
This webinar will begin shortly.

January 2025 in Sight: DORA State of Play

November 13, 2024

Reminders

- The webinar will be recorded and posted to the FIA website within 24 hours of the live webinar.
- Please use the “question” function on your webinar control panel to ask a question to the moderator or speakers.
- *Disclaimer: This webinar is intended for informational purposes only and is not intended to provide investment, tax, business, legal or professional advice. Neither FIA nor its members endorse, approve, recommend, or certify any information, opinion, product, or service referenced in this webinar. FIA makes no representations, warranties, or guarantees as to the webinar’s content.*

Presenters

Host:

Jean Pierre Salendres, Director of EU Policy, FIA

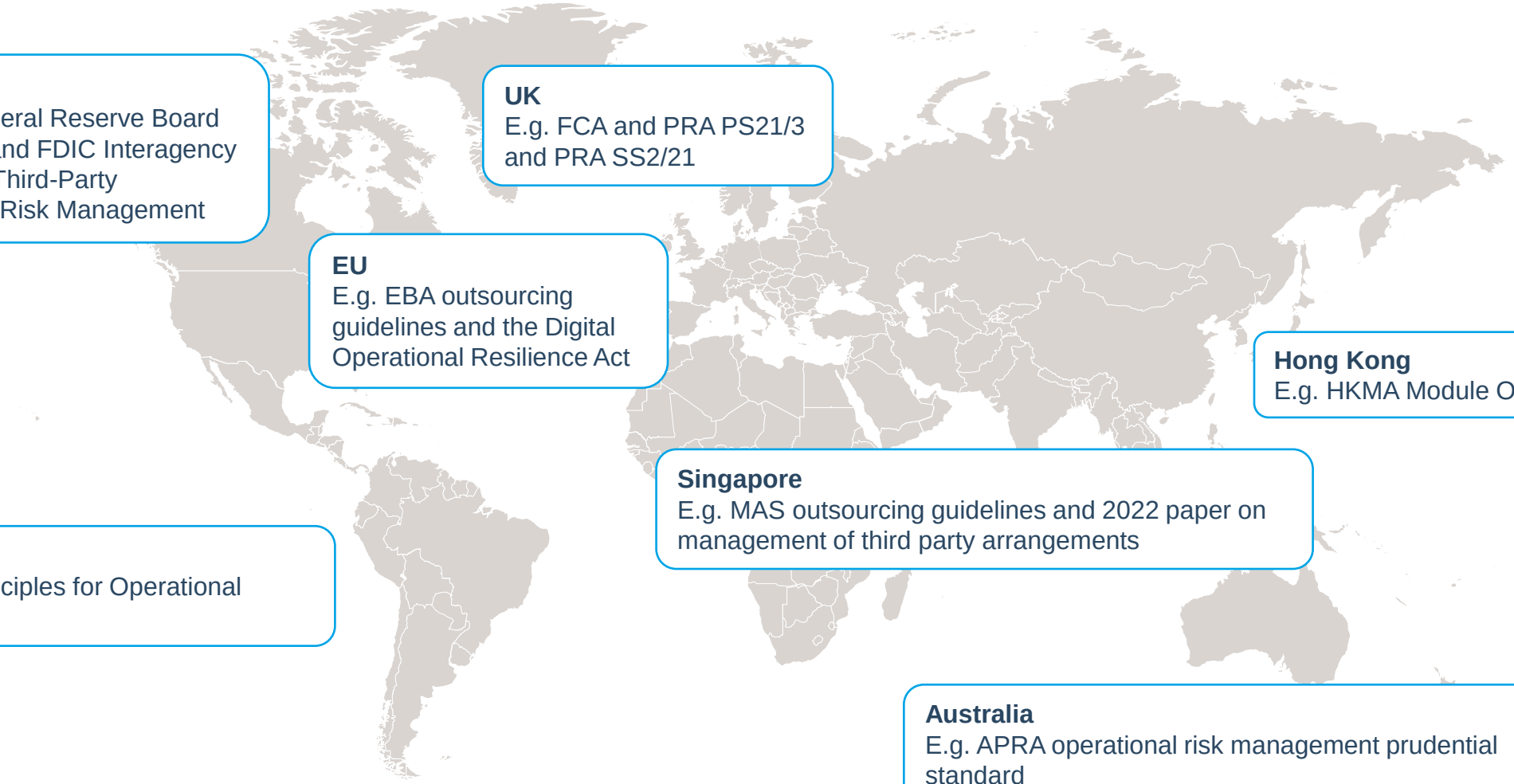
Speakers:

Boris Augustinov, Policy Officer, European Commission, DG FISMA
Raza Naeem, Partner, Linklaters
Simon Treacy, Senior Associate, Linklaters

Presentation prepared by Linklaters

Setting the scene: Comments by
Boris Augustinov, Policy Officer, European Commission, DG FISMA

DORA is part of wider drive to improve operational resilience in financial services



US
E.g. OCC, Federal Reserve Board of Governors and FDIC Interagency Guidance on Third-Party Relationships: Risk Management

UK
E.g. FCA and PRA PS21/3 and PRA SS2/21

EU
E.g. EBA outsourcing guidelines and the Digital Operational Resilience Act

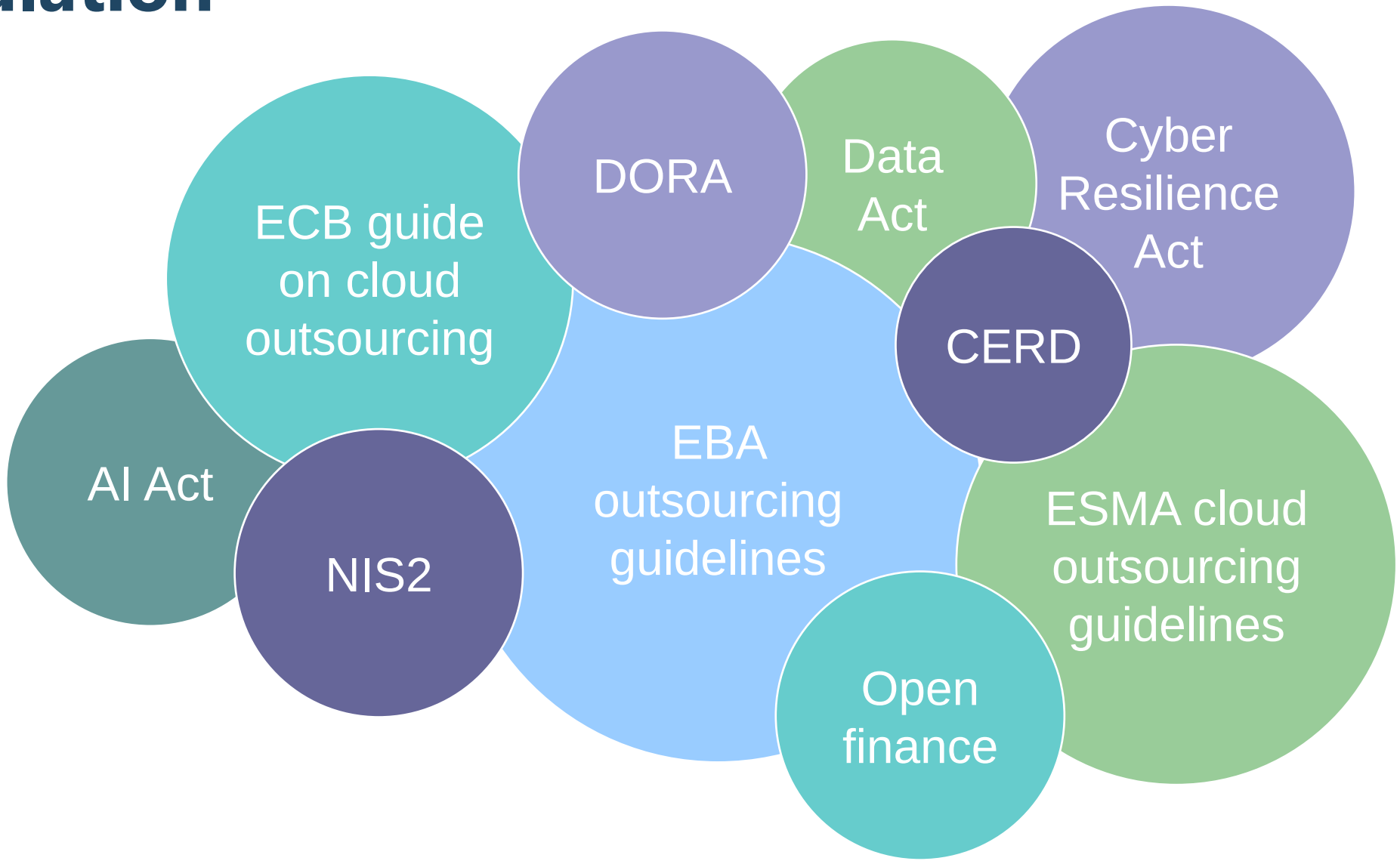
Hong Kong
E.g. HKMA Module OR-2

Singapore
E.g. MAS outsourcing guidelines and 2022 paper on management of third party arrangements

International
E.g. BCBS Principles for Operational Resilience

Australia
