

ALLEN & OVERY

The Digital Operational Resilience Act - DORA

9 December 2020



Speakers



Ben Regnard-Weinrabe

Financial Services Regulation, Fintech and Payments

London

Contact

+44 20 3088 3207

ben.regnard-weinrabe@allenoverly.com



Dr Catherine Di Lorenzo

Data and Technology

Luxembourg

Contact

+352 44 44 5 5129

Catherine.DiLorenzo@AllenOverly.com



Nikki Johnstone

Financial Services Regulation, Fintech and Payments

London

Contact

+44 20 3088 2325

Nikki.Johnstone@AllenOverly.com



Tom Anderson

Risk Management, A&O Consulting

London

Contact

+44 20 3088 6435

Tom.Anderson@AllenOverly.com



Heenal Vasu

Financial Services Regulation, Fintech and Payments


London

Contact

+44 20 3088 1447

Heenal.Vasu@AllenOverly.com

Housekeeping notes

- On joining the session your microphone will be muted and your video will be turned off
- To activate the Q&A function click  The Q&A box will appear on the right hand panel
- To submit a question use the Q&A function sending your question to “**All Panellists**”
- You will not be able to enable your video or un-mute your microphone during the session
- If you experience any technical issues and cannot submit these via Q&A please call +44 203 088 7196 or +44 203 088 7450



Agenda

‘ICT services’
means digital and
data services provided
through the ICT systems
to one or more internal
or external users

1 Key concepts and interactions with other texts

2 Scope

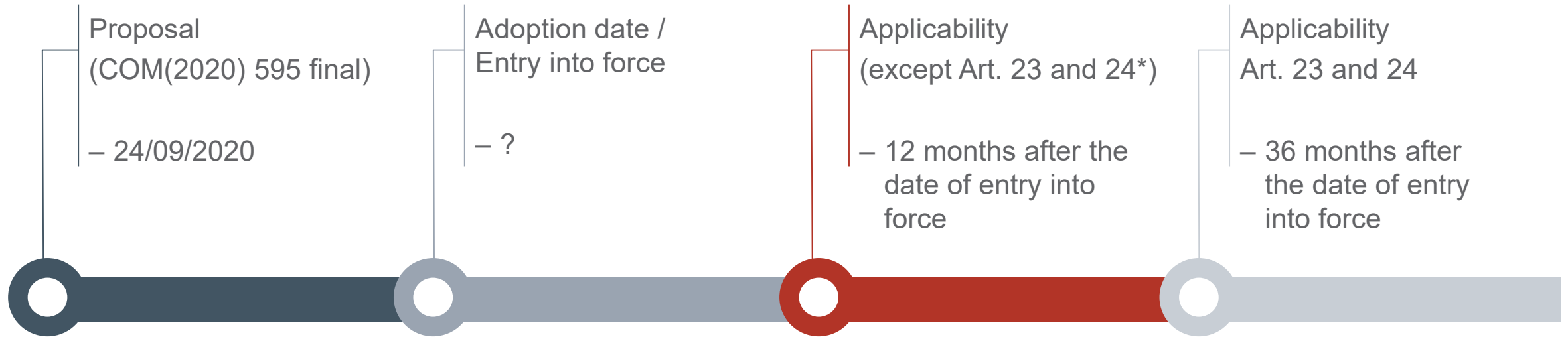
3 ICT risk management

4 ICT-related incident reporting

5 Digital operational resilience testing

6 Managing of ICT third-party risk

Introduction | Regulation on digital operational resilience for the financial sector (DORA)



**Requirement for threat-led penetration testing for significant financial entities*



Target date for implementation of Digital Finance Package is 2024



Key concepts and interactions
with other texts

Main texts under the current legal framework

Payment Services Directive (EU)
2015/2366

MiFID II Delegated Regulation

EBA Guidelines on ICT and security
risk management (EBA/GL/2019/04) –
The ICT Guidelines

