



Asociatia Auditorilor Interni din Romania (A.A.I.R.)

Annual Conference 2024

31 October 2024

Digital Operational Resilience Act (DORA)

Anestis Dimopoulos, CIA, CISA, CGEIT, CRISC, CISSP

Director, Head of Digital & Risk Advisory Services



Agenda

1

Introduction

2

DORA Regulation and Key Requirements

3

Implementation Challenges

4

Conclusion – Best Practices for Implementation

Baker Tilly South East Europe

Baker Tilly South East Europe is a full-service accounting and advisory firm that offers industry-specialised services in assurance, tax and advisory.

Everyday, 500 professionals located in 7 offices in 5 countries throughout South East Europe share their expertise to accelerate your growth.



COMPLETE SPECTRUM OF SERVICES

Audit & Assurance	Tax Advisory	Financial Compliance & Reporting
Transaction Advisory	Financial Services Advisory	Risk Advisory
Corporate Services	Human Resources Advisory	Digital & Technology Advisory
Strategy & Management Consulting	ESG Advisory	Legal Services



resilience

noun [U]

uk /rɪˈzɪl.jəns/ us /rɪˈzɪl.jəns/

(also formal resiliency, uk/rɪˈzɪl.jən.si/ us/rɪˈzɪl.jən.si/)

- **the ability of a substance to return to its usual shape after being bent, stretched, or pressed**
- **the quality of being able to return quickly to a previous good condition after problems**

(Definition of resilience from the Cambridge Business English Dictionary © Cambridge University Press)

“Why is DORA needed?”

The financial sector is **increasingly dependent** on **technology** and on **tech companies** to deliver financial services. This makes **financial entities vulnerable** to **cyber-attacks or incidents**.

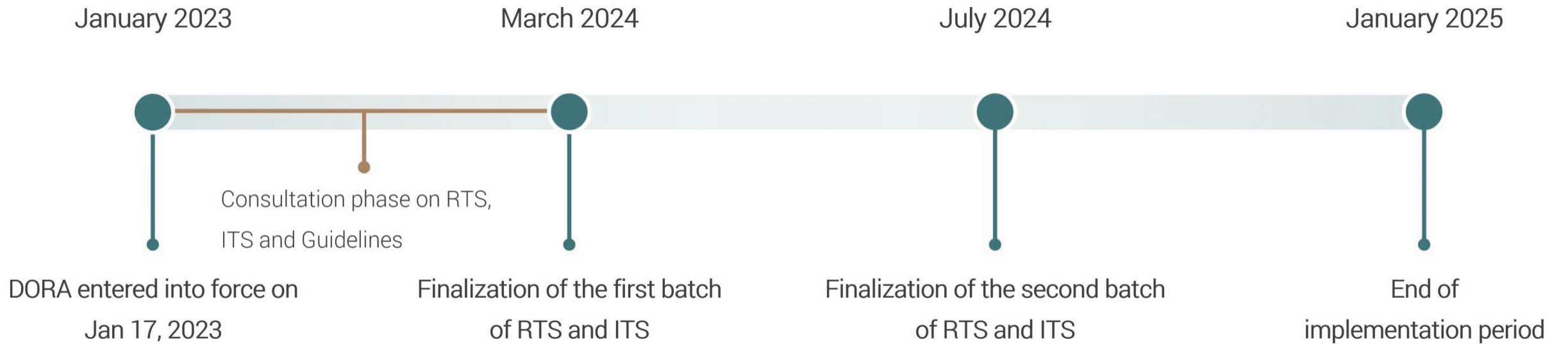
When not managed properly, **ICT risks can lead to disruptions** of financial services offered across borders. This in turn, can have an **impact on other companies**, sectors and even on the rest of the economy, which underlines the importance of the **digital operational resilience** of the **financial sector**.

This is where the Digital Operational Resilience Act, or DORA, comes into play.”