E.g. APRA operational risk management prudential standard

DORA is also part of growing field of EU digital regulation



DORA applies to EU firms and critical third parties and impacts other tech firms too

	Impact	Example requirements
EU financial entities	Direct	> ICT risk management framework > Report major ICT incidents > Maintain register of information > Repaper ICT arrangements
Critical ICT third party service providers	Direct	> Oversight framework > Subsidiary requirement > Repaper arrangements with financial entities > Monitor subcontractors
Other ICT third party service providers	Indirect	> Repaper arrangements with financial entities > Monitor subcontractors

DORA in a nutshell

Financial entities

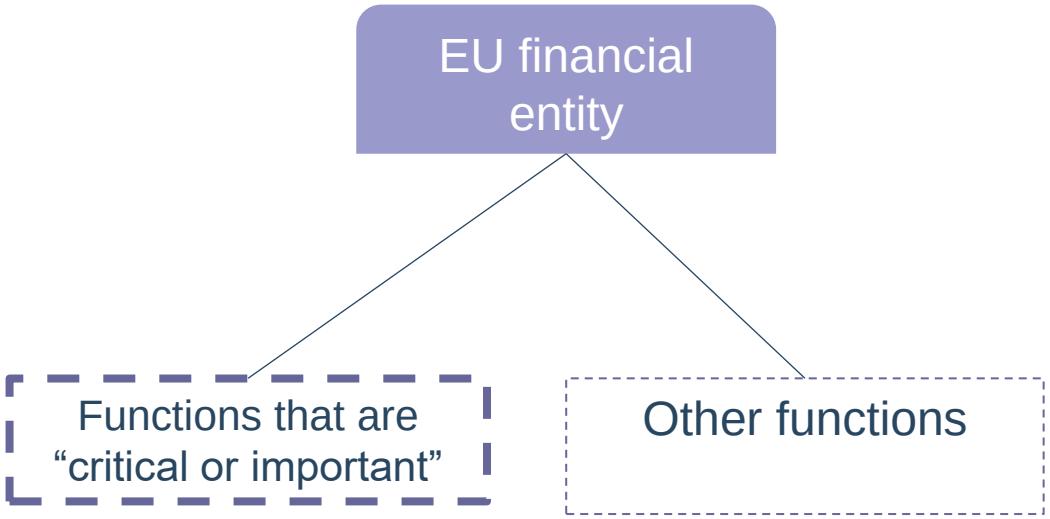
- Risk management
- Reporting ICT-related incidents
- Register of information
- Repapering