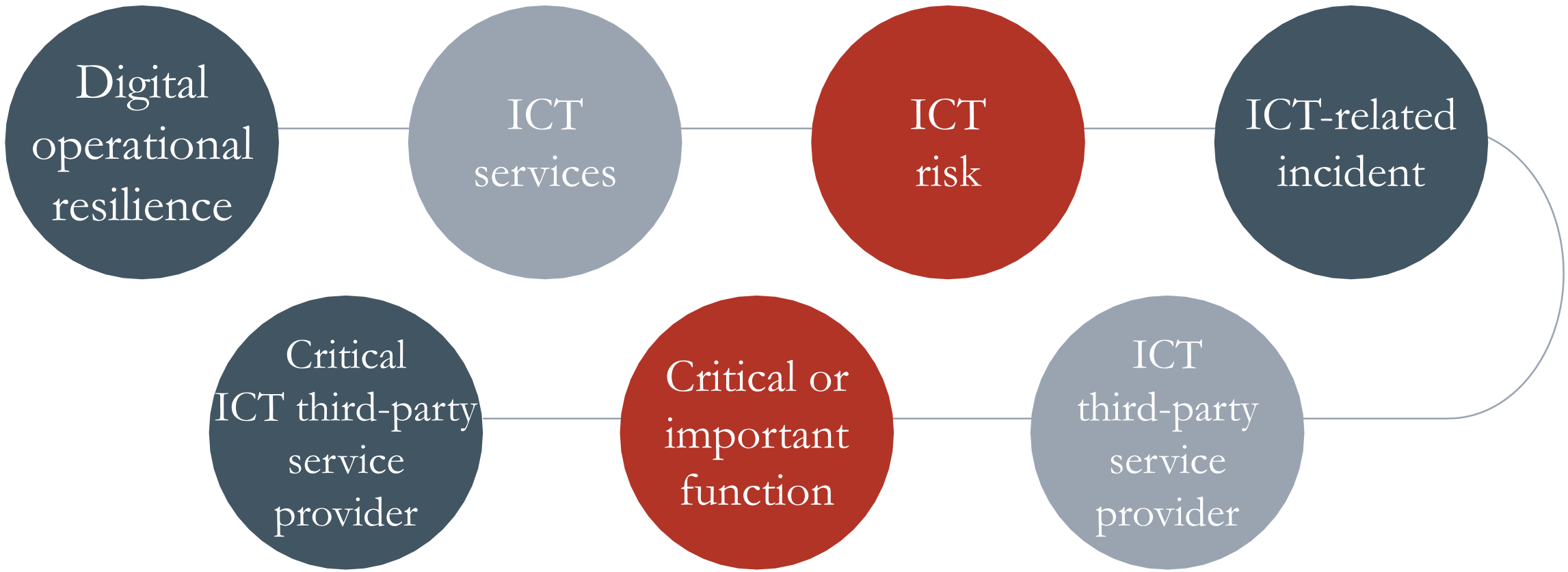
EBA Guidelines on outsourcing
arrangements (EBA/GL/2019/02), EIOPA
Guidelines on cloud outsourcing – **The
Outsourcing Guidelines**

EBA Guidelines on the notification of
major operational or security incidents
(EBA/GL/2017/10) – **The Notification
Guidelines**

Concepts under the current legal framework

Outsourcing / IT function / security	Outsourcing Guidelines	Credit Institutions and CRD investment firms, payment institutions and electronic money institutions	vs use of ICT third-party service provider
Cloud outsourcing	EIOPA Guidance on Cloud Outsourcing	EIOPA: insurance firms FCA: all FSMA firms not covered by EBA Outsourcing Guidelines	vs use of ICT third-party service provider
ICT and security risk management	ICT Guidelines	Credit institutions, CRD investment firms, payment institutions and electronic money institutions	vs ICT risk management
Operational or security incident	Notification Guidelines	Payment institutions	vs ICT-related incidents