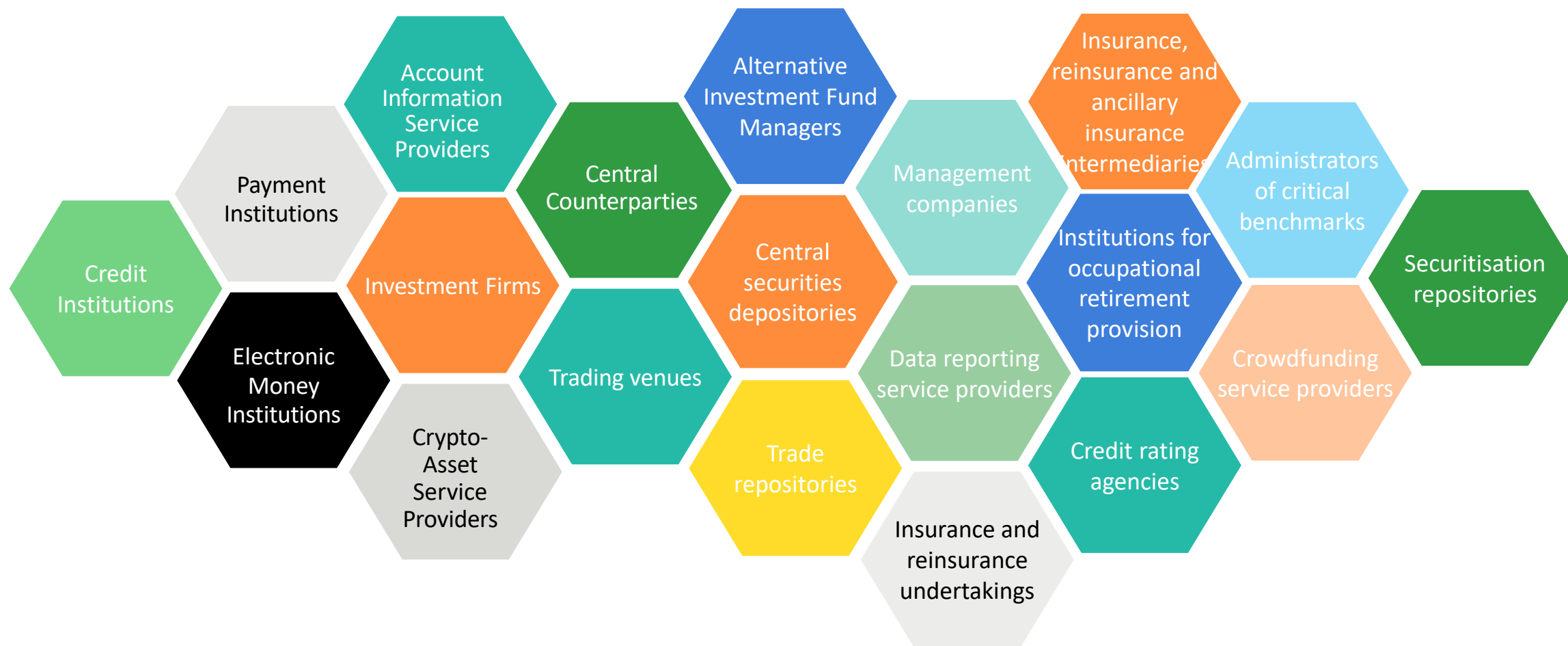
https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