Critical ICT third party service providers

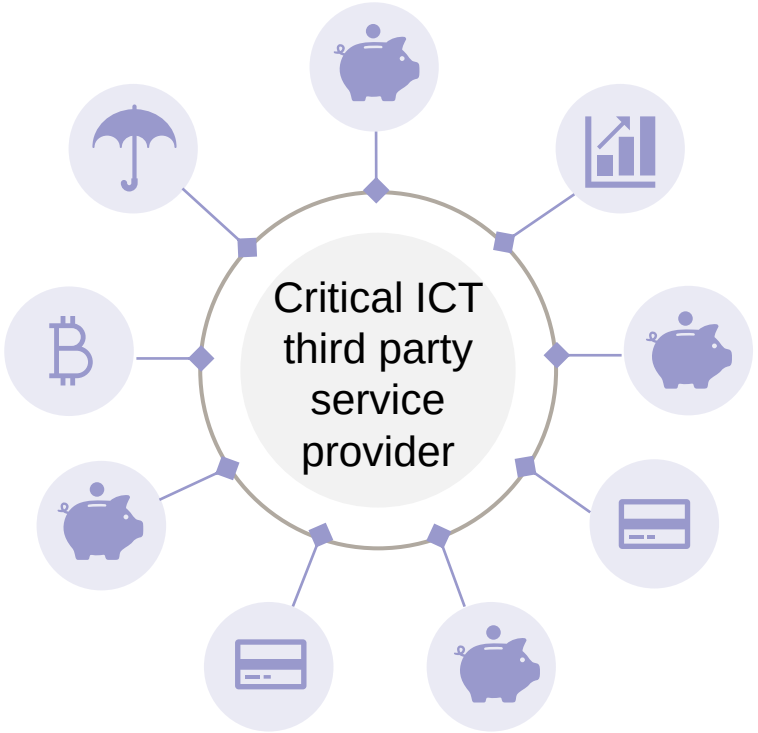
- Oversight framework
- Subsidiary requirement

“Critical” service providers vs. providers supporting “critical or important functions”

Financial entities must distinguish their more important functions from their other functions



Some ICT service providers will be designated as being “critical” to the EU financial system



Designation criteria includes considering extent to which relevant ICT services support CIFs