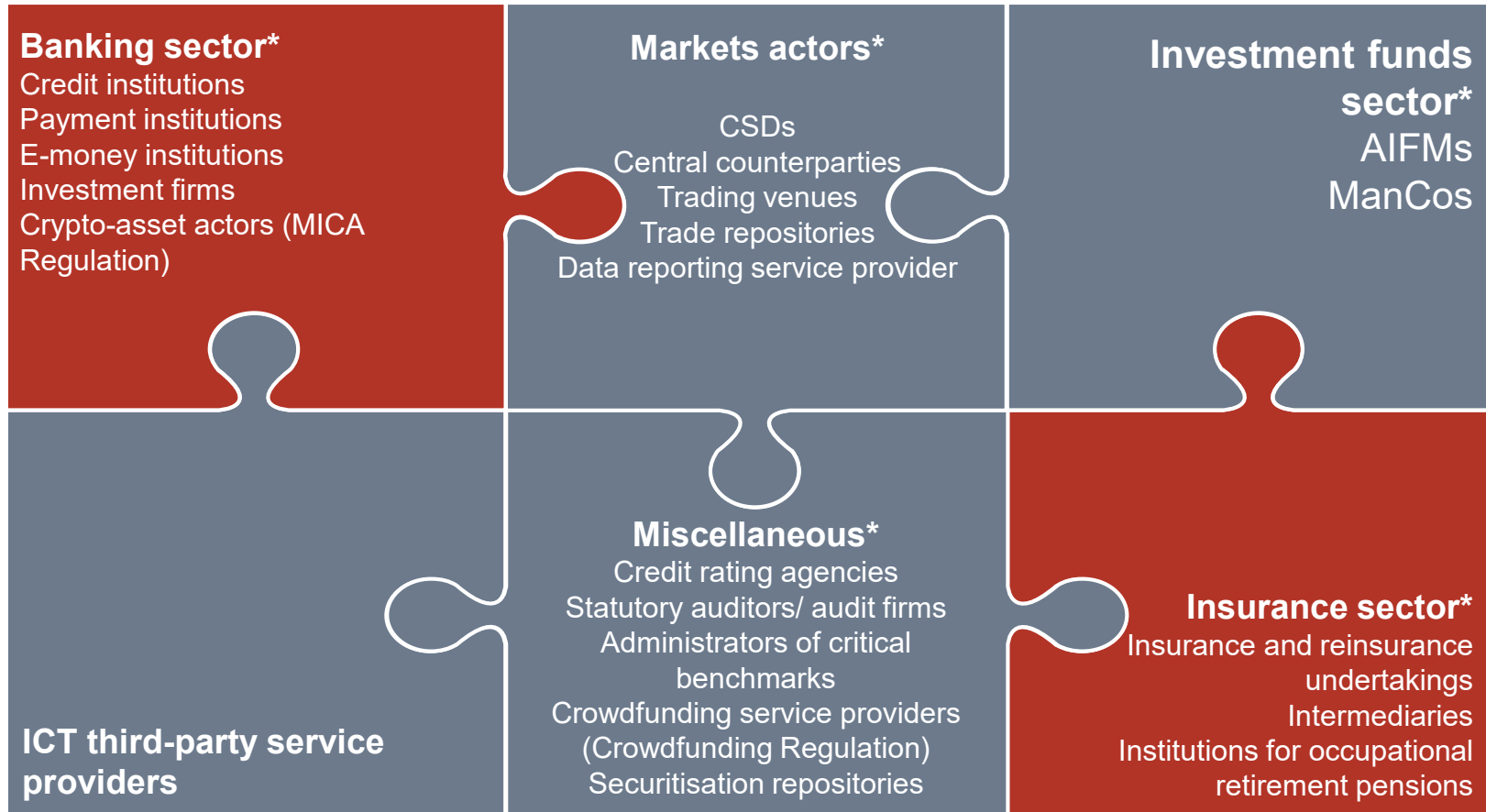
Key concepts



Scope



Financial entities* and ICT third-party service providers: an entire ecosystem is impacted



