Preparing Luxembourg's Financial Sector for DORA Compliance by January 2025

FTL annual conference_18/11/2024

Ana-Maria Fimin/ European Commission

DORA – main pillars

ICT risk management

- Set of key principles and requirements on ICT risk management framework

ICT-related incident reporting

- Harmonise and streamline reporting + extend reporting obligations to all financial entities

Digital operational resilience testing

- Subject financial entities to basic testing or advanced testing (e.g. TLPTs)

ICT third-party risk

- Principle-based rules for monitoring third-party risk, key contractual provisions + oversight framework for critical ICT TPPs

Information sharing

- Voluntary exchange of information and intelligence on cyber threats

DORA-implementation phase &policy mandates

ICT risk framework (Chapter II)

- RTS on ICT Risk Management framework (Art.15)
- RTS on simplified risk management framework (Art.16.3)
- Guidelines on the estimation of aggregated costs/losses caused by major ICT related incidents (Art. 11.1)

ICT related incident management classification and reporting (Chapter III)

- RTS on criteria for the classification of ICT related incidents (Art. 18.3)
- RTS to specify the reporting of major ICT-related incidents (Art. 20.a)
- ITS to establish the reporting details for major ICT related incidents (Art. 20.b)
- Feasibility report on further centralisation of incident reporting through the establishment of a single EU hub for major ICT-related incident reporting (Art. 21)

Digital Operational Resilience Testing (Chapter IV)

- RTS to specify threat led penetration testing (Art. 26.1)

Third-party risk management (Chapter V.I)

- ITS to establish the templates of register of information (Art.28.9)
- RTS to specify the policy on ICT services performed by third-party (Art.28.10)
- RTS to specify the elements to determine and assess when sub-contracting ICT services supporting a critical or important function (Art.30.5)

Oversight framework (Chapter V.II)

- Call for advice on criticality criteria (Art. 31.8) and fees (Art. 43.2)
- Guidelines on “CAs-ESAs cooperation” regarding DORA oversight (Art. 32.7)
- RTS on “oversight conduct” (Art. 41)

➢**DORA entered into force 17 Jan 2023** (2 years for application)

➢**DORA will apply from 17 Jan 2025**

ESAs need to deliver **12 joint policy mandates within 12-18 months** from entry into force+ the call for advice on criticality criteria and fees