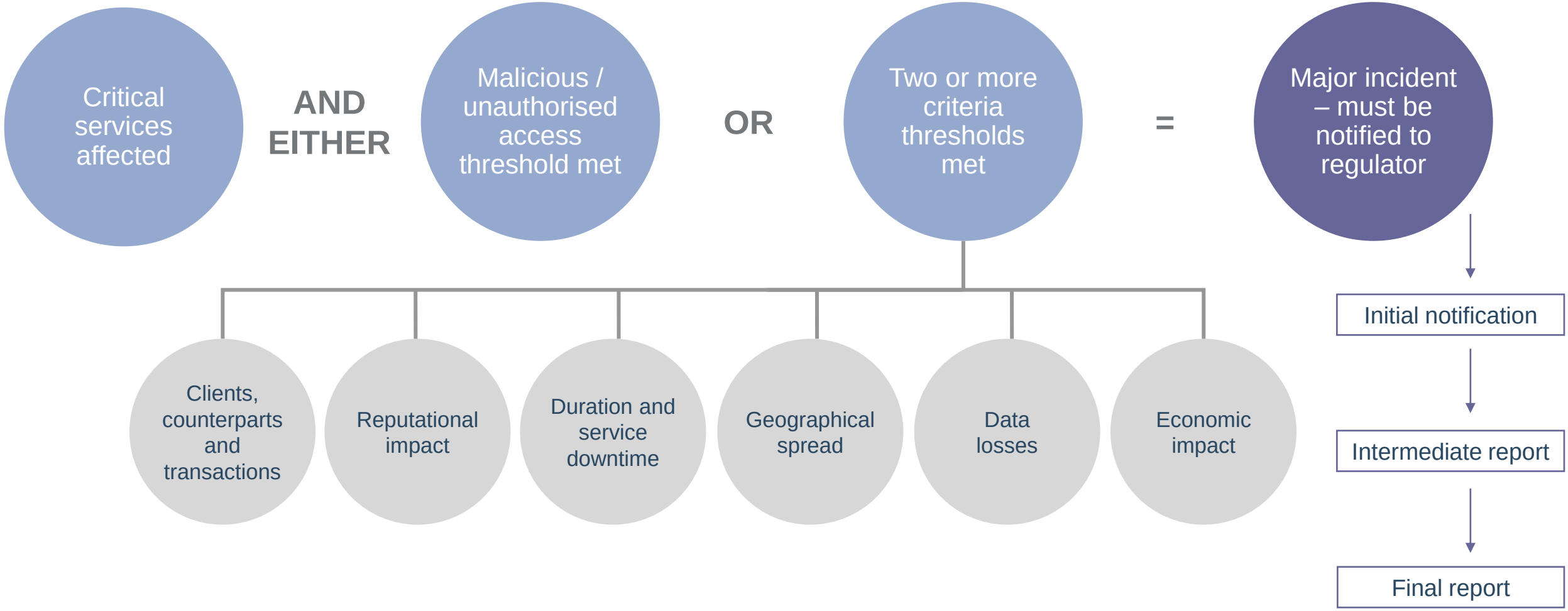
Risk management

ICT risk management framework to include:

- Inventories identifying e.g. ICT assets and ICT-supported business functions
- ICT security policies, procedures, protocols and tools
- ICT Business Continuity Policy
- ICT Response and Recovery Plans