ICT risk management



ICT risk management framework

Audit and supervision

Regular audits of framework

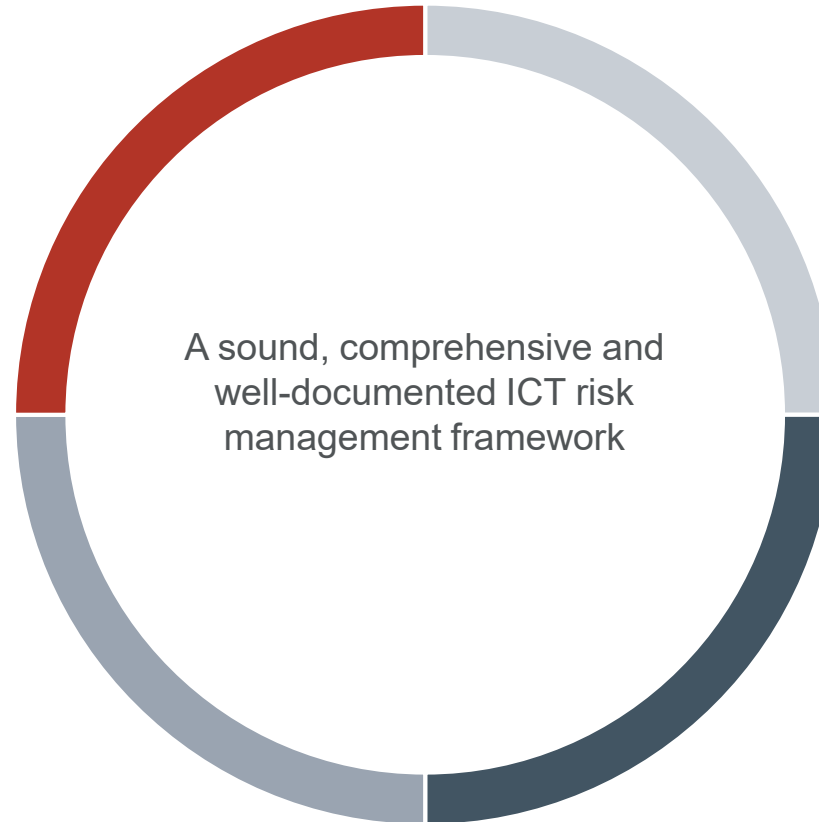
Provision information on ICT risks to authorities

