



# DORA: The final sprint

D-Day is here soon, are you ready to comply?



# Agenda

- Introduction
- DORA Recap
- Where are we in time?
- Challenges faced by financial institutions
- How to maximize your implementation during the final sprint?
- Practical exercises

# Introduction

Ali Alam  
Senior Manager @ KPMG

- DORA SME
- Part of the KPMG NL DORA Working Group - Core Team
- SME on DORA, DNB IS Good Practice and EBA ICT Guidelines and extensive experience in maturity assessments, implementations and assurance on these regulations



The background features two large, overlapping curved lines. One is a light green color and the other is a light gold or tan color. They are positioned in the top-right and bottom-left corners of the slide, framing the central text.

Let's recap

# DORA – briefly explained

The "Digital Operational Resilience" initiative was published by the EU Commission at the end of September 2020 as a proposal for a package of measures to further digitize the financial sector. The aim is to strengthen the competitiveness and innovation of the financial market.

The proposal extends existing regulations (MaGo, VAIT, etc.) and addresses requirements regarding digital risks.

Important components are the harmonization of regulations for information and communication technology (ICT) risk management, reporting, audits and for the risk evaluation of ICT third-party providers.

## Intention of DORA

DORA aims to unify existing European as well as national standards and requirements to create a detailed and comprehensive framework for the digital operational stability of EU financial firms.

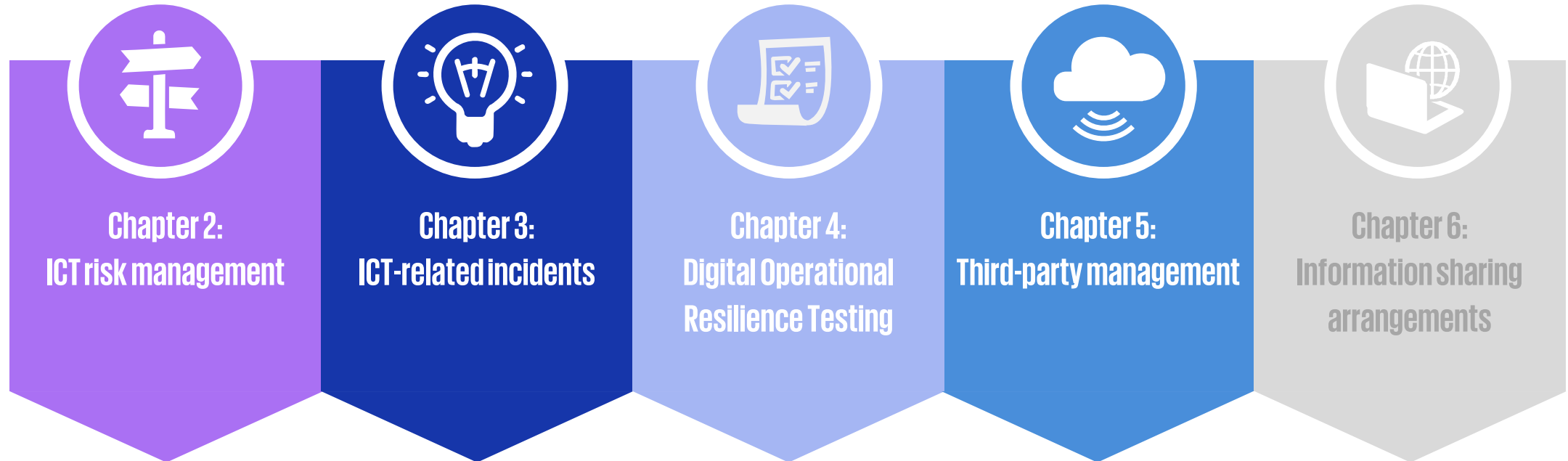
The focus is on maintaining the (digital) business operations and related processes and services in case of an ICT-related incident, if a permanent failure of these could lead to the instability of the entire European financial system.



# The DORA requirements are classified into four subject areas



... which address ICT risks within four core areas.