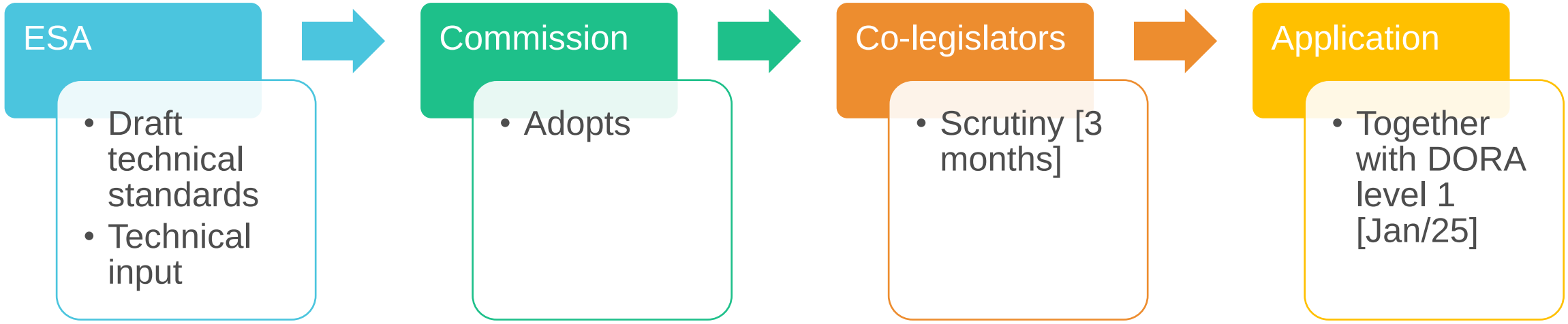
European Commission

Status of policy mandates

Art	DORA policy work	WG	ESA Lead	Status	ECB/ENISA involvement	DL	Month	Last milestone at WG level	JS SC DOR	BoSs (2)
15	**RTS on ICT risk management framework**	1	ESMA	PC ended	ENISA (consulted)	**Jan-24**	**12**	28-Apr-23	**16-May-23**	WP (5-15 June)
16	**RTS on simplified ICT risk management framework**	1	ESMA	PC ended	ENISA (consulted)	**Jan-24**	**12**	28-Apr-23	**16-May-23**	WP (5-15 June)
18.3	**RTS on criteria for the classification of ICT-related incidents**	2	EBA	PC ended	ENISA and ECB (consulted)	**Jan-24**	**12**	28-Apr-23	**16-May-23**	WP (5-15 June)
28.9	**ITS to establish the templates for the Register of information**	3	EIOPA	PC ended	na	**Jan-24**	**12**	28-Apr-23	**16-May-23**	WP (5-15 June)
28.1	**RTS to specify the policy on ICT services performed by 3rd party**	1	EBA	PC ended	na	**Jan-24**	**12**	28-Apr-23	**16-May-23**	WP (5-15 June)
31.8	**Call for advice on criticality criteria**	3	EIOPA	Delivered	na	**Sep-23**	**9**	31-Mar	**18-Apr-23**	WP early May
43.2	**Call for advice on oversight fees**	3	ESMA	Delivered	na	**Sep-23**	**9**	31-Mar	**18-Apr-23**	WP early May
na	**ESRB recommendation - interim A(1) and B**	2	EIOPA	Delivered	ECB and ESRB (together)	**Jul-23**	**6**	28-Apr-23	**16-May-23**	WP (5-15 June)
20.a	**RTS on specifying the reporting of major ICT-related incidents**	2	EBA	On-time	ENISA and ECB (consulted)	**Jul-24**	18	06-Oct	24-Oct-23	WP (10 -24 Nov)
20.b	**ITS to establish the reporting details for major ICT-related incidents**	2	EBA	On-time	ENISA and ECB (consulted)	**Jul-24**	18	06-Oct	24-Oct-23	WP (10 -24 Nov)
21	**Feasibility report on single EU Hub for major ICT-related events**	2	ESMA	On-time	ENISA and ECB (consulted)	**Jan-25**	18 (1)	06-Oct	24-Oct-23	WP (10 -24 Nov)
11.11	**Guidelines on the estimation of aggregated costs/losses caused by major ICT related incidents**	2	EBA	On-time	na	**Jul-24**	18	06-Oct	24-Oct-23	WP (10 -24 Nov)
26.11	**RTS to specify threat led penetration testing aspects**	1	CA led	On-time	ECB (in agreement)	**Jul-24**	18	06-Oct	24-Oct-23	WP (10 -24 Nov)
30.5	**RTS to specify elements when sub-contracting critical or important functions**	1	EBA	On-time	na	**Jul-24**	18	06-Oct	24-Oct-23	WP (10 -24 Nov)
32.7	**GL on cooperation between ESAs and CAs regarding the structure of the oversight**	3	EIOPA	On-time	na	**Jul-24**	18	06-Oct	24-Oct-23	WP (10 -24 Nov)
41	**RTS to specify information on oversight conduct**	3	EIOPA	On-time	na	**Jul-24**	18	06-Oct	24-Oct-23	WP (10 -24 Nov)

Level 2 – process

Link to adopted acts: https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en



ICT third-party risk

(Articles 25 to 39)

Harmonisation of key elements of relationship with ICT third-party service providers

- Minimum aspects - core areas
- Complete monitoring of ICT third-party risk conclusion, performance, termination and post-contractual stages of contractual arrangements

Union Oversight framework for critical ICT third-party service providers

- Designation by the ESAs
- ESAs as Lead Overseers with powers to monitor
- Oversight Forum - cross-sectoral coordination on all ICT risk matter and preparatory work for individual decisions and collective recommendations

Contractual arrangements

(Articles 25-27)

General principles

- Financial entities' full responsibility
- Proportionality
- ICT third-party risk strategy
- Documentation and evidence
- Register of Information
- Pre, during and post contractual principles