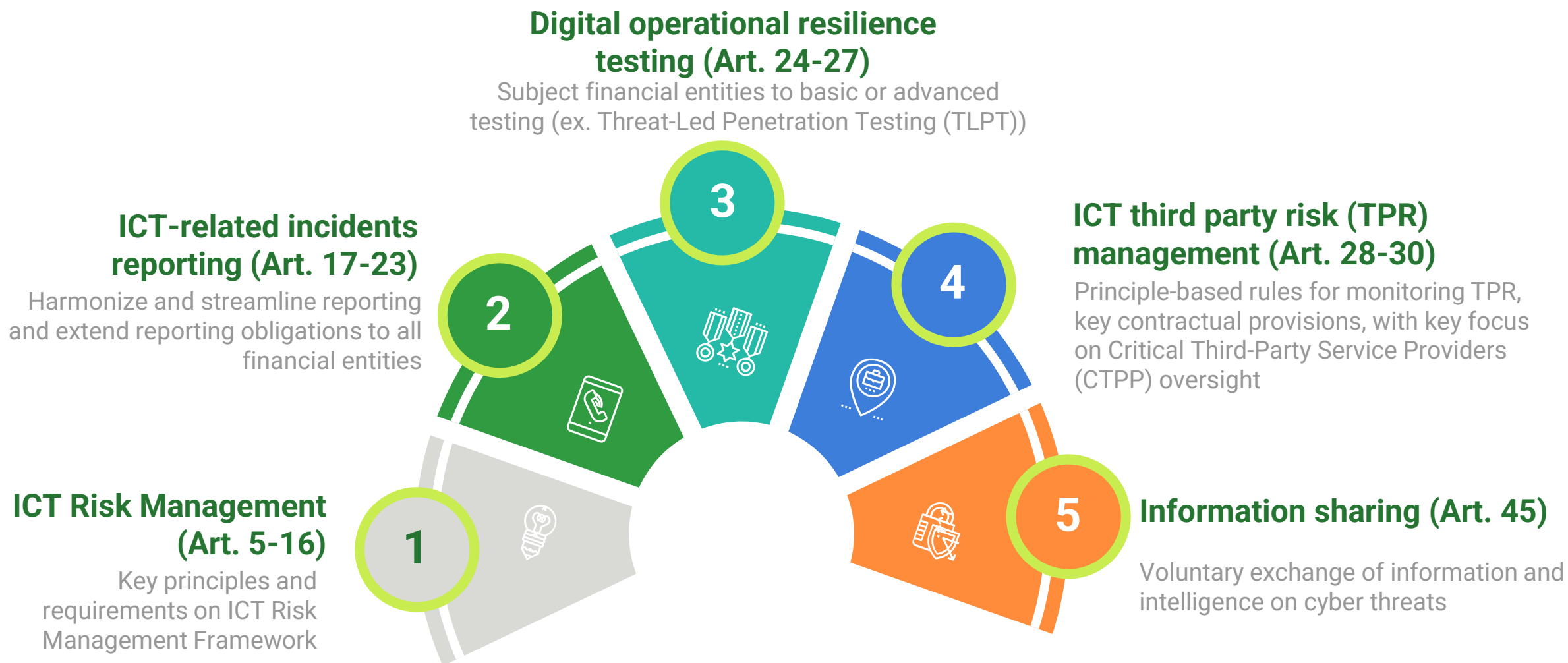


DORA IMPLEMENTATION TIMELINE



SCOPE OF DORA – ENTITIES IMPACTED BY REGULATION

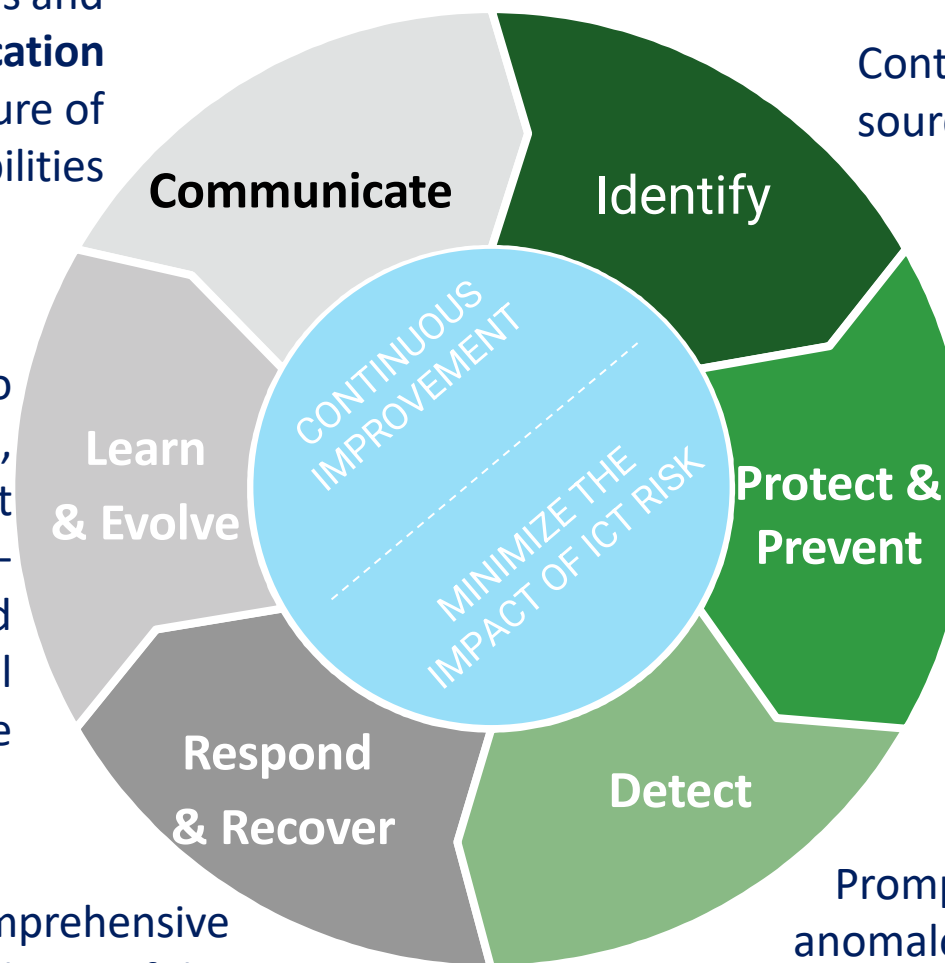




Document **communication** policies and activate, when necessary, **communication plans** that enable responsible disclosure of ICT-related incidents or major vulnerabilities