- Governance and organization (incl. DOR strategy)
- ICT risk management framework (incl. all phases)
- ICT systems, protocols and tools
- Response and recovery (incl. backup)
- Learning processes

- Detection and handling of ICT-related incidents
- Classification of ICT-related incidents
- Reporting ICT-related incidents
- Crisis communication strategies

- General requirements for testing (incl. test concept)
- Testing of ICT tools and systems (test types)
- Extended tests based on TLPT
- Requirements for the testers

- General principles of third-party management
- Concentration risk incl. dependencies
- Contract contents
- Critical ICT third-party service providers
- Multi-vendor strategy
- Evaluation of exit strategies

- Exchange of information and findings on cyber threats
- Guaranteed data security

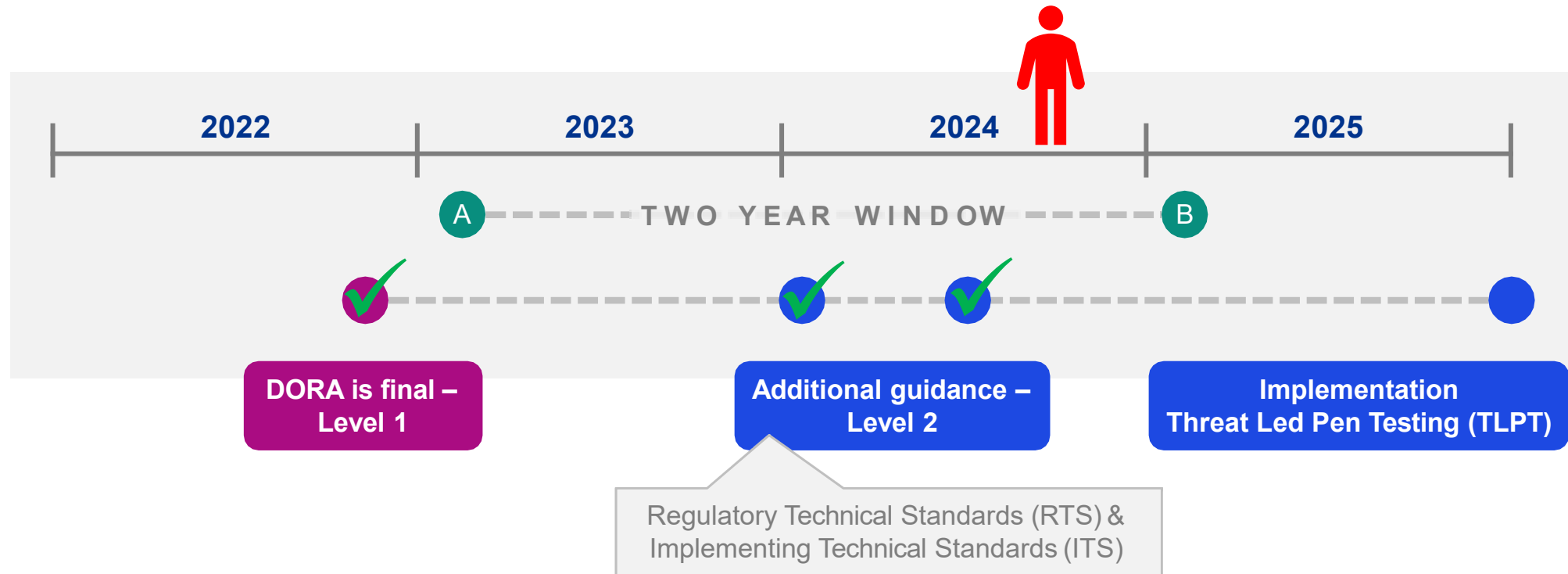
# The fields of application and recipients of DORA

see DORA Article 2 (1)

 <p><b>Credit institutions</b></p>	 <p><b>Payment institutions</b></p>	 <p><b>Electronic money institutions</b></p>	 <p><b>Investment firms</b></p>	 <p><i>Crypto asset service providers and issuers of crypto assets, asset-referenced tokens, significant asset-referenced tokens</i></p>	 <p><b>Trading venues</b></p>	 <p><b>Trade repositories</b></p>
 <p><b>Managers of alternative investment funds</b></p>	 <p><b>Management companies</b></p>	 <p><b>Central securities depositories</b></p>	 <p><b>Central counterparties</b></p>	 <p><b>Data reporting service providers</b></p>	 <p><b>Insurance and reinsurance undertakings</b></p>	 <p><b>Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries</b></p>
 <p><b>Institutions for occupational retirement provision</b></p>	 <p><b>Credit rating agencies</b></p>	 <p><b>Account information service providers</b></p>	 <p><b>Administrators of critical benchmarks</b></p>	 <p><b>Crowdfunding Service Providers</b></p>	 <p><b>Securitization repositories</b></p>	 <p><b>ICT third-party service providers</b></p>