- Digital operational resilience testing programme
- ICT-related Incident Management Policy
- Communication Strategy
- ICT Internal Audit Plans
- ICT Third Party Risk Strategy

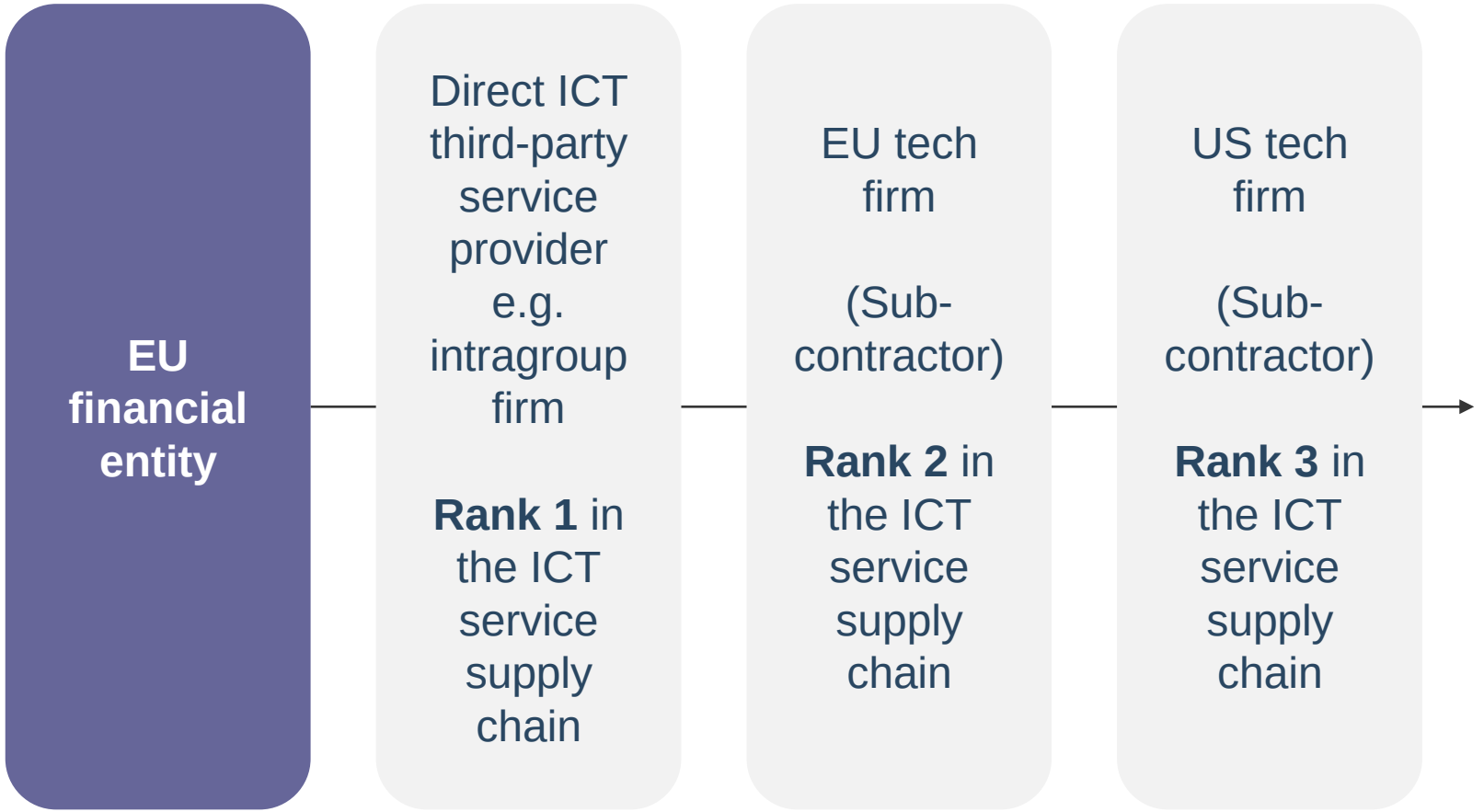
> Documented and reviewed annually
> Approved by management body
> Subject to regular audit review
> Available to regulators on request