Place capabilities and staff, according to size, business and risk profiles of the FE, for gathering **information** about vulnerabilities, cyber threats, ICT-related incidents and cyber- attacks, and **analyse** their likely impacts on digital operational resilience

Implement dedicated and comprehensive **BCP** and **DRP** as an integral part of the operational business continuity policy



General Requirements

- Establish and implement a management process to monitor, log, handle and follow-up ICT-related incidents (Art.17)
- Classify ICT-related incidents based on criteria set out in DORA and to be further developed by the ESAs (Art.18)

Reporting of major ICT-related incidents to CAs

- Harmonized reporting content and templates (Art.20)
- Initial notifications, intermediate and final reports (Art.19.4)
- NCAs to provide details to institutions and authorities (ESAs, ECB, NISD2 authorities) (Art.19.6)
- Voluntary notification of significant cyber threats to NCAs (Art.19.2)
- Single EU Hub (Art.21)
- To National Competent Authorities (Art.19.1)

General Principles

- Full responsibility of the FE
- Strategy on ICT-TPR
- Register of information (Art.28.3)
- Preliminary assessment of concentration risk

Harmonisation of key elements of relationship with ICT- TPP

- Description of functions and services
- Indication of the location/ storage of data
- Assistance by the ICT-TPP
- Right to monitor and inspect

Union Oversight Framework for critical ICT-TPP

- Designation by the ESA (Art.31)
- ESA as Lead Overseers with powers to monitor & issue recommendations
- Oversight Forum – cross-sectoral coordination on all ICT risk matter and preparatory work for individual decisions and collective recommendations
- Joint Oversight Network-Coordination between LO (Art.34)

Basic Testing

- All Financial Entities (other than microenterprises)

FEs are obliged to:

- Implement a proportional and risk-based digital operational resilience testing programme
- Provide for the execution of a full range of appropriate tests (e.g. vulnerability assessments and scans, open source analyses, network security assessment, etc.)
- Test critical ICT systems and applications annually