Documentation and review of framework

Must be documented

Must be reviewed at least once a year

Must be continuously improved



Components

Strategies, policies, procedures, ICT protocols and tools

Information security management system

Digital resilience strategy

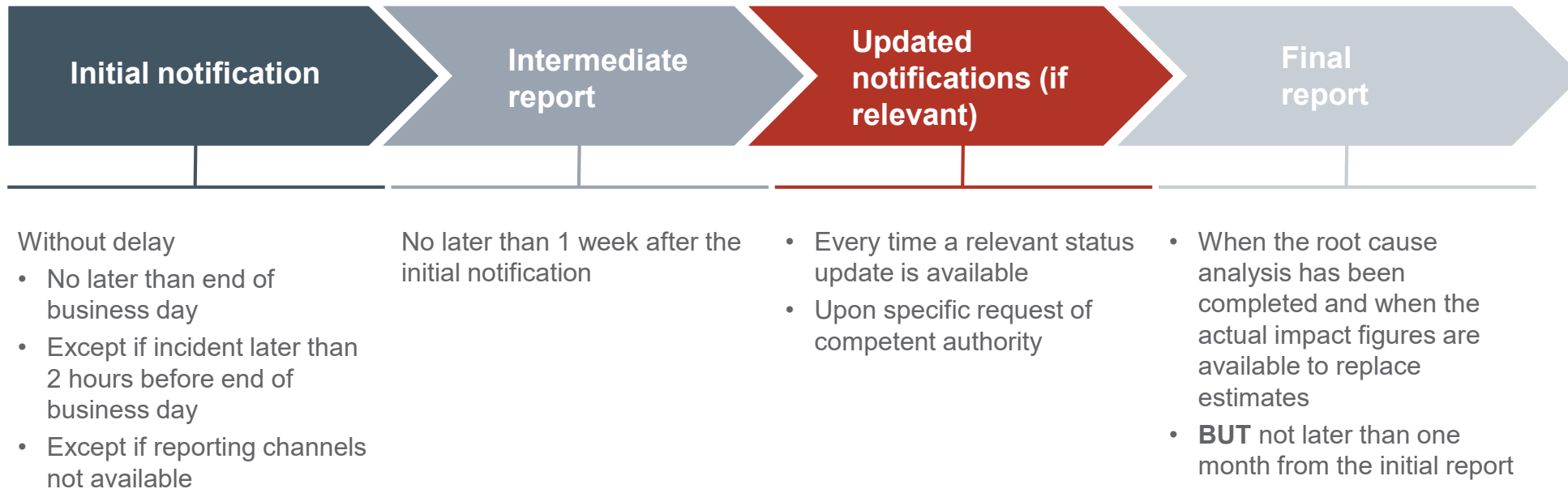
Segregation of duties

Segregation of ICT management functions vs control functions

Specific functions in ICT risk management



Reporting of major ICT-related incidents to competent authority



Competent authority to provide feedback or guidance

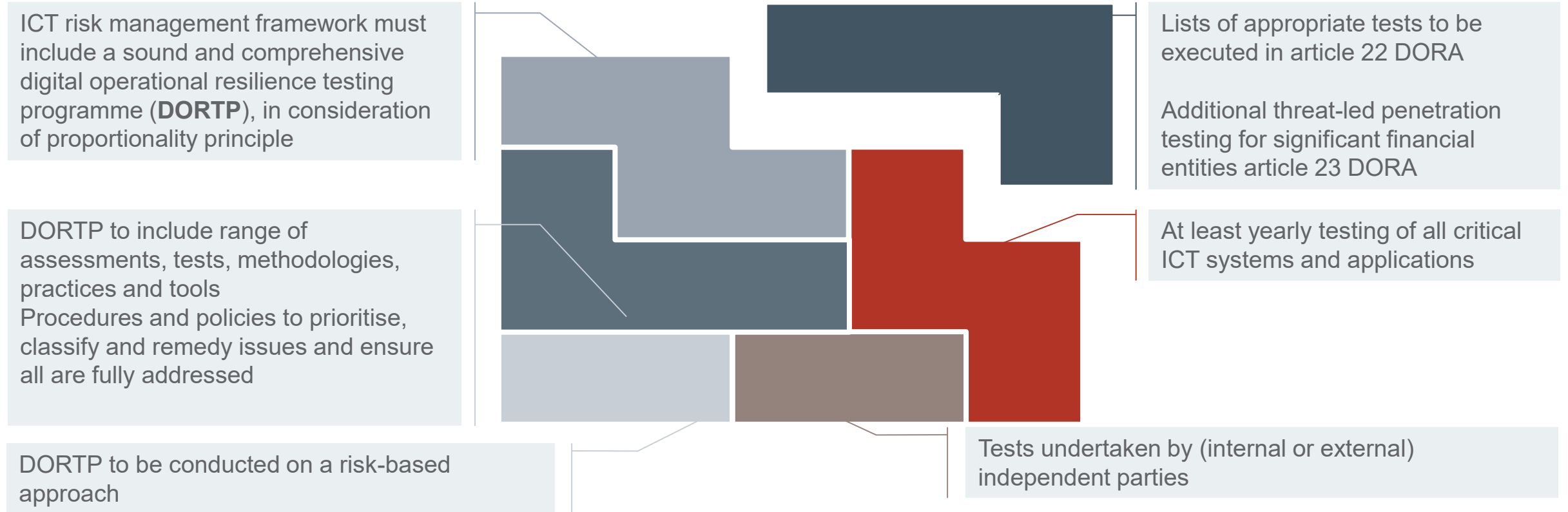
Information to service users/ clients and under other reporting regimes (eg NIS, GDPR) may be necessary in addition to the above reporting