Preliminary assessment of ICT concentration risk

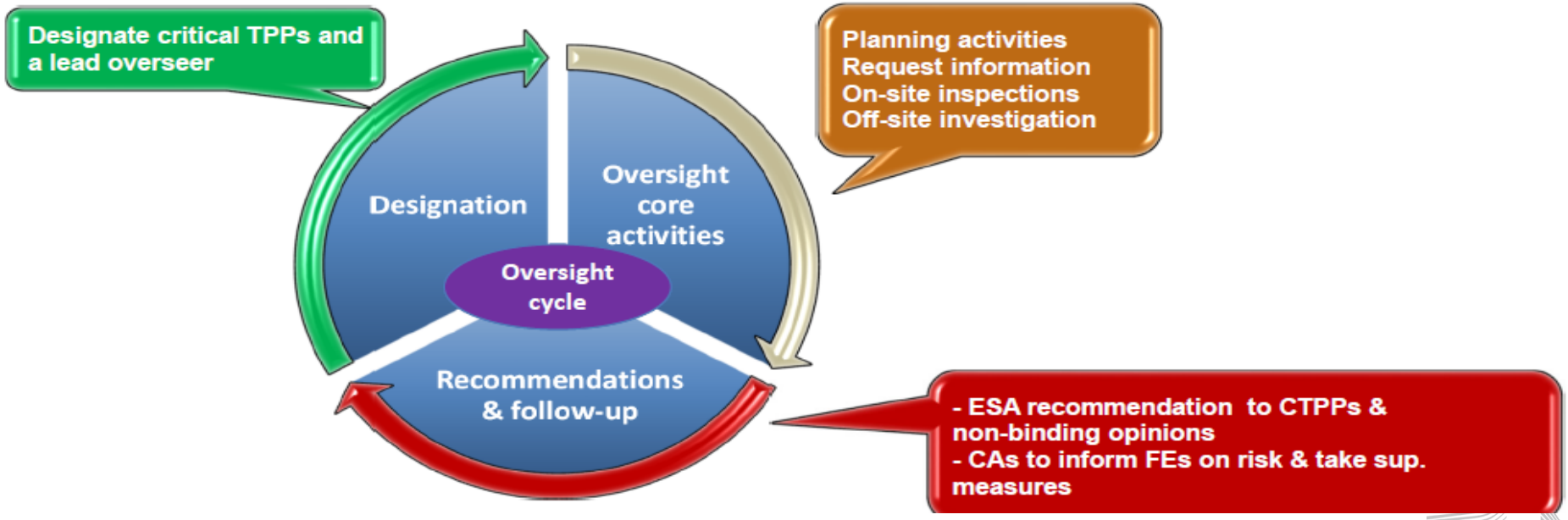
Key contractual provisions

- Description of all functions and services, service level
- Indication of location and storage of data
- Accessibility, availability, integrity, security and protection of personal data
- Full service descriptions
- Notice periods and reporting obligations of the third party provider
- Assistance by the third party provider
- Right to monitor
- Termination and exit strategies

DORA – Oversight framework

Digital Operational Resilience Act (6)
ESAs oversight activities

Objective – assessment of whether CTPPs have in place comprehensive, sound and effective rules, procedures and arrangement to manage the ICT risks, which may be posed to financial entities.



European Commission

Oversight framework

Financial entities **establish and update a Register of Information (RoI)** with all contractual arrangement on the use of ICT services provided by ICT TPPs

