determination of risk tolerances for ICT disruptions
- Continuously **identify all sources of ICT risk and define protection and prevention measures** (including comprehensive "business continuity" strategies and emergency recovery plans)
- **Implement key cyber security and resilience controls** such as IAM, SIEM, network segregation, etc.

ICT-related incidents

- Introduction of a management process for **logging and monitoring ICT-related incidents** (incl. their classification)
- Submit an initial, interim and final report on ICT-related incidents
- **Harmonise the reporting of ICT-related incidents** using the standard templates developed by the ESAs

Information sharing

- Arrangements for **sharing cyber threat information and intelligence** in a trusted environment
- Establish mechanisms to verify the information provided and take appropriate action

Digital operational resilience testing

- Advanced **threat-led penetration testing** every 3 years
- **Regular review of the ICT risk management framework** and annual review of all critical ICT applications, systems and processes
- Measures to **improve any identified deficiencies and reporting to the supervisory authorities**
- Possible regular implementation of **threat-driven penetration tests with the involvement of third-party service providers**

Management of risk by third-party ICT providers

- **Harmonisation of relations with ICT third party providers** in all phases of contractual agreements
- **Standard contractual clauses** must contain a full description of the services provided
- **Continuously monitor, document and report** on all contractual arrangements with third party providers and **identify services that support critical or important functions**

Effects of DORA

The FS industry Point-of-View

First Steps	Challenges	Additional strengthening of resilience
Gap Analysis	Critical services mapping, including tech chain and ICT TPP	TIBER-EU
Remediation Plan	Scenario-based management models evolution	Automated communication processes
New DORA responsibilities establishment	Network Segregation	Market collaboration and information sharing
Incident Management Process	Zero-Trust Implementation	**Dashboard** for Integrated **ICT/Cyber Risk Monitoring**
Threat Intelligence	Threat-led penetration tests	
ICT service provider contracts and recovery/exit measures	ICT TPP Risk Mgmt & Governance	

Common Issues

Digital Operational Resilience Strategy

New strategies and frameworks, cross-company and cross-function, integrated with existing processes. Need to set up integrated Indicators, monitoring, dashboarding

End-to-end visibility

Lack of integrated governance models and maintenance processes.

Value chain management

Need to improve outsourcing management. A clear overview of 3rd and 4th parties needs to be established.

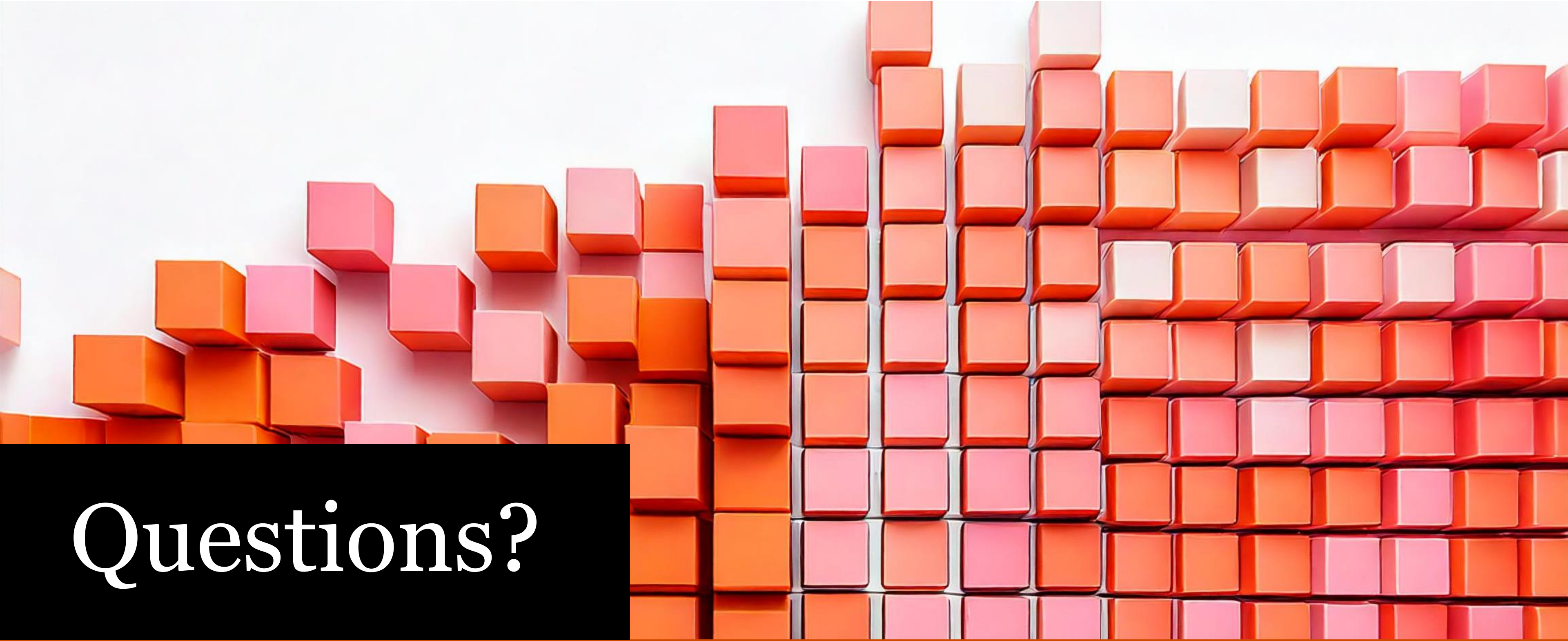
TLPT as Cyber business case (TIBER-EU)

TLPT effectiveness can be achieved through robust key cyber capabilities - e.g., threat intelligence, early warning, incident response - and strong senior leadership commitment.

IT Challenges

Configuration & Asset Management
EoL and Legacy Systems

Network Security & Segmentation
Identity and Access Management



Questions?