# Where are we now?



# Publication of regulatory standards (RTS & ITS) till date

ICT risk management framework (Chapter II)	Handling, classification and reporting of ICT-related incidents (Chapter III)	Testing digital operational resilience (Chapter IV)	ICT Third Party Risk Management (Chapter V Section I).	Monitoring framework (Chapter V Section II)
<ul style="list-style-type: none"> <li>✓ RTS on the ICT risk management framework (Art.15)</li> <li>✓ RTS on the Simplified ICT Risk Management Framework (Art.16.3)</li> <li>✓ Guidelines for estimating aggregate annual costs and losses, due to serious ICT-related incidents (Art.11.11)</li> </ul>	<ul style="list-style-type: none"> <li>✓ RTS classification of ICT-related incidents and cyber threats (Art.18.3)</li> <li>✓ RTS content of reports on serious ICT-related incidents (Art.20.a)</li> <li>✓ ITS reporting details serious ICT-related incident (Art.20.b)</li> <li>✓ ITS reporting details serious ICT-related incident (Art.20.b)</li> </ul>	<ul style="list-style-type: none"> <li>✓ RTS for advanced testing based on Threat Led Penetration Testing TLPT (Art.26.11)</li> </ul>	<ul style="list-style-type: none"> <li>✓ ITS with standard templates for information registers (Art.28.9)</li> <li>✓ RTS on the specification of the use of ICT services of ICT third party service providers (Art.28.10)</li> <li>✓ RTS on contracting out support of critical or important functions to ICT third-party services (Art.30.5).</li> </ul>	<ul style="list-style-type: none"> <li>✓ EBA seeks ESAs' views on criticality criteria (Art.31.8) and fees (Art.43.2) (September 2023, legal act July 17, 2024).</li> <li>✓ Guidelines Cooperation ESA with authorities for supervision (Art.32.7)</li> <li>● RTS on harmonization of monitoring (Art.41)</li> </ul>

(RTS) Regulatory Technical Standard // Regulatory Technical Standards (ITS) Implementation Technical Standard // Implementation Technical Standards Gray deviating timeline

DORA is complete!!

The image features a white background with decorative curved lines in shades of green and gold. One line is in the top right corner, curving downwards and then back up. Another line is in the bottom left corner, curving upwards and then back down. The text "Some reflection" is centered in the middle of the page.

Some reflection



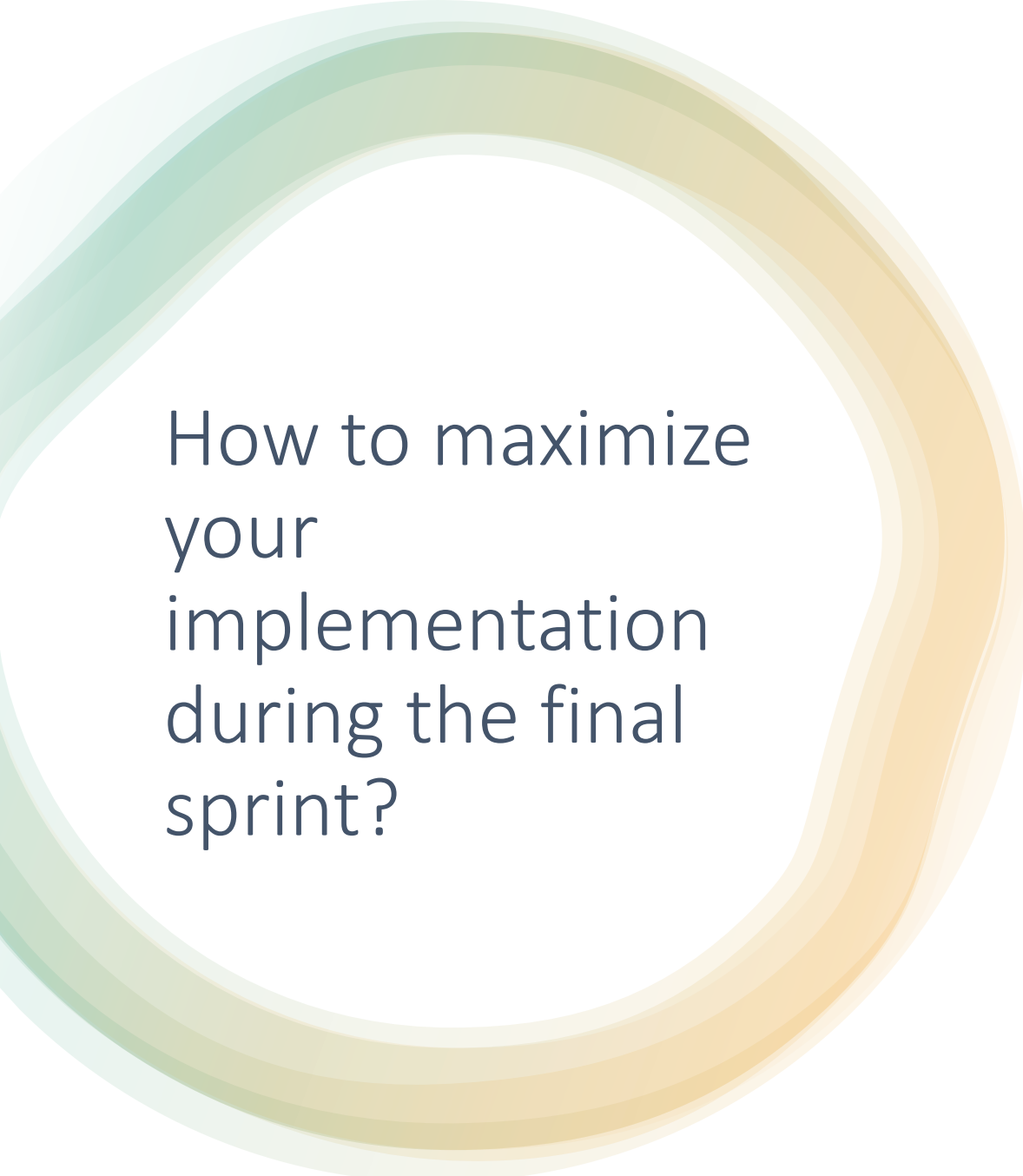
# Challenges faced by financial institutions