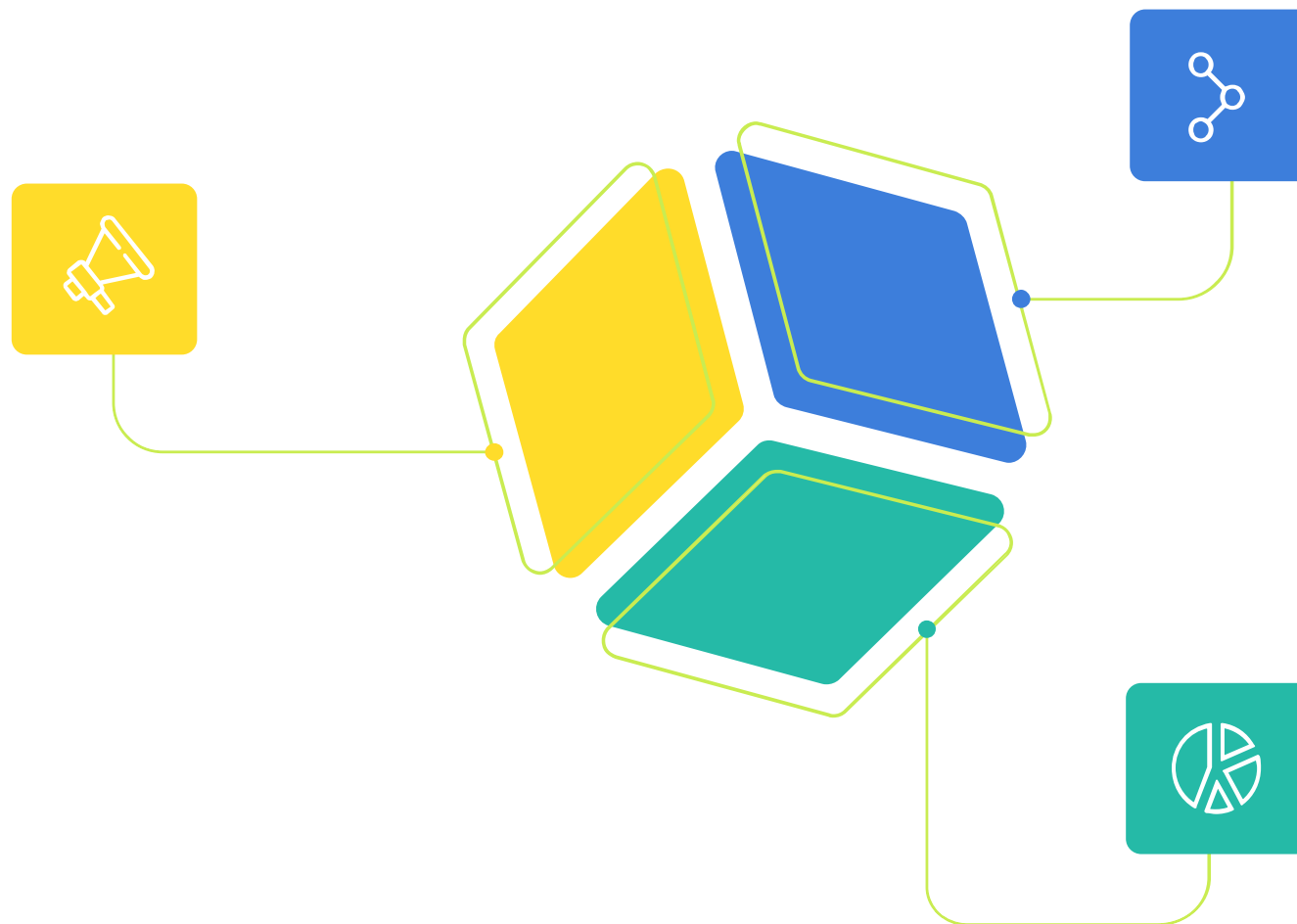
Advanced Testing

- Tests done every 3 years, frequency can be adjusted by CAs (Art.26.1)
- Mutual recognition of TLPT tests (Art.26.7)
- Use of external and internal testers (Art.27)
- Financial Entities identified by Competent Authorities (Art.26.1)

Certain FEs are required to carry out the so-called advanced TLPT once every 3 years

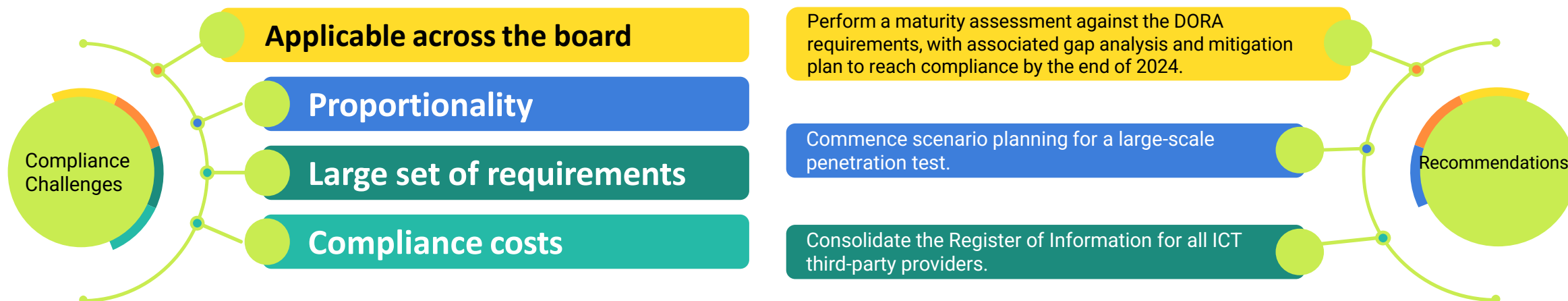
RTS to specify Thread Led Penetration Testing (TLPT) (Art.26.11)

Information sharing takes place within trusted communities and is carried out in accordance with applicable legislation (e.g. data protection, trade secrets, competition)



FE share with each other cyber threat information and intelligence

Exchange of information aims at enhancing the digital operational resilience of FE





Risk based Gap Analysis

- Risk and Impact Analysis
- Action Plan



Develop Detailed Action Plan

- Definition of projects / activities
- Assign Responsibilities
- Define and Allocate Resources