Where the incident has or may have an impact on the financial interests of service users and clients, information without undue delay about the major ICT-related incident and information, as soon as possible, on all measures which have been taken to mitigate the adverse effects of such incident



Digital operational resilience testing

General requirements: testing of ICT tools and systems for all financial entities



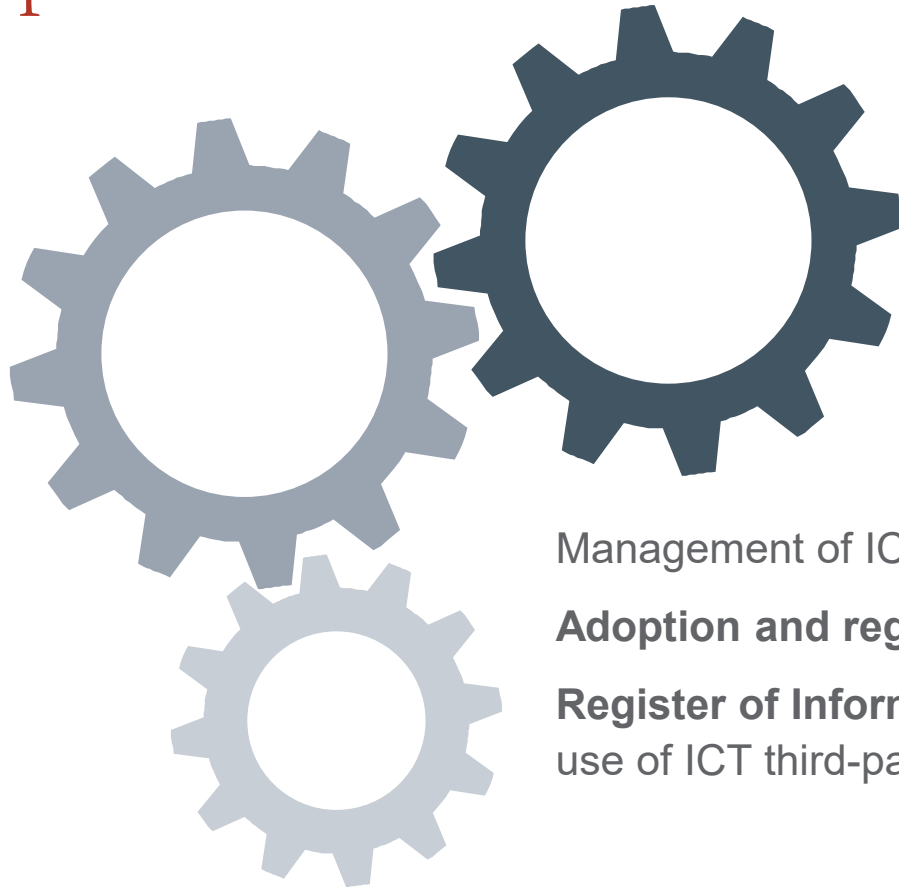


Managing of ICT third-party risk

General principles

Financial entities shall manage **ICT third-party risk** as an **integral component of ICT risk**

Remain fully responsible for the discharge of their obligations



New elements

Strategy on ICT third-party risk

Yearly reporting to authorities re. use of ICT services

Management of ICT third party risk using **proportionality principle**

Adoption and regular review of a strategy on ICT third-party risk

Register of Information in relation to all contractual arrangements on the use of ICT third-party services

Entering into a contractual arrangement

Critical or important functions

1

2

Supervisory conditions

3

Risk identification and assessment (including concentration, sub-outsourcing and third-country risk)