Reporting ICT-related incidents



Register of ICT relationships

- Map all ICT contracts and relationships with unique codes and data points
- Distinguish ICT services supporting CIFs
- Available to regulator on request
- Aim: entity and its regulators can oversee ICT relationships and dependencies to facilitate monitoring of ICT risks



Repapering: All ICT services

Conditions for participating in ICT security awareness programmes / digital operational resilience training

Termination rights and minimum notice periods

Description of all functions and ICT services

Obligation on ICT third party service provider to cooperate with firm's regulators

Locations of (sub)contracted functions and ICT services

Obligation on ICT third party service provider to assist in case of ICT incident

Data protection provisions

Service level descriptions

Provisions on recovery of data in case of insolvency / contract termination

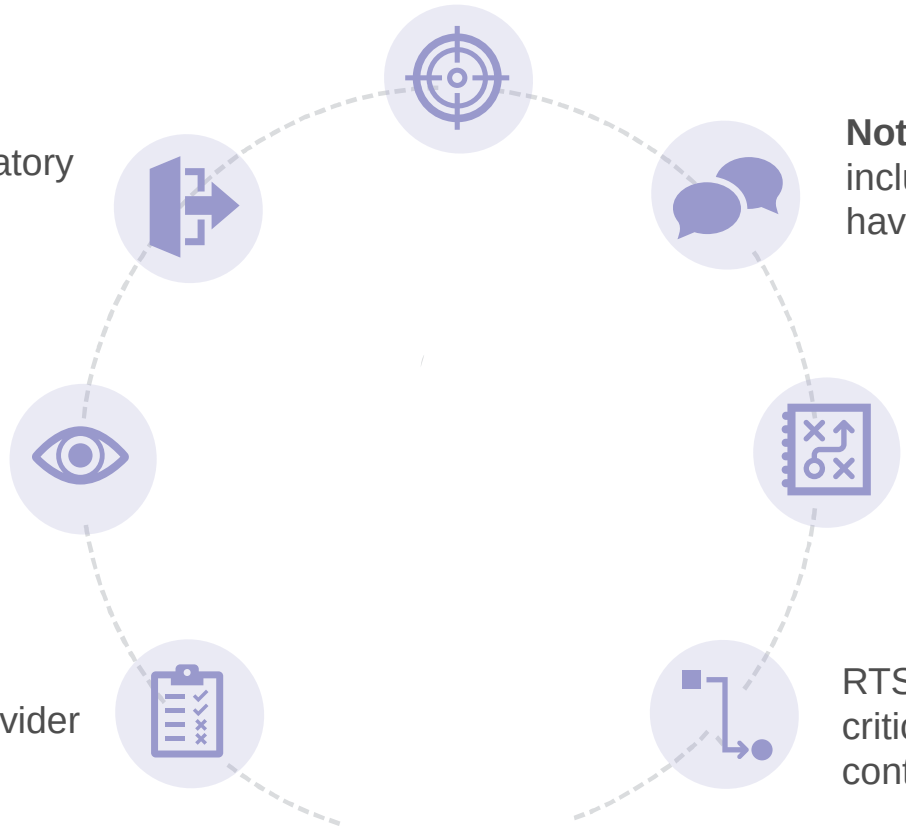
Repapering: ICT services supporting critical / important functions