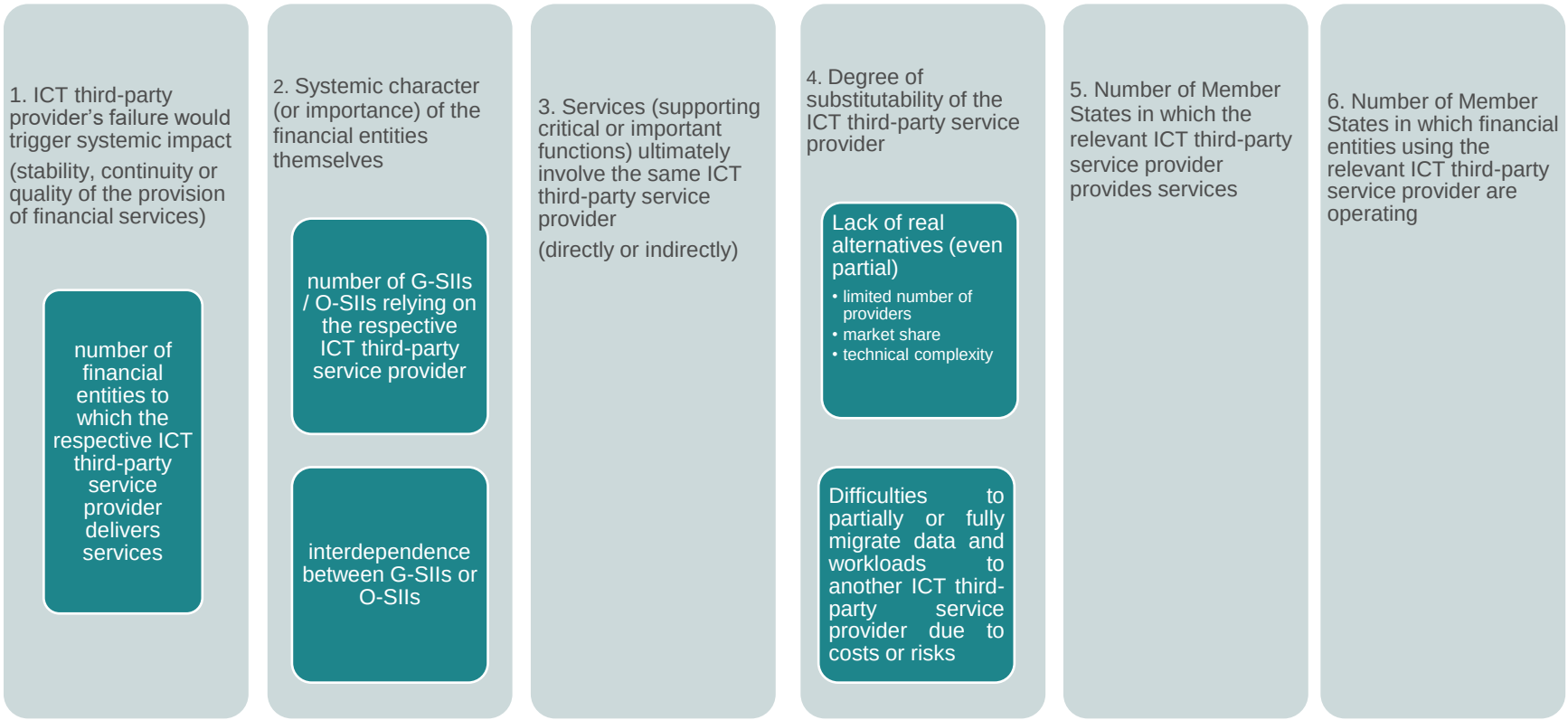
Financial entities **make available the RoI to the Competent Authorities** / report at least on a yearly basis on the **new contractual arrangements**

Competent authorities send on a yearly and aggregated basis the reports received to the **Oversight Forum** (OF support the work of the Joint Committee of ESAs and the LOs)

Designation by the ESAs, though Joint Committee of ESAs and upon recommendation from the OF, based on a set of **criteria (exemptions + voluntary opt-in)**

Oversight framework

(Article 28) Designation of critical ICT third-party providers (CTPPs) by the ESAs



European Commission

Oversight framework
(Article 28) continuation

EXEMPTION

Designation does not apply to ICT third-party service providers subject to oversight frameworks established for the purposes of supporting Treaty objectives referred to in Article 127(2) TFEU

VOLUNTARY OPT-IN

ICT third-party service providers not included may request to be subject to the Framework

LEAD OVERSEER

One ESA is appointed as Lead Overseer for each critical ICT third-party provider

(based on the value of assets of financial entities in the remit of the respective ESA)

Oversight framework (part 2)

ESAs (EBA, ESMA and EIOPA) act as **Lead Overseers (LOs)**

Critical ICT TPP – establish a subsidiary in the EU once becomes critical

LOs powers and tasks - perform **inspections and investigations**, assisted by **Joint Examination teams** + LOs perform inspections and investigations outside the EU

LOs powers and tasks – e.g. **issue recommendations to CTPPs** + **penalties** for not cooperating

Oversight framework (part 3)