- Overall late traction in the financial sector to start up with DORA
- Underestimation of DORA requirements and the collective magnitude
- Financial entities are struggling to comply with DORA within the given timelines, which include:
  - Amount of work to implement is huge
  - Lacking the resources to perform the implementation themselves
  - Little time left till deadline



# Challenges faced by financial institutions

- Fundamental elements are often not in place and hinder a structured and timely implementation. These include:
  - Definition of critical of important functions and underlying chain of ICT assets, tools and ICT Third Party Service Providers not done timely or properly, resulting in delays or rework
  - Structured ICT risk policy house
  - ICT Risk & Control Framework
  - Digital Operational Resilience Strategy
  - Outsourcing Policy
  - Centralized administration of ICT Third Party Service Providers
- Pillar Third Party Risk is the most challenging and time consuming as it requires amendment of contractual arrangements with ICT third party service providers.
- Operational resilience testing is often a result of cherry picking without a risk-based approach.



# How to maximize your implementation during the final sprint?

- Focus on achieving the implementation of the fundamentals per DORA Pillar.
- Have the reporting processes in place
- Document the TPRM Register of Information
- Have your contracts with critical and important ICT TPSPs adjusted to DORA requirements

Implement the remaining requirements in 2025!

The background features two large, overlapping, curved bands. The upper band is primarily green with a gold-to-yellow gradient at its outer edge. The lower band is primarily gold with a green-to-teal gradient at its outer edge. Both bands have a soft, glowing effect.

# Practical Exercises

# Let's do some practical exercises

- **Article 3, subarticle 22**
- Critical or important function' means a function, the disruption of which would materially impair the financial
  - performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued,
  - defective or failed performance of that function would materially impair the continuing compliance of a financial
  - entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.
- **As a group, please explain how you would identify the critical or important functions and related ICT assets and ICT TPSPs?**
- *Break-out lead by Ali*





# Let's do some practical exercises

- **Article 5, subarticle 4**
- Members of the management body of the financial entity shall actively keep up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the financial entity, including by following specific training on a regular basis, commensurate to the ICT risk being managed.
- **As a group, please explain how you would approach compliance with this requirement while taking into account time pressures that management bodies often have and the diversity of topics they need to be informed about**
- *Break-out lead by Gracia*



# Let's do some practical exercises

- **Article 24, subarticle 6**
- Financial entities [...] shall ensure, at least yearly, that appropriate tests are conducted on all ICT systems and applications supporting critical or important functions.
- **As a group, please explain how you would approach the determination of the appropriateness of the testing.**
- *Break-out lead by Jasper*