Full-service level descriptions, including updates and revisions with quantitative and qualitative performance targets within agreed service levels and consequences for non-compliance

Exit strategies, including mandatory adequate transition period

Notice periods and reporting obligations, including notification of developments that might have material impact on the provision of ICT services

Right to monitor on an ongoing basis the ICT third party service providers' performance, including:
> rights of access, inspection and audit,
> right to agree on alternative assurance levels, etc.

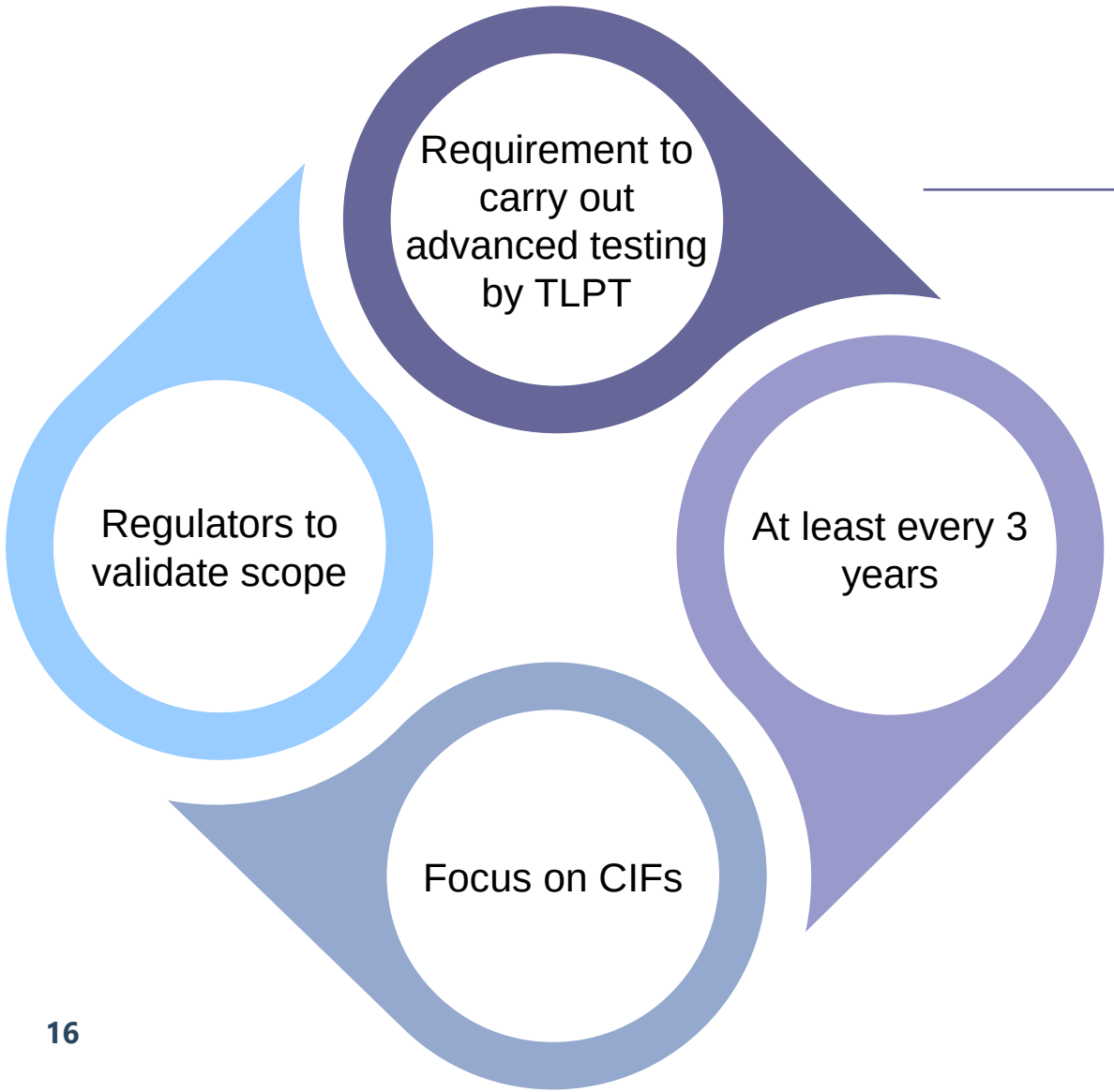


Requirement on ICT third party service provider to implement and test **business contingency plans** and have in place ICT security measures

Obligation on ICT third party service provider to **participate and cooperate in TLPT**

RTS on **sub-contracting** ICT services supporting critical or important functions sets out the contractual terms re subcontractors

Threat led penetration testing



Applies to some types of firm by default

Other firms may be asked to perform TLPT on basis of impact / systemic character / ICT risk-related factors

Oversight framework for critical ICT third party service providers

Designation

- EU level designation regime for critical ICT service providers
- Includes non-EU businesses
- Criticality to be assessed on factors such as:
  - number of EU clients (and their systemic character / importance)
  - criticality of ICT services provided
  - substitutability

Lead Overseer

- Supervisor will be one of ESMA, EIOPA or EBA depending on ICT firm's EU client base
- Lead Overseer to focus on critical services provided to financial sector but may also have jurisdiction over non-critical services
- Lead Overseer will assess ICT risk framework of ICT provider and make recommendations for remedial action

Subsidiary requirement

- Restriction on financial entities using services of ICT third party service provider with no EU subsidiary within 12 months of designation as critical
- DORA does not require technology or data localisation within the EU and ICT services or technical support can still be provided from non-EU jurisdiction
- Lead Overseer will likely have expectations regarding technical specialists, governance / board and control functions

DORA implementation FAQs

1. Scope of ICT services
2. Identifying critical or important functions
3. Intragroup impact
4. Governance requirements
5. Repapering exercise
6. ICT-related incident reporting
7. DORA register

Next steps


DORA applies as of 17 January 2025
Some Level 2 technical standards remain outstanding
Day 1 / Day 2 compliance?
Engagement with national regulators
Designation of critical ICT third party service providers

Get in touch

Raza Naeem

Financial Regulation Group,
Partner, London

Tel: + 44 20 7456 5272

raza.naeem@linklaters.com

Simon Treacy

Financial Regulation Group,
Senior Associate, London

Tel: + 44 20 7456 2451

simon.treacy@linklaters.com

One Silk Street
London EC2Y 8HQ
Tel: (+44) 20 7456 2000
Fax: (+44) 20 7456 2222

www.linklaters.com

Thank you for joining us today!

Upcoming Webinar:

EMIR 3.0: Key Requirements and State-of-Play
02:00 – 03:15 PM GMT

Self-Reporting in the Age of Whistleblowers
10:00 – 11:00 AM ET


FIA