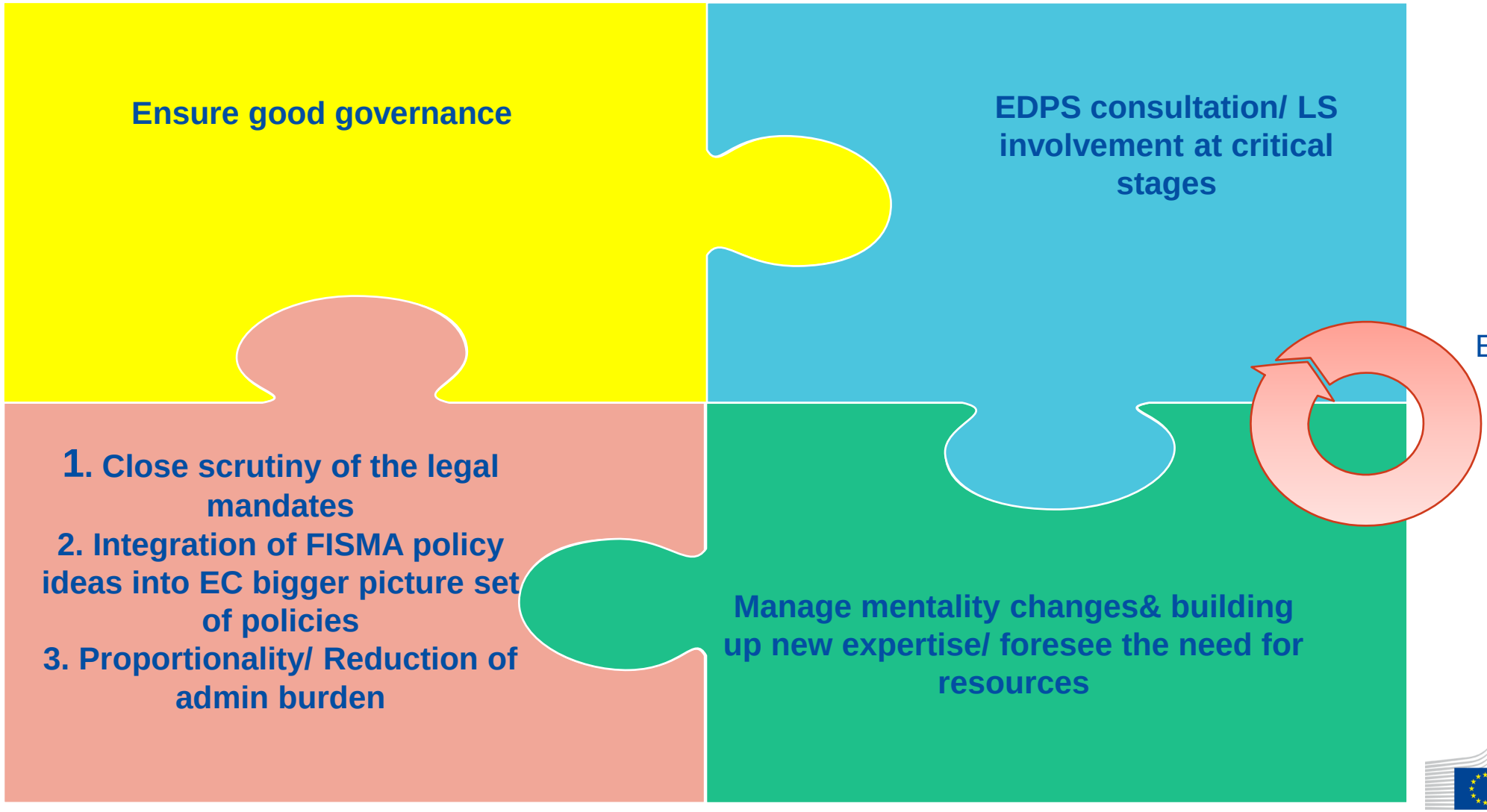
Joint Oversight Network – to ensure enhanced coordination among the LOs

Competent authorities – enforce the recommendations through financial entities

Oversight fees – to cover LOs necessary expenditure in relation to the conduct of oversight tasks

International cooperation – to conclude administrative arrangements with 3rd country regulatory and supervisory authorities to foster international cooperation

DORA level II phase- lessons learnt



Elements to have in mind

Thank you

ana-maria.fimin@ec.europa.eu

European Commission