Adopt Controls Approach and Align with DORA Requirements

- Controls proportionality
- Adaptive approach



Monitoring and Continuous Progress Reporting

- Progress reporting mechanisms
- Interim assessments
- Corrective actions



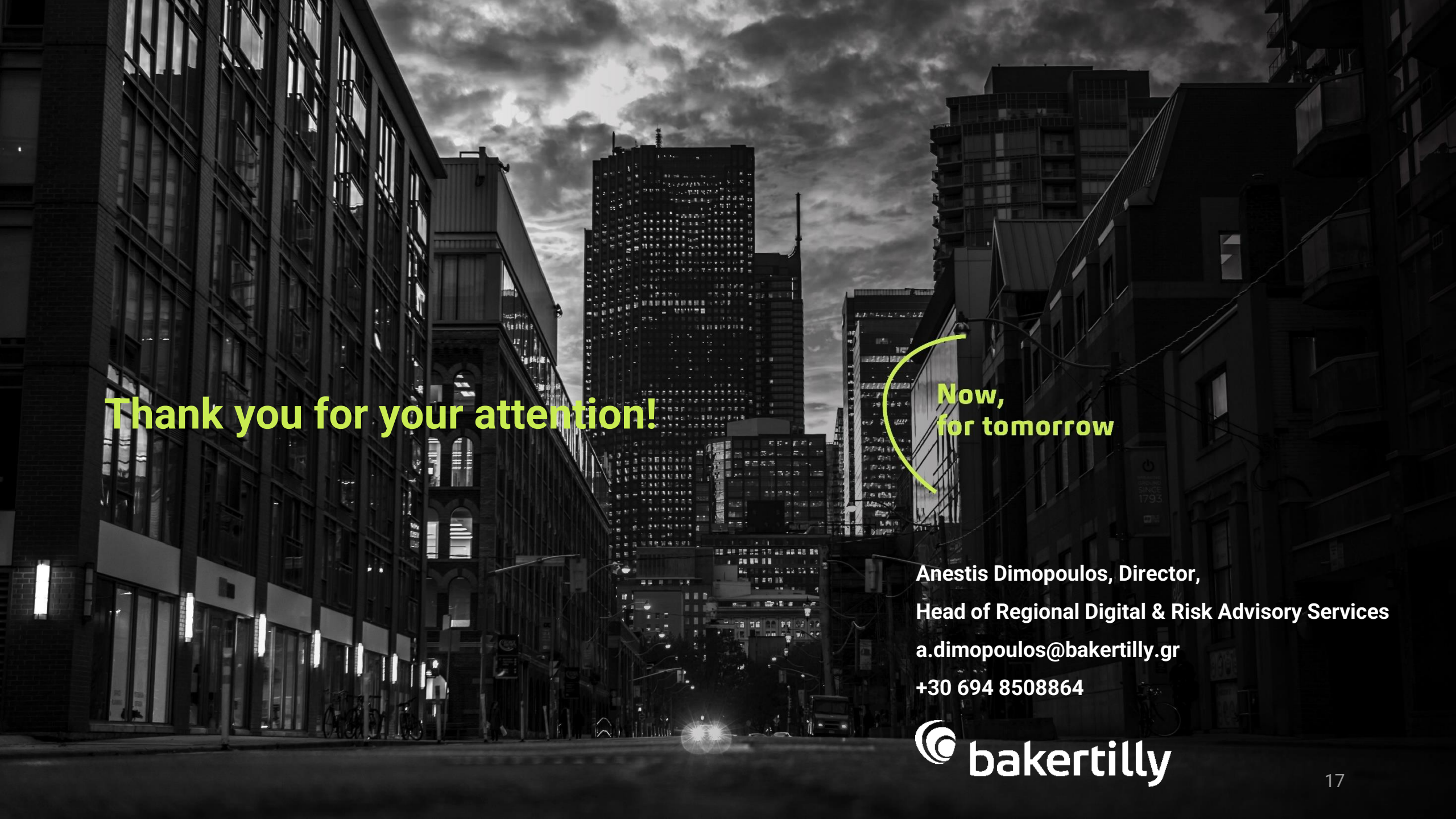
Continuous Improvement

- Evaluate effectiveness of compliance program
- Adapt to compliance changes



Documentation and Compliance Reporting

- Progress Reporting
- Baseline and compliance reporting
- Continuous monitoring



Thank you for your attention!

**Now,
for tomorrow**

**Anestis Dimopoulos, Director,
Head of Regional Digital & Risk Advisory Services
a.dimopoulos@bakertilly.gr
+30 694 8508864**