4

Due diligence on third-party service provider

Monitoring of risks and third-party service provider

8

Termination and exit plan

7

6

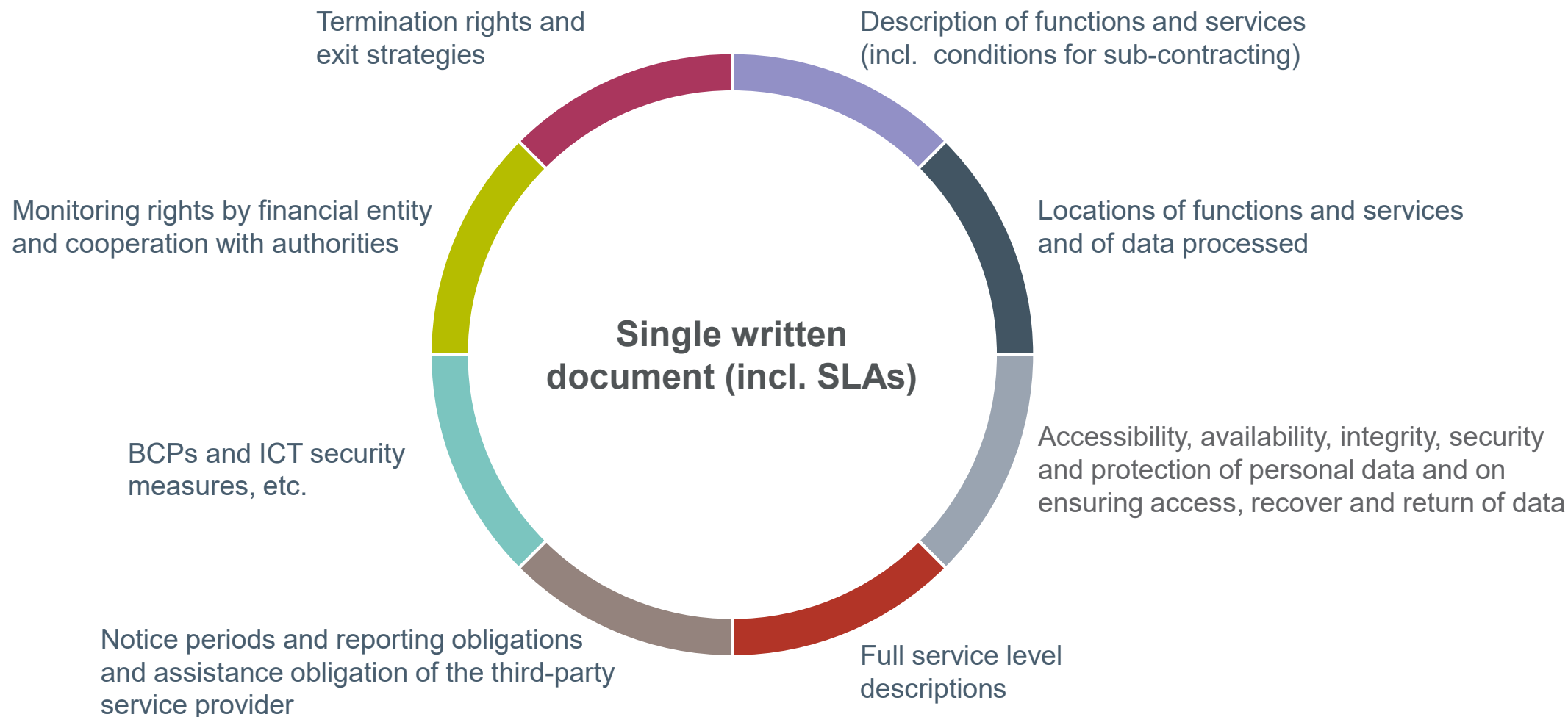
Conclusion of contract

5

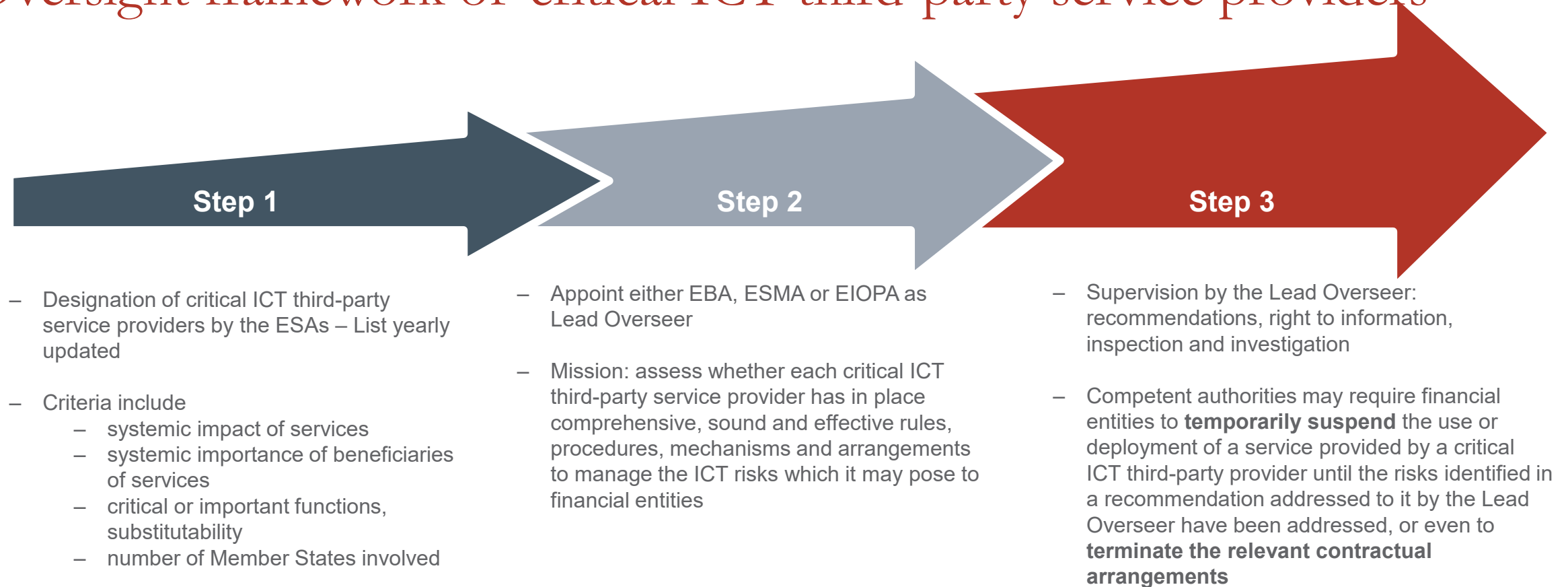
Conflicts of interest

Not possible to use of an ICT third-party service provider established in a third country that would be designated as critical if it was established in the Union

Documentation



Oversight framework of critical ICT third-party service providers



Key takeaways

1 Uplift will vary between sectors – eg banking sector entities may be more familiar with the requirements than AIFMs

2 ICT third-party service providers may now be regulated entities

3 Even if not regulated, ICT third-party service providers may need to adapt their contracting, service provision and pricing to reflect the obligations of their clients

4 Preparation:

- Undertake a GAP analysis early to give time for any compliance build-out
- Specific to business, strategy, financial plan and current regulatory framework
- Look at processes, policies and procedures that you may have to adapt
- Allocate budget and workforce – focus on people competences
- Don't underestimate the complexity of implementation

Questions?

These are presentation slides only. This document is for general guidance only and does not constitute advice.

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. Allen & Overy LLP is a limited liability partnership registered in England and Wales with registered number OC306763. Allen & Overy (Holdings) Limited is a limited company registered in England and Wales with registered number 07462870. Allen & Overy LLP and Allen & Overy (Holdings) Limited are authorised and regulated by the Solicitors Regulation Authority of England and Wales.

The term partner is used to refer to a member of Allen & Overy LLP or a director of Allen & Overy (Holdings) Limited or, in either case, an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings. A list of the members of Allen & Overy LLP and of the non-members who are designated as partners, and a list of the directors of Allen & Overy (Holdings) Limited, is open to inspection at our registered office at One Bishops Square, London E1 6AD.

Allen & Overy is an international legal practice with approximately 5,500 people, including some 550 partners, working in more than 40 offices worldwide. A current list of Allen & Overy offices is available at allenoverly.com/global/global_coverage.

© Allen & Overy LLP 2020